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!

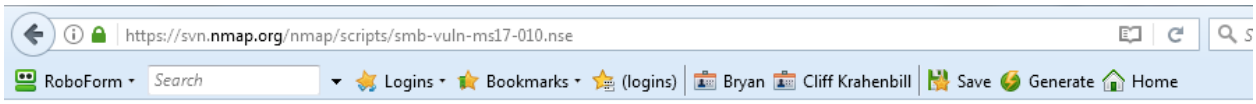
1. Download the needed script from **https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html**

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.

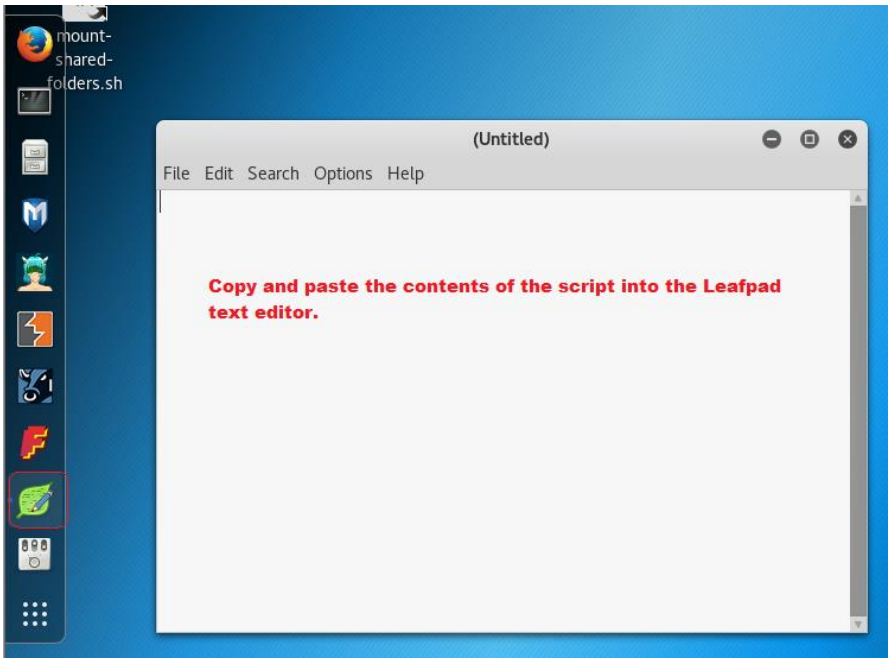
1. To highlight the contents, click anywhere inside the web page, hold down the Ctrl key and hit the 'a' key one time (Ctrl+a)
2. Next, hold down the Ctrl key and hit the 'c' key (Ctrl+c) to copy the contents.



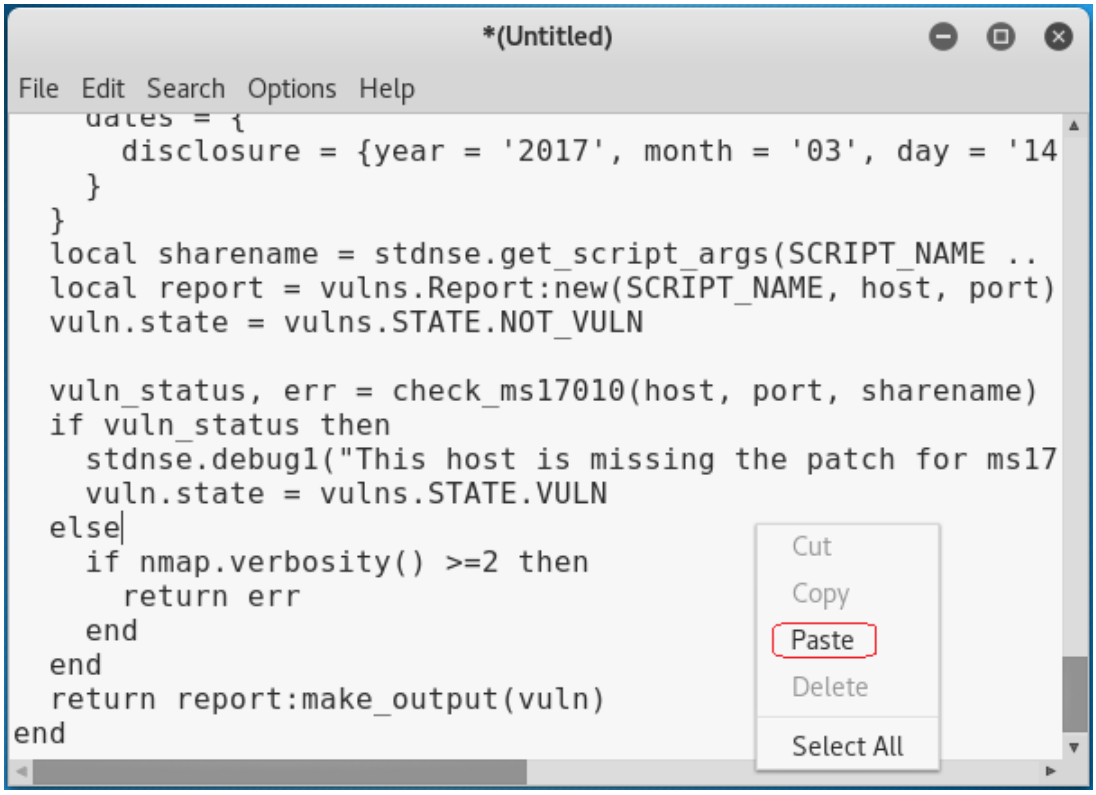

```
local smb = require "smb"
local vulns = require "vulns"
local stdnse = require "stdnse"
local string = require "string"

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.

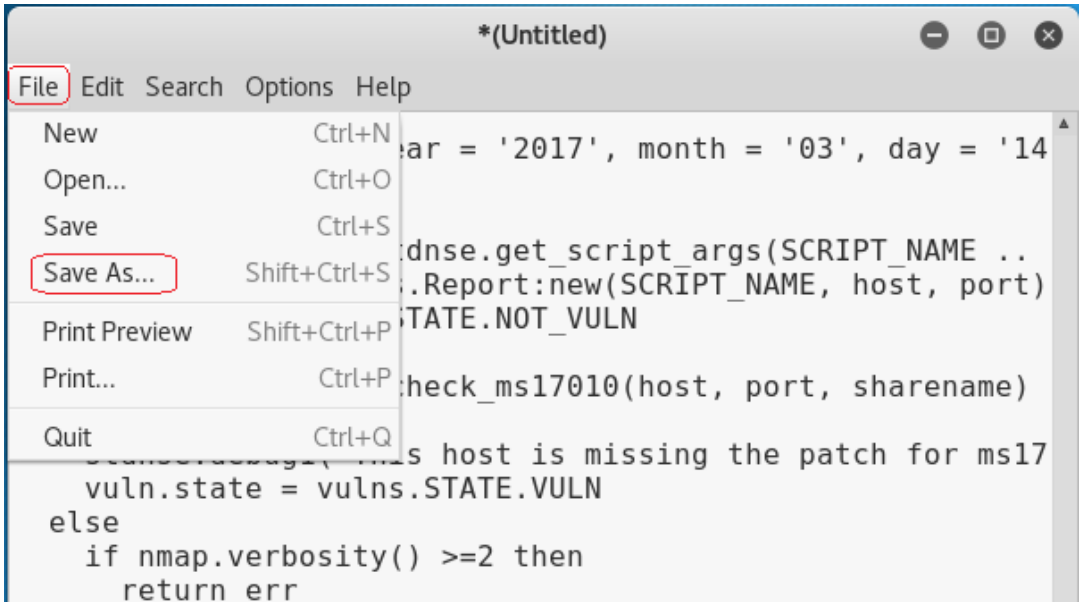


Paste the script contents into the editor:

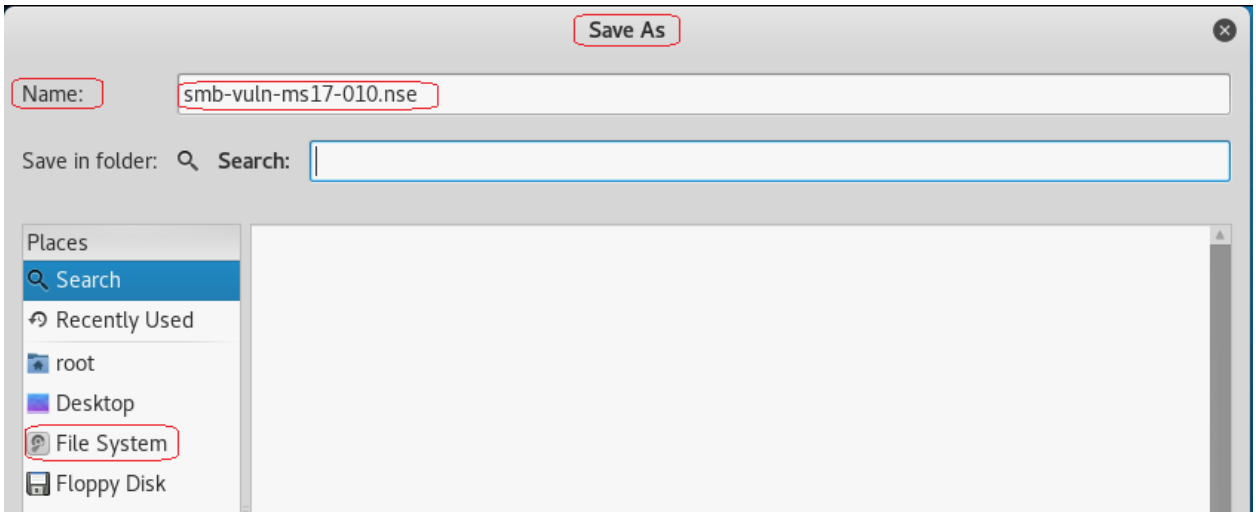


We next need to save the script to the nmap script folder inside the Kali file system.

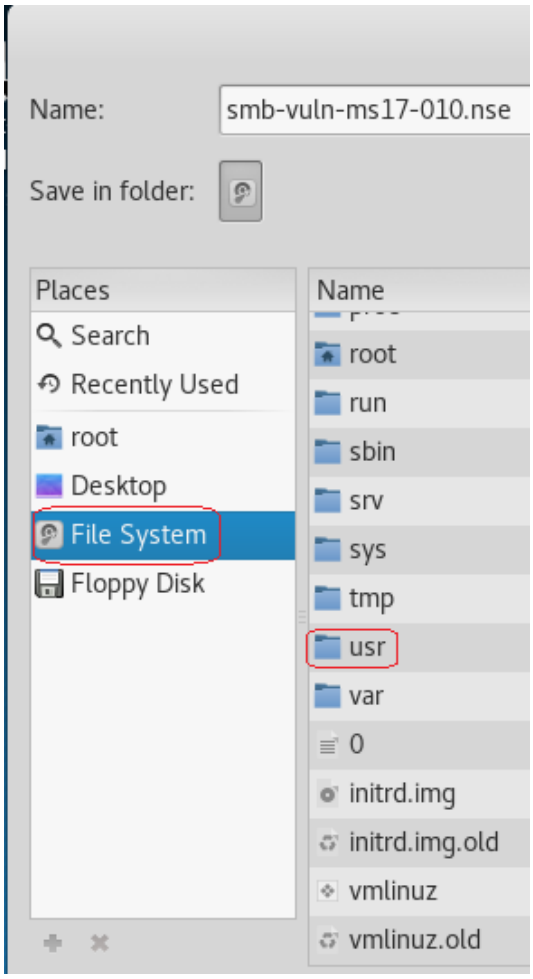
From the Leafpad file menu, select Save As,



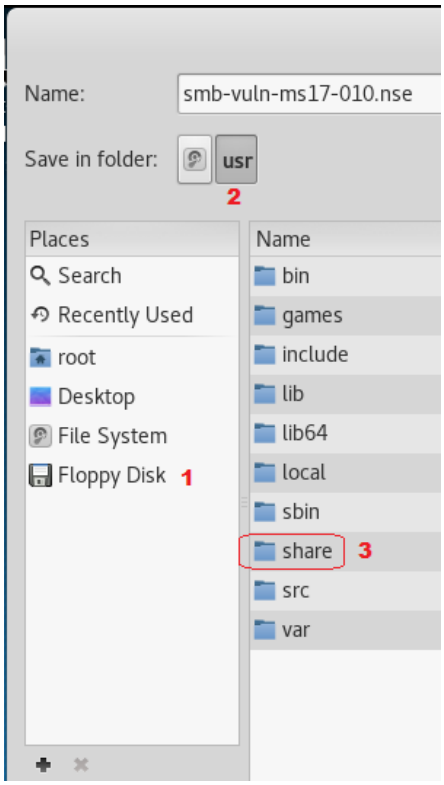
Important! Save the script using the file name of **smb-vuln-ms17-010.nse**



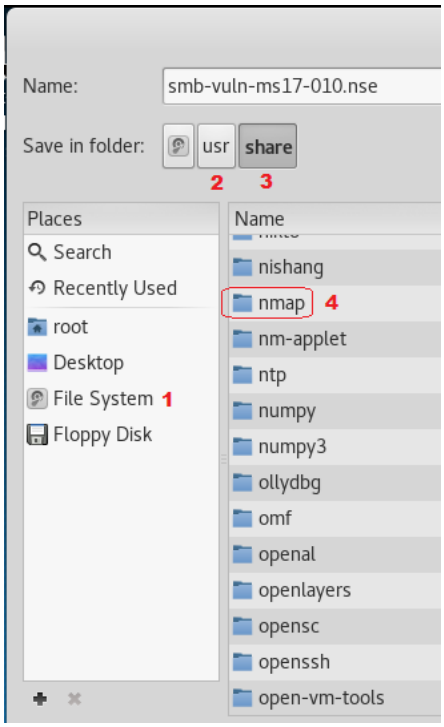
Next, under Places click on File System, scroll down to the USR folder, click to open.



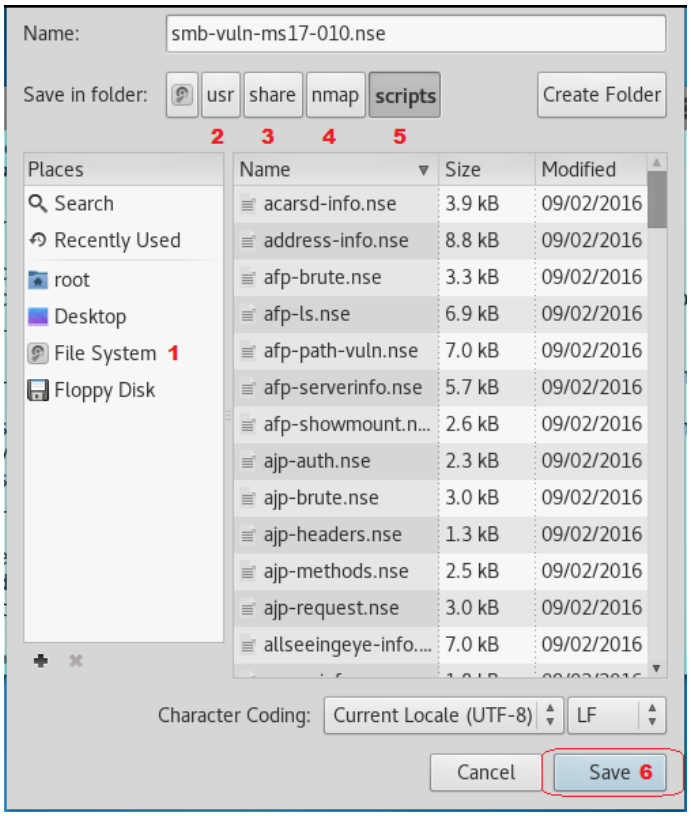
Inside the USR folder, click on the **share** folder.



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



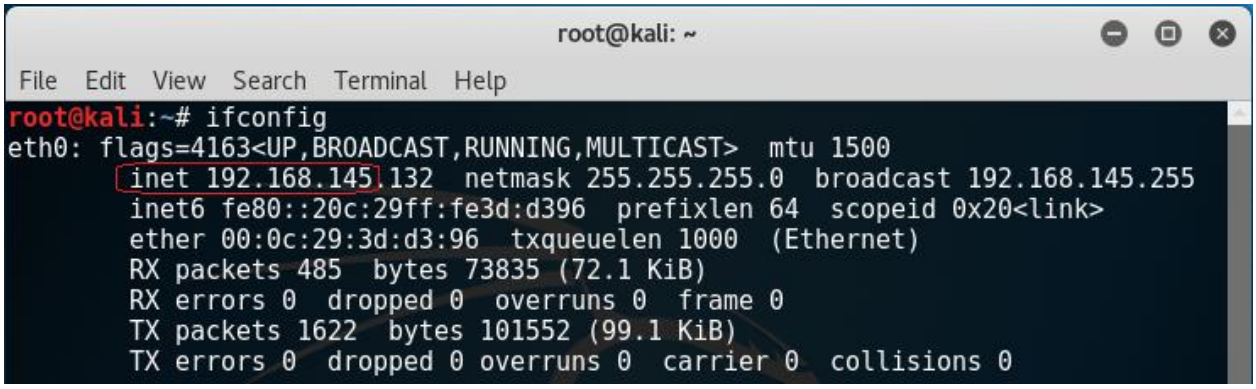
Inside the **nmap** folder, click on the **scripts** folder, click on the **save** button. Script is now saved in the **Nmap/script folder**



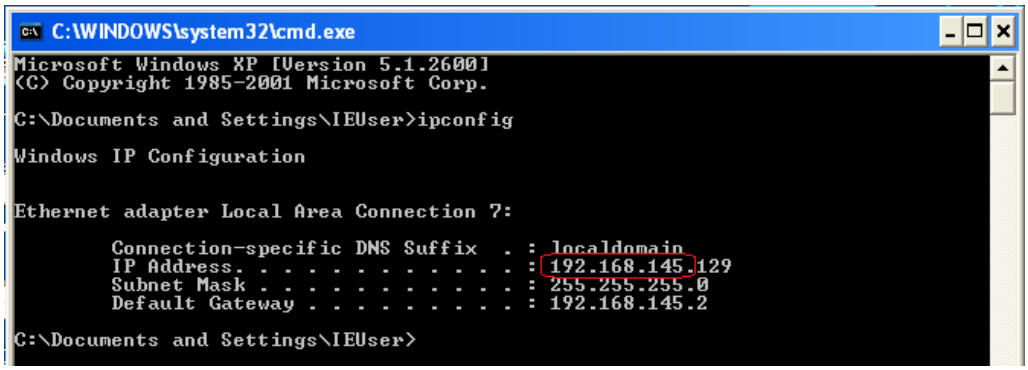
We are now ready to run the script and check our network for the ExternalBlue vulnerability.

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:



This is the network IP fro my Windows XP:

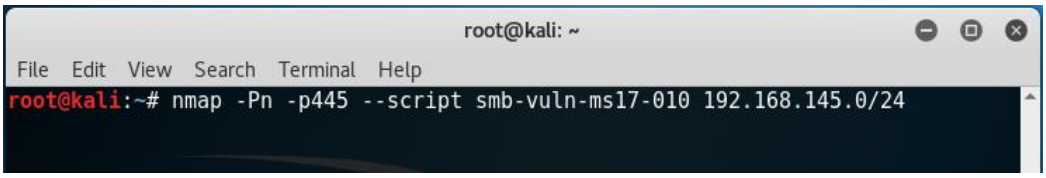


Both my machines are on the same network. Your network IP may differ. This is my network IP, not yours.

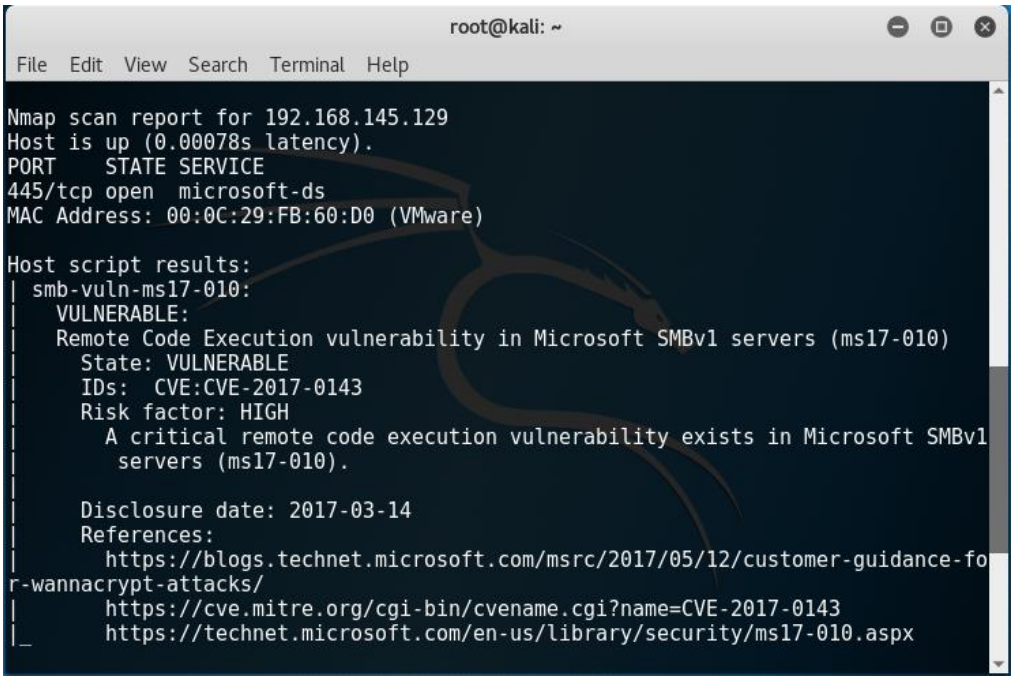
From the Kali desktop, open a new terminal and type the following command:

```
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.



Your target may differ. Hit enter.



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 likelily 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.