# MINT 709

# CAPSTONE PROJECT REPORT

## DESIGNING NETWORK SECURITY LABS

By

Gowri Sarvepalli

## Faculty Advisor

M.H. MacGregor, PhD, PEng, SMIEEE
Professor and Chair
Department of Computing Science
University of Alberta
221 Athabasca Hall
Edmonton, Alberta, Canada T6G 2E8

## Contents

## Table of figures

# 1.0 Introduction

## 1.1 What Network Security is?

Network security is becoming more and more important as people spend more and more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more common. There are a number of good tools to assist with network security.

Bringing up **what is network security?** Security can be defined based on CIA Model that consists of the three core concepts: Confidentiality, Integrity and Availability.

*Confidentiality* means that information must not be disclosed to any unauthorized person.

*Integrity* means that the system must not corrupt data, and must disallow unauthorized, malicious or other accidental data changes.

*Availability* is the presence of objects or services in a usable form and capacity to meet service needs[1].

In general networks are of two types **Closed Networks and Open Networks**. Closed network can be defined as a dedicated line between headquarters and remote office location using PSTN as a medium for communication. These networks are less prone to malicious attacks since it uses dedicated line for communication. This type of networks is not cost effective because it always needs dedication lines for their medium for communication but at the same time it reduces the risk of attack.

The rapid growth in use of internet developed Open Networks. These networks have open access all throughout the world making it easy prone to malicious threats and attacks based on the attack tools that are available open source.

Considering the above network types, network security model has been devised as Open, Restrictive and Closed. So the security policies thus differ from high level to low level management.

Some of the trends that affect network security are,

- Increase in network and sophisticated attacks
- Increase in dependency of networks
- Lack of awareness and security policies
- Wireless Access

The network vulnerabilities depend on Technology, Configuration and Policy. Technology causing ease prone to attacks due to use of protocols like http, FTP and ICMP which are inherently insecure. The operating system and network equipment are also prone to attacks due to lack of authentication, routing protocols and firewall holes[2].

[1] Linux Security HOWTO by Kevin Fenzi and Dave Wreski

[2] Network Security Modules by Mohammed Amin

## 2.0 Project Description

### 2.1 Objective

- To develop a system, that implements a list of events that would establish a secured network lab using specified tools.
- This system will be crafted to shield specific network threats considering certain scenarios.
- To analyse the use of each tool, with examples of its use during the setup and testing of the lab environment.

### 2.2 System Overview

The project aims in building a network lab which will be crafted to shield specific network threats considering certain scenarios. The design of the project would involve implementing a list of events that would establish a secured network lab using specified tools. The key modules that form the part of this application are as follows:

1. Developing a software platform for network lab
2. Detecting Live systems
   - ✓ Port scanning with NMAP and Super scan
3. Enumerating systems
   - ✓ SNMP Enumeration
   - ✓ Enumerating Routing Protocols
4. Understanding Cryptographic tools
   - ✓ Rainbow crack
   - ✓ Crypt tool
5. Defeating Malware
   - ✓ Virus signatures
   - ✓ Building Trojans
   - ✓ Defeating Malware
6. Intrusion Detection
7. Forensic detection

### 2.3 Functional Overview

The application has been developed for the better understanding of security tools and provides service to develop specific tools which helps to secure our network. The system facilitates by providing the network with security measures by the analysis of specific tools to prevent unauthorised access, misuse, modification or denial of network and network accessible resources. The system also provides with high maintenance and advanced software and hardware to prevent malicious attacks like hacking and spamming. The functionalities provided by the application are explained in detail in the subsequent sections.

## 3.0 Development of Hardware and Software Platform

The security professionals and hackers use certain tools for causing attacks to the systems. These tools can be divided software and hardware. There are some software tools which can be used for good and also for malicious purposes like Port scanners, Ping sweep tools, Vulnerability assessment tools, OS fingerprinting tools, Exploit frameworks, Decompilers and Port redirection tools. Also there are some tools such as virus generators designed to create Trojans which spreads malware and causes problems. Some tools which are used to create attacks and threats are Trojans, Viruses, Worms, Malware, Spyware and Backdoors. Some of Hardware hacking tools which be used for good and nefarious purposes are Wi-Fi detectors, Lock picks, Phone taps.

### 3.1 Essential Hardware and Software Gear

To develop this application Designing Network Security Labs we require some of hardware devices like Cables, NAS, Computers, Hubs, Switches, Routers, Firewalls, Wireless Access Points, Suppressors and power strips.

This system requires at least two computers one to attack and other one to monitor the network behaviour to which the attack has been launched. The computers with fast processor, lot of memory and with good disk space can be better. It also requires variety of cables to configure the network in different ways. Specific configurations are required for different scenarios. Network Attached Storage can be useful in many ways like to store copies of configuration files, and software.

Hubs, Switches and routers are the building blocks of network infrastructure. These devices perform different roles like hub is a common connection point for all devices which contains multiple ports. Switches are device that filters and forwards packets between LAN segments. Routers are used for filtering data packets along the networks. Routers are usually located at the gateways[3].

An internet connection is a necessary. A firewall can be used to protect our primary network from the unpleasant things that can occur in the lab which is one of important component. It can be either hardware based or software based. Some of the software based firewalls are Kaspersky Internet security, Outpost, Comodo. We also need a Wireless Access Point if need security mandate for wireless networking. Some of the other essential hardware devices like power strips, surge suppressors, UPS etc.

### 3.2 Network Design

To develop this project we need a Network design which includes two computers where one should run windows and other should run Linux. This can be designed by using two computers or by using some type of virtual machine like VMware player. Then there should be at least one router that connects to

[3] Difference between network devices by Ron Pacchiano

outside world. This could be either internet connection or a connection that connects to other network. Now we need to assign IP addresses for the PCs and default gateway.

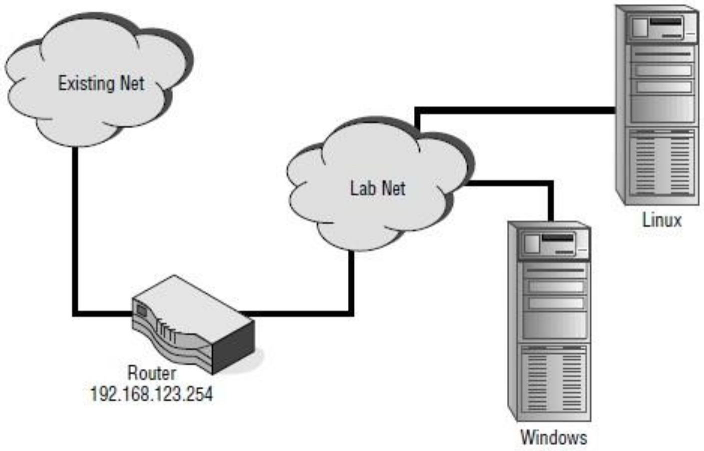


Figure 1 Basic Network design

To build the network we need to consider certain steps like Start to clean the devices like routers, switches and bring it back to the factory defaults using commands like erase nvram. Configure the router that a DHCP server will lease an IP address and associated information to the WAN (Ethernet1) interface on the router. Also the LAN side (Ethernet0) interface is set up to serve DHCP to clients. Addresses on the LAN are from the 192.168.123.0/24 subnet. Addresses in the range 192.168.123.1 through 192.168.123.100 have been excluded from the DHCP pool so that you may use them for static address assignments.

The next important thing is whether to use hubs or switches in your lab network. By default, switches may eventually need to be included. Install the Operating System Windows or Linux on the two computers. To connect everything together, we need to connect the devices as given in figure 1 and determine the IP addresses for the systems and ping them back and forth to ensure connectivity. Next thing is to add a wireless gear, so Wireless Access Point is a simple and Economical addition to the network. Some software alternatives that might help in this regard, VMware and similar products allow one physical machine to host multiple operating systems simultaneously.

## 4.0 Detecting Live Systems

Detecting live systems on a network is to determine the border of target network, to facilitate network mapping, to build an inventory of accessible system on the network. Port Scanning is one of the most widely used methods for detecting systems. Tools used in this method include Wardialing, Wardriving and Ping utilities.

## 4.1 Wardialing

Wardialing is a tool used for scanning the pool of telephone numbers in an organisation to detect vulnerable modems which provides access to systems.

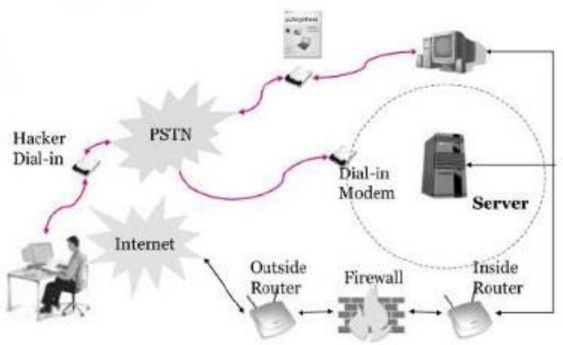


Figure 2 Wardialing[4]

A demon dialer is a tool used for monitoring specific phone number and target it modem to gain access. Threats are expected to be high in systems with poor configuration to remote access providing entry to larger networks. Some of the tools include THC-scan, ToneLoc, TBA .The term war dialing implies the development of an organization's telephone, dial, and private branch exchange (PBX) systems to pass through the internal network and use of computing resources during the actual attack.

Wardriving is the updated form of Wardialing which is the act of driving around for open wireless access points. Wardriving helps to find and identify the Wireless Access Points. In an organisation there is a need check for signal strength of the access points and find the rogue access points. Usually in organisations the network will be secured but there is always a possibility an employee having unsecured access points which leads to attacks and threats to the organisations. Most of the networks should have been controls like

Firewalls: Acts like a shield in an organisation which prevents unauthorised and unwanted communications between the network and hosts.

VPNs: Virtual Private Networks uses authentication in an organisation to deny unauthorised users, and provided with encryption to prevent unauthorised users to access network traffic. VPNs are used for send any kind of traffic including voice and data.

IDS (Intrusion Detection System) is a software that monitors network and system activities to detect the malicious attacks or policy violations and provides with report.

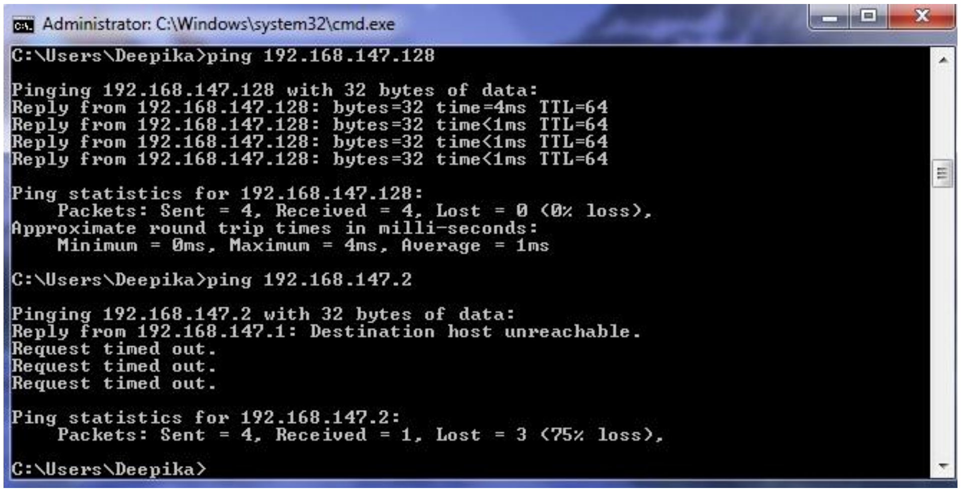
Encryption: Process of transforming plain text to make it unreadable to prevent unauthorised eavesdropping of information to be transmitted or stored.

[4] Basics of Ethical Hacking by Manthan Desai

Almost all the networks are been installed with these controls but by installing single wireless access point all these controls can be negated. Wireless access points should be installed with security. Our earliest Wireless Security Implemented was Wired Equivalent Privacy (WEP) which generates a secret key for security purposes but as the updates were done attackers found easy way to generate these secret keys. Then Wi-Fi Protected Access (WPA) was created to address the issues with WEP. These tools offer a way to find and identify systems. The basic method that can be used to determine whether the system is active. This is a process of using ping utilities.

## 4.2 Ping Utilities

ICMP (Ping) is a process of sending ICMP Echo Request packet and waits for ICMP Echo Reply from a live system. If the ping is blocked then the TCP/UDP packets are sent. Any network device using TCP/IP has the capability of send, receive, or process ICMP messages. ICMP messages won't flood the network; they are given no special priority. ICMP messages are usually treated as normal messages. The most common type of ICMP message is Ping. ICMP Ping helps in measuring network traffic by time- stamping each packet. Ping can also be used for resolving host names. An example as follows



```
C:\Users\Deepika>ping 192.168.147.128

Pinging 192.168.147.128 with 32 bytes of data:
Reply from 192.168.147.128: bytes=32 time=4ms TTL=64
Reply from 192.168.147.128: bytes=32 time<1ms TTL=64
Reply from 192.168.147.128: bytes=32 time<1ms TTL=64
Reply from 192.168.147.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.147.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\Users\Deepika>ping 192.168.147.2

Pinging 192.168.147.2 with 32 bytes of data:
Reply from 192.168.147.1: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.147.2:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),

C:\Users\Deepika>
```

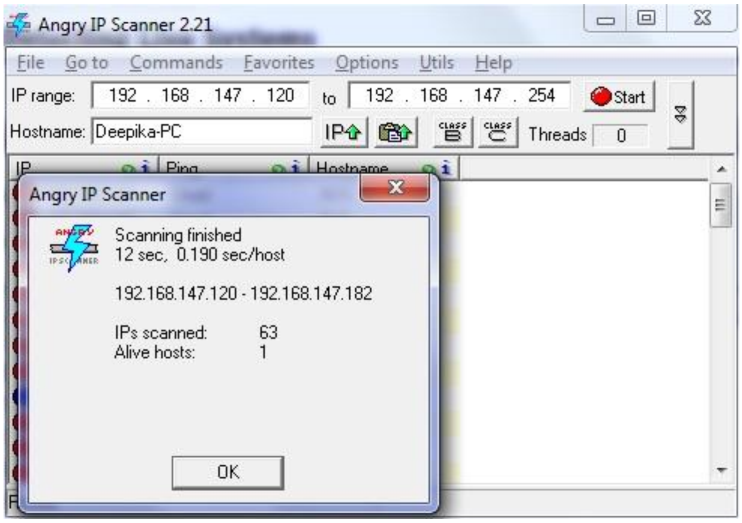
.

Figure 3 ICMP Ping message

If the target device is unreachable, request timeout is returned. You can see the example above when I pinged a firewalled host 192.168.147.2.

Thus ping is a useful tool to identify active systems and measure the speed at which packets are moved from one host to another.

To ping large number of hosts, a ping sweep is usually performed. Program that perform ping sweeps typically sweep through a range of devices to determine which one are active. . Some of the tools includes Angry IP scanner, NetScan, NMap, HPing, ProPack, ICMPenum, WS_Ping, Pinger .Angry IP Scanner is an example of one of the programs that can scan ranges of IP addresses. After you open the program, you will want to first configure the type of scan. Figure 4 shows the configurable options.



IP range: 192 . 168 . 147 . 120 to 192 . 168 . 147 . 254

Hostname: Deepika-PC

Threads 0

Scanning finished
12 sec, 0.190 sec/host

192.168.147.120 - 192.168.147.182

IPs scanned: 63
Alive hosts: 1

Figure 4 Angry IP Scanner

After configuring Angry IP Scanner, click the Start button to start the scan and it shows completed scan report with the number of Active hosts.

Ping does have drawbacks like it only identifies that a particular system is active on the network. Ping does not identify which services are running. Second, many network administrators have now blocked ping and no longer allow it to pass the border (gateway) device. Finally, if ping is used from the command line, only one system at a time is pinged. Although ping may offer only limited information, there is still one other method that is considered the most reliable, and that is port scanning.

Ping tools are usually detected by IDS. We can detect the ping sweep through software like SNORT IDS, BlackICE and Scanlogd.

## 4.3 Port Scanning

Port Scanning is a process of connecting TCP and UDP port to find the open services on the target devices. Once open services are discovered the attacker can easily access the system.

TCP/IP Basics

Three-Way Handshake

**H1--SYN----->H2**
**H1<-SYN/ACK--H2**
**H1--ACK----->H2**

Port Scanning manipulates the three way handshake to find the open ports available. Most targets are found on the running services on well known ports. There are different scan techniques used like FTP bounce scan, Idle Scan, Sweep, UDP Scan, Fragmented packets.

A tool like Super Scan scans both live and open ports. If hosts don’t reply then there is a block of ICMP packets and lack of route back.

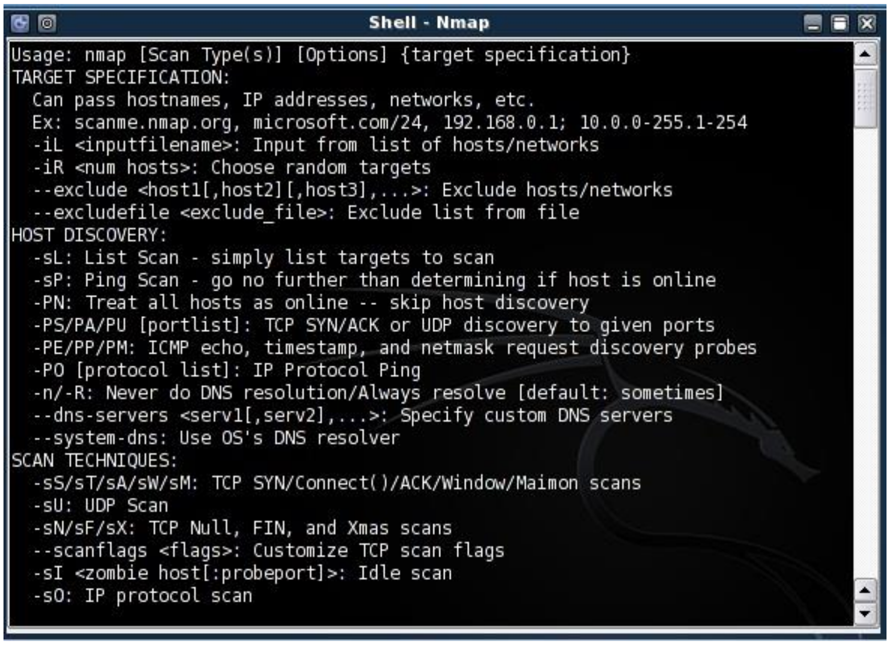
Stealth Scan allows tricking the IDS systems. NMap allows scanning specific range of ports.

Socks Chain allows getting through HTTP proxies and allows finding traffic which are allowed to go through.

A proxy server acts as the man-in-the-middle and has the control of allowed behaviours. A proxy server also caches sites so they load faster for end-users. Proxy servers can be used to anon. web surfing. Proxy servers can also protect the local network from outside access.

We can bypass firewalls through Httptunnel. Httptunnel creates a bidirectional virtual data path tunnelled in HTTP requests. The requests can be sent via an HTTP proxy. HTTPPort allows bypassing an HTTP proxy. It serves as a kind of port translation. We just have to find the rules of the security device, then craft the packets to match those rules[5].

NMap allows different kind of scans. The most basic is the Connect Scan. Connect Scan does the three-way handshake and is very noisy. There are a few stealth modes like the FIN Stealth Scan which alters the way TCP behaves. Right after the SYN/ACK reply from a host, the system would reply with a FIN, which terminates the connection.

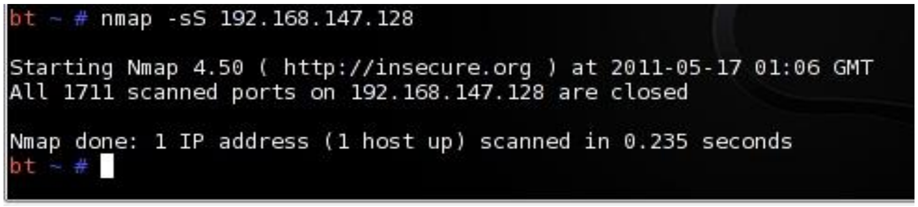


```
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO [protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sO: IP protocol scan
```

Figure 5 NMap Basic Output

NMap shows its basic output is shown in figure 5 when no scan is performed but it shows types of scans which can be performed using NMap. An example performing Stealth Scan in a network as follows,

[5] Basic Draft ethical hacking by Kevin Ang



```
bt ~ # nmap -sS 192.168.147.128

Starting Nmap 4.50 ( http://insecure.org ) at 2011-05-17 01:06 GMT
All 1711 scanned ports on 192.168.147.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.235 seconds
bt ~ # 
```

Figure 6 NMap Stealth Scan

Next we can have a look at GUI scanning program called Super Scan which can scan both live and open ports and perform ping scans. It gives customized scan ranges and customized reporting status.

## 4.4 OS Fingerprinting

OS Fingerprinting describes the method of using the information gathered about the target host, find which OS it works on. In this approach Operation System is the major key information. As long as the information is not revealed, the attacker is limited to variety of attacks, probes and exploits.

The detection of operating system can be done in two ways: Active and Passive OS fingerprinting tool. A Passive tool does not directly interact with the target system. It monitors the network traffic and analyses the pattern which has the characteristic of known Operating system. Due to its stealth and low network impact, the most accurate results are achieved when connected directly.

An active OS fingerprinting tool interacts directly with target network. After analysing the responses received from the target network, it is possible guess the Operating system accurately.

**Passive Fingerprinting**

Passive Fingerprinting is one way to identify certain information like IP addresses, active systems and open ports. While determining these information we never what type of system we are dealing with. Passive sniffing is done to examine the packets as they come by. Then these packets are been examined to determine the Operating System. Commonly examined items to fingerprint an OS are,

IP TTL Value: Different OS sets the TTL to unique values on outbound packets.

TCP Window Size: OS vendors usually use different window size for different OS

IP DF option: Not all vendors handle fragmentation in the same way.

IP TOS Option: This option controls the priority of specific packets. This differs in each OS depending on the vendors.

These are four possibilities which can be done on passive fingerprinting. Some of the tools include Linux-based tool, P0f. P0f passively fingerprints the source of incoming connections when the tool is running and looks specifically at IP and TCP fields:

**IP Headers**

Initial Time to live

Don’t Fragment

**TCP Headers**

Overall SYN packet size

TCP options such as windows scaling and segment size

TCP Windows size

P0f usually looks at TCP session start-ups in particular the SYN segment. P0f.fp file uses the following format,

**wwww:ttt:D:ss:OOO...:QQ:OS:Details**

| | |
|---|---|
| wwww | - window size (can be * or %nnn or Sxx or Txx) |
| ttt | - initial TTL |
| D | - don’t fragment bit (0 - not set, 1 - set) |
| Ss | - overall SYN packet size (* has a special meaning) |
| OOO | - option value and order specification (see below) |
| QQ | - quirks list (see below) |
| OS | - OS genre (Linux, Solaris, Windows) |
| Details | - OS description (2.0.27 on x86, etc) |

When P0f operates in the promiscuous mode we can use –p option, we can monitor the network connections. Analysing the SYN segment of TCP start up session means just fingerprinting the system that initiates the connection. So we need to focus on ACK-SYN to fingerprint the system. While passive fingerprinting is not as accurate as active fingerprinting, it is a stealth way to identify the system.

**Active Fingerprinting**

Active fingerprinting is more powerful then the active fingerprinting because it doesn’t require random packet for analysis. This tool just waits for the user to inject the packets into the network. As we did the four possible differences in implementation of TCP/IP stack on vendors in passive fingerprinting, the same analysis is done in active fingerprinting. Therefore, if someone probes for the differences the OS can be easily determined. Some of basic methods in Active fingerprinting,

FIN probe: A FIN packet is sent to open port, and the response has been recorded. Here some OS including windows will respond with a reset.

Bogus Flag probe: A bogus Flag probe sets one of the used flags along with SYN flag in an initial packet. Os like Linux will respond to this by setting the same flag in the subsequent packet.

Initial Sequence number sampling: This done by looking the patterns of ISN number. Here some systems will use some random numbers whereas others have increment in the number by a small fixed amount.

IPID Value: Many systems increment the IPID value when they send each packet. OS like windows increment by value by 256 for each packet.

TCP Initial Window: This technique works by tracking the window size in packets returned from the target device. Many operating systems use the exact size that can be matched against a database to uniquely identify OS.

ACK Value: Here again vendors differ in the ways they have implemented the TCP/IP stack.

Type of Service: By examining the Type of Service (TOS) field, some use 0 and other return different values.

TCP Options: Different vendors support different TCP options. By sending packets with different options set, the responses help to find the server's fingerprint.

Fragmentation Handing: Different OS vendors handle fragmented packets differently.

## 4.5 OS Fingerprinting Tools

Nmap is most used fingerprinting tool. For reliable prediction open port and closed port is required. An example fingerprint scan is

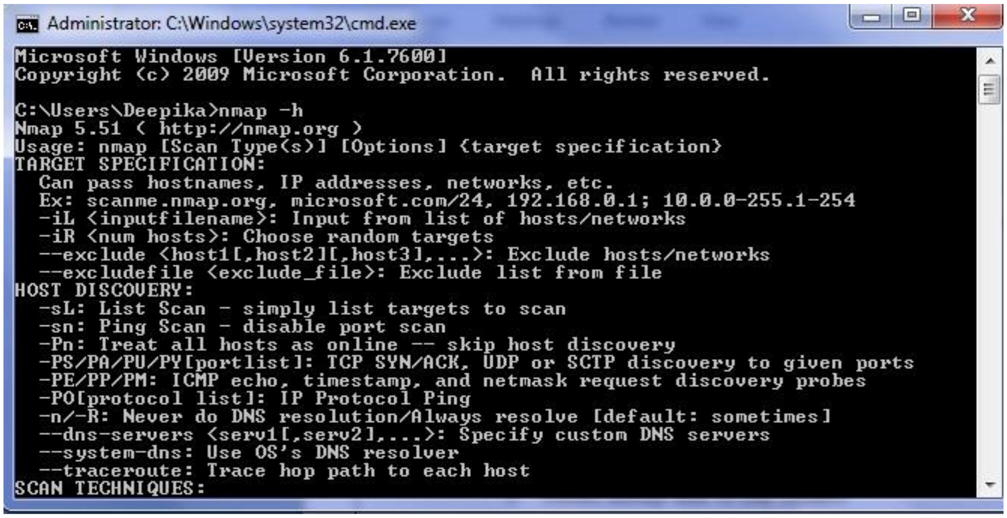
Xprobe2 is another active operating system fingerprinting tool with a different approach to OS fingerprinting. Xprobe2 relies on fuzzy signature matching. The target will be run through number of tests. It is also unique in using a mixture of TCP, UDP, and ICMP to split past firewalls and avoid IDS systems.

## 4.6 Examples

Best tools used for specific scenarios as described above,

### 4.6.1 Port Scanning with NMap

1. Install NMap tool in the system
2. In the command line, enter the following,
   Nmap –h

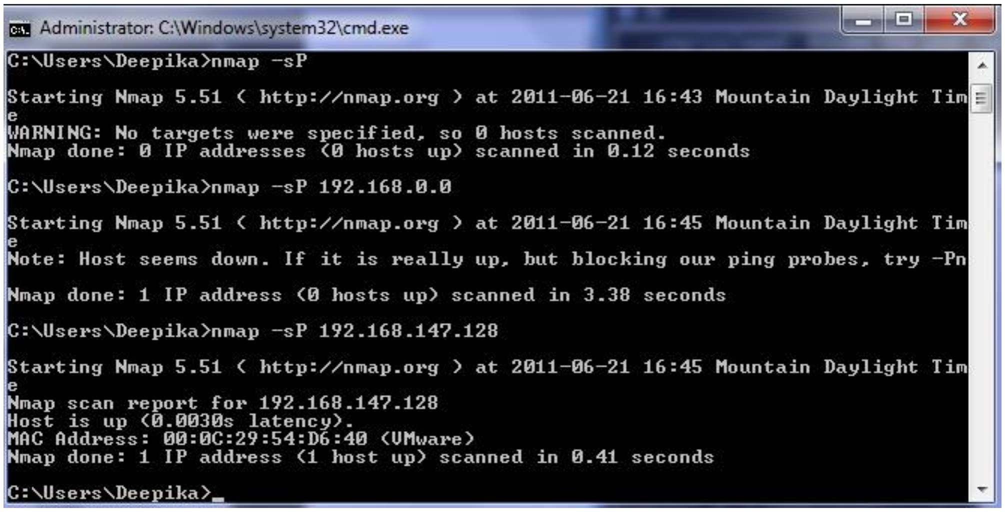


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Deepika>nmap -h
Nmap 5.51 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

This provides list of command syntax of Nmap and some of the types of scan it can perform.

3. Enter the IP address within our network and enter the following in the command line, nmap –sP <IP Address>

The output will be,



Administrator: C:\Windows\system32\cmd.exe

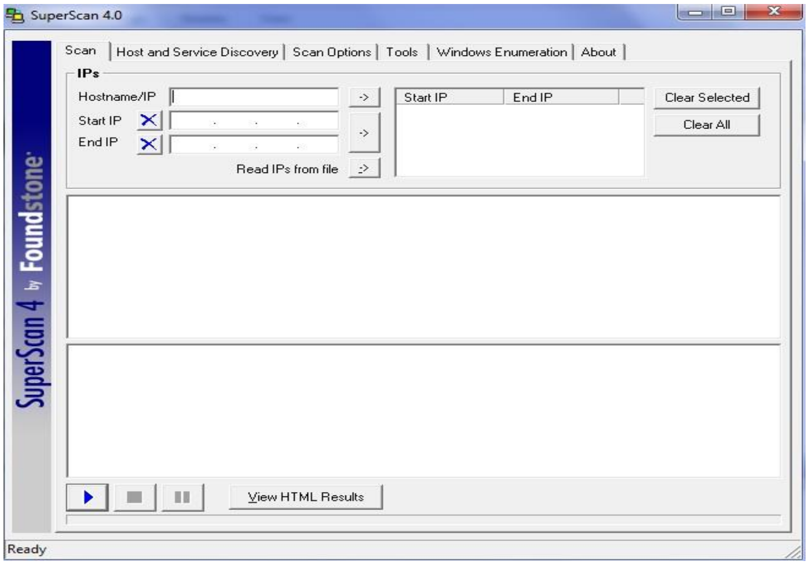
```
C:\Users\Deepika>nmap -sP

Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-21 16:43 Mountain Daylight Tim
e
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds

C:\Users\Deepika>nmap -sP 192.168.0.0

Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-21 16:45 Mountain Daylight Tim
e
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 3.38 seconds

C:\Users\Deepika>nmap -sP 192.168.147.128

Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-21 16:45 Mountain Daylight Tim
e
Nmap scan report for 192.168.147.128
Host is up (0.0030s latency).
MAC Address: 00:0C:29:54:D6:40 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

C:\Users\Deepika>_
```

This option provides Nmap scan report with details host and its MAC address.

This is how the scanning tools like Nmap works. We can also see how the GUI based scanning tool Superscan works.

### 4.6.2 Port Scanning with Superscan

1. Install the Superscan program as shown in the figure below,



2. Enter the starting IP address and ending IP address and start scanning.
3. Select Host and Service Discovery tab, the respective details will appear.
4. After the scan is complete, the report will be generated by selecting HTMP report.

This report helps us to examine open services and determine which ports and services are open or secured.

## 5.0 Enumerating Systems

Enumeration is the ability to convince a machine to give information that would help in the attack. Enumeration can help find accounts, and other hosts on the network[6].

This means identifying the open ports, applications, vulnerable services, DNS or NetBIOS names, and IP addresses before an attack.

NetBIOS names are one of the basic ways to do enumeration. Here a Null Session will be established with windows host by logging on with a null username and password. These null connections will help us to gather information about the host,

- Lists of users and groups
- List of hosts
- List of Processes

NBTscan helps us to scan for any NetBIOS name information about the target network. If any hosts are found, it gives a list of IP addresses, computer name, user name, and MAC address.

DumpSec also uses Null session to enumerate printers, to access some user control lists and accounts, sharing files. NetBIOS Auditing tool explores the file sharing services and these sessions can be established through TCP port 139.

Enumeration is not just a window type of activity. But this can be performed on different system and services like,

- SNMP (Simple Network Message Protocol)
- Routing Devices
- Some Vulnerable services

### 5.1 SNMP Services

Simple Network Management Protocol is a TCP/IP standard for remote monitoring and management of hosts, routers and other nodes and devices on the network. SNMP interacts with various devices; it also sends requests to mediators and gets replies back. Any SNMP utility can easily enumerate the information, if something significant happens in the system like reboots and disk failures.

[6] Basic Draft ethical hacking by Kevin Ang

SNMP are attracted by both attackers and network managers for,

SNMP can be used to manage and report on servers, routers, switches, and hubs.

It is also a part of larger framework called Internet Standard Network Management Framework.

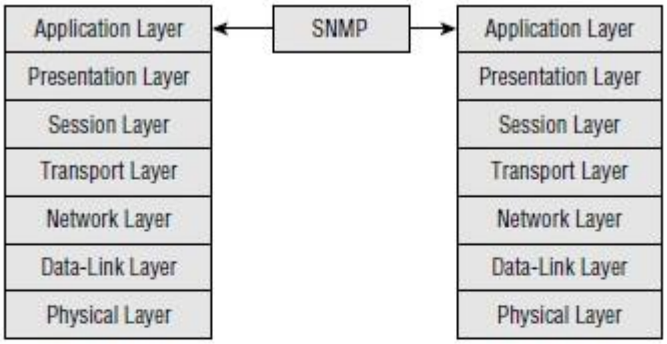


Figure 7 SNMP and OSI Model

SNMP uses two components like Manager and Agent. The manager sends requests and the agent replies back to the request.  Both of them use something called Management Information Base (MIB). MIBs are organized structure with set of managed objects. Some of the other components in SNMP include managed objects and protocol data units.

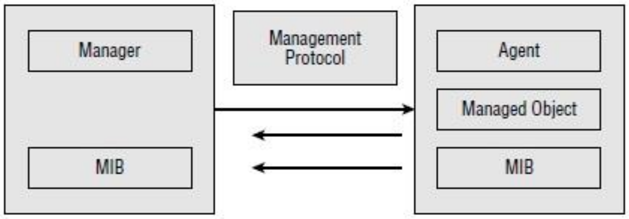


Figure 8 SNMP Structure

Management stations can also send request to set values for some variables. Traps set thresholds to alert managers that something significant has occurred, like reboots and interface failures. SNMP was designed to keep the protocol simple and UDP protocol was implemented.

SNMP has been released in different versions. Version 1 is a provided limited security and is a clear text protocol. SNMP v3 provides with encryption and authentication.

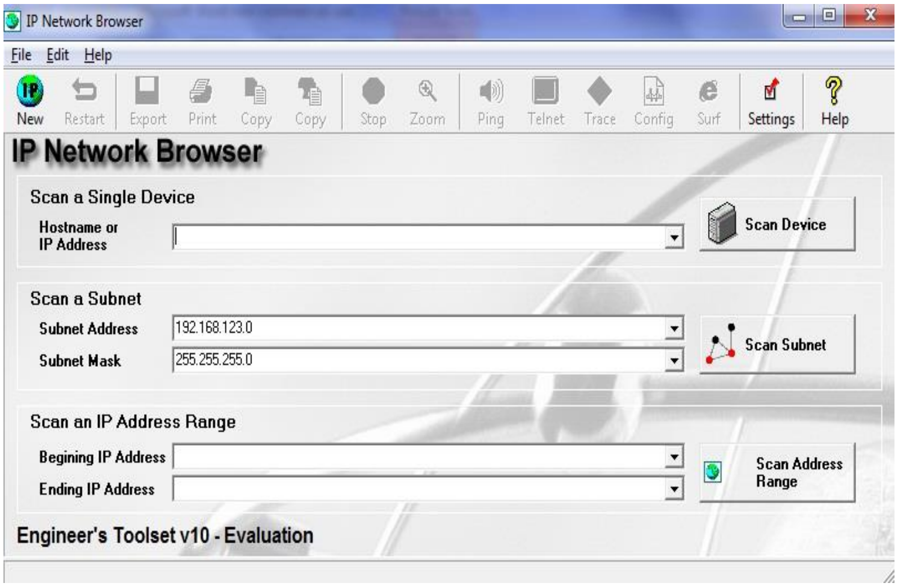
### 5.1.1 SNMP Enumeration Tools

SNMP acts as attractive target for the attackers who attempt to enumerate the network.  Attackers approach is to use the default community strings. If the attackers don’t succeed in this approach they attempt to sniff the community strings and determine what they are.

SNMP-enabled devices share a lot of information.  Considering how attackers use this type of data by knowing the usernames, by which half of the information will be known to gain access to many systems. SNMP enabled devices are considered to be more vulnerable. Considering some of the SNMP tools,

**SNMPUtil** is a command line utility which allows querying the MIB information from a network device. By using SNMPUtil we can SNMP OID and get the information to gain access.

**Solarwinds IPNetwork  browser**: Using this tool we can perform the network discovery on single subnet or range of subnets using ICMP and SNMP and displays discovered devices at run time. Information is gathered through ICMP and SNMP local or remote network. IP Network browser scans single IP or IP address range and displays the network devices as they are discovered in real time, providing with the information regarding the devices on the network.



Subnet Address 192.168.123.0

Subnet Mask 255.255.255.0

Figure 9 IP Network Browser

**GetIF:** GetIF is a free multi-functional windows GUI based Network Tool which is an excellent SNMP tool that allows gathering information from SNMP devices. GetIF is much more than an SNMP browser that as ability to graph OID values over time, display the device's interface information, routing and ARP tables, as well as do basic port scans, Traceroutes, NSLookups, and IP scans.

### How does SNMP Enumeration Process Works?

- Attacker begins by port scanning for port 161
- Attacker attempts to connect to SNMP-enabled devices using default community strings or by sniffing community strings.
- Attacker by using the information acquired makes an attempt to login to an enumerated system.
- Attacker escalates privilege.

### SNMP Enumeration Countermeasures

The best defence against SNMP Enabled devices to disable it when it is not required. In case if it is required block port 161 at network choke-points. And we can also change the community strings, doing so will make them different in each zone of the network. Finally, we can implement ACL filtering to only access read-write community approved from stations or subnets.

## 5.2 Routing Devices

Routers are one of the basic building blocks of networks because they communicate with the networks. Routers use the routing protocols to help packets find the best path to a target network. Routers are primarily devices which are concerned with routing and routed protocols. Routing table helps the router to examine the target IP address and determine to handle the information.

Routing begins when a packet is built and prepared to send. Here the routing protocol examines the packet's destination and compares it with the routing table. On more complicated networks the packets are routed dynamically using certain metrics,

Bandwidth: Determines the capacity of the link and here the router chooses the one with the highest bandwidth.

Cost: Consider an organization may have a dedicated T1 and an ISDN line. If the ISDN line has the highest cost the traffic will be routed through the T1 line.

Delay: This depends on many factors like router queues, bandwidth and congestion.

Distance: This metric is calculated in hops.

Load: Determines the measurement of load that is being placed on particular router that can be calculated by the processing time or CPU utilization time.

Reliability: By examining arbitrary reliable ratings, determine the most reliable link to be used.

By considering these metrics and by consulting the routing table, the routing protocol determines the best path for traversing. Routing protocols can be of two categories like Static routing and Dynamic routing.

Static routing works better when it is for small networks. Dynamic routing uses the above explained metrics to determine the best path for the packets to traverse and send it to determined destination. Some of the dynamic routing protocols are,

RIP: Routing Information Protocol for designed especially for the small network environments with limited number of machines, and these are connected with the links that had identical characteristics. Rip enabled devices updates message every 30 seconds which includes the following information,

- Destination address of host or network
- The IP address of the default gateway
- A metric determining the number of hops i.e. distance

IGRP- Interior Gateway Routing Protocol which is stable, optimal routing for the large inter-networks with no routing loops and it has the ability to handle multiple types of services. Low overhead when in terms of bandwidth and router process utilization. IGRP has ability to split traffic into several parallel routes when they are of roughly equal desirability.

OSPF: Open Shortest Path First is a open standard implemented by all major router manufacturers. OSPF is a classic link state routing protocol and requires that the network be physically configured in a routing hierarchy and uses the shortest path algorithm and it only supports routing for IP.

Integrated IS-IS: Intermediate System to Intermediate System which is used by routers to talk with each other which is a link state protocol and is utilized in Digital Equipment. This was made Integrated because it can carry route information for protocols other than OSI, most notably TCP/IP protocols. The technology behind IS-IS is similar to OSPF.

EGP and BGP: These protocols are designed to regulate traffic that can travel between different systems and protect each from any bugs in another system.

Routers and Routing Protocols are a potential target for because they offer lot of information to the attacker to use. Information that can be gathered by attacking these devices includes,

- Network addressing topologies
- Information about the network owner and location of the routing device
- Interesting hosts that may be attacked
- Routing policies and rules and implemented security levels

### 5.2.1 Routing Enumeration Tools

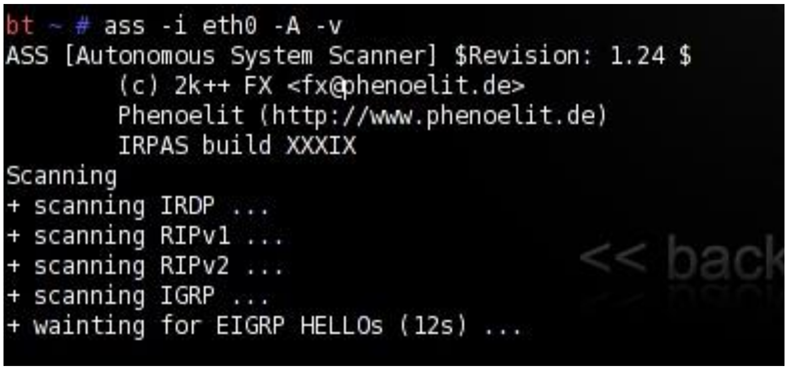
One way to start the enumeration process is to use browser by just using online searches like Google Hacking, we might be able to find the vulnerabilities. The entities which can be found includes,

- Usernames
- Encrypted Passwords
- TFTP servers
- IP Addresses of Routers
- Access lists
- Routing tables

The first best enumeration tool as discussed above is browser which helps the attacker to find the above mentioned entities.

Next thing is Autonomous System Scanner which works with following protocols like: IRDP, IGRP, EIGRP, RIP v1, RIP v2, CDP and OSPF. This program works in two modes active and passive mode.

In passive mode, **(./ass –i eth0)** the program listens to the routing protocol packets, such as broadcast and multicast hellos. In active mode, **(./ass –i eth0 -A)** , the program tries to discover the routers by retrieving the information. Usually passive mode can’t be easily detected whereas the active mode is more accurate.



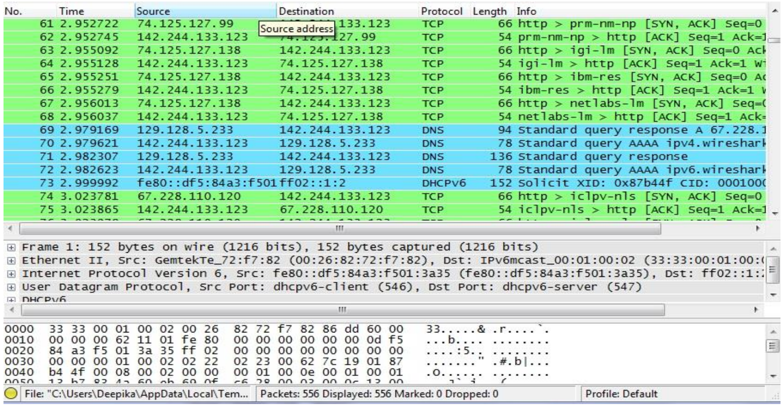
```
bt ~ # ass -i eth0 -A -v
ASS [Autonomous System Scanner] $Revision: 1.24 $
        (c) 2k++ FX <fx@phenoelit.de>
        Phenoelit (http://www.phenoelit.de)
        IRPAS build XXXIX
Scanning
+ scanning IRDP ...
+ scanning RIPv1 ...
+ scanning RIPv2 ...
+ scanning IGRP ...
+ wainting for EIGRP HELLOs (12s) ...
```

Figure 10 ASS Active mode

When we are using RIP protocol, we will have issues like,

- No security
- Based on the hop counts
- Uses UDP
- Uses broadcasts
- Sends full updates about every 90 seconds

If the attacker discovers the system with RIP protocol, it takes few steps to redirect the traffic flow and launch the denial of service. Each request is sent considering the entities like unspecified address, routing tag, netmask, and the next hop. Autonomous System Scanner works well against all versions of RIP, it does not work well with Open Shortest Path First (OSPF). This routing protocol works differently from RIP because it is considered to be as Link State routing Protocol. We can easily determine the type of routing protocol on the network by using Wireshark.



```
No.   Time       Source              Destination       Protocol Length Info
   61 2.952722   74.125.127.99       142.244.133.123   TCP        66 http > prm-nm-np [SYN, ACK] Seq=0
   62 2.952745   142.244.133.123     74.125.127.99     TCP        54 prm-nm-np > http [ACK] Seq=1 Ack=1
   63 2.955092   74.125.127.138      142.244.133.123   TCP        66 http > igi-lm [SYN, ACK] Seq=0 Ack
   64 2.955128   142.244.133.123     74.125.127.138    TCP        54 igi-lm > http [ACK] Seq=1 Ack=1 Wi
   65 2.955251   74.125.127.138      142.244.133.123   TCP        66 http > ibm-res [SYN, ACK] Seq=0 Ac
   66 2.955279   142.244.133.123     74.125.127.138    TCP        54 ibm-res > http [ACK] Seq=1 Ack=1 W
   67 2.956013   74.125.127.138      142.244.133.123   TCP        66 http > netlabs-lm [SYN, ACK] Seq=0
   68 2.956037   142.244.133.123     74.125.127.138    TCP        54 netlabs-lm > http [ACK] Seq=1 Ack=
   69 2.979169   129.128.5.233       142.244.133.123   DNS        94 Standard query response A 67.228.1
   70 2.979621   142.244.133.123     129.128.5.233     DNS        78 Standard query AAAA ipv4.wireshark
   71 2.982307   129.128.5.233       142.244.133.123   DNS       136 Standard query response
   72 2.982623   142.244.133.123     129.128.5.233     DNS        78 Standard query AAAA ipv6.wireshark
   73 2.999992   fe80::df5:84a3:f501 ff02::1:2         DHCPv6    152 Solicit XID: 0x87b44f CID: 0001000
   74 3.023781   67.228.110.120      142.244.133.123   TCP        66 http > iclpv-nls [SYN, ACK] Seq=0
   75 3.023865   142.244.133.123     67.228.110.120    TCP        54 iclpv-nls > http [ACK] Seq=1 Ack=1

⊞ Frame 1: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
⊞ Ethernet II, Src: GemtekTe_72:f7:82 (00:26:82:72:f7:82), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:0
⊞ Internet Protocol Version 6, Src: fe80::df5:84a3:f501:3a35 (fe80::df5:84a3:f501:3a35), Dst: ff02::1:2
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊞ DHCPv6

0000  33 33 00 01 00 02 00 26  82 72 f7 82 86 dd 60 00   33.....& .r....`.
0010  00 00 00 62 11 01 fe 80  00 00 00 00 00 00 0d f5   ...b.... ........
0020  84 a3 f5 01 3a 35 ff 02  00 00 00 00 00 00 00 00   ....:5.. ........
0030  00 00 00 01 00 02 02 22  02 23 00 62 7c 19 01 87   ......." .#.b|...
0040  b4 4f 00 08 00 02 00 00  00 01 00 0e 00 01 00 01   .O...... ........

File: "C:\Users\Deepika\AppData\Local\Tem...   Packets: 556 Displayed: 556 Marked: 0 Dropped: 0   Profile: Default
```

Figure 11 Wireshark

From which we can see OSPF uses authentication where as RIP v1 has no authentication. If OSPF has turned off the , we can easily inject OSPF packets into the network that causes various types of havoc.

### 5.2.2 Routing Enumeration Countermeasures

We can block the routing enumeration in several different ways,

**Higher-end switches** - These devices are designed for high level of security with advanced features.

**Dynamic ARP inspection** - A feature provided especially in the man in the middle attacks.

**Anti-Sniffing** - Detecting fake ARP traffic or flooding attempts to bypass the functionality of the switch.

**Promiscuous mode detection** - This detects NIC that are listening to traffic.

**Improved routing protocols** - Moving from RIP to OSPF which provide special type of authentication.

**Signatures added to IDS** – IDS can be used to detect signatures of router enumeration and router attacks.

Now, we can consider Sniffing which is one of the primary ways to find what protocols are running. Sniffing would be easier when the attacker targets on hubs, he can just plug into open RJ-45 to sniff the traffic. When it is not hubs, then the attacker has to use active sniffing. When it is switches that limits the traffic that sniffer can see to broadcast packets. Two ways the attacker can attempt to overcome the switch are MAC-flooding and ARP poisoning.

Mac-flooding is a method that can be used to impact security protocols of different types of different switches. This floods the network switch with data packets that disrupts the flow of data i.e. common with the MAC addresses. Thus resulting the data distributed all over the ports rather only between sender and recipient. But MAC-flooding is not effective against higher-end switches.

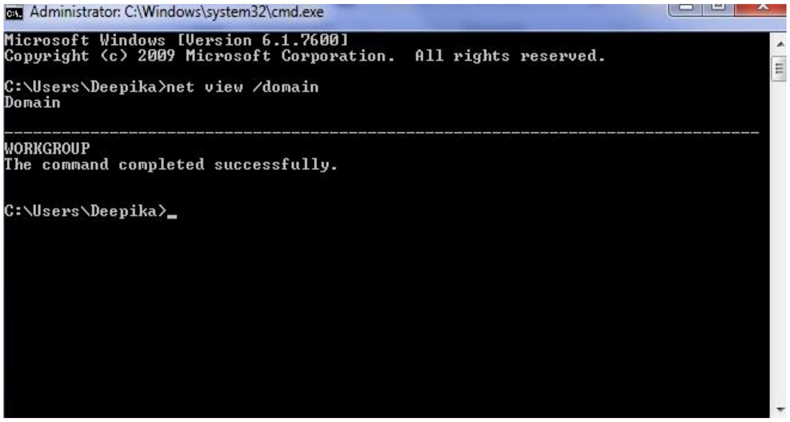
ARP Poisoning is usually attackers target MAC address and they try to change it. Also, ARP spoofing attacks which is effective for both wired and wireless local networks. ARP poisoning attacks includes like gathering the information from the system without authentication, eavesdrop using man in the middle methods. But ARP Poisoning can be detected and blocked. DAI(Dynamic ARP Inspection) which is built by Cisco to handle this type of attacks. DAI validates the ARP packets on the network. Thus this technology protects the network from the attacks includes intercepting, logging and discarding invalid ARP packets.

If the switch does not support the DAI technology there are still other ways to protect the network. Anti-sniffing is one way to detect the sniffers on the network. Tools such as Sniffdet, Sentinel, and Anti-sniff were developed for the Anti-sniffing purpose.

Another defence against the routing enumeration is choosing the improved routing protocols. For example when we can RIP which does not provide authentication as OSPF protocol provides. When we are using OSPF we need to make sure whether we have enabled the routing authentication and doing so enables the password protection on all packets.

**Server Message Block (SMB) and Interprocess Communication:**

SMB makes it possible for users to share files and folders and IPC offers a default share on windows systems. When the concept of SMB was originally created, security was not been implemented. IPC deals with the techniques and mechanisms that facilitate communication between processes. IPC mechanisms can be classified as pipes, FIFO, shared memory, mapped memory, message queues and sockets. The most basic connection possible with IPC is the NULL or anonymous connection. I t achieves this by using basic net command. There's entire host of net commands. For example we can see screen below which shows net command.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Deepika>net view /domain
Domain

-------------------------------------------------------------------------------
WORKGROUP
The command completed successfully.


C:\Users\Deepika>_
```

Figure 12 Starting Net Command

To query any specific domain group, we can just use the net command again in the form of **net view/domain: domain_name**.

## 5.3 Windows Enumeration Tools

Mainly attackers target the administrator account to know what is actually going on the target systems. This can be done using set of tools like USER2SID and SID2USER. The goal of these utilities is to obtain the SID from the account name or the account name from the SID. The guest account will be usually a good target for the USER2SID tool.

SID2USER tool attacks the target device to gather information about the account name of the specific SID. Therefore, SID as given in the previous used tool where there will be change in RID from 501 to 500 because 500 would reveal the true administrator.

DumpSec is a Windows-based GUI enumeration tool that enables to remotely connect to the windows device and dump account details, share permissions, and user information.

DumpSec GUI based tool which is easy to take the results and port them into spreadsheet which provides information about the usernames, SIDs, RIDs, account comments, comment policies, and dial-in information.

A host of tools can be used for enumeration. Some of other tools that perform the same type of enumeration,

**UserInfo** – This is a command line tool which retrieves all the available information about any known user for any windows systems. The *userinfo* command displays user information (for one or multiple users as requested), adds or deletes users, and updates information about the related user. Specifically, by calling *NetUserGetInfo* API call at level 3, UserInfo returns standard info which includes,

- SID and primary group
- Logon restrictions and smart card requirements
- Special group information
- Password expiration information

Some of the other tools that can be used with the Linux OS include,

- RPCDump
- SMB ServerScan
- Smb4k

### 5.3.1 Windows Enumeration Countermeasures

Blocking or reducing the amount of information that can be gathered by enumeration. The controls that we can apply to reduce this type of information leakage include,

- Block ports
- Disable unnecessary services
- Use the Restrict Anonymous setting

Blocking ports starts with 135, 137, 139, 389, and 445. The NETBIOS null session uses specific port numbers on the target device. Null sessions require access to TCP ports. Closing these ports and disabling the SMB services on the individual hosts by unbinding TCP/IP client from the interface on the network.

## 5.4 Advanced Enumeration

Attackers who get well dealing with all these basic steps will typically gain access and control of the system. If attackers have gone through the basic steps of enumeration, they might attempt to use the acquired information to log in the system.

The basic goal of the enumeration is to gather information to gain access. The attacker may attempt to access in the following ways,

- Guessing Usernames and passwords
- Sniffing Password hashes
- Exploiting Vulnerabilities

Guessing the username and password can be done through enumeration that may have returned the router configuration with the password that could be cracked, some user accounts with default or no passwords can be cracked. Tools such as DumpSec are used to find whether the system has lock out policy. All of this information is useful when the attacker attempts to guess username and passwords. Guessing passwords may be limited because of the lock out policy which is set to low value.

### 5.4.1 Password Cracking

When considering the encrypted passwords, the attacker can easily crack the passwords. Password cracking can be divided into two basic categories like encrypted results and pre-computed hashes. If the user uses weak algorithm to encrypt the passwords which makes it easier for attacker to obtain them by using cryptanalysis approaches.

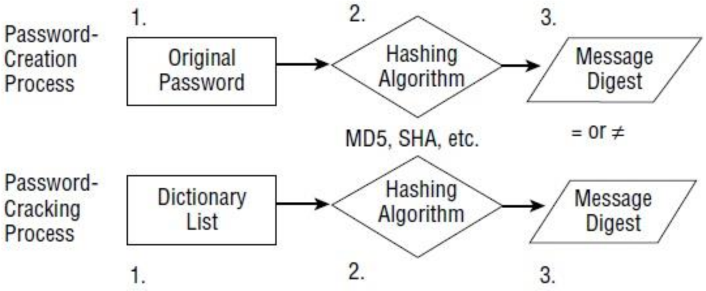


Figure 13 Password Cracking Process

With hash calculation we can use dictionary, hybrid or brute force password cracking. From the figure we can see the password cracking process is actually like comparative process/ Each word in the dictionary is been hashed with the same algorithm and been compared to encrypted value. If the values match the password used to create the hash which would same as that of the original hash.

A hybrid attack also uses a dictionary or word list but it appends and prepends characters or numbers in an attempt to crack the password.  This approach involves various approaches to increase the odds of successfully cracking the password.

Brute-Force attacks use the random numbers and characters to crack the password. A brute-force usually is long time process when cracking encrypted passwords. The rate of success depends on the speed the system. Brute-force audits attempt every combination of letters, numbers and characters.

Some of the password cracking tools includes,

**John the Ripper**- An password-auditing tool that is available for UNIX systems and Windows. It can crack almost common passwords which includes Windows OS hashes. A large number of add-on modules are available for John that can allow to crack open passwords, windows credentials, caches, and MySql passwords.

**L0phtcrack** - An older password-cracking tool and became famous as the premiere Windows password cracking tool. Symantec now owns the rights to this tool, but it continues to be improved. It can extract hashes from the local machine, a remote machine, and can sniff passwords from the local network.

**Cain & Abel-** A multipurpose tool that can perform multiple tasks which includes Windows enumeration, sniffing, and password cracking. The password-cracking part of the program can perform dictionary and brute-force analysis and can use pre-computed hash tables.
**Brutus**— A brute-force password cracker using dictionaries and that supports Telnet, FTP, HTTP, and other protocols.
**cURL**—A set of tools that support multi-protocol transfers of data to or from a server with minimal user involvement. cURL provides proxy support, SSL connection support, cookies, and user authentication.

### Protecting Passwords

We have some strategies to discuss about the password protection before moving to other password attacks. We have certain protection methods like,

- Do not reveal your passwords to others.
- If possible, use stronger authentication mechanisms, such as challenge response, Kerberos, SecureID, and public key encryption.
- Always log out of a session during which you used your password in a public computer or kiosk.
- Avoid using software that recalls your passwords and automatically fills them in for you.
- Be aware of personal, email, and telephone social engineering attacks attempting to get you to reveal your passwords.
- Do not write passwords on notepads and leave them in the vicinity of your computer.
- Use encryption programs to protect passwords stored on your computer.

## 5.4.2 Sniffing Password Hashes

Sniffing passwords is another way for the attackers to gain access. When considering a network with large amount of traffic congestion and a significant portion might not be encrypted. Even it is encrypted; the algorithm used for this type of encryption will be weak or vulnerable. Sniffing password and hashes on the network requires the attacker to have some type of access. If the attacker can gain access till this on the network, then he can gain the access to sniff required credentials on the network.

ScoopLM and BeatLM are two tool which were used to gain access to sniff the passwords. These products mainly targets to sniff the Windows authentication traffic.  Now the traffic is being captured and detected and now we can use ScoopLM built in dictionary or brute-force cracker for sniffing passwords. BeatLM shows the list of authentication attempts made. If the authentication is failed it is been indicated as NG and if the attempt is successful it displays OK which shows that the captured hash is valid. This valid hash is ready to dictionary or brute-force attack. Certain tools are being used to capture and crack Kerberos authentication.

Kerberos protocol was developed to provide secure means of mutual authentication between client and server. Single sign-on (SSO) was implemented with the organization which was offered by this protocol. KerbCrack is a tool that can be used to attack Kerberos. It consists of two separate programs. The first portion is a sniffer that listens on port 88 for Kerberos logins; the second portion is used as a cracking program to launch a dictionary or brute-force attack on the password.

### 5.4.3 Exploiting Vulnerabilities

Vulnerabilities are typically reported as Common Vulnerabilities and Exposures (CVEs). CVEs are weaknesses or holes in the computers and other equipment that can be exploited by hackers. When a CVE is reported, it is catalogued and named by MITRE Corporation.

Let's look at how the vulnerability process might be used by the attacker.

- The attacker enumerates a system to find the services and versions are running. For this example, let's suppose the attacker identifies the system as Red Hat Linux 6.1.
- The attacker surfs the web for vulnerabilities for Red Hat Linux 6.1. There are reported vulnerabilities for race conditions and the programmable authentication module (PAM). With several vulnerabilities discovered, the attacker now searches the web for exploit code.
- The attacker downloads the code and launches it against the vulnerable target. If it is successful, the attacker has now gained access. If it is unsuccessful, the attacker renews his search and tries another exploit.
- When the attacker exploits the vulnerability, he has most likely gained some level of access to the computer system. If the attacker has been able to gain access to a Windows system as a standard user, the next step is escalation of privilege. Whether this is necessary depends on the level of access provided by exploitation of the vulnerability. If the vulnerable service is already operating with privileged access, escalation is not needed.

Other ways that attackers gain access by means of exploit code include the following:

- Trying to make users executing the malicious program. Email is a common attack vector. Copying it to the system and scheduling it to run at a predetermined time; for example, with the AT command.
- Exploiting interactive access to the system; for example, with Terminal Server, PC Anywhere, or the like. It's important to realize that the exploit code used to gain access is limited by type and version of software.

Enumeration is a critical step for the attacker as he is attempting to identify the services, protocols, and applications that are being used. Security professionals should enumerate their own networks to see what type of information is available. Just consider the fact that no attack occurs in a void. If the attacker wants to attack the network, he/she must first know what services, protocols, and applications are available.

## 5.5 Examples

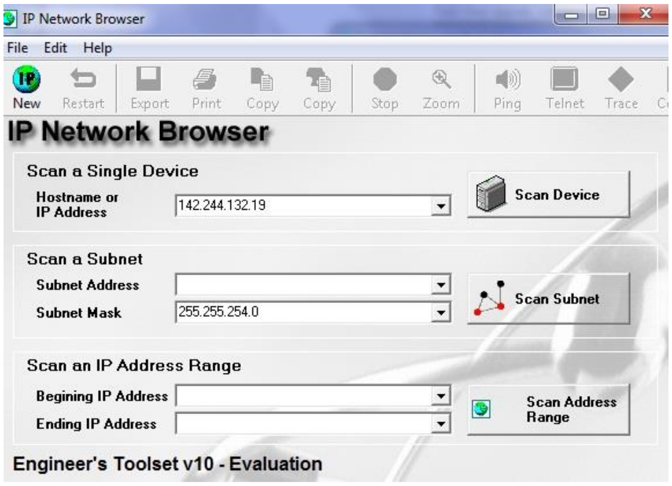
Best tools used for specific scenarios as described above,

**SNMP Enumeration**

The SolarWinds IP Network Browser to display information gathered from active SNMP devices:

1. We need to install the SolarWinds IP Network Browser on windows OS.
2. Next we need to start SNMP on a Windows by changing settings of windows component tools.
3. Once SNMP is installed, install the SolarWinds network management tools. After the installation has completed, start the IP network browser.
4. Now we need to enter the IP address and subnet mask as shown,

5. Note that default strings are Public and private that have been already entered. Now we need just start scan,


IP Network Browser
File Edit Help
New Restart Export Print Copy Copy Stop Zoom Ping Telnet Trace C
IP Network Browser
Scan Device
Scan Subnet
Scan Address Range
Engineer's Toolset v10 - Evaluation

Scan a Single Device

Hostname or IP Address: 142.244.132.19

Scan a Subnet

Subnet Address:

Subnet Mask: 255.255.254.0

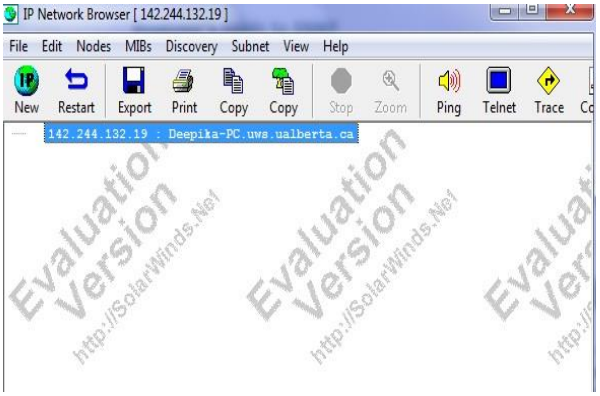
Scan an IP Address Range

Begining IP Address:

Ending IP Address:

Figure 14 Solar Winds IP Network browser

6. When scanning starts it gather the information of the target network. These information are visible only if the Windows restrict Anonymous settings have been put in place.

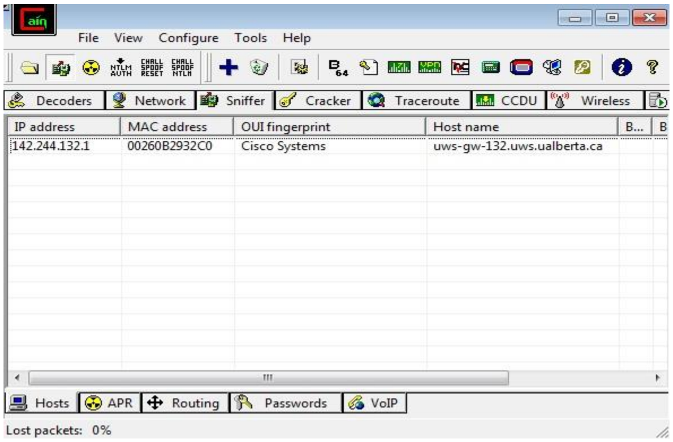

IP Network Browser [ 142.244.132.19 ]
File Edit Nodes MIBs Discovery Subnet View Help
New Restart Export Print Copy Copy Stop Zoom Ping Telnet Trace Co
Evaluation Version http://SolarWinds.Net

142.244.132.19 : Deepika-PC.uws.ualberta.ca

7. If SNMP is enable we can the information about the system.

## Enumerating Routing Protocols

1. Download and Install Cain & Abel.
2. Start Cain and Abel and choose the sniffer tab.



| IP address | MAC address | OUI fingerprint | Host name | B... | B |
|---|---|---|---|---|---|
| 142.244.132.1 | 00260B2932C0 | Cisco Systems | uws-gw-132.uws.ualberta.ca | | |

Lost packets: 0%

Figure 15 Cain and Abel

3. While on the Sniffer tab, start the capture by clicking the Start/Stop Sniffer button. Make sure that you are on the routing tab that is displayed at the bottom of the page. Routing updates can take several minutes to occur, so a brief delay might occur while the program captures the information.
4. Click on routing tab to update information about the routers.

## 6.0 Understanding Cryptographic tools

One of the most important scenarios in real time environment is cryptographic systems and process that deals with the encryption in one form or another. For instance, Using debit cards at ABM or at other places where we need to enter the passwords, here the encryption involves.

For anyone working with security should know basics of cryptographic systems which include symmetric encryption, asymmetric encryption, and public key infrastructure (PKI). Understanding the cryptographic systems helps the security professionals to identify and authenticate systems. Authentication can be based on the passwords, tokens and biometrics. Understanding cryptographic systems will also help in password-cracking.

### 6.1 Encryption

Encryption concept was developed to maintain secret keys and passwords. Encryption can be different forms like secret key or symmetric encryption. It’s effective but requires a common shared key. Common shared key can be a problem because key must not be disclosed to a third party; otherwise, confidentiality cannot be ensured. Asymmetric encryption overcomes some of the problems associated with symmetric encryption but comes with its own drawbacks. But this is much slower than symmetric encryption. Hashing is one-way of cryptographic process. The study of cryptology comprises cryptography and cryptanalysis.

### 6.1.1 Secret Key Encryption

Symmetric Encryption is a technology where we use single secret key for both encryption and decryption. When providing a secret key with a combination of numbers, it is always hard to remember the numbers. So encryption offers a solution for this by keeping the message which is exposed in clear text. This can be done by using an algorithm and in addition to it a cryptographic key. The overall process may not be the straight forward nowadays but it still process is same.

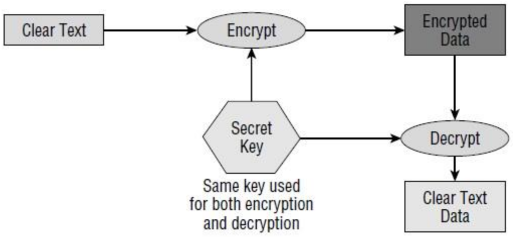


Figure 16 Symmetric Encryption

For symmetric encryption there are two dual-use keys which mean same keys can be used to lock and unlock data. Symmetric encryption provides confidentiality because only the people who know the keys know the true contents of message. This requires a secure key exchange which is the disadvantage of Symmetric encryption. Exchange of secret key from one person to other is really hard in this type of encryption.

Symmetric encryption suffers from scalability issues because the communication between users for secret key is difficult. But still it has some good features like fast and very hard to break if large key is used. Some of the symmetric algorithms include,

AES - Advanced Encryption Standard is a symmetric key encryption comprises of block ciphers like AES-128, AES-192, and AES-256. AES ciphers are analyzed extensively and used worldwide.[7]

Blowfish – This is a general purpose symmetric algorithm for the replacement of Data Encryption Standard (DES) algorithm.

DES- Data Encryption Standard one of the most common symmetric algorithms used.

IDEA- International Data Encryption Algorithm is a block cipher that uses 128 bit key to encrypt 64-bit blocks of plain text. It is used by PGP (Pretty Good Privacy).

RC4 - Rivest Cipher 4 is a stream based Cipher. Stream Ciphers treat data as a stream of bits.

RC5 - Rivest Cipher 5 is a block- based cipher where RC5 processes data in blocks.

Rijndael- This is a block cipher as adopted by AES.

[7] Advanced Encryption Standard from Wikipedia

SAFER – Secure and Fast Encryption Routine is a block- based cipher that processes data in blocks of 64 and 128 bits.

When these algorithms are applied in real time lab environment, they are really interesting and exciting and can be applied as security solutions.

### 6.1.2 Data Encryption Standard

DES is a symmetric encryption Standard which is based on 64 bit block. DES processes 64 bits of plain text at a time which results 64 bit blocks of cipher text. DES uses 56 bit and has four common modes of operation,

Electronic Codebook (ECB)

Cipher Block Chaining (CBC)

Cipher Feedback (CFB)

Output Feedback (OFB)

These four modes uses 56 bit key but actually the specified standard is 64 bits, but 8 bits are parity bits. Thus we used practically we can use only 56 bits long. The plaintext is processed by the key through 16 rounds of transpositions and substitutions.

**Electronic Codebook Mode**

ECB is the native encryption mode of DES. This is given priority of highest standard but it is also easy to break because when large amounts of data are processed using same key encryption will produce the same cipher text. Thus this type of encryption is used only small amounts of data like PIN's and in ATM.

**Cipher Block Chaining Mode**

This standard is similar to ECB. CBC process 64 bits of data but takes some of the Cipher text created from the precious block and inserts into next one. This is called XORing. This makes the cipher text more secure and cannot be cracked easily.

**Cipher Feedback Mode**

CFB is a stream Cipher which is used in encryption of individual characters which is similar to OFB. Cipher text is processed together here; errors and corruption can propagate through the encryption process.

**Output Feedback Mode**

OFB is also a Stream Cipher. Unlike CFB, OFB uses plain text to feedback into stream of cipher text. Errors and corruption do not propagate in this mode.

### 6.1.3 Triple DES

For better usage of DES encryption standard, triple DES was designed. First, developing double DES may have problems like man in the middle attack, so triple DES was developed. 3DES uses two or more keys to encrypt data. Although it is more secure, it is slower than the 56 bit DES. Triple DES can be implemented in different ways,

DES EEE2- This uses two keys. The first key is reused during the third round of encryption. The encryption process is performed three times (encrypt, encrypt, encrypt).

DES EDE2- This uses two keys. Again, the first key is reused during the third round of encryption. Unlike DES EEE2, DES EDE2 encrypts, decrypts, and then encrypts.

DES EEE3- This uses three keys and performs the encryption three times.

DES EDE3- This uses three keys but operates by encrypting, decrypting, and then encrypting, decrypting and then encrypting the data.

### 6.1.4 Advanced Encryption Standard

Rijndael was developed for the replacement of DES which serves as Advanced Encryption Standard. Rijndael is a block cipher that supports variable key and block lengths of 128, 192, or 256 bits and it is also very secure. Even if attackers use distributed computing AES should be resistant for many years. Thus, it is symmetric algorithm in case of high security.

### 6.1.5 One-Way Functions (Hashes)

Hashes are unique in the way they are one-way. It’s nearly impossible to derive the original text from the hash string. It is easy to compute in one direction yet hard to reverse. Actually not all hashes are considered of the same strength. Both MD4 and MD5 hash algorithms are weak because hash collisions have been demonstrated for both algorithms, which effectively break the usage in cryptographic community.

**MD Series**

MD series started with MD2 which was optimized for 8-bit computers and has been found to suffer from collisions. MD4 was developed for processing a message 512 bit blocks and 64 bit binary representation of original length of the message is added to the message. But with MD2 and MD4 it was found that it was so vulnerable to attacks. So MD5 came into development which processes variable size imput and produces a fixed 128 bit output. But with MD4, it processes the data in blocks off 512 bit. So MD5 has also been broken.

**SHA**
SHA, SHA-1 and SHA-2 are a family of secure hashing algorithms that are similar to MD5. SHA provides with a 160 bit message digest. SHA-1 processes messages in 512 bit blocks and adds padding, if needed to get the data with right number of bits. SHA-1 has only 111 bit effectiveness. SHA-0 is not more secure and it is easily vulnerable to attacks. A safe replacement for SHA-0 was SHA-2 family which includes SHA-256 and SHA-512.

## 6.2 Public Key Encryption

Public Key Encryption is a type of cryptography also known as asymmetric cryptography. As in symmetric encryption, here also we use two unique keys where one key to encrypt the data and other key to decrypt the data. Most specific feature implemented in Asymmetric Encryption to overcome symmetric encryption is key distribution.

**How Asymmetric Encryption does works?**

We want to send a message to client, we use client's public key to encrypt the message. When the client receives the message, he uses his private key to decrypt it. So the message is encrypted with public key and decrypted with the matching private key. The private keys are usually kept secret whereas public key can be given to anyone.

Public key cryptography is made possible for one-way functions. A one-way function is nothing but math operation that is easy to compute the one direction but impossible to compute the other. Math operations like logarithm problem or factoring large number into the prime numbers are been computed.

One way function or trap door allows someone with the public key to reconstruct the private key if he knows the trap-door can perform the function easily in both directions, but anyone lacking the trap door can perform the function only in one direction. The forward direction is used for decryption and inverse and backward direction is used for decryption and signature generation.

**RSA**

RSA was similar to symmetric encryption standards but it much slower. It offers a secret key exchange and is very secure. RSA uses prime numbers whose product is much larger than that of 129 digits for security as 129 decimal numbers have been factored using a number field sieve algorithm.

Cryptanalysis or anyone attempting to crack RSA would be left with a difficult challenge because of the difficulty of factoring of large integer into two factors. Cracking requires large distribution of computers and processing power and time.

**Diffie-Hellman**

Diffie-Hellman was one of the first public key exchange algorithm and was developed for key exchange, not for data encryption of digital signatures. The Diffie-Hellman protocol allows two users to exchange a secret key over an unsecure medium.

Diffie-Hellman is vulnerable to man-in-the-middle attacks because the key exchange does not authenticate the participants. To avoid these vulnerabilities we need to use digital signatures. So Diffie-Hellman is usually been used as medium for several authentication methods which includes even Internet Key Exchange.

**EI Gamal**

EI Gamal is an extension to Diffie-Hellman key exchange. This is usually used for key exchanges, Digital signatures and encryption. This is being done by three discrete components: a key generator, an encrypted algorithm and decryption algorithm.

## 6.3 Authentication

Authentication is the act of proving an identity, whereas identification is the process of distinguishing yourself specifically. Identification is usually performed by entering the username and authentication can be done in several ways by, Passwords, Tokens, smart cards and certificates, Biometrics.

The most common authentication is been accomplished by means of passwords. This can be done by some form of encryption or hashing process. In FTP the passwords are sent as clear text. Authentication can also be done challenge-response mechanism. Other ways of authentication include public key infrastructure (PKI), tokens, and biometrics.

### 6.3.1 Password Authentication

Passwords are the simplest form of authentication which are been used over centuries. Technically, passwords are secret keys and to say there are three types of authentication which are been most widely used. Password authentication fails because users should control of the password and if the password is weak, simple, and easy to guess; or the authentication system need to be designed securely so that passwords are being protected.

For password based authentication to be effective, passwords cannot be shared with others or it cannot be written and stored. This shows the real problem because people cannot remember complex passwords.

**Password Hashing**

To prevent hackers from capturing your password from your computer's hard disk, most passwords are not stored in plain text. Password hashing can be done using lot of hashing algorithms like Secure

Hashing Algorithm (SHA-1) but it seems much weaker algorithms to be used. Thus for certain purposes like digital signatures, stronger algorithms like SHA-256, SHA-512 are being used. A hash is nothing but a digital fingerprint of a piece of data. We can do fixed length hashing using one way mathematical process. It is also unlikely that any different text string will give you an identical hash – "Hash Collision".

These hash properties are ideally used for the application passwords. So for the attackers they can retrieve only hash passwords but the original passwords cannot be revealed. There are number of strong hashing algorithms like AD5 and SHA-1. But these hashing algorithms are accepted only with 56 bits.

Techniques which can be used to retrieve original text from the hashes are Cracking or "Brute forcing". Using this methodology attacker can easily generate hashes for potential passwords and try to match them with the hashes that are stored in the database.

Most of the computer hardware easily can generate MD5 and SHA-1 hashes very quickly. Thus strong passwords and long pass phrases should be used.

### Challenge – Response

Password hashes works well on computer system but while providing authentication over a large network it is not possible. If password hash is used, the attacker can intercept the hash, it becomes trivial to simply replay it again to gain access. Challenge-response authentication can be used to encrypt the hashed password using secret key encryption.

A challenge-response authentication can be processed as,

Client computer requests for connection to server

Server sends a secret value to the client

Client encrypts the secret value using a hashed password and transmits result to the server.

Server decrypts the secret using the stored hashed password and compares it to the original secret value to decide whether to accept the logon.

This authentication can be either synchronous or asynchronous authentication based on time and is not synchronized to an authentication server. This authentication works as follows,

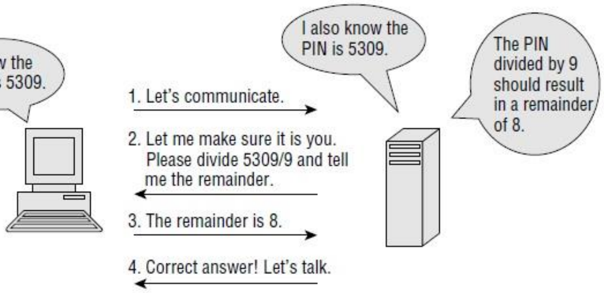

I know the PIN is 5309.
I also know the PIN is 5309.
The PIN divided by 9 should result in a remainder of 8.
1. Let's communicate.
2. Let me make sure it is you. Please divide 5309/9 and tell me the remainder.
3. The remainder is 8.
4. Correct answer! Let's talk.

Figure 17 Challenge-Response Authentication

Synchronous systems are synchronized to authentication server. This means each time client authenticate itself by using pass code or authentication which is valid for only short period of time. RSA's SecureID is an example for synchronous systems where it changes it password for every 60 seconds. Asynchronous and synchronous systems work because hashed password is never transmitted only a random number is been transmitted every time.

### 6.3.2 Session Authentication

Session Authentication is similar to challenge-response authentication which validates users and creates a session value that represents the authentication. This type of authentication is widely being used on web applications. Instead of passing actual username and passwords, session authentication passes either cookies or query strings to the server. Session authentication ensures that after authentication has occurred; all subsequent communications can be trusted.

### 6.3.3 Public Key Authentication

Public Key Authentication is a method of using public keys to authenticate users. This form of authentication can be seen in services such as Secure Socket Layer (SSL), Transport Layer Security (TLS), Pretty Good Privacy (PGP), and Public Key Infrastructure (PKI)

**Public Key Infrastructure**

PKI has solved many issues that occur when dealing with unknown parties on the internet. When dealing certain businesses we can see the store, talk to employees and get a good look at how they do business. Internet transactions are much less transparent. We can't see who is dealing with whom, what type of operation they run, and we cannot trust them.

PKI is nothing but a framework of hardware, software, and policies that exist to manage, create, store and distribute keys and digital certificates. The components of this framework include the following,

- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Revocation List (CRL)

- Digital Certificates
- Certificate distribution system

### 6.3.4 Biometrics

Biometric Authentication uses sensors to detect patterns that uniquely identify persons such as facial features, fingerprints, and hand prints and so on. Thus, biometrics is nothing by authentication that is based on behavioural or physiological characteristics that is unique to each individual.

In many organizations, they take the employee finger print for authentication purpose, and store it in the database. This can be done using biometric palm scanner, it is used for comparing the ridges and creases found on employee's palm to the one that is identified about the individual in the database. This comparison helps to find whether information has access or not.

Determination of employee's granted access depends on the Accuracy of the biometric system. Different systems have different levels of accuracy. The accuracy can be measured by the TYPE I errors and TYPE II errors. TYPE I errors are percentage of people getting access even though they are not in the system. TYPE II errors are people who can get through in but will not be allowed.

There are many different types of biometric systems,

Palm Scan- This is done by analyzing the ridges and creases of an individual's palm and storing it in the database and comparing it for match if required.

Hand Geometry- This system gets the unique geometry of person's hand and fingers to determine the identity.

Iris recognition- This is very accurate as it has over 400 points of reference. It matches the person's blood vessels on the back of the eye.

Retina Pattern- This requires to place the person's eye near the reader to identify the person's eye.

Fingerprint- This is widely used in many facilities and also on items like laptops which identify the details about the peaks, valleys and ridges of fingers.

Facial Scan- Requires the user to place his or her face about 2 feet to from the camera and uses mathematical comparison with the face prints it holds in a database to allow block access.

Voice Recognition- This can done by voice analysis for identification and authentication.

## 6.4 Encryption and Authentication Attacks

As long as a secret password exists they always people trying to break it. The cracking of cryptographic codes can be done using frequency analysis. Frequency analysis is a study of how frequently letters or groups of letters appear in cipher text. There are several ways of authentication attacks done to the system.

### Extracting Passwords

Attackers can extract passwords to gain access in several different ways,

- Gain physical access
- Use keystroke logger
- Gain logical access
- Guess a Weak password

If the attacker gains the physical access to targeted systems, he can reset passwords of the OS by using several tools. Keystroke loggers are the software or hardware devices used to monitor activity. While the outsider might have some trouble getting one of these devices installed. Hardware keystroke loggers are usually installed while users are away from their desks and they are undetectable for their physical presence.

Passwords can be attacked electronically over the network by gaining remote access and using some tools like pwdump to extract details from SAM. Considering weak passwords, if they are easy to guess that make attackers to easily gain access to targeted systems.

### Password Cracking

Password cracking as discussed earlier it can be done using three methods say dictionary attacks and brute force attacks or a rainbow table.

Dictionary attack uses a predefined dictionary to look for a match between encrypted password and encrypted dictionary word. Many times these attacks can be done in few minutes because individuals tend to use easily remember passwords. If the passwords are well known, dictionary based words, dictionary tools can easily crack them.

Brute force attack is a type of encrypted passwords which takes years to crack them depending on the complexity of the password.

Rainbow Table is a new approach for cracking passwords. This Rainbow crack technique works by pre-computing all possible passwords in advance. Once this process is done the passwords and their corresponding encrypted values are stored in a file that is called Rainbow table. An encrypted password can be quickly compared with the vales stored in the table and can be cracked in few seconds. Orphcrack is an example of this type of program. The disadvantage of rainbow table, it needs to store large amount of data.

Some of the common cryptographic attacks are Cipher test-only attack, Man-in-the-middle attack; Chosen cipher text, Chosen plaintext, Replay attack.

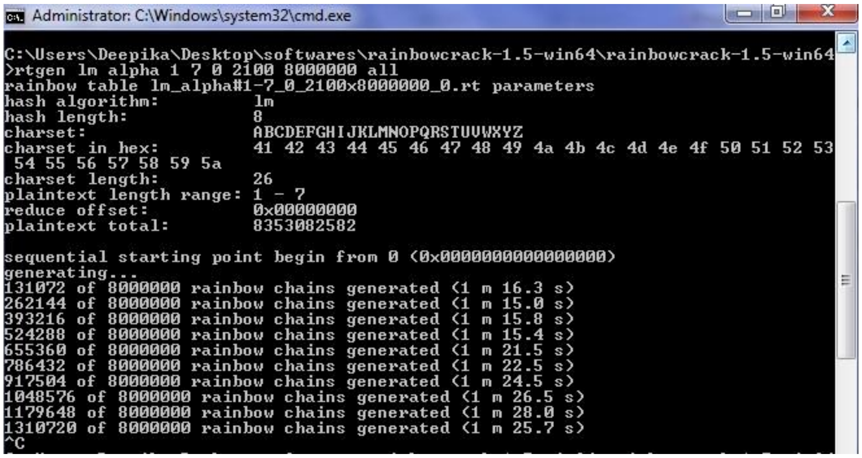
## 6.5 Examples

Best tools used for specific scenarios as described above,

### Rainbow Crack

This tool helps to process of generating a small rainbow table and verifying its operation,

1. Download and install rainbow crack. Open a command prompt and issue the following command as shown in the figure. When the command is completed,



```
C:\Users\Deepika\Desktop\softwares\rainbowcrack-1.5-win64\rainbowcrack-1.5-win64
>rtgen lm alpha 1 7 0 2100 8000000 all
rainbow table lm_alpha#1-7_0_2100x8000000_0.rt parameters
hash algorithm:         lm
hash length:            8
charset:                ABCDEFGHIJKLMNOPQRSTUVWXYZ
charset in hex:         41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53
 54 55 56 57 58 59 5a
charset length:         26
plaintext length range: 1 - 7
reduce offset:          0x00000000
plaintext total:        8353082582

sequential starting point begin from 0 (0x0000000000000000)
generating...
131072 of 8000000 rainbow chains generated (1 m 16.3 s)
262144 of 8000000 rainbow chains generated (1 m 15.0 s)
393216 of 8000000 rainbow chains generated (1 m 15.8 s)
524288 of 8000000 rainbow chains generated (1 m 15.4 s)
655360 of 8000000 rainbow chains generated (1 m 21.5 s)
786432 of 8000000 rainbow chains generated (1 m 22.5 s)
917504 of 8000000 rainbow chains generated (1 m 24.5 s)
1048576 of 8000000 rainbow chains generated (1 m 26.5 s)
1179648 of 8000000 rainbow chains generated (1 m 28.0 s)
1310720 of 8000000 rainbow chains generated (1 m 25.7 s)
^C
```

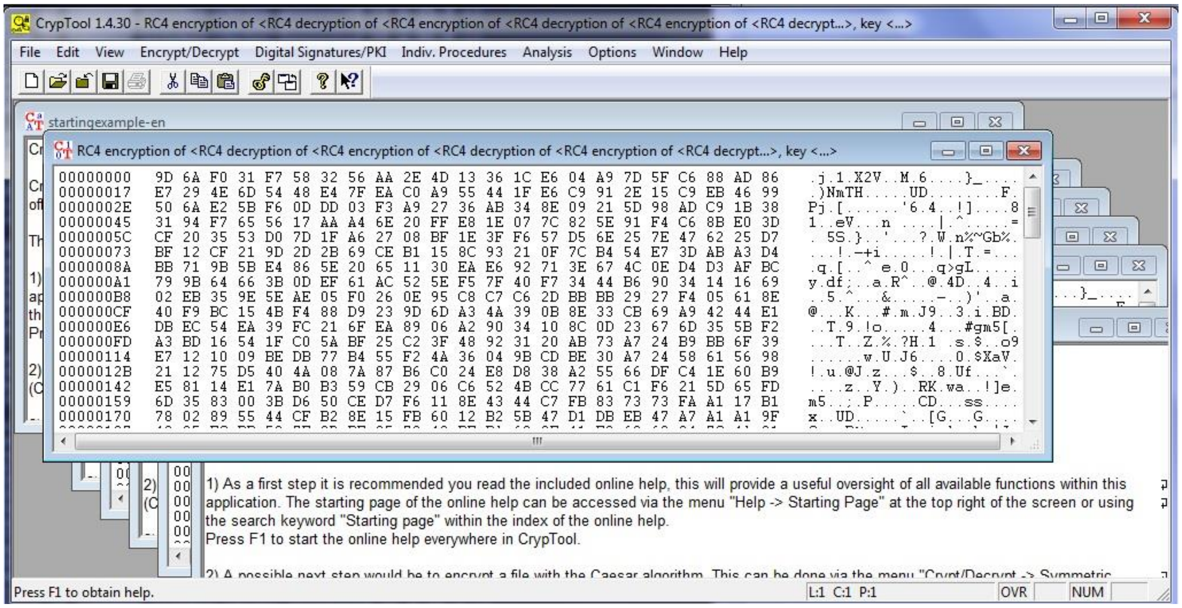
Figure 18 Rainbow Crack Tool

2. When the tables are complete we may need to sort the files by using the following command,
3. Now add some users and passwords to the local computer and should be not more than 7 characters.
4. Now download Pwdump3 and run it against the local SAM by issuing the following command,
5. Now execute rainbow crack with the following parameters,

   Now we can see the passwords given as the program can quickly crack the passwords.

### Cryp Tool

1. Download and install Cryptool and accept all defaults as given in the tool.
2. From the menu, choose crypt/decrypt and select symmetric (modern)-> RC4. Choose 8-bit brute force encrypt, and it is shown as below

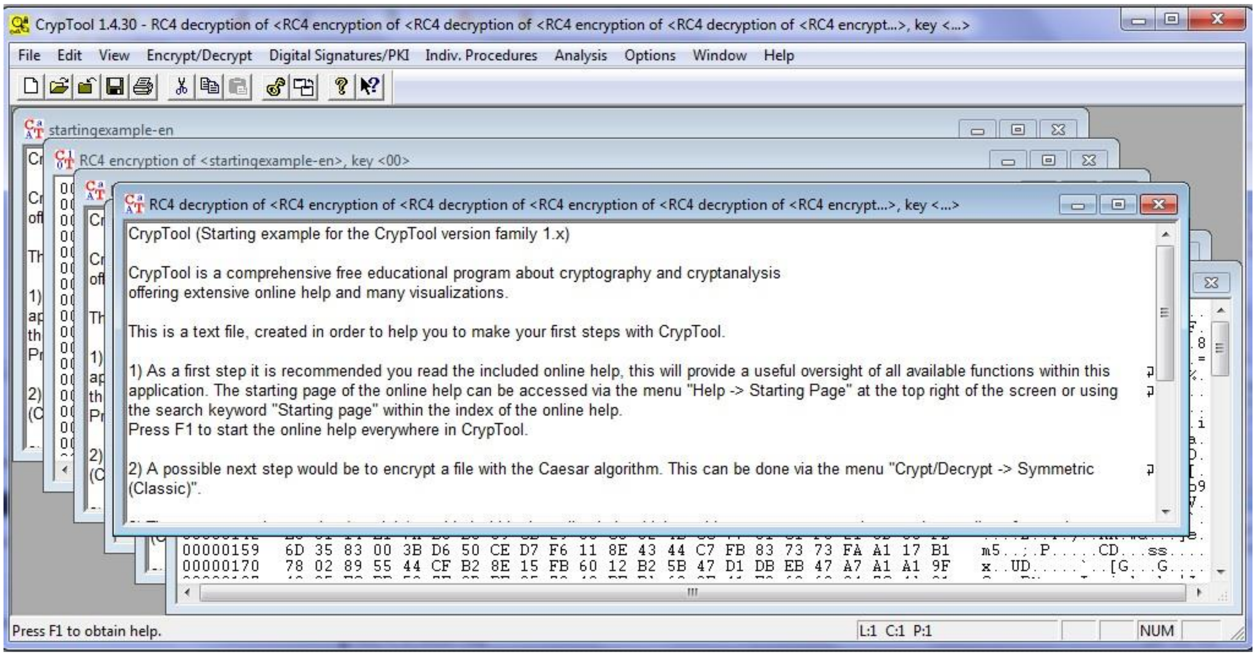

CrypTool 1.4.30 - RC4 encryption of <RC4 decryption of <RC4 encryption of <RC4 decryption of <RC4 encryption of <RC4 decrypt...>, key <...>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
startingexample-en
RC4 encryption of <RC4 decryption of <RC4 encryption of <RC4 decryption of <RC4 encryption of <RC4 decrypt...>, key <...>

```
00000000  9D 6A F0 31 F7 58 32 56 AA 2E 4D 13 36 1C E6 04 A9 7D 5F C6 88 AD 86   .j.1.X2V..M.6....}_....
00000017  E7 29 4E 6D 54 48 E4 7F EA C0 A9 55 44 1F E6 C9 91 2E 15 C9 EB 46 99   .)NmTH.....UD........F.
0000002E  50 6A E2 5B F6 0D DD 03 F3 A9 27 36 AB 34 8E 09 21 5D 98 AD C9 1B 38   Pj.[......'6.4..!]....8
00000045  31 94 F7 65 56 17 AA A4 6E 20 FF E8 1E 07 7C 82 5E 91 F4 C6 8B E0 3D   1..eV...n ....|.^.....=
0000005C  CF 20 35 53 D0 7D 1F A6 27 08 BF 1E 3F F6 57 D5 6E 25 7E 47 62 25 D7   . 5S.}..'...?.W.n%~Gb%.
00000073  BF 12 CF 21 9D 2D 2B 69 CE B1 15 8C 93 21 0F 7C B4 54 E7 3D AB A3 D4   ...!.-+i.....!.|.T.=...
0000008A  BB 71 9B 5B E4 86 5E 20 65 11 30 EA E6 92 71 3E 67 4C 0E D4 D3 AF BC   .q.[..^ e.0...q>gL.....
000000A1  79 9B 64 66 3B 0D EF 61 AC 52 5E F5 7F 40 F7 34 44 B6 90 34 14 16 69   y.df;..a.R^..@.4D..4..i
000000B8  02 EB 35 9E 5E AE 05 F0 26 0E 95 C8 C7 C6 2D BB BB 29 27 F4 05 61 8E   ..5.^...&.....-..)'..a.
000000CF  40 F9 BC 15 4B F4 88 D9 23 9D 6D A3 4A 39 0B 8E 33 CB 69 A9 42 44 E1   @...K...#.m.J9..3.i.BD.
000000E6  DB EC 54 EA 39 FC 21 6F EA 89 06 A2 90 34 10 8C 0D 23 67 6D 35 5B F2   ..T.9.!o.....4...#gm5[.
000000FD  A3 BD 16 54 1F C0 5A BF 25 C2 3F 48 92 31 20 AB 73 A7 24 B9 BB 6F 39   ...T..Z.%.?H.1 .s.$..o9
00000114  E7 12 10 09 BE DB 77 B4 55 F2 4A 36 04 9B CD BE 30 A7 24 58 61 56 98   ......w.U.J6....0.$XaV.
0000012B  21 12 75 D5 40 4A 08 7A 87 B6 C0 24 E8 D8 38 A2 55 66 DF C4 1E 60 B9   !.u.@J.z...$..8.Uf...`.
00000142  E5 81 14 E1 7A B0 B3 59 CB 29 06 C6 52 4B CC 77 61 C1 F6 21 5D 65 FD   ....z..Y.)..RK.wa..!]e.
00000159  6D 35 83 00 3B D6 50 CE D7 F6 11 8E 43 44 C7 FB 83 73 73 FA A1 17 B1   m5..;.P.....CD...ss....
00000170  78 02 89 55 44 CF B2 8E 15 FB 60 12 B2 5B 47 D1 DB EB 47 A7 A1 A1 9F   x..UD.....`..[G...G....
```

1) As a first step it is recommended you read the included online help, this will provide a useful oversight of all available functions within this application. The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the screen or using the search keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CrypTool.

Figure 19 CrypTool Encryption

3. From the menu, choose crypt/decrypt and select symmetric (modern)-> RC4. Choose 8-bit brute force decrypt, and it is shown as
   below


CrypTool 1.4.30 - RC4 decryption of <RC4 encryption of <RC4 decryption of <RC4 encryption of <RC4 decryption of <RC4 encrypt...>, key <...>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
startingexample-en
RC4 encryption of <startingexample-en>, key <00>
RC4 decryption of <RC4 encryption of <RC4 decryption of <RC4 encryption of <RC4 decryption of <RC4 encrypt...>, key <...>

CrypTool (Starting example for the CrypTool version family 1.x)

CrypTool is a comprehensive free educational program about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This is a text file, created in order to help you to make your first steps with CrypTool.

1) As a first step it is recommended you read the included online help, this will provide a useful oversight of all available functions within this application. The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the screen or using the search keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CrypTool.

2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)".

```
00000159  6D 35 83 00 3B D6 50 CE D7 F6 11 8E 43 44 C7 FB 83 73 73 FA A1 17 B1   m5..;.P.....CD...ss....
00000170  78 02 89 55 44 CF B2 8E 15 FB 60 12 B2 5B 47 D1 DB EB 47 A7 A1 A1 9F   x..UD.....`..[G...G....
```

Figure 20 CrypTool Decryption

4. Now we can repeat the encryption for 16-bit and 32-bit encryption and decryption.

## 7.0 Defeating Malware

Malware is short term for malicious software which includes virus and spyware to steal personal information, send spam and commit fraud. Malware is a kind of programming which helps attackers to gather information that causes loss of privacy or exploitation; he can easily gain access to the targeted system resources.

Malware is not same as the defective software that is, it is software that contains bugs. Malware has been changing constantly as it was in early days. Thus other malicious codes like Rootkits, spyware, and phishing will also be analysed. Now are we are going to look at the methods which detects, eradicates and prevents such treats in the system.

### 7.1 Viruses and Worms

Viruses and Worms plays great role in large category of malicious code, or malware. Viruses and worms are nothing but programs which causes damage from displaying messages to make programs work erratically and even destroying the hardware. When these kinds of programs are executed they infect more programs and they replicate again and again.

In this internet era, viruses spread easily on the personal computers by infecting the executable disks. This happens by inserting a copy of it into machine code instructions into executable codes, these viruses cause to run whenever the disk is booted. These can be easily spread by exchanging bootable disks.  Unlike virus, these worms did not insert themselves into other programs. Instead it exploited security holes in the network server programs and starts running itself as a separate process. Today worms are mainly written on Windows OS, but still few worms like Mare-D and Lion Worm are also written on Linux and Unix Systems.

With the rise of Windows application, the macros of its application became possible to write infectious macro codes in MS word and similar applications. The macro viruses infect document and templates rather than application itself.

After a computer has been infected, the computer virus can do number of things and some viruses causes fast infection. This fast infection viruses can cause infection to any type of file while others limit the rate of infection. This type of infection is called Sparse Infection. This means virus takes time for spreading to other files and spreading its damage. Some other viruses which load themselves into RAM which is called RAM resident which is only way to spread boot sector viruses.

As the development of anti viruses to detect the viruses and virus writers also tried developing viruses which are hard to detect. One such technique developed was multipartie virus. And other technique developed was virus polymorphic that can change their signature every time they replicate and infect a new file. The three main components of polymorphic virus are virus body, decryption routine, and a mutation engine.

Stealth viruses are other kind of viruses that attempts to hide their presence from both OS and even the antivirus software by doing the following,

- Hiding the change in the file's date and time
- Hiding the infected file's size by increasing it
- Encrypting themselves

**Worms**

Worms are unlike virus which can self-replicate. True worm are hard to create and they do not attach a host file but are self-contained and propagate across the networks automatically. It always targets on the aspects of send mail, finger, and weak passwords. A very common payload for worms is to install a backdoor in the infected computer to create Zombie computer by getting computer control under worm author. Networks of such machines are often referred to as botnets and are very commonly used by spam senders for sending junk mail or to cloak their website's address.

Worms are spread exploiting vulnerabilities in operating system. If vendors have security problems they always supply with regular security updates. If these are installed on the system major worm will be unable to spread. If a vulnerability is disclosed before the security patch released by vendor , a zero day attack is possible.

A zero-day attack is nothing but a computer threat that tries to exploit computer application vulnerabilities that are unknown to others that is also called zero-day vulnerabilities. Zero-day exploits are used or shared by attackers before the developer of the target software knows about the vulnerability[8].

Users should not open the mails which are unexpected and should not run the attached files or programs or visit websites that are linked to such emails. As with the ILOVEYOU worm and it was increasing growth and efficiency of phishing attacks, it remains tricking the end user running into malicious code.

Anti-virus and Antispyware can be used for preventing these attacks and should be updating the security related software.

### 7.1.1 Detecting and Preventing

Prevention is always better, so before running programs and executable files it should be always checked. This can be done by using required antivirus and antispyware installed on the system and should need an update often. We should check and should not open if they are unexpected mails and attachments in the mail. We should keep the system patched so that many virus and worms exploit vulnerabilities that have been previously found

Although we prevent our system from virus defects, the only way to protect your data from viruses is to maintain copies of data. We should always make sure the system backups. Many tools are available to help with this task, and high external hard disks can be used.

[8] From http://en.wikipedia.org/wiki/Zero-day_attack

## 7.2 Trojans

Trojans are malicious programs to accomplish its goals like it must be able to run without shutting down, or deleted by the user of the system on which it is running. Before a Trojan program can act, it must trick the user into downloading it or performing some type of action.

Consider when a user downloads a movie from internet. After completing the download, when he tries the play the movie it interrupts to download movie player. As per the instructions, user downloads the movie player, but it also downloads the built-in Trojan with it. The Trojan was actually a part of the player.

Trojans can be configured to do many things such as log keystrokes, add the user's system to botnet or even give the attacker to gain full access of the targeted system. A user might think it is harmless and downloads it to system but it downloads malicious program to the system. Unlike virus or worms Trojans cannot spread themselves.

### Infection Methods

Trojans are usually found on the peer-to-peer sites or other locations where people are downloading software. Installed programs can be uninstalled but Trojans cannot be erased. Some malicious users even host their own websites to unlock demo programs or offer free materials which have in built Trojans in it.

Another common infection method is email. You may receive an email with an attachment or other executable. Social engineering plays a great infection process. Even Instant messaging and Internet relay chat can be spread Trojans. IM users are at great risk of becoming target for Trojans and other types of malware.

### Well-known Trojans

The best way to understand Trojans are,

**NetBus** helps the attackers by informing about the Trojan installed in the system. NetBus could also redirect input from a specified port to another IP address via another machine.

**Trojan Horse** is a program that claims to rid your computer of viruses but instead introduces viruses into the system. Trojan horses are broken down in classification based on how they breach systems and the damage they cause. The seven main types of Trojan horses are:
Remote Access Trojans
Data Sending Trojans
FTP Trojans
Proxy Trojans
Destructive Trojans
Security Software Disabler Trojans
Denial of Service attack (DOS) Trojans

**Distributing Trojans**

Distributing Trojans is not easy job. Users are more careful while clicking on unknown mails and more likely would be running antivirus. Wrappers offer hackers another, more advanced way to slip past a user's normal defences. A wrapper programs helps to combine two or more executables into a single packaged program.

Wrappers are always referred to as binders, packers and EXE binders. Some wrappers only allow programs to be joined, others allow the binding together. Many of these programs are available to the hacker underground.

## 7.3 Rootkits

Rootkit can be defined by breaking into two components root and kit. Root is a UNIX/Linux term that's the equivalent of Administrator in Windows. The word kit denotes programs that allow someone to obtain root or admin level access to the computer by executing the programs in the kit all of which is done without end-user consent or knowledge.

Rootkits have two primary functions like backdoor and software eavesdropping. Rootkits allow someone, legitimate or otherwise to administratively down which means executing files, accessing logs, monitoring user activity and even changing computer's configuration.

Many tools can be used to identify the system which is infected. Some of the good tools include the following,

Task Manager- This is built-in windows application which gives the detailed information about all running process in the system.

PS- This command used to display the currently running process on Unix/Linux systems.

NetStat-This displays active TCP connections, ports on which the computer is listening, Ethernet statistics, IP routing table, IPv4 statistics. It also shows running list of open ports and processes.

Tlist- A windows tool used to display a list of currently running processes on either a local or remote machine.

TCPView- A GUI tool used to display running processes

An attacker may decide to destroy the targeted system in attempt to cover his tracks, after his discovery. Once it is isolated form network performing forensic research. There are two major tools which we can use to further investigate systems with suspected rootkits,

**Chkrootkit**— An excellent tool that can be used to search for signs of a rootkit. It can examine system binaries for modification.
**Rootkit Hunter**— Another tool that scans file and system binaries for known and unknown rootkits.

Rootkits are very sophisticated as they make hackers very difficult to find. They are often used to infect other computers and enslave them as zombies, forcing them to attack other machines, distribute spam or steal passwords. When attempting to track a rootkit's creator, the search usually ends with the first zombie while the hacker goes undetected.

## 7.4 Spyware

Spyware is another form of malicious code that is very similar to Trojan that tracks and reports your computer activity without consent. It was actually not designed to cause damage but still it terribly affects the performance of the system over time. Spyware usually comes bundled with free software and automatically installs itself with the program you intended to use. Spyware causes modification to our web browser, redirects our search attempts and frequent displaying of pop-ups. In this instance, spyware can also termed as adware which is essentially add-supported software that has ability to track your activity.

Spyware is basically used for two purposes,

Surveillance – It is used to determine buying habits, like and dislikes and it reports to demographic marketers.

Advertising - We will be targeted for advertising by spyware vendor, who has been paid to deliver it.

Programs advertise themselves as spyware-removal tools and really function to install spyware on a victim’s system. Some of these programs include AdProtector, BPS Spy-Ware Remover, SpyBan, SpyFerret, SpyGone, SpyHunter, SpyKiller, Spy Wiper, SpyWare Nuker.

These tools are corporate-wide solutions; we can even perform some quick fixes to reduce the probability of infection.

Patch- Spyware programs take advantage of known security vulnerabilities. So we need to make sure the browser are patched and up-to date.

Use a firewall- Principle of least privilege

Change Browsers – Many spyware programs are written for IE, so avoid using IE. Other browser like chrome, Firefox has additional built in security features.

Beware of free programs— Peer-to-peer programs and other so-called ‘‘free programs’’ can be supported by spyware. After all, someone must pay the bills! Don’t install software without knowing exactly what comes with it. Take the time to read the end-user license agreement. We can only hope that the legislative and legal systems take action to prevent the ever-increasing problem of spyware.

A good offense is about defence. By implementing the solutions offered above and making the decision to deploy an enterprise-class spyware solution, we can address this problem. Although there is no guarantee that we will not become infected, there are ways to reduce the possibility. Install antispyware programs. It’s a good practice to use more than one anti-spyware program to find and remove as much spyware as possible. Well-known anti-spyware programs include the following:

Ad-Aware, HijackThis, PestPatrol, Spy Sweeper, Spybot Search & Destroy, Spyware Blaster, McAfee AntiSpyware

A final threat worth mentioning is a web bug. Web bugs are small amounts of code embedded in web pages or HTML email to monitor the reader. The bugs can be concealed in tiny pixel image tags, although any graphic on a web page or in an email can be configured to act as a web bug. Web bugs send information back to the hacker.

## 7.5 Botnets

Botnets are nothing but a collection of comprised computers connected to the internet, termed as bots used for malicious purposes. Botnets are usually controlled via protocols such as IRC and http. In many ways botnets have replaced Denial of Service attack. DOS tools were designed to purpose of denying a person or person’s access and availability.

Bots are considered to be useful tool without any significant malicious overtone, they were originally developed as a virtual individual that sits on IRC channel and it performs tasks of user, when he is busy. With the first IRC bot few worms exploited vulnerabilities in IRC clients began to appear bots were used to steal passwords, log keystrokes, and hide their identity.

Botnets plays significant role in the internet, but its hidden. Often botnets includes variety of connections and network types. Sometimes a controller will hide an IRC server installation on an educational or corporate site where high speed connection support large number of other bots. Botnets perform tasks such as distribution of spam. Botnets can also used for mass distribution new viruses, Trojans, or other malware, or they can direct to a specific domain if the website owner refuses to pay up a fee.These are not the only threats. Spambots are another emerging threat which is designed to acquire email addresses from the internet in order to build mailing list for sending spam.

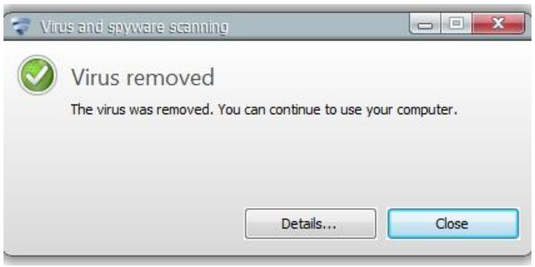
## 7.6 Examples

Best scenarios explaining above detailed topics,

**Virus Signatures**

1. Copy the following information on the text file

   X5O!P%@AP[4\PZX54(P^)7CC)7$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
2. Once the text file has been created, save it as virusdemo.txt. After it has been created, rename the extension as an executable so that the file is now named virusdemo.exe.
3. Now when we start scanning our antivirus it shows system has malicious code



Virus removed

The virus was removed. You can continue to use your computer.

**Building Torjans**

1. Create a text file named autorun.ini. Inside this text file, add the following contents:
   **[autorun]**
   **Open paint.exe**
   **Icon=paint.exe**
2. Place the autorun.ini file and a copy of paint.exe into a folder to be burned to a CD.
3. After you have completed making the DVD, reinsert it in the DVD RW drive and observe the results. It should auto start and automatically start the Paint program.
4. When this exercise was started, you could have just as easily used a Trojan program that had been wrapped with a legitimate piece of software. Just leaving the DVD lying around or giving it an attractive title, might lead someone to pick it up to see exactly what it is. Anyone running the DVD would then become infected. Even with AutoRun turned off, all it would take is for the user to double-click the DVD RW icon and the program would still run.

## 8.0 Intrusion Detection

An Intrusion Detection System is used to monitor network traffic, check for suspicious activities and notifies the network administrator or the system. Sometimes it might also detect the malicious or anomalous traffic and will take action such as barring the user or perhaps the IP address source from accessing the system.

IDS are available in many different types and will approach the mission of uncovering shady traffic n various ways. We can find using HIDS (Host based IDS) and NIDS (Network based IDS). There are also IDS which detects particular signatures of well-known threats, just like the way how antivirus software generally detects and safeguards against malware.

The following explains the types of IDS,

NIDS- These are installed at a tactical point or maybe points inside the network in order to monitor all traffic on the network. It checks incoming and outgoing traffic, but doing this could produce a bottleneck which would damage the all round speed of the computer network.

Signature Based- This can be used to monitor the packets on the system and then do a comparison against the database of attributes or signatures from recognized malicious threats. It is similar to how most anti-virus software would detect malware. However, there is a downside with the system when there will be a lag in between when new threats are identified and also the signature for finding that threat being used on IDS. In that lag period the IDS will be unable to identify any new threat.

HIDS- These operate on individual devices or hosts on the system. This will monitor all the incoming and outgoing packets on the device only and can notify the administrator or user of any suspicious activity.

Most IDSs consist of more than one application or hardware device. IDSs are usually composed of,

- **Network sensors**— Detect and send data to the system
- **Central monitoring system** — Processes and analyzes data sent from sensors
- **Report analysis**— Offers information about how to counteract a specific event
- **Database and storage components**— Perform trend analysis and store the IP address and information about the attacker
- **Response box**— Inputs information from the previously listed components and forms an appropriate response

Intrusion Detection Engines or techniques can be divided into two distinct types or methods: signatures and anomaly.

A signature-based IDS depends on a database of known attacks. These known attacks are loaded into a system as signatures. As soon as the signatures are loaded into the IDS, it can begin to guard the network. The signatures are usually given a number or name so that the administrator can easily identify an attack when it sets off an alert. Alerts can be triggered for fragmented IP packets, streams of SYN packets (DOS), or malformed ICMP packets. The alert might be configured to change to the firewall configuration, set off an alarm, or even page the administrator.

The biggest disadvantage of signature-based systems is that they can trigger only on signatures that have been loaded. Snort is a good example of Signature Based IDS.

Intrusion Detection is not the only method of detecting attacks or intrusion. Even before IDS there were other methodologies used for detecting unauthorized activity. One such method used was Integrity Verification. An example of this technology is Tripwire that works by building a profile of the system in a known state. This can be done by MD5 or SHA checksums.

Intrusion Detection System can take on many different forms and has evolved. Some early systems worked much like Tripwire, in that they detected changes in individual files, but newer systems can even block attacks in real time. As a whole no tool provides real security. A lone IDS cannot provide true security.  When coupled with firewalls, encryption, system hardening, physical security, policies such as incident response, however, an IDS can start to enhance security and play an effective role.

## 9.0 Forensic Detection

Forensic Detection is nothing but others may have thoughts of tracking a hacker in the midst of computer break-in. It is nothing but conducting a computer investigation after the fact to gather electronic evidence that can be used by the organization to determine if some type of incident or cybercrime has occurred. A forensic investigation must follow a strict set of rules that govern how the evidence is obtained, collected, stored, and examined.

For any type of Forensic work, forensic analysts must set up an area in which they can complete the required tasks. Forensic work area must account for who has access to data and to forensic workstations. This system should not have internet access, to reduce the risk of the system becoming infected with viruses, spyware, or malicious code. Without the internet access the data cannot be accessed remotely or tampered with. A real forensic lab needs a safe/controlled area in which to store evidence. Common forensic lab equipment includes like computers, printers, scanners, Spare hard drives, RAID arrays, Digital camera, Write blockers, IDE and Serial ATA cables, USB and FireWire adapters and cables.

Computer forensics follows a three-phase process: Acquisition, Authentication and Analysis. These component phases build on each other and ensure that all evidence remain credible, relevant, and admissible.

### Acquisition

Acquisition occurs through taking physical possession of something or contracting to take possession. In many cases, forensic analysts acquire hard drives, computers, media, or other items on-site. Analysts should always record all the physical evidence they recover.

The acquisition phase follows these steps:

- Collect and document the evidence.
- Protect the chain of custody
- Identify, transport, and store the evidence
- Duplicate the suspected evidence

There are also lot of requirements when conducting an investigation, which includes

- Antistatic bags
- Cable ties
- Evidence bags
- Antistatic bubble wrap
- Evidence tape
- Nonstatic potential packing materials
- Packing tape
- Various sizes of sturdy boxes

There are lot of ways to collect and handle evidence, but we need to record everything. It is always a good idea to record any identifying numbers, too, such as a Media Access Control (MAC address). By this process and by storing the adequate records, we can begin to build a proper chain of custody. The chain of custody is nothing but a process of documenting all evidence which is under control. We must always maintain the integrity of the evidence. That integrity will also make a difference to defend the credibility which we have collected.

Before storing the data it should be tagged and verified. We can tag it with our own evidence tags and documents. With all these collected evidence we need to copy to hard disks or fixed disks. This copy stored can be used for investigation. This process usually consists of three steps,

- Remove the drive from the suspect's computer
- Connect to the suspect's drive to write blocker and fingerprint
- Use a clean wiped drive to make a copy of the suspect's computer

Evidence must be protected throughout the evidence lifecycle or it will not be acceptable in court. For evidence to be admissible in court, it must be relevant, legally permissible, reliable, properly identified, and properly preserved.

### Authentication

Whenever the data is handled it should remain unchanged. Not every investigation but it is always a good practice to make the evidence to be authenticated and unchanged from the moment of discovery to the point of disposal. The evidence lifecycle includes the following

- Discovery and Recognition
- Protection
- Recording
- Collection
- Collect all relevant storage media
- Make an image of the hard disk
- Print out the screen
- Avoid degaussing equipment
- Identification
- Preservation
- Storing in a proper environment
- Transportation
- Return to evidence to owner

The primary concern is to ensure the data remains unchanged by using integrity algorithms that fingerprints the original drive and the forensically produced copy. Integrity provided for the right information. Integrity allows users information to have confidence in its correctness. Normally computer systems have many methods to protect data. This can be done through parity, checksums, or redundancy. A key objective of computer forensic is to provide integrity. Integrity is part of CIA triad i.e. nothing but Confidentiality, Integrity and Availability.

Forensics also requires cryptographic algorithms. These routines use one-way hashing algorithms that is being discussed earlier like MD5, SHA.

### Trace Evidence Analysis

Analysis is the process of examining the evidence and it is always analyzed before it is copied or authenticated. Forensic analysts typically make two copies of the original drive and work with one of the copies.

In real time, forensic investigators use many different programs when conducting their analysis. Likewise, you are unlikely to find a single program that will do everything we need to perform analysis. The two leading programs which are used are FTK (Forensic Toolkit) and Encase by Guidance.

In an investigation there is always a question arising about the trace evidence. It should be “Yes” because there should be some trace evidence.

Whenever two objects come in contact a transfer of material occurs. This is called Locard’s exchange principle and is almost universally accepted by all forensic analysts. According to this principle even if someone tries really hard, some trace evidence always remains. The complexity of modern computer leaves forensic analysts many places to look for existence. Even though suspects can make recovery harder by deleting files and caches they always leave some trace evidence. During this investigation, they examine the slack space, cache, registry, browser history and pagesys file to make sure that we can discover potential evidence.

One of the great things about IT security is that it is such a diverse field. There are many areas in which someone can specialize. Forensics is one such realm. Forensics deals heavily in process and procedure. This requires good documentation and the ability to control evidence and information that is being examined. Although a background in law enforcement is not required to become a forensic expert, it does help. After all, those individuals have a good understanding of concepts such as chain of custody. What can be said about forensics is that it is an area that is going to continue to grow. An ever-increasing number of companies are using computers, the Internet, and online databases to store massive amounts of information. This means that without a massive increase in security, cyber-hacks, attacks, and the use of computers in criminal endeavours will increase in number and scope. In turn, the demand for individuals who can work with these software tools and technology will increase.

## 10.0 Conclusion

This report details about the required deliverables as mentioned, Open source tools are installed, configured and tested in the virtual lab environment. It also details the use of each tool, with examples of its use during the setup and testing of the lab environment. It also details which tools were found to be useful and relatively easy to use. Many other alternative tools tested for various tasks, nothing their individual strengths and weaknesses, and recommending either a specific tool as completely adequate, or specifying the changes and additions required to make the best tool really useful.

This project report details about building a network lab which will be crafted to shield specific network threats considering various certain scenarios. The design of the project as mentioned it involves with various tools for establishing a network security lab.

## References

1. Gregg, Michael. Building your own security lab: Field Guide for Network Testing. Wiley Publications Inc.

2. WiseGeek Articles. What is MAC flooding?

3. Chris Lewis. Cisco TCP/IP Routing Professional Reference (2000). Computing McGraw-Hill.

4. Computer Network Security Training. What is ARP poisioning?

5. Osischool Interactive Networking. ARP spoofing.

6. James Mc Glinn. Password Hashing. Nerds Inc.

7. Michael Kassner (2008). Things to know About Rootkits.

8. Webopedia. Trojan horse.

9. From Wikipedia. Malware

10. From Wikipedia. Botnets

11. From Wikipedia. Zero-day attack

12. Spam Laws. Types of Malware