Imran Ahmed

Network Security:
Penetration Test

Objective:
1. A penetration testing over the security of a network by simulating an attack from a malicious source.
2. Using/learning the tools to carry out the penetration testing.
3. Investigate the security of potential vulnerabilities.

Tools:
Penetration testing tools:
- Nmap
- Nessus
- Metasploit

Intrusion prevention tools:
- Snort

Nmap is a powerful Network Scanner that is used for:
- Discover computers and services
- Scan ports
- OS detection

Nessus is a is a comprehensive vulnerability scanning software,
that can:
- scan for port, exploits, vulnerabilities, misconfigurations
- launch DOS attack
- crack passwords

Metaslpoit is a "framework for developing and executing exploit code against a remote target machine
Steps to exploit a system:
1. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 300 different exploits for Windows, Unix/Linux and Mac OS X systems are included);
2. Checking whether the intended target system is susceptible to the chosen exploit
3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry, for instance a remote shell or a VNC server);
4. Choosing the encoding technique to encode the payload so that the Intrusion-prevention system will not catch the encoded payload
5. Executing the exploit."   -Wiki: http://en.wikipedia.org/wiki/Metasploit

Snort is "a Network Intrusion Detection/Prevention system, that can "detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web application attacks, SMB probes, and OS fingerprinting attempts, amongst other features."
Wiki: http://en.wikipedia.org/wiki/Snort_(software)

Penetration Test Preparation:

To perform penetration test, we need a host and target system on network. Sun Virtual Box has been setup. The host or malicious source is a fully patched Windows XP system and the target system is a Virtual client running Windows XP with SP2.

Port and OS Scanning with Nmap:

We need to discover a system over network and find out what ports, services and OS that system is running. Since, we are running Windows, we can use the GUI version called Zenmap. The interface has a target, profile and command field. In the target field, the IP address of the targeted system is entered. For this test the IP address entered is **192.168.1.1-90**. Then we choose the "Quick Scan Plus" from profile field. As the profile is changed, the command field automatically generates the set of commands and switches needed to scan and detect the target system. For "Quick Scan Plus" profile, the Nmap command is "**nmap –sV –T4 –O –F 192.168.1.1-90**". After scanning, it outputs a report of ports found on the given IP range. Our test show that there is an interesting ports on **192.168.1.65**. It also shows us what OS and services that system is running.

Now, we have three crucial information about the targeted system i.e. IP, ports and OS.

Vulnerability Scanning with Nessus:

Nessus is developed as a server/client application. First, we need to run the Nessus server or Nessusd service, in order to run Nessus . Nessus client does all the scanning, reporting and managing work. The Nessus client first requires to connect to Nessus server. After successful connection, we scan the targeted system vulnerabilities by entering the targeted IP address. The scan result will return the list of vulnerabilities risk wise. We need to look for the "High Risk Vulnerability" marked in red fonts. Nessus also provide the details of that exploit and also provide the link of the patch to download. In our test, we have selected a high risk "**windows/smb/ms_08_067/netapi**", a Windows SMB buffer overflow vulnerability. The information, we gathered from nessus scan is that the targeted system can be exploited and now we are ready to exploit the system.

Exploit with Metasploit:

Since we are using Windows, the metasploit console feature is not available. So, the web interface is used in this test. The version 3.2 and 3.3 has metasploit web interface. After a long initialization of metasploit framework, it will launch the web browser with 127.0.0.1:55555 address. In the metasploit web console, we enter "show exploits" to show the list of exploits currently in framework. In the list, we see the "windows/smb/ms_08_067/netapi" exploit. Then the command "**use windows/smb/ms_08_067/netapi**" will change the "msf >>" prompt to " msf exploit windows/smb/ms_08_067/netapi >>" . The new prompt shows us that msf framework will launch the selected exploit. Now, we need to select a payload. A payload is "the code carried by the exploit to the target computer and then executed there."- taken from wiki: http://en.wikipedia.org/wiki/Payload_%28software%29. The command "show payloads" shows the list of payloads of the selected exploit that can be executed. We have selected a type of VNC payload by entering the "**set payload windows/vncinject/bind_tcp**" command. To configure the payload, we entered "show options" command and it shows the module options and the fields needed to execute the exploit. In VNC inject over TCP port payload, we need only RHOST IP address to fully configure the payload. The command “**set RHOST 192.168.1.65**” sets the RHOST for the payload. And now, we are ready to execute the exploit. The command “**exploit**” checks if the targeted system is penetrable. After successful penetration test, it launches a VNC viewer shell and the remote targeted system is exploited and taken over by the malicious attacker.

Detecting and Preventing with Snort:

To prevent this kind of malicious attacks, we need to monitor the network and stop the exploits. Snort is installed on the Virtual client. Snort needs to be configured and has to use “Rules”, in order to detect and prevent suspicious traffics. Some basic steps are sufficed to log the traffic and setup the alert/ block system for Snort. First, we enter “**snort /service /install**” and “**snort /service /start**” command to install and start the snort as a background service. By entering “**snort -A full -c /etc/snort/snort.conf**” command, it will be linked to default snort configuration file. Now, we need “Rules” file for snort. Rules are set of instructions, that directs snort how to react when an intrusion or suspicious traffic is monitored. So the rules are download from Snort official website and by “**snort -A full -c [direct to rules file]”** command, the snort is fully configured. Most of the port scanning tools uses port knocking. In the test Nmap tries to scan the port and an alert message pops up by the snort at the targeted client. Then the Snort log file is viewed and all the details like source IP, time stamp and type of attack(in this case Port knocking) is recorded.

Conclusion:

When it comes to network security, all the systems connected should be fully upgraded and patched. Strict rules should be set for Firewalls. The penetration test carried out shows that how vulnerable a system is, if best measures are not taken to secure it. The Windows SMB overflow exploit has been fixed and the patch is already at Microsoft website. A network Intrusion Detection tool like Snort is an effective tool to detect and prevent a malicious attack.

“Prevention, is the best defense”

Reference:

- Overview of Metasploit taken from http://en.wikipedia.org/wiki/Metasploit

- Overview of Snort taken from http://en.wikipedia.org/wiki/Snort_(software)

- Defination of Payload taken from http://en.wikipedia.org/wiki/Payload_%28software%29