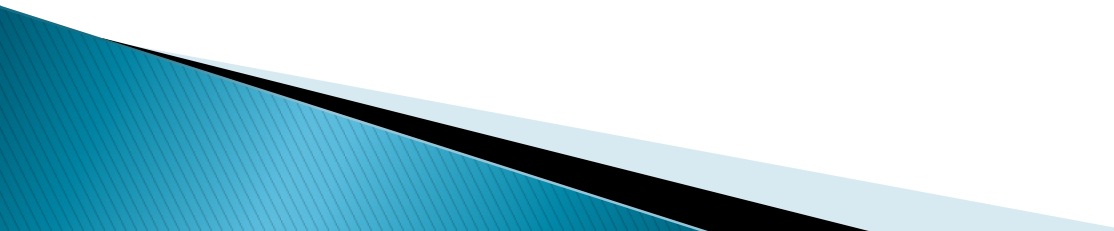


Network Reconnaissance


Steps for Gathering Information

- ▶ Find out initial information
 - Open Source
 - Whois
 - Nslookup
 - ▶ Find out address range of the network
 - ARIN (American registry for internet numbers)
 - Traceroute
 - ▶ Find active machines
 - Ping
 - ▶ Find open ports or access points
 - Portscanners (Nmap, ScanPort)
 - War Dialers (THC, Toneloc)
 - ▶ Figure out the OS (nmap, Queso)
 - ▶ Figure out which service are running on each port
 - ▶ Map out the network (traceroute, visual ping, cheops)
- 

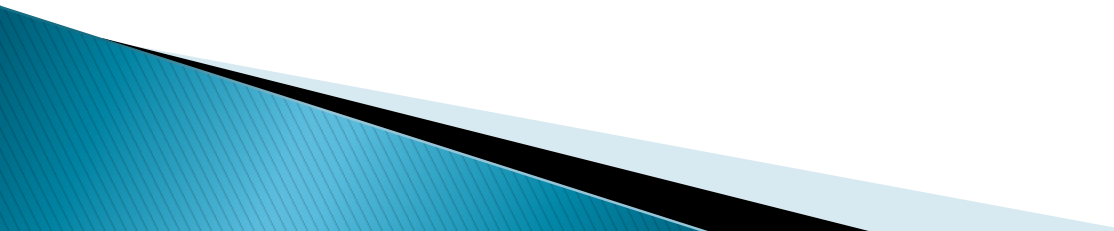
Social Engineering

- ▶ Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem. —From the Jargon File

whois

- ▶ Most versions of UNIX come with a whois
 - ▶ Third-party tools available with capability (e.g. Sam Spade)
 - ▶ Run on the target's domain name.
 - ▶ Goal is to find some more information out about your target, such as IP addresses as well as more 'mundane' information such as a possible POC, phone numbers, mail address, etc.
 - ▶ Try accessing the ARIN site to do whois search (American Registry for Internet Numbers)
- 

nslookup

- ▶ Often comes with UNIX or NT box
 - ▶ Can also use third-party program (e.g. Sam Spade)
 - ▶ Goal is to find out IP addresses
 - ▶ May also try to simply ping the domain name (it will try to resolve the host name to an address – which is what you wanted anyway – and display this address)
- 

traceroute

- ▶ Based on ping program
- ▶ Takes advantage of TTL (time to live) field
 - Normally when $TTL=1$ system won't forward packet if next hop is not destination but will return a "time exceeded" message.
- ▶ traceroute sends out a ping with a TTL of 1, then 2, then 3 and so on until it has a packet reach the destination.
 - This way it will know each intermediate hop will be discovered.
 - Doing this you can often determine the IP address for the main router, firewall, etc. the company is using.

Finding Active Machines

- ▶ Often company will get a range of IP addresses assigned to it but may not be using all of them (may have some to “grow into”). Question then is which addresses that were assigned to it ARE being used?
- ▶ Ping sweep often used to do this
 - You provide the program a range of addresses and it determines which systems in that range are “alive”
- ▶ NAT may affect the amount of information that I can obtain.

Find open ports

- ▶ OK, now that I know which machines are responding (are “alive”), I want to determine what services are available (running) on them.
- ▶ Port scanners (e.g. ScanPort, nmap)
 - Some only scan low numbered ports (1–1024), some will allow you to scan all (1–65,525)
 - Want to do for both TCP and UDP (different scans)

Port Scanning

- ▶ Several different types
 - TCP connect scan – tries to connect to each port (complete 3-way handshake). Noisy scan and can be easily detected.
 - TCP SYN scan – set the SYN bit, system will respond with SYN/ACK, don't respond with final ACK, thus never complete the connection. "Half-open" connection and may not be logged, thus less noisy.
 - FIN scan – if rogue FIN sent to open port it is ignored. If it is sent to a closed port it will respond with RST. Thus if you get something back it isn't open. Generally very stealthy since most system don't log these packets.
 - ACK scan – similar to FIN scan except send a rogue ACK.

War Dialing

- ▶ Don't forget to see if they have connections via modem to the network.
 - Common to have remote access servers (RAS) for mobile employees (e.g. sales force)
 - May also have “rogue” or unauthorized modems attached by employees.
- ▶ Separate lesson later on on war dialing.

Determine the OS

- ▶ OK, now we know which machines are alive, and we also know what ports are open on them, now we would like to determine what OS is running on the system.
- ▶ Several different programs will do OS identification (Queso, nmap)
 - Work by sending “abnormal” packets and check to see how the system responds
 - Different OS’s respond in different ways
 - For example: If a FIN packet is sent to an open port (as previously discussed) the correct behavior is not to respond to it, however some implementations (Windows NT) will respond with a FIN/ACK.

Identifying the Services

- ▶ We've got a list of systems and a list of open ports on those systems. We also know what the OS is that is running on the system, now we'd like to know what services are running on those open ports.
- ▶ Defaults: Common port numbers for all or specific OS's.
 - e.g. port 25 is generally used for mail
 - If OS is UNIX system is probably running sendmail
 - If OS is NT system is probably running Exchange
- ▶ Can also telnet to port on system – frequently system will display welcome banner listing service

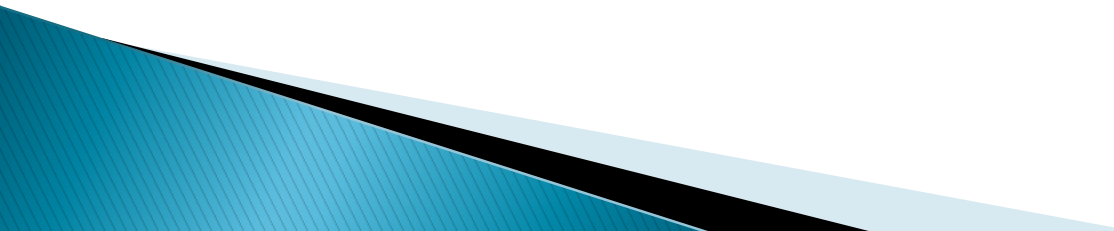
Map out the network

- ▶ After several traceroutes, you will have a list of IP addresses and the hops it took to get to them. May be able to start making guesses at what the connectivity is like for the target network.
- ▶ Some programs are available to automate this process
 - e.g. Visual Ping, Cheops

Protection against Info Gathering

- ▶ We, of course, are more interested in securing our systems, so what can we do so that others can't use these techniques against us?
 - Whois – limit the information that you provide, general data as opposed to specific.
 - Nslookup – try to minimize info in DNS records. Also any address listed should be statically mapped through a firewall with only a specific port allowed through.
 - ARIN web search – not a lot you can do since controlled externally. Try to limit addresses listed to external addresses.
 - Traceroute – can turn off ICMP but this can be useful tool too. Use private addresses inside your firewall.

Protection (cont)

- ▶ Ping – can disable ICMP but then you lose valuable tool for your own use. Use private addressing inside of your firewall to limit the machines the attacker can ping.
 - ▶ Mapping the network – block traffic at firewall and only allow traffic on specific ports to specific machines.
- 



Exploiting the system


- ▶ Back to the attacker's point of view...
- ▶ Now that we have mapped the system, what next?
 - Want to start trying to penetrate.
 - Goal is to find vulnerability that can be exploited.
 - Combination of OS and program being used.
 - Check web to find if any known vulnerabilities exist

Good Security Sources

- ▶ www.cert.org
- ▶ www.ciac.org/ciac/
- ▶ www.auscert.org.au
- ▶ www.atstake.com
- ▶ www.insecure.org
- ▶ www.securityfocus.com
- ▶ www.packetstormsecurity.com
 - packetstorm.decepticons.org
- ▶ numerous other sites

CERT Homepage

http://www.cert.org/GoSearchKeyword

**Carnegie Mellon
Software Engineering Institute**

Welcome to the **CERT®/CC**

CERT® Coordination Center | [Home](#) | [What's New](#) | [FAQ](#) | [Site Contents](#) | [Contact Us](#) | [SEARCH](#)

[About Us](#) | [Alerts](#) | [Events](#) | [Improving Security](#) | [Other Resources](#) | [Reports](#) | [Survivability Research](#) | [Training & Education](#)

Who We Are

The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise. It is located at the [Software Engineering Institute](#), a federally funded research and development center operated by [Carnegie Mellon University](#).

What We Do

At the CERT®/CC, we study Internet security vulnerabilities, provide incident response services to sites that have been the victims of attack, publish a variety of security alerts, do research in wide-area-networked computing, and develop information and training to help you improve security at your site.

What's New

- **[An Introduction to the OCTAVE Method: Jan 30, 2001](#)**
This new document details the characteristics, processes, and phases of the [OCTAVE](#) Information Security Risk Evaluation.
- **[Participate in the CERT/CC security survey: Jan 9, 2001](#)**
CERT/CC is conducting a study into the security practices of systems and network administrators. The aim of this study is to develop a set of incident response guidelines based on real experience. We encourage you to [participate](#).
- **[Results of the Security in ActiveX Workshop: Dec 21, 2000](#)**
Twenty invited experts address security issues related to ActiveX controls, identifying situations under which ActiveX and related technologies may be used safely. (pdf)

Search the CERT/CC web site

SEARCH
[Focused Search](#)

Communication & Reporting Procedures

- [Report an Incident](#)
- [Report a Vulnerability](#)
- [Sending Sensitive Information](#)
- [Incident Reporting Guidelines](#)
- [Detect and Recover from an Incident](#)
- [Subscribing to our mailing list](#)

Latest Alerts


Advisories & Incident Notes

- **CA-2001-02**
[Multiple Vulnerabilities in BIND](#)
- **IN-2001-01**
[Widespread Compromises via "ramen" Toolkit](#)
- **CA-2001-01**
[Interbase Server Contains Compiled-in Back Door Account](#)
- **CA-2000-22**
[Input Validation Problems in LPRng](#)

CIAC Homepage

Microsoft Internet Explorer
http://ciac.llnl.gov/ Go Search Keyword

Computer Incident Advisory Capability
"Keeping DOE Secure"




U.S. Department of Energy

CSTC	DOE-IS	CIAC-NT	FIRST
------	--------	---------	-------


Bulletins	Viruses
Hoaxes	Tools
Documents	C-Notes
	Chain Letters
Operating Systems	Security Resources

WARNING! Use of this system constitutes consent to security monitoring and testing. All activity is logged with your host name and IP address.



Latest Bulletins (2/2/2001)

- [The Ramen Worm \(L-040\)](#) Released (02/2/2001)
- [FreeBSD sort Uses Insecure Temporary Files \(L-039\)](#) Released (02/1/2001)
- [FreeBSD inetd ident Server Vulnerability \(L-038\)](#) Released (02/1/2001)
- [FreeBSD periodic Uses Insecure Temporary File \(L-037\)](#) Released (02/1/2001)
- [FreeBSD procfs Vulnerabilities \(L-036\)](#) Released (02/1/2001)
- [HP-UX Support Tools Manager Vulnerability \(L-035\)](#) Released (01/31/2001)
- [HP Security Vulnerability in man\(1\) Command \(L-034\)](#) Released (01/31/2001)
- [Sun Java Web Server Vulnerability \(L-033\)](#) Released (01/31/2001)
- [Class Loading Vulnerability in Sun Java \(TM\) Runtime Environment \(L-032\)](#) Released (01/30/2001)
- [Sun AnswerBook2 Vulnerability \(L-031\)](#) Released (01/30/2001)



What's New (11/15/2000):

Security Awareness and Training

- ▶ We keep saying that people are the biggest problem, so...
- ▶ Why not train them so we can get rid of (or reduce) the problem????
- ▶ What types of things would be useful?
 - General security training
 - passwords, social engineering, viruses
 - Administrator training
 - specialized training for specific OS and security devices (e.g. firewalls, IDS...), vulnerability/risk assessments,

System Penetration

From *Hacking Exposed*, 2ed

- ▶ Three steps before penetration occurs
 - Footprinting
 - Attempt to discover information related to Internet, intranet, remote access, and extranet activities for an organization.
 - Analogous to “casing a place for information”
 - Scanning
 - Non-intrusive probing
 - Analogous to “knocking on the walls to find all the doors and windows.”
 - Enumeration
 - Involves active connections to systems and directed queries.

Footprinting

- ▶ Step 1: Determine the Scope of your Activities
 - The entire organization or a specific location?
 - Open source research (look at their web page for example, also view the HTML source code, search for newsgroup postings by employees or partners, EDGAR (SEC)search...)
- ▶ Step 2: Network Enumeration
 - Attempt to identify domain names and associated networks (whois databases, internic)
- ▶ Step 3: DNS Interrogation
 - Determine host names and IP's (*nslookup* useful)
- ▶ Step 4: Network Reconnaissance
 - Attempt to determine information about the network
 - *traceroute*

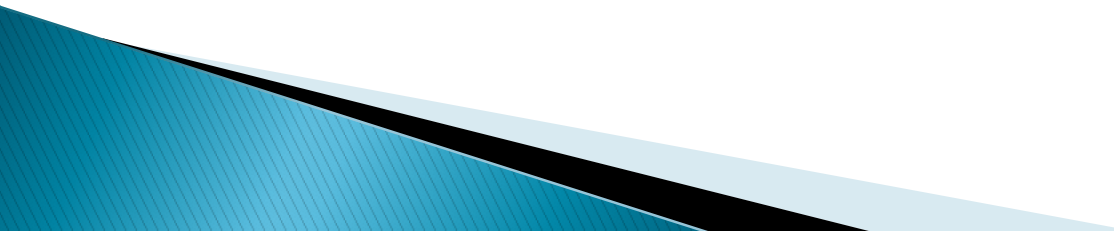
Scanning

- ▶ Network *ping* sweep to determine if systems are “alive” (number of tools to do this).
- ▶ ICMP queries to determine a number of different things
 - ICMP can request time (determine timezone of site) and address mask information (possibly orient your attack to specific subnets)
- ▶ Port Scanning – the process of connecting to TCP and UDP ports to determine what services are running or in a LISTENING state.
 - numerous tools to do this with different types of scans – *nmap* the “premier” tool

Enumeration

- ▶ Attempt to identify valid user accounts or poorly protected resource shares.
- ▶ Mostly operating system specific so will vary greatly depending on target
- ▶ A number of tools that are available for helping with this aspect.
 - As an example, *finger* in UNIX systems (for those systems still running it). Can provide usernames and idle times (e.g. is root active?)

Post-Enumeration

- ▶ After enumeration, serious penetration attempts begin.
 - ▶ One of the first steps is to determine if a known exploit exists for the system/services discovered:
 - CERT advisories
 - ▶ Seldom does penetration involve creating a new exploit or discovering a new vulnerability.
- 


SecurityFocus.com

SecurityFocus - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: <http://www.securityfocus.com/> What's Related

 **BUGTRAQ**

SecurityFocus.com

Our Services Sign-in Your Account About Us About This Site Advertise

Entire Site Search

Home The Basics Microsoft Sun Linux IDS Incidents Virus

September 11, 2001

News
Vulnerabilities
advisories
database
list of bids
statistics
Tools
Library
Products
Services
Multimedia
Bugtraq
Mailing Lists
Guest Feature

by vendor by title by keyword by bugtraq id by cve id

vendor

title version

- [2001-09-06: NetBSD 10ctl Denial of Service Vulnerability](#)
- [2001-09-06: NetBSD semop Arbitrary Code Execution Vulnerability](#)
- [2001-09-06: Microsoft Exchange OWA Global Address List Disclosure Vulnerability](#)
- [2001-09-06: DLink IP Fragment Denial Of Service Vulnerability](#)
- [2001-09-05: Baltimore Technologies WEBSweeper Restricted Directory Disclosure Vulnerability](#)
- [2001-09-05: Multiple IDS Vendor Encoded IIS Attack Detection Evasion Vulnerability](#)
- [2001-09-05: ShopPlus Cart Arbitrary Command Execution Vulnerability](#)
- [2001-09-05: GNU Mailman Empty Password Blank Salt Vulnerability](#)

Document: Done

QUESTIONS ??????????????????????

