Global Information Assurance Certification Paper

Tools, tools, and TOOLS!!

GSEC Practical Assignment
Version 1.2f

Name: Firas Shaheen

Have you ever said to yourself, "***There are just so many tools, and it's hard to keep track of all of them and know what each one does?"*** Well I do all the time, that's why I decided to write this quick reference on popular tools (It's impossible to cover all tools, but I will try to cover as much as possible), with a brief explanation on how they work, and where to get them. I am going to cover tools for both Linux and Windows platforms, those tools will consist of (IDSes, Firewalls, Exploits, Scanners, Reconnaissance, Password crackers, Auditing, etc). But before I start I would like to talk in general about a successful attack and some of the tools involved. Why? Because:

"IN ORDER TO BEAT AN ATTACKER, YOU'VE GOT TO THINK LIKE A HACKER."

Successful Attacks *consists of:*

1. **Network Reconnaissance**: ***"When thieves decide to rob a bank, they don't just walk in and start demanding money (not the smart ones, anyway). Instead, they take great pains in gathering information about the bank - the armored car routes and delivery times, the video cameras, and the number of tellers, escape exits, and anything else that will help in a successful misadventure.*** *Hacking Exposed - Second Edition."* The same requirement applies to successful attackers. Network recon is like having a blue print of the network you're planning to attack, thus making your job easier and safer in terms of getting caught. How does network recon works? By finding out valuable information about the target network like (Domain Names, IP Blocks, IDSes, Services running, Firewalls, Platforms supported, Protocols used, DMZ, and the infrastructure of the network). How do I find all this information? Use the reference at the end for the tools required and how to use them.

2. **Gaining Access**: Gaining access can be achieved by simple methods, i.e. running an exploit against the target server, or advance methods, i.e. session or TCP hijack. Recall Mr. Kevin Mitnick's attack against Tsutomu Shimomura's system, ***"The attack used two techniques: SYN flooding and TCP hijacking. The SYN flood kept one system from being able to transmit. While it was in a mute state, the attacker assumed its apparent identity, and hijacked the TCP connection. Mitnick detected a trust relationship between two computers***

and exploited that relationship. *Network Intrusion Detection, an Analyst's Handbook - Second Edition."* Access can also be achieved by many other ways, Ex. password cracking, sniffing, physical access to a machine, default accounts, social engineering, etc. Which method shall I use? It depends on the environment, nature of the attack, and the info gathered from your network recon. What are the tools and techniques required for the attack? Use the reference at the end for the tools required and how to use them.

3. **Covering you Tracks:** So you got in!! And you have a blueprint of the network, now what? ***"Usually after committing a crime, the next step would be to alter the seen as if it never happened."*** This is done by:

    a. *Eliminating traces*: Fingerprints, video surveillance, missing items. From a security professional perspective, this could mean: Editing and clearing security logs, compromising the Syslog server, replacing system files by nested similar files. Tools like rootkits do that for you.
    b. *Disguise*: You're in a place were everyone is a doctor and you don't want to be detected, what would you do? Get dressed like a doctor. The same applies when talking about network security, but instead of getting dressed like a doctor, we create legitimate accounts on the compromised server and use those for our disguise.
    c. *Backdoors*: What was the scope of your attack in the first place, was it a one-hit-finish? *"Break-in, get the prize, then leave"* or was it a continues attack? *"Setup a sniffer on the compromised system, then check on the collected goodies now and then. It could be credit card numbers on an e-commerce site or password hashes on an NT based network waiting to be cracked by L0pht Crack."* If that was the case then setting up a backdoor is a must, because you wouldn't want to set off sensors by using the same exploit over and over. A backdoor could be a Trojan Virus (SubSeven, NetBus), or in step "**b.**" the creation of legitimate accounts.

Now that we have seen the steps a successful attack consists of, we will demonstrate each step with a simple example on some of the tools needed:

Technique	Tools	Platform	Download
Network Reconnaissance	Nmap 2.54BETA30 Hping2	Linux Linux	http://www.insecure.org/nmap/nmap_download.html http://www.hping.org/download.html

1- Finding machines that are up on the network

"Obvious answer: send an ICMP echo-request (ping) packet to each IP address and wait for a reply to determine which hosts are up. But many hosts filter out ping requests or replies! Example:

```
amy~> ping microsoft.com
```

```
PING microsoft.com (207.46.230.219) from 208.184.74.98 : 56(84)
bytes of data.
--- microsoft.com ping statistics ---
8 packets transmitted, 0 packets received, 100% packet loss
```

Solution: "TCP" ping. **Nmap -sP** By default, Nmap sends a TCP ACK (acknowledgement) packet to port 80 in parallel with an ICMP ping request. If a RST packet (or a ping reply) comes back, we know the host exists.

In some cases you may want to probe machines with a TCP SYN packet instead of an ACK. This is done with ***-PS***. This option uses SYN (connection request) packets instead of ACK packets for root users. Hosts that are up should respond with a RST (or, rarely, a SYN|ACK). *http://www.insecure.org/nmap/OSDEM_Presentation/ "*

2- Determining the ports that are open

"Open TCP ports can be determined by a SYN scan. This is the preferred general-purpose TCP scan type, also known as half-open scanning. Give Nmap the `-sS` argument to perform this kind of scan. Don't forget UDP scanning! (Nmap option: `-sU`). Other scan types: FIN, XMAS, and NULL scans (`-sF, -sX, -sN`). More details on the mechanics of these scans are available in the Nmap man page (http://www.insecure.org/nmap/nmap_manpage.html)

Advanced scan type: ACK scan (`-sA`) for probing firewalls/filtering systems.

Advanced scan type: IP Protocol scan ***-sO***. Nmap usually focuses on TCP, UDP, and ICMP, but there is a whole World of other protocols available for advanced attacks and information gathering. The Protocol Scan cycles through the 8-bit protocol field sending raw IP headers without any data. An ICMP Protocol Unreachable error means the target does not accept packets for the given protocol.

For example, here is a SYN scan:

```
#nmap -sS target.example.com/24
```

```
This command will launch a stealth SYN scan against each machine that is up
out of the 255 machines on class 'C'where target.example.com resides.
http://www.insecure.org/nmap/OSDEM_Presentation/ "
```

3- Determining network architecture

```
hping2 --traceroute -t 1 -2 --baseport 53 -keep -V -p 5023 gw.target.com
```

This means do a traceroute, starting with ttl=1 using UDP packets with a source port of 53 (dns) and a destination port of 5023 against gw.target.com. -V just turns on verbosity. Traceroute will give us an idea of how the network structure looks like (Firewalls, Routers, etc).

Finding what OS is running is an important step in gathering

information (Network recon.) and some of the ways to find out this information is by issuing the command:

```
nmap -O targethost.com
```

Nmap (with -O) can usually determine the OS in use via a technique known as TCP/IP fingerprinting.

Also if the target host was running a web server you can telnet to it on port 80 and get the server version i.e. (IIS 5.0) thus the host is running a version of NT.

```
# telnet target.com 80
>GET /blah HTTP/1.1
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
....
....
```

A lot of services give out valuable information like in our previous example, web servers, others like DNS servers with zone transfer enabled can give a great deal of information.

```
# nslookup
>server 11.12.13.2 (we specify a domain server)
>set type=any  (will list all domains and hosts)
>ls -d target.com.    >> ./Zonetransfer.out
```

Zonetransfer.out will have a list of all the hosts with the name target.com. Tools like axfr would do the whole work for you, DNS zone transfers.

ARIN "American Registry for Internet Numbers"

```
#whois "target.com."@whois.arin.net
```

(Would give you address blocks e.g. 11.12.13.0-11.12.13.255)

```
#whois 11.12.13.0@whois.arin.net
```

(Would give you the ISP and the backbone address block of the domain)

Technique	Tools	Platform	Download
Gaining Access	Legion	Windows	http://www.rhino9.com
	L0pht crack	Windows	http://www.l0pth.com

1- Finding shares on the target network

Example: After doing a network recon you find out that the target network xyz.com:

- Is an NT based network
- Has a class C with IP blocks of 11.12.13.255

Next step is to use Legion 2.1 to scan for open shares. In the IP range we enter 11.12.13.0 – 11.12.13.255. Legion will first attempt to check those IP ranges to see weather or not they are up and support NetBIOS, then it will scan those hosts that are up for open shares and will display the results in the format of IP address plus the directory shared. *"You will be surprised to see how many people share their whole C: drive with full access permissions (Read, Write, and Delete)".* We found out the IP address 11.12.13.14 has the C: drive shared with FULL ACCESS, now we map it to our local drive then we browse to:
C:\Documents and Settings\All Users\Start Menu\Programs and we place a preconfigured password sniffer so that it starts up next time the system reboots
.

2- Collecting the goodies

After we have collected the sniffed hashes and user accounts, now its time to crack them, for that purpose we use the best cracking tool for windows L0pthCrack. After successfully cracking a password we then use it to log onto the DC, thus, acting as a legitimate user.

Technique	Tools	Platform	Download
Covering you Tracks	Wipe	Linux	ftp://ftp.technotronic.com/unix/log-tools/wipe-1.00.tgz
	Zap	Linux	ftp://ftp.technotronic.com/unix/log-tools/zap.c

Wipe: Removes log entries from UTMP, WTMP, LASTLOG and ACCT entries. It will compile on virtually anything and wipe the logs CORRECTLY for that variant of UNIX system.

Zap: Will fill the Wtmp and Utmp entries corresponding to the entered username. It also Zeros out the last login data for the specific user, fingering that user will show 'Never Logged In'.

"The Utmp log records, among other things: the username, device name, time, and origin in a binary format. Programs like who, users, and finger read the utmp file and display its contents.

Wtmp can be found in /var/log, and is the same as utmp in terms of file type and format. It records the username, device, event time, and connection origin as a binary file. The major difference in file content lies in the fact that wtmp keeps a history of all logins, logouts, and system events, unlike Utmp which acts like a snapshot. *GSEC – UNIX Auditing"*

Okay, so we looked at how attacks are done and we mentioned "some" of the tools

used and when they're used. Its time to look at other tools, though we couldn't possibly mention all of them here, I left some links for more tools at the references part.

The main purpose of this write was to give you a sense of how and when tools are used. From an attackers point of view tools can be separated into 3 categories: **Reconnaissance**, **Gaining Access, and Covering Tracks.** Where from a security professional point of view tools can be separated into: **Defense in Depth tools (HIDS/NIDS, Firewalls, Antivirus, Honeypots, etc) and personal security assessment tools (Scanners, Password Crackers, Exploits, anti reconnaissance tools, etc).**

Argus
Argus is a generic IP network transaction auditing tool. Argus runs as an application level daemon, promiscuously reading network datagram's from a specified interface, and generates network traffic status records for the network activity that it encounters.
Download:
ftp://ftp.andrew.cmu.edu/pub/argus/**Asax**
Asax. An Advanced Security audit trail Analysis on uniX.
Download:
ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/asax**Asmodeous Port Scanner (WebTrends)**
Asmodeous network security scanner for Windows NT.
Download:
http://www.webtrends.com/products/wsa/**COPS version 1.04**
The Computer Oracle and Password System (COPS) package from Purdue University. Examines a system for a number of known weaknesses and alerts the system administrator to them; in some cases it can automatically correct these problems.
Download:
ftp://ftp.jaring.my/pub/cert/tools/cops/**Fremont**
Fremont is a research prototype for discovering key network characteristics, such as hosts, gateways, and topology. It runs on SunOS, and has been tested on both Sun3 and Sun4 hardware, on SunOS 4.1.1. The ARPwatch and RIPwatch Explorer Modules use the Sun's Network Interface Tap. This directory contains information, the latest version and patches.
Download:
ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/fremont **HPing**
A network analysis tool, HPing is a tool which enables you to send packet with non traditional IP stack parameters and gather information from the results of the incoming packets (which were generated in responds to the sent packet), this information isn't displayed by regular application since much of it is for debugging and internal network functionality.
Download:
http://www.kyuzz.org/antirez/oldhping.html**Internet Security Scanner (ISS) (Evaluation copy)**
ISS versions 1.21 and 1.3. This is a program by Christopher Klaus. A multi-level security scanner that checks a UNIX system for a number of known security holes such as problems with sendmail, improperly configured NFS file sharing, etc.

Download:
ftp://ftp.iss.net/pub/iss/**NESSUS Alpha 2 -fix 4**
Nessus is a free, open sourced and easy-to-use security auditing tool for Linux, BSD and some other system. It is multithreaded and plugin based, and has a nice X11 interface.
Download:
http://www.nessus.org**Nss**
nss is a Perl script that scans either individual remote hosts or entire subnets of hosts for various simple network security problems. The majority of the tests can be performed by any non-privileged user on a typical Unix machine.
Download:
http://www.ja.net/CERT/Software/nss/**SAINT**
SAINT is the Security Administrator's Integrated Network Tool. In its simplest mode, it gathers as much information about remote hosts and networks as possible by examining such network services as finger, NFS, NIS, ftp and tftp, rexd, statd, and other services. The information gathered includes the presence of various network information services as well as potential security flaws -- usually in the form of incorrectly setup or configured network services, well-known bugs in system or network utilities, or poor or ignorant policy decisions. It can then either report on this data or use a simple rule-based system to investigate any potential security problems.
Download:
http://wwdsilx.wwdsi.com/saint/**SARA 2.0.5**
"Security Auditor's Research Assistant"-security audit tool, GPL license.
Download:
http://home.arc.com/sara/index.html**SATAN version 1.1.1**
SATAN, the System Administrator Tool for Analyzing Networks, is a network security analyzer designed by Dan Farmer and Wietse Venema. SATAN scans systems connected to the network noting the existence of well known, often exploited vulnerabilities. For each type of problem found, SATAN offers a tutorial that explains the problem and what can be done.
Download:
http://www.fish.com/satan/**Tiger version 2.2.3 and 2.2.4**
Tiger (from Texas A & M University) is a set of scripts that scan a Unix system looking for security problems, in the same fashion as COPS.
Download:
ftp://net.tamu.edu.pub/security/TAMU/**Web Trend Security Analyzer (Evaluation pack)**
WebTrends Security Analyzer helps you discover and fix the latest known security vulnerabilities on your Internet, intranet and extranet. Systems are analyzed on demand or at scheduled intervals, allowing prioritization and comparative reports to be generated with recommended fixes that resolve possible exploitations.
Download:
http://www.webtrends.com/products/wsa/

References:

Network Reconnaissance Techniques,
URL: http://www.insecure.org/nmap/OSDEM_Presentation/

Fyodor. "Nmap network security scanner man page",
URL - http://www.insecure.org/nmap/nmap_manpage.html.

Fobic. "Examining Advanced Remote OS Detection Methods/Concepts using Perl",
Feb 03, 2001
URL - http://www.packetnexus.com/kb/greyarts/docs/981766898:16776.html.

CERT® Summary CS-2001-02,
URL: http://www.cert.org/summaries/CS-2001-02.html

NT Security Pointers and Resources,
URL: http://www.lanw.com/training/tisc/securityurls.htm

Rhino9 Products,
URL: http://packetstorm.decepticons.org/groups/rhino9/

Automated DNS Zone Transfer Resolution,
URL: http://www.isi.edu/~govindan/cs558f97/labs/dnszone.html

More Tools,
http://www.hackingexposed.com/tools/tools.html (Both Linux and Windows)

http://www.linux.org/apps/all/Networking/Security_/_Admin.html (Linux)

http://www.nmrc.org/files/snt/ (Windows)

http://netsecurity.about.com/cs/hackertools/ (Windows)

Bibliography:

“Hacking Exposed: Network Security Secrets and Solutions – Second Edition" McGraw Hill Professional Publishing, 2001.

“Network Intrusion Detection: An Analyst’s Handbook – Second Edition” New Riders Publishing, 2001.

Thank you, for you time and I hope you found it of use.

Sincerely,

Firas Shaheen