**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.

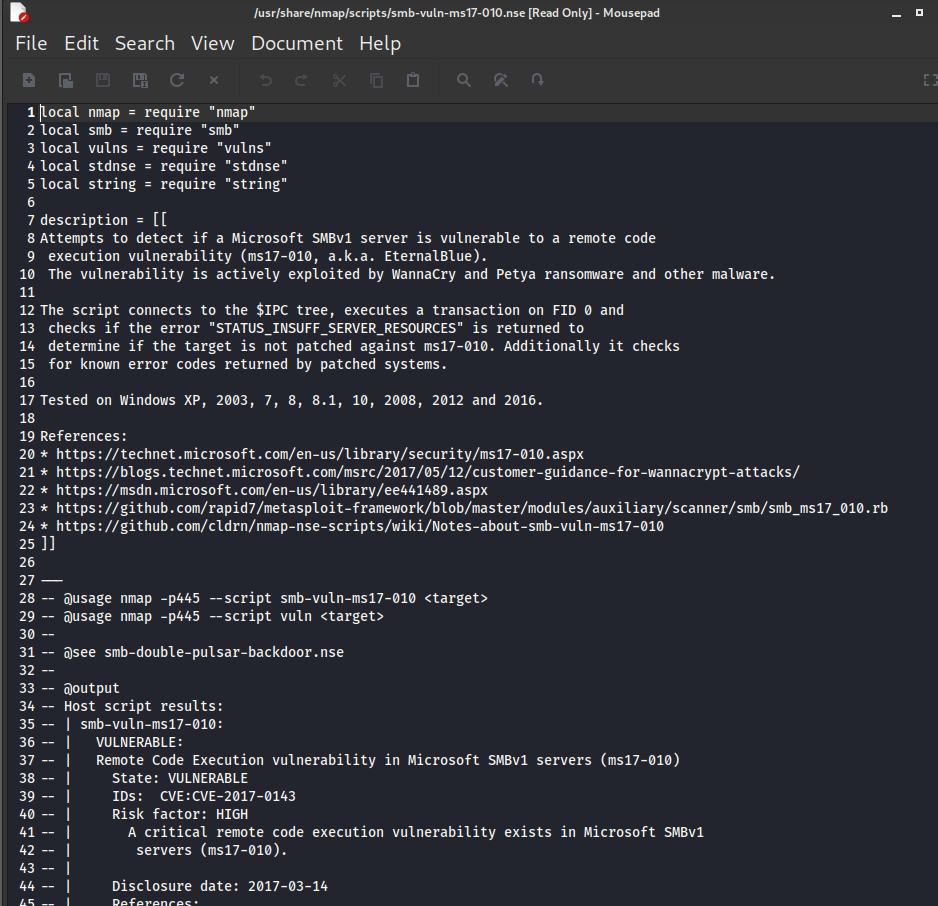
# Nmap Scripting Engine (NSE)

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.

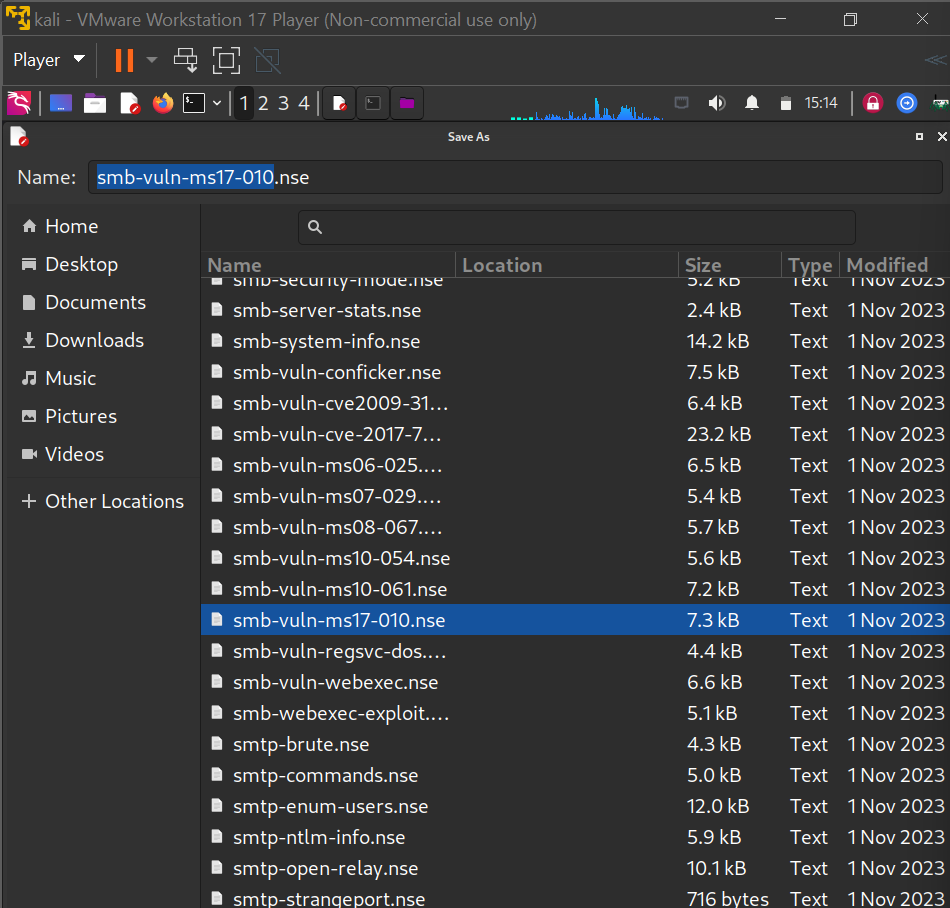
In this lab, students will download and save the smb-vuln-ms17-010.nse Nmap script and conduct a network scan for unpatched Windows machines vulnerable to the WannaCry ransomware attack.

**Begin the Lab!**

1. Download the needed script from [**https://nmap.org/nsedoc/scripts/smb-vuln-ms17010.html**](https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html)

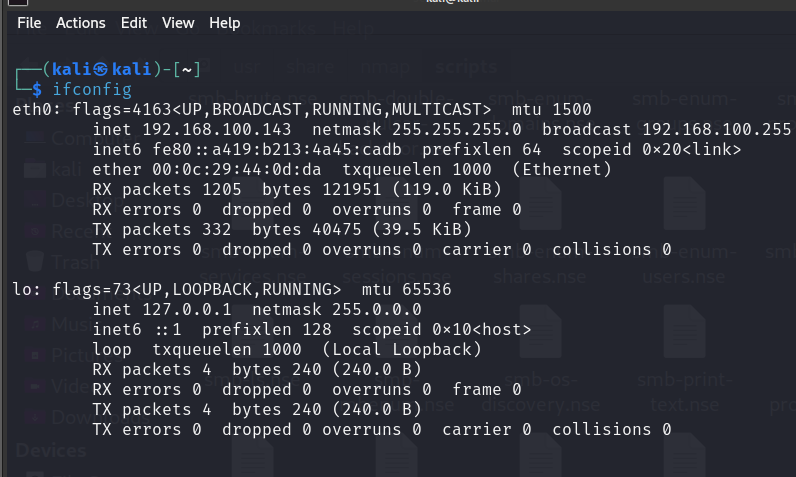


Inside the **nmap** folder, click on the **scripts** folder, click on the **save** button. Script is now saved in the **Nmap/script folder**

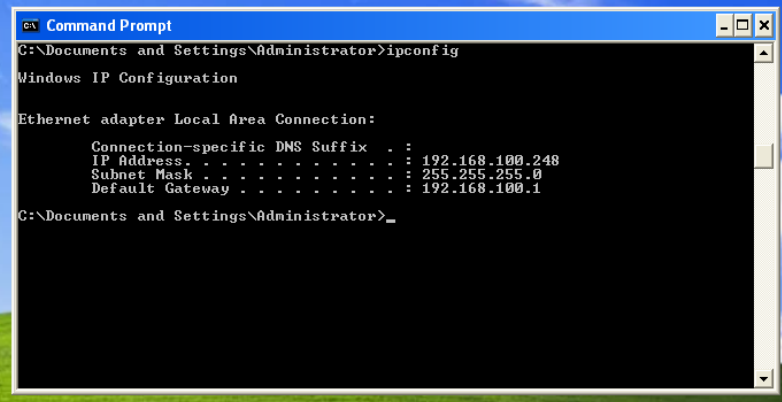


We are now ready to run the script and check our network for the ExternalBlue vulnerability.

This is the network IP for my Kali:



This is the network IP fro my Windows XP:



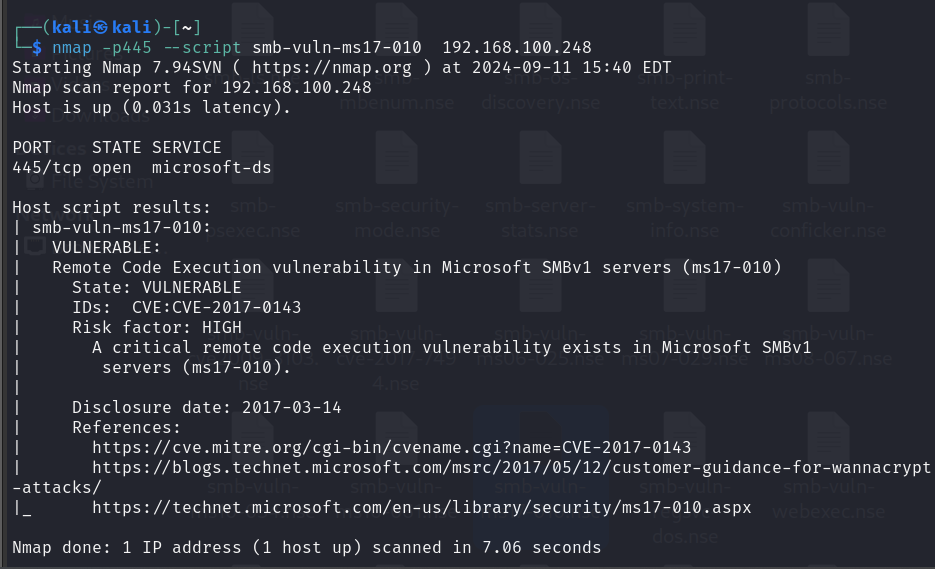
|  |  |
| --- | --- |
| Both my machines are on the same network. Your network IP may differ. This is my network | |
| IP, not yours. |  |

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.

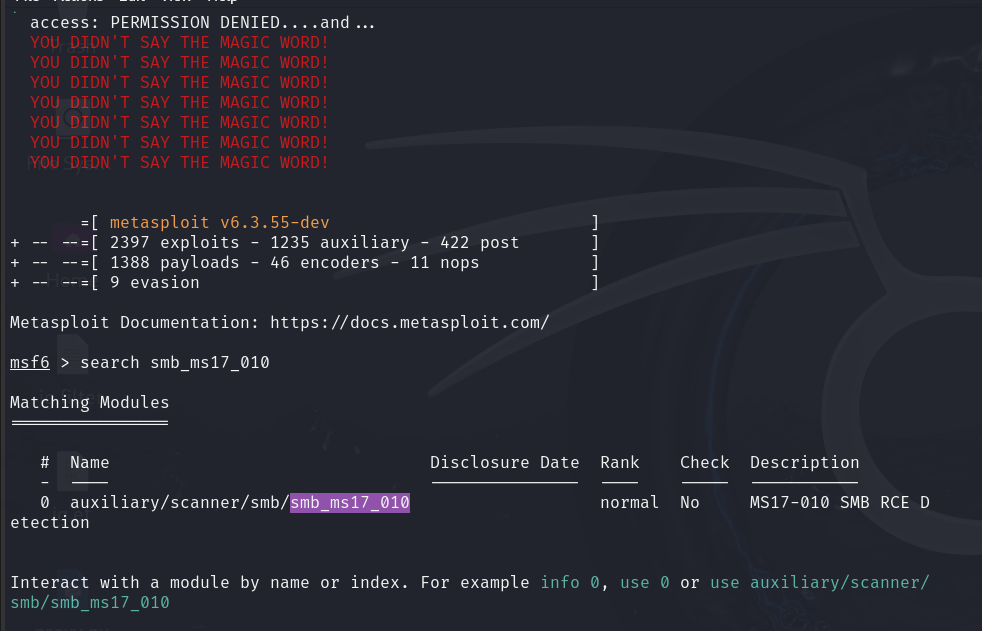
Take note of the vulnerable IP address. For me, that would be 192.168.145.129.

**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!



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.

A screen shot of a computer screen

Description automatically generated