BS3944: Penetration Testing

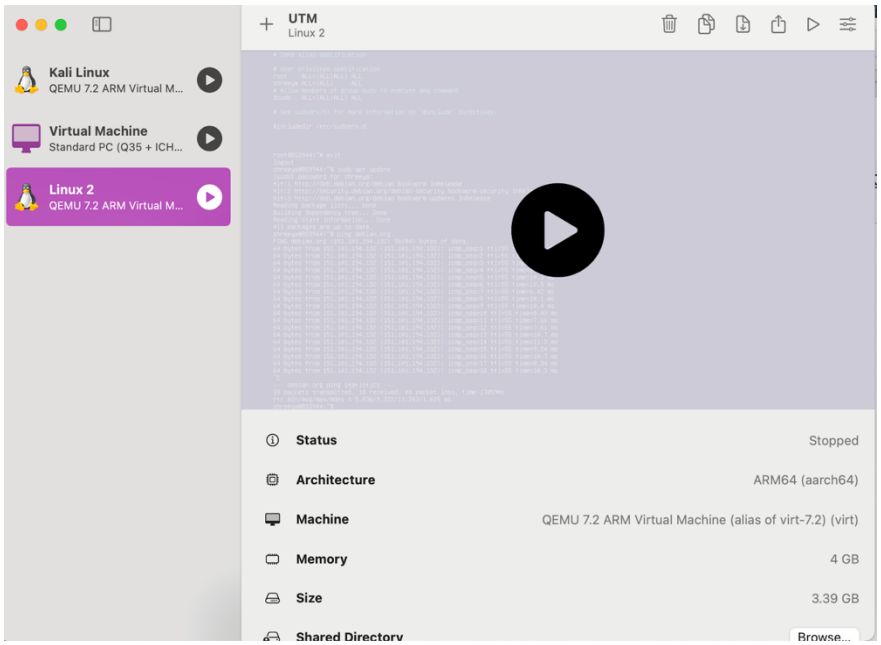
Practical Work

Figure 1: Illustration of penetration testing concepts (Evalian®, 2024).

Table of Contents

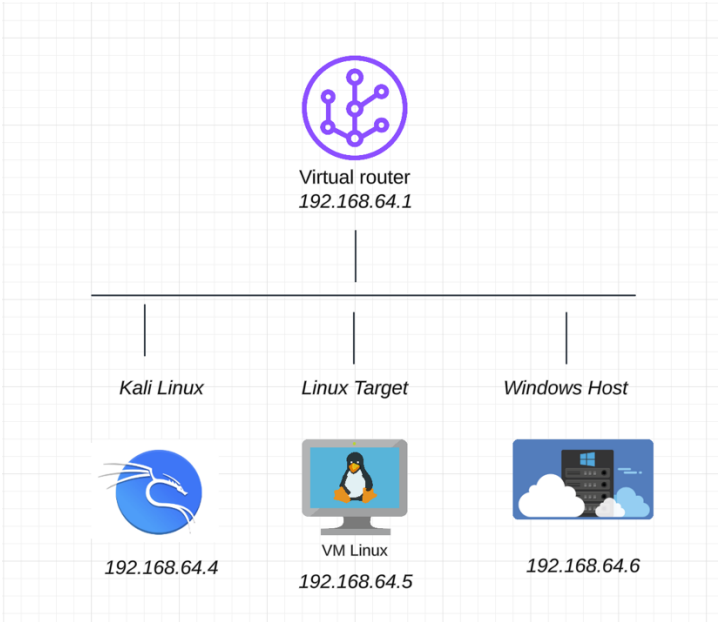
Virtual Lab Setup

Environment Description



A virtual lab with Linux and Metasploitable workstations connected over an isolated, host-only network.

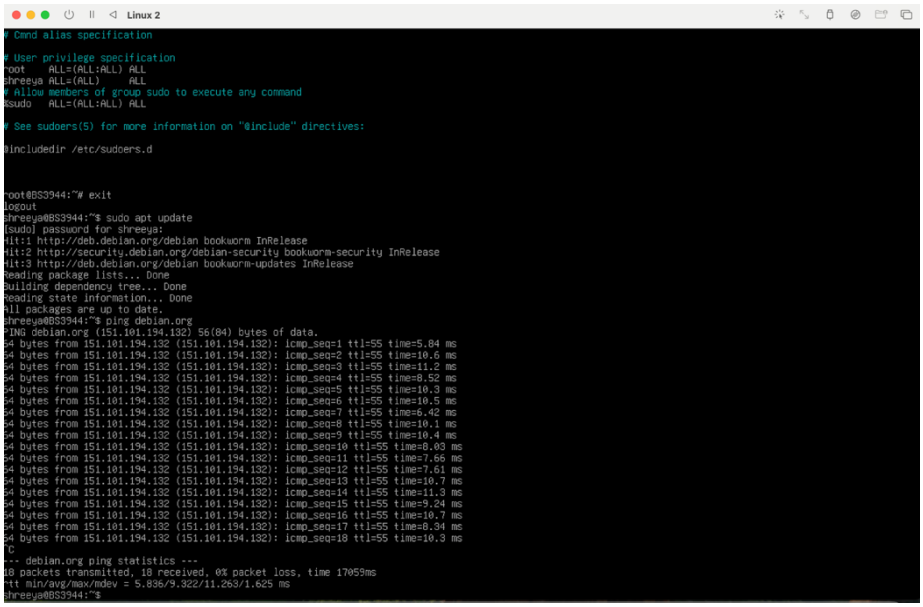
Network Configuration Diagram



The network diagram clearly depicts device functions, IP allocations, and virtual router links, ensuring communication channels are transparent.

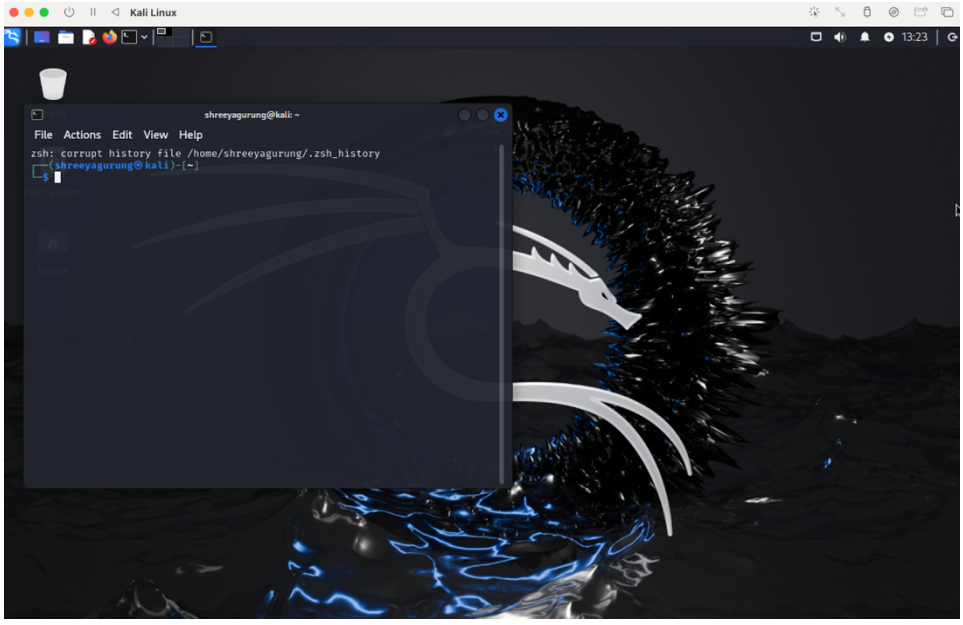
Set up Documentation

Linux



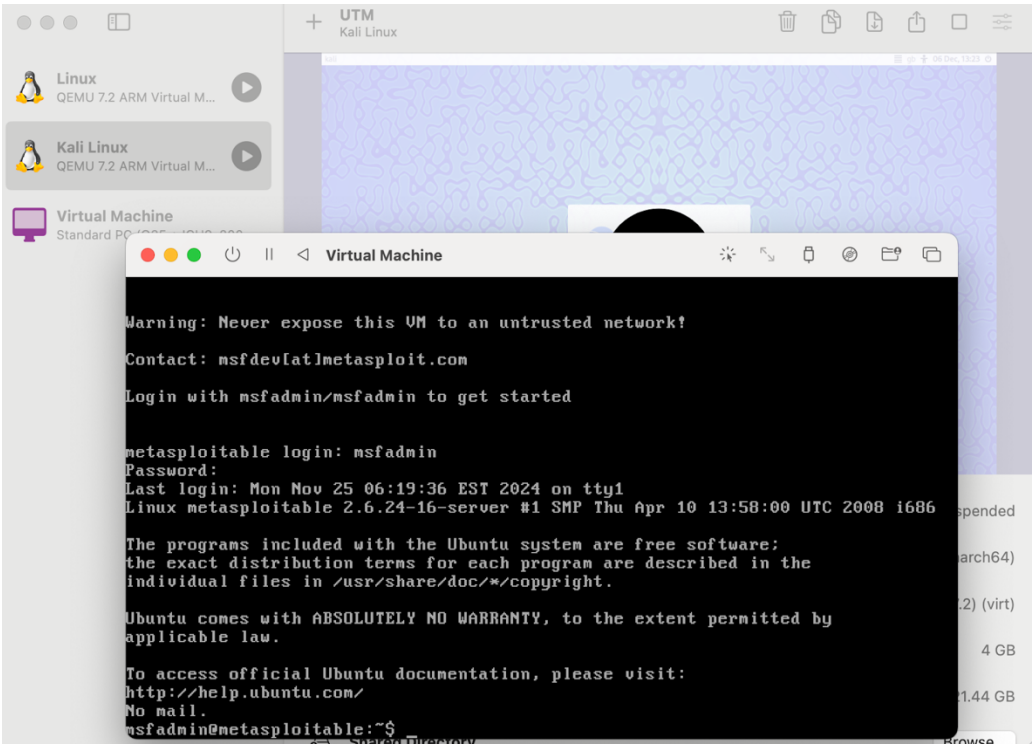
The Linux system was installed, upgraded, and configured with user privileges. Successful ping testing to other lab machines demonstrated connectivity.

Kali Linux



The Kali Linux system was installed and configured on the same isolated network, ready for testing.

Virtual Machine



Utilising its known vulnerabilities, Metasploitable was set up for testing and initialised with default credentials.

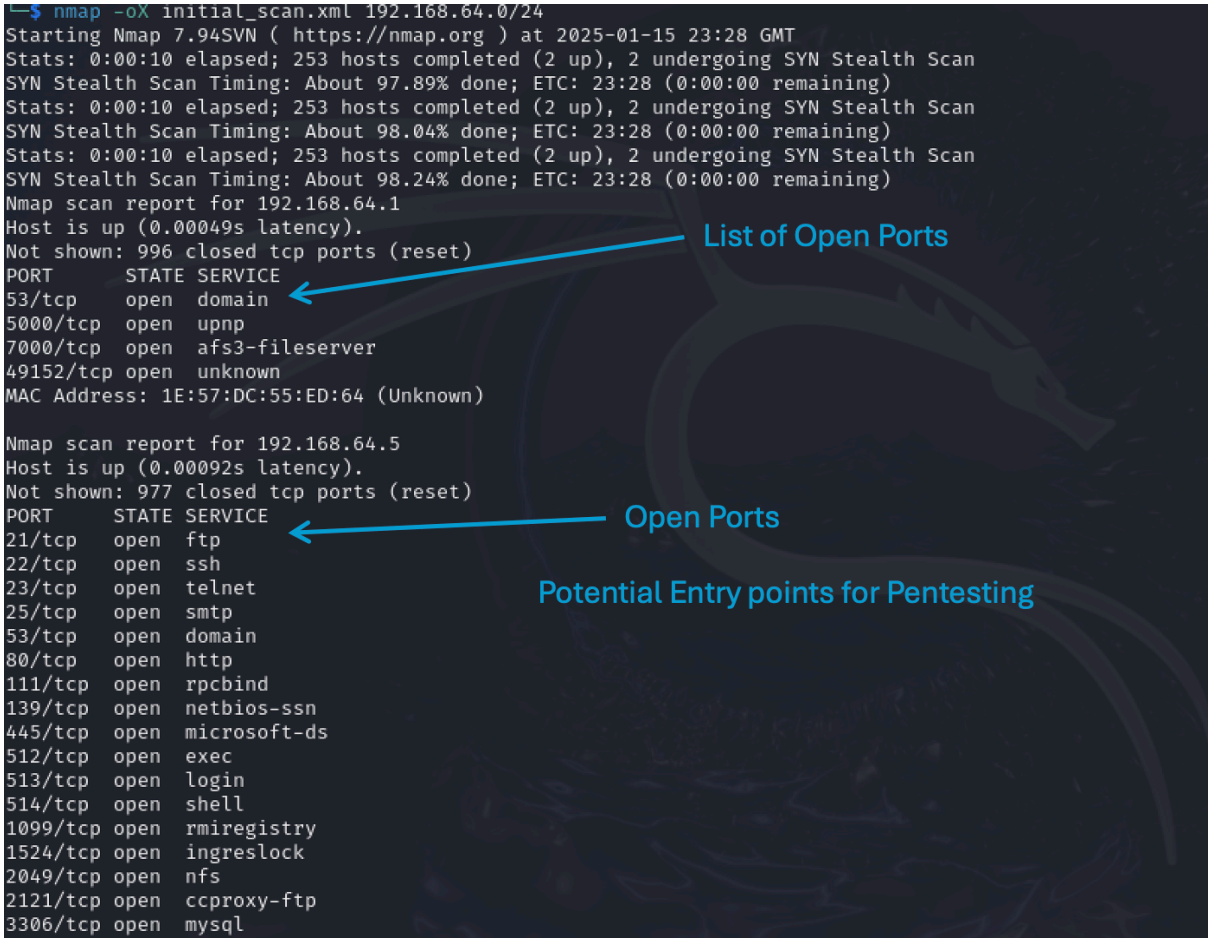
Reconnaissance Phase

Nmap

Tools and Methods:

For host identification, port scanning (-sS, -sV), service detection, and vulnerability analysis, Nmap was used (Yen, 2024). Followed up with, inspecting open ports, and export results using -oX.

Evidence:

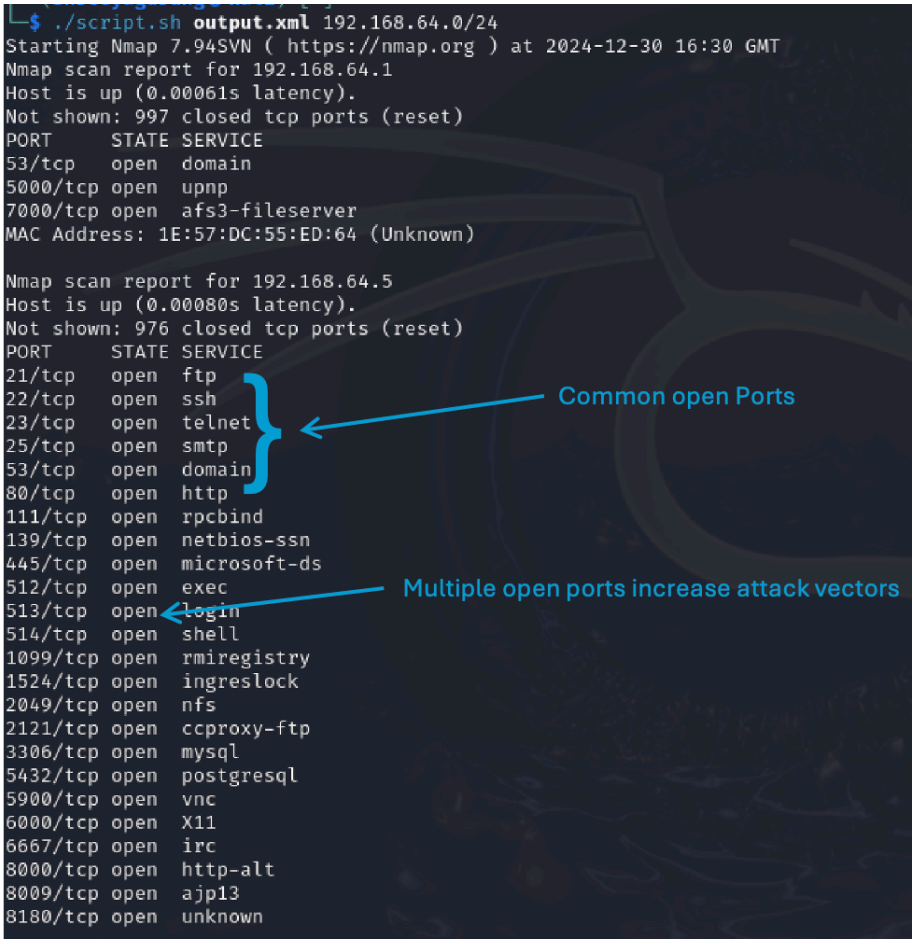


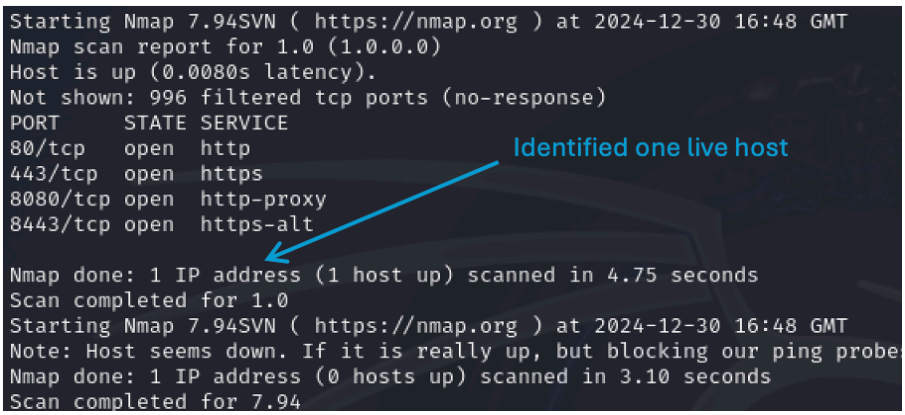
```
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: CA:EC:BC:CC:4F:C5 (Unknown)

Nmap scan report for 192.168.64.4
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.64.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 11.42 seconds
```

Analysis:

Open ports on 192.168.64.1 and 192.168.64.5, which host services like FTP, SSH, HTTP, databases, and RPC, are discovered by the scan. A more thorough vulnerability evaluation is necessary for these possible entry points.

Script to Automate Nmap Scans + Discover live hosts






```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 16:48 GMT
Nmap scan report for 1.0 (1.0.0.0)
Host is up (0.0080s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds
Scan completed for 1.0
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 16:48 GMT
Note: Host seems down. If it is really up, but blocking our ping probe
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
Scan completed for 7.94
```

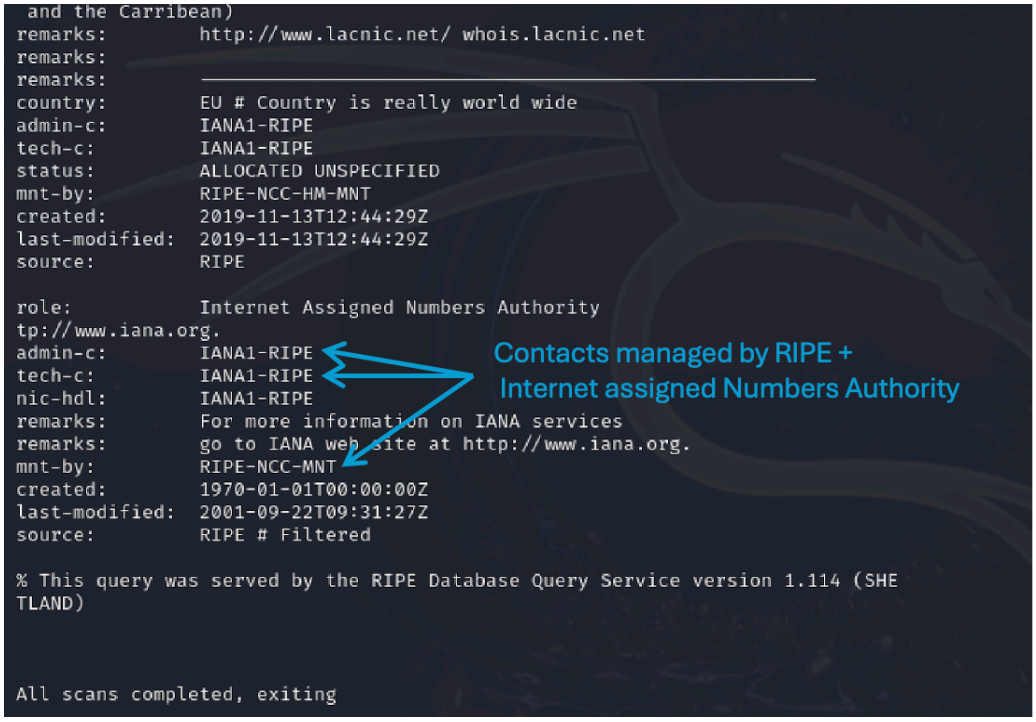
Dmitry

Tools and Method:

Dmitry employs reconnaissance and information gathering. In order to facilitate additional evaluation or possible exploitation, it gathers technical and public information about a target, including emails, open ports, subdomains, and WHOIS data (*GeeksforGeeks,* 2021).

Evidence:


```
└─$ dmitry -wi 192.168.64.5
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.64.5
Continuing with limited modules
HostIP:192.168.64.5
HostName:

Gathered Inet-whois information for 192.168.64.5
---------------------------------


inetnum:        192.168.0.0 - 192.169.95.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA

remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
 and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
```



Analysis

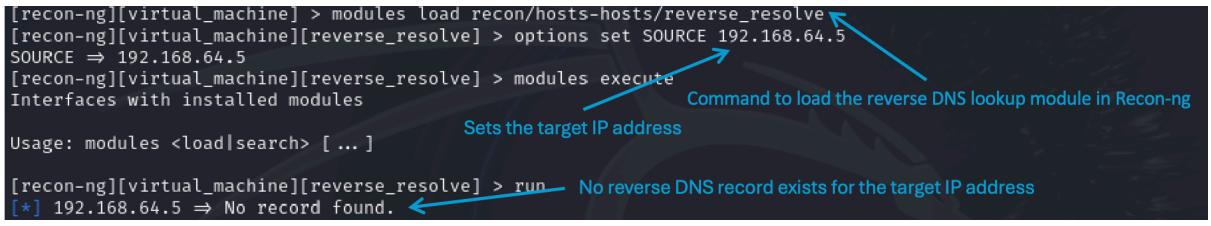
The scan indicates limited external accessibility since 192.168.64.5 is part of an IANA-managed reserved private IP range that lacks a hostname or specific ownership.

Recon-ng

Tools and Method:

Recon-ng's reverse_resolve module was utilised to look up IP 192.168.64.5 in reverse DNS. Setting the target IP and running the hostname resolution module are two steps in the process.

Evidence:



Analysis:

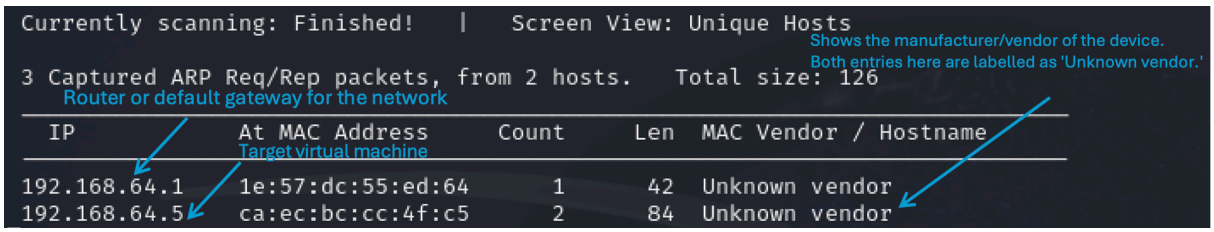
The IP does not have hostname mapping, as the scan showed no reverse DNS record for it. It's probably an unregistered or private IP address that's utilised in internal networks. Finding more specific information on the target was far more difficult in the absence of a domain.

Netdiscover

Tools and Method

In order to find active hosts and their MAC addresses within the subnet, Netdiscover was utilised for ARP-based network discovery. The process entailed scanning 192.168.64.0/24, emphasising the devices linked to the network and its structure.

Evidence



Analysis

The target virtual machine (192.168.64.5) and the gateway (192.168.64.1) are the two active hosts displayed in the results. Although their MAC addresses were found, vendor details are not available, suggesting that there aren't many network devices in the area.

Vulnerability Scanning

NIKTO

Tools and Method:

The web server at 192.168.64.5 on port 80 was scanned using Nikto. The technique finds weaknesses such as sensitive data, exposed directories, missing headers, and out-of-date software (*Vaishnavi*, 2024).

Evidence:

Analysis

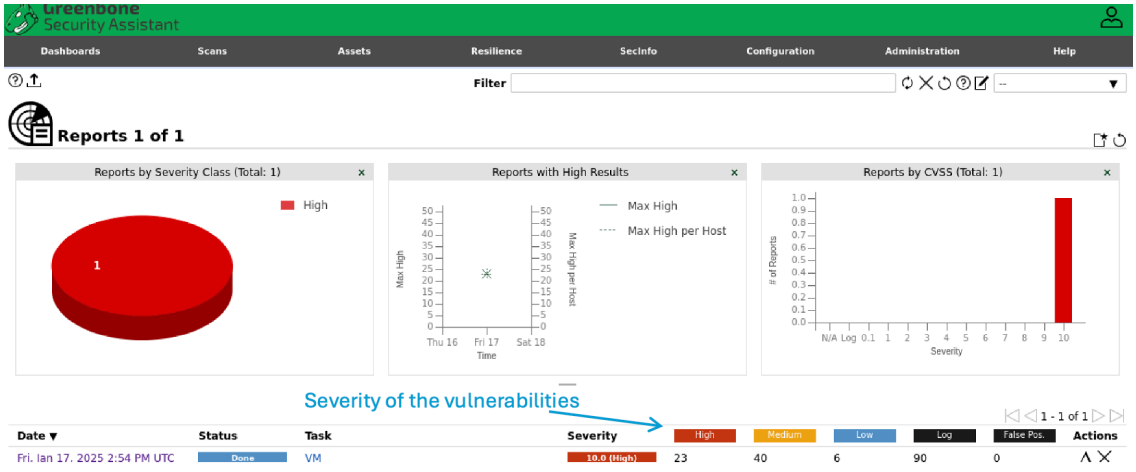
Critical vulnerabilities discovered by the scan included an out-of-date Apache version (2.2.8), missing security headers, phpinfo.php and phpMyAdmin that were accessible to the public, and the TRACE method enabled. Updates, turning off TRACE, and protecting private data are all examples of immediate mitigation.

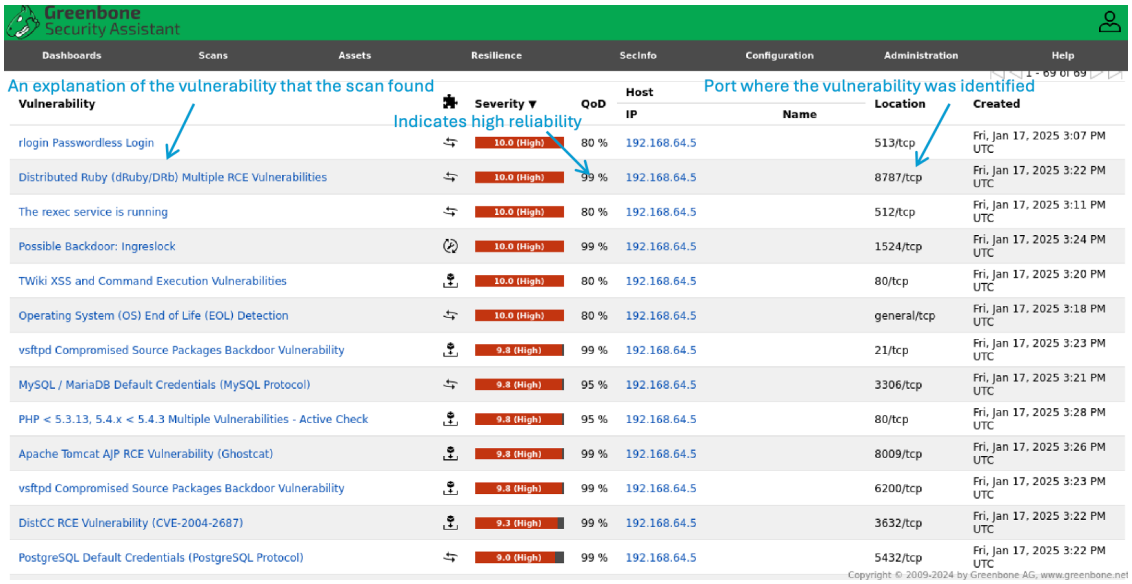
OPENVAS

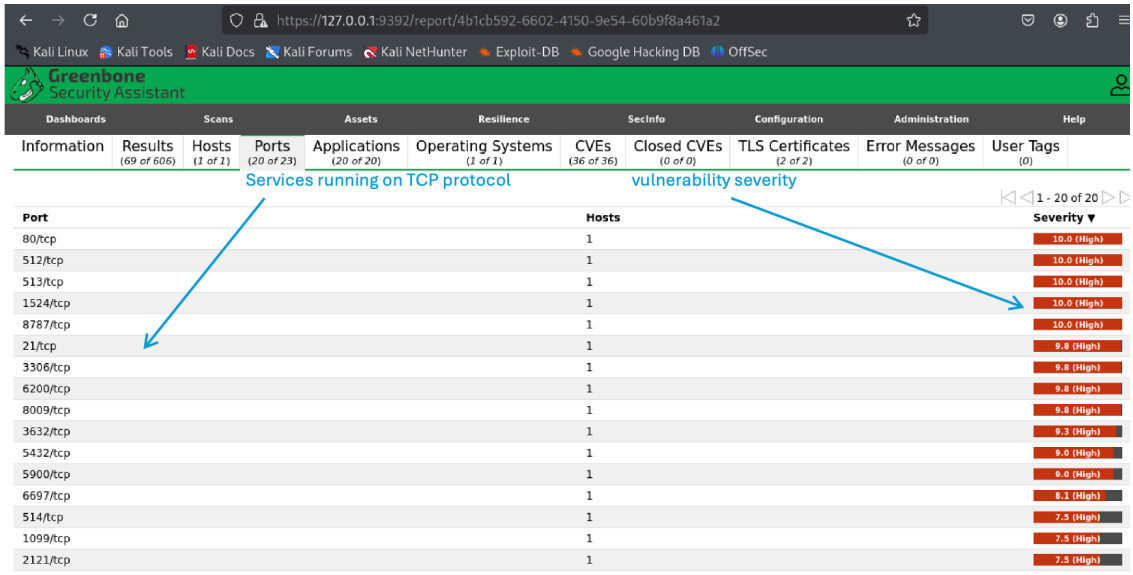
Tools and Method:

OpenVAS evaluates security vulnerabilities using vulnerability scanning technologies such as Greenbone Vulnerability Manager (GVM) (Yasani, 2015). Through automated vulnerability tests, port scanning, service detection, and CVE matching, it finds vulnerabilities.

Evidence:


Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Reports 1 of 1
Reports by Severity Class (Total: 1)
High
1
Reports with High Results
Max High
Max High per Host
Thu 16
Fri 17
Sat 18
Time
Reports by CVSS (Total: 1)
# of Reports
Severity
Severity of the vulnerabilities
1 - 1 of 1
Date
Status
Task
Severity
High
Medium
Low
Log
False Pos.
Actions
Fri, Jan 17, 2025 2:54 PM UTC
Done
VM
10.0 (High)
23
40
6
90
0


Greenbone Security Assistant
An explanation of the vulnerability that the scan found
Indicates high reliability
Port where the vulnerability was identified
Vulnerability
Severity
QoD
Host
IP
Name
Location
Created
rlogin Passwordless Login
10.0 (High)
80 %
192.168.64.5
513/tcp
Fri, Jan 17, 2025 3:07 PM UTC
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities
10.0 (High)
99 %
192.168.64.5
8787/tcp
Fri, Jan 17, 2025 3:22 PM UTC
The rexec service is running
10.0 (High)
80 %
192.168.64.5
512/tcp
Fri, Jan 17, 2025 3:11 PM UTC
Possible Backdoor: Ingreslock
10.0 (High)
99 %
192.168.64.5
1524/tcp
Fri, Jan 17, 2025 3:24 PM UTC
TWiki XSS and Command Execution Vulnerabilities
10.0 (High)
80 %
192.168.64.5
80/tcp
Fri, Jan 17, 2025 3:20 PM UTC
Operating System (OS) End of Life (EOL) Detection
10.0 (High)
80 %
192.168.64.5
general/tcp
Fri, Jan 17, 2025 3:18 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability
9.8 (High)
99 %
192.168.64.5
21/tcp
Fri, Jan 17, 2025 3:23 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)
9.8 (High)
95 %
192.168.64.5
3306/tcp
Fri, Jan 17, 2025 3:21 PM UTC
PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check
9.8 (High)
95 %
192.168.64.5
80/tcp
Fri, Jan 17, 2025 3:28 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)
9.8 (High)
99 %
192.168.64.5
8009/tcp
Fri, Jan 17, 2025 3:26 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability
9.8 (High)
99 %
192.168.64.5
6200/tcp
Fri, Jan 17, 2025 3:23 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)
9.3 (High)
99 %
192.168.64.5
3632/tcp
Fri, Jan 17, 2025 3:22 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)
9.0 (High)
99 %
192.168.64.5
5432/tcp
Fri, Jan 17, 2025 3:22 PM UTC
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


https://127.0.0.1:9392/report/4b1cb592-6602-4150-9e54-60b9f8a461a2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Information
Results (69 of 606)
Hosts (1 of 1)
Ports (20 of 23)
Applications (20 of 20)
Operating Systems (1 of 1)
CVEs (36 of 36)
Closed CVEs (0 of 0)
TLS Certificates (2 of 2)
Error Messages (0 of 0)
User Tags (0)
Services running on TCP protocol
vulnerability severity
1 - 20 of 20
Port
Hosts
Severity
80/tcp
1
10.0 (High)
512/tcp
1
10.0 (High)
513/tcp
1
10.0 (High)
1524/tcp
1
10.0 (High)
8787/tcp
1
10.0 (High)
21/tcp
1
9.8 (High)
3306/tcp
1
9.8 (High)
6200/tcp
1
9.8 (High)
8009/tcp
1
9.8 (High)
3632/tcp
1
9.3 (High)
5432/tcp
1
9.0 (High)
5900/tcp
1
9.0 (High)
6697/tcp
1
8.1 (High)
514/tcp
1
7.5 (High)
1099/tcp
1
7.5 (High)
2121/tcp
1
7.5 (High)

Analysis

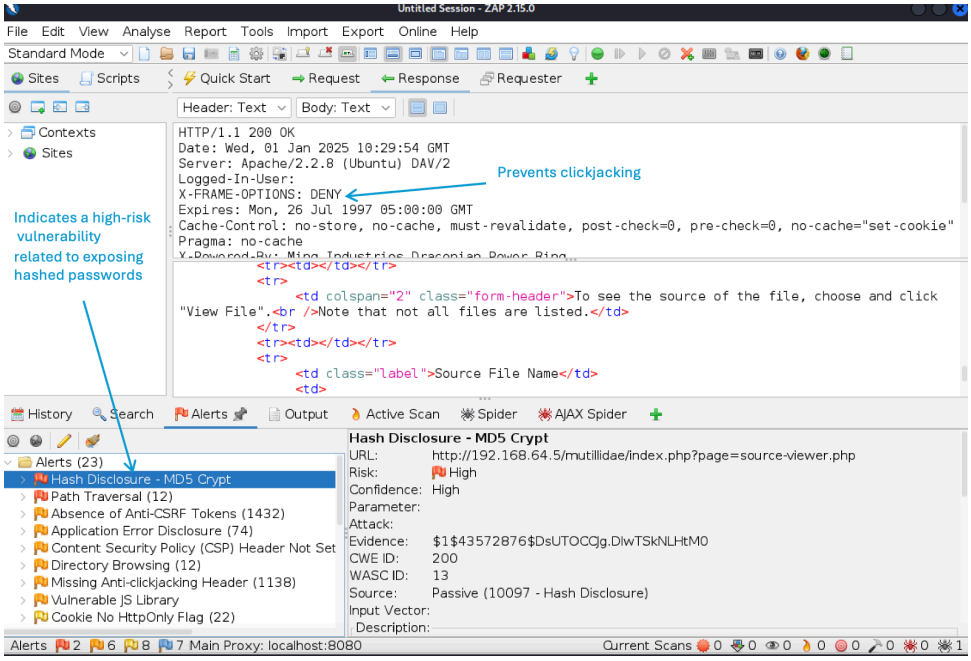
Several high-severity vulnerabilities are found in the OpenVAS results, including backdoor detections, default credentials for all services, and rlogin passwordless login. These flaws make the system vulnerable to data breaches, remote code execution, and illegal access.

OWAS ZAP

Tools and Method:

OWASP ZAP analyses application endpoints using active scanning, AJAX scanning, and automated spidering (Vaishnavi, 2024). By detecting flaws like missing headers, unsafe setups, and injection threats, it produces thorough risk-based reports.

Evidence:



Alert type	Risk	Count
Hash Disclosure - MD5 Crypt	High	1 (4.3%)
Path Traversal	High	12 (52.2%)
Absence of Anti-CSRF Tokens	Medium	1450 (6,304.3%)
Application Error Disclosure	Medium	74 (321.7%)
Content Security Policy (CSP) Header Not Set	Medium	1427 (6,204.3%)
Directory Browsing	Medium	12 (52.2%)
Missing Anti-clickjacking Header	Medium	1140 (4,956.5%)

Critical issue for directory or file exploitation

Application security issue

Absence of CSP

Can expose file structures

Analysis:

Findings from OWASP ZAP highlight serious threats including route traversal and MD5 hash disclosure, which expose private information and make system compromise possible. Missing headers and CSRF tokens are examples of medium hazards that need to be fixed right away.

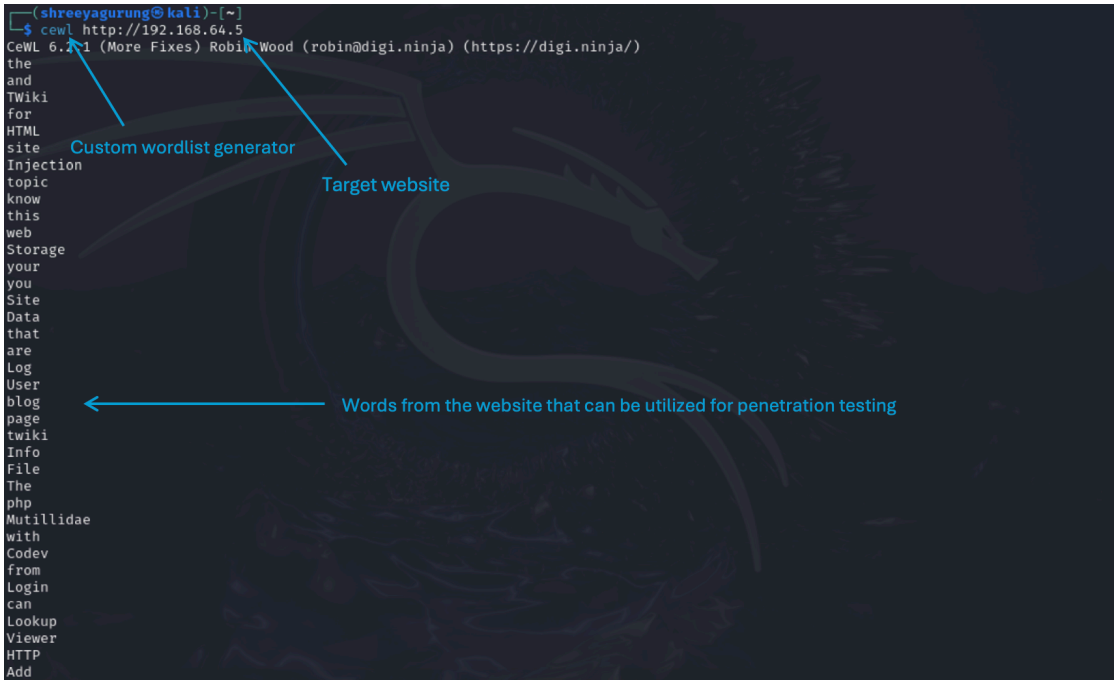
Password Analysis

CeWL

Tools and Method

CeWL analyses the target page (http://192.168.64.5) to create a custom wordlist. Extracted words help with brute-forcing, password cracking, and creating customised penetration test assaults.

Evidence



Analysis:

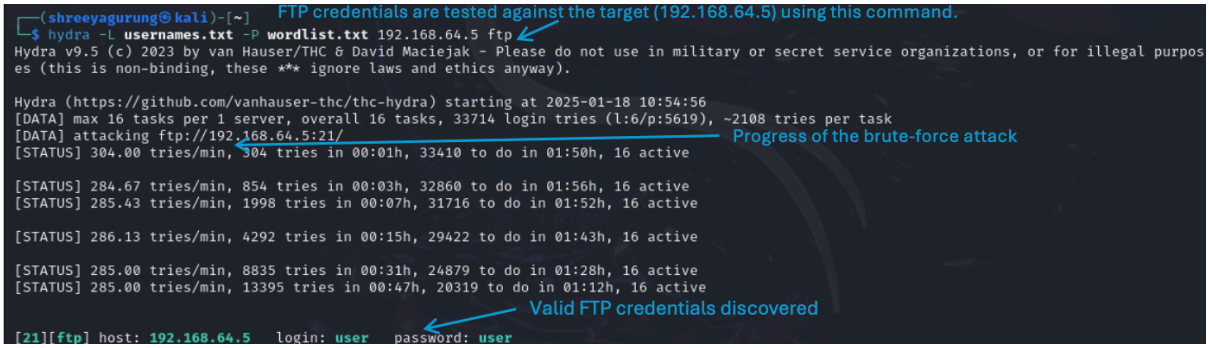
Potential passwords, keywords, or sensitive information can be discovered using extracted website material. For dictionary-based password cracking, brute-force assaults, or spotting trends for specific exploitation, these terms can be essential.

Hydra

Tools and Method:

The target's FTP service (192.168.64.5) was subjected to a brute-force attack using Hydra, which tested password wordlist (wordlist.txt) and username list (usernames.txt) combinations.

Evidence:



Analysis:

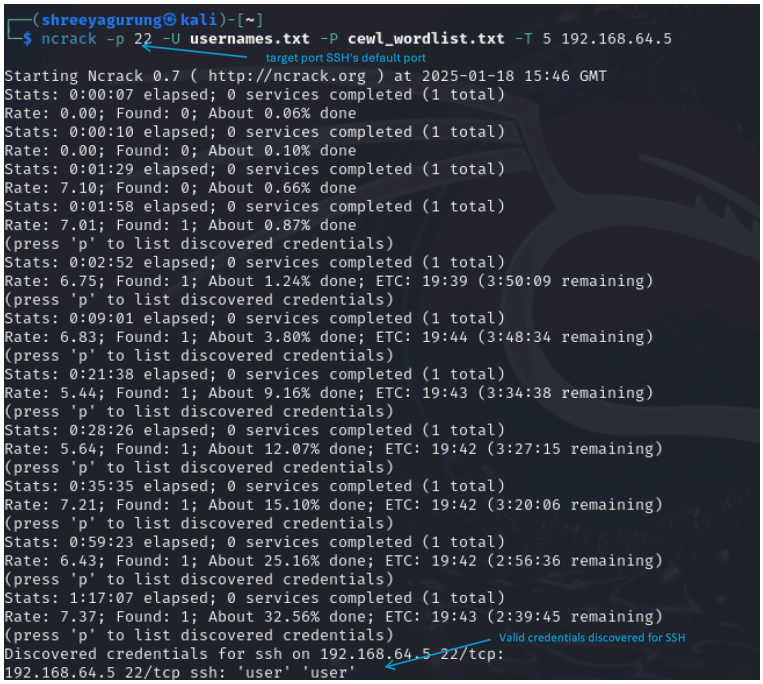
Hydra successfully identified the FTP service's weak default credentials (user:user), exposing the system's susceptibility to brute-force attacks. This indicates inadequate password management, which increases the possibility of malicious file uploads to the server, data leaks, and illegal access.

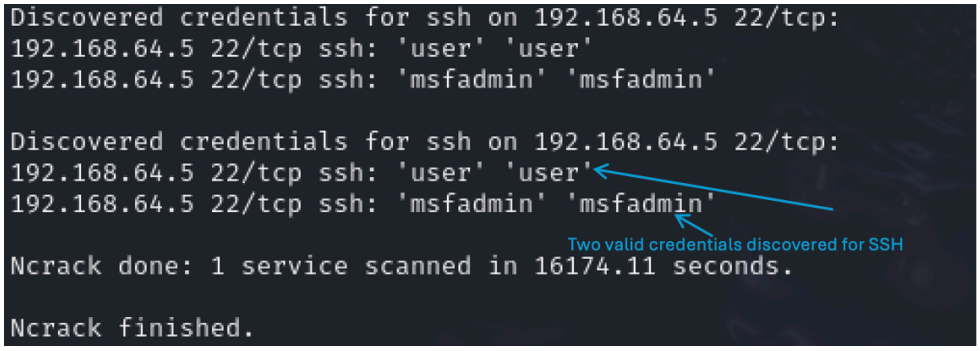
Ncrack

Tools and Method:

Ncrack tests username-password combinations for services like SSH or FTP using brute-force attacks. It does this by using parallel threads and user-provided wordlists to quickly find legitimate credentials (Anto, 2024).

Evidence:





Analysis:

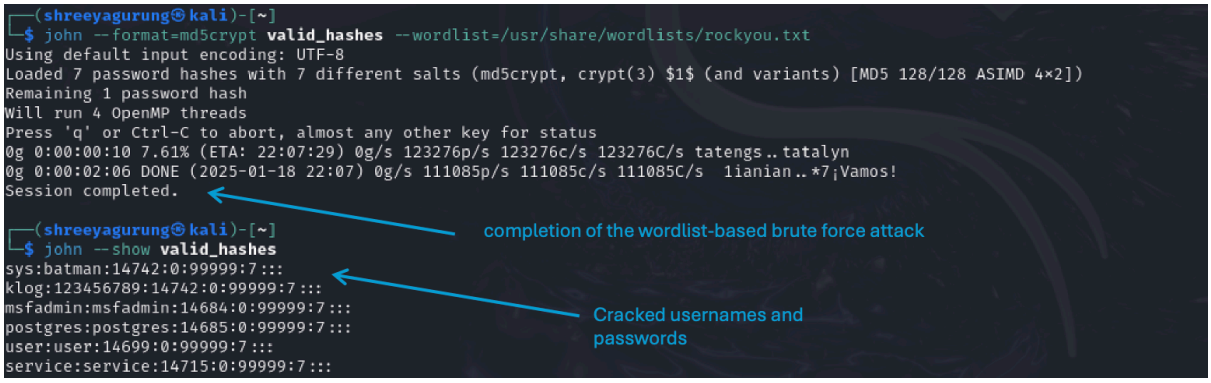
Ncrack identifies weak passwords such as "user:user" and "msfadmin:msfadmin," which reveal inadequate password regulations. Because of these flaws, there is a greater chance of data breaches, system penetration, and lateral attacker movement due to unauthorised access.

John

Tools and Method:

John the Ripper finds weak passwords stored in hashed formats by using dictionary and brute-force assaults, as well as wordlists like rockyou.txt and customisable hash format choices.

Evidence:



Analysis:

Weak credentials such as sys:batman, klog:123456789, msfadmin:msfadmin, postgres:postgres, user:user, and service:service was cracked by John the Ripper, exposing flaws that permit illegal access, data breaches, and system exploitation. To reduce risks, make authentication stronger.

Exploitations

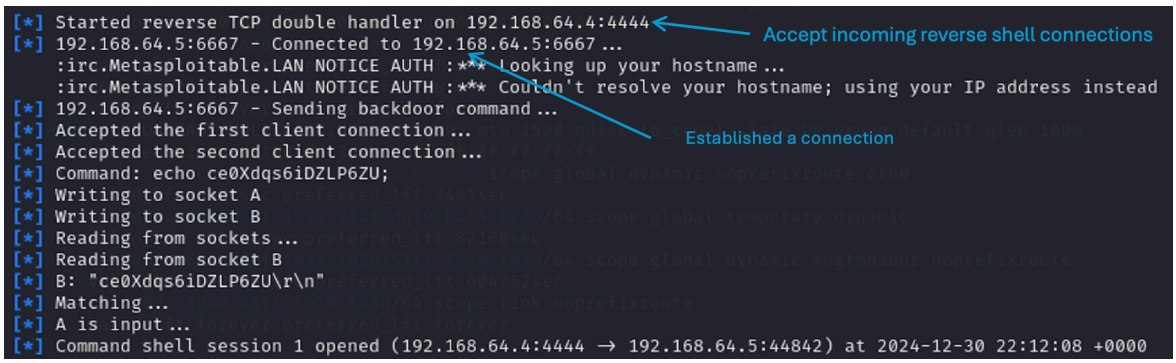
Metasploit Framework

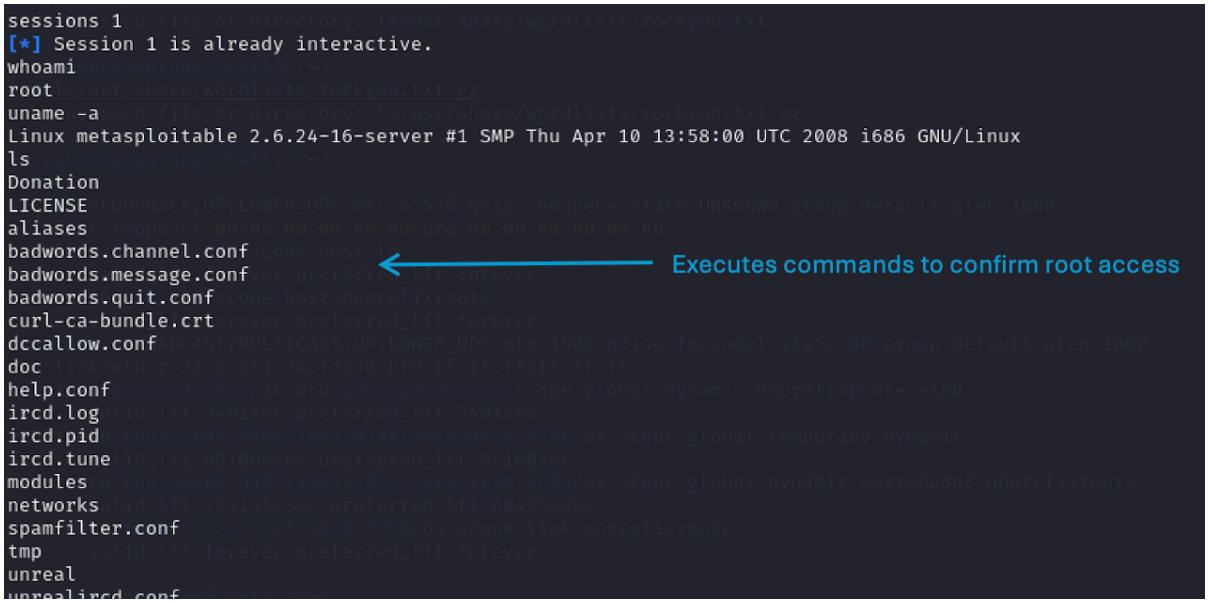
Backdoor

Tools and Method:

By using a reverse TCP payload and Metasploit Framework, the attack was able to take advantage of the target machine's weaknesses and obtain system information by running commands and granting remote shell access.

Evidence:





Analysis:

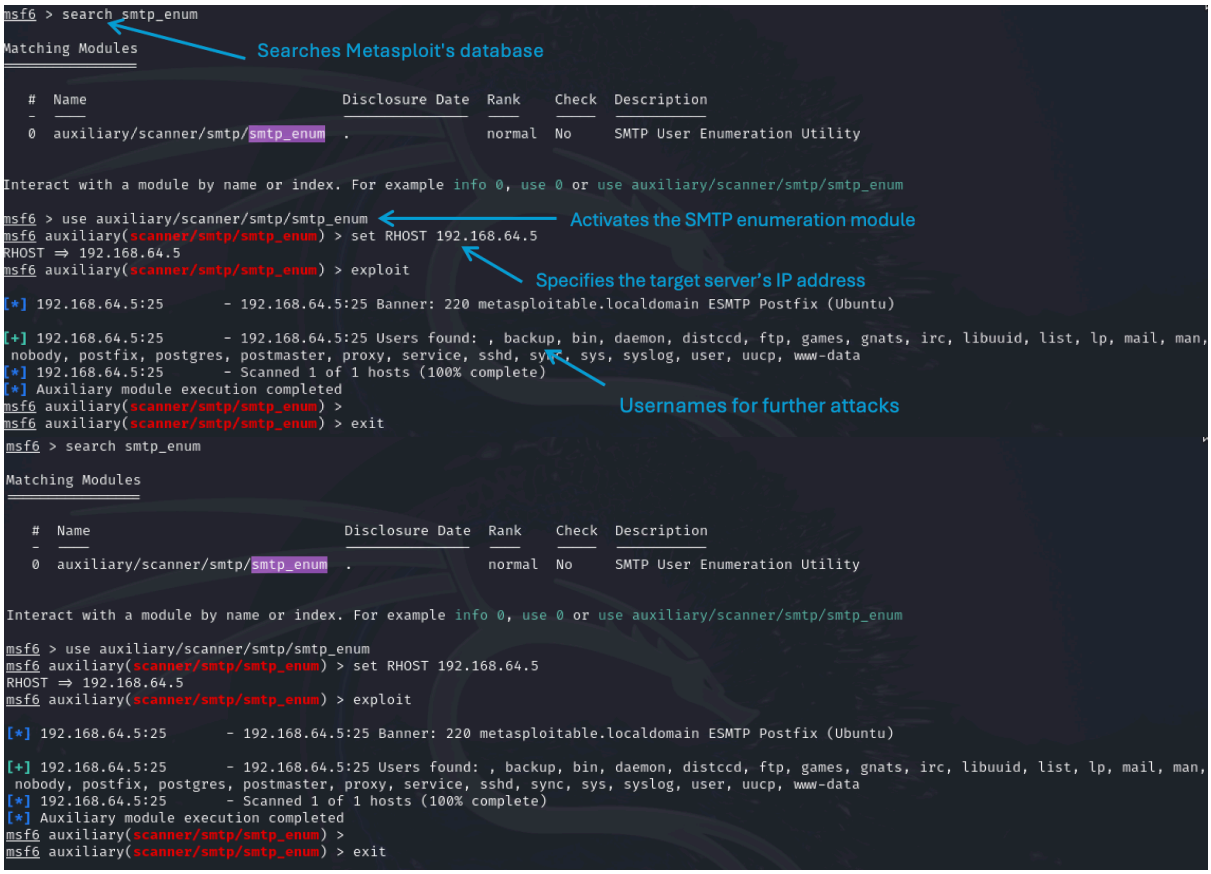
A critical vulnerability was confirmed when the exploit was able to obtain root access on the target computer. File listings demonstrated complete system control, and commands like whoami and uname -a verified access.

SMTP Enumeration

Tools and Method:

SMTP enumeration uses programs like Metasploit, Nmap, Telnet, or SMTPEnum to find legitimate usernames on a server. Sending VRFY/EXPN instructions and examining server answers for user validation are the methods used.

Evidence:




```
msf6 > search smtp_enum

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum    .                normal  No     SMTP User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.64.5
RHOST => 192.168.64.5
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.64.5:25       - 192.168.64.5:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[+] 192.168.64.5:25       - 192.168.64.5:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man,
 nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.64.5:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
msf6 auxiliary(scanner/smtp/smtp_enum) > exit
msf6 > search smtp_enum

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum    .                normal  No     SMTP User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.64.5
RHOST => 192.168.64.5
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.64.5:25       - 192.168.64.5:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[+] 192.168.64.5:25       - 192.168.64.5:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man,
 nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.64.5:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
msf6 auxiliary(scanner/smtp/smtp_enum) > exit
```

Analysis:

Valid SMTP usernames that indicate the existence of accounts on the server are shown by the findings. As a result, there is a chance of unauthorised access and exploitation through the use of brute-force attacks, privilege escalation, or phishing attempts.

Reference

Anto Online, 2024. Ncrack Command-Line Cheat Sheet. [online. Available at: https://anto.online/ncrack-network-authentication-cracking-cheat-sheet/ [Accessed 18 January 2025].

Evalian®, 2024. *What is a penetration test and when should you get one?*, [Image], Evalian®. Available at: https://evalian.co.uk/what-is-a-penetration-test/ [Accessed 1 January 2025]

GeeksforGeeks, 2021. Dmitry – Passive Information Gathering Tool in Kali Linux. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/dmitry-passive-information-gathering-tool-in-kali-linux/ [Accessed 15 January 2025].

Pentest Lab, 2012. SMTP User Enumeration. [online] Available at: https://pentestlab.blog/2012/11/20/smtp-user-enumeration/ [Accessed 18 January 2025].

Vaishnavi, 2024. *Best Practices for Using OpenVAS in Vulnerability Assessment | Overview, Features, and Why Ethical Hackers Should Use It.* [online] WebAsha. Available at: https://www.webasha.com/blog/best-practices-for-using-openvas-in-vulnerability-assessment-overview-features-and-why-ethical-hackers-should-use-it [Accessed 15 January 2025].

Vaishnavi, 2024. *OWASP ZAP | Overview, Features, and How Ethical Hackers Use It for Web Application Security Testing*. [online] WebAsha. Available at: https://www.webasha.com/blog/owasp-zap-overview-features-and-how-ethical-hackers-use-it-for-web-application-security-testing#:~:text=OWASP%20ZAP%20is%20an%20open-source%20web%20application%20security,designed%20to%20find%20security%20vulnerabilities%20in%20web%20applications[Accessed 16 January 2025].

Yasani, R., 2015. Introduction to OpenVAS: Open-Source Vulnerability Scanning. [online] Kali Linux Tutorials. Available at: https://kalilinuxtutorials.com/introduction-to-openvas-open-source-vulnerability-scanning/#:~:text=OpenVAS%20is%20a%20full-featured%20vulnerability%20scanner%20that%20is,identifying%20vulnerabilities%20that%20could%20be%20exploited%20by%20attackers[Accessed 15 January 2025].

Yen, L., 2024. *Nmap Vulnerability Scan: How to Easily Run and Assess Risk. [online] Datamation*. Available at: https://www.datamation.com/security/how-to-easily-run-a-vulnerability-scan-using-nmap/ [Accessed 15 January 2025.

Appendices

Table 1: Port Vulnerabilities

Open Ports	Service	Potential Vulnerabilities
21	FTP	Unencrypted communication and brute force attacks
22	SSH	Weak Credentials, Outdated SSH version
23	Telnet	Unencrypted communication, Outdated Protocol
25	SMTP	Open relay, Spoofing
53	DNS	DNS amplification attack, Misconfigured zone transfer
80	HTTP	Outdated web server, cross-site scripting (XSS)
111	RPCBind	Unauthorized access, Information Leakage
139	NetBIOS-SSN	SMB vulnerabilities, Lateral movement
445	Microsoft-DS	SMBv1 vulnerabilities (EternalBlue). Unauthorized access
512	Exec	Unauthorized remote execution
513	Login	Weak Authentication, information disclosure
514	Shell	Remote code execution, weak authentication
1099	RMI Registry	Java RMI exploits, Unauthorized access
1524	Ingreslock	Backdoor Access
2049	NFS	Unauthorized file access, weak permissions
3306	MySQL	Weak Credentials, SQL injection
5432	PostgreSQL	Weak Credentials, SQL injection
5900	VNC	Unauthorized access, Weak authentication
6000	X11	Remote desktop hijacking information disclosure
6667	IRC	Flood attacks and Unauthorized usage

8009	AJP13	Path traversal, remote code execution