Network Hacking

Ways To Attack a Network:

Ping

The IP address gives the attacker’s Internet address. The numerical address like 212.214.172.81 does not reveal much. You can use PING to convert the address into a domain name in WINDOWS: The Domain Name Service (DNS) protocol reveals the matching domain name. PING stands for “Packet Internet Groper” and is delivered with practically every
Internet compatible system, including all current Windows versions.
Make sure you are logged on to the net. Open the DOS shell and enter
the following PING command:
Ping –a 123.123.12.1
Ping will search the domain name and reveal it. You will often have information on the provider the attacker uses e.g.:
dialup21982.gateway123.provider.com
Pinging is normally the first step involved in hacking the target. Ping uses
ICMP (Internet Control Messaging Protocol) to determine whether the target host is reachable or not. Ping sends out ICMP Echo packets to the target host, if the target host is alive it would respond back with ICMP
Echo reply packets.
All the versions of Windows also contain the ping tool. To ping a remote host follow the procedure below.
Click Start and then click Run. Now type ping <ip address or hostname>
(For example: ping yahoo.com)
This means that the attacker logged on using “provider.com”.
Unfortunately, there are several IP addresses that cannot be converted
into domain names.
For more parameter that could be used with the ping command, go to
DOS prompt and type ping /?.

Ping Sweep

If you are undetermined about your target and just want a live system, ping sweep is the solution for you. Ping sweep also uses ICMP to scan for live systems in the specified range of IP addresses. Though Ping sweep is similar to ping but reduces the time involved in pinging a range of IP addresses. Nmap (http://www.insecure.org) also contains an option

to perform ping sweeps.

Tracert:

Tracert is another interesting tool available to find more interesting information about a remote host. Tracert also uses ICMP.

Tracert helps you to find out some information about the systems involved in sending data (packets) from source to destination. To perform a tracert follow the procedure below.

Tracer connects to the computer whose IP has been entered and reveals all stations starting from your Internet connection. Both the IP address as well as the domain name (if available) is displayed. If PING cannot reveal a name, Traceroute will possibly deliver the name of the last or second last station to the attacker, which may enable conclusions concerning the name of the provider used by the attacker and the region from which the attacks are coming.

Go to DOS prompt and type tracert <destination address>

(For example: tracert yahoo.com).

But there are some tools available like Visual Traceroute which help you

even to find the geographical location of the routers involved.

http://www.visualware.com/visualroute

Port Scanning:-

After you have determined that your target system is alive the next important step would be to perform a port scan on the target system.

There are a wide range of port scanners available for free. But many of them uses outdated techniques for port scanning which could be easily recognized by the network administrator. Personally I like to use Nmap (http://www.insecure.org) which has a wide range of options. You can download the NmapWin and its source code from:

http://www.sourceforge.net/projects/nmapwin.

Apart from port scanning Nmap is capable of identifying the Operating system being used, Version numbers of various services running,

firewalls being used and a lot more.

Common ports:

Below is a list of some common ports and the respective services

running on the ports.

20 FTP data (File Transfer Protocol)

21 FTP (File Transfer Protocol)

22 SSH

23 Telnet

25 SMTP (Simple Mail Transfer Protocol)

53 DNS (Domain Name Service)

68 DHCP (Dynamic host Configuration Protocol)

79 Finger

80 HTTP

110 POP3 (Post Office Protocol, version 3)

137 NetBIOS-ns

138 NetBIOS-dgm

139 NetBIOS

143 IMAP (Internet Message Access Protocol)

161 SNMP (Simple Network Management Protocol)
194 IRC (Internet Relay Chat)
220 IMAP3 (Internet Message Access Protocol 3)
389 LDAP
443 SSL (Secure Socket Layer)
445 SMB (NetBIOS over TCP)
Besides the above ports they are even some ports known as Trojan
ports used by Trojans that allow remote access to that system.
Vulnerability Scanning:
Every operating system or the services will have some vulnerabilities due to the programming errors. These vulnerabilities are crucial for a successful hack. Bugtraq is an excellent mailing list discussing the vulnerabilities in the various system. The exploit code writers write exploit codes to exploit these vulnerabilities existing in a system.
There are a number of vulnerability scanners available to scan the host for known vulnerabilities. These vulnerability scanners are very important for a network administrator to audit the network security.
Some of such vulnerability scanners include Shadow Security Scanner,Stealth HTTP Scanner, Nessus, etc. Visit
http://www.securityfocus.com vulnerabilities and exploit codes of various
operating systems. Packet storm security
(http://www.packetstormsecurity.com) is also a nice pick.
Free Hacking Training Online

http://www.cybrary.it/?utm_source=hoc&utm_medium=banner&utm_campaign=purplebanner

Tools Descriptions:

1. Nmap

I think everyone has heard of this one, recently evolved into the 4.x series.

Nmap (Network Mapper) is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free and open source.

Can be used by beginners (-sT) or by pros alike (packet_trace). A very versatile tool, once you fully understand the results.

Get Nmap Here - http://www.insecure.org/nmap/download.html

2. Nessus Remote Security Scanner

Recently went closed source, but is still essentially free. Works with a client-server framework.

Nessus is the worlds most popular vulnerability scanner used in over 75,000 organizations world-wide. Many of the worlds largest organizations are realizing significant cost savings by using Nessus to audit business-critical enterprise devices and applications.

Get Nessus Here - http://www.nessus.org/download/

3. John the Ripper

Yes, JTR 1.7 was recently released!

John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

You can get JTR Here - http://www.openwall.com/john/

4. Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).

Nikto is a good CGI scanner, there are some other tools that go well with Nikto (focus on http fingerprinting or Google hacking/info gathering etc, another article for just those).

Get Nikto Here - http://www.cirt.net/code/nikto.shtml

5. SuperScan

Powerful TCP port scanner, pinger, resolver. SuperScan 4 is an update of the

highly popular Windows port scanning tool, SuperScan.

If you need an alternative for nmap on Windows with a decent interface, I suggest you check this out, it’s pretty nice.

Get SuperScan Here - http://www.foundstone.com/index.htm subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan4.htm

6. p0f

P0f v2 is a versatile passive OS fingerprinting tool. P0f can identify the operating system on:

- machines that connect to your box (SYN mode),
- machines you connect to (SYN+ACK mode),
- machine you cannot connect to (RST+ mode),
- machines whose communications you can observe.

Basically it can fingerprint anything, just by listening, it doesn’t make ANY active connections to the target machine.

Get p0f Here - http://lcamtuf.coredump.cx/p0f/p0f.shtml

7. Wireshark (Formely Ethereal)

Wireshark is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. The goal of the project is to create a commercial-quality analyzer for Unix and to give Wireshark features that are missing from closed-source sniffers.

Works great on both Linux and Windows (with a GUI), easy to use and can reconstruct TCP/IP Streams! Will do a tutorial on Wireshark later.

Get Wireshark Here - http://www.wireshark.org/

8. Yersinia

Yersinia is a network tool designed to take advantage of some weakeness in different Layer 2 protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems. Currently, the following network protocols are implemented: Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), Dynamic Host Configuration Protocol (DHCP), Hot Standby Router Protocol (HSRP), IEEE 802.1q, Inter-Switch Link Protocol (ISL), VLAN Trunking Protocol (VTP).

The best Layer 2 kit there is.

Get Yersinia Here - http://yersinia.sourceforge.net/

9. Eraser

Eraser is an advanced security tool (for Windows), which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Works with Windows 95, 98, ME, NT, 2000, XP and DOS. Eraser is Free software and its source code is released under GNU General Public License.

An excellent tool for keeping your data really safe, if you’ ve deleted it..make sure it’ s really gone, you don’ t want it hanging around to bite you in the ass.

Get Eraser Here - http://www.heidi.ie/eraser/download.php

10. PuTTY

PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator. A must have for any h4. 0r wanting to telnet or SSH from Windows without having to use the crappy default MS command line clients.

Get PuTTY Here. - http://www.chiark.greenend.org.uk/~sgtatham/putty/

11. LCP

Main purpose of LCP program is user account passwords auditing and recovery in Windows NT/2000/XP/2003. Accounts information import, Passwords recovery, Brute force session distribution, Hashes computing.

A good free alternative to L0phtcrack.

LCP was briefly mentioned in our well read Rainbow Tables and RainbowCrack article.

Get LCP Here - http://www.lcpsoft.com/english/download.htm

12. Cain and Abel

My personal favourite for password cracking of any kind.

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

Get Cain and Abel Here - http://www.oxid.it/cain.html

13. Kismet

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

A good wireless tool as long as your card supports rfmon (look for an orinocco gold).

Get Kismet Here - http://www.kismetwireless.net/download.shtml

14. NetStumbler

Yes a decent wireless tool for Windows! Sadly not as powerful as it’s Linux counterparts, but it’s easy to use and has a nice interface, good for the basics of war-driving.

NetStumbler is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses:

Verify that your network is set up the way you intended.
Find locations with poor coverage in your WLAN.
Detect other networks that may be causing interference on your network.
Detect unauthorized rogue access points in your workplace.
Help aim directional antennas for long-haul WLAN links.
Use it recreationally for WarDriving.

Get NetStumbler Here - http://www.stumbler.net/

15. Hping

To finish off, something a little more advanced if you want to test your TCP/IP packet monkey skills.

hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping unix command, but hping isn’t only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

Get hping Here - http://www.hping.org/