# EternalBlue

## What is EternalBlue?

* EternalBlue is a dangerous exploit that can be used to spread malware and put Windows users at risk
* EternalBlue is a Windows exploit created by the US National Security Agency (NSA) and used in the 2017 Wanna Cry ransomware attack.
* The exploit, officially named **MS17-010** by Microsoft — gave the US National Security Agency (NSA) back end access to devices running Windows operating systems like Windows XP and Windows 7.
* It was leaked by the Shadow Brokers hacker group on April 14, 2017, one month after Microsoft released patches for the vulnerability.
* On May 12, 2017, the worldwide Wanna Cry ransomware used this exploit to attack unpatched computers.
* On June 27, 2017, the exploit was again used to help carry out the 2017 NotPetya cyber attack on more unpatched computers.

### Which Vulnerability is Exploited by this exploit?

* EternalBlue exploits a vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol. The vulnerability is denoted by **CVE-2017-0144** in the common vulnerabilities and Exposures catalog. This vulnerability exists because the SMB version 1 server in various version of Microsoft Windows mishandles specially crafted packets from remote attackers allowing them to remotely execute code on the target computer.
* This dupes a Windows machine that has not been patched against the vulnerability into allowing illegitimate data packets into the legitimate network. These data packets can contain malware such as a Trojan, ransomware or similar dangerous program.

**SMB** is a protocol that creates a connection between client and server by sending responses and requests.

### How does it work?

The EternalBlue exploit worked by taking advantage of the unsecure SMBv1 protocol. This protocol allowed Microsoft devices to communicate with other Microsoft systems — carrying out file and print services.

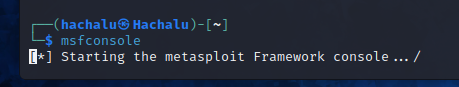
To carry out the EternalBlue exploit, attackers just needed to send a malicious SMBv1 data packet to a Windows server that had the vulnerability. The packet would contain a payload of malware, which could then be rapidly disseminated to other devices installed with the vulnerable Microsoft software.

Once the Shadow Brokers leaked the exploit in 2017, hackers took advantage of the vulnerability to carry out devastating attacks and spread massive amounts of malware. Two notable incidents exemplify the effects of the vulnerability.

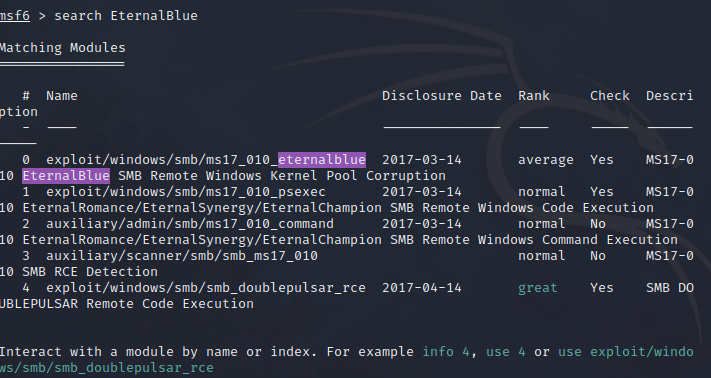
### How can we exploit it?

We have to open our linux operating system.

1. First we start our metasploit by typing msfconsol



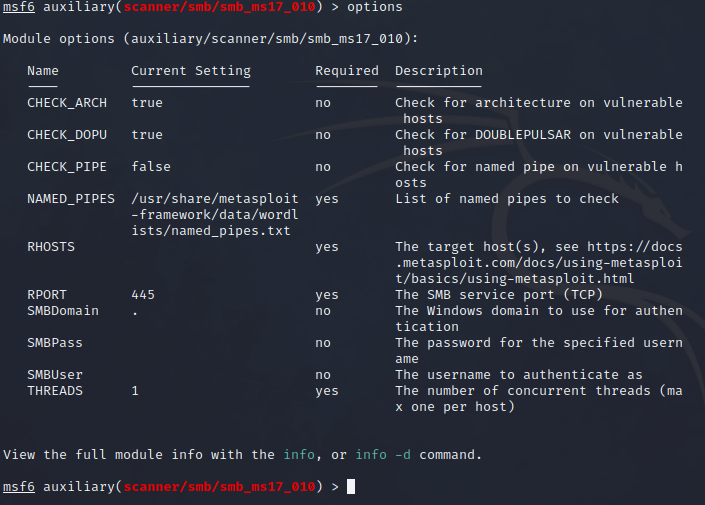
1. Then we search for eternalblue



1. Then we use the auxiliary scanner

scan

1. Then we search for options



1. Then we set RHOST

RU

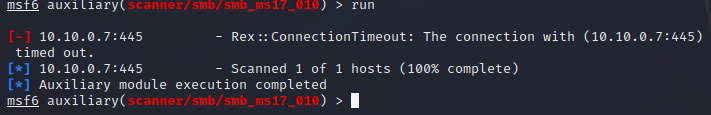
If this doesn’t work try

run2

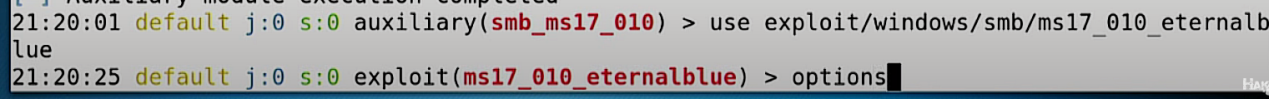
Then

RU

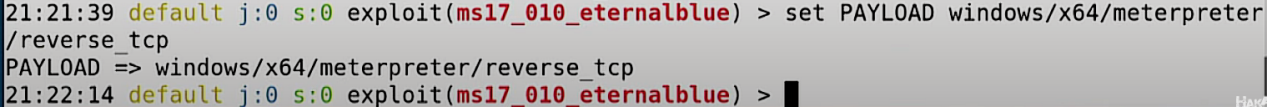
You will get something like this:



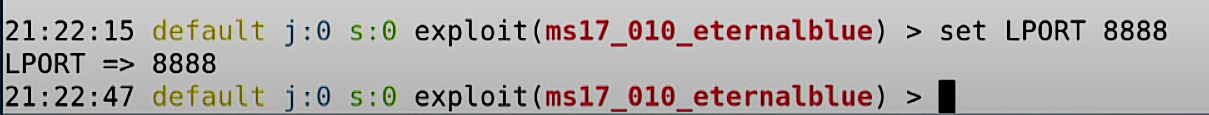
1. Now we can Exploit it



1. Then we set our payload



1. We set LPORT



1. Finally we can exploit it



Then BOOOM

