

Information Security for Technical Staff

Module 7:

Prelude to a Hack

Networked Systems Survivability

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

© 2002 Carnegie Mellon University
© CERT, CERT Coordination Center and Carnegie Mellon are registered in the
U.S. Patent and Trademark Office



Instructional Objectives

Define Footprinting and discuss the basic steps to information gathering

Define Scanning and the various tools for each type of scan

- Ping Sweeps
- Port Scans
- OS Detection


Define enumeration and the types of information enumerated

- Windows enumeration
- Unix enumeration
- Network enumeration

Networked Systems Survivability

Overview

- Footprinting
- Scanning
- Enumeration



© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 3

The illustration shows a bald man in a blue shirt and shorts standing on a grassy hill, looking through blue binoculars. In the background, there is a multi-story building with a sign that says 'ABC Computers'. A yellow van with 'ABC' on its side is parked in front of the building. The scene is set in a green landscape with trees and a path leading to the building.

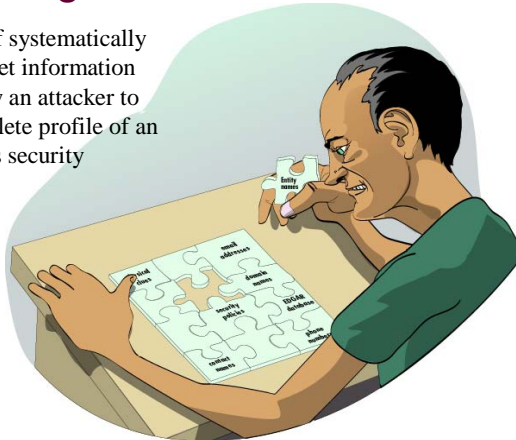
Footprinting, scanning, and enumeration are technical methods of gathering information crucial to aiding an intruder's attack.

Before a burglar breaks into a home it is natural that he first take the time to gather information, better known as casing, to help aid his intrusion. He wants to determine the best means of entry and identify deterrents such as a security alarm, watching neighbors, or a dog. System intruders must perform a similar type of casing before attempting an attack. They need to identify an entry point into the network that isn't blocked by a firewall or watched by an Intrusion Detection System.

The techniques used by hackers to case, or gather information about a system, include footprinting, scanning, and enumeration. These techniques are used to find weaknesses that can be exploited such as flawed operating system software, careless system administrators, or gullible privileged users.

Footprinting Defined

The fine art of systematically gathering target information that will allow an attacker to create a complete profile of an organization's security posture.



© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 4

Information is an intruder's greatest weapon and they must gather a wealth of it to execute a focused attack that won't be readily caught. What they end up with is a unique *footprint* or profile of an organization's Internet, remote access, and intranet/extranet presence. By following a structured methodology, attackers can systematically glean information from a multitude of sources to compile this critical footprint on any organization. [McClure 01]

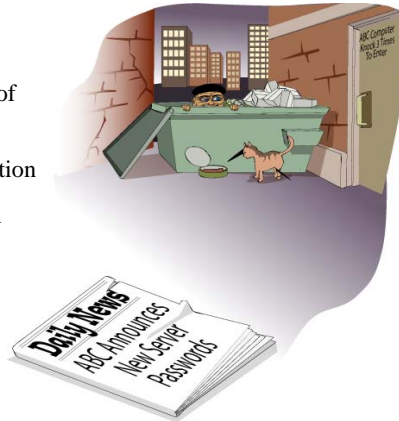
There are various ways an attacker can perform this network exploration. There are multiple sources to collect information and new tools released daily. It is important that an organization minimize the amount and types of information leaked by their Internet presence, while also implementing a vigilant monitoring practice.

These footprinting activities should also be done by system administrators for internal auditing to detect any vulnerabilities. Although it can prove to be a grueling task, it is imperative in order to determine the security posture of an organization.



Footprinting -1

- Step 1: Determine Scope of Activities
- Step 2: Network Enumeration
- Step 3: DNS Interrogation
- Step 4: Network Reconnaissance



Providing a step-by-step guide on footprinting is difficult as it is an activity that may lead down several paths. However, there are basic steps that should allow a thorough footprint analysis to be completed. [McClure 01]



Footprinting -2

Step 1: Determine Scope of Activities

Open Source Search

- Organization Websites
- Dumpster Diving
- News Articles/Press Releases
- Administrator Mailing Lists
- Social Engineering

Demo – Web weaving

Step 1: Determine the Scope of Activities

The first task is to decide the scope of the footprinting activities. Should the focus be on certain branches or the entire organization? Intruders research organizations in order to create a network diagram. Having a network diagram helps determine the scope of the testing and the time it takes to complete the scanning that is discussed later. [Stephanou 01]

The Internet provides a vast pool of resources that can be used to help narrow the scope of activities and provide insight as to the types and amount of information publicly available about a company and their employees. Organizations may be unintentionally revealing sensitive information about themselves.

For instance, organizations often have too much information listed on their website. Information including locations, related companies, merger or acquisition news, phone numbers, contact names and email addresses, security policies, and links to other web servers related to the organization can aid an attacker. In addition, the HTML source code may contain items that are not for public viewing buried in comment tags.

After studying web pages, attackers perform an open source search for information related to the target organization. These searches many times yield news articles or press releases that provide clues to the state of an organization. Additional searches can be performed against system administrators' mailing lists or postings such as UUNET where system specific technical issues are discussed. An example of this type of organizational leaking, *The Internet – Friend or Foe?*

by Lawrence Rogers, can be found at <http://www.cert.org/archive/pdf/homeusers/friendorfoe.pdf>.

For targets that are publicly traded companies, one can consult the Securities and Exchange Commission's EDGAR database at <http://www.sec.gov>. Searching these documents for 'subsidiary' or 'subsequent events' may reveal a merger. Entity names different from the parent company may surface. Chaos caused from rushing to connect an acquired entity to the network may leave security holes. [McClure 01]

Intruders also hunt for physical clues. One way of obtaining physical information about a company is to look through the trash, better known as "Dumpster Diving". *Dumpster Diving* is the description of the process of sifting through the garbage of companies searching for manuals, computer output, or other information on how to access corporate networks as well as ideas for social engineering attacks.

Student Workbook – Module 7: Prelude to a Hack

Social Engineering is a low-tech means of obtaining information. It is typically done by manipulating people inside the network into providing information that will grant access to an intruder. This technique has been proven to be very effective. Some of the most famous hackers of our time, Kevin Poulsen and Kevin Mitnick, owe their success to naïve employees and their own social engineering skills.

The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen by Jonathan Littman details the story of Poulsen who was the first computer criminal in America to be charged with espionage.

The Fugitive Game: Online with Kevin Mitnick by Jonathan Littman is a compelling, journalistic look at the events that led up to the capture of this fugitive hacker. This book includes conversations the author had with the hacker himself.

Footprinting -3

Step 2: Network Enumeration

Identify domain names and network addresses

- InterNIC, ARIN, allwhois.com

Queries

- Registrar
- Organizational
- Domain
- Network
- POC

Demo – Sam Spade

© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 7

Step 2: Network Enumeration

The first step to network enumeration is to identify domain names and associated networks related to a particular organization. To enumerate the domains and discover networks attached to them, you must query the domain registrar's whois databases. One of the most complete whois resources especially for finding whois servers outside of the United States is <http://www.allwhois.com>. Additional information on submitting searches can be found at: http://www.networksolutions.com/en_US/help/whoishelp.html

Whois queries may also be done online using a nice user interface from Sam Spade, www.samspace.org. This site has a slew of online tools including many that are discussed in this module, available at no cost to aid enumeration activities.

Following are the query types that yield the majority of information needed for hackers to begin their attack:

Registrar Query

The registrar query gives specific registrar information and associated whois servers. It is important to determine the correct domain registrar so that detailed queries can be submitted to the correct database in subsequent steps. The whois.crsnic.net server can be consulted to obtain a listing of potential domains that match the target and their associated registrar information.

Organizational Query

All information related to a particular organization is discovered with an organizational query. Once a registrar is identified (i.e. Network Solutions) an organizational query can be submitted. This searches for a specific registrar for all instances of the entity name and is broader than looking for a just domain name. There may be many domains associated with an organization, but they may just be registered for future use, or to protect trademarks. Further drilling may be required to find a live network.

Domain Query

A domain query yields all information related to a particular domain such as the registrant, the domain name, the administrative contact, the date the record was created and updated, and the primary and secondary DNS servers.

This information needs further analysis but may entice a hacker into a more focused attack. Voice and fax numbers are important for dial-in penetration. The administrative contact information can be used for

Student Workbook – Module 7: Prelude to a Hack

social engineering schemes. The dates of last registration are used to determine if the information is reliable or out of date. The DNS information can be used for DNS interrogation and the network range is a good starting point to use for the network query of the ARIN database, www.arin.net.

Network Query

This query displays all information related to a particular network or a single IP address.

The American Registry for Internet Numbers (ARIN) is another database that can be used to determine networks associated with the target domain. ARIN provides a handy web-based query mechanism. The database maintains specific network blocks that an organization owns. This is an important search to determine if a system is actually owned by the target organization or if it is being co-located or hosted by another organization or ISP.

Point of Contact (POC) Query

A POC query reveals all information related to a specific person, typically the administrative contact. It is advantageous to perform a POC query of the administrative contact since they may be the contact for multiple organizations.

Attack Scenario



Let's introduce and follow an intruder, Jack, who has harsh feelings towards and wants to attempt an attack on the company ABComp. Jack interviewed for this Silicon Valley startup company, and took the rejection personally. He started by looking at their website, and found they had only a single physical location.

Jack next consulted the `whois.crsnic.net` server to find potential domain names associated with this organization. He enters the following command at a UNIX command shell.

```
whois abcomp@whois.crsnic.net
```

The results yielded `abcomp.com` which Jack is confident is his targeted organization. He further queries to determine the registrar.

```
whois abcomp.com@whois.crsnic.net
```

This query gives Jack the domain name, the registrar, whois server, referral URL, and name servers. He can see that the registrar is Network Solutions, Inc. and is ready to perform the specific queries to obtain further information.

The organizational query may list numerous domain names associated with an organization, but they are not necessarily alive. As mentioned earlier, they may just be purchased for trademark reasons or for future use. Jack's organizational query with the keyword *name*, looks like this:

```
whois 'name ABComp'@whois.networksolutions.com
```

Based on these results, Jack again chose the most likely domain name, `abcomp.com`, and performs his domain query.

```
whois abcomp.com@whois.networksolutions.com
```

Jack now has the registrant, domain name, administrative contact, the date for the record creation and the DNS servers. He can determine with relative certainty at this point whether or not this is his target organization based on this information.

He now wants to find out if the network is owned by ABComp or if it is being co-hosted by another organization or ISP. The ARIN database is consulted to help answer this:

```
whois @whios.arin.net">"ABComp.com."@whios.arin.net
```

Student Workbook – Module 7: Prelude to a Hack

With one final query, the POC query, Jack attempts to obtain the list of all email addresses for this domain:

whois "@abcomp.com"@whois.networksolutions.net

Footprinting -4

Step 3: DNS Interrogation

Misconfigured DNS

Zone Transfers

- nslookup, axfr



© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 8

Step 3: DNS Interrogation

After all the associated domains have been identified, you can begin to query the Domain Name System (DNS). DNS is a distributed database used to map host names back to IP addresses and vice versa. It is possible to obtain revealing information about an organization if DNS is not configured securely.

One of the most serious misconfigurations a network administrator can make is allowing untrusted Internet users to perform a DNS zone transfer. A *zone transfer* allows a secondary master server to update its zone database from the primary master. The secondary server provides redundancy when running DNS should the primary become unavailable.

Some DNS servers are misconfigured and provide a copy of the zone to anyone that asks. The problem occurs when an organization does not use a public/private DNS mechanism to segregate their external DNS information (which is public) from its internal, private DNS information. This discloses internal hostnames and IP addresses to the attacker which is similar to providing a complete blueprint of an organization's internal network. [McClure 01]

There are several tools used to perform zone transfers. The most common are *nslookup* and *axfr*. Nslookup is a simple way to perform zone transfer. It returns the default name server that nslookup is querying, which is usually the organization's DNS server or a DNS server provided by an ISP. Axfr is a utility that recursively transfers zone information and creates a compressed database of zone and host files.

Another tool for querying DNS servers is *dig*. Dig (domain information groper), is a command line tool available with most versions of UNIX, with two modes for use. It can be used in simple interactive mode for single queries, or batch mode to execute a query for each in a list of several query lines. Dig is easier to use than nslookup, and is suited for use within shell scripts. For more information on using dig, visit www.rt.com/man/dig.1.html.

Attack Scenario



Using the information Jack gathered with the whois queries, he will now attempt to perform a zone transfer using the nslookup client that is provided with most UNIX implementations. With the domain query, he found that the name and IP address of the primary DNS server for ABComp is DNS.abcomp.com (10.10.10.5).

Student Workbook – Module 7: Prelude to a Hack

Because he wants to get any DNS records available, he will set the record type to *any* and then use the *ls -d* option to get all the associated records for the domain. Should he want to save and use this information later, Jack could also specify a file to which the results will be directed.

```
nslookup server 10.10.10.5 set type=any ls -d ABComp.com >> /temp/abc
```

The platform or type of operating system can be identified for some of the records in the output file. Jack can now use *grep*, *awk*, or *perl* to manipulate these records. For instance, let's suppose he wants to find test systems. Test systems are an intruder's favorite. Most likely, these systems do not have any security mechanisms employed and they're not monitored or logged. [McClure 01]

```
grep -i test /temp/abc |wc -l
```

Footprinting -5

Step 4: Network Reconnaissance

Discover Network Topology

- Traceroute
- VisualRoute



Demo – Traces

© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 9

Step 4: Network Reconnaissance

Now that we have identified potential networks, we can attempt to determine their network topology as well as potential access paths into the network. To accomplish this task, we can use *traceroute*. Available at <ftp://ftp.ee.lbl.gov/traceroute.tar.gz>, traceroute comes with NT and most flavors of UNIX.

Traceroute is a diagnostic tool that lets you view the route that an IP packet follows from one host to the next. This may allow an attacker to discover the network topology employed by the target network in addition to identifying access control devices (application-based firewall or packet-filtering routers) that may be filtering the traffic. [McClure 01]

It is beneficial for an intruder to map your entire network using traceroute. After running traceroute to multiple systems on the network, the intruder can begin to create a network diagram that depicts the architecture of the Internet gateway and the location of devices that are providing access control functionality. This is referred to as an *access path diagram*.

VisualRoute and *NeoTrace* perform traceroute and graphically display each network hop. *VisualRoute* will integrate it with whois queries. Although this tool is visually impressive, it does not scale well for large networks.

Attack Scenario



Jack will try to derive an access path diagram using traceroute. Again at his UNIX command line, Jack types:

```
traceroute DNS.ABCComp.com
```

With this command, he will see the path the packets traverse enroute to their final destination. There may be multiple routing paths. Also, there may be interfaces that deny the requests because of ACLs that have been applied. He needs to use additional switches or options to get past these access control devices.

One option, `-p n`, allows him to specify a starting UDP port number that is incremented by one. Adding the `-S` switch will stop the incrementation so that every packet is forced to a fixed port number and ideally passed through the access control device. For instance, UDP port 53 is used for DNS queries. Since he already knows the target system is a name server, it is probable that the device allows inbound DNS queries and will pass this packet. There are techniques such as *firewall protocol scanning* to determine specific ACLs that are in place, but that is beyond the scope of this discussion. [McClure 01]

Student Workbook – Module 7: Prelude to a Hack

Jack's new probe with specific port UDP 53 defined, looks like this:

```
traceroute -S -p53 10.10.10.5
```



Scanning Defined

The use of a variety of tools and techniques to determine what systems are alive and reachable from the Internet.



© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 10

The next step of information gathering after footprinting is scanning. We will now determine which of the discovered systems are alive and reachable from the Internet using a variety of tools and techniques such as ping sweeps, port scans, and automated discovery tools. [McClure 01]



Scanning

Ping Sweeps

Port Scans

OS Detection

Ping sweep tools help identify systems that are alive and can pinpoint potential targets. TCP and UDP scanning tools help to identify services that are listening and make some assumptions about the level of exposure associated with each system. Attackers then use OS detection software to determine with relative certainty the specific OS used by the target system. This information is key to mounting a focused attack.

Networked Systems Survivability

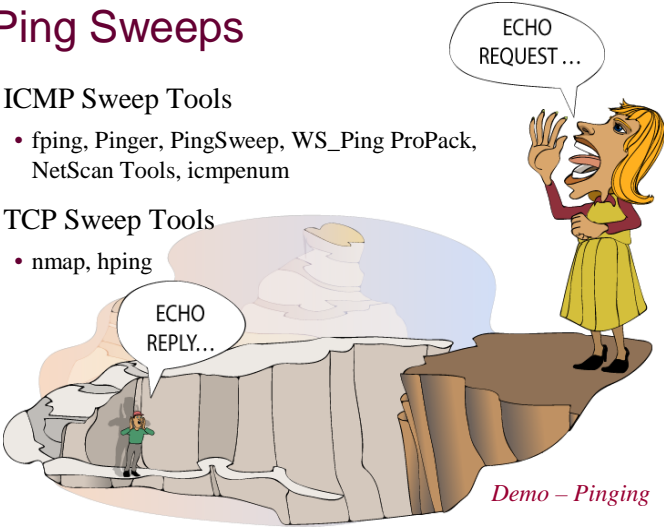
Ping Sweeps

ICMP Sweep Tools

- *fping*, *Pinger*, *PingSweep*, *WS_Ping ProPack*, *NetScan Tools*, *icmpenum*

TCP Sweep Tools

- *nmap*, *hping*



Demo - Pinging

© 2002 Carnegie Mellon University Module 7: Prelude to a Hack - slide 12

Determining if the System is Alive

One of the most basic steps in mapping out a network is performing an automated ping sweep. A ping sweep is an attack that sends Internet Control Message Protocol (ICMP) echo requests (“pings”) to a range of IP addresses, with the goal of receiving an ICMP ECHO_REPLY indicating the system is alive and can be probed for vulnerabilities. The *Ping* utility is acceptable to determine the number of systems alive in a small network, but it is inefficient for larger networks.

There are numerous ping sweep tools available for both UNIX and Windows. One such tool in the UNIX world is *fping*. This utility does not wait for a response from each target before moving on. It sends out mass ping requests making *fping* much faster than ping.

A freeware product, *Pinger*, is one of the fastest ping sweep utilities available for Windows. Commercial Windows products include *Ping Sweep*, *WS_Ping ProPack*, and *NetScan Tools*. These tools have nice graphical interfaces, but limit your ability to script and automate ping sweeps.

Another tool, *nmap* provides the capability to perform ICMP sweeps with an advanced option called *ping scan*. This option spews out TCP ACK packets to the target network and waits for returning RST packets, indicating which hosts are alive. This can elude some static packet filtering access control implementations (see Module 11).

A TCP ping utility, *hping* has functionality beyond *nmap*. It allows the user to control specific options of the TCP packet that may allow it to pass through certain access control devices. You can use *hping* to perform TCP ping sweeps and it has the ability to fragment packets, potentially bypassing some access control devices.

A handy ICMP enumeration tool, *icmpenum*, allows you to quickly identify systems that are alive by sending the traditional ICMP ECHO packets, as well as ICMP TIMESTAMP REQUEST and ICMP INFO requests.

If ICMP is blocked at the firewall, port scanning is the first technique to determine live hosts. By scanning for common ports on every potential IP address, an intruder can determine which hosts are alive if we can identify open or listening ports on the target system. This technique is somewhat time consuming and is not always conclusive.

Attack Scenario



Jack now wants to see which systems he learned of previously are alive. He could use `fping` that allows him to use the file he saved from his `nslookup` output using the `-f` parameter.

```
fping -f abc.txt
```

He may also choose to use the `-a` parameter to parse only those systems that are alive.

Nmap is a great tool for Jack to use for this:

```
nmap -sP -v -oN nmap-scan.txt 10.10.10.1-254
```

This command will perform a ping sweep on the IP range `10.10.10.1-254` and place the results of all live hosts in that range in a file called `nmap-scan.txt`. This file acts as his target list so he now has a list of hosts he can probe. [Stephanou 01]

The `-sP` option offers ping sweep capabilities which finds reachable machines. The `-v` option provides verbose output, and the `-oN` option saves the results in a human readable format.



Port Scans

- Identify both the TCP and UDP services running
- Identify the type of operating system
- Identify specific applications or versions of a particular service

Port Scan Types

TCP connect scan	TCP ACK scan
TCP SYN scan	TCP Windows scan
TCP FIN scan	TCP RPC scan
TCP Null scan	UDP scan
TCP Xmas Tree scan	<i>Demo – NMAP/Languard</i>

© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 13

Determine which Services are Running or Listening

Once you have determined which systems are alive using ICMP or TCP sweeps, you are ready to begin port scanning each system. Port scanning is the process of connecting to TCP and UDP ports on the target system to determine what services are running or are in a LISTENING state. Identifying listening ports is critical to determining the type of operating system and applications in use.

The following (but not limited to) objectives are to be accomplished when port scanning targets:

- Identify both the TCP and UDP services running on the target system
- Identify the type of operating system of the target system
- Identify specific applications or versions of a particular service

[McClure 01]

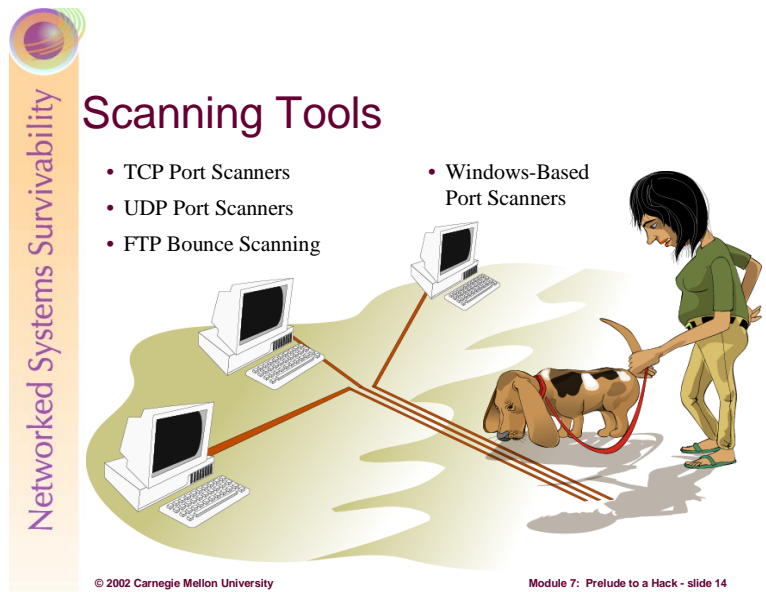
Different network services run on different ports. Active network services have a particular IP address (such as 10.10.10.5) and may be listening on one or more port numbers between 0 and 65535. [Norton 00]

Scan Types

There are various scanning techniques available many of which are incorporated into the *nmap* tool.

Scan Type	Description
TCP connect scan	This scan type connects to the target port and completes a full three-way handshake. It is easily detected by the target system.
TCP SYN scan	This technique is called half-open scanning because a full TCP connection is not made; a SYN packet is sent to the target port. SYN/ACK received - it is in a listening state. RST/ACK received - it is not listening. An RST/ACK will be sent by the system performing the port scan so that a full connection is never established. This is stealthier than a full TCP connect, and it may not be logged by the target system.
TCP FIN scan	This technique that usually only works on UNIX-based TCP/IP stacks, sends a FIN packet to the target port. The target system should send back an RST for all closed ports.
TCP Xmas Tree scan	This technique sends a FIN, URG, and PUSH packet to the target port. The target system should send back an RST for all closed ports.
TCP Null scan	This technique turns off all flags. The target system should send back an RST for all closed ports.
TCP ACK scan	This technique is used to map out firewall rule sets. It will help determine if the firewall is a simple packet filter allowing only established connections or a stateful firewall performing advance packet filtering.
TCP Windows scan	This technique may detect open as well as filtered/nonfiltered ports on some systems due to an anomaly in the way the TCP windows size is reported.
TCP RPC scan	Specific to UNIX systems, this technique is used to detect and identify Remote Procedure Call (RPC) ports and their associated program and version number.
UDP scan	This technique sends a UDP packet to the target port. If the port responds with an “ICMP port unreachable” message, the port is closed. If the message is not received we can deduce the port is open. UDP is known as a connectionless protocol and the accuracy of this technique is dependent on many factors related to the utilization of network and system resources. This type of scanning is also very slow and may produce unreliable results.

[McClure 01]



TCP and UDP Port Scanners

A good port scanning tool is critical to the footprinting process. There are many port scanners available for both UNIX and Windows. Following are the more popular and time-proven port scanners.

Strobe is a respected TCP port scanning utility that has been around for some time and is one of the fastest and most reliable scanners available. The features of *strobe* include the ability to optimize system and network resources and scan the target system in an efficient manner. In addition to efficiency, *strobe* grabs the associated banner (if available) of each port they connect to. This helps identify the operating system and the running service.

Strobe is reliable, but also has some limitations. It does not provide UDP scanning capabilities. *Strobe* only employs TCP connect scanning technology when connecting to each port. This adds to the reliability, but also makes ports scans easily detectable by the target system.

udp_scan, originally from the Security Administrator Tool for Analyzing Networks (SATAN), is one of the most reliable UDP scanners available. It does however, tend to trigger a SATAN scan message on many major IDS products.

Netcat or *nc* can perform many tasks including basic TCP and UDP port scanning capabilities.

The premier port scanning tool available is *nmap* which provides basic TCP and UDP scanning capabilities as well as incorporating other scanning techniques. *Nmap* makes it easy to scan a complete network and save the output to a separate file.

If you have discovered that an organization is using a simple packet-filtering device, *nmap* will fragment the packets and, therefore, makes it harder for access control devices or IDS systems to detect the scan. *Nmap* offers additional decoy capabilities such as launching decoy scans at the same time as the real scan. The target system responds to the spoofed addresses as well as the real port scan. The target site now has the burden of tracking down all the scans and determining which are legitimate and which are bogus.

Ident scanning is a technique most useful against a UNIX target. It is used to determine the identity of a user of a particular TCP connection by communicating with the authentication service on TCP port 113.

FTP Bounce Scanning

FTP bounce scanning technique is an attack with a dangerous method of laundering connections through an FTP server by abusing the support for “proxy” FTP connections. This FTP bounce attack can be used

to post virtually untraceable mail and news, hammer on servers at various sites, fill up disks, try to hop firewalls, and generally be annoying and hard to track down at the same time. You can bounce port scans off the FTP server to hide your identity or bypass access control mechanisms. This can be a slow process and many new versions of FTP server do not allow this type of activity to happen.

Windows-Based Port Scanners

NetScan Tools Pro 2000 (NSTP2K) is one of the most versatile discovery tools around offering just about every utility imaginable under one interface. Some of these utilities include: DNS queries including nslookup and dig with axfr, whois, ping sweeps, NetBIOS name table scans, and SNMP walks. This tool also has the ability to multitask.

There are less costly products such as *NetScan Tools*, but it has nowhere near the features of the professionally written NSTP2K.

SuperScan is available at no cost and is another fast and flexible TCP port scanner. The *Extract From File* option is especially convenient. It scans through any text file and extracts valid IP addresses and hostnames. When all hostnames are found you can perform a Resolve to convert all hostnames into numeric IP addresses in preparation for the port scan.

WinScan is a free TCP port scanner that comes in both graphical and command-line versions. The command-line version is popular because unlike the graphical version, it has the ability to scan Class C sized networks and its output is easily parsed.

ipEye can perform source port scanning, as well as SYN, FIN, and Xmas scans from the Windows command line. The limitations are that it only runs on Windows 2000 and only scans one host at a time. Source port scanning can potentially evade ACL controls by masquerading as inbound communications traffic such as DNS, SMTP, and HTTP.

WUPS is a windows UDP port scanner that is reliable, graphical, and relatively snappy even if it can only scan one host at a time for sequentially specified ports.

It is important to understand how to analyze the data that is received from each tool. Regardless of the tool used, you are trying to identify open ports that provide signs of the operating system.

Attack Scenario



For his scanning activities, Jack again chooses the nmap utility. He starts by editing the file he created with his ping sweep so that it contains only IP addresses. The results can now be used to perform a comprehensive port scan on the systems that he knows to be up. The purpose of this scan is to identify what services the target hosts are offering. Once this is established, Jack can decide which hosts to test for vulnerabilities. [Stephanou 01]

```
nmap -sT -vv -p 1-65535 -oN nmap-tcp.txt -iL nmap-scan.txt
```

This command will run a TCP port scan on all 65535 ports on all machines identified in the nmap-scan.txt file and have the output written to nmap-tcp.txt. Jack could also use the decoy capabilities (-D option) of nmap here to help his scans remain undetected.

Based on this information, Jack could try to make an educated guess as to what operating system is being used, or just use the -O option with nmap that uses TCP/IP fingerprinting to guess the remote operating system.

```
nmap -sT -O -D -vv -p 1-65535 -oN nmap-tcp.txt -iL nmap-scan.txt
```

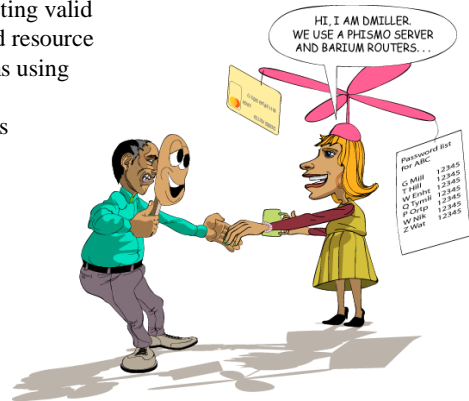
In this command, the -O option is the operating system detection, the -D option is used to hide the scan using many decoys, and the simple -sT option establishes the TCP connection or the three way handshake. The -v option seen earlier gives us verbose output. Hence, the -vv option gives us very verbose output.

Student Workbook – Module 7: Prelude to a Hack

The `-p` option is used to specify a range that is to be scanned, the `-oN` option is again used to save the results in human readable format. The final option used here, `-iL`, specifies the file to get targets from.

Enumeration Defined

A process of extracting valid account or exported resource names from systems using active connections and directed queries



© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 15

Through a process called *enumeration*, an attacker tries to identify valid user accounts or poorly protected resource shares. The enumeration discussed here is different from that discussed in footprinting as it is intrusive, involving active connections to systems and directed queries. Hence, these activities could be logged or otherwise noticed.

In general, once a valid username or share is enumerated, it's usually only a matter of time before the intruder guesses the corresponding password or identifies some weakness associated with the resource sharing protocol.



Enumeration

Operating System Specific Techniques

Types of information enumerated

- Network resources and shares
- Users and groups
- Applications and banners

Demo – NMAP

The information gathered through scanning is essential for the enumeration as these techniques are OS specific.

The information enumerated by attackers can be grouped into the following categories:

- Network resources and shares
- Users and groups
- Applications and banners



Windows Enumeration Techniques

Resources and Shares

- CIFS/SMB and NetBIOS
- Null Sessions

Users and Groups

- SNMP
- Security Identifier (SID) & Relative Identifier (RID)
- Active Directory

Applications and Banners

© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 17

Enumerating Windows Resources and Shares

Because of the Common Internet File System/Server Message Block (CIFS/SMB) and NetBIOS protocols that NT network services are dependant on, remote pilferers are able to obtain free information. Windows 2000 comes configured with these insecurities, but it does have the ability to run TCP/IP natively and live without NetBIOS.

Microsoft provides free Windows Resource Kits--a supplementary set of documentation and software utilities for administering Windows networks. These tools are a must-have for any Windows administrator. However, intruders can use many of these tools to gain valuable information--earning it the name "The Windows Hacking Kit". The Windows 2000 version of this kit has the same reputation. The Support\Tools folder of the server CD contains utilities that can aid an intruder.

The CIFS/SMB and NetBIOS standards include Application Programming Interfaces (API) that return rich information about a machine via TCP port 139—sometimes even to unauthenticated users. To access these APIs remotely, create an unauthenticated connection to an NT/2000 system using the "null session" command. This can be the single most devastating network foothold sought by intruders. [McClure 01]

```
net use \\192.168.202.33\IPC$ "" /u: ""
```

A connection is made to the hidden interprocess communications "share" (IPC\$), at the given IP address as the built in anonymous user (/u: "") with a null password (""). If successful, an attacker now has an open channel over which to attempt various techniques to pillage as much information as possible from the target: network information, shares, users, groups, Registry keys, etc. Many information gathering techniques take advantage of this out of the box security failing of Windows NT/2000. This is also known as the Red Button vulnerability, null session connections, or anonymous logon. [McClure 01]

When an intruder is well informed of an NT/2000 network, he tries to get a sense of what exists on the wire or "enumerate the NetBIOS wire," taking advantage of the NetBIOS naming services.

Most tools for enumerating the NetBIOS wire are built right into the OS. One such tool is a command-line utility called *net view*. Net view lists the domains on a network and the machines within. The information from the Ping Sweeps can convert the IP addresses to NetBIOS names of the machines.

Nbtstat is another OS built in tool. It calls up the NetBIOS Name Table from a remote system. This table contains information such as the machine name, the domain it belongs in, logged on users, services running, and the MAC address. The output is limited to a single host at a time and is coded in NetBIOS

Student Workbook – Module 7: Prelude to a Hack

service codes. This can be easily improved by the free tool *nbtscan* that works on an entire network and format the output in a user-friendly manner.

Primary and Backup Domain Controllers can be identified with the NT Resource Kit tool called *nltest*. Setting up a null session takes this a step further and share-enumeration tools such as *rmtshare*, *srvcheck*, and *srvinfo* can be used. *Rmtshare* generates output as done with net view, *srvcheck* displays shares and authorized users, and *srvinfo* lists shares and other potentially revealing information.

DumpSec (DumpACL), is one of the best tools for enumerating NT shares. It is available free from Somarsoft and audits everything from file system permissions to services available on remote systems.

Legion is a NetBIOS scanner that checks entire networks rapidly for exposed shares. It has a graphical interface and the newer versions include a tool that tries to connect to a given share using a list of passwords supplied by a user.

The NetBIOS Auditing Tool (NAT) is a graphical interface that not only finds shares, but attempts forced entry using user-defined username and password lists.

Mentioned earlier, a source of footprinting information is the Domain Name System (DNS). The Active Directory in Windows 2000 is based on DNS. In order for clients to locate Windows 2000 domain services such as the Active Directory, Windows 2000 relies on the DNS SRV record that allows servers to be located by service type and protocol. Hence, a zone transfer enumerates a lot of interesting network information.

A few other NT network enumeration tools include *epdump*, *getmac*, *netdom*, and *netviewx*. The features included in these tools include showing services bound to IP addresses and port numbers, displaying MAC addresses and device names of network interface cards on remote machines. *Netdom* is most useful as it enumerates key information about NT domains on a wire, including domain membership and the identities of Backup Domain Controllers. *Netviewx* is most commonly used to probe for the NT Remote Access Service (RAS).

Enumerating Windows' Users

The identification of usernames eliminates a lot of the effort in cracking an account because of easily guessed passwords. User information can be discovered as easily as shares. Again, there are utilities from the Resource Kit such as, *usrstat*, *showgrps*, *local*, and *global* that helps enumerate information about users along with a slew of other tools like *DumpSec*. *DumpSec* can pull a list of users, groups, and the system's policies and user rights.

To extract user accounts, shares, and trust accounts, there are various tools that set up and tear down a null session, extract information, and perform remote password guessing, and display the findings in a nice HTML report. Some of these handy tools worth mentioning are *Winfo*, *NbtDump*, *enum*, and *nete*.

If NetBIOS services are tightly secured, it may still be possible to obtain information if the Simple Network Management Protocol (SNMP) is running. Using *snmputil*, an SNMP browser from the Resource Kit, makes enumerating NT users simple. The information can be displayed nicely with a graphical SNMP browser called *IP Network Browser* from Solarwinds.

To identify accounts, there are two powerful enumeration tools *sid2user* and *user2sid*. These command line tools look up SIDs from username input and vice versa. The SID is the security identifier issued to an NT system at installation. Once the SID is known, intruders can use the numbers to enumerate the corresponding usernames. Using *user2sid* also gives the relative identifier (RID) that is predefined for users and groups. The Administrator user's RID is 500; the Guest user's is 501.

The first account created on an NT/2000 system is assigned a RID of 1000. Each subsequent object gets the next sequential number and the numbers are not reused. Once the SID is known, the intruder can use a script to enumerate every user and group.

UserDump enumerates the remote system SID and then uses expected RID values to collect user account names. *GetAcct* does this same technique with an added graphical interface.

The Active Directory within Windows 2000, from an enumeration point of view, could be the best source of information. The support tools that come with Windows 2000 include an Active Directory Administration Tool, *ldp.exe* that browses the contents of the directory. Existing users and groups can be enumerated with an LDAP query if an intruder has already compromised an account.

Windows Banner and Application Enumeration

The network and account enumerations were done through functions built into the OS. There are applications installed on NT/2000 that reveal even more information about the system. An intruder will try a technique called *banner grabbing* which is connecting to a remote application and observing the output. The software and version running on the server is enough to determine vulnerabilities.

Telnet is one of the popular mechanisms for enumerating banners and application information. *Netcat* is a more advanced probing tool. This tool is equally useful for the administrator as it is harmful if used by the attacker. The information gleaned from netcat will focus an intruder's effort as he can now concentrate on platform-specific techniques and known exploits.

There is information that can be obtained from the Windows registry if one knows where to look. It is difficult to gain access to the Registry as the default configuration only allows Administrators, and will not typically work over null sessions. An exception is the AllowedPath key specifying other keys to be accessible via null session.

Should an intruder gain access and be able to dump the Registry, there are tools to assist him: *regdmp* from the NT toolkit and *DumpSec*. The regdmp utility simply dumps the entire registry. DumpSec achieves the same thing, but with nicer output.

Attack Scenario



As most of these techniques require a null session, Jack will attempt to set one up in his quest for information. Assuming that TCP port 139 is listening from previous port scans:

```
net use \\192.168.202.33\IPC$ "" /u:""
```

This syntax connects to the hidden interprocess communications "share" (IPC\$) at IP address 192.168.202.33 as the built-in anonymous user (/u:"") with a null ("") password. If successful, Jack now has an open channel over which to attempt the various techniques discussed to pillage as much information as possible from the target: network information, shares, users, groups, Registry keys, and so on. [McClure 01]

Let's assume Jack was lucky enough to set up a null session on this target computer. He can now use a tool like DumpSec to generate a file containing user information.

```
dumpsec /computer=\\192.168.202.33 /rpt=usersonly /saveas=tsv /outfile=c:\temp\users.txt
```

He then uses a simple command to display the user information just retrieved and saved to users.txt

```
cat c:\temp\users.txt
```

[McClure 01]



UNIX Enumeration Techniques

Network Resources and Share Enumeration

Users and Group Enumeration

Applications and Banner Enumeration

SNMP Enumeration

UNIX Network Resources and Shares

UNIX, which relies on TCP/IP networking, is not likely to give up information as easily as NT does via NetBIOS. UNIX systems can still be enumerated; it just depends on the system and how well it is configured.

Scanning, that was discussed earlier, is one of the best ways to obtain UNIX network information. However, there are useful enumeration tools. One such tool *showmount*, will enumerate NFS-exported file systems (TCP port 2049), to see what directories are being shared. Showmount can be logged, so the requests may be detected.

The Network Information System (NIS), is another potential source for UNIX information. This distributed database of network information allows you to get NIS maps by using a simple RPC query (TCP port 111), once you know the NIS domain name of a server.

UNIX User Enumeration

The *finger* utility is a well known tool for enumerating users. Finger gives out user information and was a convenient tool back when the Internet was smaller. The most helpful information an intruder gets from this is who is currently logged on and possibly watching. One may also use this information for their social engineering tactics. Most system administrators will not leave the finger service (TCP port 79), running on their system.

Rusers and *rwho* (UDP port 513), are tools similar to finger. They return information about who is currently logged into the system. Again, admins generally turn these services off.

The Simple Mail Transfer Protocol (SMTP) (UDP port 161/162), contains two commands that assist with user enumeration. The first command, *VERFY* confirms the names of valid users. *EXPN* gives the actual delivery addresses of aliases and mailing lists. This information can assist an intruder with forging mail.

The biggest enumeration score would be obtaining the `/etc/passwd` file. The most popular way to obtain this file is through the Trivial File Transfer Protocol (TFTP) on TCP port 69. The common use of a shadow password file also removes the actual password hashes from the traditional password file. Again, most administrators will block this, but should an attacker be so lucky, they now have a list of users and a password file to crack.

UNIX Application Enumeration

In order for applications to talk to each other over the network, a protocol such as the Remote Procedure Call (RPC) is used. This protocol uses a program called portmapper (or rpcbind) to communicate between client requests. *Rpcinfo* is similar to finger, and can be used to enumerate RPC applications on remote hosts. The attacker may be able to find what applications the host is running. Using a tool like *pscan* will enumerate this information further.

Nmap is a great RPC scanning tool. With *nmap*, there is no need to guess program numbers (i.e. 100083) to determine if it is running. *Nmap* will do that for you. Telnet and netcat mentioned in the Windows section are equally useful enumeration tools for UNIX.

SNMP can provide helpful information to attackers. Many versions of UNIX come with a tool called *snmpwalk*. Queries conducted with *snmpwalk* provide information such as the UNIX version and kernel version running.

Attack Scenario



Jack is looking through his gathered information and choosing identified hosts that he wants to enumerate. He has concluded that the hosts he is intrigued by are UNIX machines.

Again, Jack is trying to be cautious as to not be noticed poking around the ABComp network. Hence, he will not attempt resource and share enumeration as the requests from tools such as showmount are usually logged.

He will however, check to see if the finger, rusers and rwho services have been left on. Having user names will help him if he wants to try social engineering, and also so that he can see who is logged on and for how long.

finger -l @hostname.abcomp.com

The *-l* option produces a multi-line format with all available information about a user. He will test for rwho and rusers in the same manner.



Network Enumeration Techniques

Routing Protocol Enumeration

- Border Gateway Protocol (BGP)
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Almost all routed networks these days utilize a dynamic routing protocol for managing routing tables. Examples are RIP, OSPF, IGRP, and BGP. There are methods for enumerating information from all of these. BGP, RIP, and OSPF will be addressed here.

The routing protocol used throughout the Internet, Border Gateway Protocol (BGP), is used to route IP packets to their destination. One can determine the networks associated with an organization by looking at the BGP routing tables. To perform BGP route enumeration:

1. Determine the Autonomous System Number (ASN) of the target organization.
2. Execute a query on the routers to identify all networks where the AS Path terminates with the ASN. [McClure 01]

This protocol relies on IP addresses and ASNs. The 16-bit integer ASN is purchased by an organization from ARIN to identify itself on the network. If you have the company name, you can do a whois search on the ARIN database. BGP is primarily used by larger organizations and core Internet routers, hence an ASN may not be found. One could try to use a known IP address to query a router in an attempt to discover the ASN, but this tedious process may only reveal that an ISP is announcing BGP messages on behalf of a customer.

The two most widely used standard routing protocols are the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). RIP is a distance vector protocol that maintains a list of the distances to other networks measured in hops. RIP broadcasts updates every 30 seconds in the form of a full route table. [Antoine 01]

RIP is UDP based (port 520/UDP) and therefore connectionless, so it will gladly accept a packet from anyone despite never having sent an original packet. RIP v1 has no authentication mechanism, allowing anyone to send a packet to a RIP router and have it picked up. RIP v2 has a rudimentary form of authentication allowing a cleartext password of 16 bytes, but of course, as you've learned by now, cleartext passwords can be sniffed. [McClure 01]

RIP is easily spoofable. An attacker can send packets to a RIP router, telling it to send packets to his desired destination instead of the intended system. If an attacker is able to spoof a legitimate router, it will accept and then employ unauthorized, malicious, or corrupted routing updates that would compromise the security or availability of a network. This would lead to re-routing of traffic, a denial of service, or simply give access to certain packets of data to an unauthorized person. [Antoine 01]

Student Workbook – Module 7: Prelude to a Hack

OSPF is a link state protocol that uses a link speed-based metric to determine paths to other networks. The updates that are sent via multicast are only sent when the network configuration changes. The update only includes changes to the network instead of the full route table. This protocol has more security mechanisms built in that limit an attacker's RIP spoofing ability. [Antoine 01]

A further discussion of OSPF including security features is covered in the routing section of Module 10: Securing Network Infrastructure.

Attack Scenario



Jack's final move will be to attempt to redirect the traffic through his own system so that he can listen to the traffic and possibly grab sensitive information such as passwords. For the RIP attack, he must first identify his target router by port scanning for UDP port 520, and then determine the routing table.

Being that Jack is remote and it is unlikely that he will be able to capture packets on the wire, he will use *rprobe* by Humble to find out what routes are available from the RIP router.

```
rprobe -v 192.168.51.102
```

[McClure 01]

He then uses a packet capturing software such as *tcpdump* in another window to read the router's response. His next step is to add a route to the RIP router to redirect the traffic through his system. He will need a tool such as *srip*, again from Humble, to accomplish this.

```
srip -2 -n 255.255.255.255 172.16.41.200 192.168.51.102 10.45.33.10 1
```

[McClure 01]

The first IP address is the Netmask, the second is the address of the machine Jack is redirecting to, the third is the address of the RIP router, and the final is the original packets' destination from ABCComp.

Jack must use *fragrouter* or kernel-level IP forwarding in order to further forward the packets he has captured. There are also Linux packet analyzers such as *dsniff* that can be set up to help reveal sensitive usernames and passwords. This score, if successful, would put ABCComp in the palm of his hand.



Review Questions

1. Define footprinting.
2. List the 4 steps for completing a footprint analysis.
3. Define scanning.
4. What are three objectives of port scanning?
5. Define enumeration.
6. What types of information can be enumerated?

© 2002 Carnegie Mellon University

Module 7: Prelude to a Hack - slide 20

1. Footprinting is the fine art of systematically gathering target information that will allow an attacker to create a complete profile of an organization's security posture.
2. The four steps to completing a footprint analysis are:
 - 1) Determine the scope of activities
 - 2) Network enumeration
 - 3) DNS interrogation
 - 4) Network reconnaissance
3. Scanning is the use of a variety of tools and techniques to determine what systems are alive and reachable from the Internet.
4. The three objectives of port scanning are:
 - 1) Identify both the TCP and UDP services running
 - 2) Identify the type of operating system
 - 3) Identify specific applications or versions of a particular service
5. Enumeration is a process of extracting valid account or exported resource names from systems involving active connections and directed queries.
6. The types of information that is typically enumerated are network resources and shares, users and groups, and applications and banners.



Summary

Footprinting
Scanning
Enumeration

Footprinting, scanning and enumeration are technical methods of gathering information crucial to aiding an intruder's attack. Now that we've seen some of the tactics used by hackers to gather information to aid their attack, what can be done to prevent it?

As mentioned, one of the most effective techniques is social engineering. The solution to this security risk of course is education and planning, including telling users that *nobody* in the organization will ever ask for their passwords for any reason. [Norton 00]

Depending on the host's operating system, there are utilities that can be run to notify when a port scan occurs. If an organization recognizes that they're being scanned, they should assume they're at risk of an attack and act accordingly. There are also tools that can be used to scan hosts to check for vulnerabilities such as weak passwords, missing or weak security such as anonymous FTP access, or accessible UDP or TCP ports. Keep current on security bulletins and advisories.

Prevention and protection tools are released almost as often as new security holes are discovered, and many times these tools are available at no cost. The core problem is that the system administrator has to close every single hole, while the attacker only needs to find a single exposure. [Stephanou 01]

References:

[McClure 01] McClure, Stuart, Scambray Joel, and Kurtz, George. *Hacking Exposed: Network Security Secrets and Solutions, Third Edition*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

[Norton 00] Norton, Peter and Stockman, Mike. *Peter Norton's Network Security Fundamentals*. Indianapolis, IN: Sams, 2000.

[Stephanou 01] Stephanou, Tony. *Assessing and Exploiting the Internal Security of an Organization*. SANS Information Security Reading Room, 2001. Available at:
http://www.sans.org/infosecFAQ/audit/internal_sec.htm

[Antoine 01] Antoine, V., Bosmajian, P., Duesterhaus, D., Dransfield, M., Eppinger, B., Houser, J., Kim, A., Lee, P., Opits, D., Wiacek, M., Wilson, M., and Ziring, N. *Router Security Configuration Guide*. National Security Agency, Report Number: C4-054R-00, November 2001. Available at:
<http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf>