

Master of Science in Internetworking

MINT 709 - Capstone Project Report

Extensive Penetration Testing to Secure Network Devices

Prepared by : Mohammad AlzobiDirector: Dr. Mike MacGregor, Director of MINT program at University of AlbertaReader: Raghavendra Jayaraman

Table of Contents

Table of Contents
1. Introduction
2. Problem Description
2.1 Password cracking
2.2 Web Server Scanning
2.3 SNMP Enumeration
2.4 SSL/TLS scanning
2.5 Protocol flooding
2.6 Web Server Stressing
2.7 Brute force directory & files
2.8 Fuzzing
3. Methods of Examination
3.1 Password cracking using MEDUSA
3.2 Web server scanning using NIKTO and SKIPFISH6
3.3 SNMP enumeration using SNMP Check
3.4 SSL/TLS scanning using SSLScan and TLSSLED7
3.5 Protocol flooding using UDP.pl and Hping37
3.6 Web server stressing using SIEGE
3.7 Brute force directory & files using DIRB
3.8 Fuzzing using SPIKE, BED, SICKFUZZ, SFUZZ,9
4. Analysis of Results9
4.1 Analysis of Router Results9
4.1.1 Router Password cracking Analysis (MEDUSA)9
4.1.2 Router Web server scanning Analysis (Router NIKTO, Skip fish)11
NIKTO11
SKIPFISH12
4.1.3 Router SNMP Enumeration Analysis (SNMP Check)14
4.1.4 Router SSL/TLS Scanning Analysis (SSL Scan, TLSSLED)15
4.1.5 Router Protocol Flooding Analysis (UDP.pl, Hping3)16
UDP.pl Flood Attack16
Hping3 SYN Attack17
4.1.6 Router Web Server Stressing Analysis (SIEGE)18
4.1.7 Router Brute Force Directory and files Analysis (DIRB)

4.1.8 Router Fuzzing Analysis (BED, SPIKE, SICKFUZZ, SFUZZ)	20
BED	20
SPIKE	20
SICKFUZZ	21
SFUZZ	22
4.2 Analysis of Switch Results	22
4.2.1 Switch Password cracking Analysis (MEDUSA)	22
4.2.2 Switch Web server scanning Analysis (NIKTO, Skip fish)	23
NIKTO	23
SKIPFISH	23
4.2.4 Switch SSL/TLS Scanning Analysis (SSL Scan, TLSSLED)	25
SSLSCAN/ TLSSLED	25
4.2.5 Switch Protocol Flooding Analysis (UDP.pl, Hping3)	25
UDP.pl Flood Attack	25
Hping3SYN Attack	26
4.2.6 Switch Web Server Stressing Analysis (SIEGE)	27
4.2.7 Switch Brute Force Directory and files Analysis (DIRB)	28
4.2.8 Switch Fuzzing Analysis (BED, SPIKE, SICKFUZZ, SFUZZ)	28
BED	
SPIKE	29
SICKFUZZ	29
SFUZZ	29
5. Conclusions and Recommendations	
Countermeasures against Password Cracking Tools	
Countermeasures against Vulnerabilities Reported During Web Server Scanning	
Ways to secure SNMP communication in the network	
Measures to improve SSL/TLS communication performance	
Countermeasures against Flooding Attacks	
Additional security measures to improve the overall network security	
Appendices	A
Appendix A - Password cracking tests screen shots	A
Router test screen shot	A
Router website show version command	A
Router wireshark screen shot	В
Switch test screen shot	В

Switch website show version commandC
Appendix B - Web server scanning tests screen shotsD
Router Nikto test screen shotD
Router Nikto test outputD
Router Skipfish test screen shotF
Switch Nikto test screen shot G
Switch Nikto test output example G
Switch Skipfish test screen shotH
Appendix C - SNMP enumeration tests screen shotsI
Router SNMP enumeration test screen shotI
Switch SNMP enumeration test screen shotI
Appendix D - SSL/TLS scanning tests screen shotsJ
Router SSLSCAN test screen shotJ
Router TLSSLed test screen shot1J
Router TLSSLed test screen shot2K
Switch SSLSCAN test screen shotK
Switch TLSSLed test screen shotL
Appendix E - Protocol Flooding tests screen shotsM
Switch UDP.pl test wireshark screen shotM
Appendix F - Web Server stressing test screen shotsN
Router SIEGE 15 users test screen shot N
Router SIEGE 100 users test screen shot N
Switch SIEGE 15 users test screen shot O
Switch SIEGE 100 users test screen shot O
Appendix G - Brute Force Directory and file test screen shotsP
Router DIRB screen shotP
Switch DIRB screen shotP
Appendix H - Fuzzing tests screen shotsQ
Router BED screen shot1 Q
Router BED screen shot2Q
Router BED No buffer FailuresR
Router SPIKE test screen shotR
Router SPIKE test No buffer failuresS
Router SICKFUZZ test screen shot
Router SICKFUZZ test buffer failuresT

	Router SFUZZ test screen shot	Т
	Router SFUZZ test No buffer failures	. U
	Switch BED screen no buffer failures	. U
	Switch SPIKE test screen shot	V
	Switch SPIKE test no buffer failures screen shot	V
	Switch SICKFUZZ test screen shot	W
	Switch SICKFUZZ test buffer failures screen shot	W
	Switch SFUZZ test screen shot	Х
	Switch SFUZZ test No buffer failures screen shot	Х
A	ppendix I - References	Y

1. Introduction

Network security is an integral part of network planning. Today, networks are prevalent in almost all forms of communications and transactions through internet use, accessing bank accounts at ATM machines, to sending faxes, or even when placing a phone call. Enterprises and institutions are increasing their dependency on networks between their branches in different cities and even across different countries. It is more evident than ever that these networks need to be secured from intruders and hackers to prevent access to personal account data and confidential information. As long as hackers are on the rise, there will always be an increase in demand for effective network security.

Communications at the lowest layers of a network are performed using routers and switches via routing and directing packets. Existing commercial vulnerability scanners produce loads of information on vulnerabilities reflected in isolation. However, these scanners only provide limited ideas as to how attackers might combine them to perform an attack. One method of examining the level of security is by Penetration Testing, a method which is used to evaluate network security by simulating hacker attacks. A hacker can be an outsider who is not authorized to access the network, or an insider with limited access. Therefore, a penetration test is mandatory for network devices before deploying them in the network to enhance security.

The purpose of this project is to use the Penetration Test to find the weaknesses related to network security as a result of improper or poor configurations, and either software or hardware limitations, or both, related to a router and a switch. The results of the Penetration Test are used to provide system owners and organization executives with a better idea of the status of their networks which will help them to improve their network infrastructure and security. The importance of the Penetration Test lies in the fact that it can identify high risk vulnerabilities that might be difficult to detect with commercial scanning software. It will also identify high risk vulnerabilities that are a result of multiple lower risk vulnerabilities if performed in a certain sequence.

There are two types of Penetration Tests that can be performed; the White Box test or the Black Box test. With the White Test, the testers will have physical access to the devices, knowledge of the infrastructure, network mapping and IP addressing information. With the Black Box test, the tester will not have physical access or information about the devices and will play the role of an uninformed attacker trying to gather information about the target over the web and other information gathering methods. The type of Penetration Test used in this project is the White Box Penetration test, with access to the router and switch under test via fast ethernet ports and known IP addresses for both devices.

There are various benefits of performing the White Box Test, such as:

- Maximizing the time to perform the tests
- A through security test
- Test different areas that a Black box test would not be able to reach
- Identifying existing vulnerabilities and categorizing them

In most of the tests performed, the main focus was given to the HTTP server on both devices. The findings and recommendations from these tests will help the client repair any vulnerability and miss configurations and avoid costs associated with network down time.

2. Problem Description

Various tests will be conducted to cover the most common vulnerabilities used by hackers. These tests will reveal the following:

- Router/switch weaknesses and vulnerabilities;
- Different ways attackers can gather information;
- Configuration flaws;
- Identification of missing software and IOS updates that may be required.

The results will also show how an attacker can use the weaknesses and vulnerabilities discovered to exploit, and either control the system or cause service interruption like Denial of Service.

2.1 Password cracking

Password cracking is one of the most destructive exploit methods. If carried out successfully, an attacker with a valid username and password can cause grave damage that might be irreversible, especially if that compromised account is an administrator or a privileged account. The process of password cracking might not be straight forward and might take a very long time depending on the level of security implemented on the target.

One type of password cracking is a Brute Force password. In this type, a tool can be used to try all possible keys in order to decrypt the password. This type of password cracking can take a very long time depending on the number of bits used for the key and the speed of the computer processor. Another type of password cracking is dictionary attack, this type might take less time; it is a technique that successively tries all words from a list that contains millions of possible usernames and passwords. If none of the words in the list matches any of the target user's credentials, then the attack will not be successful.

2.2 Web Server Scanning

Web server scanning tools are used to scan the web server for vulnerabilities and weaknesses which can be used to exploit the server. These tools are automated where the attacker runs the tool and waits for the report. The report lists all the vulnerabilities applicable to the server. An example of some of the vulnerabilities that can be found using these tools are Cross-Site-Scripting (XXS), Cross-site Request Forgery (XSRF) and Click Jacking. It also might reveal insecure server configurations.

2.3 SNMP Enumeration

Simple Network Management Protocol (SNMP) is an application layer protocol used by administrators to monitor and manage devices such as routers, switches and servers on the network directly or via a network management system. An administrative computer called "manager" sends requests using UDP to the agent's port 161 and receives the response from the agent on port 162. The agent is software running on the managed device.

SNMP is not enabled by default on the routers/switches. The administrator can enable SNMP and assign communities, like read and write community strings, depending on the SNMP version used. Administrators should make sure to change these communities as an attacker may try them to collect information about the devices. The problem with the public and private communities is that they are the most commonly used community strings. SNMP uses UDP protocol which is a clear text protocol; as a result it is vulnerable to Spoofing attacks and it can allow attackers to use "sniffers" to collect important information about the system.

2.4 SSL/TLS scanning

Secure Socket Layer and Transport Layer Security, or SSL and TLS, are both protocols being used to secure websites from unauthorized users trying to access sensitive information. The idea behind these protocols is to encrypt the data being transmitted between the client and the server during the user's session. SSL is widely used over the internet since it is able to secure transmissions over TCP. One example of a SSL application is HTTPS, which is a clear-text HTTP protocol that is secured by using SSL or TLS tunnels. Both SSL and TLS use encryption to provide communication privacy and certificates for authentication. An attacker can use SSL scanner to discover what weak ciphers the server supports and then use that knowledge to exploit the server. The use of weak ciphers can compromise the web server's security.

The use of certificates on the server side will ensure clients that the server is legitimate. The digital certificates can be acquired from Certificate Authority, or CA. SSL uses public key cryptography for data encryption. The web server will have a public key and a private key. The public key can be published while the private key is kept on the server. When a client uses that server's public key to encrypt the data, only then will the server decrypt that data with its private key. The role of the certificate authority is to secure the initial communication between client and server until the "hand shaking" is complete. At this point, the client and server can then communicate directly.

Certificates work by the web server first creating public and private keys then apply to have a certificate from an authorized third party (CA). The third party then provides the web server with a new public key that has information that validates the server's identity. The information will be encrypted using the third party's private key. When a client communicates with the web server, the web server sends back the public key provided from the third party and information about what ciphers (encryption algorithms) it supports. CA's are usually trusted by default on most internet browsers, which will have predefined public keys for the CA's. The client browser decrypts the message received from the server and verifies that the public key from the server is

actually from a trusted CA. The client then chooses one of the supported ciphers from the list it received from the server for encryption method. It then generates a password to be used with that particular cipher. This password is then encrypted using the server's public key and sent to the server. The server will be the only one that can decrypt the password with its own private key. The client/server can then start transmitting and receiving encrypted data using the password and cipher for decryption. This way, no one else can decrypt the data since they do not know the password or the cipher being used.

2.5 Protocol flooding

Protocol flooding is a form of attack that will result in Denial of Service (DoS). The idea behind the attack is to send hundreds of thousands of packets to the target with malformed requests. This will result in the target resources consumed trying to respond to all of these requests. During the attack, legitimate requests sent from normal users to the server will be timed out.

There are different types of DoS attacks such as UDP flooding attack. This attack uses UDP protocol which is a session-less and connectionless protocol. In this type of protocol flooding, the attacker will send a large number of UDP packets with malformed data to a certain or random UDP port on the target. The target resources will be consumed so fast trying to respond to these random requests.

Another type of protocol flooding is TCP SYN flood attack. In this type of attack, the attacker will send large numbers of sync messages to the target. The target will reserve space for each of these messages and change the connection state to "SYN-RCVD" and send back "SYNK-ACK" messages. In response, the attacker will ignore these and will not send the final ACK message to the server, resulting in a large number of half open TCP connections. Therefore, the target will eventually reach its valid TCP connection limit resulting in DoS.

2.6 Web Server Stressing

Web Server Stress testing checks the web server's ability to handle concurrent users and checks its stability and performance. An attacker can use an overload attack that will result in service disruption.

The server's performance can be measured as follows:

- Number of requests handled per second;
- Response time;
- Availability percentage;
- Throughput.

2.7 Brute force directory & files

Sometimes files on the web server will not be linked anywhere, so unless one knows the directory and file name they might not be able to access them. The files and directories might be left unlinked intentionally as security by the administrator.

An attacker will use the Brute Force Directory attack to attempt guessing and locating directories on the web server that are not meant for public access. The tool will try to find existing directories on the web server by reading a large list that contains thousands of common directory names, a request will be sent with each entry from that list to the web server. If the directory does exist on the web server the request will be successful otherwise a "401 not found" will be sent back. These directories and files might hold sensitive information about the website and might also disclose information about the web server environment and may allow the attacker to find other severe vulnerabilities.

2.8 Fuzzing

One of the most useful penetration tests is a Fuzzing test. The technique used behind this test is to send a large number of malformed data within actual or fake commands to the targeted server in order to generate failures and expose flaws which can later be used to exploit and attack the system. The web-server, which in this case will be the switch and router HTTP server, will be monitored for problems or crashes as a result of these invalid inputs.

Some of the common vulnerabilities these Fuzzing tools can detect are buffer overflows, format string bugs, denial of service, and coding errors. The advantage of Fuzz testing is that it might reveal defects that were overlooked by human testers during development stages. In this case HTTP was the attempted Fuzzed protocol.

3. Methods of Examination

This section will describe all the tools that were used to perform the Penetration Test.

3.1 Password cracking using MEDUSA

MEDUSA is a dictionary login brute-force tool that will try to guess username and password. It supports different modules like HTTP, SSH, SNMP etc.

SSH module supports SSHv2, which is a more secure version than SSHv1. SSH is a protocol used to secure client-server communication over the network by encrypting data during transmission, it also prevents root access which is used in network applications such as FTP and telnet. SSH v1 and SSHv2 are completely different protocols and will not communicate with

each other. SSHv2 added more features and is more secure and offers the following protection that is not available in SSHv1:

- Protection from the "man in the middle", which is a very serious threat in the Ethernet networks;
- Protect against Eavesdropping by encrypting data and making it difficult to comprehend;
- SSHv2 will protect against IP spoofing by cryptographically verifying the identity of the server.

The basic idea of MEDUSA is to try and guess the user name/password and to gain access to the router and switch web user interface which will give the attacker control over the devices and can cause serious network outage and damage.

MEDUSA tool will try to match the username and password against a predefined list which contains over 14 million commonly used usernames/passwords, other larger lists can be downloaded from the internet. The attacker tries to use usernames/passwords from this list to guess the target administrator's credentials. If successful, it receives the "200 OK" message from the router then it stops and displays the username/password it used to login. If the administrator does not select a strictly complicated username/password, it will be much easier for the attacker to guess the username/password using this tool.

3.2 Web server scanning using NIKTO and SKIPFISH

The tools used for the web server scanning test are **NIKTO** and **SKIPFISH**. **NIKTO** is an Open Source web server scanner. It performs extensive tests against web servers for different potentially insecure files/CGIs and server configurations, and identifies installed software and captures received cookies. This tool will generate thousands of HTTP GET requests which will leave behind a large footprint. This becomes an effective way to test the Intrusion Detection systems in place.

SKIPFISH is another web server scanner. Web developers use SKIPFISH to discover vulnerabilities they missed while developing websites and servers. It is a very important tool developed by Google that provides an interactive map of the targeted website. It carries out a crawl and dictionary based scan of the website and performs security checks looking for security gaps and web application vulnerabilities. When the test is done it will provide a final report that helps the web developer with security assessments. It can take several hours for this test to complete depending on the target performance, the connection quality, and on the options used; such as complete, medium or minimal.

3.3 SNMP enumeration using SNMP Check

The tool used for the SNMP enumeration is called "SNMP-Check". It is a tool that can be used to gather information about the targeted system. Developers and testers use this tool to

enumerate SNMP to check the website security. This tool will generate a report at the end of the test which includes information about the targeted device such as:

- System information, like hostname, uptime, etc;
- Device information, like information about the running interfaces and processors;
- Storage information, such as physical/virtual memory details, buffer details and cached/shared memory details;
- Processes and details about running processes;
- Network information, which is details about the Network configuration such as IP forwarding, TTL and TCP/UDP packet counters;
- Routing information;
- List of listening TCP/UDP ports.

3.4 SSL/TLS scanning using SSLScan and TLSSLED

For this test the following tools were used, SSLScan and TLSSLed. These tools are used to scan web servers to discover what type of protocols and ciphers the server supports and prefers as the encryption methods, also giving information about the SSL certificates. The tools will also look for the version of SSL and TLS being used.

SSLScan/ TLSSLed:

These tools will provide the attacker with important information such as weak ciphers used by the server which can be used to exploit it. Web server miss configurations can allow attacker to use weak ciphers to gain access to the web server. An example of a weak cipher is the one that uses 40 bits as key length; this key can be broken, allowing attackers to decrypt the data transmitted.

A cipher suite is specified by an encryption protocol such as DES, RC4 and AES, and a hash algorithm such as SHA and MD5 used for integrity checking. Different ciphers have different key lengths like DES uses 40 bits, RC4 uses 56 bits and AES uses 128 bits.

3.5 Protocol flooding using UDP.pl and Hping3

UDP flooding attack:

UDP.pl flood attack tool was used against the router and switch. An attacker can use this tool to target different ports on the target; the port that was used for this test was 123 which is a UDP port used for NTP (Network Time Protocol).

NTP is used for time synchronization between the server and client. When the attacker sends a large number of malformed messages to that port it will cause DoS and result in poor time synchronization.

TCP SYN Flood attack:

The tool used for TCP sync flood attack was **Hping3**. This tool can be used to do different types of attacks by customizing its parameters. Hping3 will open a large number of TCP connections with the targeted server and never respond and complete the TCP connection process resulting in the target connections stuck in the SYN_RECV state. When a legitimate user tries to establish a connection with the server it will time out, as all of the server resources will be used up as a result of the sync attack.

Hping3 man page, mentions that it can be used for jobs other than security testing such as:

- Advanced port scanning;
- Manual path MTU discovery;
- Advanced trace route, under all the supported protocols;
- Remote OS fingerprinting;
- Remote uptime guessing;
- TCP/IP stacks auditing;
- Firewall testing.

3.6 Web server stressing using SIEGE

The objective here is to find out the stability of the router and switch HTTP server and its performance during high traffic periods. If not configured correctly and efficiently, a web server can stop responding if it is under high demand which will result in a service interruption.

SIEGE was the tool used for this part, it is a multithreaded tool that will allow developer to test their code under stressful situation and measure the web server performance. The tool can be configured in different ways, like how many concurrent users and how long to run the test for.

The output report will show number of transactions, web server availability, response time, transaction rate, throughput, concurrency, number of successful transactions, number of failed transactions, longest transaction, and shortest transaction. Overloading the router/switch with multiple user requests results in the HTTP server will not be responding to requests from legitimate user causing DoS.

3.7 Brute force directory & files using DIRB

DIRB was the tools used for the Brute force directory & files. It is a Web Content Scanner also called web crawler, it looks for hidden Web Objects. As mentioned in the description for Brute Forcing Directories, DIRB uses a dictionary based attack against web server and finds out the directories and its contents. This tool can be useful for auditing the web site and web server configuration.

3.8 Fuzzing using SPIKE, BED, SICKFUZZ, SFUZZ,

SPIKE is very powerful, flexible, and largely used Fuzzing tool. It is a Fuzzer creation kit that allows users to create their own Fuzzers using C language. The main purpose of SPIKE is to find exploitable bugs on the target. SPIKE comes with large built-in strings that can be used during the Fuzzing process which might produce various errors on the target.

BED (Brute force Exploit Detector) is a plain-text protocol Fuzzer. It checks the target for common vulnerabilities like buffer overflows, format string bugs, and integer overflows. The tool will send a large number of commonly known strings impeded in an actual command like the HTTP command "GET" that might cause problems to the server in hopes of revealing weaknesses that can be used to exploit the target. This tool supports different protocols such as HTTP, FTP, and SMTP.

SICKFUZZ is a web server Fuzzer. The strength of this tool comes from the fact that it is made of several SPIKE scripts saved in a spk file and a python script interface that handles running the spk files. It has predefined scripts to Fuzz HTTP functions such as HEAD, GET, etc. SICKFUZZ allows hacker can run multiple SPIKEs with one command.

SFUZZ (Simple Fuzz) is a tool with strong capabilities. It provides a simple, easy to learn interface, while SPIKE is very powerful but it will take time for users to learn their way around it. Basically, it follows the same idea of all other Fuzzing tools, where it will send a large amount of malformed data to the target in order to cause a crash or failure. The tool includes a number of predefined scripts to Fuzz widely used protocols such as HTTP.

4. Analysis of Results

This section will discuss the results from the tests performed on the router and the switch.

4.1 Analysis of Router Results

4.1.1 Router Password cracking Analysis (MEDUSA)

As previously mentioned, MEDUSA supports different modules like HTTP and SSH. It was discovered that the router does not support SSHv2 as running the tool using SSH module returned error as it shows in Figure 1.

root@bt:~# MEDUSA -h 192.168.10.1 -U /pentest/passwords/wordlists/mazusr.txt -P
/pentest/passwords/wordlists/mazpwd.txt -0 /root/Desktop/MEDUSA-test.log -t 1 -v 5 -f -M ssh
MEDUSA v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ERROR: ssh.mod: Failed establishing SSH session (1/4): Host: 192.168.10.1 User:
administrator Pass: turtle
ERROR: [ssh.mod] Failed to exchange encryption keys. Are you sure this is a SSHv2 server?

Figure 1: MEDUSA Router SSHv2 not supported

Instead, HTTP module was used. The tool ran against the router HTTP server for several minutes and it was able to determine the login username and then the password. After running for a few minutes the tool found the correct credentials (Figure 2).

MEDUSA -h 192.168.10.1 -U /pentest/passwords/wordlists/mazusr.txt -P
/pentest/passwords/wordlists/mazpwd.txt -0 /root/Desktop/MEDUSA-test.log -t 1 -v 5 -f -M http
ACCOUNT FOUND: [http] Host: 192.168.10.1 User: admin123 Password: mypassword [SUCCESS]
MEDUSA has finished (2013-08-23 20:43:10).

Figure 2: MEDUSA Router Result

After finding the username/password, an attempt to access the router web user interface was successful. Also commands were executed from the web interface, and retrieved information about the router and its configurations. Figure 3 shows the results from an attempt to execute commands on the router from the web user interface. The "show run" command provided details about the router, its specifications, and the IOS installed.

Command base-URL was: /level/15/exec/-Complete URL was: /level/15/exec/-/show/version/CR Command was: show version Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.3(22), RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by cisco Systems, Inc. Compiled Wed 24-Jan-07 16:48 by ccai Image text-base: 0x80008098, data-base: 0x81A11604 ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1) ROM: C2600 Software (C2600-IK903S3-M), Version 12.3(22), RELEASE SOFTWARE (fc2) maz uptime is 22 minutes System returned to ROM by reload System image file is "flash:c2600-ik9o3s3-mz.123-22.bin" This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html If you require further assistance please contact us by sending email to export@cisco.com. cisco 2621 (MPC860) processor (revision 0x101) with 59392K/6144K bytes of memory. Processor board ID JAB032601FP (1236506842) M860 processor: part number 0, mask 49 Bridging software. X.25 software, Version 3.0.0. 2 FastEthernet/IEEE 802.3 interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write)

Figure 3: MEDUSA Test, Show run

This is a very serious problem where the network is now vulnerable and the attacker can seize control over the user's router, make changes, cause damages and service interruption. Using simple usernames/passwords is never recommended, especially for administrator accounts. A strong username/password is more difficult for an attacker to guess by launching dictionary attack or brute force attack.

Also the router does not support SSHv2 which makes it vulnerable to **IP spoofing attack** and **Man in the middle attack** MiTM.

IP Spoofing attack is when the IP packet's header is forged to have an incorrect source IP address. This way, the attacker can hide his identity and make it harder to locate the packet's actual source. This can be used during DoS attacks, since the attacker does not care about the response coming back from the target; they spoof the source IP so the response will go somewhere else. Spoofed addresses are more difficult to be filtered as it seems that they are random IPs and not a certain pattern that can be filtered. Packet Filtering can be used to protect against IP spoofing, where ingress filtering will block packets from outside the network that appears to have a source address from within the network.

Man in the middle attack MiTM, is when an attacker intercepts a public key exchange between the sender and receiver and then uses that information to send his own public key to both sides. This will trick both sides to thinking they are still in communication with each other, while in fact the attacker is intercepting the messages and changing them to whatever he wants then sending them to the destination. Strong encryption can be used to protect against this type of attacks. A latency examination also can be used to protect against this attack where if the duration to reach each party is exceeding the normal time, it will indicate that there is a third party intercepting the messages.

4.1.2 Router Web server scanning Analysis (Router NIKTO, Skip fish)

NIKTO

The test was started using the HTTPS module which uses port 443. The test took approximately 5 hours and 22,083 requests were made. Most of the requests came back with 404 messages which mean the received command was not found; the router logs were being monitored using the router web interface. It was noticed that the router was receiving and processing most of the requests from the tool as it shows from the "show interface fastethernet 0/1 stats" command, 245647 in packets and 205649 out packets.

When the test was complete, it reported few problems. First it found that the router HTTP server is vulnerable to Clickjacking.

The anti-clickjacking X-Frame-Options header is not present.

Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user thinks they are clicking on, this might reveal confidential information or make their system vulnerable to be controlled by the attacker. It is a browser

security issue and is vulnerable across a variety of browsers and platforms. When a webpage is click jacked it means it was allowed to be framed from a domain other than the real one. A Clickjack takes the form of a hidden script that can execute without the user's knowledge, such as clicking on something that appears to perform another function.

An attempt to clickjack the router website was successful as shown in Figure 4. A test HTML page was used to load the router webpage inside a frame after entering the target URL.

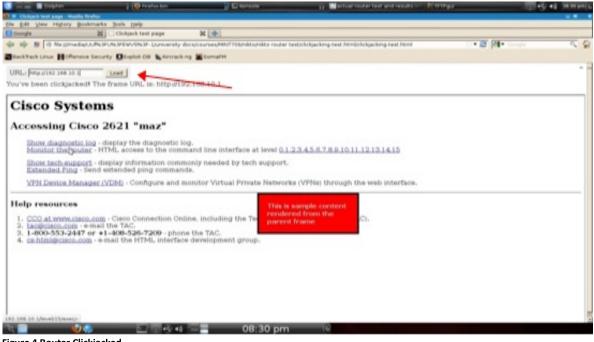


Figure 4 Router Clickjacked

Another finding from the test was that the **SSL certificate was either expired** or it was not signed by an authorized Certificate Authority.

+ GET Hostname '192.168.10.1' does not match certificate's CN 'maz.mint709-domain unstructured Name=maz.mint709-domain'

It was also discovered that the router's web install **allows arbitrary commands to be executed remotely**. This vulnerability allows attackers to control the router remotely and run commands on the router using the router's web interface.

After testing HTTPS module was complete, the test was repeated but this time HTTP module was used on port 80. The results were the same except there was no mention of the certificate mismatch as it did for https.

SKIPFISH

The Skipfish tool ran against the router for approximately 7.5 hours and was interrupted manually then it generated the report. There were 30 high risks reported with respect to 'Incorrect or missing character set' and 'Cross site scripting attack' (Figure 5).

Incorrect or missing character set. The purpose of the character sets is to inform the browser what type of text to expect from the website. The risk of leaving no character set is that the browser might guess the character set which might be incorrect. In that case an attacker can use this vulnerability to generate special scripts and send it to the website which will lead to **cross site scripting attack (XXS)** against the site users.

→ C <a>b file:///G:/university%20docs/courses/MINT709/skip%20fish/skipfish-router-test/maz-skipfish-router.txt/index.html#				
skipfish	Scanner version: Random seed:	2.10b 0xe2910e53	Total time:	Mon Sep 2 02:26:51 20 7 hr 28 min 58 sec 910
			Problems with	this scan? Click here for a
rawl results - click to expand:				
•				
ocument type overview - click to expand:				
application/xhtml+xml (1)				
1. https://192.168.10.1/ping (326 bytes) [show trace +]				
text/html (23)				
and time anomian which to arrive de				
sue type overview - click to expand:				
Incorrect or missing charset (higher risk) (30)				
XSS vector in document body (30)				
HTML form with no apparent XSRF protection (43)				
SSL certificate host name mismatch (1)				
Self-signed SSL certificate (1)				
SSL certificate expired or not yet valid (1)				
Node should be a directory, detection error? (1)				
Response varies randomly, skipping checks (16)				
Resource fetch failed (172)				
Numerical filename - consider enumerating (15)				
Incorrect or missing charset (low risk) (128)				
HTML form (not classified otherwise) (43)				
Unknown form field (can't autocomplete) (4)				
Hidden files / directories (1)				
New 404 signature seen (11)				
New 'Server' header value seen (1)				

Cross site scripting attack (XXS) is a very common application layer web attack. It targets the scripts that supposed to be executed on the user side browser instead on the server side. It can be used to bypass same-origin policy which is one of the access control methods. The same-origin policy is a method used by programmers where it will allow scripts to run on pages that are originated from the same site to access each other with no restriction while preventing access from other sites. This method used for web applications that depends on HTTP cookies to maintain user session authentication. An attacker might write a script to be downloaded on the client browser, and then collect cookies that might reveal some important information about the router. Most hackers will use this type of attack during the information gathering phase.

Another critical vulnerability revealed by the test was **HTML form with no apparent XSRF protection**. Cisco website identifies that IOS images from 11.0 to 12.4 are vulnerable to **XSRF**. This could allow malicious users to execute commands on the device through the web interface under the privileges of an already logged-in user. The risk of XSRF is mainly that an unknown user can send HTTP requests that will cause unwanted actions if the browser uses authentication by cookies. The exploit works by hiding a link or a script within another link that might seem harmless, such as an image. When the user clicks on the link the script will run and perform actions that the user is unaware of and did not authorize. An example of XSRF is one where a hacker might access a user's friend's email and send the user an email with a hidden script behind an image. The user is lead to believe it is a safe image from a friend and therefore clicks on the image to view. By opening the image, the script will run and might link to the user's banking website if the user did not delete their saved browser cookies. A saved login

cookie from the user's banking website can be used by the browser to logon automatically leading to a transaction that might occur without user's authorization.

4.1.3 Router SNMP Enumeration Analysis (SNMP Check)

The SNMP Check tool was run using the 'private' community string to see if it was configured on the router. The test was successful, giving a detailed report as shown in Figure 6. The information provided in the report can be a gold mine for attackers. One of the risks of SNMP is if it were not configured properly it would be exposed to spoofing attacks. Spoofing attacks will allow the hacker to gain access and control of the targeted device then use it to attack other hosts on the network, steal data, or spread viruses and malwares. Since SNMP v1/v2 uses UDP, which does not provide a mechanism to authenticate source and destination messages, it will open the door for SNMP spoofing attacks (Figure 6).

Since SNMP v1 and v2 use 'community string' to perform SNMP actions between client and server, weak community string usage is considered to be really insecure as it can be guessed by the attacker if he runs a simple script containing a list of community strings against the server. Using a strong community string might resolve the issue but doesn't fix the security threat completely. Moreover communications using SNMP v1/v2 is in transmits data in plain text thereby disclosing the 'community string' if the hacker is sniffing on the network traffic. Once the community string is obtained, the hackers can view/get/set data into the router and switch by IP spoofing.

An attacker can create fake SNMP packets using private community strings and set new data values in the router. Also, by using any SNMP MIB browser, new data insertion or modifications can be carried out in the router using the SNMP 'set' function.

🥨 🚞 📰 snmp-router-	te 🛛 🕹 How to Configura	University of AT	E konsole	11 snmp-test-nor	notes.docx - 0	M TETPgui	etho (Wiresh	📕 xpdf	i 🗉 🚭 📢	38:45 pm(C
snmpcheck hash										_ # X
File Edit View Bookma	rks Settings Help									
	connoctions' enumerati t in seconds: default i : Nu:									Î
rootgbt:/pentest/enumerat snmpcheck.pl vl.0 - SNMP Copyright (c) 2005-2011 b	enumerator									
<pre>[*] Try to connect to 19 [*] Connected to 192.168 [*] Starting enumeration</pre>	10.1									
(*) System information										
Hostname : Description : rtCopyright (c) 1986-2007 Liptime system : Liptime SMMP daemon :	maz.mint709-domain Cisco Internetwork Ope	rating System Soft Compiled Wed 24-Jas	ware 105 (tm) C n-07				FTWARE (fc2)⊺echni			/techsuppo
[*] Network information										
Default TTL TCP segments received TCP segments sent TCP segments retrans. Input datagrams Delivered datagrams	1 883									10
[*] Network interfaces										
Interface Speed IP Address Noteask	: 00:08:21:96:f3:00 : 100 Mbps : 192:160.10.1 : 255.255.255.0 : 1500									
Interface	I up I FastEthernet0/									
Hardware Address Interface Speed	: 00:08:21:96:f3:01									0
		pcheck : bash								
۲ <u>۲</u>		<))	08	8:45 pm	G					

Figure 6 Router SNMP-check results

4.1.4 Router SSL/TLS Scanning Analysis (SSL Scan, TLSSLED)

SSLScan test was done using port 443 on the router. The test results found ciphers that were being accepted and preferred by the router (Figure 7).

Accepted ciphers by router (Current SSL cipher strength): DES-CBC3-SHA which uses SSLv3 (SSL Cipher strength: Strong) DES-CBC-SHA which uses SSLv3 (SSL Cipher strength: Weak) RC4-SHA uses SSLv3 (SSL Cipher strength: Medium) RC4-MD5 uses SSLv3 (SSL Cipher strength: Medium) Preferred cipher by router: DES-CBC3-SHA

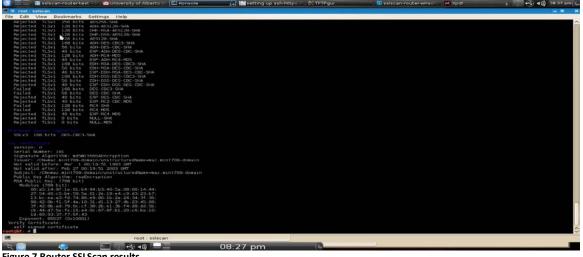


Figure 7 Router SSLScan results

It was also observed that the certificate expired in Feb 2003; also the RSA key length used was 768, which is considered insecure. Another finding is that the router used **MD5 Message-Digest Algorithm** which is considered to be vulnerable to **Spoofing attacks** as it is not collision resistant. MD5 collision attacks can create a rogue Certification Authority trusted by all common web browsers. This allows an attacker to perform transparent "man-in-the-middle" attacks against SSL connections and monitor or tamper with traffic to the router.

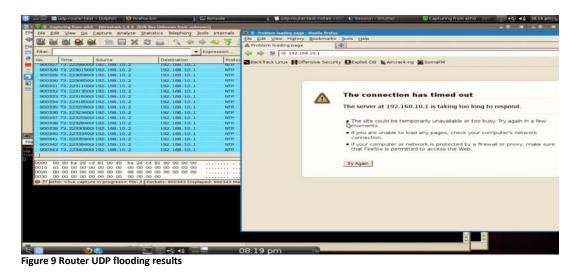
	d Dolohin	where is tissled in backtrack	Konsole	1 System Monitor	Intissied router test notes edt	() +() 4)) 25:13 pm(
S Usaled TLASLe		where is tissled in backtrack / t		a) the system Monitor	tissied router test notes.out 10	an an an sarabul
	lookmarks Settings	Help				
Not valid befor	1 23:09:34 UTC 2013 e: Mar 1 00:04:59 1 Feb 27 00:04:59 20	DD3 OKT				
 1 Checking prefer Prefered Server C 555.v3 108 bits 						
*) Testing for sec ecure Renegotiatio	ure renegotiation n IS NOT supported					
Accepted SSLv3 Accepted SSLv3 Accepted SSLv3	v3 and TLSv1 support 108 bits DES-CBC3 50 bits DES-CBC3 128 bits RC4-5HA 128 bits RC4-HD5					
*1 Testing for TLS he local openaal v	vi.i support eraion does NOT supp					
*] Testing for TLS he local opensal v	vl.2 support ersion does NOT supp					
rw-rr 1 root r rw-rr 1 root r	001 4247 2013-09-01 001 1736 2013-09-01 001 1556 2013-09-01 001 419 2013-09-01 1	17:09. selscan_192.168.10.1.443.2013-09 27:09 opensst_HEAD.192.168.10.1.443.20 17:09 opensst_HEAD.192.168.10.1.443.20 7:09 opensst_HEAD.192.168.10.1.443.20 109 openset_HEAD.192.168.10.1.443.20	013-89-01_170964.log 2013-09-01_170904.log 213-09-01_170904.err			
-1 done						
	umeration/tlasteds					
		tissled : TLSSLed.sh				
	10 C		05:13 pm	(0		

Figure 8 Router TLSSLed results

4.1.5 Router Protocol Flooding Analysis (UDP.pl, Hping3)

UDP.pl Flood Attack

UDP.pl tool ran against the router using NTP port 123. The test duration was 100 seconds. During the test the router web interface was not responding and the connection was timing out when a legitimate user tried to access the web interface (Figure 9). This is the result of the DoS attack.



Wire shark showed that over 1,200,000 NTP packets were sent. After 100 seconds the web server started responding again (Figure 11).

The technician support page on the website showed that the interface Fastethernet 0/1 was receiving a huge amount of dropped packets and input errors; due to the fact that the data sent from udp.pl was malformed data, as shown in Figure 10.

```
FastEthernet0/1 is up, line protocol is up
 Hardware is AmdFE, address is 00d0.ba2d.cd81 (bia 00d0.ba2d.cd81)
  Internet address is 192.168.10.1/24
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
   Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
 ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:33, output 00:00:09, output hang never
 Last clearing of "show interface" counters never
  Input queue: 0/75/619606/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
 Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     361 packets input, 22764 bytes
     Received 4 broadcasts, 0 runts, 0 giants, 0 throttles
     545301 input errors, 0 CRC, 0 frame, 545301 overrun, 0 ignored
     0 input packets with dribble condition detected
     119 packets output, 60521 bytes, 0 underruns
```

Figure 10 Router UDP flooding, Interface stats

The full View Go	Capture Analyze Statis	v 39941 from /trunk-1.6)]				
e For Den No						
		C & & @ 2.	2 00	QQQE	😹 XX 🥵 🛠 🙀	
ter			· Expression.	Clear Apply		
Time	Source	Destination	Protocol	ength Info		
1 0.0000000	0 C1sco_2d:cd:81	Cisco_2d:cd:81	LOOP	60 Reply		
2 1.3643230	0 192.168.10.2	192.168.10.1	NTP	43 reserved	reserved[Malformed Packet]	
3 1.3643410	0192.168.10.2	192.168.10.1	NTP	43 reserved	reserved[Malformed Packet]	
	00192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	00192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	00192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	0 192.168.10.2	192.168.10.1	NTP.		reserved[Halformed Packet]	
	00192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	0192,168,10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	0 192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	0 192.168.10.2	192.108.10.1	NTP		reserved[Malformed Packet]	
	00 192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	00 192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	00 192.168.10.2	192.168.10.1	NTP		reserved[Malformed Packet]	
	0 192.168.10.2	192.168.10.1	NTP	43 reserved	reserved[Malformed Packet]	
thernet II, s internet Proto ser Datagram Source port: Destination Length: 9 Checksum: Ox		:66 (00:1e:ec:8d: : 192.168.10.2 (19 : 52096 (52096), 1	91:66), Dst: 92.168.10.2)	cisco_2d:cd:81 , Dst: 192.168.	(00:00:ba:3dr:dd:B) 10.1 (192:166.10.1)	
came 92 43 by thermet 13, 5 mternet Proto iser Datagram Source port Destination Length: 9 Checksum: 0h [Good Chec [Bad Chec] etwork Time F Flags: 0x30 00, 	<pre>irc: compails.66198 col version 4, Src Protocol, src Port S2096 (2096) port: ntp (123) v056e (validation 4 ksum: false] rotocol = Leap Indicator: - version number: = Node: reserved (kett Nrm] o (crror/Nalformed)</pre>	<pre>ide (00:12:ecc.8d); 192:168.10.2 (1) isabled] isabled] no warning (0) reserved (6) 0) Halformed Packet</pre>	01:66), Dot: 92.168.10.2) Dot Port: nt	<pre>cticco_2dicdi8i , Dst: 192.168. p (122)</pre>		
came 37 43 by thermet 13, 5 internet Proto bestination Lengthi 9 Checkswn 0n [Good Chec [Bad Check etwork Time 9 6 Flags: 0x30 00,0000 00,0000 00,0000 00,0000000000	<pre>crc compairs.86092 col version 4, Src Protocol, src Port S2096 (2096) port: np (123) obser [validation d ksum: False] rotocol rotocol - worsion number: - Words reserved () (Cerror/Malformed) malformed Packet () Revel: Feror]</pre>	<pre>ide (00:12:ecc.8d); 192:168.10.2 (1) isabled] isabled] no warning (0) reserved (6) 0) Halformed Packet</pre>	01:66), Dot: 92.168.10.2) Dot Port: nt	<pre>cticco_2dicdi8i , Dst: 192.168. p (122)</pre>		
Trame 9: 41 by Thermet Proto User Datagram Source port Destination Length: 9 Checksum: 00 [Good Chec [Mad Check Wetwork Time P = Flags: 0x30 00, .11 0 (Cood Check Mad Check Mad Check (Checksum) 00 00, 	<pre>crc compairs.86092 col version 4, Src Protocol, src Port S2096 (2096) port: np (123) obser [validation d ksum: False] rotocol rotocol - worsion number: - Words reserved () (Cerror/Malformed) malformed Packet () Revel: Feror]</pre>	<pre>ide (00:12:ecc.8d); 192:168.10.2 (1) isabled] isabled] no warning (0) reserved (6) 0) Halformed Packet</pre>	01:66), Dot: 92.168.10.2) Dot Port: nt	<pre>cticco_2dicdi8i , Dst: 192.168. p (122)</pre>		
Common 2 41 b) Ethernet 18, 5 Marken 18, 5 Marken 18, 5 Checksum: 0 Checksum:	Inc. Compaindist. Col. Version 4, SrC. S2006 (S2006) S2006 (S2006) S007 (S2006) S2006 (S2006) S2016 (S2007) S2016 (S	<pre>ide (00:12:ecc.8d); 192:168.10.2 (1) isabled] isabled] no warning (0) reserved (6) 0) Halformed Packet</pre>	91:66), Dat: 92:168:10:22 Dot: Port: nt t (Exception s))	<pre>cfscc_ddcdi8; ost: 192,168; p (123) occurred)] occurred)]</pre>	10.1 (192.166.10.1)	Profile Default

Hping3 SYN Attack

The Hping3 tool ran against the router port 22 using the following command:

root@bt:~# hpgin3 -V --flood -S -p 22 192.168.10.1

When the test began, wireshark was running to capture the packets and it was immediately noticed that the memory on the computer, where the tool was running from, was being consumed rapidly and the CPU usage was nearing 100%. After a few minutes, the computer's memory was consumed and the test had to be interrupted to avoid the risk of freezing the computer and loosing test results. The test duration was enough to notice that the SYN attack was causing DoS.

Wireshark showed that 1,500,000 packets were captured within a few minutes. The web user interface was not responding from the beginning of the test, as shown in Figure 12.

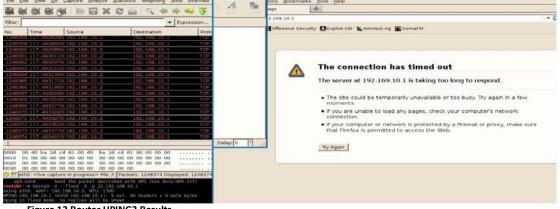


Figure 12 Router HPING3 Results

When Hping3 was interrupted, it reported that over 18,000,000 packets were sent. The technician support page showed over a million input errors and dropped packets (Figure 13).



Figure 13 Router HPING3, interface stats

An attempt to access the web interface from another computer on the network was timing out. This confirms that the router was not responding due to the fact that it was under a DoS attack (Figure 14). The test confirmed that an Hping3 SYN attack can cause service interruptions for all users.

192.168.10.1 This page can't be displayed Make sure the web address http://192.168.10.1 is correct Look for the page with your search engine · Refresh the page in a few minutes. Fix connection problems EN 🚎 🥠 🛊 🖓 all 🕴 12:59 PM Figure 14 Router HPING3, No connection

4.1.6 Router Web Server Stressing Analysis (SIEGE)

The test was setup to run against the router with 15 concurrent users for duration of three minutes. During the test, the web server was responding slower than normal. The username and password from the first test were used.

The test results show that the router availability was about 86%, with 32 failed transactions and 200 successful transactions. The concurrency, which is the number of simultaneous connections, was only 7.74. Concurrency will increase when the server performance decreases. At the end of the test, the web server resumed responding to requests normally.

When tested again with 100 concurrent users, the web site was not responding and connection requests timed out (Figure 15). When three minutes passed the website responded normally.



Figure 15 Router SIEGE results

With 100 concurrent users the web site availability went down to approximately 54% and the response time was higher than with 15 concurrent users. The number of failed transactions was almost the same as the successful ones. The concurrency increased to 11.25, meaning the server performance decreased with a higher number of concurrent users.

	15 Concurrent Users	100 Concurrent Users
Availability	86.15%	54.98%
Response time	6.97 secs	7.61 secs
Concurrency	7.74	11.25
Failed Transactions	32	217
Successful Transactions	200	275
Longest transaction	43.39	46.52
Transactions	199 hits	256 hits
Elapsed time	179.38 secs	179.38 secs
Data transferred	0.29 MB	0.36 MB
Transaction rate	1.11 trans/sec	1.48 trans/sec

Table 1 shows statics from both SIEGE tests:

Table1- Router SIEGE tests statistics

4.1.7 Router Brute Force Directory and files Analysis (DIRB)

The DIRB tool was used for the Router Brute Force Directory test. The tool reported a list of 11 directories found on the router HTTP server. The username/password found from previous tests was used to successfully run the command. DIRB was able to find important information about directories on the web server that is not meant for public access (Figure 16).

DIRB v2.03 By The Dark Raver OUTPUT FILE: /root/Desktop/DIRB-router START_TIME: Tue Sep 17 20:02:48 2013 URL_BASE: http://192.168.10.1/ WORDLIST_FILES: wordlists/big.txt AUTHORIZATION: admin123:mypassword GENERATED WORDS: 4217 ---- Scanning URL: http://192.168.10.1/ ----+ http://192.168.10.1/configure (FOUND: 200 [Ok] - Size: 13417) + http://192.168.10.1/controller (FOUND: 200 [Ok] - Size: 20) + http://192.168.10.1/exec (FOUND: 200 [Ok] - Size: 4297) + http://192.168.10.1/filter (FOUND: 200 [Ok] - Size: 359) + http://192.168.10.1/gateway (FOUND: 200 [Ok] - Size: 831) + http://192.168.10.1/interface (FOUND: 200 [Ok] - Size: 19) + http://192.168.10.1/line (FOUND: 200 [Ok] - Size: 6634) + http://192.168.10.1/ping (FOUND: 200 [Ok] - Size: 326) + http://192.168.10.1/roles (FOUND: 200 [Ok] - Size: 689) + http://192.168.10.1/router (FOUND: 200 [Ok] - Size: 25) + http://192.168.10.1/template (FOUND: 200 [Ok] - Size: 1198) DOWNLOADED: 4217 - FOUND: 11

4.1.8 Router Fuzzing Analysis (BED, SPIKE, SICKFUZZ, SFUZZ)

BED

The BED test against the router took approximately 7 hours, during that the router web server was functioning normally. Over 200,000 HTTP packets were transmitted to the router and there was no evidence of any problems with router functionality. After the test completed, there was no sign or report of buffer failures or overflows on the router.

SPIKE

The SPIKE test lasted several minutes and over 21,000 packets were processed by the router. The website was slower and at times the connection requests were timing out which indicates the web server is too busy (Figure 17). There was no buffer failure reported on the router. After the test had completed, the web server responded normally.

Figure 16 Router DIRB results

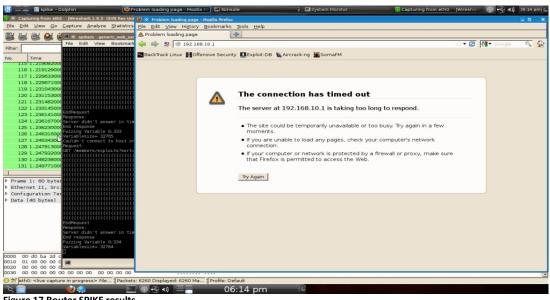


Figure 17 Router SPIKE results

SICKFUZZ

The SICKFUZZ test lasted about 70 minutes and caused the router to stop responding to requests, causing buffer failures. The test was stopped after 70,000 packets were transmitted; it took a few minutes until the router recovered and started to respond to requests again. The router's technician support webpage showed that the Fastethernet interface 0/1 received about 52,000 packets and that there were buffer failures mostly in the small buffers (Figure 18).

```
Buffer elements:
      1119 in free list (1000 max allowed)
      130880 hits, 0 misses, 1119 created
Public buffer pools:
Small buffers, 104 bytes (total 98, permanent 50, peak 98 @ 00:04:32):
      98 in free list (20 min, 150 max allowed)
73752 hits, 73 misses, 0 trims, 48 created
31 failures (0 no memory)
Middle buffers, 600 bytes (total 36, permanent 25, peak 36 @ 00:04:33):
      36 in free list (10 min, 150 max allowed)
2486 hits, 10 misses, 0 trims, 11 created
      1 failures (0 no memory)
Big buffers, 1536 bytes (total 53, permanent 50, peak 53 @ 01:30:14):
      53 in free list (5 min, 150 max allowed)
      36114 hits, 1 misses, 0 trims, 3 created
      0 failures (0 no memory)
VeryBig buffers, 4520 bytes (total 10, permanent 10):
      10 in free list (0 min, 20 max allowed)
      0 hits, 0 misses, 0 trims, 0 created
      0 failures (0 no memory)
Large buffers, 5024 bytes (total 0, permanent 0):
      0 in free list (0 min, 10 max allowed)
0 hits, 0 misses, 0 trims, 0 created
```

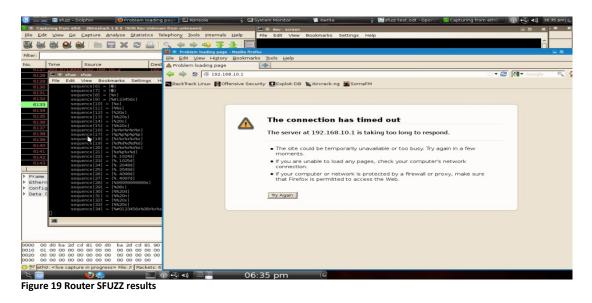


SFUZZ

The SFUZZ test was setup to target port 80 on the router using the command shown below. A predefined fuzz-script (basic.http) was used for this test.

```
SFUZZ -TO -f SFUZZ-sample/basic.http -S 192.168.10.1 -p 80
```

The test lasted several minutes during which about 15,000 packets were received by the router. No buffer failures were reported and during the test the website was responding slower and some connection requests were timing out (Figure 19).



By checking the router's web server technician support page it was noticed that a high number of requests were received and that the Headers buffer number of free buffers dropped below the minimum threshold level which resulted in the creation of nine new buffers (Figure 20).

```
Header pools:
Header buffers, 0 bytes (total 137, permanent 128, peak 137 @ 00:49:37):
9 in free list (10 min, 512 max allowed)
125 hits, 3 misses, 0 trims, 9 created
0 failures (0 no memory)
128 max cache size, 128 in cache
0 hits in cache, 0 misses in cache
```

Figure 20 Router SFUZZ Header buffers

4.2 Analysis of Switch Results

4.2.1 Switch Password cracking Analysis (MEDUSA)

The password cracking tool MEDUSA ran against the switch's HTTP server for several minutes and it was able to determine the login username and then the password (Figure 21). A successful attempt was made to access the switch's web user interface and remotely execute

commands on the switch. The executed commands gave information about the switch specifications and its IOS.

```
# MEDUSA -h 192.168.10.3 -U /pentest/passwords/wordlists/username.txt -P
/pentest/passwords/wordlists/rockyou.txt -0 /root/Desktop/MEDUSA-switch-test.log -t 1 -v 5
-f -M http
ACCOUNT FOUND: [http] Host: 192.168.10.3 User: admin Password: theking [SUCCESS]
# MEDUSA has finished (2013-09-03 20:55:54).
```

Figure 21 Switch MEDUSA results

When trying to run MEDUSA with SSHv2 module, it was found that the switch does not support SSHv2. As a result of that the switch is vulnerable to **IP spoofing attack** and **Man in the middle attack MiTM**.

4.2.2 Switch Web server scanning Analysis (NIKTO, Skip fish)

NIKTO

While running NIKTO test on the switch it was noticed that the switch had some limitations. Trying to use HTTPS module to run NIKTO test did not work because the switch does not support HTTPS and alternatively HTTP module was used for this test. Similar to the router, the switch was vulnerable to the **clickjacking attacks**.

The following identifies some of the benefits of HTTPS over HTTP:

- HTTP is vulnerable to eavesdropping, so data such as username/password can be compromised if someone is eavesdropping on the connection. HTTPS is more immune to eavesdropping;
- HTTPS transmits over port 443 through an encrypted system where it is harder for parties other than the client and the server to access the data. HTTPS will provide confidentiality by encrypting the payload by tunneling the HTTP over SSL/TLS (Secure Socket Layer/Transport Layer Security);
- HTTPS server must have a public key certificate, which embeds key information with a verification of owner's identity. These certificates are verified by a third party (Certificate Authority) who assures the clients that the key is secure.

SKIPFISH

The SKIPFISH test against the switch found vulnerabilities that were similar to the ones found on the router. There was an additional vulnerability on the switch which was not found on the router, **incorrect or missing MIME type** (Figure 22).

Types of Multi-purpose Internet Mail Extensions, or MIME, tell the browser what type of file is being received from a website. For example, if a website is receiving http messages, the MIME type will be text/html. An example of incorrect MIME type is if a web site treats a received image file as text file, or in other cases there would be no type specified. The risk of incorrect or missing MIME lies in the fact that the browser might mistakenly guess the type; this would open the door for Cross Site Scripting attack. For example, if the browser mistakenly guesses the file type as text instead of an image, the attacker can prepare a special image that when the browser processes it as text, it will execute a harmful script causing damages on the user's computer.

C Is file///G/university%20docs/courses/MINT709/skip%20fish/skipfish-switch/maz-skipfish-switch4/index.html	Scanner version:	a tab fam i	ate: Mon Sep 16 31/30/32 2013
skipfish		exby/recab Total	ime: thr 27 min 50 sec trams
and any second		Pything	a with this scart' Click bars for adva
Crawl results - click to expand:			
Document type overview - click to expand:			
application/javascript (z)			
image/gif (1)			
text/html (34)			
ssue type overview - click to expand:			
Incorrect or missing charset (higher risk) (10)			
XSS vector in document body (10)			
HTML form with no apparent XSRF protection (19) Limits exceeded, fetch suppressed (80)			
Resource fetch failed (s)			
Numerical filename - consider enumerating (a)			
Incorrect or missing charset (low risk) (20)			
Incorrect or missing MIME type (low risk) (3)			
HTML form (not classified otherwise) (64)			
Unknown form field (can't autocomplete) (g)			
Resource not directly accessible 🔂			
New 404 signature seen (9)			
New 'Server' header value seen (3)			
OTE: 103 aangles maximum per issus of document type.			
9 📺 🖪 🙆 🖉 😰	DI 5 <u>, 8.</u>		0 2040 20100-05

4.2.3 Switch SNMP Enumeration Analysis (SNMP Check)

When the SNMP-check tool was run against the switch; it was able to retrieve details about the switch and its configurations (Figure 23). As mentioned before, the risk of poor SNMP configuration using a weak community string can allow IP-spoofing, Fake SNMP requests and other attacks.

pcheck.pl v1.8 - SNMP enu					
-h : show help menu; tgbt:/pentest/enumeration pcheck.pl v1.8 - SNMP enu					
tgbt:/pentent/enumeration pcheck.pl v1.8 - SNMP enu					
pcheck.pl v1.8 - SNMP enu					
	Hatteo Cantoni (www.nothink.org)				
Try to connect to 192.1 Connected to 192.168.10 Starting enumeration at					
System information					
scription : Ci: 12 by cisco Systems, Inc.Ci time system : 0.1 time SMMP daemon : 32	int700-switch isco Internetwork Operating System Softwar Compactod Fra 13-Feb-02 10:51 by antenino Co seconds 2 minutes, 22.20 SouthObject		OXL-C3H2S-M), Version 12.0(5)M	KC3b, RELEASE SOFTWARE (fo	
Network information					
fault TTL : 2 P segments received : 1 P segments sent : 4 P segments retrans. : 0 put dategrams : 1 Tivered datagrams : 1	ne 255 26 26 20 20 21 25 5 1125 1125 2125 2125 2125		•		
1 Network interfaces					
Netwask : 2 MTU : 1 Bytes In : 9	00:08:54:53:00 10:46ps 10:25:26:30:525:0 255:255:255:0 1500 20047 20051				
	snmpcheck : bash				
a 0.	🔍 🚽 🖓 📢 🚍	06:48 pm	6		

4.2.4 Switch SSL/TLS Scanning Analysis (SSL Scan, TLSSLED) SSLSCAN/ TLSSLED

The SSLScan and TLSSLed tools were used to test the switch using port 80. Results from the test confirmed that the switch does not support SSL/TLS (Figure 24). This is a security threat as HTTP is vulnerable to various attacks since it is a clear-text protocol.

root@bt:~# SSLScar	192.168.10	3:80
	1-1	
//		
<u>\ \</u>	\ <u>\ \ (_ </u>	
/	/_ /\	_ _ _
	Version 1.8.	2
	//www.titani	
Copyright	Ian Ventura-	Whiting 2009
Testing SSL server	192.168.10	.3 on port 80
Company and Company	(distance) :	
Supported Server Rejected SSLv		DES-CBC3-MD5
	2 56 bits	DES-CBC-MD5
	2 40 bits	EXP-RC2-CBC-MD5
		RC2-CBC-MD5
Rejected SSLv Rejected SSLv		EXP-RC4-MD5 RC4-MD5
Failed SSLV		ADH-AES256-SHA
Failed SSLv		DHE-RSA-AES256-SHA
Failed SSLv		DHE-DSS-AES256-SHA
Failed SSLv		AES256-SHA
Failed SSLv Failed SSLv		
Failed SSLV		
Failed SSLv	3 128 bits	AES128-SHA
Failed SSLv		ADH-DES-CBC3-SHA
Failed SSLv Failed SSLv		ADH-DES-CBC-SHA EXP-ADH-DES-CBC-SHA
Failed SSLV		ADH-RC4-MD5
Failed SSLv	3 40 bits	EXP-ADH-RC4-MD5
Failed SSLv	3 168 bits	EDH-RSA-DES-CBC3-SHA
	3 56 bits 3 40 bits	EDH-RSA-DES-CBC-SHA EXP-EDH-RSA-DES-CBC-SHA
		EDH-DSS-DES-CBC-SHA
	3 56 bits	EDH-DSS-DES-CBC-SHA
Failed SSLv		EXP-EDH-DSS-DES-CBC-SHA
Failed SSLv		
Failed SSLv Failed SSLv		DES-CBC-SHA EXP-DES-CBC-SHA
Failed SSLV		EXP-RC2-CBC-MD5
Failed SSLv		RC4-SHA
Failed SSLv		RC4-MD5
Failed SSLv Failed SSLv		EXP-RC4-MD5 NULL-SHA
Failed SSLV		NULL-MD5
Failed TLSv	1 256 bits	ADH-AES256-SHA
Failed TLSv		
Failed TLSv Failed TLSv		DHE-DSS-AES256-SHA AES256-SHA
Failed TLSV Failed TLSV		ADH-AES128-SHA
Failed TLSv	1 128 bits	DHE-RSA-AES128-SHA
		DHE-DSS-AES128-SHA
		AES128-SHA ADH-DES-CBC3-SHA
	1 56 bits	ADH-DES-CBC-SHA ADH-DES-CBC-SHA
Failed TLSv	1 40 bits	EXP-ADH-DES-CBC-SHA
Failed TLSv	1 128 bits	ADH-RC4-MD5
Failed TLSv		EXP-ADH-RC4-MD5
Failed TLSv Failed TLSv		EDH-RSA-DES-CBC3-SHA EDH-RSA-DES-CBC-SHA
Failed TLSV		EXP-EDH-RSA-DES-CBC-SHA
Failed TLSv	1 168 bits	EDH-DSS-DES-CBC3-SHA
Failed TLSv		EDH-DSS-DES-CBC-SHA
Failed TLSV		EXP-EDH-DSS-DES-CBC-SHA DES-CBC3-SHA
Failed TLSv Failed TLSv		DES-CBC-SHA DES-CBC-SHA
Failed TLSV		EXP-DES-CBC-SHA
Failed TLSv	1 40 bits	EXP-RC2-CBC-MD5
Failed TLSv		RC4-SHA
Failed TLSv Failed TLSv		RC4-MD5 EXP-RC4-MD5
Failed TLSV		NULL-SHA
Failed TLSv	1 0 bits	NULL-MD5

Figure 24 Switch SSLScan results

4.2.5 Switch Protocol Flooding Analysis (UDP.pl, Hping3)

UDP.pl Flood Attack

Running the test against the switch showed a similar pattern of results to that seen in the router's UDP flood test. The switch web user interface was not responding during the test and

new connection requests were timing out. This indicates that the switch was under a DoS attack (Figure 25). About 1,280,000 NTP packets were captured by wireshark which shows that the packets were malformed NTP packets.



Hping3SYN Attack

Running Hping3 against the switch gave similar results as it did when ran against the router. The computer's memory and CPU were getting consumed rapidly and the test had to be interrupted (Figure 26). The web user interface was not responding during this test. Hping3 reported that over 12,000,000 packets were sent within a few minutes. It was noticed that wireshark captured only 1,400,000 of those packets and was not able to capture the rest since the computer's memory and CPU were almost consumed.

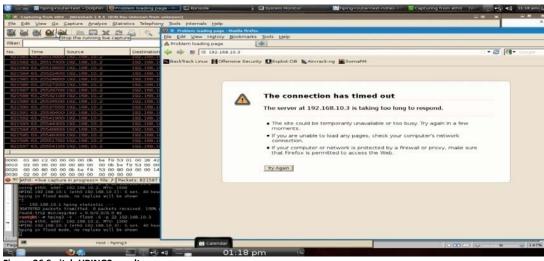


Figure 26 Switch HPING3 results

The technician support page on the web interface was checked when the switch recovered from the DoS attack. It was noticed that over 11,000,000 packets were received and the input rate was 11,106 packets/sec (Figure 27). This shows how fast a DoS attack can cause the switch to be busy and stop responding to legitimate requests.

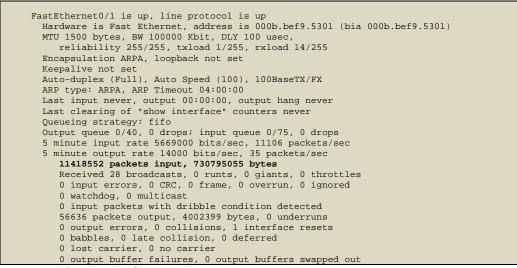


Figure 27 Switch HPING3 interface stats

4.2.6 Switch Web Server Stressing Analysis (SIEGE)

The SIEGE test on the switch was setup to run with 15 concurrent users for three minutes. During the test it was noticed that the web interface was responding very slowly and occasionally timed out (Figure 28).



Figure 28 Switch SIEGE results

From the test results, it was found that availability was only 55% with 15 concurrent users; concurrency was 3.45 and approximately 1,800 failed transactions and 2,200 successful ones.

The second test was setup to run 100 concurrent users for three minutes. During the test, the switch web interface did not respond and requests were timing out. Availability went down to 40% and concurrency increased to 9.68 indicating that the switch performance degraded.

Table 2 shows statics from both SIEGE tests completed on the switch:

	15 Concurrent Users	100 Concurrent Users
Availability	55.7%	40.55%
Response time	0.27secs	6.17 secs
Concurrency	3.45	9.68
Failed Transactions	1816	412
Successful Transactions	2283	303
Longest transaction	0.85	96.18
Transactions	2283 hits	281 hits
Elapsed time	179.71 secs	179.22 secs
Data transferred	3.85MB	0.41MB
Transaction rate	12.7 trans/sec	1.57 trans/sec

Table 2- Switch SIEGE tests statistics

4.2.7 Switch Brute Force Directory and files Analysis (DIRB)

When a DIRB test was conducted on the switch, it did not finish completely. It found four directories and gave an error "FATAL: Too many errors connecting to host" (Figure 29).

```
DIRB v2.03
By The Dark Raver
OUTPUT_FILE: /root/Desktop/DIRB-switch
START_TIME: Tue Sep 17 19:51:48 2013
URL_BASE: http://192.168.10.3/
WORDLIST_FILES: wordlists/big.txt
AUTHORIZATION: admin:theking
GENERATED WORDS: 4217
---- Scanning URL: http://192.168.10.3/ ----
+ http://192.168.10.3//
    (FOUND: 200 [Ok] - Size: 1781)
+ http://192.168.10.3/configure
   (FOUND: 200 [Ok] - Size: 4436)
+ http://192.168.10.3/exec
   (FOUND: 200 [Ok] - Size: 2953)
+ http://192.168.10.3/filter
    (FOUND: 200 [Ok] - Size: 262)
(!) FATAL: Too many errors connecting to host
    (Possible cause: OK)
DOWNLOADED: 1572 - FOUND: 4
```

Figure 29 Switch DIRB results

4.2.8 Switch Fuzzing Analysis (BED, SPIKE, SICKFUZZ, SFUZZ)

BED

The BED test conducted against the switch took approximately seven hours. During this test it was noticed that the switch web interface was responsive and functioned normally. Over 157,000 HTTP packets were transmitted to the switch and no evidence was found indicating a switch functionality problem and no buffer failures or overflows were found.

SPIKE

The SPIKE test on the switch did not affect the web server's operation and no buffer failures or overflows were reported. From the technician support page it was noticed that the small buffers were mostly used. There was six misses, which means that in six different instances the number of available buffers in the free list dropped below the minimum level and additional buffers were required. In general, the switch handled the large amount of requests and it did not crash during this test.

SICKFUZZ

This SICKFUZZ test against the switch lasted several minutes. The switch was responding slower during the test and occasionally connection requests timed out. After the test was complete, a check for buffer overflows confirmed that they occurred during the test (Figure 30).

派 二二	🔡 sickfuzz-swite	ch – Dolphir	mint709-switch /level/1	5/e 🖆 Konsole	🗧 🖃 System Monitor	sickfuzz-router-test-notes.	sickfuzz-switch-wireshark	(⊆ 😌 ◀)) 08:00 pm
			/buffers/failures - Mozilla Firefox					_ 8 X
<u>Eile Edit</u>	⊻iew History	Bookmark	s <u>T</u> ools <u>H</u> elp					
[]] mint709	-switch /level/15	5/exec/-/	45					
🗢 🏟 🕱 192.168.10.3/level/15/exec/-/show/buffers/failures								ilo 🔍 🏠
BackTrac	k Linux 🚮 Offe	nsive Secu	rity DExploit-DB Aircrack	-ng 📓 SomaFM				
min	t709-	swit	ch					
		~						
Comman	d							
Output								
Complete URI	e-URL was: /level L was: /level/15/	exec/-/shew/	huffers/failures					
Conrrand was	shov buffers f	ailures						
Caller 0xD1030 0xD1030	Pool CPU12 CPU12	Size 1524 1524	When 00:02:56 00:02:55					
0xD1030 0x1979C4 0x1979C4 0x1979C4	CPU12 CPU12 CPU12 CPU12	1524 1524 1524 1524	00:02:52 00:02:49 00:02:40 00:00:13					
0x1979C4 0x1979C4 0xD1030	CPU12 CPU12 CPU12	1524 1524 1524	00:00:10 00:00:04 00:00:04					
0x1979C4	CPU12	1524	00:00:04					
command co	mpleted.							
**								
💥 Find:					Reached end of page, continued	d from top		
2	(2	💽 🕤 😌 ୶)	- 0	3:00 pm 🧉			
Figure	30 Switc	h SICK	FUZZ results					

SFUZZ

The switch was responding normally during the SFUZZ test. The test lasted several minutes; about 14,000 packets were received on the switch interface and no buffer failures were reported. However, it was noticed that the switch buffers need to be tuned as the big-buffers show that there were 4,735 hits, 759 misses, 2,271 trims, and 2,277 buffers created (Figure 31).

Public buffer pools:
Small buffers, 104 bytes (total 43, permanent 25): 34 in free list (20 min, 60 max allowed) 299809 hits, 6 misses, 0 trims, 18 created 0 failures (0 no memory)
Middle buffers, 600 bytes (total 15, permanent 15): 14 in free list (10 min, 30 max allowed) 2366 hits, 0 misses, 0 trims, 0 created

	0 failures (0 no memory)
J	Big buffers, 1524 bytes (total 11, permanent 5):
	10 in free list (5 min, 10 max allowed)
	4735 hits, 759 misses, 2271 trims, 2277 created
	0 failures (0 no memory)
1	VeryBig buffers, 4520 bytes (total 2, permanent 0):
	2 in free list (0 min, 10 max allowed)
	2 hits, 1 misses, 0 trims, 2 created
	0 failures (0 no memory)
J	Large buffers, 5024 bytes (total 0, permanent 0):
	0 in free list (0 min, 5 max allowed)

Figure 31 Switch SFUZZ results

The following data* provides meaning and information about hits, misses, trims, and created listed in Figure 31:

- Hits identify the number of buffers that have been requested from the pool. The hits counter provides a mechanism to determine which pool must meet the highest demand for buffers;
- Misses identifies the number of times that a buffer has been requested and the RP detected in which pool additional buffers were required. In other words, the number of buffers in the free list drops below minimum level. The misses' counter represents the number of times the RP has been forced to create additional buffers;
- Trims identify the number of buffers that the RP has trimmed from the pool, when the number of buffers in the free list exceeded the number of max-allowed buffers;
- Created identifies the number of buffers that have been created in the pool. The RP creates buffers in these situations:
 - When demand for buffers has increased until the number of buffers in the free list is less than the min buffers;
 - A miss occurs because there are no buffers in the free list;
 - Both of the previous situations.

*Text taken from http://www.cisco.com/en/US/products/hw/modules/ps2643/products_tech_note09186a0080093fc5.shtml

5. Conclusions and Recommendations

The main purpose of network security for most businesses is to maintain availability, confidentiality, and integrity. As found from the tests conducted on the router and switch, both devices show vulnerabilities and weakness that affect security. An attacker can use these vulnerabilities to gain access and control of the devices, causing service interruptions such as a DoS attacks or flood attacks.

To help increase securing of the switch and the router, the following are recommended:

Countermeasures against Password Cracking Tools

- Upgrade the router's and switch's IOS to one that supports SSHv2.
- Use a minimum of 8 characters for passwords and ensure that password complexity requirements are met with a mixture of upper case, lower case, numeric, and special characters.
- Using default user account names, such as "admin", "operator", and "guest", should be avoided.
- Ensure the password does not contain any continuous part of the user account characters, such as "admin123".
- Enable and apply lockout policies to all user accounts to limit the number of retry attempts to guess passwords using password cracking tools.
- Enable and apply lockout policies based on individual protocols. E.g. SSH lockout after the configured number of retry attempts should not affect HTTPS login attempts.
- Configure a time delay between every retry login attempt. This will consume more time for the brute force and dictionary attack to process.
- o Disable all unused user accounts in the router and switch.
- Configure and enable remote syslog to track continuous login failures within a given interval and to record all login combinations such as invalid usernames, invalid passwords, empty usernames and empty passwords. These failed login attempts should be audited and an alarm should be configured on the device whenever an authentication failure occurs.
- Authenticate passwords using remote RADIUS server or TACACS+ server apart from local authentication for enhanced security.

- Password reset/change, user account creation, and permissions must require administration level privileges. All other user accounts must not have the same level of controls.
- Do not use shared user accounts since the original source cannot be determined.
- Use a policy that will require the administrator to change password after a defined period of time.
- Disable the use of concurrent logins with the same user name.
- Limit the number of failed attempts from an IP address and lock it out. The use of IOS Login Enhancements (Login Block) feature will prevent "Dictionary-attacks / Brute-force attacks".
- Always upgrade the router and switch to the latest software release to avoid security vulnerabilities related to authentication and for enhanced feature support.

Countermeasures against Vulnerabilities Reported During Web Server Scanning

- Protecting the router and the switch from **Clickjacking:**
 - The web interface developer should send the proper browser response headers that instruct the browser not to allow framing from other domains. Another way is for the web interface developer to use frame-braking script.
 - Use Access Control Lists (ACLs). The network administrator can restrict the sessions to be from a trusted source, network, or IP address by using Access Control Lists (ACLs). By default there is no access control on any of the VTY ports. Using ACLs will add a layer of difficulty for hackers to attempt to break as they need to be in the trusted network to gain access to the router.
- Protecting against the XXS and XSRF vulnerabilities:
 - Cisco describes these vulnerabilities as they are about escaping characters in the URL that are sent to the HTTPS server. The fix for these vulnerabilities is to escape special characters in the URL string echoed in the response generated by the web application.
 - Security products such as Cisco Iron port Web Security Appliances and Cisco ACE Web Application Firewall can be used to protect against objects that trigger malicious requests.
- To protect against **MIME incorrect or missing types**, an IOS Firewall can be used. It will provide MIME type filtering service.

Ways to secure SNMP communication in the network

- It is highly recommended to use SNMP v3 since it supports both Authentication and Privacy. SNMP v3 provides secure communication between the SNMP client and server by authenticating each other using a secret key and encrypting the data between them with configured privacy keys.
- Moreover, the following steps can be enforced in the router and switch to enhance SNMP security:
 - Disabling the SNMP service and closing the port whenever not in use;
 - Configuring the device to raise alarms whenever there is a SNMP action with wrong community strings;
 - Enabling SNMP syslogs will log configuration changes;
 - Enabling and using strong authentication protocol (MACSHA) instead of weak protocols (HMACMD5) for SNMPv3;
 - Enabling and using strong privacy protocol (CBC-DES) for SNMPv3 in the device;
 - Controlling the read and write permissions in the router and switch when SNMP is enabled;
 - Enabling automatic SNMP disabling whenever:
 - More than certain SNMP authentication retries are performed in a given interval. This prevents the attacker from running any tool or script which tries to figure out the SNMP authentication password;
 - There are a series of community string mismatches within a given interval while using SNMP v1 or v2.

Measures to improve SSL/TLS communication performance

- Ensure to disable weak protocols like SSLv2 as it is vulnerable to "man-in-the-middle" attacks in which an active attacker can force both the client and the server to use 40-bit encryption. It exclusively uses the MD5 hash function and uses a weak message authentication code (MAC). It also uses the same key for authentication and encryption.
- It is highly recommended to ensure the devices have a valid certificate with the correct domain name and issued by a trusted Certificate Authority.
- Renew or request for new certificates before it expires since expired certificates are considered invalid and can lead to potential security issues.

- Try to avoid using self-signed certificates. A self-signed certificate will allow the application to encrypt data and ensure its integrity in transit, but it provides no authentication.
- Do not use certificates with public key lengths less than 1024 bits.
- Never use NULL cipher suites as it leaves the communication channel in plain text and susceptible to eavesdropping attacks. A cipher suite is a set of authentication (RSA, DSA), encryption (3DES, AES, IDEA, RC4), and data integrity algorithms (SHA, MD5) used for exchanging messages between network entities.
- Do not use weak ciphers like the one using 40 or 56 bit key lengths. Weak ciphers could be broken and would allow the decryption of communications.
- Use strong ciphers like AES and 3DES with 128 bit key lengths or more.
- Use secure hashing algorithms (SHA) for signing the digital certificate other than MD5.
 MD5 is vulnerable to collision attacks in which an attacker can construct forged data in a variety of forms that will cause the application to incorrectly identify it as trustworthy.
- Use of strong cipher suites (SSL_RSA_WITH_AES_256_CBC_SHA) is highly recommended over weak cipher suites (SSL_EXP-RC4-MD5).
- To prevent denial-of-service (DoS) attacks, it is a good idea to disable client-initiated SSL renegotiation.
- Client certificates can be used with TLS to prove the identity of the client to the server.
- Configure and enable HTTP traffic redirection to HTTPS port 443 for secure communication over SSL/TLS.
- TLS compression must be disabled in the server to protect against CRIME (Compression Ratio Info-leak Made Easy) attack.

Countermeasures against Flooding Attacks

Clearly a DoS attack is very bothersome and will affect service quality and reliability. An online business might suffer a financial loss as a result. Following are some recommendations to help protect against such attacks:

- Disable any unused TCP/UDP services. If the service is required, a proxy can be configured and used to help protecting against DoS.
- Disable NTP if not required. If it is required then ensure using a trusted source for time synchronization with a proper NTP version that supports authentication.

- Define connection limits to increase the size of the TCP connection queue, to decrease the connection establishment period, and to employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted.
- Use resource and bandwidth throttling techniques for incoming TCP/UDP packets.
- Configure and enable port rate limiting in all ports.
- Configure and enable Control Planning Plane (CoPP) if supported by the specific router/switch. It will ensure device stability and packet delivery.
- Validate and filter all incoming traffic in each port.
- Use a network Intrusion Detection System (IDS) to automatically detect and respond to SYN attacks.

Additional security measures to improve the overall network security

- o Disable all unused protocols, services and unnecessary ports.
- Use Committed Access Rate (CAR) to limit or drop suspicious traffic. The use of CAR along with ACLs will monitor traffic and drop additional traffic when the average rate and burst rate are exceeded.
- A Firewall can be used as a first line of defense. It can monitor the incoming packets to check for any malformation, which if detected it will be dropped, and log the event and the offender information.
- Use buffer auto tuning. This feature when enabled will help set the buffer parameters properly to provide better performance.
- Apply Thresholds and Timeouts. This will help detect auto tools that are being used for sending frequent requests. It also helps to identify frequent attempts to submit requests to the same URL as happens during a Fuzzing attack. The idea of this solution is to preset the threshold to a certain number, start a counter for every session ID, and then increment the counter every time a request from the same session ID is received. When the counter reaches the threshold, the session ID will be revoked and any further data submitted from this session ID will be ignored.
- Encrypt communication fully, including authentication credentials. This prevents sniffed packets from being useful for an attacker. SSL and IPSec (Internet Protocol Security) are the best encryption solutions.
- Filter outgoing packets that appear to originate from an invalid local IP address.
- Use TLS/SSL to create a secure communication channel and only pass the authentication cookie over an HTTPS connection.

- Configure expired sessions (timeouts) appropriately, including all cookies and session tokens. This forces authentication after a relatively short time interval. Although this does not prevent replay attacks, it reduces the time interval in which the attacker can replay a request without being forced to re-authenticate because the session has timed out.
- Configure session inactivity timeout based on balancing risk and functional requirements.
- Verify device log files for any backend TLS connection failures, attempts to connect with invalid or expired session tokens, and access control failures.
- Service-accounts or accounts supporting connections to or from external systems should have the least privilege possible.
- Ensure routers, switches, servers, frameworks and system components are running the latest approved version.
- Regularly regenerate cryptographic keys and certificates for SSH and SSL to avoid security issues.
- Monitor the status of all routers and switches by deploying Network Management Systems.
- Use the router/switch IOS that supports the following security features; Stateful firewall, IPS, VPN Routing and Forwarding aware firewall.

Appendices

Appendix A - Password cracking tests screen shots

Router test screen shot

2 00 metaka metaka 200 m	
COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta22 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta22 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4 complete) Password jerthia (150 of 402 complete) COMM GCC: [http: Hest: 122.100.10.1 (i of 1. 0 complete) her: delta23 is of 30.4	
CANT OEC: [http://dx.iii.02.160.10.1 [c] of 1, 0 complete) User: stanl22 (5 of 302, 4 complete) Assumption (stanler) (200 or (100 or (
COMP GEC: [http://soil.10.1.64.0.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 complete) Research charter IGG of 402 cmglete) COMP GEC: [http://soil.10.1.6.0.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 complete) Research charter IGG of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research charter IGG of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research charter IGG of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research charter IGG of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] (16 of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] (16 of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] (16 of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] (16 of 402 cmglete) COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Research subset] COMP GEC: [http://soil.10.1.6 of 1. 0 cmglete) Der: sdinl23 (5 of 80.4 cmglete) Researc	
COMF GECS: [http://doi.org/10.0000/000000000000000000000000000000	
COMT OECC: [http://dx:120.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B3 of 402 complete) COMT OECC: [http://dx:120.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B3 of 402 complete) COMT OECC: [http://dx:120.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B3 of 402 complete) COMT OECC: [http://dx:120.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B3 of 402 complete) COMT OECC: [http://dx:120.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B5 of 402 complete) COMT OECC: [http://dx:120.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B5 of 402 complete) COMT OECC: [http://dx:130.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B5 of 402 complete) COMT OECC: [http://dx:130.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B5 of 402 complete) COMT OECC: [http://dx:130.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B5 of 402 complete) COMT OECC: [http://dx:130.106.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtre (B5 of 402 complete) COMT OECC: [http://dx:130.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtra (D f 402 complete) COMT OECC: [http://dx:130.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtra (D f 402 complete) COMT OECC: [http://dx:130.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtra (D f 402 complete) COMT OECC: [http://dx:130.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtra (D f 402 complete) COMT OECC: [http://dx:130.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtra (D f 402 complete) COMT OECC: [http://dx:130.10.1 [d f], 0 complete) User: seturi2 (d f 20, 4 complete) Password: subtra (D f 4	
COMT OECC: [http://strip.doi.of.u.doi.o	
CANT OECC: [http://striplestri	
COMT OECC: [http: Host: 122.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: setures: [] Of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: setures: [] Of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: setures: [] Of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] Of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] Of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: Patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: patrames: [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete) User: setuni22 (] of 302, 4 complete) Password: setune [] of 402 complete) COMT OECC: [] http: Host: 120.160.10.1 [] of 1, 0 complete] User: setuni22 (] of 302, 4 complete) Password:	
QMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal starwars.(100 of 402 complete) QMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal starwars.(100 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal starwars.(100 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal bits (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal bits (1 of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal bits (1 of 4 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal bits (1 of 4 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal bits (1 of 4 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 b of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4 complete) Personal star (1 b of 402 complete) DMUT OECC: Introj Hesti 120:100.101 (i of 1. 0 complete) User admin120 (b of 302, 4	
DWT OECK: [http://sori 102.100.10.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password whily (122 of 402 complete) AWT OECK: [http://sori 102.100.10.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password while (123 of 402 complete) DWT OECK: [http://sori 102.100.10.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password while (123 of 402 complete) DWT OECK: [http://sori 102.100.10.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password while (123 of 402 complete) DWT OECK: [http://sori 102.100.10.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.10.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password parallel (liz of 402 complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password parallel (liz of 402 complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password parallel (liz of 402 complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password parallel (liz of 402 complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password parallel (liz of 402 complete) DWT OECK: [http://sori 102.100.1 [cf 1. 0 complete) User addmil2 (c of 302. 4 complete) Password parallel (liz of 402 compl	
DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal kelly (172 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Lution (173 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Lution (175 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Lution (175 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Lution (175 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Lution (175 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Lution (175 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Rution (175 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Rution (115 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Rution (101 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Rution (101 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Rution (101 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal Rution (101 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal (101 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302, 4 complete) Personal (101 of 402 complete) DWT GEC. Intrp: Hest: 192,103,10.1 dt of 1. 0 complete) Her: admin123 (5 of 302,	
CMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (17 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (18 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (18 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (12 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (12 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (12 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (100,000) (100 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h of 1, 0 complete) User: addm.123 (5 of 302, 4 complete) Password: marks (100 of 402 complete) DMUT GECOL (http: Hest 152,108,10.1 (h	
AMT GECC: [http: Hest: 122.100.10.11 (i of 1. 0 complete) use: admin.22 (5 of 202.4 complete) Password: bitsed (177 of 402 complete) AMT GECC: [http: Hest: 122.100.10.11 (i of 1. 0 complete) use: admin.22 (5 of 202.4 complete) Password: bitsed (177 of 402 complete) DAT GECC: [http: Hest: 122.100.10.11 (i of 1. 0 complete) use: admin.22 (5 of 202.4 complete) Password: bitsed (177 of 402 complete) DAT GECC: [http: Hest: 122.100.10.11 (i of 1. 0 complete) use: admin.22 (5 of 202.4 complete) Password: bitsed (177 of 402 complete) DAT GECC: [http: Hest: 122.100.10.11 (i of 1. 0 complete) use: admin.22 (5 of 202.4 complete) Password: password: bitsed (177 of 402 complete) DAT GECC: [http: Hest: 122.100.10.11 (i of 1. 0 complete) use: admin.22 (5 of 202.4 complete) Password: pa	
AME OFCON: IntEp Hest: 122.100.10.1 (1 of 1. 0 complete) User: admini22 (5 of 302, 4 complete) Password: miring in the Car of 402 complete) AME OFCON: IntEp Hest: 122.100.10.1 (1 of 1. 0 complete) User: admini22 (5 of 302, 4 complete) Password: miring in the Car of 400 complete) AME OFCON: IntEp Hest: 122.100.10.1 (1 of 1. 0 complete) User: admini22 (5 of 302, 4 complete) Password: miring in the Car of 400 complete) AME OFCON: IntEp Hest: 122.100.10.1 (1 of 1. 0 complete) User: admini22 (5 of 302, 4 complete) Password: password	
<pre>XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (179 of 402 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (100 of 402 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (120 of 402 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (120 of 402 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (120 of 402 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (1 of 2 of 422, complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (1 of 2 of 422, complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, system (1 of 2 of 422, complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 of 2 of 420 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 of 422 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 of 420 complete) XMT OEC: Intpl Hest 122.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 user 1402 complete) XMT OEC: Intpl Hest 132.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 user 1402 complete) XMT OEC: Intpl Hest 132.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 user 1402 complete) XMT OEC: Intpl Hest 132.200.10.1 (1 of 1, 0 complete) user, admini22 (5 of 322, 4 complete) Password, share (1 user 1402 complete) XMT OEC: Intpl Hest 132.200.10.1 (1 of 1, 0 complete) user, admini23</pre>	
AMT OECC: Intpl Hest: 102.100.10.10 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) pogsimb (101. of 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: geraid (122.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: geraid (122.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: geraid (122.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: geraid (122.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: geraid (122.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: geraid (122.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: docdmyntl (120.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: docdmyntl (120.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: docdmyntl (120.6 402 complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 of 202.4 complete) Password: complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 d) 202.4 complete) Password: complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.22 (5 d) 202.4 complete) Password: complete) Password: complete) XMT OECC: Intpl Hest: 102.100.10.1 (1 of 1. 0 complete) user: admin.23 (5 d) 202.4 complete) Password: plates plates XMT OECC: Intpl Hest: 102.100.1 (1 of 1. 0 complete) user: admin.23 (5 d) 202.4 complete) Password: plates plates XMT OECC: Intp	
URT GECC. [http] Hott. 102.106.10.1 [d fl. 0 complete) User: admini22 (S of 302.4 complete) Passwort: jordani [102 of 402 complete) DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete) User: admini22 (S of 302.4 complete) Passwort: jordani [102 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete) User: admini22 (S of 302.4 complete) Passwort: jordani [102 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete) User: admini22 (S of 302.4 complete) Passwort: jordani [102 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete) User: admini22 (S of 302.4 complete) Passwort: jordani [103 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete) Passwort: jordani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete) Passwort: jordani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete) Passwort: jordani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.10.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete) Passwort: jordani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete] Passwort: joldani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete] Passwort: joldani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete] Passwort: joldani [105 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S of 302.4 complete] Passwort: joldani [106 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S d 302.4 complete] Passwort: joldani [106 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S d 302.4 complete] Passwort: joldani [106 of 402 complete] DRT GEC. [http] Hott. 102.106.1 [d fl. 0 complete] User: admini22 (S d 302.4 complete	
DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: 0.00003 (166 of 402 complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: dady1 (185 of 402 complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: dady1 (185 of 402 complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: dady1 (185 of 402 complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: dady1 (185 of 402 complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: dady1 (185 of 402 complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: admini2 (5 of 822. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: admini2 (5 of 822. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: admini2 (5 of 822. ecomplete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini22 (5 of 822. 4 complete) Password: admini2 (5 of 822. ecomplete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini23 (5 of 822. 4 complete) Password: admini2 (5 of 482. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini23 (5 of 822. 4 complete) Password: admini2 (5 of 482. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) user: admini23 (5 of 882. 4 complete) Password: admini (5 of 482. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) User: admini23 (5 of 882. 4 complete) Password: admini (5 of 482. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete) User: admini23 (5 of 882. 4 complete) Password: admini (5 of 482. complete) DMF OFCN: [http: Host: 192.108.10.1 G of 1. 0 complete)	
AMT OBCON: [http://doi.org/1.102.109.10.11.11.07.1.0 complete/users/mathrmat/21.07.07.092.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4.4	
XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini122 (5 of 302, 4 complete) Password; diddysjsrl (BF of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; billbookgn (BB of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; billbookgn (BB of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; fromy (Bo of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; fromy (Bo of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; fromy (Bi of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (2 of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.108.10.1 (1 of 1, 0 complete) user; admini21 (5 of 302, 4 complete) Password; erks (1 go of 402 complete) XMT OECC: [http://bst.102.10.1 (bo of 0, 0 complete) use	
UMT (DECX: [http:/Hoit.102.108.10.11 (d f L 0 complete) user: admini22 (5 of 22.2 complete) billabog (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.10.11 (d f L 0 complete) user: admin22 (5 of 22.2 complete) Password: carbear (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.10.11 (d f L 0 complete) user: admin22 (5 of 23.2 complete) Password: carbear (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.10.11 (d f L 0 complete) user: admin22 (5 of 23.2 complete) Password: carbear (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.10.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: plays (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: plays (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: plays (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: plays (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: plays (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: plays (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: skare (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 23.2 complete) Password: skare (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 38.2 complete) Password: skare (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 38.2 complete) Password: skare (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 38.2 complete) Password: skare (100 of 402 complete) MMT (DECX: [http:/Hoit.102.108.11 (d f L 0 complete) user: admin23 (5 of 38.2 complete) Password: skare (100 of 48.2 complete)	
VMF OHECN: [http:/Host.102.108.1.07.1.07.1.07.1.07.1.07.1.07.1.07.	
UMT GECK: [http://exi.loz.1.G.afl.g.Complete/user.adsnill.22_G.5d?202_4.complete/Password_pinky [G3.6f.4G2_Complete) MMT GECK: [http://exi.loz.1.G.afl.g.Complete/user.adsnill.22_G.5d?302_4.complete/Password_erikk_G2.6f.4G2_Complete) UMT GECK: [http://exi.loz.1.G.afl.g.Complete/user.adsnill.22_G.5d?302_4.complete/Password_erikk_G2.6f.202_complete) UMT GECK: [http://exi.loz.1.G.afl.g.Complete/user.adsnill.22_G.5d?302_4.complete/Password_erikk_G2.6f.36f.4G2_complete)	
UMT O BECX: [http]Host. 192.168.10.1 (1 of 1, 0 complete)User: admin123 (5 of 382, 4 completes)Password: ancar (192 of 402 complete) MET O BECX: [http]Host. 192.168.10.1 (1 of 1, 0 completes)User: admin123 (5 of 382, 4 completes)Password: skater	
100 - 2000 [11110] - 2011 - 2012 - 20	

Router website show version command

🖉 💷 🔤 Delphin	🤰 🙋 Firefox-bin	👔 🖬 Konsole	👔 🔡 setting up ssh-https.odt – 🛛 🛗 test notes and results.oc 👘 🛠 TFTPgu	🕤 🚭 4)) 38.13 pm(
• maz Aevel/15/exec/show/tec				19 2 8 19
ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> o	and the second se			
maz /level/15/exec/show/te				
🗧 📫 😽 😽 192.168.10.	1/exec/show/tech-support/cr		습 • 🗃 🚺 · Goog	
BackTrack Linux 👔 Offensiv	re Security DExploit-DB Airo	crack-ng 📓 SomaFM		
	sion			
Cisco Internetwork Operating IOS (tm) C2600 Software (C28 Fechnical Support: http://w Copyright (c) 1985-2007 by o Compiled Wed 24-Jan-07 16:4 Image text-base: 0x80008098.	800-IK903S3-M), Version 12.3(2 ww.cisco.com/techsupport cisco Systems, Inc. B by ccai	2), RELEASE SOFTWARE (fc2)		
ROM: System Bootstrap, Vers: ROM: C2600 Software (C2600-1	ion 11.3(2)XA4, RELEASE SOFTWAI IK90353-M), Version 12.3(22), I	RE (fcl) RELEASE SOFTWARE (fc2)		
waz uptime is 20 minutes System returned to RCM by re System image file is "flash	eload :c2600-ik903s3-mz.123-22.bin*			
States and local country law use. Delivery of Cisco crypt hird-party authority to imp importers. exporters, distri- compliance with U.S. and loc ugree to comply with applics	ographic features and is subje- we governing import. export, to tographic products does not im- port, export, distribute or us- ibutors and users are responsil cal country laws. By using thi- able laws and regulations. If 7 al laws, return this product ii	ransfer and ply e encryption. ble for s product you you are unable		
summary of U.S. laws gover http://www.cisco.com/wwl/exp	rning Cisco cryptographic prode port/crypto/tool/stqrg.html	ucts may be found at:		
f you require further assis xport@cisco.com.	stance please contact us by se	nding email to		
Processor board ID JAB03260 4060 processor: part number Bridging software. X.25 software. Version 3.0.0 2 FastEthernet/IEEE 802.3 in 13% bytes of non-volatile co	0, mask 49 0. nterface(s)	K/6144K bytes of memory.		
Configuration register is G	×2102			
£ Find:	(Province) P. Naut ()	Same Match case		
			98:13 pm	

Router wireshark screen shot

🐝 🚍 🗃 Dolphin 👔 🕲 Using Hydra and 🕅 🖉 Foofus Net	orking 🗈 Konsole 🦩 🗊 Kwrite 🤰 🕅 TFTPgui 🚺 medusa-packets. 🕽 🎘 Xpdf: /me	rdia/8858 👔 😪 <) 09:16 pm 🌘
🚺 🛇 medusa-packets.log [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]	A Follow TCP Stream	× _ = ×
Eile Edit View Go Capture Analyze Statistics Telephony Tools	Stream Content	
	GET / HTTP/1.1 Host: 192.168.10.1:80	-
Filter: tcp.stream eq 3243	User-Agent: Teh Forest Lobster Authorization: Basic YWRtaW4xMjM6bXlwYXNzd29yZA==	
No. Time Source Destination	HTTP/1.1 200 0K	-
33198 3862.215842 192.168.10.1 192.168.10.2	Date: Mon, 01 Mar 1993 00:57:08 GMT	
33199 3862.215857(192.168.10.2 192.168.10.1	Server: cisco-IOS Transfer-Encoding: chunked	
33200 3862.215889(192.168.10.2 192.168.10.1	Content-Type: text/html	
33201 3862.228799(192.168.10.1 192.168.10.2	Expires: Mon, 01 Mar 1993 00:57:08 GMT	
33202 3862.228817(192.168.10.2 192.168.10.1	Last-Modified: Mon, 01 Mar 1993 00:57:08 GMT	
33203 3862.229210(192.168.10.2 192.168.10.1 33204 3862.230837(192.168.10.1 192.168.10.2	Cache-Control: no-store, no-cache, must-revalidate Accept-Ranges: none	
33204 3852.23083/192.168.10.1 192.168.10.2 33205 3862.230853(192.168.10.2 192.168.10.1	Accept-Hanges: hone	
33205 3862,231963(192,168,10,1) 192,168,10,2		
33207 3862.231967(192.168.10.2 192.168.10.1		
33208 3862.233070/192.168.10.1 192.168.10.2		
00000 0000 00003 H 100 1 00 1 0 0 1 00 1 0		•
Frame 33203: 54 bytes on wire (432 bits), 54 bytes captured by the state of the		
 Ethernet II, Src: CompalIn_8d:91:66 (00:1e:ec:8d:91:66), Internet Protocol Version 4, Src: 192.168.10.2 (192.168) 		
Transmission Control Protocol. Src Port: 37384 (37384).	Entire conversation (411 bytes)	
Fransmission control Protocol, Src Port. 37364 (37364),	Save As Print ASCII EBCDIC Hex Dump C Arrays ● Raw	
	₩ Elep Stream Close	
		-
0000 00 08 21 96 f3 01 00 1e ec 8d 91 66 08 00 45 00 .		
	(.@.@.	F
0020 0a 01 92 08 00 50 02 16 2c 2a 7f af fb a2 50 11 .	P. ,*P.	
0030 3c b8 95 6e 00 00 <	.n	-
● M File: "/root/Desktop/medusa-packet Packets: 33210 Displayed:	13 Marked: 0 Load time: 0:00.736 Profile: Default	
?< 🗃 🔹 💽 🖗 📣 💻	09:16 pm (C	

Switch test screen shot

1 1	medusa-router	📲 🙋 Cisco Catalyst 🔅	😢 Firefox-bin	2 🗈 Konsole	🧃 🚺 Kwrite	3 🔚 test notes and 👘 🚵 OpenOffice.or 3 🕺 TFTPgui	📶 Capturing from 👔 🚭 d	08:56 pm((
🖿 🔹 : medus	a							- 5 1
		s Settings Help						
			1. O complete) L	Jser: admin (1 of (6. O complete) Password	: janice (858 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of)	1, O complete) U	Jser: admin (1 of 6	6, O complete) Password	: cowboys (859 of 14344392 complete)		
						: myself (860 of 14344392 complete)		
						: lipgloss (861 of 14344392 complete) : jazmin (862 of 14344392 complete)		
						: jazmin (862 of 14344392 complete) : rosita (863 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of	1, O complete) (Jser: admin (1 of 6	5, O complete) Password	: happyl (864 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of :	1, O complete) U	Jser: admin (1 of 6	5, O complete) Password	: felipe (865 of 14344392 complete)		
						: chichi (866 of 14344392 complete)		
						: pangit (867 of 14344392 complete) : mierda (868 of 14344392 complete)		
						: genius (869 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of	1, O complete) L	Jser: admin (1 of 6	6, O complete) Password	: 741852963 (870 of 14344392 complete)		
						: hernandez (871 of 14344392 complete)		
						: awesome (872 of 14344392 complete)		
						: walter (873 of 14344392 complete) : tinker (874 of 14344392 complete)		
						: arturo (875 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of)	1, O complete) L	Jser: admin (1 of 6	6, O complete) Password	: silvia (876 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of	1, O complete) l	Jser: admin (1 of 6	5, O complete) Password	: melvin (877 of 14344392 complete)		
						: celeste (878 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of .	1, U complete) (Jser: admin (1 of (G complete) Password: G complete) Password: 	: pussycat (879 of 14344392 complete) : gorgeous (880 of 14244392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of	1. O complete) L	ser: admin (1 of (6. 0 complete) Password	: davidl (881 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of)	1, O complete) L	Jser: admin (1 of 6	6, O complete) Password:	: molly (882 of 14344392 complete)		
						honeyko (883 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of	1, 0 complete) (Jser: admin (1 of 6	6, O complete) Password	: mylife (884 of 14344392 complete) : animal (885 of 14344392 complete)		
						: animal (885 of 14344392 complete) : penguin (886 of 14344392 complete)		
						: babyboo (887 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of)	1, O complete) L	Jser: admin (1 of 6	6, O complete) Password	: loveu (888 of 14344392 complete)		
						: simpsons (889 of 14344392 complete)		
						: lupita (890 of 14344392 complete)		
						: boomer (891 of 14344392 complete) : panthers (892 of 14344392 complete)		
						: hollywood (893 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of)	1, O complete) L	Jser: admin (1 of 6	6, O complete) Password:	: alfredo (894 of 14344392 complete)		
						: musica (895 of 14344392 complete)		
						: johnson (896 of 14344392 complete) : ilovegod (897 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host: K: [http] Host:	192.168.10.3 (1 of .	1, O complete) (1. O complete) (lser: admin (1 of 6	5, O complete) Password 5, O complete) Password	: hawaii (898 of 14344392 complete)		
						: sparkle (899 of 14344392 complete)		
ACCOUNT CHECK	K: [http] Host:	192.168.10.3 (1 of)	1, O complete) U	Jser: admin (1 of 6		: theking (900 of 14344392 complete)		
ACCOUNT FOUND	D: [http] Host:	192.168.10.3 User:	admin Password:	theking [SUCCESS]				
root@bt:/#								
					_			
			: medusa					
20 🖂 🚽	()	<u></u>		8-10 March 100	08:56 pm			
				112	00.50 pm			

Switch website show version command

mint709-switch /level/15/exec//show/version - Mozilla Frefox		
⊙ mm//09-awtch/level/12/exeC/vahowkretaion - Mozila Hrefox le Edit View History Bookmarks Tools Help		- 8
mit709-switch /eve/l/switch/		
S (192.168.10.3/level/15/exec/-/show/version	्रे र 🔁 🛃 र Google	0
BackTrack Linux MOffensive Security MExploit-DB MAircrack-ng SomaFM		
mint709-switch		
Command		
eenmene		
utput		
nomand have UNL star / Inver(2)/secor/- mental star = there(13)/secor/-/show/version encode star = show version		
isco Internetwork Operating System Software G5 (tm) (25000L, 50ftware (23000L,-CB425-W), Version 12.0(5)wC3b, RELEASE SOFTWARE (fc1) oppright (c1) 0Be5-002 by ciscos Systems, Inc. omple text-base: 000003000, data-base: 0000337600		
OM: Bootstrap program is C3500XL boot loader		
inf700-switch uptime is 3 minutes griem returned to FCM by relaad griem issage file is "flash:c55000L-c5N2s-mz.120-5.WC30.bin"		
isco NS-C3524-PWR-XL (PowerPC403) processor (revision 0x01) with 8152K/1024K bytes of memory. rocessor board ID O-KN0730MPB, with hardware revision 0x00 ast reset from ware-reset		
rocessor is running Enterprise Edition Software Luster command avitch capable Luster member suitch capable and		
2 A bytes of flash-simulated non-volatile configuration memory. ase ethernat MAC Address: 00.08/BE/B9/33:00 totherboard sessial number: LT0702000A otherboard serial number: LT0702000A		

Appendix B - Web server scanning tests screen shots

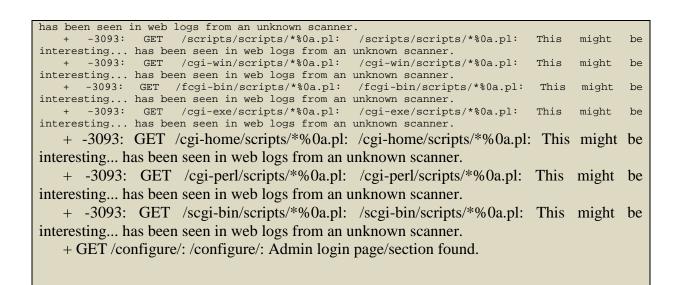
Router Nikto test screen shot

	Maz nevel/15/exec/sno V Hrelox-bin	3 Ankto -C all - Google St La Konso	10 actual router test and	Thicto-router-nitps-wire	33.5
nikto : perl					-
Edit View Bookmarks Settin					
'force_bodysnatch' 'http_eol' => *\r\n 'force_close' => 0, 'N4GIC' => 31339 },					
'User-Agent' => 'Mozilla/5. 'Host' => '192.168.10.1:443	00 (Nikto/2.1.5) (Evasions:None) (Test:00 VRtaW4xMjM6bXl√YXNzd29yZA=='	36608)*,			
hu Sep 5 01:45:01 2013 'Result 'connection' => 'close', 'whisker' => { 'protocol' => 'HTTP 'lowercase_incoming, 'http_space2' => ' 'stats reas' => 219'	headers' => 1,				
'http_spacel' => ' 'code' => 404, 'ssl_cert_issuer' =: 'ssl_cert_subject' 'stats_syns' => 220	', > '/CN=maz.mint709-domain/unstructuredNam →> '/CN=maz.mint709-domain/unstructuredNa 31,				
'message' => 'Not F 'header_order' => ['date', 'server', 'connection	≥r_sync.php?c-phpinfo()', >und',				
'accept-ran], 'http_data_sent' => 'socket_state' => O 'ssl_cipher' => 'DE 'MAGIC' => 31340, 'http_eol' => *\r\n					
}, 'date' => 'Mon, Ol Mar 1993 'accept-ranges' => 'none', 'server' => 'cisco-IOS'					
nd Time: 2013-09-05 01	nd 48 item(s) reported on remote host 45:01 (GMT-6) (18358 seconds)				
host(s) tested hu Sep 5 01:45:01 2013 + 22083 hu Sep 5 01:45:01 2013 T:Thu Se tabt:/pentest/web/nikte=					
1	nikto : perl				
R R		03.55 am			

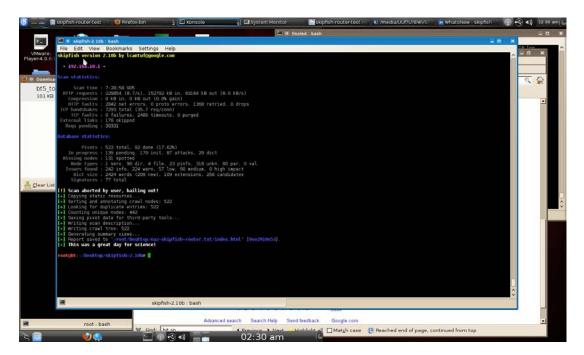
Router Nikto test output

- Nikto v2.1.5/2.1.5
+ Target Host: 192.168.10.1
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
- Nikto v2.1.5/2.1.5
+ Target Host: 192.168.10.1
+ Target Port: 443
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /: Hostname '192.168.10.1' does not match certificate's CN 'maz.mint709-
domain/unstructuredName=maz.mint709-domain'
+ GET /: Successfully authenticated to realm 'level 15 access' with user-supplied
credentials.
+ GET /exec/show/config/cr: /exec/show/config/cr: The Cisco router's web install allows
arbitrary commands to be executed remotely.
+ -3092: GET /template/: /template/: This may be interesting as the directory may hold
sensitive files or reveal system information.
+ -3093: GET /cqi.cqi/ncommerce3/ExecMacro/macro.d2w/%0a%0a:
/cqi.cqi/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting has been seen in
web logs from an unknown scanner.
+ -3093: GET /webcqi/ncommerce3/ExecMacro/macro.d2w/%0a%0a:
/webcgi/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting has been seen in
web logs from an unknown scanner.
+ -3093: GET /cqi-914/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /cqi-
914/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting has been seen in web
logs from an unknown scanner.
+ -3093: GET /cgi-915/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /cgi-
915/ncommerce3/ExecMacro/macro.d2w/80a80a: This might be interesting has been seen in web
logs from an unknown scanner.
+ -3093: GET /bin/ncommerce3/ExecMacro/macro.d2w/%0a%0a:
/bin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting has been seen in web
logs from an unknown scanner.
+ -3093: GET /cqi/ncommerce3/ExecMacro/macro.d2w/%0a%0a:
/cgi/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting has been seen in web
logs from an unknown scanner.

/mpcgi/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgi-bin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /cgibin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. /ows-bin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: -3093: GET /owsbin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /cgi-sys/ncommerce3/ExecMacro/macro.d2w/%0a%0a: + /cgisys/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. /cgi-local/ncommerce3/ExecMacro/macro.d2w/%0a%0a: -3093: GET /cqilocal/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: /htbin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: GET /htbin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /cgibin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /cgibin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. GET /cgis/ncommerce3/ExecMacro/macro.d2w/%0a%0a: -3093: /cgis/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /scripts/ncommerce3/ExecMacro/macro.d2w/%0a%0a: + /scripts/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /cgi-win/ncommerce3/ExecMacro/macro.d2w/%0a%0a: + /cqiwin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /fcgi-bin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /fcqibin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /cgi-exe/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /cgi-+ exe/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /cgi-home/ncommerce3/ExecMacro/macro.d2w/%0a%0a: + /cgihome/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /cgi-perl/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /cgiperl/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. -3093: GET /scgi-bin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: /scgibin/ncommerce3/ExecMacro/macro.d2w/%0a%0a: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgi.cgi/scripts/*%0a.pl: /cgi.cgi/scripts/*%0a.pl: This might be interesting ... has been seen in web logs from an unknown scanner. + -3093: GET /webcgi/scripts/*%0a.pl: /webcgi/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. GET /cgi-914/scripts/*%0a.pl: /cgi-914/scripts/*%0a.pl: + -3093: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgi-915/scripts/*%0a.pl: /cgi-915/scripts/*%0a.pl: This might be interesting ... has been seen in web logs from an unknown scanner. + -3093: GET /bin/scripts/*%0a.pl: /bin/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgi/scripts/*%0a.pl: /cgi/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /mpcgi/scripts/*%0a.pl: /mpcgi/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgi-bin/scripts/*%0a.pl: /cgi-bin/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /ows-bin/scripts/*%0a.pl: /ows-bin/scripts/*%0a.pl: This might be interesting ... has been seen in web logs from an unknown scanner. GET /cgi-sys/scripts/*%0a.pl: /cgi-sys/scripts/*%0a.pl: + -3093: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgi-local/scripts/*%0a.pl: /cgi-local/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /htbin/scripts/*%0a.pl: /htbin/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner. + -3093: GET /cgibin/scripts/*%0a.pl: /cgibin/scripts/*%0a.pl: This might be interesting ... has been seen in web logs from an unknown scanner. + -3093: GET /cgis/scripts/*%0a.pl: /cgis/scripts/*%0a.pl: This might be interesting...



Router Skipfish test screen shot



Switch Nikto test screen shot

🚍 📰 nikto switch test – 🛛 🕹 Authoriza	tion Requi 😢 Firefox-bin	2 🖾 Konsole	🧃 🚺 Kwrite	3 📔 nikto-switch-test-r	🔀 TFTPgui	Capturing from eth	ি 😌 ব	09:36 pm
nikto : perl								- 6
Edit View Bookmarks Settings Help	, ,							
simpleLogin/: Admin login page/section fo	und.							
smblogin/: Admin login page/section found								
sql-admin/: Admin login page/section foun ss vms admin sm/: Admin login page/sectio	id.							
ssladmin/: Admin login page/section found								
staradmin/: Admin login page/section four								
sub-login/: Admin login page/section foun Super-Admin/: Admin login page/section fo	id.							
support_login/: Admin login page/section to support_login/: Admin login page/section								
sys-admin/: Admin login page/section four								
sysadmin/: Admin login page/section found								
SysAdmin/: Admin login page/section found SysAdmin2/: Admin login page/section foun								
sysadmins/: Admin login page/section four								
system_administration/: Admin login page/	section found.							
system-administration/: Admin login page/	section found.							
ur-admin/: Admin login page/section found useradmin/: Admin login page/section found								
JserLogin/: Admin login page/section four	id.							
utility_login/: Admin login page/section	found.							
/2/painel/: Admin login page/section four vadmind/: Admin login page/section found.								
/mailadmin/: Admin login page/section found.	ind.							
vebmaster/: Admin login page/section four								
vebsvn/: Admin login page/section found. vizmysqladmin/: Admin login page/section								
vp-admin/: Admin login page/section vp-admin/: Admin login page/section found	tound.							
<pre>wp-login/: Admin login page/section found</pre>								
<pre>clogin/: Admin login page/section found.</pre>								
maint/: This might be interesting jk-status: mod_jk status page is visible.								
balancer-manager: mod proxy balancer mana	gement page is visible.							
servlets-examples/: Tomcat servlets examp	les are visible.							
admin-console: JBoss admin console is vis								
SVDB-3092: /messages/: This might be inte SVDB-3092: /cms/: This might be interesti	resting							
SVDB-3092: /helpdesk/: This might be inte	resting							
3rdparty/phpMyAdmin/: phpMyAdmin director	y found							
ohpMyAdmin/: phpMyAdmin directory found Brdparty/phpmyadmin/: phpMyAdmin director	w found							
phpmyadmin/: phpMyAdmin directory found	y Toulia							
oma/: phpMyAdmin directory found								
openadmin/: Informix OpenAdmin tool admin	istration login							
545 items checked: 1588 error(s) and 1006 nd Time: 2013-09-03 21:31:21 (0		ote nost						
host(s) tested								
t@bt:/pentest/web/nikto#								
	nikto : perl							
	nikto : pen							_
		00.0	6 pm	- (C				

Switch Nikto test output example

- Nikto v2.1.5/2.1.5

+ Target Host: 192.168.10.3

+ Target Port: 80

+ GET /: The anti-clickjacking X-Frame-Options header is not present.

- Nikto v2.1.5/2.1.5

+ Target Host: 192.168.10.3

+ Target Port: 80

+ GET /: The anti-clickjacking X-Frame-Options header is not present.

+ GET /: Successfully authenticated to realm 'level 15 access' with user-supplied credentials.

+ GET /kboard/: /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php

+ GET /lists/admin/: /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist

+ GET /ssdefs/: /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.

+ GET /sshome/: /sshome/: Siteseed pre 1.4.2 has 'major' security problems.

+ GET /tiki/: /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin

+ -637: GET /~root/: /~root/: Allowed to browse root's home directory.

+ GET /cgi-bin/wrap: /cgi-bin/wrap: comes with IRIX 6.2; allows to vie



Appendix C - SNMP enumeration tests screen shots

Router SNMP enumeration test screen sho	t
---	---

			and rest sporte	110 Peteropeteropeter	Income indoces a com	erito twitesti		
Snmpcheck : bash								
File Edit View Bookma								-
Interface	: up FastEthernet0							
Interface speed IP Address Netmask	: 00:08:21:96:f3:00 : 100 Mbps : 192,168.10.1 : 255,255.255.0 : 1500							
Interface Speed MTU Bytes In	: 00:08:21:96:f3:01 : 100 Mbps : 1500 : 90246 (89K) : 104648 (103K)							
Interface Speed MTU	: 1.544 Mbps : 1500							
Interface Speed MTU	: 1.544 Mbps : 1500							
Interface Speed	: 4294.967295 Mbps : 1500							
[*] Listening UDP ports								
192.160.10.1 161 192.160.10.1 162 192.160.10.1 2517 192.160.10.1 5060 192.160.10.1 50230								
[*] Enumerated 192.168.1 rootcbt:/pentest/enumerat								
8	sn	mpcheck : bash						
2 2	E 3 😪	(1)	08	:46 pm	(6			

Switch SNMP enumeration test screen shot

😡 — 🔤 snmp-switch	h - Dolphin 🦉 Catalyst 2950 and Car 🖾 Konsole	e 👘 🖬 System Monitor	a router-sept9-config	🚺 etho (Wireshark 1.8 🛛 🕤 🧐 🖓 📢 🥵 49 pm 😭
🔳 🔍 snmpcheck : bash	en reen hander in the			28.3
File Edit View Bookm				
Bytes In Bytes Out	: 64 (64) : 854 (854)			
Interface Speed MTU Bytes In	: 00:00:be:f9:53:00 : 100 Mbps : 1500 : 64 (64) : 856 (856)			
	: [up] FastEthernet0/11			
Interface Speed MTU Bytes In	: 03:0b:be:f9:53:0b : 1:00 Mbps : 1:500 : 64 (64) : 886 (886)			
Interface Speed NTU Bytes In	: 00:06:56:19:53:0c : 1:00 Mbps : 1:500 : 64 (64) : 886 (866)		•	
	: [up] FastEthernet0/13			
Interface Speed MTU Bytes In	: 00:0b:be:f9:53:0d : 100 Hbps : 1500 : 64 (64) : 866 (866)			
	: [up] FastEthernatO/14			
Interface Speed MTU Bytes In	: 00:0b:be:f9:53:0e : 1:00 Mbps : 1:500 : 64 (64) : 866 (866)			
Interface Speed MTU Bytes In	: 00:05:56:53:0f : 100 Mbps : 1500 : 64 (64) : 896 (896)			
2	snmpcheck : bash			
20		06:49 pm	(6)	
		00.49 pm		

Appendix D - SSL/TLS scanning tests screen shots

Nouter SSLSCAN test screen	SHUL				
🔣 🚍 🔤 ssiscan-router-test - 💷 🗹 University of Alberta 🕅 🗈 Konsole	14 setting up ssh-https.	🕅 TETPaui	ssiscan-router-wiresh	🗮 Xpdf 👔 🕤 😪 📢 08:	26 pm(6
	14			3 6 6 14	
🕮 📀 reet : ssiscan					6 X
File Edit View Bookmarks Settings Help					
root@bt:~# sslscan 192.168.10.1					~
<u>CCC(6(6]])</u>					
Version 1.8.2					
http://www.titania.co.uk					
Copyright Ian Ventura-Whiting 2009					
Testing SSL server 192.168.10.1 on port 443					
Supported Server Cipher(s):					
Rejected SSLv2 168 bits DES-CBC3-MD5 Rejected SSLv2 56 bits DES-CBC-MD5					
Rejected SSLV2 56 bits DES-CBC-MD5 Rejected SSLV2 40 bits EXP-RC2-CBC-MD5					
Rejected SSLV2 40 bits EAP-RL2-CBC-MD5 Rejected SSLV2 128 bits RC2-CBC-MD5					
Rejected SSLv2 40 bits EXP-RC4-MD5					
Rejected SSLv2 128 bits RC4-MD5					
Rejected SSLv3 256 bits ADH-AES256-SHA					
Rejected SSLv3 256 bits DHE-RSA-AES256-SHA					
Rejected SSLv3 256 bits DHE-DSS-AES256-SHA					
Rejected SSLv3 256 bits AES256-SHA					
Rejected SSLv3 128 bits ADH-AES128-SHA Rejected SSLv3 128 bits DHE-RSA-AES128-SHA					
Rejected SSLV3 128 bits DHE-DSS-AES128-SHA					
Rejected SSLv3 128 bits AES128-SHA					
Rejected SSLv3 168 bits ADH-DES-CBC3-SHA					
Rejected SSLv3 56 bits ADH-DES-CBC-SHA					
Rejected SSLv3 40 bits EXP-ADH-DES-CBC-SHA					
Rejected SSLv3 128 bits ADH-RC4-MD5					
Rejected SSLv3 40 bits EXP-ADH-RC4-MD5					
Rejected SSLv3 168 bits EDH-RSA-DES-CBC3-SHA Rejected SSLv3 56 bits EDH-RSA-DES-CBC-SHA					
Rejected SSLV3 50 bits EXP-EDH-RSA-DES-CBC-SHA					
Rejected SSLv3 168 bits EDH-DSS-DES-CBC3-SHA					
Rejected SSLv3 56 bits EDH-DSS-DES-CBC-SHA					
Rejected SSLv3 40 bits EXP-EDH-DSS-DES-CBC-SHA					
Accepted SSLv3 168 bits DES-CBC3-SHA					
Accepted SSLv3 56 bits DES-CBC-SHA					
Rejected SSLv3 40 bits EXP-DES-CBC-SHA Rejected SSLv3 40 bits EXP-RC2-CBC-MD5					
Accepted SSLv3 40 DIts EXFIN2-CBC-NDS					
Accepted SSLv3 128 bits RC4-MD5					
Rejected SSLv3 40 bits EXP-RC4-MD5					
Rejected SSLv3 0 bits NULL-SHA					
Rejected SSLv3 0 bits NULL-MD5					
Rejected TLSv1 256 bits ADH-AES256-SHA					
Rejected TLSv1 256 bits DHE-RSA-AES256-SHA					-
Rejected TLSv1 256 bits DHE-DSS-AES256-SHA					
root : ssiscan					
	00.20				
^ (글 🔍 🔄 🖸 😌 🐗 💻	08:26 pm				

Router SSLSCAN test screen shot

Router TLSSLed test screen shot1

🛛 🔤 📰 tis sled – Dolphin	🥹 where is tissled in backtrack - G	🔄 🛅 Konsole	👔 💷 System Monitor	tissied-router-test-notes.odt - 0p 🕤 🕤	😌 📢) 🛛 35:11 p
tissled : TLSSLed.sh					- 6
e Edit View Bookmarks Settings	Help				
<pre>tgbt:/pentest/enumeration/tlssled# vi tgbt:/pentest/enumeration/tlssled# ./</pre>	TLSSLed.sh 192.168.10.1 443				
SSLed - (1.2) based on sslscan and op. by Raul Siles (www.tadd			•		
openssl version: OpenSSL 0.9.8k 25 Mar sslscan version 1.8.2					
Analyzing SSL/TLS on 192.168.10.1:44					
The target service 192.168.10.1:443	seems to speak SSL/TLS				
ot@bt:/pentest/enumeration/tlssled# ./	/TLSSLed.sh 192.168.10.1 443				
LSSLed - (1.2) based on sslscan and op by Raul Siles (www.tadd	iong.com)				
openssl version: OpenSSL 0.9.8k 25 Mar sslscan version 1.8.2					
Analyzing SSL/TLS on 192.168.10.1:44					
] The target service 192.168.10.1:443	seems to speak SSL/TLS				
] Running sslscan on 192.168.10.1:443.					
Accepted SSLv3 56 bits DES-CBC-S	SHA				
Testing for strong ciphers (AES)					
Testing for MD5 signed certificate . Signature Algorithm: mdSWithRSAEncry					
] Testing for certificate public key l RSA Public Key: (768 bit)					
] Testing for certificate subject					
	tlssled : TLSSLed.sh				
s 🗃 🔹 🌒 🛋		05:11 pm	C		

Router TLSSLed test screen shot2

🔣 🔤 🔚 🖬 tis sled – Dolphin	Where is tissled in backtrack - G	🗖 🖾 Konsole	🛓 💷 System Monitor	tissled-router-test-notes.odt - Op	👔 😪 4)) 05:12 pm(🦕
tissled : TLSSLed sh					_ 8 X
File Edit View Bookmarks Settings H RSA Public Key: (768 bit)	lelp				
[*] Testing for certificate subject Subject: /CN=main:mint709-domain/unstru	ucturedName=maz.mint709-domain				
[*] Testing for certificate CA issuer Issuer: /CN-maz.mint709-domain/unstruc					
[*] Testing for certificate validity perior Today: Sun Sep 1 23:09:34 UTC 2013 Not valid before: Mar 1 00:04:59 1990 Not valid after: Feb 27 00:04:59 2003	зомт				
[*] Checking preferred server ciphers Prefered Server Cipher(s): SSLv3 168 bits DES-CBC3-SHA					
[-] Testing for SSLv3/TLSv1 renegotiation					
[*] Testing for secure renegotiation Secure Renegotiation IS NOT supported					
[-] Testing for TLS v1.1 and v1.2 (CVE-201	11-3389 aka BEAST)				
[*] Testing for SSLv3 and TLSv1 support fi Accepted SSLv3 168 bits DES-CBC3-SF Accepted SSLv3 56 bits DES-CBC-SFW Accepted SSLv3 128 bits RC4-SHA Accepted SSLv3 128 bits RC4-MD5					
<pre>[*] Testing for TLS v1.1 support The local openssl version does NOT support</pre>					
[*] Testing for TLS v1.2 support The local openssl version does NOT support					
[-] Testing for SSL/TLS HTTPS security hea	aders				
[*] Testing for Strict-Transport-Security	(STS) header				
[*] Testing for cookies with the secure f					
[*] Testing for cookies without the secure					
[-] New files created: -rw-rr 1 root root 4247 2013-09-01 17:	:09 sslscan 192.168.10.1 443 2013-09	9-01 170904.log			-
	tissled : TLSSLed.sh				
≥c 🗃 🕹 🧶	S (4)	05:12 pm	(6)		

Switch SSLSCAN test screen shot

			A					
🔲 🔹 reat : l	bash <2>							- 8
File Edit	View Bo	okmarks	Settings Help					
Failed	SSLV3	168 bits	ADH-DES-CBC3-SHA					
Failed	SSLv3	56 bits	ADH-DES-CBC-SHA					
Failed		40 bits	EXP-ADH-DES-CBC-SHA					
Failed	SSLv3	128 bits	ADH-RC4-MD5					
Failed			EXP-ADH-RC4-MD5					
Failed			EDH-RSA-DES-CBC3-SHA					
Failed	SSLV3	56 bits	EDH-RSA-DES-CBC-SHA					
Failed			EXP-EDH-RSA-DES-CBC-SHA					
Failed	SSLV3	168 bits	EDH-DSS-DES-CBC3-SHA					
Failed	SSLV3	56 bits	EDH-DSS-DES-CBC-SHA					
Failed			EXP-EDH-DSS-DES-CBC-SHA					
Failed	SSLV3	168 bits	DES-CBC3-SHA					
Failed	SSLV3	56 Dits	DES-CBC-SHA					
Failed	SSLV3	40 bits	EXP-DES-CBC-SHA					
Failed	SSLV3	40 Dits	EXP-RC2-CBC-MD5					
Failed	SSLV3	128 bits 128 bits	RC4-SHA					
Failed Failed								
Failed	SSLV3	0 bits	EXP-RC4-MD5 NULL-SHA					
Failed		0 bits	NULL-MD5					
Failed			ADH- AES256- SHA					
Failed			DHE-RSA-AES256-SHA					
Failed			DHE-DSS-AES256-SHA					
Failed	TL Sv1	256 hits	AES256-SHA					
Failed	TL Sv1	128 bits	ADH- AES128- SHA					
Failed	TLSv1	128 pits	DHE-RSA-AES128-SHA					
Failed			DHE-DSS-AES128-SHA					
Failed	TLSv1	128 bits	AES128-SHA					
Failed	TLSv1	168 bits	ADH-DES-CBC3-SHA					
Failed		56 bits	ADH-DES-CBC-SHA					
Failed	TLSv1	40 bits	EXP-ADH-DES-CBC-SHA					
Failed			ADH - RC4 - MD5					
Failed	TLSv1	40 bits	EXP-ADH-RC4-MD5					
Failed			EDH-RSA-DES-CBC3-SHA					
Failed			EDH-RSA-DES-CBC-SHA					
Failed			EXP-EDH-RSA-DES-CBC-SHA					
Failed			EDH-DSS-DES-CBC3-SHA					
Failed			EDH-DSS-DES-CBC-SHA					
Failed			EXP-EDH-DSS-DES-CBC-SHA					
Failed			DES-CBC3-SHA					
Failed Failed	TL Sv1	40 bits	DES-CBC-SHA EXP-DES-CBC-SHA					
Failed	TL SVI	40 bits	EXP-DES-CBC-SHA EXP-RC2-CBC-MD5					
Failed	TI SVI	128 bits	PCA-SHA					
Failed	TI Sv1	128 bits	RCA-MD5					
Failed			EXP-RC4-MD5					
Failed			NULL-SHA					
Failed		0 bits	NULL-MD5					
Prefered								
root@bt:-#	sslscan 19	92.168.10.	3:80					
1200								
			root : bas	in				
		100		S <1) = 1	06:27 pm	6		
		- C			00.27 pm	6		

notes.rtf - OpenOf

test-notes.odt

ark 1.8 🗍 😪 <) 36:27 pm(C

Switch TLSSLed test screen shot

10 ===	📰 tissled-switch – Dolphin	dev : screen	tissled : TLSSLed.sh	root : bash	System Monitor	Capturing from eth0 [Win	🕤 🥶 📢) 🛛 56:07 pm (🖕
🗖 🔹 tissler	d : TLSSLed sh						_ 6 X
File Edit	View Bookmarks Settings	s Help					
	entest/enumeration/tlssled#	./TLSSLed.sh 192.168.10.3 44	3				^
TI SSLed -	(1.2) based on ssiscan and	openssl					
	(1.2) based on sslscan and by Rat. Siles (www.ta	addong.com)					
+ openssl v	version: OpenSSL 0.9.8k 25 M						
+ sslscan	version: OpenSSL 0.9.8k 25 № version 1.8.2						
[-] Analyzi	ing SSL/TLS on 192.168.10.3:						
/TI CEI ad a	ch. line 121, kill, (1924)	No such process					
[+] ERROR:	sh: line 131: kill: (1824) The target service 192.168.	.10.3:443 does not seem					
	to speak SSL/TLS or is not	available!!					
rootebt:/pe							
							^
200		tissled : TLSSLed.sh					~
-							
5	e	🚬 🕤 🚭 📢	06:07 pm	n (6			

Appendix E - Protocol Flooding tests screen shots

Image: Source Image: Source<	💶 🚍 udp-router-test – Dolphin 🛛 🕹	Problem loading page - M 👘 🖡	🛛 Konsole	👌 💷 System Monitor	📜 Kwrite	2 Tetho (Wireshark 1.8	3 🕤 🕤 🚭 📢 🛛 🗤
Imm Source Destination Protocol Length Info Imm Source Destination Protocol Length Info Add66 100:0137730 132: 108: 10.2 192: 108: 10.3 NTP 42 reserved, reserved/Nafformed Packet] Add66 100:0137520 132: 108: 10.2 192: 108: 10.3 NTP 42 reserved, reserved/Nafformed Packet] Add68 100:0137520 132: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add69 100:0137520 132: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add70 100:0135750 102: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add70 100:0135750 102: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add71 100:0135600 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add72 100:0135600 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add73 100:013500 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add74 100:013500 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add78 100:01500 192: 108: 10.2<	etho (Wireshark 1 # 3 (SVN Rev Unknown f	rom unknown))					2 K X
Imm Source Destination Protocol Length Info Imm Source Destination Protocol Length Info Add66 100:0137730 132: 108: 10.2 192: 108: 10.3 NTP 42 reserved, reserved/Nafformed Packet] Add66 100:0137520 132: 108: 10.2 192: 108: 10.3 NTP 42 reserved, reserved/Nafformed Packet] Add68 100:0137520 132: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add69 100:0137520 132: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add70 100:0135750 102: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add70 100:0135750 102: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add71 100:0135600 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add72 100:0135600 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add73 100:013500 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add74 100:013500 192: 108: 10.2 192: 108: 10.3 NTP 43 reserved, reserved/Nafformed Packet] Add78 100:01500 192: 108: 10.2<	Edit <u>V</u> iew <u>Go</u> <u>C</u> apture Analyze S	tatistics Telephony Tools	Internals Help				
Time Source Destination Protocol Length Info 1 Time Source Destination Protocol Length Info 4466 100:01377301192:.0160:10.2 102:1061:10.3 NTP 42 reserved, reserved[Nalformed Packet] 4466 100:01375201192:.0160:10.2 102:1061:10.3 NTP 42 reserved, reserved[Nalformed Packet] 4468 100:01375201192:.0160:10.2 102:1061:10.3 NTP 43 reserved, reserved[Nalformed Packet] 4469 100:01375201192:.0160:10.2 102:1061:10.3 NTP 43 reserved, reserved[Nalformed Packet] 4470 100:01356001192:.0160:10.2 102:1061:10.3 NTP 43 reserved, reserved[Nalformed Packet] 4472 100:0135601192:.0160:10.2 102:1061:10.3 NTP 43 reserved, reserved[Nalformed Packe							
Time Source Petretation Protocol Length Model 64605 100:0157/301 120:106:10.2 152:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 64605 100:0157/301 120:106:10.2 152:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 64605 100:0157/301 120:106:10.2 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 64605 100:0157/801 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 64605 100:0157/801 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 6470 100:0157/801 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 6471 100:0156/801 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 6472 100:0156/8001 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 6472 100:0156/8001 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet] 6472 100:0159/8001 120:106:10.3 NTP 43 reserved, reserved[Malformed Packet]			¥ 🚯 🛣 🔲 🖼	ि ् ् थ् 🛅 👹	i 🔟 🚮 🎇 🖽		
6409 100.9157730152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6409 100.9157501152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6408 100.9157501152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6408 100.9157501152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6409 100.9157501152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6407 100.9155001152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6471 100.91550001152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6472 100.91550001152.108.10.2 192.106.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6473 100.91550001152.108.10.2 192.106.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6475 100.91550001152.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6475 100.9155001192.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 6475 100.9155001192.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Reiformed Packet] 64475 100.9155001192.108.10.2 </td <td>ar:</td> <td>▼ Expr</td> <td>ession Clime Apply a</td> <td>3100 C</td> <td></td> <td></td> <td>oogle 🔍 🔍</td>	ar:	▼ Expr	ession Clime Apply a	3100 C			oogle 🔍 🔍
4447 100.01957300132.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4468 100.01975701012.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4469 100.01975701012.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4470 100.0195000122.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4471 100.0195000122.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4472 100.0195000122.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4472 100.0195000122.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4473 100.0195000122.106.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4474 100.0195000121.006.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4477 100.0195000121.006.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4477 100.0195000121.006.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4477 100.0195000122.006.10.2 192.106.10.3 NTP 43 reserved, reserved[Ma[formed Packet] 4480 100.01950200122.006.10.2 <td>Time Source</td> <td>Destination</td> <td>Protocol Length Inf</td> <td>0</td> <td></td> <td></td> <td>-</td>	Time Source	Destination	Protocol Length Inf	0			-
4468 00.0157580152.0186.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4469 100.0157590152.0186.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4467 100.01558100152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4477 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4473 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4473 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4474 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4475 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4475 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4477 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4478 100.0155900152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4479 100.015590152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4479 100.015590152.108.10.2	54466 100.9157130 192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	ned Packet]		
4468 00.0157580152.0186.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4469 100.0157590152.0186.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4467 100.01558100152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4477 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4473 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4473 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4474 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4475 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4475 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4477 100.0155800152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4478 100.0155900152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4479 100.015590152.108.10.2 102.108.10.3 NTP 43 reserved, reserved[Naiformed Packet] 4479 100.015590152.108.10.2							
4470 100.9153100/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4470 100.9155000/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4473 100.9155000/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4473 100.9155000/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4473 100.9155000/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4475 100.9155000/192.108.10.2 192.106.10.3 NTP 43 reserved, reserved[Malformed Packet] 4475 100.9155000/192.108.10.2 192.106.10.3 NTP 43 reserved, reserved[Malformed Packet] 4475 100.9155000/192.108.10.2 192.106.10.3 NTP 43 reserved, reserved[Malformed Packet] 4477 100.9155000/192.108.10.2 192.106.10.3 NTP 43 reserved, reserved[Malformed Packet] 4479 100.91550192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4479 100.9155000/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4479 100.9155000/192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4479 100.9155000/192.108.1	4468 100.9157650(192.168.10.2	192,168,10,3					
4471 100.91295000 102.108.10.2 102.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4472 100.9159600 102.108.10.2 102.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4473 100.9159600 102.108.10.2 102.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4474 100.9159600 102.108.10.2 102.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4474 100.9159600 102.108.10.2 102.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4475 100.9159600 102.108.10.2 192.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4476 100.9159600 102.108.10.2 192.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4476 100.9159600 102.108.10.2 192.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4478 100.9159600 102.108.10.2 192.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4479 100.9159600 102.108.10.2 192.108.10.3 NIP 43 reserved, reserved[Malformed Packet] 4470 100.9159600 192.108.10.2 192.109.10.3 NIP 43 reserved, reserved[Malformed Packet] 4470 100.9159600 192.108.10.2 192.109.10.3 NIP 43 reserved, reserved[Malformed Packet] 4481 100.9159600 192.1	4469 100,9157910 192,168,10,2	192,168,10,3	NTP 43 re	served, reserved[Malform	med Packet]		
2422 00.01586000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4473 100.0156000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4473 100.0156000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4473 100.0156000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4475 100.0156000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4475 100.0156000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4477 100.0156000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4479 100.0155000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4479 100.0155000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4479 100.0155000 102.168.10.2 102.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4479 100.0155000 102.168.10.2 192.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4470 100.0155000 102.168.10.2 192.168.10.3 NIP 43 reserved, reserved[Malformed Packet] 4470 100.0155000 102.16	4470 100.9158160 192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
4473 100.9156900 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4473 100.9156970 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4475 100.9156900 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4475 100.9156900 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4476 100.9156900 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4478 100.9156900 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4479 100.9155010 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4479 100.9155010 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4480 100.9155020 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4480 100.9155020 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 4490 100.9155020 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 440 100.9155020 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 450 0.5 00 00 192.168.10	H471 100.9158500(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
1474 100.01567701102.168.10.2 1102.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1475 100.015569001192.108.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1475 100.015569001192.108.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1477 100.01569001192.108.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1477 100.01569001192.168.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1479 100.01550101192.168.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1479 100.015502001192.168.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 1481 100.015502001192.168.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 149 100.015502001192.168.10.2 192.168.10.3 NTP 43 reserved, reserved/Malformed Packet] 100.01550200119	472 100.9158600(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
H475 100, 9159600 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H475 100, 9159600 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H477 100, 91596300 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H477 100, 91596300 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H477 100, 91596300 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H479 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H480 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H480 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H490 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H400 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H400 100, 915920 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H410 00 00 40 00 01 11 a5 7a c0 a8 00 20 c0 a8 5f.f.E. 6.e	4473 100.9158690(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
H475 100, 9159600 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H475 100, 9159600 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H477 100, 91596300 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H477 100, 91596300 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H477 100, 91596300 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H479 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H480 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H480 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H490 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H400 100, 9159200 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H400 100, 915920 192, 160, 10.2 192, 160, 10.3 NTP 43 reserved, reserved/Malformed Packet] H410 00 00 40 00 01 11 a5 7a c0 a8 00 20 c0 a8 5f.f.E. 6.e	474 100.9158770(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
H477 100.91590301 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H478 100.015010 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H479 100.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H480 100.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H480 100.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H480 100.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H100 0.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H100 0.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] H100 0.9150200 192.168.10.2 192.168.10.3 NTP 43 reserved.reserved[Malformed Packet] H100 0.9150200 192.168.10.3 NTP 43 reserved.reserved[Malformed Packet] 100 H100 0.9150200 192.168.10.3 NTP 43 reserved.reserved[Malformed Packet] 100 H100 0.915020 192.168.10.3 5f.f.E. 5	4475 100.9158860(192.168.10.2	192.168.10.3					
HATP: 100.015010102.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Malformed Packet] HATP: 100.9155010192.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Malformed Packet] HADD: 100.91592000192.108.10.2 192.108.10.3 NTP 43 reserved, reserved/Malformed Packet] HADD: 100.9159200192.108.102.1 192.108.103 NTP 43 reserved, reserved/Malformed Packet] HADD: 100.91592000192.108.102.1 192.108.103	4476 100.9158940/192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
A479 100.91591901 192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] A400 100.91592800 192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] A400 100.91592800 192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] A470 100.91592480 192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] A470 100.91592480 192.108.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] A470 100.91592480 192.108.10.2 192.168.10.3 NTP 43 reserved, reserved[Malformed Packet] 00 06 be f9 53 00 00 1e ec 8d 91 66 08 00 45 00 5f.f.E.	477 100.9159030(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	ned Packet		
H400 100.91592000 192.108.10.2 192.169.10.3 NTP 43 reserved, reserved/file/ormed Packet] H81 100.91592000 192.108.10.2 192.168.10.3 NTP 43 reserved, reserved/file/ormed Packet] H81 100.91592000 192.108.10.2 192.168.10.3 NTP 43 reserved, reserved/file/ormed Packet] H01 00.91592000 192.108.10.2 192.168.10.3 NTP 43 reserved, reserved/Halformed Packet] H01 00.9159200 100.11 x57.168.10.3 NTP 43 reserved/malformed Packet] 10 H01 00.9159200 100.11 x57.168.10.2 192.168.10.3 NTP 43 reserved/Halformed Packet] H01 00.9159200 100.11 x57.a 180.02	478 100.9159110(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	ned Packer		
4481 100.915963001192.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 4482 100.91504001102.108.10.2 192.108.10.3 NTP 43 reserved, reserved[Malformed Packet] 000 0b te 19 53 00 00 1e ec 0d 91 66 00 00 45 00 5f.E.	4479 100.9159190(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
Build Displayed Displayed <thdisplayed< th=""> <thdisplayed< th=""> <thdispl< td=""><td>4480 100.9159280(192.168.10.2</td><td>192.168.10.3</td><td>NTP 43 re</td><td>served, reserved[Malform</td><td>med Packet]</td><td></td><td></td></thdispl<></thdisplayed<></thdisplayed<>	4480 100.9159280(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
00 0b be f9 53 00 00 1e ec 8d 91 66 08 00 45 00	4481 100.9159360(192.168.10.2	192.168.10.3	NTP 43 re	served, reserved[Malform	med Packet]		
00 0b be f9 53 00 00 1e ec 8d 91 66 08 00 45 00 5fE. 00 1d 00 00 40 00 40 11 a5 7a c0 a8 0a 02 c0 a8 6.e.	4482 100.9159460(192.168.10.2	192,168,10,3	NTP 43 re	served, reserved[Malform	med Packet1		.
0 00 0b e 19 53 00 00 1e e ce dd 91 66 08 00 45 00							-
0 0a 03 b6 95 00 75 00 09 95 70 30(p0	00 0b be f9 53 00 00 1e ec 8d	91 66 08 00 45 00		(and and a second se			
File: "tmp/wireshark_eth0_2013100 Packets: 1280896 Displayed: 1280896 Profile: Default							
	0a 03 b6 95 00 7b 00 09 95 70	30	{p0				
							<u> </u>
Mt : /pentest/mtsc/unj-pt#_U		Packets: 1280896 Displayed	: 1280896 Profile: Del	aut			
	at:/pentest/misc/udp-pl# []						
						U	
						0) (
		al and	and the second s			1000	

Switch UDP.pl test wireshark screen shot

Appendix F - Web Server stressing test screen shots

🐻 🚞 🗐 Dolphin	ž 🙆 Frefox bin	j 🗈 Konsole	🧿 💷 System Monitor	siege router test-notes o	Capturing from eth0 (W.	🕥 😪 4)) - 39:06 pm (_
a root : siege						
	kmarks Settings Help					
itian: 2012-01-20 21-05 Itian: 2013-01-20 21-05	14 HTTP/1.1.200.15.25. 1423 16 HTTP/1.1.200.15.22. 1623	1, 7, 0, 2013-09-29 21, 05, 22 1, 7, 0, 2013-09-29 21, 05, 23				~
[alert] socket: -12626 [alert] socket: -13384 [alert] socket: -13384 [alert] socket: -13210 [alert] socket: -13132 [alert] socket: -12292 [alert] socket: -12300 [alert] socket: -13300	38410 select timed out: Connects 57000 select timed out: Connects 45710 select timed out: Connects 45712 select timed out: Connects 23824 select timed out: Connects 9784 select timed out: Connects 09282 select timed out: Connects 53008 select timed out: Connects 53008 select timed out: Connects	on timed out on timed out				
Lifting the server sie						
Transactions: Availablity: Elapsed time: Data transferred: Pesponse time: Transaction rate: Throughput: Concurrency: Successful transaction Hailed transactions: Longet transaction:	199 hits 86 j.5 % 179.38 secs 6.97 secs 1.11 trans/sec 0.00 MR/wec 7.74 41 200 32 43.39 0.04					
	nnoying message by editing our home directory: change					
2	root : :	siege				
20		and the second se	00.06 pm			

Router SIEGE 15 users test screen shot

Router SIEGE 100 users test screen shot

R = 1	🔤 🔝 Delphin	🛓 🐸 Firefox-bin 🕴 🧯	E Konsole	👸 💷 System Monitor	Siege-routentest-notes.odt - 0:	🕤 🍜 📢 29:15 pm(C
• r6	ot : siege					_ # X
File E	dit View Bookmarks Settings He	NP.				
	socket: -1480385680 connection time					~
1540 25						
1567 25	113-05-22 21 3-29 HTTP/1.1,200, 11					
	socket: -1597883536 connection time	40 11027 / 0 2010 09 20 21 13 13				
		ed out.: Connection timed out				
error		ed out.: Connection timed out				
		ed out.: Connection timed out				
		ed out.: Connection timed out				
	socket: -1463600272 connection time	ed out.: Connection timed out				
error		ed out.: Connection timed out ed out.: Connection timed out				
error		ed out.: Connection timed out				
error		ed out.: Connection timed out				
error	socket: -1371280528 connection tim	ed out.: Connection timed out				
	socket: -1354495120 select timed or	ut: Connection timed out				
	socket: -1589490832 select timed or					
	socket: -1455207568 select timed or					
	<pre>socket: -1220211856 select timed or socket: -1207353488 select timed or</pre>					
	socket: -1488778384 select timed of					
	socket: -1320924304 select timed or					
[alert]	socket: -1253782672 select timed or	ut: Connection timed out				
[alert]	socket: -1295746192 select timed or	ut: Connection timed out				
alert	socket: -1547527312 select timed or	ut; Connection timed out				
atert	socket: -1307709712 select timed o	ut) connection timed out				
Lifting	the server siege done.					
Transact	tions: 265 hits					
Availabi Elapsed	time: 179.29 secs					
Data tra	insferred: 0.36 Mi					
Response	ansferred: 0.36 MD e time: 7.61 secs tion rate: 1.40 trans.					
Transact	tion rate: 1.48 trans.					
Throughp	out: 0.00 MB/se					
Concurre	ency: 11.25 ful transactions: 275 transactions: 217					
Eaclard 1	transactions: 217					
Locoest	transaction: 46.52					
Shortest	t transaction: 0.00					
FILE: A	sr/local/var/siege.log					
tou can	disable this annoying message by en	0111ng				
the dire	retive "show lostile" to false	change				
rootcht	ngerc file in your home directory; : cctive "show-logfile" to false. #∎					
						~
						· · ·
100		root : siege				
20			09:15 pm	10		
5			09.15 pm			

Switch SIEGE 15 users test screen shot

🔣 🚍 🗐 Dolphin	2 🕙 mint 709-switch Home	Siege JoeDog - Mozil	🖾 Konsole	🖥 System Monitor	siege-router-test-note	Capturing from eth0) 🕤 🚭 🕪	93:25 pm(
root : bash <3>								_ 8 X
File Edit View Bookmarks	Settings Help							
errori socket: read error Co terrori socket: read error co	nnection reset by peer sock c. nnection reset by peer sock c.	479: Connection reset b 479: Connection reset b	ý peer y peer y peer y peer y peer y peer y peer					
[error] socket: read error Co	nnection reset by peer sock.c	479: Connection reset b						
[error] socket: read error Co	nnection reset by peer sock.c	:479: Connection reset b						
[Sun, 2013-09-29 15:23:43] HT [Sun, 2013-09-29 15:23:43] HT								
Lifting the server siege								
Transactions: Availability: Elapsed takerred: Response time: Transaction rate: Throughput: Successful transactions: Ealed transactions: Longest transaction:	2237 hits 54.94 % 179.07 % 179.07 % 0.28 sets 0.28 sets 0.24 % 1.2.49 trans/sec 0.02 % 1.2.49 trans/sec 0.24 % 1.2.49 trans/sec 0.3.47 1.237 1.835 1.20 0.13							
FILE: /usr/local/var/siege.lo You can disable this annoying the .siegerc file in your hom the directive 'show-logfile' rootgbt:-# ■	message by editing e directory: change							
	root : bash							
°⊂ 🗃 🛛 📦 🤇) E G 🕫	<pre>>></pre>	03:25 pm	(6				

Switch SIEGE 100 users test screen shot

🐮 📰 🖬 🖬	Dolphin	2 🔮 Firefox-bin	2 🖾 Konsole	6 🔳 Syst	em Monitor	siege-router-test-notes.od	siege-switch-wireshark-10	🕤 😪 📢	03:53 pm
• root : siege									- 6 >
File Edit Vier		Help							
error] socket:	-2008847504 connection		n timed out						-
[error] socket:	-1564034192 connection	timed out.: Connection	n timed out						
	-176545 088 connection								
	-1874564240 connection								
	-1530463376 connection -1782244496 connection								
	-1480107152 connection								
	-2034025616 connection								
	-1715102864 connection								
	-1580819600 connection	n timed out.: Connection	n timed out						
ERROR from http									
	-1664746640 connection -1824208016 connection								
	-1538856080 connection								
	-1950098576 connection								
error] socket:	-1849386128 connection	timed out.: Connection	n timed out						
	-1446536336 connection								
	-1673139344 connection								
	-1656353936 connection								
	-1866171536 connection -1245111440 connection								
	-1916527760 connection								
	-1312253072 connection								
	-1799029904 connection								
	-1219933328 connection								
[error] socket:	-1899742352 connection	n timed out.: Connection	n timed out						
error socket:	-1228326032 connection -1605997712 connection	timed out.: Connection	n timed out						
	-1555641488 connection								
	-1261896848 connection								
(error) socket.	1201030040 connection	reality out. Connection	i timed out						
	281 1								
wailability:	40.55 %								
lapsed time:	179.22 s								
lata transferre									
esponse time: ransaction rat	6.17 s	secs trans/sec							
hroughput:	0.00 1								
Concurrency:	9,68								
Successful tran									
Failed transact									
ongest transac									
Shortest transa	iction: 0.03								
FILE: /usr/loca	l/var/siege.log								
	this annoving message	by editing							
the .siegerc fi	le in your home directo	ry; change							
the directive '	show-logfile' to false.								
root@bt : 🛹									
		root : siege							
2	(C) (S)		(1)	03:53 pm	0				
				05.55 pm					

Appendix G - Brute Force Directory and file test screen shots

Router DIRB	screen shot
--------------------	-------------

🛾 🔤 🧱 dirb-switch – Dolphin	🗈 Konsole	🗧 System Monitor	lirb-switch-test-notes.odt - Open	Capturing from eth0 [Wiresh	1ar 🕤 🚭 📢	
◇ dirb : dirb						- 6
Edit View Bookmarks Settings	Help					
h: /dirb: No such file or directory t cbt:/pentest/web/dirb# ./dirb http:/	/192.168.10.1 wordlists/big.txt	: -u admin123:mypassword -o /root/Desk	ktop/dirb-router			
B v2.03						
The Dark Raver						
PUT_FILE: /root/Desktop/dirb-router						
ART_TIME: Tue Sep 17 20:02:48 2013 _ BASE: http://192.168.10.1/						
RDLIST FILES: wordlists/big.txt						
THORIZATION: admin123:mypassword						
NERATED WORDS: 4217						
Scanning URL: http://192.168.10.1/ http://192.168.10.1/configure						
(FOUND: 200 [Ok] - Size: 13417)						
(FOUND: 200 [0k] - Size: 20)						
http://192.168.10.1/exec						
(FOUND: 200 [Ok] - Size: 4297) http://192.168.10.1/filter						
(FOUND: 200 [Ok] - Size: 359)						
http://192.168.10.1/gateway						
(FOUND: 200 [Ok] - Size: 831) http://192.168.10.1/interface						
(FOUND: 200 [Ok] - Size: 19)						
http://192.168.10.1/line (FOUND: 200 [0k] - Size: 6634)						
http://192.168.10.1/ping						
(FOUND: 200 [Ok] - Size: 326) http://192.168.10.1/roles						
(FOUND: 200 [Ok] - Size: 689)						
http://192.168.10.1/router						
(FOUND: 200 [Ok] - Size: 25) http://192.168.10.1/template						
(FOUND: 200 [Ok] - Size: 1198)						
NLOADED: 4217 - FOUND: 11						
ot@bt:/pentest/web/dirb#						
	dirb : dirb					
: 🗃 🕹 🧶		09:01 pm	6			

Switch DIRB screen shot

irb : dirb : dirb File Edit View Book rootgbt :/pentest/web/di	./dirb http://192.168.	10.3 wordlists/big.txt -u adm	in:theking -o /root/Desk	:top/dirb-switch	_ 6 X
File Edit View Book root@bt:/pentest/web/di	./dirb http://192.168.	10.3 wordlists/big.txt -u adm	in:theking -o /root/Desk	top/dirb-switch	^
root@bt:/pentest/web/di	./dirb http://192.168.	10.3 wordlists/big.txt -u adm	in:theking -o /root/Desk	top/dirb-switch	^
DIRB v2.03 By The Dark Raver					
By The Dark Raver					
OUTPUT_FILE: /root/Desk START_TIME: Tue Sep 17 URL_BASE: http://192.16 WORDLIST_FILES: wordlis AUTHORIZATION: admin:th	top/dirb-switch				
START_TIME: Tue Sep 17	19:51:48 2013				
WORDLIST_FILES: wordlis	ts/big.txt				
AUTHORIZATION: admin:th	eking				
GENERATED WORDS: 4217					
Scanning URL: http + http://192.168.10.3//	://192.168.10.3/				
(FOUND: 200 [0k] -	Size: 1781)				
+ http://192.168.10.3/c	onfigure				
(FOUND: 200 [Ok] - + http://192.168.10.3/e	Size: 4436)				
(FOUND: 200 [Ok] -					
+ http://192.168.10.3/f					
(FOUND: 200 [Ok] -	51Z0: 202)				
(!) FATAL: Too many err	ors connecting to host				
(Possible cause: OK					
DOWNLOADED: 1572 - FOUN rootgbt:/pentest/web/di	D: 4				
rootgoer/pencese/nes/us					
					~
		dirb : dirb			
≥ 😭	(1) (2)		07:55 pm	6	
			07.35 pm		

Appendix H - Fuzzing tests screen shots

Router BED screen shot1

👫 💷 📰 Dolphin 💈	🕙 Cisco IOS Secur 🛛 🕹 Firefox-bin 🔒	🙆 Router /level/15 🛛 🛅 Konsole	🔜 🚺 spike notes – K	🛛 📄 OpenOffice.or 🤰 🐝 TFTPgui	📈 Xpdf	3 (j) 🚭 ◀))) 07:28 pm(🦕
bed : bed.pl						
File Edit View Bookmarks	Settings Help					
The Lot them booking to	Sectings help					^
BED 0.5 by mjm (www.codito.	de) & eric (www.snake-basket.de)					
Usage:						
usage:						
./bed.pl -s <plugin> -t <tar< td=""><td>get> -p <port> -o <timeout> [depends</timeout></port></td><td>on the plugin]</td><td></td><td></td><td></td><td></td></tar<></plugin>	get> -p <port> -o <timeout> [depends</timeout></port>	on the plugin]				
- 1	TP/IRC/IMAP/PJL/LPD/FINGER/SOCKS4/SOCK					
<target> = Host to check (</target>						
<port> = Port to connect</port>	to (default: standard port)					
	after each test (default: 2 seconds)					
use "./bed.pl -s <plugin>" to</plugin>	o obtain the parameters you need for t	he plugin.				
Only -s is a mandatory switch						
root@bt:/pentest/fuzzers/bed#	./bed.pl -s http -t 192.168.10.1 -p 8	0 -0 3				
RED 0.5 by mim (www.codito.u	de) & eric (www.snake-basket.de)					
+ Buffer overflow testing:						
testing: 1	HEAD XAXAX HTTP/1.0 HEAD / XAXAX					
testing: 2						
testing: 3 testing: 4	GET XAXAX HTTP/1.0 GET / XAXAX					
testing: 5	POST XAXAX HTTP/1.0					
testing: 6	POST / XAXAX					
testing: 7						
testing: 8						
+ Formatstring testing:						
testing: 1	HEAD XAXAX HTTP/1.0					
testing: 2	HEAD / XAXAX GET XAXAX HTTP/1.0					
testing: 3 testing: 4	GET XAXAX HTTP/1.0 GET / XAXAX					
testing: 5	POST XAXAX HTTP/1.0					
testing: 6	POST / XAXAX					
testing: 7						
testing: 8						
* Normal tests						
+ Buffer overflow testing:	User-Agent: XAXAX					
testing: 1 testing: 2	Host: XAXAX					
testing: 3	Accept: XAXAX					
testing: 4	Accept-Encoding: XAXAX					
testing: 5	Accept-Language: XAXAX					
testing: 6	Accept-Charset: XAXAX					
testing: 7	Connection: XAXAX					
testing: 8 testing: 9	Referer: XAXAX Authorization: XAXAX					
testing: 9 testing: 10	From: XAXAX					
testing: 10	Charge-To: XAXAX					~
121	bed : bed.pl					
-						
~c 🖂 🔹 🧶		07:28 pm	(6)			

Router BED screen shot2

10 == 1	Dolphin 2	Cisco IOS Secu	Hindlok-on 4 D	Houter nevel Konsole	11 spike notes - 1	Openomice.cl 2 Scittingui	PH Xpdr	3 1 32 39 bm (
🔳 🔹 bed : b	ed al							
	View Bookmarks	Cattings Hale						
Pile Edit								
	testing: 5 testing: 6		ХАХАХ					-
	testing: 7	Connection: XAXAX						
	testing: 8	Referer: XAXAX						
	testing: 9	Authorization: XA	XAX					
	testing: 10							
	testing: 11							
	testing: 12	Authorization: XA						
	testing: 13							
	testing: 14	Authorization: fo	0 : XAXAX					
	testing: 15	If-Modified-Since	: XAXAX					
	testing: 16	ChargeTo: XAXAX .						
	testing: 17	Pragea: XAXAX						
+ testing i	misc strings 19:							
	testing: 1 testing: 2	User-Agent: XAXAX Host: XAXAX						
	testing: 3	Accept: XAXAX						
	testing: 4		хахах					
	testing: 5		ХАХАХ					
	testing: 6		AXAX					
	testing: 7							
	testing: 8	Referer: XAXAX .						
	testing: 9							
	testing: 10							
	testing: 11							
	testing: 12		XAX					
	testing: 13		XAX : foo					
	testing: 14 testing: 15	Tf. Modified, Since	0 : XAXAX					
	testing: 16	ChargeTo: XAXAX						
	testing: 17	Pragaa: XAXAX						
· Other test								
* All tests								
root@bt:/per								
								U
								~
			1200 100					~
-		b	ed : bed.pl					
2			A Designed	07.20	e			
5		1 I I I I I I I I I I I I I I I I I I I	w = -	07:29 pm	_ (e			

Router BED No buffer Failures

Router DED no buller ranures	
🚯 💳 🔤 bed-router 🤇 😻 Downloads 🔍 Exploiting (🛛 🥹 mint 709 s.) 🕲 max Jevel (🛛 🕹 mint 709 s.) 🖾 Konsole 🚊 Exploiting (🗎 System Mor	🔡 BED actual 🔹 Session - S 🔛 Xpdf. (tmp.) 🕤 😌 4)) 27:07 am (
	C T 😰 🔯 Google 🔍 😥
Source Section Sectio	
mint709-switch	
Command	
butput	
Complete WML vas: /level/15/exec/-/shov/buffers/all	
28	
tung .	
eader	
acket	
Show buffer header and packet data	
command completed.	
14 12	
କ 🚍 🛛 💱 🗐 🔄 🗐 🚽 🗧 🛛 07:07 am	
Kouter SPIKE test screen snot	
💈 🚍 📓 spike-router+/2 – Dolphin 🛛 🔌 maz /level/15/exec/-/show// 🖆 Konsole 🦷 😚 🖬 System Monitor 👘 🔡 spik	xe-router-test-notes.od 🛛 📶 wireshark 🛛 [Wireshark 1.8 🛛 🕤 🚭 🐗 🖬 🤉 26:40 pn
	- 8
id response zzing Variable 0:2042	
ist: www.immunitysec.com	writer, annlication/wnd stardivision
vriter-global, application/x-starwriter, application/vnd.sun.xml.writer.template :cept: application/vnd.sun.xml.calc, application/vnd.stardivision.calc, application/x-starcalc, application/vnd.sun.xml.calc.templ	
application/vnd.stardivision.impress, application/vnd.stardivision.impress-packed	
ccept: application/x-starimpress, application/vnd.sun.xml.impress.template, application/vnd.sun.xml.draw, application/vnd.stardivi olication/vnd.sun.xml.draw.template, application/vnd.sun.xml.math	
:cept: application/vnd.stardivision.math, application/x-starmath, application/msword, text/sgml, video/mpeg, image/jpeg, image/tif :tmap, image/x-xbm, image/gif, application/postscript, */*;q=0.01	f, image/x-rgb, image/png, image/x-x
ser-Agent: Lynx/2.8.5dev.3 libwwv-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6c	
er-Agent: Ljnx/2.0.00er.3 LL0###-FP/2.14 SSL-NH/1.4.1 OpenSSL/0.9.0L	
dRequest	
sponse: rver didn't answer in time limit	
nd response	

💻 \circ spike/s : bash		
File Edit View	Bookmarks Settings Help	
End response		
Fuzzing Variable Request:	0:2042	
	loits?sort=all!@#\$%%^#\$%#\$%#\$%\$\$@#\$%^^**(() HTTP/1.0	
Host: www.immunit		
		ter.global, application/vnd.stardivision.writer, application/vnd.stardivision
.writer-global, a	application/x-starwriter, application/vnd.sun.xml.writer.template	rcalc, application/vnd.sun.xml.calc.template, application/vnd.sun.xml.impress
	J.stardivision.impress, application/vnd.stardivision.impress-packed	rate, application/who.sun.xmt.cate.template, application/who.sun.xmt.impress
Accept: application	ion/x-starimpress, application/vnd.sun.xml.impress.template, application/vn	nd.sun.xml.draw, application/vnd.stardivision.draw, application/x-stardraw, a
	un.xml.draw.template, application/vnd.sun.xml.math	
	lon/vnd.stardivision.math, application/x-starmath, application/msword, tex: «bm, image/gif, application/postscript, */*;g=0.01	t/sgml, video/mpeg, image/jpeg, image/tiff, image/x-rgb, image/png, image/x-x
Accept-Language:		
	/2.8.5dev.3 libwwv-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6c	
EndRequest		
Response:		
	swer in time limit	
End response		
Fuzzing Variable Request:	0:2043	
	loits?sort=all%01%02%03%04%0a%0d%0aADSF_HTTP/1.0	
Host: www.immunit	tysec.com	
Accept: text/html	l, text/plain, application/vnd.sun.xml.writer, application/vnd.sun.xml.wri application/x-starwriter, application/vnd.sun.xml.writer.template	ter.global, application/vnd.stardivision.writer, application/vnd.stardivision
		rcalc, application/vnd.sun.xml.calc.template, application/vnd.sun.xml.impress
	.stardivision.impress, application/vnd.stardivision.impress-packed	
		nd.sun.xml.draw, application/vnd.stardivision.draw, application/x-stardraw, a
	un.xml.draw.template, application/vnd.sun.xml.math	t/saml, video/mpeq, image/ipeg, image/tiff, image/x-rgb, image/png, image/x-x
	lon/vnd.stardivision.math, application/x-starmath, application/msword, tex kbm, image/gif, application/postscript, */*;g=0.01	t/sgmt, video/mpeg, image/jpeg, image/tiff, image/x-rgo, image/png, image/x-x
Accept-Language:		
User-Agent: Lynx/	/2.8.5dev.3 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6c	
EndRequest		
Response:		
	swer in time limit	
End response Done.		
	/fuzzers/spike/src# ./generic web server fuzz 192.168.10.1 80 immunitysec.s	spk O G
	spike/s : bash	
-		
[−] C [−]	🚽 🕘 🕤 🚭 💵 💻 🛛 06:4	.0 pm (C

R

Router SPIKE test No buffer failures

🥨 🚍 📾 spike-router-v2 - Dolphin 🛛 🕑 maz /level/15/exec/-/show 🗋 🖾 Konsole	🙀 🖾 System Monitor	Spike-router-test-notes.od	eth0 [Wireshark 1.8.3 (S	🗊 🚭 4)) 🛛 56:38 pm (🗲
😢 🔹 maz /level/15/exec/-/show/buffers/failures - Mozilla Firefox				_ # X
Ele Edit View Higtory Bookmarks Tools Help				
🗇 maz /level/15/exec/-/show/buffer				
🜳 🌳 😏 🕙 192.168.10.1/level/15/exec/-/show/buffers/failures			☆▼ 😂 🚺 • Google	۹ 🔒
🔁 BackTrack Linux 👖 Offensive Security 🛄 Exploit-DB 🐚 Aircrack-ng 📓 SomaFM				
maz				
Home Exec Configure				
Command				
Output				
Comand Nacr-UR. was: //www/i/Si/sec/- complete UR. was: //www/i/Si/sec/-/shor/fors/fallures Comand was: shew boffers fallures				
Caller Pool Size When				
command completed.				

²<, 🛜	0		06:38 pm			
Route	<pre>cube put cube put c</pre>					
🐮 📄 🖬 sir 🖾 🔹 sickfuzz : bar	ck-fuzz-router-v2 – Dolphin 🐧 sh	🕑 Problem loading page - Mo 🖺 Konsole		lonitor 📄 Sickfuzz-rou	tertest-notes 🛛 📶 sickfuzz-router-v2	-wireshar 👔 😪 <)) 27:47 pm(
Host: User-Agent: Mozi Accept: text/htm Accept-Language:	illa/5.0 (%indows;en-GB; m al,application/xhtml+xml,a : en-us,en;q=0.5	rv:1.8.0.11) Gecko/20070312 Firefox/1. application/xml;q=0.9,*/*;q=0.8	5.0.11			Â
Host: User-Agent: Mozi Accept: text/htm Accept-Language: Accept-Charset:	illa/5.0 (Windows;en-GB; r nl,application/xhtml+xml,s : en-us,en;q=0.5 TSC.00550.1 utf.0.g=0.7 *	rv:1.8.0.11) Gecko/20070312 Firefox/1.5 application/xml;q=0.9,*/*;q=0.8				
Accept-Language: Accept-Charset: Keep-Alive: 300 Proxy-Connection Referer: http://	: en-us.en;q=0.5 ISO-8859-1,utf-8;q=0.7,*; 1: keep-alive /www.example.com pplication/x-www-form-urle		20000000000000000000000000000000000000			
***Server closed ^C [>] Stopping fu 2330 packets dro [>] Done!	uzzing and tshark, please					
72347 packets ca	ptured //fuzzers/sickfuzz#					
		sickfuzz : bash				
S 🖸	U		07:47 pm	(6		

Router SICKFUZZ test buffer failures

«/buffers/failu Bookmarks w/buffer		X				- 8
w/buffer						
10.1/level/15	/exec/-/show/bu	ffers/failures			Google	٩ (
nsive Security	y DExploit-DB	Nircrack-ng SomaFM				
			_			
15/ever/						
xec/-/show/bu	ffers/failures					
	Ľ,	>				
Size	When					
60	00:05:18					
60	00:05:18					
60	00:05:18					
	00:05:18 00:05:18					
	13//mar(/, carc/,/shav/bu ltares 60 60 60 60 60 60 60 60 60 60 60	33/stree/. see://Jack/buffers./fallures illures 51.ze When 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18	13/cmc/- sec/-/bw/mffrs/falters lares 51ze Wen 60 00:65:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18	33/stree/. Size //hon/buffers/fallwes illeres 5ize When 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18 60 00:05:18	33/srec./ sec./hu/fors/fallures illeres 51.2e When 00 00:05:18 00 00:05:18	33/sree/ 33/sree/ Size When 0 00:05:18 0 00:05:18

Router SFUZZ test screen shot

ेंद 📄 🛛 🕹 💭 🖸 😌 🐠 💻 07:49 pm 🕡

🥸 🚃 📰 sfuzz - Dolphin 🛛 🕲 maz Home Page - Moz	Konsole 6	System Monitor	🚺 Kwrite	2 Sfuzz test.odt - Open	stuzz-router-wireshark	🕤 🚭 4)) 06:58 pm 🧲
Sfuzz : bash						_ 6 X
File Edit View Bookmarks Settings Help						
literal[65] = [////etc/passwd]						<u>^</u>
<pre>literal[66] = [/////etc/passwd] literal[67] = [//////etc/passwd]</pre>						
literal[68] = [.//etc/passwd]						
literal[69] = [.///etc/passwd]						
literal[70] = [.///etc/passwd]						
<pre>literal[71] = [.////etc/passwd] literal[72] = [./////etc/passwd]</pre>						
literal[73] = [./////etc/passwd]						
literal[74] = [.///////etc/passwd]						
sequence[1] = [%n]						
sequence[2] = [%f] sequence[3] = [%n]						
sequence[3] = [4] sequence[4] = [A]						
sequence[5] = [0]						
sequence[6] = [0]						
sequence[7] = [0] sequence[8] = [%n]						
sequence[9] = [%#123456x]						
sequence[10] = [%s]						
sequence[11] = [%%s]						
sequence[12] = [%20s] sequence[13] = [%%20s]						
sequence[13] = vecos] sequence[14] = vecos]						
sequence[15] = [%20x]						
sequence[16] = [%n%n%n%n%n]						
sequence[17] = [%p%p%p%p%p%p] sequence[18] = [%x%x%x%x%x]						
sequence[18] = [%d%d%d%d%d]						
sequence[20] = [%s%s%s%s%s]						
sequence[21] = [%s%p%x%d]						
sequence[22] = [%.1024d] sequence[23] = [%.1025d]						
sequence[24] = [%.2048d]						
sequence[25] = [%, 2049d]						
sequence[26] = [%.4096d]						
sequence[27] = [%.4097d] sequence[28] = [%99999999999s]						
sequence[29] = [%08x]						
sequence[30] = [%20d]						
sequence[31] = [%20n]						
sequence[32] = [%20x] sequence[33] = [%20s]						
sequence[33] = [%#0123456x%08x%x%s%p%d%n%o%u%c%h%]	4d%j%2%2%t%j%e%d%f%a%C%S	08x%1				
root@bt:/pentest/fuzzers/sfuzz# sfuzz -TO -v -L /root/Desk	top/sfuzz-router -e -f sf	fuzz-sample/basic.http ·	S 192.168.10.1 -p 80			
						^
						~
sfuzz : bash						
2 🖸 🛛 🚱 🕢 🕞 🖓 🚱		06:58 pm	6			

Router SFUZZ test No buffer failures

U	📰 sfuzz – Dolphin	🕑 maz //r	vel/15/exec/++ 🛛 Konsole	👸 🛄 System Monitor	L Karite	🤰 🔛 sfuzz test.odt - Openic	sfuzz-router-wiresham	🕤 🚭 4)) 37:01 pm(C
	evel/15/exect-tshow/bu							_ # X
Eile Edit	View Higtory Doc	kmarks Ipols	Help					
🗆 maz /le	/el/15/exec/-/show/b	uffer 💁						
* *	S 3 192.168.10.	1/level/15/exec/-/	show/buffers/failures				- Coog 🛃 🖓 🕈 Coog	- <u></u>
BackTra	ck Linux 🕅 Offensiv	e Security DEx	ploit-DB 🐚 Aircrack-ng 📓 Soma	FM				
maz	5							
Hone E	ec <u>Configure</u>							
10 generation								
Comman	bd							
Output								
Complete UP	e-URL wass /level/15/s L wass /level/15/exec	/·/sheu/huffers/fa	lares					
Connand vas	: show buffers faile	res						
	0							
Caller	Pool S	ize When						
command ci	ampleted.							
C.								

ेद 📄 🛛 🕹 🖳 🔄 😌 🐗 💻 🗧 07:01 pm 💚

Switch BED screen no buffer failures

	tunb/uo
🕘 🔗 mint709-switch /kevel/15/exec//show/buffers/failures - Mozilla Firefox	_ 8 ×
Ele Edit View Higtory Bookmarks Tools Help	
🛿 how to log buffer activeties in 🐒 🗍 mint709-switch /level/15/exec 💥 M Gmail: Email from Google 🛛 💥 👍	
💠 🛸 🕱 🛞 142.168.10.3/level/15/execi/jshow/buffers/failures 💿 🐨 🐼	🕶 Google 🔍 🙀
BackTrack Linux 🖬 Offensive Security 🛄 Exploit-DB 🐚 Aircrack-ng 📓 SomaFM	
mint709-switch	
Command	
Output	
Consund Name UBL var. / Arex/1235/srev/. Compate UBL var. / Arex/125/srev/. Compand var. shew boffers fallures	
Caller Pool Size When	
command completed.	
##	

ें 🖻 🛛 🕹 🔄 🖸 😌 🐗 🔚 👘 🖓

Switch SPIKE test screen shot



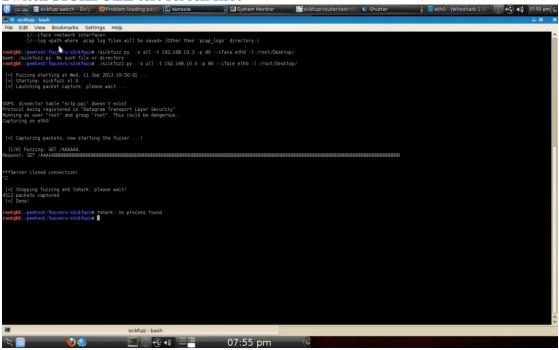
Switch SPIKE test no buffer failures screen shot

े 📄 🛛 🗐 😌 🐗 🖃 🗧 07:36 pm

🕘 💿 mint709-switch /level/15/exec/-/show/buffers/failures - Mozilla Rirefox			_ 6 X
<u>File Edit View History Bookmarks Tools Help</u>			
mint709-switch /level/15/exec/-/			
🖕 🔿 😒 🕘 192.168.10.3/level/15/exec/-/show/buffers/failures		😭 🕶 🥪 😽 🕶 Google	A 1
🕿 BackTrack Linux 👖 Offensive Security 🛄 Exploit-DB 🐚 Aircrack-ng 📓 SomaFM			
mint709-switch			
Command			
Output			
Consume bases HFL over // Const/JS/STREC/- Complete HFL over // Trest/JS/Strec/-/ heu/huffers/fallures Consumad was: show huffers fallures			
Caller Pool Size When	D		
command completed.			
##			
M. Sale Surgers and Strategies and Strat	a local at a second second second second		

A1 17-36

Switch SICKFUZZ test screen shot



Switch SICKFUZZ test buffer failures screen shot

2 A mint?		1 - Dolphin		h /level/15/e	🥱 🔜 System Monitor	sickfuzz-router-test-notes	sickfuzz-switch-wireshark j	(1) 38:00 pm
			/buffers/failures - Mozil	la Firefox				- 8
	⊻iew History §	-						
mint70	e-switch /level/15/	exec/-/	40					
-	S 🕙 192.168.	10.3/level/	15/exec/-/show/buffer	s/failures			🏠 🕶 🛃 🚺 🕶 Google	٩ ٢
BackTra	ck Linux 👖 Offen	sive Secu	rity 🚺 Exploit-DB 🐚	Aircrack-ng 📓 SomaFM				
min	t709-s	wit	ch					
		-						
Comman	hd							
output								
Conplete UR	e-URL vas: /level/ L was: /level/15/e : show buffers fai	xec/-/show/	buffers/failures					
aller	Pool	Size	When					
xD1030	CPU12 CPU12	1524 1524	00:02:56 00:02:55					
xD1030 x1979C4	CPU12 CPU12	1524 1524	00:02:52 00:02:49					
x1979C4	CPU12	1524	00:02:40					
x1979C4 x1979C4	CPU12 CPU12	1524 1524	00:00:13 00:00:10					
x1979C4	CPU12	1524	00:00:04					
xD1030 x1979C4	CPU12 CPU12	1524 1524	00:00:04 00:00:04					
ommand c	ompleted.							
,								
#								
#								
	username		Previous Ne	ext <mark>∕9</mark> Highlight <u>a</u> ll Match cı	ase 🚺 Reached end of page, contin	ued from top		

Switch SFUZZ test screen shot

Bit Gott Werk File Edit Werk Istrani[02] = 1//././file/passed] Istrani[02] = 1//./././file/passed] Istrani[02] = 1//./././file/passed] Istrani[02] = 1//./././/file/passed] Istrani[02] = 1//./././//file/passed] Istrani[02] = 1//./././//file/passed] Istrani[02] = 1///././//file/passed] Istrani[02] = 1///././//file/passed] Istrani[02] = 1//////file/passed] Istrani[02] = 1//////file/passed] Istrani[02] = 1/////file/passed] Istrani[02] = 1////file/passed] Istrani[02] = 1///file/passed] Istrani[02] = 1///file/passed] Istrani[02] = 1//file/passed]	💈 🚃 📰 sfuzz-switch – Dolphin	i 🥹 mint 709-switch Home Page [🖾 Kons	sole 👸 🔲 System Mo	nitor 📄 sfuzz test.odt - OpenOf	fice 🛛 📶 Capturing from eth0 🛛 [Wir	🗻 🕤 😪 4)) 07:28 pm((
literal[02] = [////cfc/passed] literal[04] = [////cfc/passed] literal[05] = [////cfc/passed] literal[05] = [////cfc/passed] literal[05] = [//cfc/passed] literal[05] = [/cfc/passed] literal[05] = [/cf	Sfuzz : bash					_ 8
Literal(8) = [//./et/passed] Literal(8) = [///et/passed] Literal(8) = [///et/passed] Literal(8) = [///et/passed] Literal(8) = [///et/passed] Literal(8) = [///et/passed] Literal(7) = [///et/passed] Literal(7) = [///et/passed] Literal(7) = [////et/passed] Literal(7) = [////et/passed] Literal(7) = [//////et/passed] Literal(7) = [///////et/passed] Literal(7) = [///////et/passed] Literal(7) = [///////et/passed] Literal(7) = [////////et/passed] sequence(1) = [/////////et/passed] sequence(1) = [/////////.//./	File Edit View Bookmarks Se	ttings Help				
	Literal[62] = [//64. Literal[63] = [//././ Literal[64] = [//./ Literal[64] = [//./ Literal[67] = [//./ Literal[67] = [//./ Literal[67] = [//./ Literal[67] = [//./ Literal[72] = [/// Literal[72] = [/// Literal[72] = [// Literal[72] = [// Beguince[3] = [Wh] Beguince[3] = [Wh] Beguince[passel] (*tc/passd] (*tc/passd] (*, *tc/passd] (*, *tc/passd] (*, *tc/passd] (*, *tc/passd] (*, *tc/passd] (*, *, *tc/passd] (*, *tc., *tc		192.168.10.3 -р вб		
sfuzz : bash	-					and the second second second
ेद्र 📄 🛛 🕹 😓 🔄 🖸 🚭 🐗 💻 🛛 07:28 pm 🕜	<u>ି କା</u>		07·28 pm	(C)		

Switch SFUZZ test No buffer failures screen shot

遼 二二	📰 sfuzz-switch	n - Dolphin	🕑 mint 709	-switch /level/15/exec/-/s	🗈 Konsole	6 🔲 System Monitor	sfuzz test.odt - OpenOffice.org 🗤	🕤 😪 🕪	97:31 pm
🕘 🔹 mint7	109-switch /level/	15/exec/-/show	/buffers/failures - Mozill	a Firefox					_ 6 ×
<u>File E</u> dit	<u>V</u> iew History	Bookmark	s <u>T</u> ools <u>H</u> elp						
() mint70	9-switch /level/	15/exec/-/	4						
4 4	S 🕲 192.16	8.10.3/level/	15/exec/-/show/buffer	/failures			🏠 🕈 🛃 🛃 🗸 Google		् 🏠
BackTra	ick Linux 🚺 Off	fensive Secu	rity 🚺 Exploit-DB 🐚	Aircrack-ng 📓 SomaFN	1				
min	t709-	swit	ch						
Comma	nd								
Complete U	se-URL was: /lev RL was: /level/1 s: show buffers	5/exec/-/show/	buffers/failures						
	0								
Caller	Pool	Size	When						
command c	ompleted.								
**									

ेंद्र 📄 🛛 🔮 🚱 🖉 🖉 🖉 🖉 🖓 💻 🖉

Appendix I - References

http://www.secforce.com/blog/2008/11/black-box-penetration-testing-vs-white-box-penetration-testing/ http://www.redsphereglobal.com/content/penetration-testing https://learningnetwork.cisco.com/blogs/network-sheriff/2008/09/22/sshv1-or-sshv2-whats-the-big-deal http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php http://searchitchannel.techtarget.com/feature/Password-protecting-a-router http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_login_enhance_ps6922_TSD_Products_Config uration_Guide_Chapter.html#wp1054087 http://www.cirt.net/nikto2 http://cirt.net/nikto2-docs/introduction.html http://en.wikipedia.org/wiki/Common Gateway Interface http://althing.cs.dartmouth.edu/local/www.thoughtcrime.org/ie-ssl-chain.txt " http://en.wikipedia.org/wiki/Clickjacking https://www.cirt.net/clickjack-test https://www.codemagi.com/blog/post/194 http://www.technicalinfo.net/papers/StoppingAutomatedAttackTools.html http://code.google.com/p/skipfish/wiki/SkipfishDoc https://www.golemtechnologies.com/articles/character-set http://www.acunetix.com/websitesecurity/xss/ http://en.wikipedia.org/wiki/Same_origin_policy http://en.wikipedia.org/wiki/Cross-site_request_forgery https://www.golemtechnologies.com/articles/incorrect-mime-types http://www.cert.org/advisories/ http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/white_paper_c11-458827.pdf https://www.golemtechnologies.com/articles/incorrect-mime-types http://en.wikipedia.org/wiki/Simple Network Management Protocol http://www.vulnerabilityassessment.co.uk/enum snmp.htm http://www.webpronews.com/snmp-enumeration-and-hacking-2003-09 http://www.symantec.com/connect/articles/cisco-snmp-configuration-attack-gre-tunnel http://www.question-defense.com/2012/12/29/snmpcheck-backtrack-5-information-gathering-network-analysis-snmp-analysissnmpcheck http://www.veracode.com/security/spoofing-attack http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html http://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx http://archangelamael.blogspot.ca/2010/05/SSLScan-in-bt.html http://luxsci.com/blog/how-does-secure-socket-layer-ssl-or-tls-work.html http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029?show=ssl-tls-beginners-guide-1029&cat=protocols http://www.redspin.com/blog/2009/08/24/enumerating-ssl-ciphers-with-SSLScan/ https://www.owasp.org/index.php/Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection (OWASP-EN-002) http://archangelamael.blogspot.ca/2010/05/SSLScan-in-bt.html http://pastebin.com/vcbZvap4 http://tipstrickshack.blogspot.ca/2012/10/dos-attack-from-linux-using-hping3.html http://geekinessthecoolway.blogspot.ca/2011/12/dos-attackthe-evil-and-madness.html#!/ madness.html http://www.dba-oracle.com/forensics/t_forensics_ntp.htm http://www.cert.org/advisories/CA-1996-01.html http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/copp.html http://www.windowsecurity.com/whitepapers/firewalls and VPN/Improving Security on Cisco Routers.html http://www.packet-craft.net/Malicious/ http://www.cisco.com/en/US/tech/tk59/technologies white paper09186a0080174a5b.shtml http://en.wikipedia.org/wiki/Denial-of-service attack http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products tech note09186a00800fb50a.shtml http://book.soundonair.ru/cisco/ch23lev1sec2.html] http://www.cisco.com/en/US/products/hw/modules/ps2643/products_tech_note09186a0080093fc5.shtml http://www.technicalinfo.net/papers/StoppingAutomatedAttackTools.html http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/ns391/guide c07-494658.html http://www.securityfocus.com/archive/1/archive/1/499685/100/0/threaded