

# Lab - Scanning for WannaCry Ransomware

## Overview

EternalBlue, sometimes written as ETERNALBLUE, is an exploit believed to have been developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on April 14, 2017, and was used as part of the worldwide WannaCry ransomware attack on May 12, 2017.

EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. CVE-2017-0144 denotes this vulnerability in the Common Vulnerabilities and Exposures (CVE) catalog. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows accepts specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.

## Lab Requirements

- Virtual install of Kali Linux up and running
- Virtual install of Windows XP unpatched up and running and on the same network as the Kali machine

## Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. Those scripts are executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap or write their own to meet their custom needs.

In this lab, students will download and save the smb-vuln-ms17-010.nse Nmap script and conduct a network scan for unpatched Windows machines vulnerable to the WannaCry ransomware attack.

## Begin the Lab!

1. Download the needed script from <https://nmap.org/nse/doc/scripts/smb-vuln-ms17-010.html>

## File smb-vuln-ms17-010

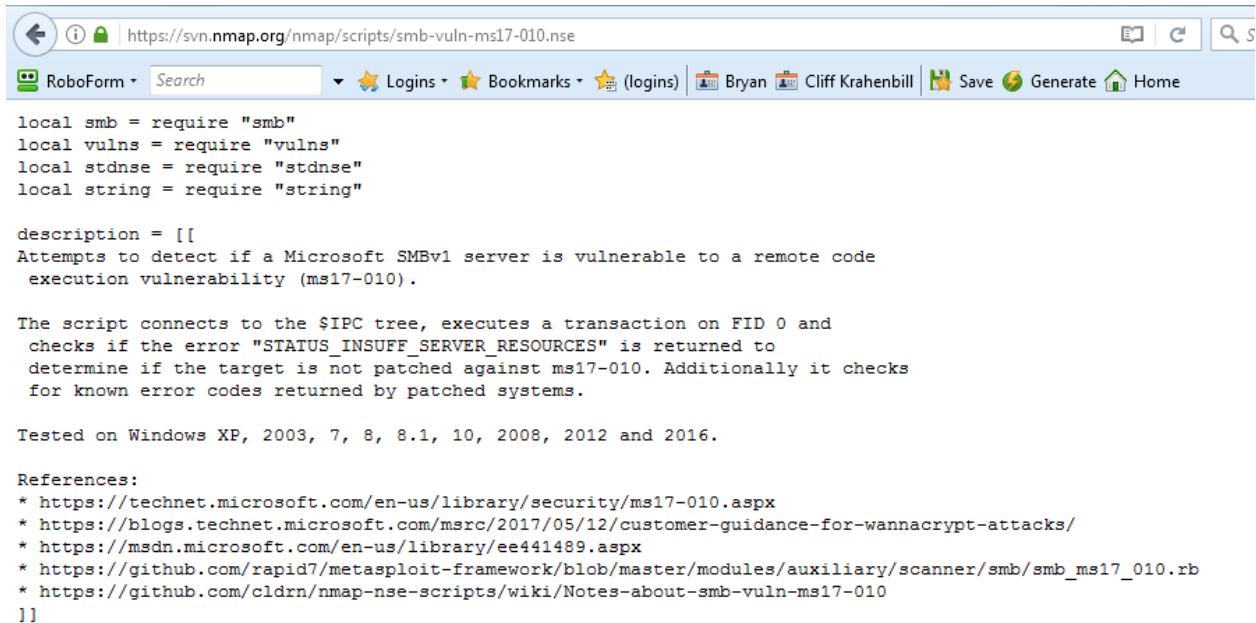
Script types: *hostrule*

Categories: *vuln, safe*

Download: <https://svn.nmap.org/nmap/scripts/smb-vuln-ms17-010.nse>

Click on the download link and on the next page, highlight and copy the contents of the script.

1. To highlight the contents, click anywhere inside the web page, hold down the Ctrl key and hit the 'a' key one time (Ctrl+a)
2. Next, hold down the Ctrl key and hit the 'c' key (Ctrl+c) to copy the contents.



The screenshot shows a web browser window with the address bar displaying `https://svn.nmap.org/nmap/scripts/smb-vuln-ms17-010.nse`. The browser's toolbar includes a search bar, a 'Logins' dropdown, a 'Bookmarks' dropdown, and a '(logins)' dropdown. The main content area displays the Nmap script `smb-vuln-ms17-010.nse`. The script is written in Ruby and includes a description, a list of references, and a list of tested operating systems.

```
local smb = require "smb"
local vulns = require "vulns"
local stdnse = require "stdnse"
local string = require "string"

description = [[
Attempts to detect if a Microsoft SMBv1 server is vulnerable to a remote code
execution vulnerability (ms17-010).

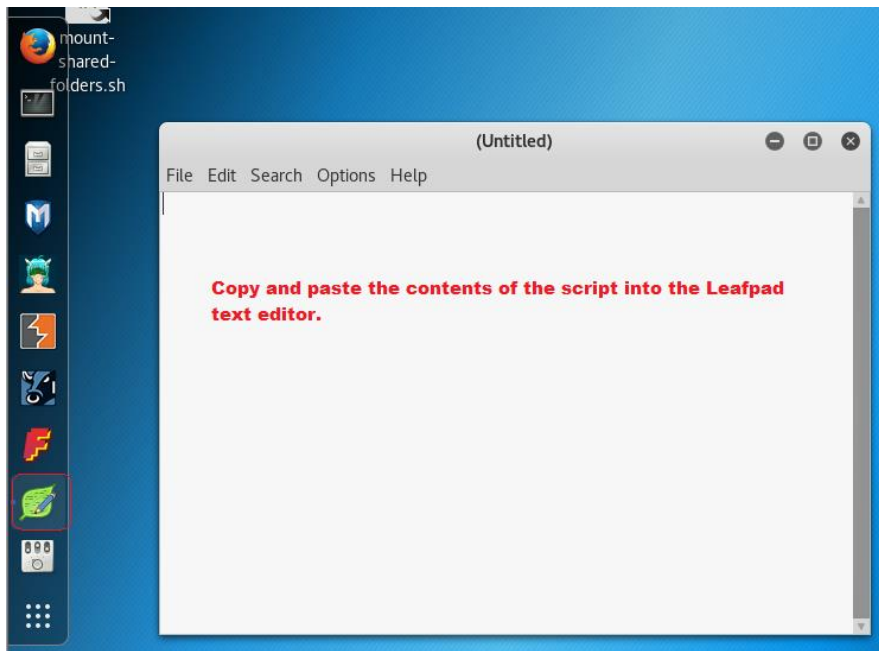
The script connects to the $IPC tree, executes a transaction on FID 0 and
checks if the error "STATUS_INSUFF_SERVER_RESOURCES" is returned to
determine if the target is not patched against ms17-010. Additionally it checks
for known error codes returned by patched systems.

Tested on Windows XP, 2003, 7, 8, 8.1, 10, 2008, 2012 and 2016.

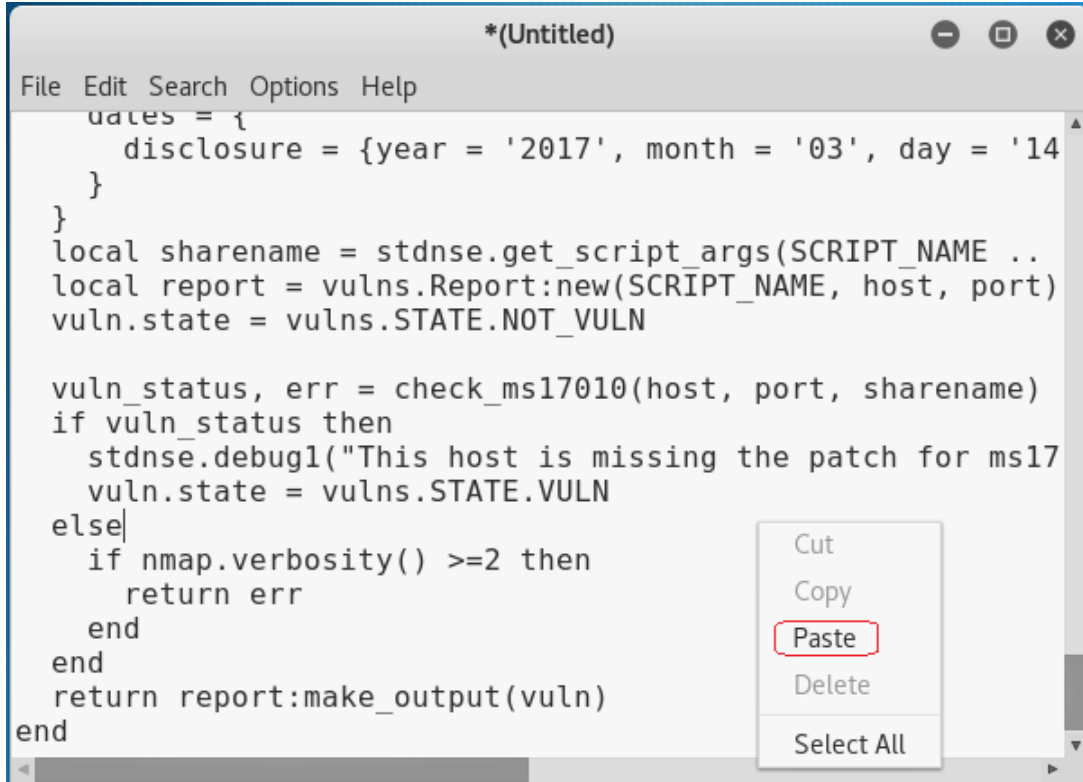
References:
* https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
* https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
* https://msdn.microsoft.com/en-us/library/ee441489.aspx
* https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb
* https://github.com/cldrn/nmap-nse-scripts/wiki/Notes-about-smb-vuln-ms17-010
]]
```

(Content was cut short)

Next, from your Kali desktop application launcher, open your Leafpad text editor. Right-click on the white space of the text page and from the connect menu, select paste.



Paste the script contents into the editor:



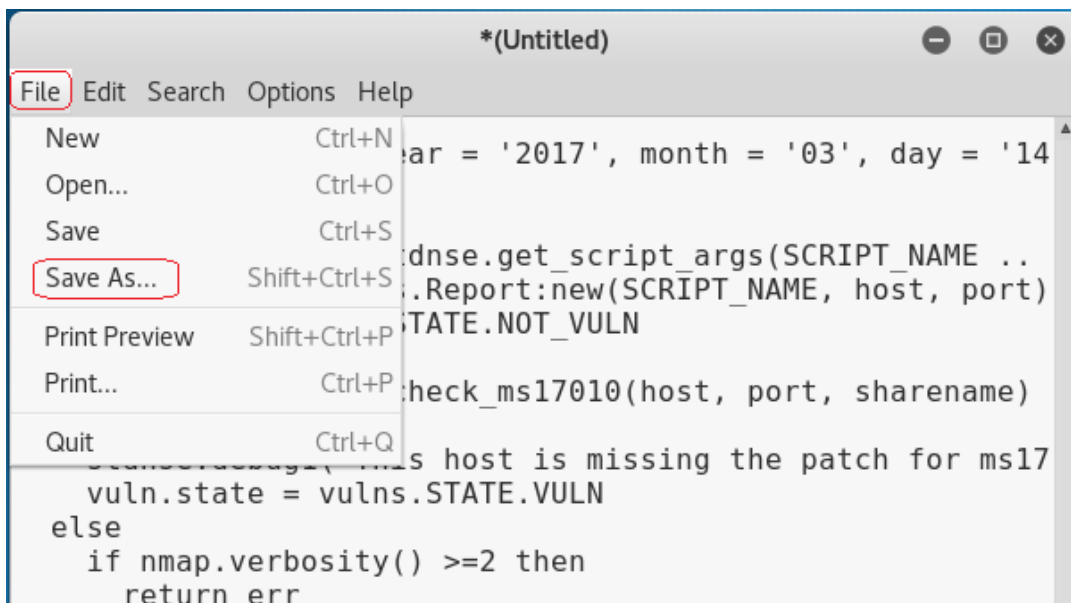
```
*(Untitled)
File Edit Search Options Help
dates = {
  disclosure = {year = '2017', month = '03', day = '14'
}
}
local sharename = stdnse.get_script_args(SCRIPT_NAME ..
local report = vulns.Report:new(SCRIPT_NAME, host, port)
vuln.state = vulns.STATE.NOT_VULN

vuln_status, err = check_ms17010(host, port, sharename)
if vuln_status then
  stdnse.debug1("This host is missing the patch for ms17
  vuln.state = vulns.STATE.VULN
else
  if nmap.verbosity() >=2 then
    return err
  end
end
return report:make_output(vuln)
end
```

Cut  
Copy  
**Paste**  
Delete  
Select All

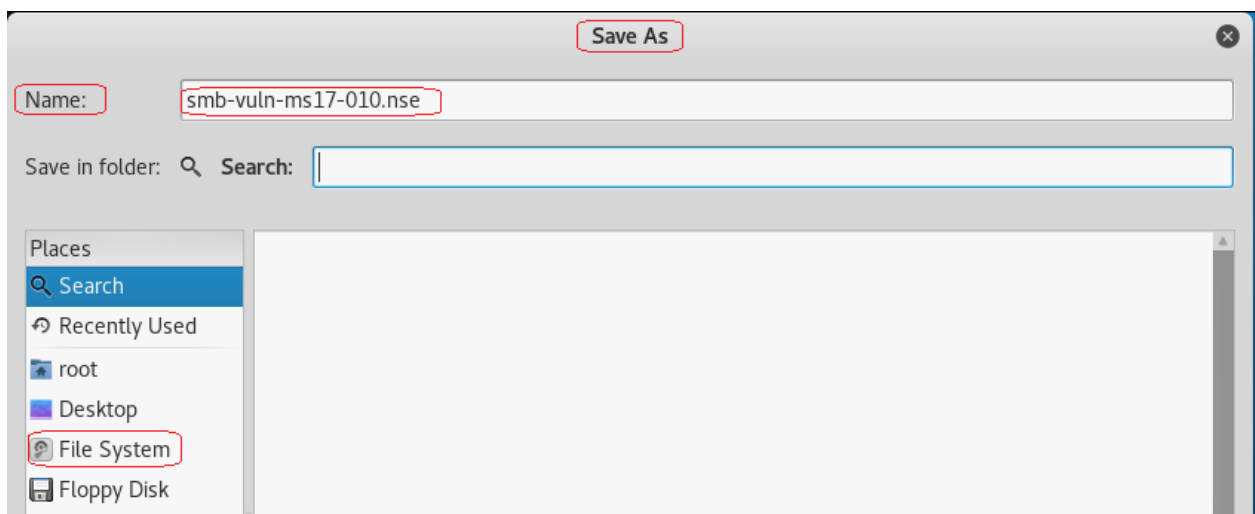
We next need to save the script to the nmap script folder inside the Kali file system.

From the Leafpad file menu, select Save As,

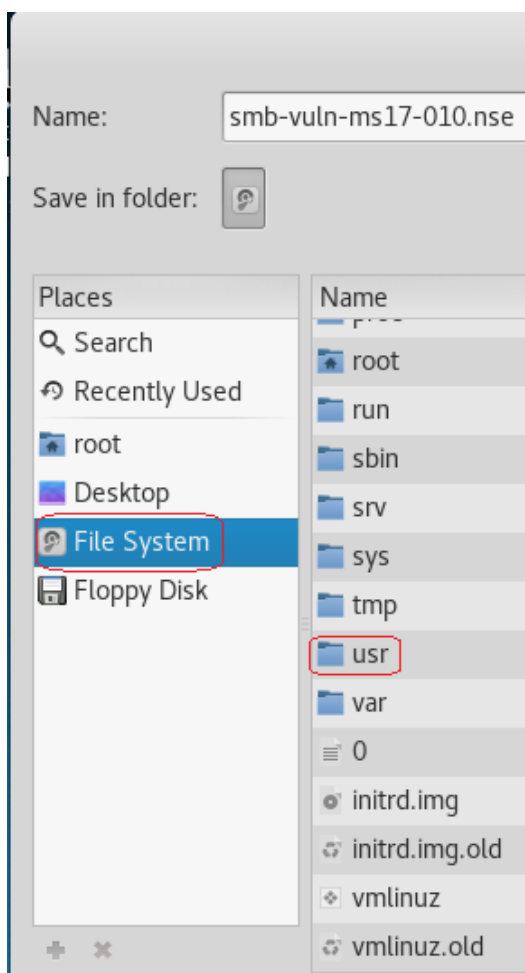


```
*(Untitled)
File Edit Search Options Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As... Shift+Ctrl+S
Print Preview Shift+Ctrl+P
Print... Ctrl+P
Quit Ctrl+Q
ar = '2017', month = '03', day = '14
dse.get_script_args(SCRIPT_NAME ..
.Report:new(SCRIPT_NAME, host, port)
STATE.NOT_VULN
check_ms17010(host, port, sharename)
This host is missing the patch for ms17
vuln.state = vulns.STATE.VULN
else
  if nmap.verbosity() >=2 then
    return err
```

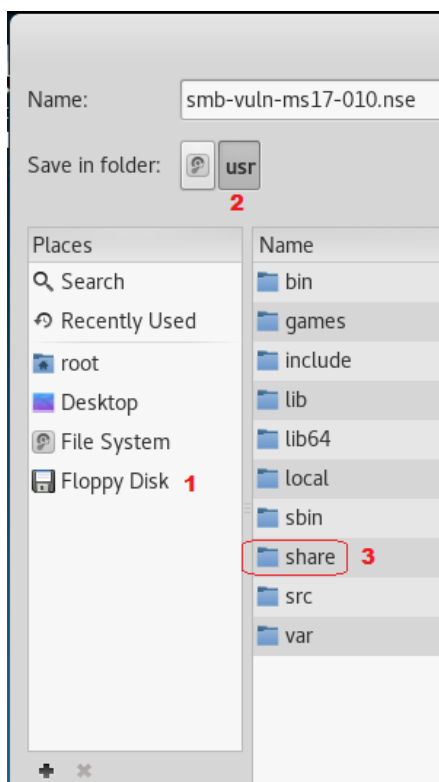
Important! Save the script using the file name of **smb-vuln-ms17-010.nse**



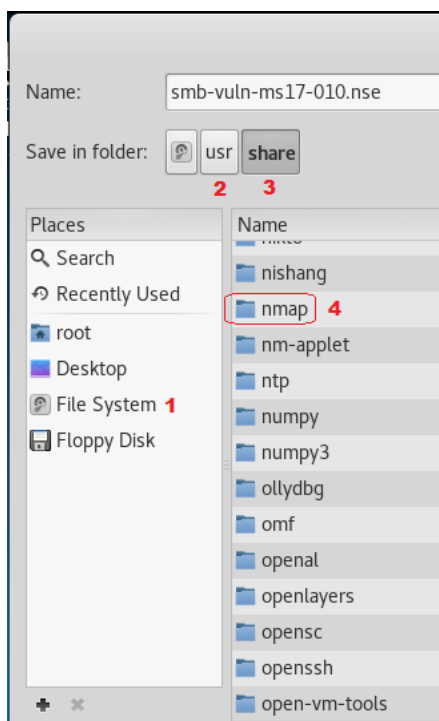
Next, under Places click on File System, scroll down to the USR folder, click to open.



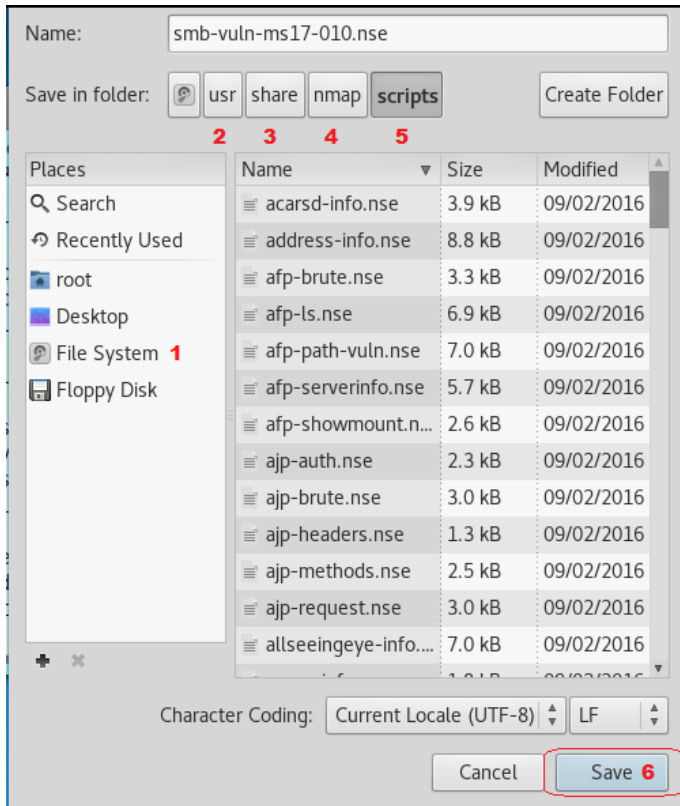
Inside the USR folder, click on the **share** folder.



Inside the **share** folder, scroll down, find, and click on **nmap**



Inside the **nmap** folder, click on the **scripts** folder, click on the **save** button. Script is now saved in the **Nmap/script folder**



We are now ready to run the script and check our network for the ExternalBlue vulnerability.

For this next part of the lab, I have checked my Kali and my Windows XP victim to ensure they are both on the same network. I need the network IP to be able to scan for the vulnerability, and I need to ensure that all my devices can see each other.

This is the network IP for my Kali:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.145.132 netmask 255.255.255.0 broadcast 192.168.145.255  
    inet6 fe80::20c:29ff:fe3d:d396 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:3d:d3:96 txqueuelen 1000 (Ethernet)  
    RX packets 485 bytes 73835 (72.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1622 bytes 101552 (99.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

This is the network IP from my Windows XP:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 7:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . : 192.168.145.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.145.2

C:\Documents and Settings\IEUser>
```

Both my machines are on the same network. Your network IP may differ. This is my network IP, not yours.

From the Kali desktop, open a new terminal and type the following command:

```
nmap -p445 --script smb-vuln-ms17-010 <target>
```

My target is 192.168.145.0/24. I am scanning all 254 IP address on my network.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -Pn -p445 --script smb-vuln-ms17-010 192.168.145.0/24
```

Your target may differ. Hit enter.

```
root@kali: ~
File Edit View Search Terminal Help

Nmap scan report for 192.168.145.129
Host is up (0.00078s latency).
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:FB:60:D0 (VMware)

Host script results:
| 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
```



I found one machine (my XP victim). We now need to see if we can exploit the vulnerability using Metasploit.

Take note of the vulnerable IP address. For me, that would be 192.168.145.129.

### Ensure your system is updated!

Open a new terminal and type: `apt-get update && apt-get upgrade`

Next, ensure that Metasploit is completely updated by typing: `msfupdate`

After the updates have completed, you can see if the `smb_ms17_010` is present by typing `search smb_ms17_010`. Success!

```
      =[ metasploit v4.14.23-dev ]
+ -- --=[ 1657 exploits - 949 auxiliary - 293 post ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search smb_ms17_010
[!] Module database cache not built yet, using slow search

Matching Modules
=====
   Name                                     Disclosure Date  Rank   Description
   ----                                     -
auxiliary/scanner/smb/smb_ms17_010         normal          MS17-010 SMB RCE
Detection

msf > 
```

We are now ready to launch the exploit at our victim.

Type the following commands one at a time and hit enter:

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.145.0/24 (My
network IP, not yours!)
msf auxiliary(smb_ms17_010) > set THREATS 10
msf auxiliary(smb_ms17_010) > run
```

Note that Metasploit scans the network in blocks giving you a readout of where it is in the scan process

The output states that my victim is likely vulnerable to ms17\_010.



```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(smb_ms17_010) > set RHOSTS 192.168.145.0/24
RHOSTS => 192.168.145.0/24
msf auxiliary(smb_ms17_010) > set THREATS 10
THREATS => 10
msf auxiliary(smb_ms17_010) > run

[*] Scanned 26 of 256 hosts (10% complete)
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 77 of 256 hosts (30% complete)
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 128 of 256 hosts (50% complete)
[+] 192.168.145.129:445 - Host is likely VULNERABLE to MS17-010! (Windows 5.1)
[*] Scanned 154 of 256 hosts (60% complete)
```

## Summary –

In this lab, students learned how to import a Nmap script to the Nmap script folder. The take away is that specific scripts available for a specific vulnerability, and when a new threat such as a ransomware attack or any attack threatens our network security, someone will write a Nmap script and that script will be made available to the Nmap community.