Date: 01/11/2023

Assessment 1: Vulnerability Analysis

This assessment encourages us to work on different tools like Nessus and Openvas to find vulnerabilities in a given target system

Objective

The objective of the assessment is to make us aware of the different tools that are available and used by cyber security analysts to find the loopholes in the system. In this assessment, we are made familiar with installation of tools, understanding the target system and scanning for loopholes and issues. This assessment builds the first step in ethical hacking called reconnaissance or finding information about the victim

Tenable Nessus

Nessus is a product which has been developed by Tenable and is a prominent tool for vulnerability scanning. It is majorly used by the cyber security analysts and ethical hackers in order to understand the loopholes in the system.

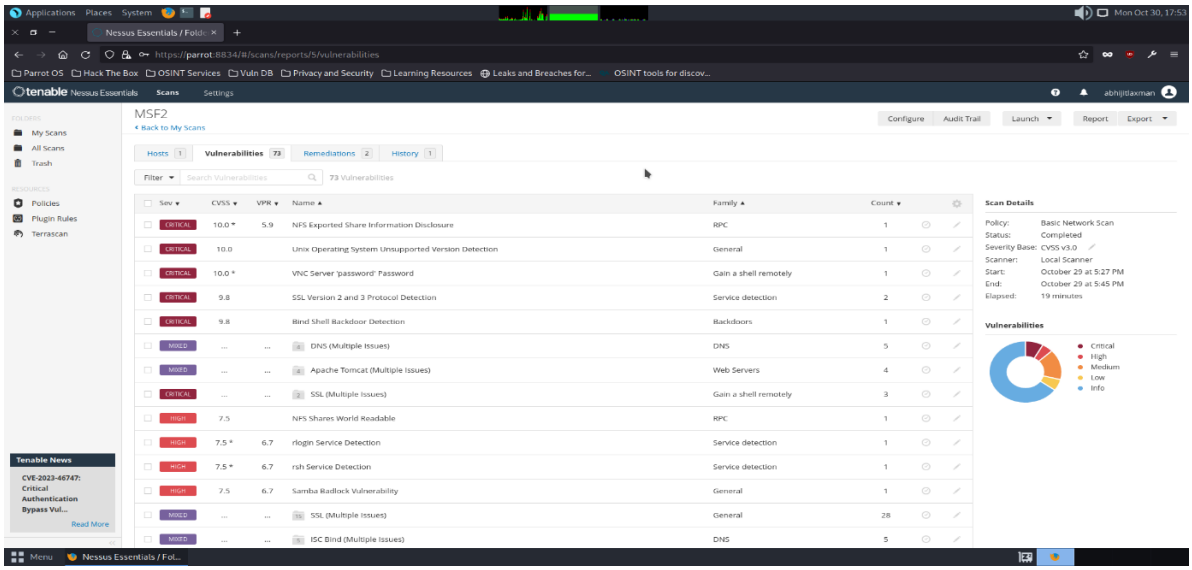
Nessus comes with different purchase levels like Nessus Essentials, Nessus Professional and Nessus Expert. Nessus Essentials is a free tool for host discovery, port scanning, and other services. Nessus Essentials provides 16 different IP addresses for scanning in 90 days. The IP address which has not been tested for more than 90 days will be removed from the list and we can replace that IP with another IP. The paid software provides unlimited IP scanning which are used in cyber cells and other cybersecurity- oriented organisations.

To use the Nessus tool, it has to be downloaded from the Tenable's website. It has to be registered with our email address to which an activation code will be sent. The website provides a .deb file which has to be installed using dkpg command. Once it is installed, the service has to be started using the systemctl command. The Nessus uses the port 8834 which can be accessed through browser.

For the first time, we have to set up our account with the activation code received and setting up the username and password. Once all this has been finished, the software will download the plugins required for scanning. This process may take a little time (about 40-45 mins). Once everything is done, we are good to go for scanning. But before scanning, determine the IP address of the target machine

Click on "New Scan" and enter the name of the scan, the IP address of the targets (comma separated) and configure the settings. Nessus provides custom configuration for scanning like the plugins to be included and the no of ports to be scanned (by

default it scans the most commonly used ports but can be changed accordingly). Once the custom configuration has been done, save it and launch the scan. Wait for the scan to finish. The scan will look something like this once finished:



We can see that Nessus gives us a detailed report and visual representation of the scan it has performed. It shows us the criticality and pie chart that increases the understanding.

I have downloaded a virtual machine from the vulndb website known as metasploitable 2. It is a virtual machine specially designed to be vulnerable to practice the demonstrations. The IP address of the attacker's machine is 192.168.119.128 and the target machine is 192.168.119.129.

There were around 73 vulnerabilities detected by Nessus out of which I'll be listing out critical vulnerabilities. Those are:

1) Anonymous FTP login enabled
2) Badly configured VNC server
3) SMB Samba Eternal Blue
4) NFS Shared Files

FTP

Files can be transferred between client and server using a protocol and this protocol is called File Transfer Protocol (FTP). FTP can be used to connect to another computer and once the connection is established, the two devices can share the files among themselves. The devices can upload and download files without the use of wired

connection. If the devices are in Local Area Network or the devices are discoverable over the internet, there has to be no physical connection between them for file sharing, The FTP uses TCP to set up the connection. FTP works on PORT 21.

The vsftpd is vulnerable version of FTP which was running on the target machine and this was detected by Nessus

How to exploit?

The attacker can try to connect himself with the “ftp <IP>” command. Once this has been executed, it asks for username and password. If the FTP configuration file has not been properly handled then the ftp supports anonymous login. This means that the attacker can anonymously login and access the files of that device. The default credentials for anonymous login is anonymous:anonymous

The attacker can upload his own script written in python, ruby or any such language and get reverse shell. We know that shell is the most important part of the OS. If the attacker gets the reverse shell or gain access to the SSH keys and get the shell and use privilege escalation to get the root access, he has the entire control over the system.

How to mitigate this?

We know that /etc folder contains the configuration files and similarly it contains configuration file for the vsftpd called vsftpd.conf. We can make changes to this file and configure it to be more secure. We should disable the anonymous_enable to NO, anon_mkdir_write_enable to NO and anon_upload_enable to NO

Other than this, the file /etc/ftpusers contains the list of usernames that are NOT allowed to login through FTP. In this file. We can add anonymous. By doing this, we cannot login as anonymous user anymore. We would require legitimate credentials to login

SMB Samba

SMB stands for Server Message Block is also a communication protocol which is used to share files, peripherals, network and IPC communications from Linux to different operating systems. SMB works on the TCP protocol in order to establish the connection between the devices. The SMB works on port 445. The user can use this utility and set up the configuration file to allow the users. The configuration files as a tradition are stored under the /etc/samba directory by the name smb.conf.

How to exploit?

Samba SMBv1 was a famous vulnerability and was brutally abused to get the unauthorised access to computers. Since organisations use Samba to a very large extent, this became quite destructive and the attack was known as the eternal blue. The Metasploit framework can be used in order to abuse this service and get a reverse_tcp meterpreter. The exploit exploit/windows/smb/ms17_010_eternalblue can be used to exploit this service with the payload set to linux/meterpreter/reverse_tcp. This will exploit the service and give us the meterpreter session that can be used to get the live screen view as well. It can also be used to play audio, get screenshot, peek through the webcam, etc

How to mitigate?

The eternal blue vulnerability works on the SMBv1. The Microsoft was made aware about this and soon there was an update. So, it's quite obvious that we should update the SMBv1 to the latest version which will recover through the vulnerability. Also, it is recommended to close the ports that are not being used. Manually closing the ports is not possible. It can be only done by stopping the service running on the port. It can be done by the "sudo service <service> stop" and can be opened again when required using the same command but replacing stop to start

VNC Server

VNC is a utility used to gain the GUI based control over a remote system. VNC uses authentication to give the control. VNC is generally preferred because of the user-friendly environment and experience. The credentials are used to authenticate the user and give the control over the system. But due to the risks associated with this service, the use of VNC server was minimised. There are different VNC service providers like TightVNC, RealVNC and others. But due to the risks associated, people started preferring Google Remote Desktop

How to exploit?

The target machine had the VNC server running and was badly configured. The password of the VNC server running was "password" itself which is counted in the most common passwords. Hence, it is quite easy to brute-force and get the access to the system. Even if not control, the attacker can at least look at the activities going on in the system. He can get the whole environment of the system and later when the system is idle, he can gain access to the device. There are two ways we can exploit this. The first one is to use Hydra tool to brute-force the credentials. The Hydra is the most prominent tool used for brute-forcing. It supports login brute-force, SMB protocol, SSH protocol, VNC protocol and others, making it more attractive. The other

method is to use the Metasploit framework and use the auxiliary/scanner/vnc/vnc_login scanner and set all the options required. We can set the PASS_FILE variable to the password wordlist we would like to use to brute-force and run the scanner. After waiting for a while, we will see that the scanner was able to crack the password and then we can connect to the VNC using those credentials as tradition

How to mitigate?

The main issue here was not the service but the weak password. We know that the attackers have been able to list out the most used and easy passwords in a file called wordlists. There are many wordlists available out of which rockyou.txt is used frequently containing a huge no of passwords. The best way to mitigate is to use a very strong, unguessable password. That's the reason organisations request you to set passwords containing uppercase, lowercase, special characters, numbers which make it quite difficult to guess. Another way to mitigate is to close the VNC server when not required. We can use the "sudo systemctl stop <service_name>" to stop the service and close the port

Conclusion

In this assessment, we learnt how to find issues associated with a system and how to compromise them to get access to the system. By knowing these, we understand how unethical hackers try to get into our devices and hence we can avoid them and make our devices more stronger and make them able to withstand the attacks