Hello everyone in this exercise you will learn about an attack based on SMB based vulnerability in Windows machines.

The SMB, which is also known as the Server Message Block can be understood as a client-server communication protocol used for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services. SMB protocol earlier used the port number 139. Latest versions of SMB use port number 445 on top of a TCP stack.

Here is an example explaining the use of SMB protocol. When you want to access the shared folder available on another machine, SMB protocol is used. Type run in windows search box and Type your remote machine's IP address and press "OK." File Explorer will display a folder with files shared on remote machine.

SMB protocol, being a very important protocol for Windows users, also suffers from a vulnerability known as MS17-010. The indicated versions of Microsoft windows suffer from this vulnerability.

Here are some effects of this vulnerability, if exploited. It can allow an attacker to get admin privileges on a vulnerable machine. Or to have full control on the remote machine.

The attacker can perform various post exploitation activities on the victim machine after compromising it.

These post exploitation activities may include opening rdp sessions, installing key loggers, performing pivoting, encrypting files for Ransom etc.

Eternal Blue is a Windows exploit created by the US National Security Agency (NSA), later stolen by Shadow Brokers hacker's group.

This group released the exploit to the public resulting in a lot many disasters. It was included in the Microsoft security bulletin as CVE name MS17-010 for protecting people from the attack.

Here are some news headlines related to the worldwide WannaCry ransomware attack that used eternal blue exploit to attack unpatched computers, for SMB based vulnerabilities.On June 27, 2017, the exploit was again used to help carry out the 2017 NotPetya cyberattack on more unpatched computers.

The WannaCry is a worm able infection, which displays following messages on an infected system.

After understanding about the SMB protocol, its vulnerabilities and the effects on target machine, let's see how attack is performed on the target machine using SMB vulnerability.

Attacker first tries to find out about the availability of this vulnerability on the target machine. He or she may use the vulnerability scanner available with Metasploit tools to check this.

The attacker creates a piece of code, undetectable by Windows defender. and attacks using Metasploit tool's eternal blue exploit.

The successful execution of the attack allows the attacker to compromise the remote target machine., you can see in the screenshot that how the window 7 machines has been compromised, which gives an interactive session to the attacker to perform various unwanted activities.

Here are some examples of post exploitation activities. The attacker can use a tool, key log recorder, to capture keystrokes on the compromised system. Can encrypt the files on the remote machine to perform a ransomware attack. Can create suspicious files on the remote machine. Can delete important files from the machine. Can steal the information. Can enable Remote Desktop and creates a user account to log into the system. And many more…

Let's see some techniques to detect whether you are under SMB attack.

The first technique to detect an ongoing SMB based attack is using Wireshark tool. You can capture the packets on your machine using Wireshark and analyze them. In case of an ongoing attack, you will see “Negotiate Protocol request” and “Negotiate Protocol Response” packets in the flow, which are used for initiating the SMB protocol communication.When you set a SMB filter, in display filter, you will see NT trans Requests packets also. These are the specially crafted packet necessary to exploit the system.

Let's learn about some of the techniques to prevent such types of attacks.

One of the approach to prevent is not to allow SMB protocol across the Internet using firewall rules; either disallow all traffic on ports 135-139 & 445 or limit access to specific IP addresses or Mac Addresses.

To block a port using firewall, first check the open ports on your windows machine. if port no 445 is found open, disable it. You can check it using the net stat command (run on command prompt) as shown here.

If port 445 is found open, block it in firewall. Open firewall by clicking on Start > Control Panel > Windows Firewall and Advanced settings, as shown.

Click on Inbound Rules > New rule. Then in the pop-up window, choose Port > Next >TCP > Specific local ports and type 445 and go to Next. Select Block the connection and click next.

You can check if rule has been created successfully by clicking on Properties, then Protocols, Ports and finally Local Port.

One thing that is important to note is, if user closes port 445, he will not be able to copy any file system data or from the path where port 445 is closed.
The best solution for this problem is security update for SMB Server. Let's see how it works.

Poor patch management can leave an organization vulnerable to a devastating security breach – even without anyone making an obvious mistake like opening a malicious attachmentThe "MS17-010-SMB_REMOTE_CODE_EXECUTION_EXPLOIT" vulnerabilities in Microsoft Server Message Block 1.0 (SMBv1) is the perfect example.

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

To Install Security Update for Microsoft Windows SMB protocol,
Go to the Microsoft Security bulletin where the links are available for the security update packages. Scroll down to

the operating system that is in use. In this example, it is Windows 10 64bits.Click on the desired package. In this example, the package used is Windows 10 for x64-based Systems (kb4012606) update. Download the package Windows 10 for x64-based Systems (kb4012606).

After the download is completed, install the update by right clicking the file and clicking on Run command. Window Prompt appears with the message "Do you want to install the following Windows software update". Press Yes and this will initialize the installation setup.
At the end of the installation, it will require to restart the computer. Restart it.

To check if the installation was successful, just go to Control Panel > Windows Updates > View update History (on the left side) and see if the Security Update for Windows is installed. It should have the current date in the Date Installed column**.** If the update has been already applied or installed, then windows appear on the screen informing about it.

Thank You.