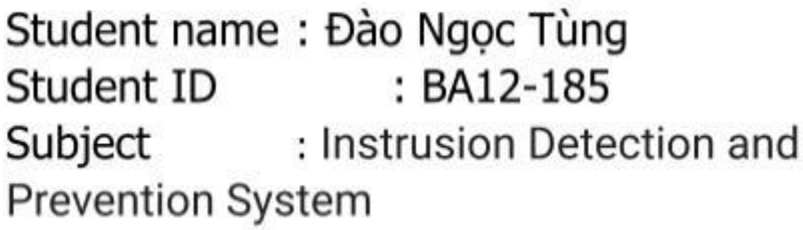
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

Information and Communication Technology Department

REPORT PROJECT

Instrusion Detection And Prevention System

FTP Unencrypted Cleartext Login



Student name : Đào Ngọc Tùng
Student ID : BA12-185
Subject : Instrusion Detection and Prevention System

HaNoi, December 2024

Table of Contents

HaNoi, December 2024

A. Introduction This Vulnerability

a. *What is this vulnerability and type of vulnerability is this?*

   i. Vulnerability: FTP Unencrypted Cleartext Login

   ii. This is a security vulnerability that allows FTP logins using unencrypted cleartext. It involves the transmission of data such as usernames and passwords over unencrypted connections, increasing the risk of information being intercepted by attackers.

b. *Outline the technical mechanism of the vulnerability*

   When an FTP service accepts login credentials without encryption, sensitive information like usernames and passwords is transmitted as cleartext over the network. This makes it possible for attackers to use network sniffing tools to capture and read this information. This vulnerability typically occurs when FTP does not employ secure protocols like FTPS (FTP over SSL/TLS) or SFTP.

c. Impact and Severity:

   i. Impact: This vulnerability can allow attackers to gain unauthorized access to an FTP system, potentially leading to the theft of sensitive data such as user information or other malicious activities on the compromised server.

   ii. Severity Level: The vulnerability is generally considered to be of low to medium risk according to common metrics because, while it is prevalent, it is usually easy to mitigate by enabling more secure FTP protocols like FTPS or SFTP. The CVSS score for this type of vulnerability might be around 4.8, indicating a medium risk with the vector string possibly like AV:A/AC:L/AU:N/C:P/I:P/A:N, suggesting a moderate exploitability factor but limited impact if properly secured.

B. Implementation

a. Create An Environment For Testing

i. Install virtual machine tools (VMWare Fusion)

ii. Install operating system

iii. Set up 3 machines:

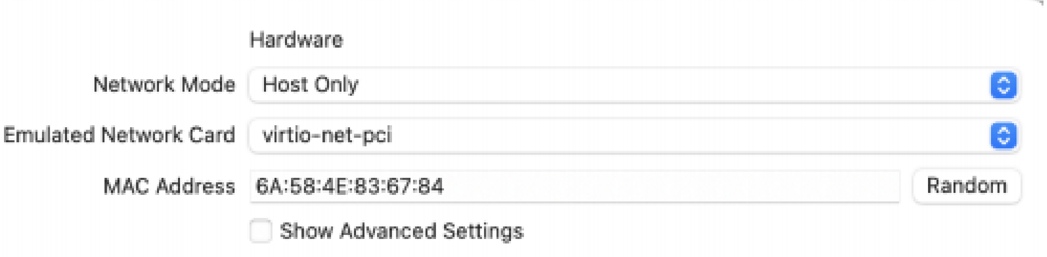
1. Attack machine 3vCPU (Kali Linux):

2. Router machine 2vCPU (Ubuntu Sever):

3. Victim machine 1vCPU (Metasploit2):

b. Create And Setup Networks On Virtual Machine Tools

i. Set up network attack machine 3vCPU (Kali Linux):



Hardware

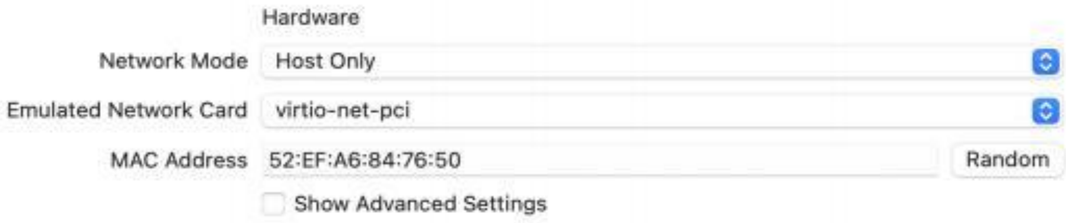
Network Mode: Host Only

Emulated Network Card: virtio-net-pci

MAC Address: 6A:58:4E:83:67:84 Random

□ Show Advanced Settings

ii. Set up network router machine 2vCPU (Ubuntu Sever):



Hardware

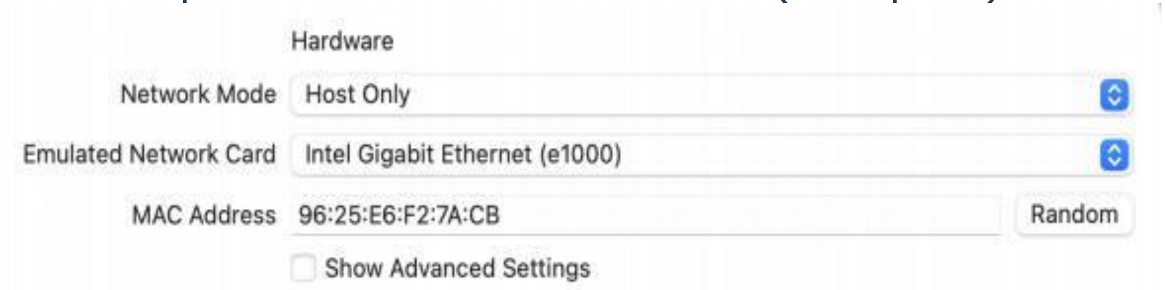
Network Mode: Host Only

Emulated Network Card: virtio-net-pci

MAC Address: 52:EF:A6:84:76:50 Random

□ Show Advanced Settings

iii. Set up network victim machine 1vCPU (Metasploit2):



Hardware

Network Mode: Host Only

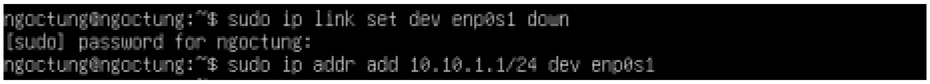
Emulated Network Card: Intel Gigabit Ethernet (e1000)

MAC Address: 96:25:E6:F2:7A:CB Random

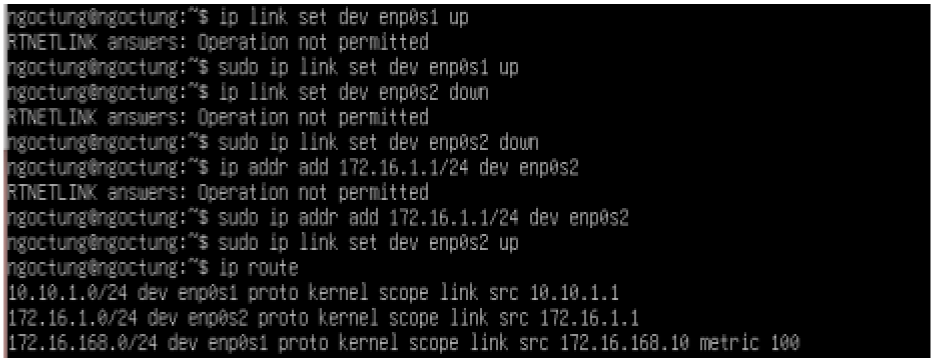
□ Show Advanced Settings

c. Configure Network For Virtual Machine

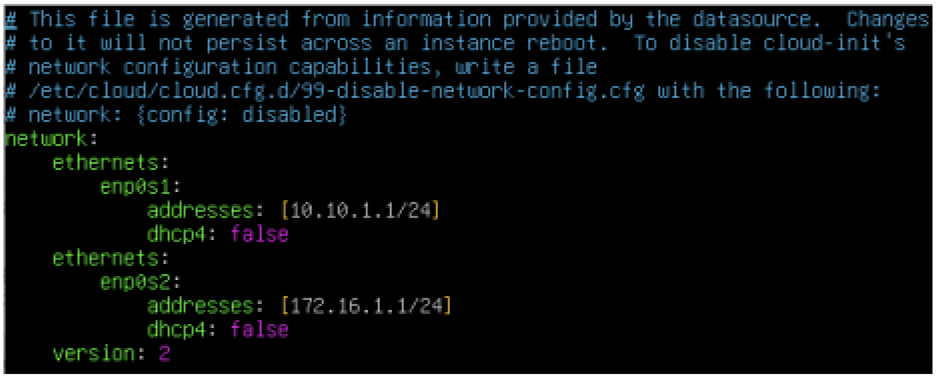
i. Configure network router machine 2vCPU (Ubuntu Sever):



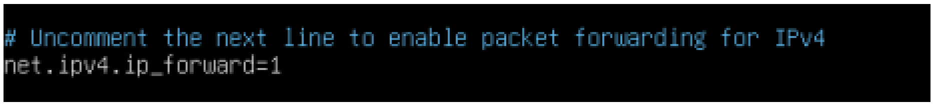
```
ngoctung@ngoctung:~$ sudo ip link set dev enp0s1 down
[sudo] password for ngoctung:
ngoctung@ngoctung:~$ sudo ip addr add 10.10.1.1/24 dev enp0s1
```



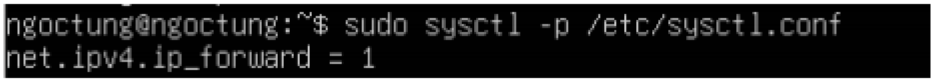
```
ngoctung@ngoctung:~$ ip link set dev enp0s1 up
RTNETLINK answers: Operation not permitted
ngoctung@ngoctung:~$ sudo ip link set dev enp0s1 up
ngoctung@ngoctung:~$ ip link set dev enp0s2 down
RTNETLINK answers: Operation not permitted
ngoctung@ngoctung:~$ sudo ip link set dev enp0s2 down
ngoctung@ngoctung:~$ ip addr add 172.16.1.1/24 dev enp0s2
RTNETLINK answers: Operation not permitted
ngoctung@ngoctung:~$ sudo ip addr add 172.16.1.1/24 dev enp0s2
ngoctung@ngoctung:~$ sudo ip link set dev enp0s2 up
ngoctung@ngoctung:~$ ip route
10.10.1.0/24 dev enp0s1 proto kernel scope link src 10.10.1.1
172.16.1.0/24 dev enp0s2 proto kernel scope link src 172.16.1.1
172.16.168.0/24 dev enp0s1 proto kernel scope link src 172.16.168.10 metric 100
```



```
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        enp0s1:
            addresses: [10.10.1.1/24]
            dhcp4: false
    ethernets:
        enp0s2:
            addresses: [172.16.1.1/24]
            dhcp4: false
    version: 2
```

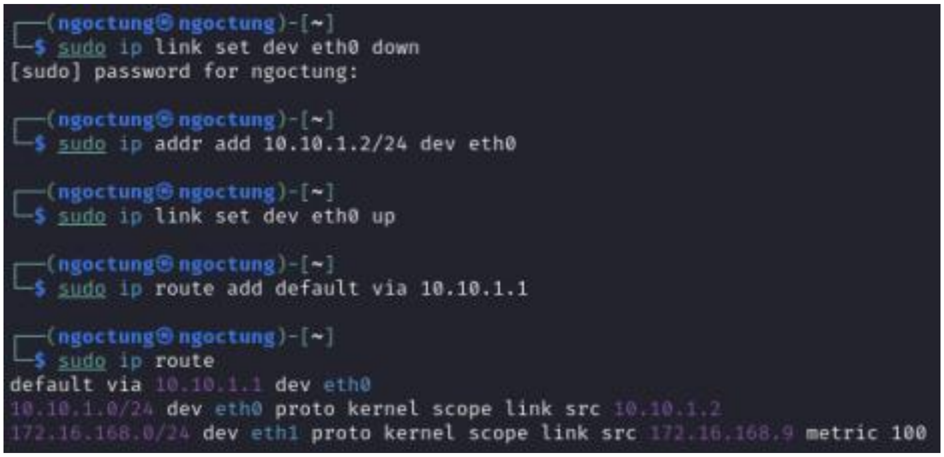


```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```



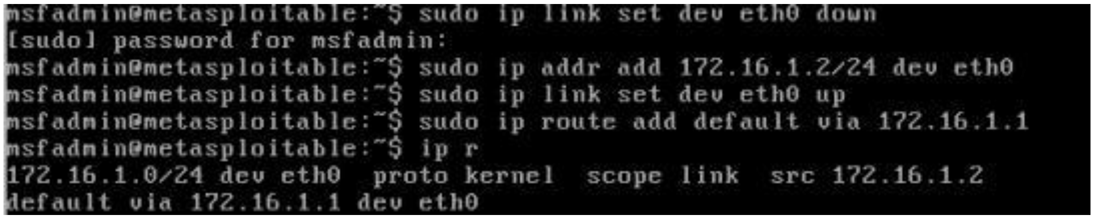
```
ngoctung@ngoctung:~$ sudo sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

ii. Configure network attack machine 3vCPU (Kali Linux):



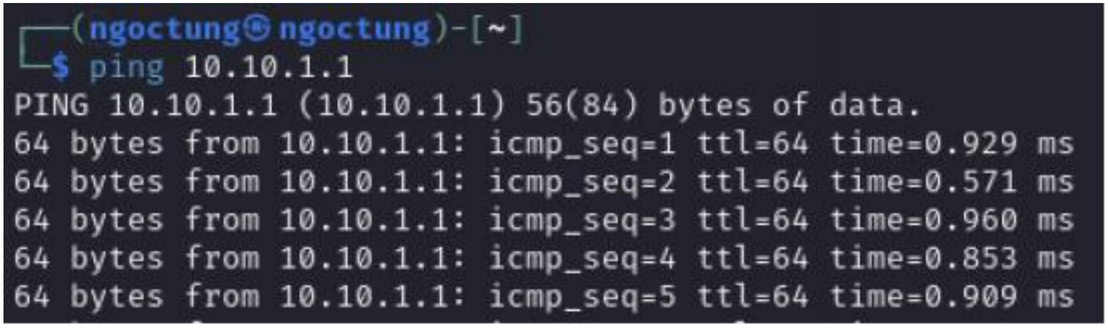
```
┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo ip link set dev eth0 down
[sudo] password for ngoctung:

┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo ip addr add 10.10.1.2/24 dev eth0

┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo ip link set dev eth0 up

┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo ip route add default via 10.10.1.1

┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo ip route
default via 10.10.1.1 dev eth0
10.10.1.0/24 dev eth0 proto kernel scope link src 10.10.1.2
172.16.168.0/24 dev eth1 proto kernel scope link src 172.16.168.9 metric 100
```

iii. Configure network victim machine 1vCPU (Metasploit):

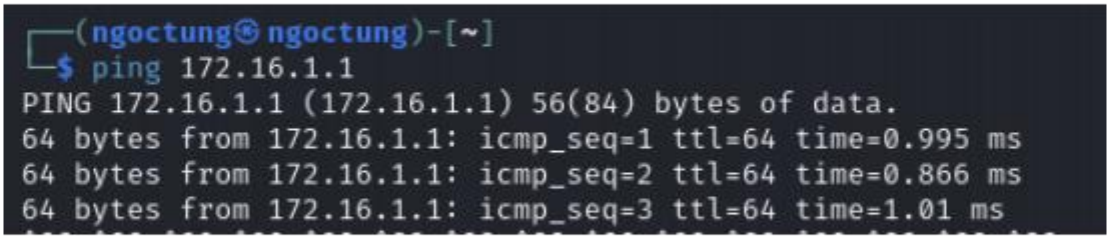


```
msfadmin@metasploitable:~$ sudo ip link set dev eth0 down
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo ip addr add 172.16.1.2/24 dev eth0
msfadmin@metasploitable:~$ sudo ip link set dev eth0 up
msfadmin@metasploitable:~$ sudo ip route add default via 172.16.1.1
msfadmin@metasploitable:~$ ip r
172.16.1.0/24 dev eth0  proto kernel  scope link  src 172.16.1.2
default via 172.16.1.1 dev eth0
```

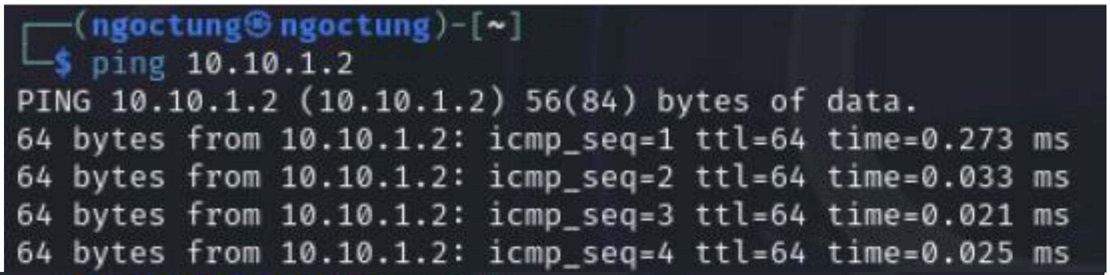
d. Check Connection



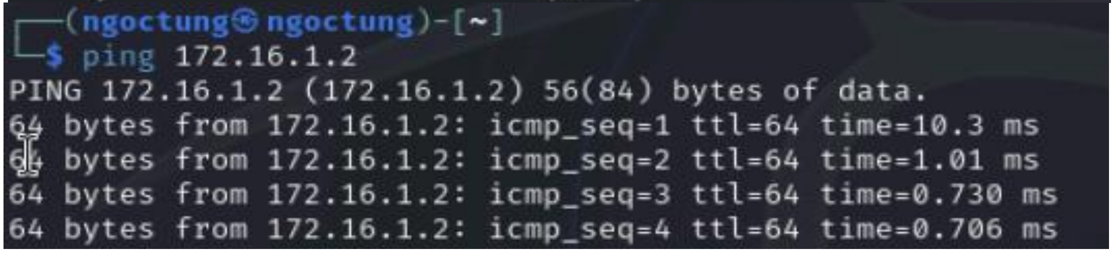
```
┌──(ngoctung㉿ngoctung)-[~]
└─$ ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1) 56(84) bytes of data.
64 bytes from 10.10.1.1: icmp_seq=1 ttl=64 time=0.929 ms
64 bytes from 10.10.1.1: icmp_seq=2 ttl=64 time=0.571 ms
64 bytes from 10.10.1.1: icmp_seq=3 ttl=64 time=0.960 ms
64 bytes from 10.10.1.1: icmp_seq=4 ttl=64 time=0.853 ms
64 bytes from 10.10.1.1: icmp_seq=5 ttl=64 time=0.909 ms
```



```
┌──(ngoctung㉿ngoctung)-[~]
└─$ ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.995 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=0.866 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=1.01 ms
```



```
┌──(ngoctung㉿ngoctung)-[~]
└─$ ping 10.10.1.2
PING 10.10.1.2 (10.10.1.2) 56(84) bytes of data.
64 bytes from 10.10.1.2: icmp_seq=1 ttl=64 time=0.273 ms
64 bytes from 10.10.1.2: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 10.10.1.2: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 10.10.1.2: icmp_seq=4 ttl=64 time=0.025 ms
```



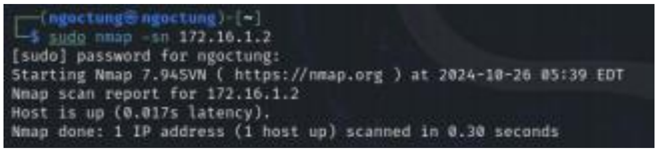
```
┌──(ngoctung㉿ngoctung)-[~]
└─$ ping 172.16.1.2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=10.3 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 172.16.1.2: icmp_seq=3 ttl=64 time=0.730 ms
64 bytes from 172.16.1.2: icmp_seq=4 ttl=64 time=0.706 ms
```

e. Vulnerability Scanning

i. Vulnerability Scanning Using Nmap

1. Step1: Host Discovery

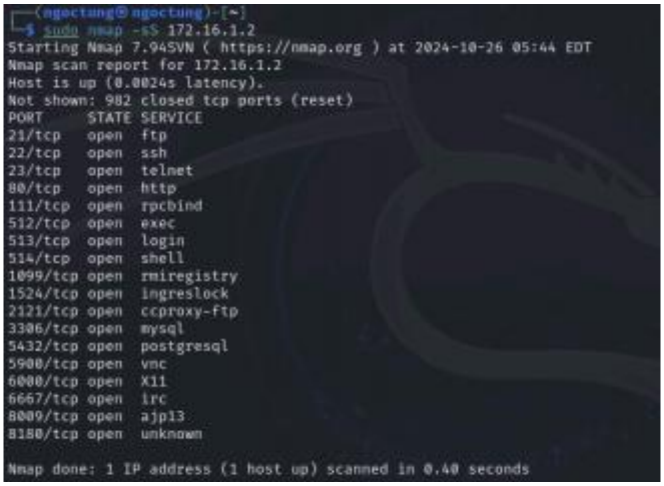
   Objective: Determine if the target machine (Metasploitable2) is active.



```
┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo nmap -sn 172.16.1.2
[sudo] password for ngoctung:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 05:39 EDT
Nmap scan report for 172.16.1.2
Host is up (0.017s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

2. Step2: Port Scanning

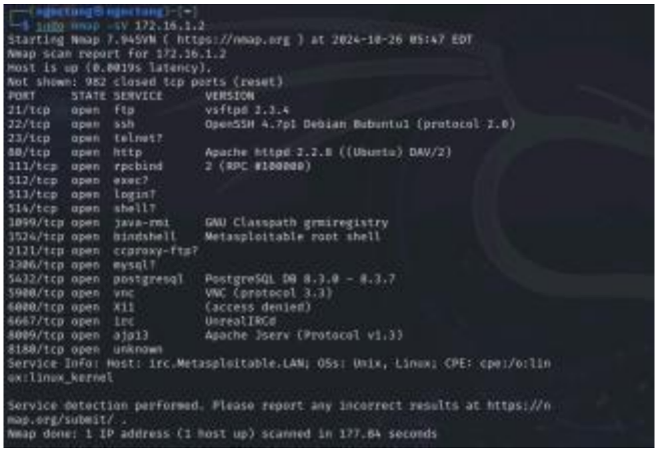
   Objective: Identify open ports on the target machine.



```
┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo nmap -sS 172.16.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 05:44 EDT
Nmap scan report for 172.16.1.2
Host is up (0.0024s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

3. Step3: Service Detection

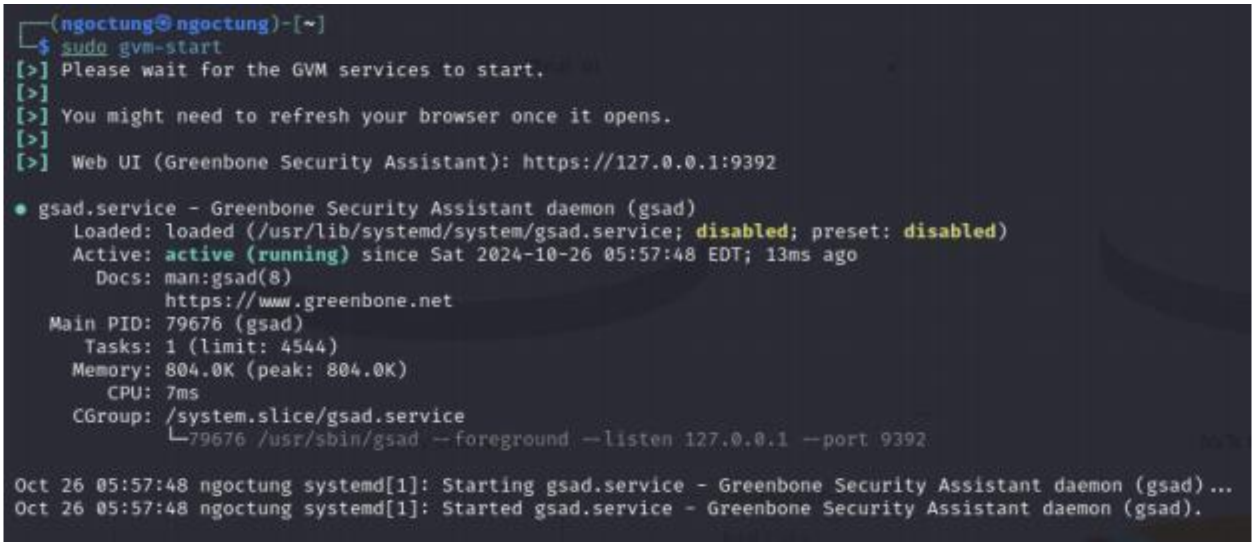
   Objective: Determine which services are running on the open ports.



```
┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo nmap -sV 172.16.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 05:47 EDT
Nmap scan report for 172.16.1.2
Host is up (0.0019s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  unknown
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 177.84 seconds
```

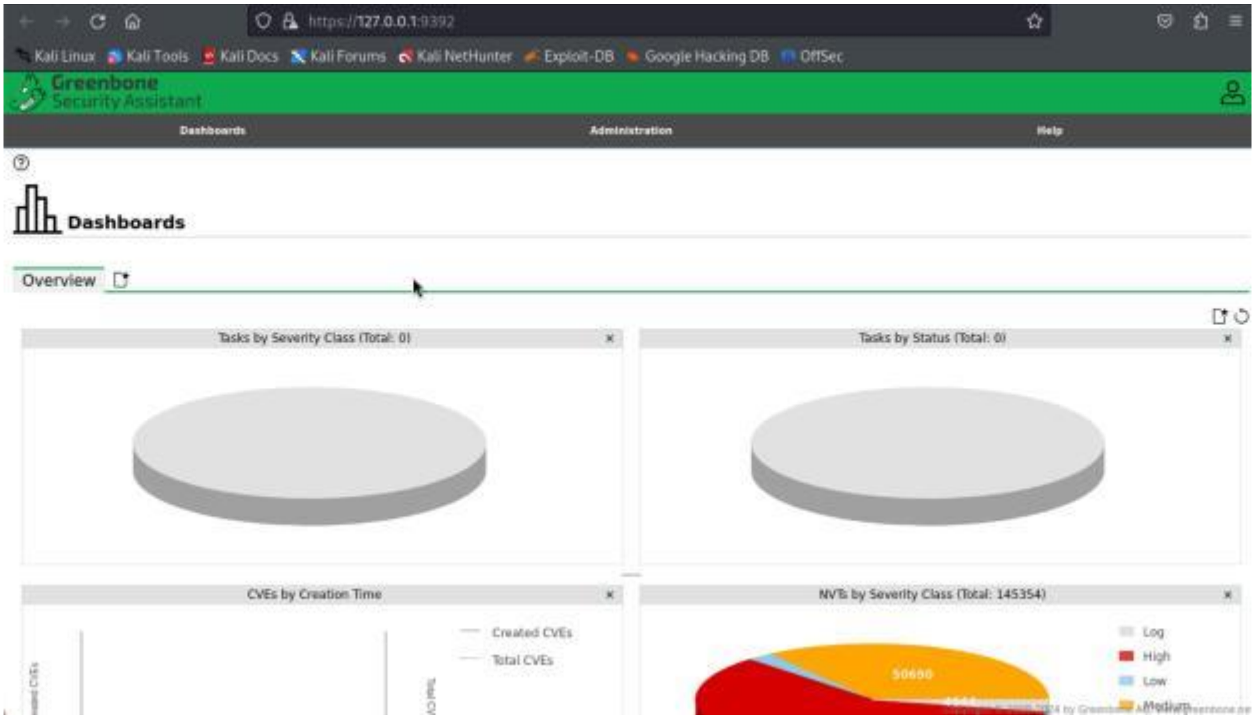
ii. Vulnerability Scanning Using OpenVAS

1. Step4: Using OpenVAS Vulnerability Scanning
   a. Start Open OpenVAS:

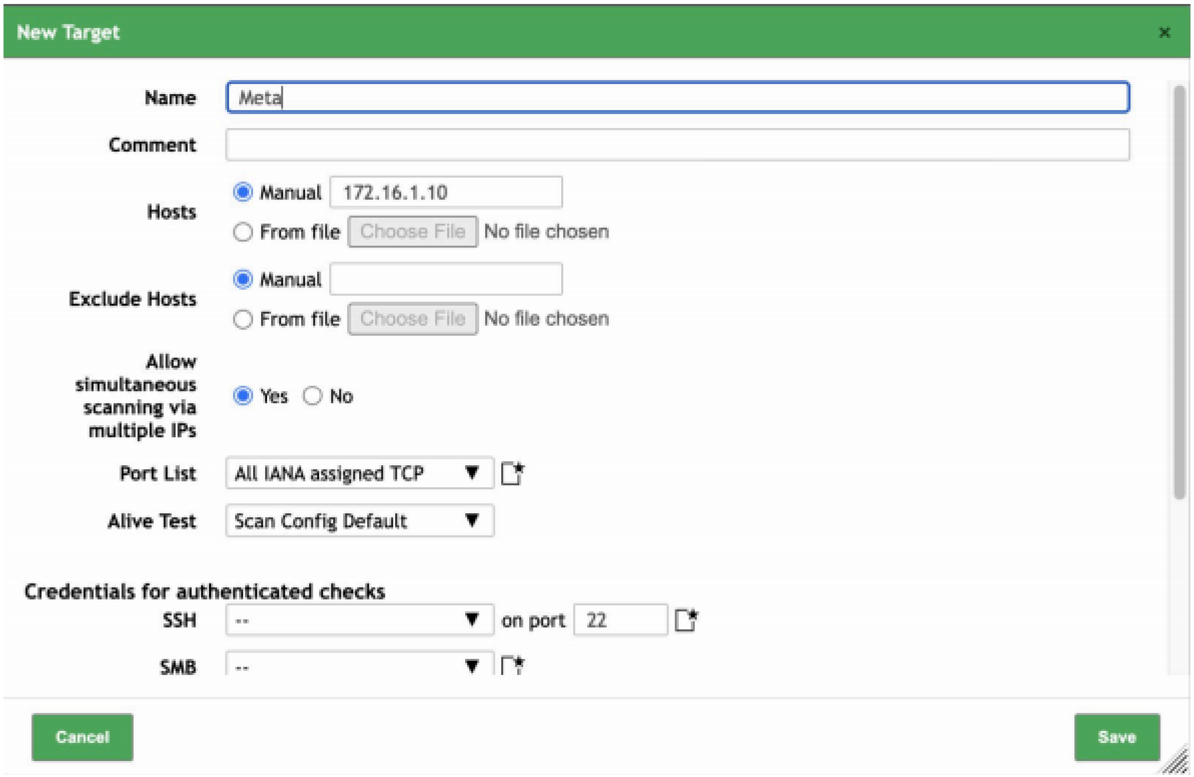


```
┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-10-26 05:57:48 EDT; 13ms ago
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 79676 (gsad)
      Tasks: 1 (limit: 4544)
     Memory: 804.0K (peak: 804.0K)
        CPU: 7ms
     CGroup: /system.slice/gsad.service
             └─79676 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Oct 26 05:57:48 ngoctung systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Oct 26 05:57:48 ngoctung systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
```

   b. Access OpenVAS Web Interface:
      Open web browser: https://localhost:9392



c. Creating a target:



New Target ×

Name: Meta

Comment:

Hosts: ● Manual 172.16.1.10
○ From file Choose File No file chosen

Exclude Hosts: ● Manual
○ From file Choose File No file chosen

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All IANA assigned TCP ▼

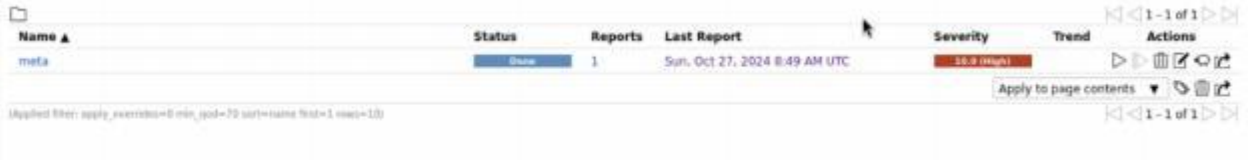
Alive Test: Scan Config Default ▼

Credentials for authenticated checks

SSH: -- ▼ on port 22

SMB: -- ▼

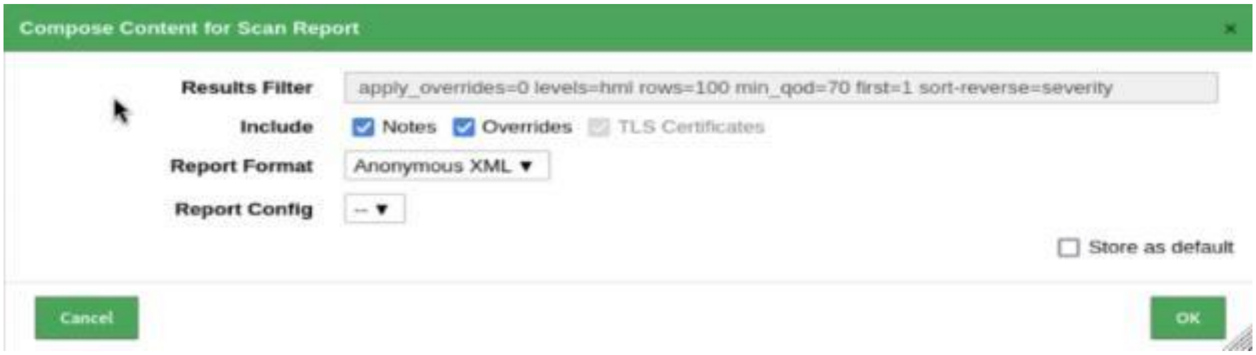
d. Start:



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
meta	Done	1	Sun, Oct 27, 2024 8:49 AM UTC	10.0 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

e. Download:



Compose Content for Scan Report ×

Results Filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity

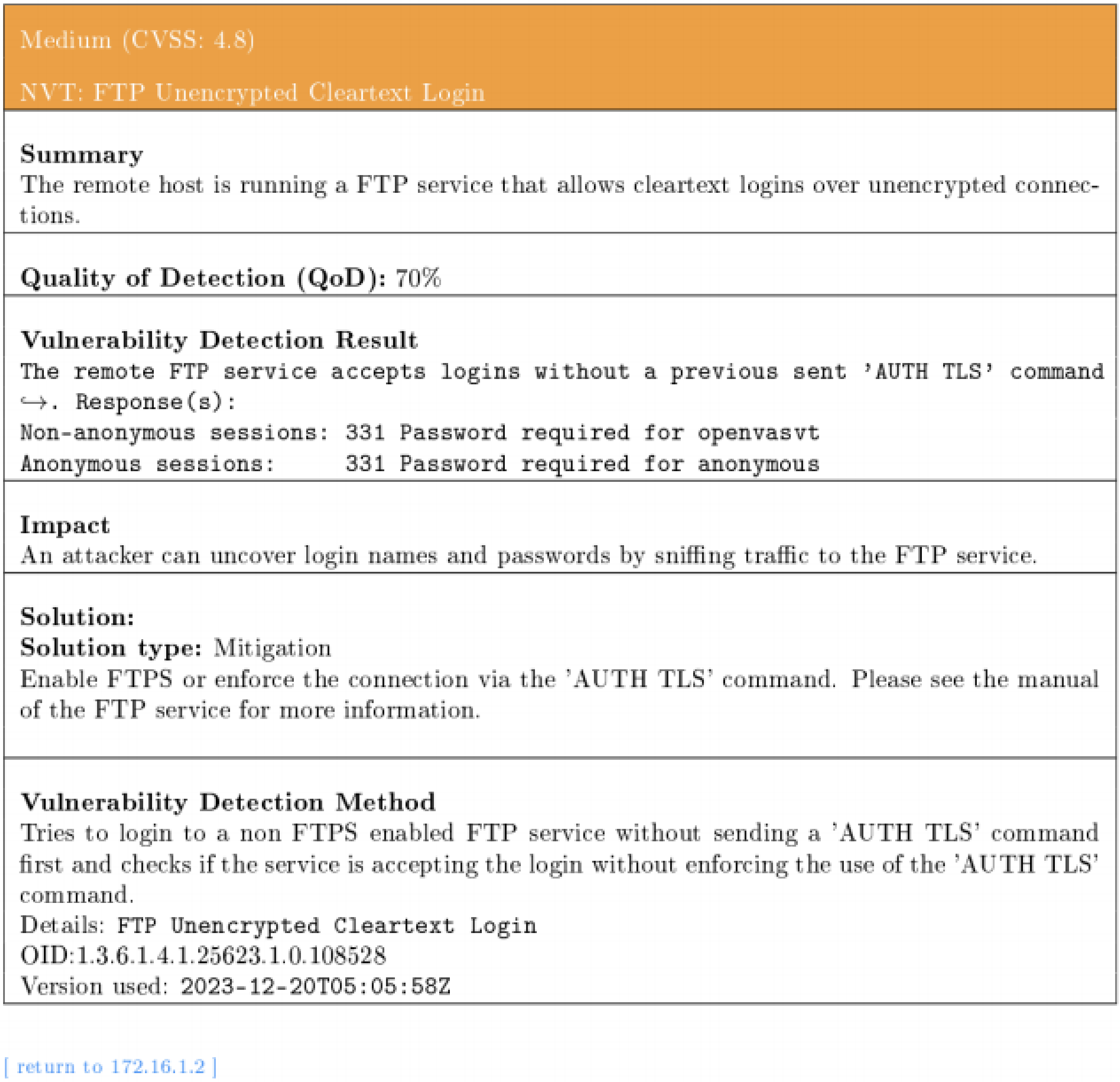
Include: ☑ Notes ☑ Overrides ☐ TLS Certificates

Report Format: Anonymous XML ▼

Report Config: -- ▼

☐ Store as default

f. Capturing the result of this vuln after exporting the report:



Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions:     331 Password required for anonymous
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

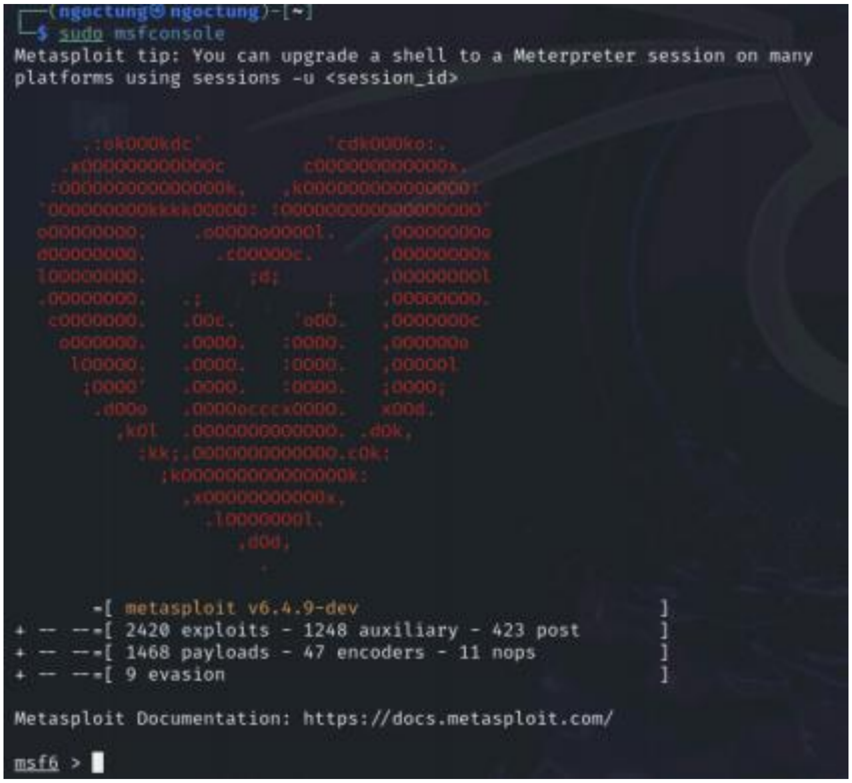
Solution:
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

[return to 172.16.1.2]

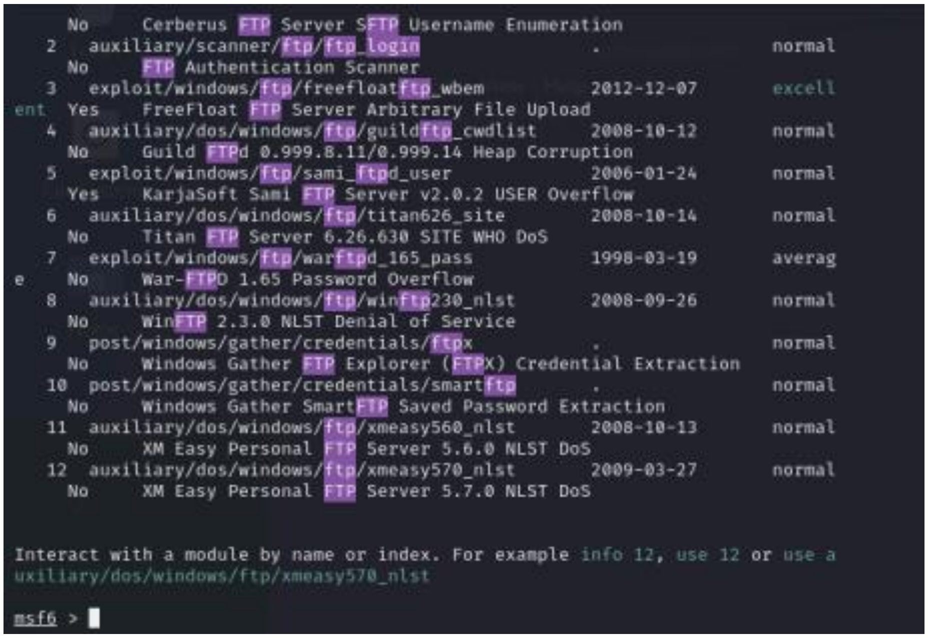
f. Exploitation Using Metasploit Framework.

i. Start Metasploit Framework



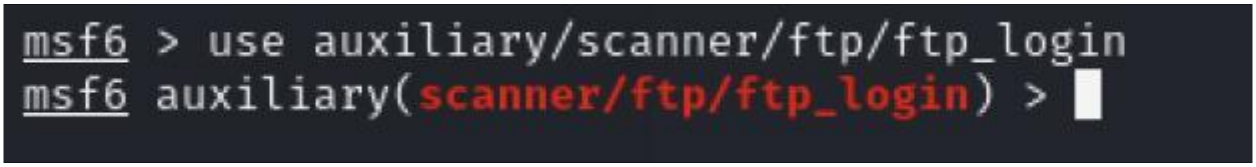
```
┌──(ngoctung㉿ngoctung)-[~]
└─$ sudo msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>


         .:okOOOkdc'           'cdkOOOko:.
       .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
      :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
     'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
     oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
     dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
     lOOOOOOOO.         ;d;         ,OOOOOOOOl
     .OOOOOOOO.   .;           ;    ,OOOOOOOO.
      cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
       oOOOOOO.   .OOOO.    :OOOO.   ,OOOOOOo
        lOOOOO.   .OOOO.    :OOOO.   ,OOOOOl
         ;OOOO'   .OOOO.    :OOOO.   ;OOOO;
          .dOOo   .OOOOocccxOOOO.   xOOd.
            ,kOl  .OOOOOOOOOOOOO. .dOk,
              :kk;.OOOOOOOOOOOOO.cOk:
                ;kOOOOOOOOOOOOOOOk:
                  ,xOOOOOOOOOOOx,
                    .lOOOOOOOl.
                       ,dOd,
                         .

       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > █
```

ii. Search Ftp Login



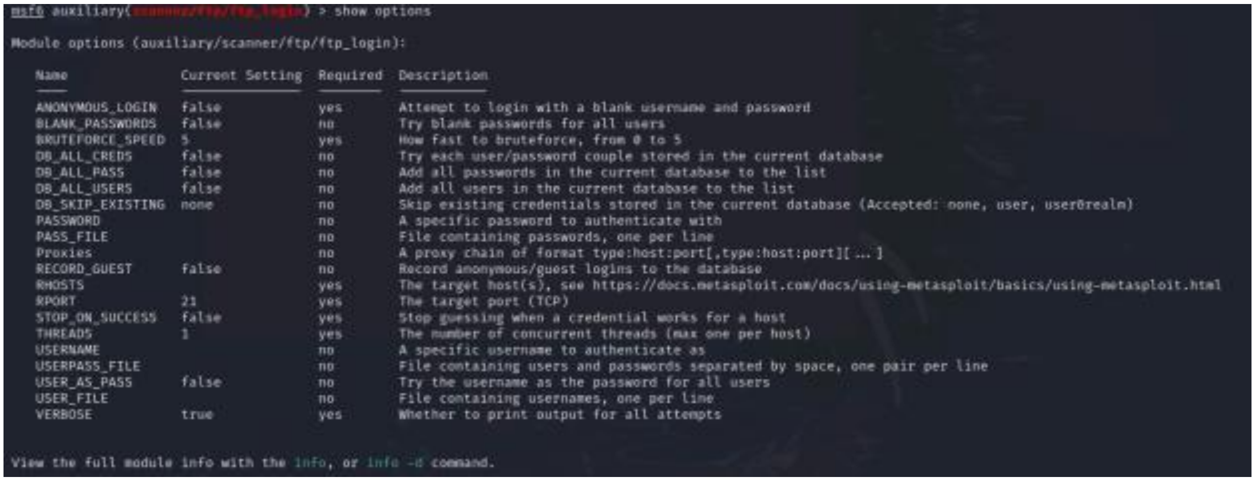
```
     No     Cerberus FTP Server SFTP Username Enumeration
   2  auxiliary/scanner/ftp/ftp_login                    .                normal
     No     FTP Authentication Scanner
   3  exploit/windows/ftp/freefloatftp_wbem              2012-12-07       excell
ent  Yes    FreeFloat FTP Server Arbitrary File Upload
   4  auxiliary/dos/windows/ftp/guildftp_cwdlist         2008-10-12       normal
     No     Guild FTPd 0.999.8.11/0.999.14 Heap Corruption
   5  exploit/windows/ftp/sami_ftpd_user                 2006-01-24       normal
     Yes    KarjaSoft Sami FTP Server v2.0.2 USER Overflow
   6  auxiliary/dos/windows/ftp/titan626_site            2008-10-14       normal
     No     Titan FTP Server 6.26.630 SITE WHO DoS
   7  exploit/windows/ftp/warftpd_165_pass               1998-03-19       averag
e    No     War-FTPD 1.65 Password Overflow
   8  auxiliary/dos/windows/ftp/winftp230_nlst           2008-09-26       normal
     No     WinFTP 2.3.0 NLST Denial of Service
   9  post/windows/gather/credentials/ftpx               .                normal
     No     Windows Gather FTP Explorer (FTPX) Credential Extraction
   10 post/windows/gather/credentials/smartftp           .                normal
     No     Windows Gather SmartFTP Saved Password Extraction
   11 auxiliary/dos/windows/ftp/xmeasy560_nlst           2008-10-13       normal
     No     XM Easy Personal FTP Server 5.6.0 NLST DoS
   12 auxiliary/dos/windows/ftp/xmeasy570_nlst           2009-03-27       normal
     No     XM Easy Personal FTP Server 5.7.0 NLST DoS


Interact with a module by name or index. For example info 12, use 12 or use a
uxiliary/dos/windows/ftp/xmeasy570_nlst

msf6 > █
```

iii. Select And Exploit



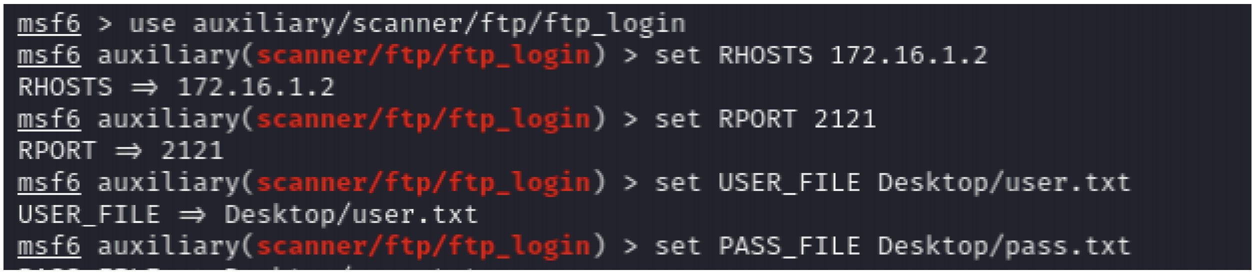
```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > 
```

iv. Show Options



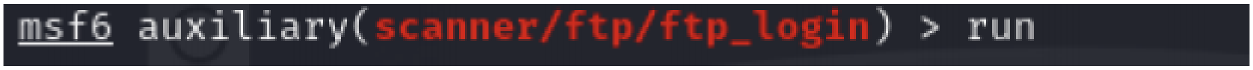
```
msf6 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   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)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

v. Set Up Payload

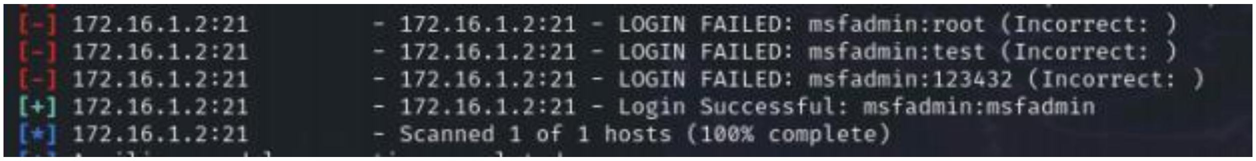


```
msf6 > use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 172.16.1.2
RHOSTS ⇒ 172.16.1.2
msf6 auxiliary(scanner/ftp/ftp_login) > set RPORT 2121
RPORT ⇒ 2121
msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE Desktop/user.txt
USER_FILE ⇒ Desktop/user.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE Desktop/pass.txt
```

vi. Excute The Exploit



```
msf6 auxiliary(scanner/ftp/ftp_login) > run
```



```
[-] 172.16.1.2:21         - 172.16.1.2:21 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 172.16.1.2:21         - 172.16.1.2:21 - LOGIN FAILED: msfadmin:test (Incorrect: )
[-] 172.16.1.2:21         - 172.16.1.2:21 - LOGIN FAILED: msfadmin:123432 (Incorrect: )
[+] 172.16.1.2:21         - 172.16.1.2:21 - Login Successful: msfadmin:msfadmin
[*] 172.16.1.2:21         - Scanned 1 of 1 hosts (100% complete)
```

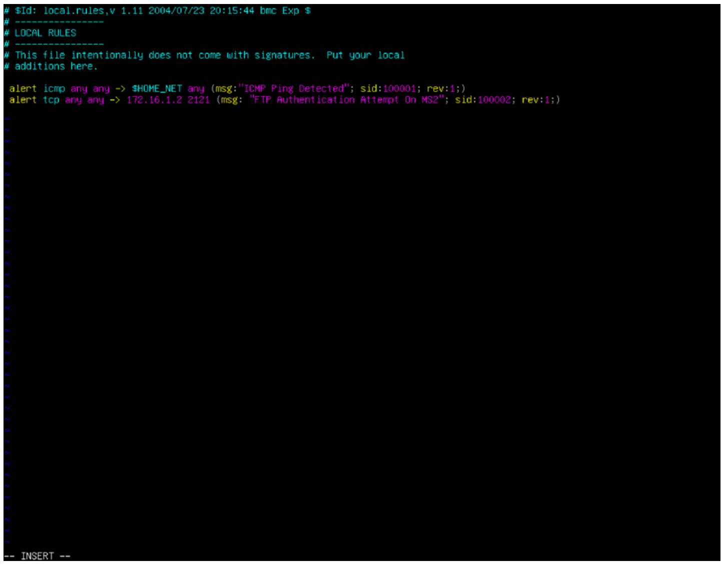
C. Mitigation And Remediation

a. Detection With Snort:

i. Install Snort: Using command apt install snort -y

ii. Rules: sudo vim /etc/snort/rules/local.rules

alert tcp any any -> 172.16.1.2 2121

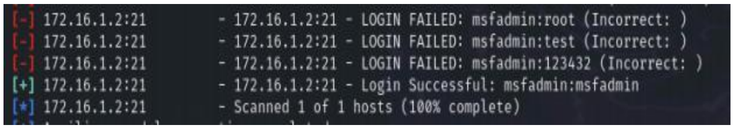


```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

 alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:100001; rev:1;)
 alert tcp any any -> 172.16.1.2 2121 (msg: "FTP Authentication Attempt On MS2"; sid:100002; rev:1;)

-- INSERT --
```

iii. Test Detection:

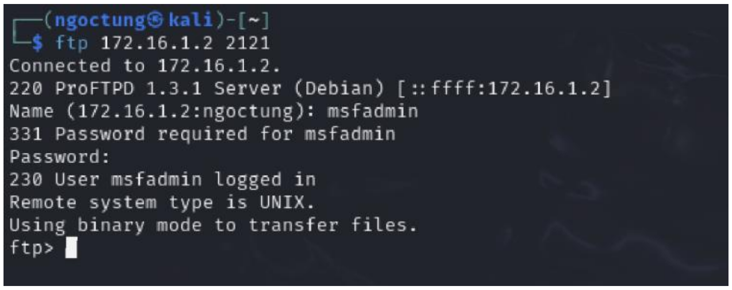
After attack with metasploit we have username

and password is msfadmin



```
[-] 172.16.1.2:21         - 172.16.1.2:21 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 172.16.1.2:21         - 172.16.1.2:21 - LOGIN FAILED: msfadmin:test (Incorrect: )
[-] 172.16.1.2:21         - 172.16.1.2:21 - LOGIN FAILED: msfadmin:123432 (Incorrect: )
[+] 172.16.1.2:21         - 172.16.1.2:21 - Login Successful: msfadmin:msfadmin
[*] 172.16.1.2:21         - Scanned 1 of 1 hosts (100% complete)
```

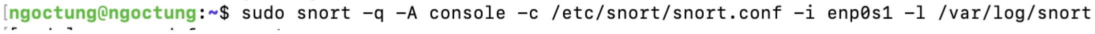
We using the ftp to attack the victim machine



```
┌──(ngoctung㉿kali)-[~]
└─$ ftp 172.16.1.2 2121
Connected to 172.16.1.2.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.1.2]
Name (172.16.1.2:ngoctung): msfadmin
331 Password required for msfadmin
Password:
230 User msfadmin logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

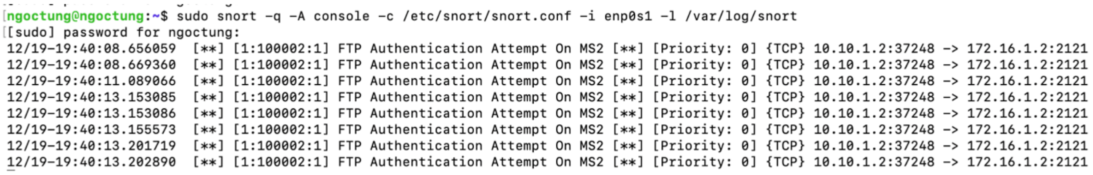
Using command: sudo snort -q -A console -c /etc/snort/snort.conf -i enp0s1 -l /var/log/snort.

This command to check log detection



```
ngoctung@ngoctung:~$ sudo snort -q -A console -c /etc/snort/snort.conf -i enp0s1 -l /var/log/snort
```

Result the detection:



```
ngoctung@ngoctung:~$ sudo snort -q -A console -c /etc/snort/snort.conf -i enp0s1 -l /var/log/snort
[sudo] password for ngoctung:
12/19-19:40:08.656059  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:08.669360  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:11.089066  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:13.153085  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:13.153086  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:13.155573  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:13.201719  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
12/19-19:40:13.202890  [**] [1:100002:1] FTP Authentication Attempt On MS2 [**] [Priority: 0] {TCP} 10.10.1.2:37248 -> 172.16.1.2:2121
```

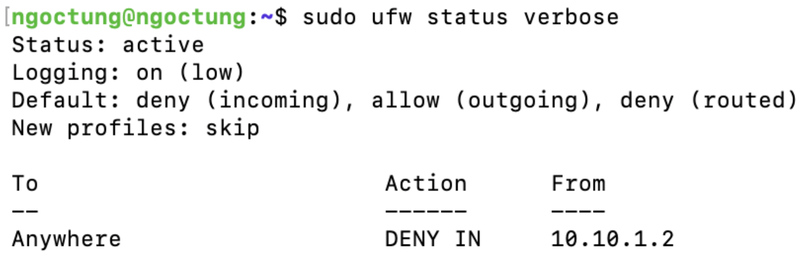
b. Configuration Fire Wall On Victim Machine (Metasploit):

i. Install Fire Wall: sudo apt install ufw

ii. Enable Fire Wall: sudo ufw enable

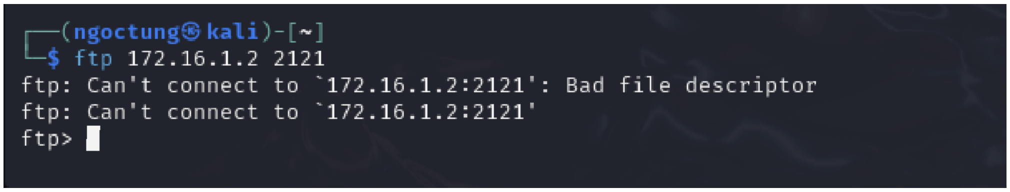
iii. Block: sudo ufw deny from 10.10.1.2

iv. Status Fire Wall: sudo ufw status verbose



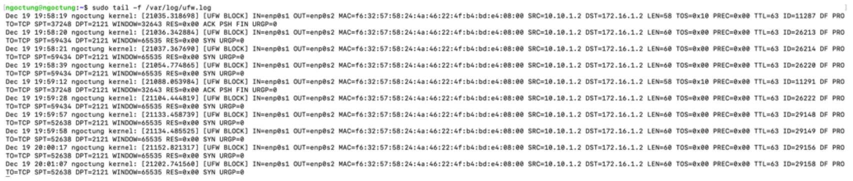
```
ngoctung@ngoctung:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
Anywhere                   DENY IN     10.10.1.2
```

v. Not Allow Attack



```
┌──(ngoctung㉿kali)-[~]
└─$ ftp 172.16.1.2 2121
ftp: Can't connect to `172.16.1.2:2121': Bad file descriptor
ftp: Can't connect to `172.16.1.2:2121'
ftp> 
```

vi. Check log ufw: sudo tail -f /var/log/ufw.log



```
ngoctung@ngoctung:~$ sudo tail -f /var/log/ufw.log
Dec 19 19:58:19 ngoctung kernel: [21035.318698] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=58 TOS=0x10 PREC=0x00 TTL=63 ID=11287 DF PRO
TO=TCP SPT=37248 DPT=2121 WINDOW=32643 RES=0x00 ACK PSH FIN URGP=0
Dec 19 19:58:20 ngoctung kernel: [21036.342884] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=26213 DF PRO
TO=TCP SPT=59434 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 19:58:21 ngoctung kernel: [21037.367690] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=26214 DF PRO
TO=TCP SPT=59434 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 19:58:39 ngoctung kernel: [21054.774865] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=26220 DF PRO
TO=TCP SPT=59434 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 19:59:12 ngoctung kernel: [21088.053984] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=58 TOS=0x10 PREC=0x00 TTL=63 ID=11291 DF PRO
TO=TCP SPT=37248 DPT=2121 WINDOW=32643 RES=0x00 ACK PSH FIN URGP=0
Dec 19 19:59:28 ngoctung kernel: [21104.444819] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=26222 DF PRO
TO=TCP SPT=59434 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 19:59:57 ngoctung kernel: [21133.458739] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=29148 DF PRO
TO=TCP SPT=52638 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 19:59:58 ngoctung kernel: [21134.485525] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=29149 DF PRO
TO=TCP SPT=52638 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 20:00:17 ngoctung kernel: [21152.821317] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=29156 DF PRO
TO=TCP SPT=52638 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
Dec 19 20:01:07 ngoctung kernel: [21202.741560] [UFW BLOCK] IN=enp0s1 OUT=enp0s2 MAC=f6:32:57:58:24:4a:46:22:4f:b4:bd:e4:08:00 SRC=10.10.1.2 DST=172.16.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=29158 DF PRO
TO=TCP SPT=52638 DPT=2121 WINDOW=65535 RES=0x00 SYN URGP=0
```

D. Conclusion

a. Key Points Summary:

i. Understanding The Vulnerability: FTP Unencryptext Cleartext Login. This security vulnerability allows FTP logins in unencrypted cleartext, exposing user name and pass words to interception by attackers.

ii. Technique Exploitation: Using Metasploit Framework. iii. Mitigation: We highlighted the significance of using firewalls as a preventive strategy. Setting up firewalls like UFW can limit access to sensitive ports and services, thereby reducing the attack surface.

b. Important Of Addressing The Vulnerability

i. Data Security: Protects sensitive information from interception

ii. Regulatory Compliance: Ensures adherence to industry regulations

iii. Reduced Attack Surface: Lowers risk by minimizing weak points

iv. Cost Savings: Prevents costly data breaches

E. References

a. https://www.clearos.com/clearfoundation/social/community/not-being-able-to-login-to-ftp-2121-port

b. https://forum.greenbone.net/t/understanding-a-specific-scan-result-ftp-unencrypted-cleartext-login/15045

c. https://www.beyondsecurity.com/resources/vulnerabilities/ftp-clear-text-authentication

d. https://www.speedguide.net/port.php?port=2121

HaNoi, December 2024