Hello! Today, we will be examining the HackTheBox machine titled Blue. It is rated as an easy machine, which is understandable as the difficulty to complete this machine requires 0 privilege escalation or exploit chaining. This machine does, however, cover a very important and well-known exploit known as EternalBlue, so let’s get into it.

 Starting with enumeration, I ran a simple nmap scan that looked like:

A computer screen capture

Description automatically generated with medium confidenceThis scan reveals a couple of interesting things.

First, we know we are working with SMB due to the port of interest being 445. We also know we are dealing with an older machine, as it is running Windows 7. Now, it is a good rule of thumb to quickly run a scan for EternalBlue when dealing with SMB, as it is an incredibly popular vulnerability, and it only takes a few seconds to check. Lucky for us, nmap comes with a script for testing this vulnerability.

A computer screen capture

Description automatically generated with medium confidenceWhen we run this command, we get a positive hit!

From here on out, exploitation is very trivial. You can do it straight from Metasploit (there is a manual way to exploit it as well, but Metasploit saves you the headache. You can read more about this vulnerability online). In Metasploit, you can simply search for EternalBlue and select the appropriate exploit.

Graphical user interface

Description automatically generated

Text

Description automatically generatedFrom there, simply fill out the RHOSTS and LHOST and then exploit. It should mention some things about a buffer and exploit packet. Don’t worry if it fails one or two times, this is a complex attack.

Lucky for us, EternalBlue provides system access. From here on out, you just have to find the flags.

IMPORTANT NOTES:

EternalBlue is an exploit that takes advantage of out-of-date Windows machines.

This exploit is utilized by ransomware such as WannaCry

Its CVE is CVE-2017-0144