60467 Project 1

Net Vulnerabilities scans and attacks

Chun Li

Hardware used:

Desktop PC: Windows Vista service pack Service Pack 2 v113
Intel Core 2 Duo 3GHz CPU, 4GB Ram, D-Link DWA-552 XtremeN Desktop wireless Adapter
MacBook Pro Laptop: Mac OS X 10.6.1 Snow Leopard
Intel Core 2 Duo 2.53GHz CPU, 4GB Ram,
Apple Airport wireless adapter

Apple AirPort Extreme Wireless Router: Based on the IEEE 802.11n specification, compatible with 802.11a/b/g.

Software Used:

Nmap: A free and open source utility for network exploration or security auditing. Support Windows, Linux, Mac, UNIX.

Version 5.00 is used for this project.

Nessus: One of the world-leader in active vulnerability scanners. Support Windows, Linux, Mac, UNIX.

(\$1200 for profession version, Free for home version, but need registration)

Version 4.0 is used for this project.

Metasploit: A free powerful tool for penetration testing and exploit research. Support Windows, Linux and UNIX.

Version 3.2 is used for this project.

In this project, I'm going to use the network exploration software called NMAP to search potential hosts inside the local wireless network, after that Nessus will be used to detect vulnerabilities on that host and at last we are going to use metasploit to exploit the selected host and try to take control of it.

First, let's start with Nmap; Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. For this project, I'll use Zenmap (The GUI version of Nmap) to explore the local wireless network. [1]

👁 Zenmap		X
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> elp		
Target:	▼ Profile: ▼ Scan Ca	ancel
Command:		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS 4 Host 4		etails

The picture above is the user interface of Nmap; we can type different IP address, web address inside the Target box to attack different targets. Inside the Command Box, we need to type different Commands to let Nmap search the network in different ways using different techniques.

-sS and –sT are the two most commonly used commands for Nmap.

-sS is called TCP SYN scan, it's the most popular scan option for Nmap, it can be performed very quickly and won't be hampered by restrictive firewalls. It will never complete TCP connections so it is very stealthy. This mode can only be used when the user has the root permission and is scanning on a IPv4 network.

-sT is called TCP connect scan, it's not as good as the –sS mode, since it will establish connections with each open target port, just like the common web browsers and P2P clients. In this way, it is not only slower than the –sS mode, but also less stealthy. So if –sS option is available, we should not use this mode unless we are scanning on a IPv6 network.

I'm going to use –sS to explore the network in this project. –O will also be used; this mode is for detecting the Operating system used for each host.

Target: 10.0.1.0/24		•	Profile:	•	Sc	an	Cancel
Comman	d: -sS -O 10.0.1.0/24						

Here are the targets that we are going to explore and the mode the Nmap going to use. 10.0.1.0/24 means 256host between 10.0.1.0 and 10.0.1.255 will be explored, this means all the potential hosts inside my

local wireless network will be explored. -sS -O is used, this means Nmap

will use TCP SYN scan mode to explore the network, operating system

used on the target hosts will also be identified.

After we click the Scan button, the Nmap will start to explore the local

network. Here is the result:

Starting Nmap 5.00 (http://nmap.org) at 2009-10-16 13:56 东部夏令时 Interesting ports on 10.0.1.1: Not shown: 997 closed ports STATE SERVICE PORT 53/tcp open domain 5009/tcp open airport-admin 10000/tcp open snet-sensor-mgmt MAC Address: 00:1B:63:F4:6B:50 (Apple Computer) Device type: general purpose Running: NetBSD 4.X OS details: NetBSD 4.99.4 Network Distance: 1 hop Skipping SYN Stealth Scan against 10.0.1.4 because Windows does not support scanning your own machine (localhost) this way. Skipping OS Scan against 10.0.1.4 because it doesn't work against your own machine (localhost) 0 ports scanned on 10.0.1.4 Interesting ports on 10.0.1.9: Not shown: 997 closed ports STATE SERVICE PORT 88/tcp open kerberos-sec 139/tcp open netbios-ssn 445/tcp open microsoft-ds MAC Address: 00:26:BB:11:1E:7C (Unknown) Device type: general purpose Running: Apple Mac OS X 10.5.X OS details: Apple Mac OS X 10.5 - 10.5.6 (Leopard) (Darwin 9.0.0b5 - 9.6.0) Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/ submit/ . <u>Nmap done:</u> 256 IP addresses (3 hosts up) scanned in 41.67 seconds

From the result, we can easily find that there are 3 hosts inside the network at the moment, the first one, 10.0.1.1, is the wireless router, there are 3 opens ports on the router, which is 53/tcp, 5009/tcp and 10000/tcp. MAC address is also detected, it's 00:1B:63:F4:6B:50 and it's

recognized as an Apple Computer. The OS running on it is NetBSD 4.99.4. The port 5009/tcp is open and the service name is called airport-admin, we can conclude that the wireless router is Apple Airport.

The second host, 10.0.1.4, it's said that SYN Scan cannot be used to scan my own machine (localhost).

The third host, 10.0.1.9, there are 3 open ports on it, 88/tcp, 139/tcp and 445/tcp. The MAC address is detected as 00:26: BB: 11:1E:7C and the OS running on it is Apple Mac OS X 10.5-10.5.6(Leopard). We can conclude that this host is a Mac.

Here we have the IP address and open ports information of all three hosts inside the network. Now I'm going to use a vulnerability scanner tool called Nessus to detect potential vulnerabilities on these three hosts.

Nessus: It's one of most popular active vulnerability scanner, featuring high speed discovery, configuration auditing, and asset profiling, sensitive data discovery and vulnerability analysis of your security posture.[2]

藍 Nessus : Untitled								
File Help								
NESSUS 4	Nessus							
Scan Report								
Network(s) to scan :	Select a scan policy :							
▼ 10.0.1.1	New policy							
▼ 10.0.1.4								
▼ 10.0.1.9								
+ - Edit	+ - Edit							
Scan Now								
Disconnect								

Here is the user interface of Nessus, we can see that I have already entered the IP addresses of the three hosts inside the network, and I have also made a scan policy called "New policy".

Number of hosts in parallel :	10						
Number of checks in parallel :	10						
Port scanner range :	default						
 Safe checks Designate hosts by their DNS name Consider unscanned ports as closed Save knowledge base on disk Log details of the scan on the server Port scanners to use: 							
Vessus SNMP Scanner							
Nessus SYN scanner							
Vessus TCP scanner							
🕼 netstat portscanner (SSH)							
v netstat portscanner (WMI)							
Ping the remote host							

Here is the policy options configuration window, we can choose different port scanners, we can set the number of hosts in parallel and the number of checks in parallel and also the port scanner range. I recommend set both the number of hosts in parallel and number of checks in parallel to 10. If you set it too large, it may cause too much traffic inside the network that may cause the wireless router to crash.

After the Scan Now button is clicked, Nessus will start to detect vulnerabilities of all three hosts in the network.

4 10.0.1.1	*	SHB Detection
general/udp		Symonsis :
general/icmp		59109313 .
general/tcp		A file / print sharing service is listening on the remote host.
unknown (57337/		Description :
mdns (5353/udp)		The remote service understands the CIFS (Common Internet File System)
nat-pmp (5351/u		or Server Message Block (SMB) protocol, used to provide shared access
syslog (514/udp)		to files, printers, etc between nodes on a network.
osu-nms (192/udp)		Risk factor :
snmp (161/udp)	=	None
bootpc (68/udp)	-	
bootps (67/udp)		flugin output .
4 10.0.1.4		A CIFS server is running on this port.
general/tcp		
http (80/tcp)		Nessus ID : <u>11011</u>
unknown (1037/tcp)		DCE Services Enumeration
unknown (5357/tcp)		Synopsis :
nco_proxy (4400/t		A DCE/RPC service is running on the remote host.
bfd (3784/tcp)		· · · · ·
bfd (3784/udp)		Description :
mysql (3306/tcp)		By sending a Lookup request to the portmapper (TCP 135 or epmapper
ms-lsa (1029/tcp)		(DCE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port.
unknown (1028/tcp)		Using this information it is possible to connect and bind to
exosee (1027/tcp)		each service by sending an AFL request to the remote port/pipe.
cap (1026/tcp)		Solution :
blackjack (1025/t		N/A
microsoft-ds (445		Right Factor ·
netbios-ssn (139/	-	AISA LOCCOL .
the second second	÷	None

Here is the scanning result. We can see there are different vulnerabilities detected for each host. The orange colored vulnerabilities mean it's at medium risk and the red colored vulnerabilities means it's at high risk and should be fixed as soon as possible. Let's take a look at the red

colored vulnerability on my own PC:

NSO9-050: Nicrosoft Windows SNB2 '_Sub2ValidateProviderCallback()' Vulnerability (975497) (uncredentialed check) Synopsis : Arbitrary code may be executed on the remote host through the SMB port Description : The remote host is running a version of Microsoft Windows Vista or Windows Server 2008 which contains a vulnerability in its SMBv2 implementation. An attacker could exploit this flaw to disable the remote host or to execute arbitrary code on it. See also : http://g-laurent.blogspot.com/2009/09/windows=vista7=smb20=negotiate=protocol.html Solution : Microsoft has released a patch for Windows Vista and Windows Server 2008 : http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx Risk factor : Critical / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE : CVE-2009-3103 BID : 36299 Other references : OSVDB:57799

Nessus ID : <u>40887</u>

So the vulnerability is that arbitrary code may be executed on the remote host through the SMB port because Windows Vista contains vulnerability in its SMBv2 implementation. Attackers can exploit this flaw to disable the remote host or to execute arbitrary code on it. Nessus also provide a solution to this vulnerability. Which is a windows patch published by Microsoft. Users should download this patch to fix the problem. We can also see the Critical base score of this vulnerability, which is 10, which means it's at the highest risk level.

Alright so we have detect the vulnerability on the host machine, now we should find a way to attack it, here I'm going to use a popular penetrating testing tool called metasploit.

Metasploit: Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. [3]

So now let's start with Metasploit, here is the user interface:

# Metasploit Frame	ework GUI v3.2-r	elease						
<u>S</u> ystem <u>W</u> indow	<u>H</u> elp							
				取消(C) 查找(E)	Jobs			
🔆 Exploits	All	loaded exploit modules (3	320)			4 lobe	Module	
Q Auxiliary	All	oaded auxiliary modules	(99)		38.	1003		
					Soccio	ne		
Module information	Module Output				- 1	arnet	Type	
This interface can b	Welcom be used in either	e to the Metasploit Fram wizard-mode or console-r	ework GUI! node. To start the	wizard, browse to a		arget	1)00	
module in the list a	module in the list above, and double-click its name. To view the source code of a module, right-click							
its name and selec	its name and select the View Code option. If you prefer to work in a msfconsole interface instead,							
Select the Console	opuon nonn une v	vindow menu (or just pres	S Control+O). Ha	ive iuni				
Loaded 320 exploits	, 217 payloads, 2	0 encoders, 6 nops, and 9	99 auxiliary		,			

We can see there are currently 320 build in exploit modules in Metasploit, and 99 Auxiliary modules. There is another important term we need to understand for this software, the payload. Payload is the tool we use to take advantages of the target machine after we successfully exploit the target machine. There are several most commonly used ones such as the bind_tcp meterpreter. If we can find the vulnerability exploit module in this software, then we can use the module to successfully exploit the target machine, then we can add a payload, which is bind_tcp meterpreter, so we can bind a shell to the target machine, which means we can start to take control the target machine by using the command lines on the local machine. Let's go back and take a look at the vulnerability that we found using the Nessus, It's called "MS09-050 Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Vulnerability (975497)". I tried to find a exploit module for this vulnerability in Metasploit but there isn't one for this so far. But if there's one there, we could simply double click the module, set up the payloads and exploit the target machine, then take control of it. References:

[1] Nmap Home Page http://nmap.org/ accessed on Oct 16, 2009.
[2]Nessus Home Page http://www.nessus.org/nessus/ accessed on Oct 16, 2009.
[3]Metasploit Home Page http://www.metasploit.com/ accessed on Oct 16, 2009.