Penetration Studies - A Technical Overview

Timothy Layton

“Penetration Studies – A Technical Overview”

GSEC Practical Assignment Version 1.3
December 12, 2001

For GIAC Certification in
Security Essentials

Timothy P. Layton, Sr.
May 30, 2002

Table of Contents

1 ABSTRACT

Jessica Lowery wrote a fantastic paper on penetration testing and it is located in the SANS Reading Room at http://rr.sans.org/penetration/third_party.php. The title of the paper is: Penetration Testing: The Third Party Hacker. Jessica's paper did a great job of outlining and defining what penetration tests are and how an organization should view and use them.

This paper builds on Jessica's research paper by drilling down on some of the most common tools and applications used to perform penetration tests. Penetration tests can be performed externally and/or internally. This paper takes the position of an unauthorized external user with no specific knowledge of the target network other then what is available via public information and what the malicious user can glean from the output of his tools and applications.

This paper will utilize tools that are freely available to any user on the Internet. Many commercial applications are available to perform many of the same tests and can cost thousands of dollars. It is unlikely that the typical malicious user is going to purchase commercial tools and attempt a hack on an organization. To this end, the focus of this paper is on freely available tools with the majority of them on the Unix platform. This paper will stop at identifying potential vulnerabilities, although some penetration studies may involve the security engineer attempting unauthorized access or to exercise the potential exploit.

This paper is divided into two parts: "Tools of the Trade" that identifies various tools for penetration testing and the second part is the technical breakdown and "how-to" of reconnaissance, scanning, and vulnerability testing.

All organizations with Internet facing assets should have a formal information security plan that is supported by the management team. Part of any security lifecycle plan should include internal and external penetration studies performed by trained employees and by an outside firm to validate the organizations security posture. The entire enterprise information security plan is outside the scope of this paper, but at a high level all plans should strike a balance of people, technologies and operations for that particular business. Organizations have different tolerances to risks, varying cultures and management styles, and different exposures based on current configurations of assets. Information security plans are living business processes that must be able to adapt and change with internal and external variables. The key to managing risk is constant monitoring and management of the existing plan.

2 TOOLS OF THE TRADE

2.1 OVERVIEW

The normal pattern for a malicious user to gain information on a target host or network starts with basic reconnaissance. This could be as simple as visiting an organizations web site or sites or using public tools to learn more information about the targets domain registrations. After the attacker has gained enough information to their satisfaction the next logical step is to scan for

open ports and services on the target host(s) or network. The scanning process may yield very important information such as ports open through the router and firewall, available services and applications on hosts or network appliances, and possibly the version of the operation system or application. After an attacker has mapped out available hosts, ports, applications, and services the next step is to test for vulnerabilities that may exist on the target host or network. This paper will stop at identifying potential vulnerabilities but an actual attacker may proceed with an attack to attempt to exploit the asset. This attack could range from denial of service, compromise the host for the purpose of launching other attacks, or to an application or operating system exploit. Typically, if the attacker has chosen to gain access to the host he or she will attempt to keep access and cover their tracks. Covering of tracks most always involves the tampering of logs or logging servers. The defense in-depth strategy is one of a layered approach and assumes the perimeter network can be compromised. With this in mind, it is critical to protect logs and logging servers. In the case of an actual intrusion, many times all an organization is left with is their logs. Protect them accordingly because this may be your only evidence of the incident.

2.2 RECONNAISSANCE

The reconnaissance phase potentially has many faces and depending on the goal of the attacker various tools and techniques will be utilized (11). Although there are several other tools available the tools and applications listed below are likely used in most reconnaissance efforts.

The most common tools used for reconnaissance are:

- Nslookup (Available on Unix and Windows Platforms)
- Whois (Available via any Internet browser client)
- ARIN (Available via any Internet browser client)
- Dig (Available on most Unix platforms and some web sites via a form)
- Web Based Tools (Hundreds if not thousands of sites offer various recon tools)
- Target Web Site (The client's web site often reveals too much information)
- Social Engineering (People are an organizations greatest asset, as well as their greatest risk)

2.3 SCANNING

After the penetration engineer or attacker gathers the preliminary information via the reconnaissance phase, they will try and identify systems that are alive. The live systems will probed for available services. The process of scanning can involve many tools and varying techniques depending on what the goal of the attacker is and the configuration of the target host or network. Remember, each port has an associated service that may be exploitable or contain vulnerabilities.

For example, if the target network has ICMP disabled then the tools to gain the information may change or the switches they use will be different. The fundamental goal of scanning is to identify potential targets for security holes and vulnerabilities of the target host or network. Scanning while based on science is definitely considered an art by those who possess the skill.

The art of scanning comes to bear when an attacker is patient and performs precision scans on target devices and based on the results of the scan data can narrow down potential exploits and vulnerability based on their experiences. Nmap is probably the best known and most flexible scanning tool available today. It is one of the most advanced port scanners available today and offers more features than I have seen in any other port scanner. Nmap provides options for fragmentation, spoofing, use of decoy IP addresses, stealth scans, and many other features.

Below is a list of some common tools to perform scanning:

- Telnet (Can report information about an application or service; i.e., version, platform)
- Nmap (powerful tool available for Unix that finds ports and services available via IP)
- Hping2 (powerful Unix based tool used to gain important information about a network)
- Netcat (others have quoted this application as the "Swiss Army knife" of network utilities)
- Ping (Available on most every platform and operating system to test for IP connectivity)
- Traceroute (maps out the hops of the network to the target device or system)
- Queso (can be used for operating system fingerprinting)

Nmap is the most widely used tool by the good guys and bad guys to gain an understanding of what ports and services that may be available on a target host or network. Nmap is very versatile and can be very cryptic to the new user. Nmap is probably the most used tool for the purpose of port scanning and operating system identification independent of commercial vs. open source software. Most security people use nmap via the command line because you can build shell scripts or Perl programs to aid in the scanning process. Table 1A below is a general overview of some of the common switches used most frequently (9). For a partial listing of the most common options execute "nmap –h" from the command line or you can use the man pages by typing "man nmap". As of the writing of this paper, nmap version 2.54 Beta 33 is the most current release. The listing below illustrates the output of "nmap –h".

```
-=[toolbox]=- -1:29am- ~/nmap/# nmap -h
Nmap V. 2.54BETA33 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
```

-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
-iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
--interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

The inexperienced user of nmap can be quickly overwhelmed by the available options. In Table 1A below is a brief outline on some of the most important switches (9).

Table 1A

Type of Scan	Switch	Summary of Scan Characteristics
TCP Connect	-sT	Completes the full three-way handshake with each scanned port. Not very stealthy..
TCP SYN	-sS	Only sends the initial SYN and awaits the SYN-ACK response to determine if a port is open. If the port is closed, the target will send a RST or possibly nothing. A little stealthier than TCP Connect scans.
TCP FIN	-sF	Sends a TCP FIN to each port. A RST indicates the port is closed, while no response may indicate the port is open. Stealthier than TCP Connect scans.
TCP Xmas Tree	-sX	Sends a pack with the FIN, URG, and PUSH bits set. Again a RST indicates the port is closed, while no response may mean the port is open.
NULL	-sN	Sends packets with no code bits set. RST indicates the port is closed, no response may mean the port is open.
TCP ACK	-sA	Sends a packet with the ACK bit set to each target port. Allows for determining a packet filter's rule regarding established connections.
Window	-sW	Similar to the TCP ACK scan, but focuses on the TCP Window size to determine if the port is open or closed a variety of operating systems.
FTP Bounce	-b	Bounces a TCP scan off of an FTP server, obscuring the originator of the scan.
UDP Scan	-sU	Sends UDP packet to target ports to see if the UDP service is listening.
Ping	-sP	Sends ICMP echo request packets to every machine on the target network, allow for locating live hosts. This is network mapping, not scanning..
RPC Scan	-sR	Scans RPC services, using all discovered open TCP/UDP ports on the target to send RPC NULL commands. Attempts to determine if an RPC program is listening at that port, and if so, identifies what type of RPC program.

2.4 VULNERABILITY TESTING

Vulnerability testing is the act of determining which security holes and vulnerabilities may be applicable to the target network or host (16). The penetration tester or attacker will attempt to identify machines within the target network of all open ports and the operating systems as well as running applications including the operating system, patch level, and service pack applied.

The vulnerability testing phase is started after some interesting hosts are identified via the nmap scans or another scanning tool and is preceded by the reconnaissance phase. Nmap will identify if a host is alive or not and what ports and services are available even if ICMP is completely disabled on the target network to a high degree of accuracy.

One of the best vulnerability scanners available today just happens to be free. Nessus is available at the following URL: http://www.nessus.org. As of May 2002 Nessus tests for over 920 specific vulnerabilities. The Nessus tool is well supported by the security community and is comparable to commercial products such as ISS Internet Security Scanner and CyberCop by CA. Any organization serious about identifying risks should use Nessus as a part of their tool bag.

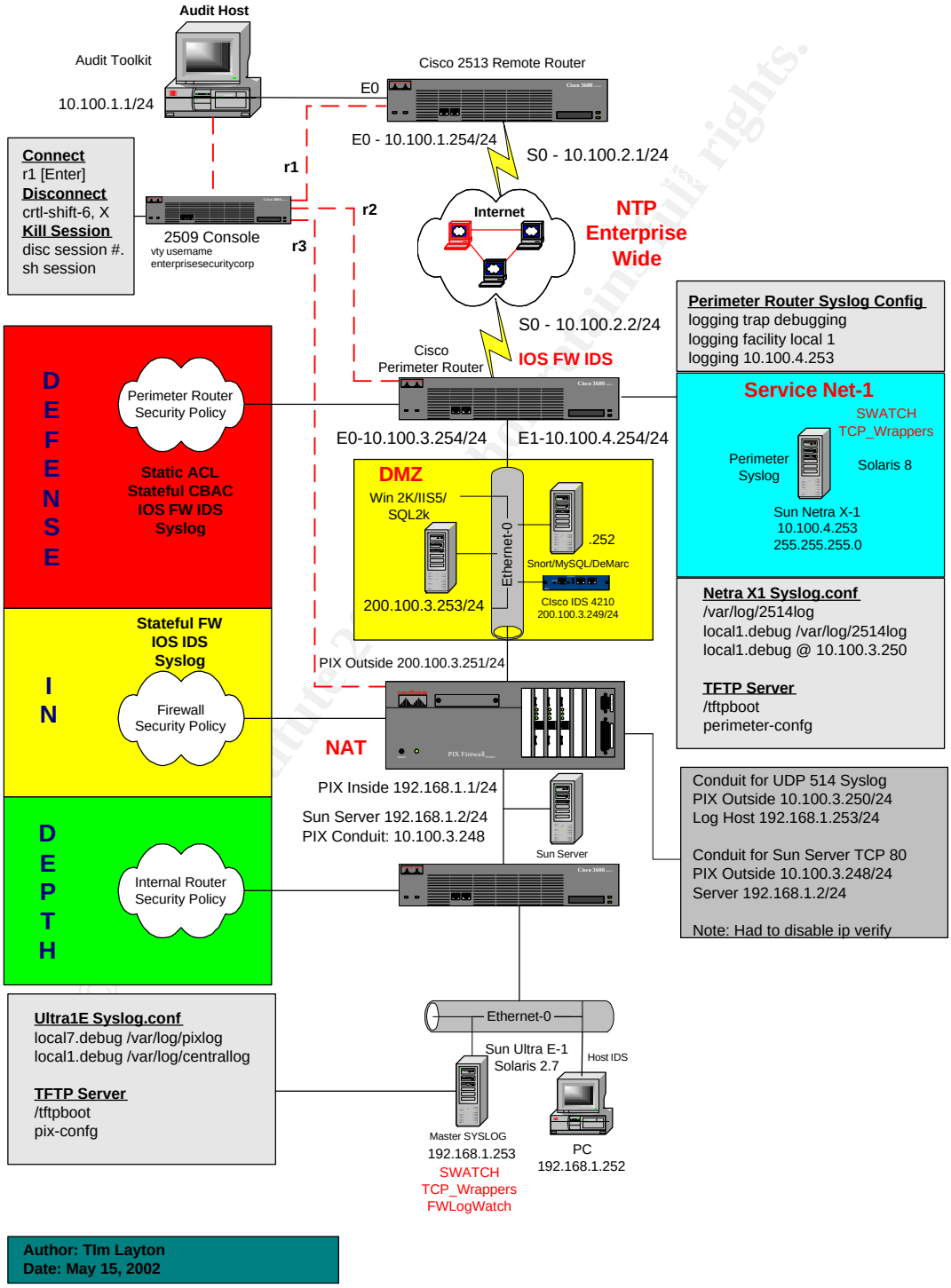
Other free vulnerability scanners include; SARA available at http://www-arc.com/sara/, a special version of SARA is available to specifically test for the SANS/FBI Top 20 most critical Internet security vulnerabilities located at http://www.sans.org/top20.htm. SARA and SAINT are both predecessors of SATAN a security administrator's tool for analyzing networks by Wietse Venema and Dan Farmer.

Once an attacker has gained a list of potential vulnerabilities for specific hosts on the target network they will take this list of vulnerabilities and search for specific exploit to utilize on their victim. Several vulnerability databases are available to anyone on the Internet. Refer to the table directly below for a sample listing.

Vulnerability Databases	
ISS X-Force	http://www.iss.net/security_center/
Security Focus Database	http://online.securityfocus.com/archive/1
InfoSysSec Database	http://www.infosyssec.com/
Exploit World	http://www.insecure.com/sploits.html

2.5 LAB NETWORK DIAGRAM

For the purpose of this paper I built the following lab to illustrate the various tools and technologies discussed in this paper.



3 RECONNAISSANCE

3.1 OVERVIEW

The next few three sections: Reconnaissance, Scanning, and Vulnerability Testing are technical "how-to" briefings for each of the tools discussed. The reconnaissance phase of penetration testing is very important. It is equivalent to a carpenter building a house; he must identify the tools he will need to perform his job and he must already know what the plan is in order to execute. The tools I have chosen to list in this section are non-evasive tools and could be used by any Internet user. All organizations must be careful of the type of information they publish.

3.2 NSLOOKUP

The nslookup program is included with Microsoft Windows and basically all flavors and versions of the Unix operating system, so the application is ubiquitous and widely available.

Nslookup is a method to map IP addresses for a particular domain. DNS servers contain all of the information on a particular domain needed to communicate with the network. The MX record is for mail and A records for hosts. Another technique is to simply try and ping the domain name "ping target.com or www.target.com". Then you can do a reverse lookup on the returned IP address.

As an example I will test with the Notarealdomain.org domain. The listing directly below was from a Windows 2000 client.

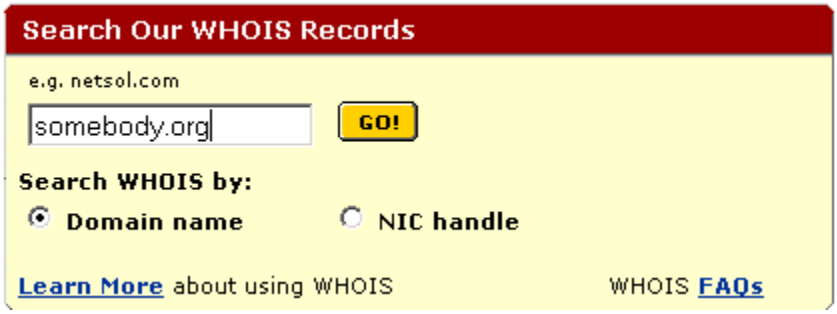
```
Microsoft Windows 2000 [Version 5.00.2195](C) Copyright 1985-1999 Microsoft Corp.

C:\>nslookup
> server ns.xxxx.com Default Server:  ns.xxxx.com
Address:  10.1.1.241
> notarealdomain.org.
Server:  ns.xxxx.com
Address:  10.1.4.241
Name:    notarealdomain.org
Address:  10.1.1.40
```

3.3 WHOIS

A great place to start when profiling an organization is to use the "whois" application. Many organizations including Verisign publish a publicly available whois server on their web site. The Verisign whois application is located at: http://www.netsol.com/cgi-bin/whois/whois

For the purpose of this paper I will use the Notarealdomain.org domain as a generic example and substitute with others in order to illustrate a particular point.

I simply went to the above mentioned link and typed in "notarealdomain.org" in the search box.



The results are listed below.

Search Results:

Registrant:
The Somebody Org (Somebody-DOM)
123 Street
Somewhere, USA 12345
US
Domain Name: Notarealdomain.org
Administrative Contact:
Domain Administration, Somebody (DAXXXXX-OR) domain@notarealdomain.org
Somebody Org
Suite 1 123 Street Ave.
Town, CA 90210
US
111-555-1212 Fax- 111-555-1234
Technical Contact:
XXXX, Jeff (XXXX) xxxx@somedomain.COM
ISP, Inc.
123 Street
Colorado Springs, CO 80921
US
111-222-3333
Record expires on XX-Aug-2009.
Record created on XX-Aug-1995.
Database last updated on 3-Jun-2002 16:14:38 EDT.
Domain servers in listed order:
SERVER.xxx.ORG x.x.x.40
NS.xxxx.COM x.x.x.241
NS2.xxxx.COM x.x.x.117

All sorts of interesting information can be gleaned from the "whois" output.

1.) The physical address of the organization.
2.) The "Admin" contacts name, address, phone number, NIC handle and email address.
3.) The address of the admin contact is different from the domain.
4.) The "Technical" contact name, address, phone number, NIC handle, and email address.
5.) The address of the technical contact is different from the admin, but the same as the domain.
6.) A listing of their DNS servers in order of precedence.

A potential hacker could use any or all of this information against an organization for the purpose of an attack. He or she knows a lot of important information in the first 30 seconds or research.

At a high level organizations should try and leverage role based accounts in lieu of individual account for both security reasons and ease of administration. The Verisign web site publishes the following information about role based accounts.

The difference between an individual contact record and a role account contact record

A role account contact record allows many people to fulfill one function for a domain name. Let´s take the Billing Contact, for example. You might want your e-mailed renewal notices sent to your Accounts Payable department, instead of having them sent to one person within your Accounts Payable department. Creating a role account contact record, and entering an e-mail address that everyone in your Accounts Payable department can access ensures this will happen.

An individual contact record is a lot like a role account contact record, except there´s only one person fulfilling that function. In a certain sense, this is a more secure than a role account contact record. If a request to update a domain name is received, chances are really good you´ll be able to pinpoint the exact person who made the request. However, if that individual leaves your company, you´ll have to ask one of the other Guardians to update the domain name to replace that person.

The registrant (the person or company to whom the domain name is registered) always has final authority on a domain name.

In addition Verisign gives an organization the following option in they don't want their record published with full whois information:

Q: What if I don't want my information to be in WHOIS?

A: ICANN requires that we provide full WHOIS information for each domain name we register. You may, however, have your domain name removed from the list of bulk registration records that we maintain. Please go to http://www.networksolutions.com/privacy if you want to take advantage of this feature.

To learn more about how to use the Verisign whois application go to the following URL: http://www.netsol.com/en_US/faq/whois/whois-learnmore.jhtml

Next, the "whois" application example is provided from a Unix command line:

```
-=[toolbox]=- -3:22pm- ~# whois notarealdomain.org
```

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

Domain Name: Notarealdomain.org
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS.xxxx.COM
Name Server: xxxx.COM
Name Server: SERVER.Notarealdomain.org
Updated Date: 05-nov-2001
>>> Last update of whois database: Mon, 13 May 2002 04:54:42 EDT <<<
The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and Registrars.

As you can see form the above output, not as much information is provided as in the web based Verisign tool.

The whois application can leverage other services such as ARIN which is discussed I the next section.

Here is the output of a Unix based whois using the ARIN host.

-=[toolbox]=- -3:45pm- ~# whois -h rs.arin.net x.x.x.10
Manoa Innovation Center (NET-XXX) XXX x.x.x.1 - x.x.x.255
Digital Island, Inc. (NETBLK-XXX-XXXX-E) MIC-XXXX-E
x.x.192.0 - x.x.207.255

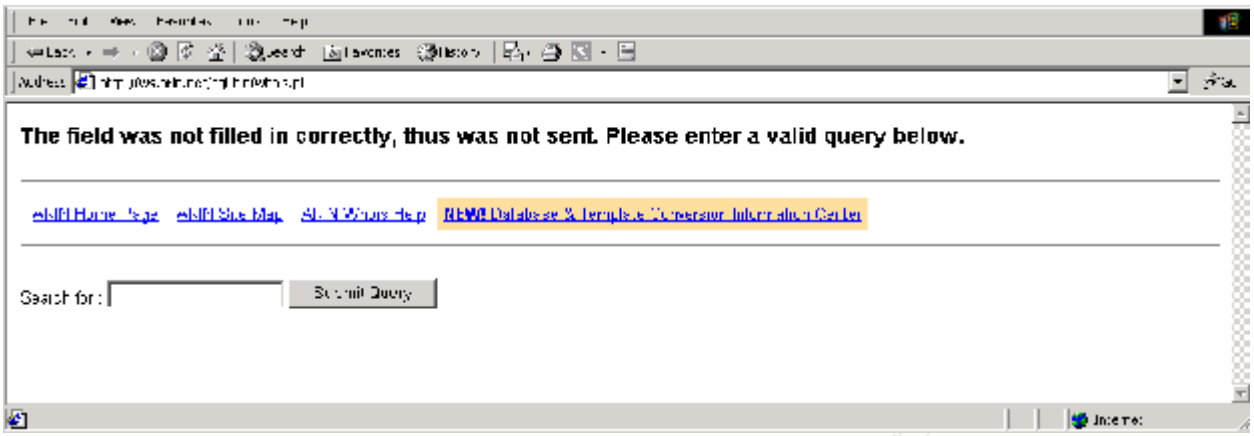
The x.x.x.10 address was captured from the first nslookup command for notarealdomain.org. The above output tells us who hosts the IP range for notarealdomain.org and the block of addresses that they may possess. It is possible that notarealdomain.org is not allocated all subnets between 192 and 207. But many times this technique will return the actual IP subnet of an organization and the potential attacker knows what range of IP address to target for an attack or exploit.

3.4 ARIN

ARIN is an acronym used to describe the American Registry for Internet Numbers. The ARIN whois application can be found online at: http://www.arin.net/whois/arinwhois.html

ARIN´s Whois program searches ARIN´s database to locate information on networks, autonomous system numbers (ASNs), network-related handles, and other related Points of Contact (POCs). This search tool will not provide information relating to domains, military networks (NIPRNET) or networks registered through RIPE NCC or APNIC. (12) ARIN is very useful when you are trying to determine the IP subnet of an organization.

In the “whois” section above I combined whois and ARIN together to locate the information I was seeking. The same information can be found via the ARIN web site as well at other web sites such as www.network-tools.com.



Simply enter the target IP address in the "Search for" field and review the results to determine if the output is helpful or not.

The www.network-tools.com web site is another very useful link when researching a domain or organization.

3.5 DIG

Dig is a tool used to interrogate a DNS server for information among other things. Of particular interest to attackers is the version of the name server the organization may be using. Many organizations use BIND and the snapshot below illustrates the output of the dig command on the notarealdomain.org primary name server.

It is very trivial to change the version information of a BIND server. In the servers configuration file add the following directive:

```
options {
        version "Not Telling You!";
};
```

Although this modification is quite simple, many organizations do not realize that providing their version of BIND is a potential security related risk. All an attacker would have to do is go research an exploited targeted at their version of BIND and launch the attack on the target via port 53. This could be something as simple as a buffer overflow vulnerability or it could lead to a complete host compromise. Depending on the trust placed on the server in question, other network assets could be compromised as well.

```
<<>>Dig 9.2.1 <<>> @x.x.x.40 version.bind txt chaos
;; Got answer:
;; ->>HEADER<<-
;; flagsL qr aa rd ra; QUERY 1, ANSWER 1, AUTHORITY 0, ADDITIONAL 0
Answer Section:
VERSION.BIND. – CH TXT "8.2.2-P7+sig+infoleak"
Query Time: 130 msec
```

Several vulnerability databases are available via the Internet at:

Vulnerability Databases	
ISS X-Force	http://www.iss.net/security_center/
Security Focus Database	http://online.securityfocus.com/archive/1
InfoSysSec Database	http://www.infosyssec.com/
Exploit World	http://www.insecure.com/sploits.html

3.6 WEB BASED TOOLS

Several web based reconnaissance tools are available to both good guys and bad guys. It is important for an organization to realize these types of tools exist and they can be potentially used against them. Many of these sites are reputable but some may not be and you should be very cautious of which sites you use.

Some example sites are located at the following URL's:

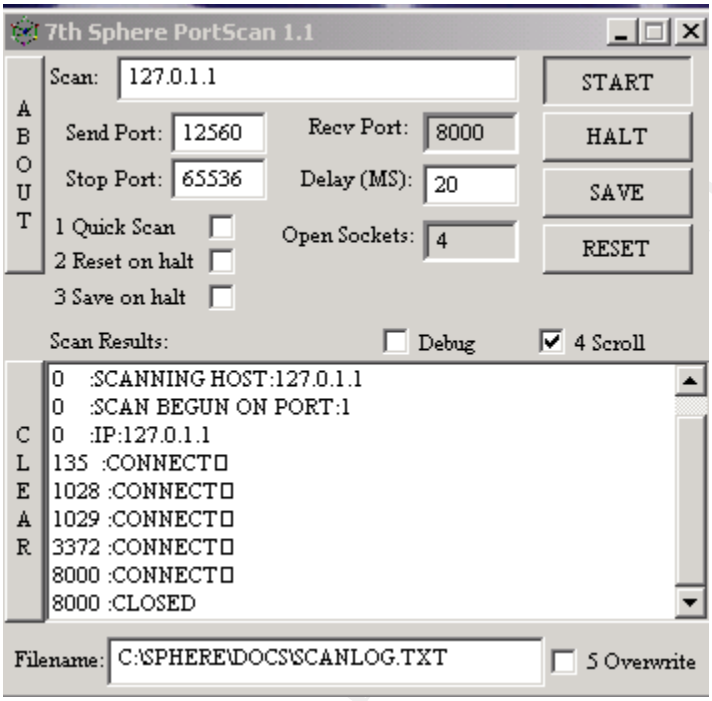
Web Based Tools	
Various Recon Tools	http://www.network-tools.com/
Various Recon Tools	http://nettool.false.net/
Lots of Recon Tools	http://www.samspade.org

Visual Traceroute (very powerful!)	http://www.visualware.com/visualroute/livedemo.html

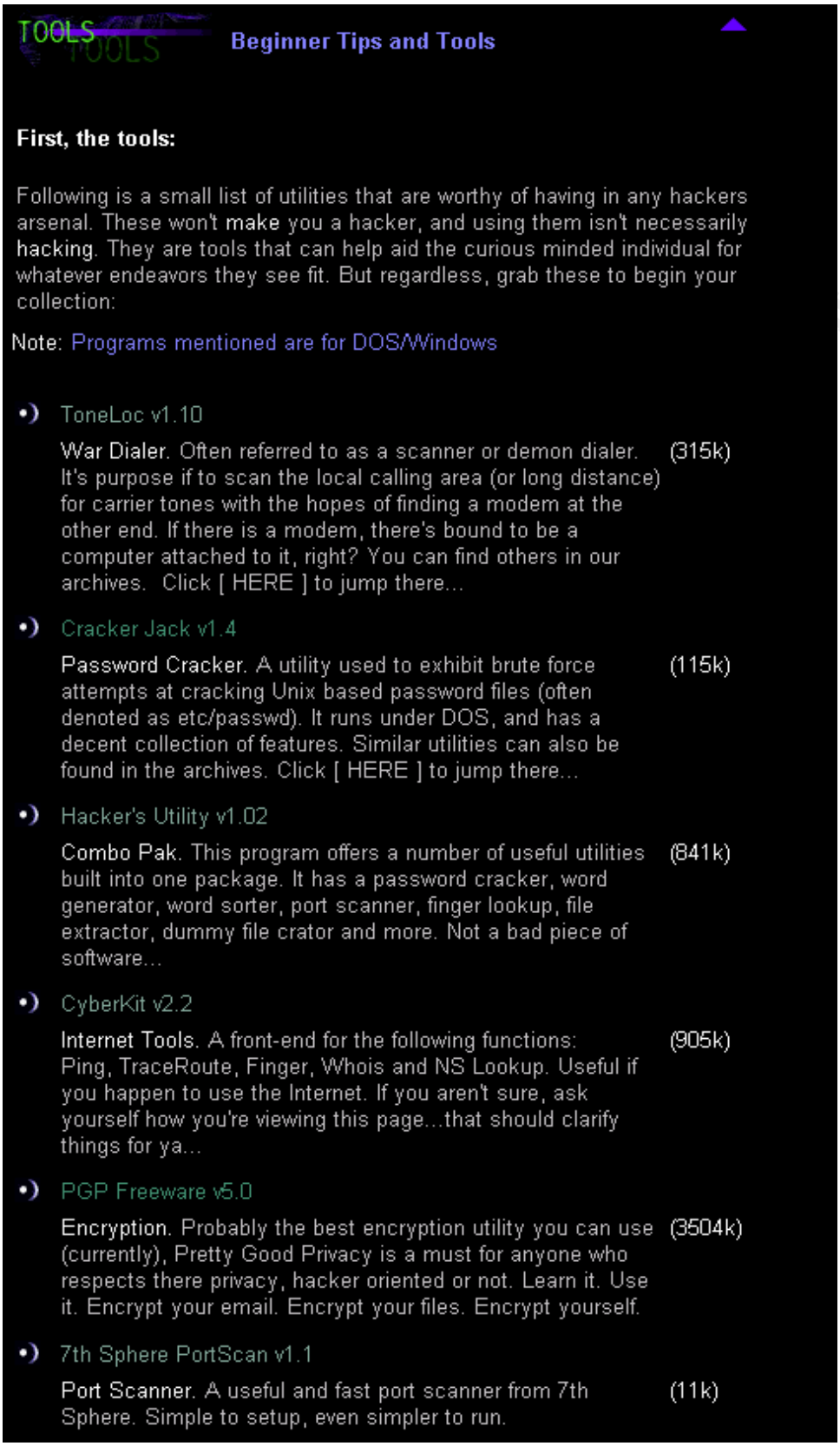
4 SCANNING

4.1 OVERVIEW

Several tools are available for scanning. The staples of scanning (nmap and hping2) are covered in detail in the next few sections. It is important to note that many scanners are available for platforms other than Unix and Linux including Microsoft Windows. A tiny (25k) Windows based port scanner 7th Sphere Portscan 1.1 is available from numerous sites including www.hackers.com.



http://www.hackers.com/html/neohaven.html



Port scanners are like other tools. When you go to the hardware store to purchase a hammer, there are many hammers on the shelf. To the untrained person all the hammers seem to be the same and to some degree this is true. They will all drive a nail at the end of the day and likely get the job done. One must ask—why are there so many different hammers? The answer is: there are different hammers because there are different goals.

The above mentioned scanners will report open ports on a host but they are not built for stealth or for scalability. Nmap is by far the most useful scanner available today. It is scalable, has numerous stealth options, gives the user full control over the type of scan they want to use and it can be integrated into scripts and programs.

Technology Review

Legal TCP connections (HTTP, Telnet, FTP, etc..) are established using the three-way handshake (SYN/SYN-ACK/ACK). This allows for the establishment of sequence numbers between the two systems. These sequence numbers are used by TCP so it can deliver the packets in the proper order on a reliable basis. Using these sequence numbers the TCP stacks of each system will retransmit lost packets and reorder packets that arrive out of sequence (9).

The TCP connect scan respects the defined TCP specifications. The source system awaits a SYN-ACK response form the target port. If the port is open, the source will complete the handshake with an ACK. If the port is closed, no SYN-ACK will be returned to the source from the target. Possible responses to the source could be: no response, a RESET packet, or ICMP port unreachable packet. These variables depend on the target network configuration.

The TCP SYN scan follows the three-way handshake but stops two-thirds of the way through the handshake sometimes referred to as the "half-open" scan. The source system will send a SYN to each target port, if the port is open the target will send back a SYN-ACK response. The source machine then immediately sends back a RESET packet aborting the connection. If the target port is closed, the source may receive no response, a RESET packet, or an ICMP unreachable packet, and this depends on the configuration of the target network.

The target system will not record the connection because a true connection never occurs because it is torn down before it is ever completed. A router or firewall that has logging enabled should be able to record the SYN packet.

4.2 TELNET

Any port this is open and listening, you can use telnet to connect to. Many times the application will return information that the target would rather you not have.
Example: #-> telnet www.company.com 80
GET /HTTP/1.0 [ENTER]

The following output is what www.notarealdomain.org reported:

-=[toolbox]=- -4:51pm- /usr/local/bin# telnet www.notarealdomain.org 80
Trying 10.x.x.46...

Connected to www.notarealdomain.org.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 301 Moved Permanently
Date: Mon, 13 May 2002 21:43:56 GMT
Server: Apache
Location: http://www.notarealdomain.org/newlook/home.php
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>301 Moved Permanently</TITLE>
</HEAD><BODY>
<H1>Moved Permanently</H1>
The document has moved <A
HREF="http://www.notarealdomain.org/home.php">here</A>.<P>
<HR>
<ADDRESS>Apache/1.3.24 Server at www.notarealdomain.org Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.

We can tell from the output that www.notarealdomain.org is running Apache as their web server. In many cases the organization does not modify the web server output and the exact version, platform and extensions are displayed to anyone that wants to know.

4.3 NMAP

For a full review of the various nmap scan types, type "nmap –h" at the command line. On Unix and Linux systems a user must be root or root equivalent to perform some of the more advanced features.

TCP SYN scans are very fast—that is the good news. The bad news is that it is possible to flood the target system with outstanding SYN's resulting in an accidental Denial of Service attack. This is more likely in older systems. I have performed thousands of TCP SYN scans and have had very few incidents ever arise. I do not mention this to lesson or weaken the previous sentence. In a production environment it is always best to error on the side of caution (9).

The FIN scan violates the TCP protocol by sending packets that are not expected at the start of a connection. A FIN packet instructs the target system that the connection should be torn down. The target sees a bunch of FIN packets arriving to tear down non-existent connections. According to the TCP specification if a closed port receives an unexpected FIN when no connection is present, the target system should respond with a RESET therefore indicating the port is closed. If the port is open when the unexpected FIN arrives, nothing is sent to the source indicating the port is open. This is not 100% reliable!

The Xmas Tree scan sends packets with the FIN, URG, and PUSH bits set. It's name comes from the observation that these code bits set in a TCP header resemble little lights on a Christmas tree. (I don't see it)

The Xmas Tree scan also violates the TCP protocol by sending packets that are not expected at the start of a connection.

The NULL scan sends TCP packets with no code bits set. The NULL scan expects the same behavior form the target system as the FIN scan: a closed port will send a RESET, while an open port sends nothing.

The Xmas, FIN, and NULL scans do not work on Microsoft 9X, NT and 2000 because they do not follow the RFC's regarding when to send a RESET. Microsoft is now able to claim a win for the continual non-compliance with the rest of the world.

The TCP ACK scan also violates the TCP protocol specification, allowing a malicious user to be stealthier and get through some packet filtering devices such as routers.

Packet filtering devices such as routers allow or deny packets based on their packet headers, both the IP header and the TCP or UDP header. By looking at the source and destination IP addresses, source and destination ports, and TCP bit flags, a packet filter will determine whether it should transmit a packet or drop it.

In a normal network configuration a company will allow internal users access to an external network, typically the internet. An external packet filtering device will allow outgoing traffic so that the internal machines can access servers and services on the Internet. The device could be a router, firewall, etc.

The packet filtering device will allow the TCP ACK packets into the internal network because it will think they are responses to outgoing connections, give that the ACK bit is set.

The attacker could conduct an ACK scan to determine which ports through the firewall allow established connection responses. If a RESET comes back from the target machine, we know our packet got through the packet filtering device.

ACK scanning can be used to determine which what kind of established connections a packet filter device, such as a router or firewall, will allow into a network. Firewalk is another tool that works well in this arena, with even more detailed options. Firewalk is available for download at http://www.packetfactory.net/Projects/Firewalk/

UDP is nothing like TCP; there is no three-way handshake, sequence numbers, or flag bits. Packets can even be delivered out of order and they are not retransmitted if they are dropped. UDP scans for the above reasons are not very reliable and should be used as a last resort.

For UDP scanning if the target returns an ICMP port unreachable, Nmap will determine the port closed. Otherwise Nmap assumes it is open. False positives are very high with this scanning method.

The results of the UDP scans will give the attacker a general idea of what is open and then they can use other tools to verify if the port is really open or not.

Nmap will send ICMP echo request packets to all addresses on the target network to determine which are listening machines. Ping sweeps can also be done via TCP in lieu of ICMP.

The more common RPC programs are Rstatd, Rwalld, Rup, and others. Unfortunately many of the well known RPC programs have vulnerabilities associated with them.

Nmap can scan any port discovered via TCP or UDP scans and connects to each of them searching for RPC services. Nmap sends NULL RPC commands to each open port in an effort to determine which RPC service is running.

To improve the chances that the packets generated by Nmap will get through the router and/or firewall you can choose specific TCP and UDP source ports for the packets transmitted during the scan.

The source port is also included in the header, which may be used by the target network to determine whether the traffic should be allowed or not. The goal is to set the source port so that the packets appear as normal traffic to the target network lowering the possibility of detection.

TCP port 80 is the default because the resulting traffic will appear to be coming from a web client using HTTP. Another choice is port 25, which appears to be traffic from an Internet mail server via SMTP.

If the attacker combines the source port with a TCP ACK scan will make the traffic look just like responses to web traffic or outgoing mail.

For scanning UDP services, a source port of 53 will look like DNS responses, and is much more likely to be allowed into the target network.

Nmap has the ability to use decoy IP addresses when scanning. The use of 30 decoys is common and the attacker's real IP address must be included in the decoy list or they will not get back the packets they are looking for.

An attacker can spread over time the request packets to the target. A patient attacker has many tools available to assist. Nmap has six modes of timing options: Paranoid sends one packet every 5 minutes, Sneaky sends one packet every 15 seconds, Polite send one packet approximately every .4 seconds, Normal runs as quickly as possible, Aggressive waits a maximum of 1.25 seconds for a response, and Insane waits a maximum of .3 seconds for any response.

While this may seem tricky, it actually has a good use. If you are worried about flooding a system, use the "Polite" mode as a good option.

Nmap also supports IP packet fragmentation which is intended to fool some of the basic IDS systems. At this day and time all of the commercial tools and even Snort is likely to pick up on this technique.

The Fragrouter tool is a tool that can be used to help evade some IDS systems. Fragrouter for the Unix operating system is available at http://www.w00w00.org/files/sectools/. It runs on BSD, Linux or Solaris. This tool supports over 35 different ways to slice and dice your target packets. An attacker could use Fragrouter with Nessus, Nmap, Hping2, Firewalk and other tools to further their efforts in evading IDS. The basic configuration is to install Fragrouter on a separate system and then create a route on your audit host to point at the Fragrouter host for the traffic destined for your target host or network. The actual configuration and use of Fragrouter with other tools is an entire paper by it self.

"Any host, network device or Intrusion Detection System may deal with IP fragments in the following ways:

- Discard the fragments. Since there is legitimate use for IP fragments this is not the best general solution. For intrusion detection systems it is advisable that they should examine these packets. When shopping for intrusion detection systems be certain to find out if they support packet reassembly.
- Letting the IP fragments flow to the final destination without trying to make a whole packet out of it. Typical example of this is what a router does (means the router cannot (always) look at the TCP headers and therefore not do proper filtering ...). You should check your filtering routers, especially if they are your only line of defense.
- The device can try to reassemble IP fragments into packets. Destination hosts have no choice but to do this. This is the only way for filtering or ID systems to get to the actual contents, or even to the full TCP headers. Since there are no guarantees about order of arrival and since storing fragments until the IP packets are complete consumes resources, there is a chance for a denial of service or for not being able to catch all the IP fragments (14)."

A paper on Fragrouter written by Brad Sanford is available at the SANS Reading Room at http://rr.sans.org/encryption/IP_frag.php. An online man page is available at the following URL: http://www.netflood.net/files/IDS/fragrouter.html. Fragrouter can be downloaded from the SecurityFocus web site at http://online.securityfocus.com/tools/176

Nmap Examples

The following nmap scan is run against the lab DNS server running Bind 9.2.1 on a Solaris 8 server fully patched. The DNS server is behind a stateful firewall with only TCP and UDP port 50 open to the outside world. The servers /etc/inetd.conf has been commented out and the only service running on the host is BIND.

```
-=[toolbox]=- -9:54pm- ~# nmap -sS -v -v -P0 -p 53 ns1.mytestlab.net
 Starting nmap V. 2.54BETA33 ( www.insecure.org/nmap/ )
Host ns1.mytestlab.net (192.168.107.66) appears to be up ... good.
Initiating SYN Stealth Scan against ns1.mytestlab.net (192.168.107.66)
The SYN Stealth Scan took 62 seconds to scan 1 ports.
Interesting ports on ns1.mytestlab.net (192.168.107.66)
Port       State       Service
53/tcp     filtered    domain
 Nmap run completed -- 1 IP address (1 host up) scanned in 62 seconds
```

The above nmap scan confirms that port 53 TCP is open and is filtered via the firewall.

The next nmap scan is on the Windows 2000 Advanced Server located in the traditional DMZ (behind the border router and in front of the Firewall). The results of this scan should indicate why an organization should not place any host or valuable asset in the old traditional DMZ and why they should establish a minimum security baseline standard for installing new external facing hosts. The number of open ports on this server is frightening! I installed Win 2000 Advanced Server and IIS 5.0 with the default options. The open ports listed in the nmap scan demonstrate how much work is actually needed before placing a host like this into production.

```
-=[toolbox]=- -9:53pm- ~# nmap -sS -v -v -P0 -O 192.168.107.2
 Starting nmap V. 2.54BETA33 ( www.insecure.org/nmap/ )
Host (192.168.107.2) appears to be up ... good.
Initiating SYN Stealth Scan against (192.168.107.2)
Adding open port 135/tcp
Adding open port 548/tcp
Adding open port 1433/tcp
Adding open port 515/tcp
Adding open port 25/tcp
Adding open port 17/tcp
Adding open port 53/tcp
Adding open port 19/tcp
Adding open port 6666/tcp
Adding open port 5631/tcp
Adding open port 139/tcp
Adding open port 445/tcp
Adding open port 1025/tcp
Adding open port 7/tcp
Adding open port 42/tcp
Adding open port 9/tcp
Adding open port 13/tcp
Adding open port 443/tcp
Adding open port 21/tcp
The SYN Stealth Scan took 69 seconds to scan 1554 ports.
For OSScan assuming that port 7 is open and port 1 is closed and neither are firewalled
Interesting ports on (192.168.107.2):
```

(The 1532 ports scanned but not shown below are in state: closed)

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
17/tcp	open	qotd
19/tcp	open	chargen
21/tcp	open	ftp
25/tcp	open	smtp
42/tcp	open	nameserver
53/tcp	open	domain
135/tcp	open	loc-srv
137/tcp	filtered	netbios-ns
139/tcp	open	netbios-ssn
443/tcp	open	https
445/tcp	open	microsoft-ds
515/tcp	open	printer
548/tcp	open	afpovertcp
1025/tcp	open	listen
1433/tcp	open	ms-sql-s
5631/tcp	open	pcanywheredata
6666/tcp	open	irc-serv
27374/tcp	filtered	subseven
31337/tcp	filtered	Elite

Remote operating system guess: Windows Millennim Edition (Me), Win 2000, or WinXP
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=3C33%IPID=I%TS=0)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%
DAT=E)
TCP Sequence Prediction: Class=random positive increments Difficulty=15411 (Worthy
challenge)
TCP ISN Seq. Numbers: F3A879C1 F3AEF79B F3B609D7 F3BC9ADC F3C32452
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 80 seconds
-=[esctoolbox]=- -9:56pm- ~#

4.4 HPING2

Hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using hping2, you can: test firewall rules, perform [spoofed] port scanning, test net performance using different protocols, packet size, TOS (type of service), and fragmentation, do path MTU discovery, tranfer files (even between really Fascist firewall rules), perform traceroute-like actions under different protocols, fingerprint remote OSs, audit a TCP/IP stack, etc. hping2 is a good tool for learning TCP/IP(15).

Erik Kamerling wrote a great paper titled "Hping2 Idle Host Scan" and it is available online at the SANS Reading Room at http://rr.sans.org/audit/hping2.php. This paper is a step-by-step guide of how to perform an idle host scan and Erik provides a lot of detail and explanation.

The Hping web site at http://www.hping.org says the following about Hping2:

Hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) 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.

While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts. A subset of the stuff you can do using hping:

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

The online man page for hping is available at http://www.hping.org/manpage.html.

Hping Examples

The first and most simple example is to issue simply pass an IP address after the hping command just like you would do with ping.

```
-=[toolbox]=- -10:42pm- ~# hping 192.168.107.2
HPING 192.168.107.2 (dmfe0 192.168.107.2): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.107.2 flags=RA seq=0 ttl=107 id=29978 win=0 rtt=59.5 ms
len=46 ip=192.168.107.2 flags=RA seq=1 ttl=107 id=29979 win=0 rtt=58.0 ms
```

len=46 ip=192.168.107.2 flags=**RA** seq=2 ttl=107 id=29980 win=0 rtt=59.5 ms
len=46 ip=192.168.107.2 flags=**RA** seq=3 ttl=107 id=29981 win=0 rtt=59.1 ms
len=46 ip=192.168.107.2 flags=**RA** seq=4 ttl=107 id=29982 win=0 rtt=59.1 ms
len=46 ip=192.168.107.2 flags=**RA** seq=5 ttl=107 id=29983 win=0 rtt=58.3 ms
^C
--- 192.168.107.2 hping statistic ---
6 packets tramitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 58.0/58.9/59.5 ms

The above example sends a TCP null-flags packet to port 0 of 192.168.107.2 every second and shows the host reply. In the reply we see that the target replies with the RST and ACK flags set. Refer to the flags= line in the above output (7).

In the next example we will send a TCP null-flags to an open port in listen state and since the port is open and listening we should get 100% packet loss, confirming that the port is open and listening. Note: this works on Unix based hosts and I have found that this does not give the same results on a Windows host.

-=[toolbox]=- -10:43pm- ~# hping 192.168.107.2 -p 53
HPING 192.168.107.2 (dmfe0 192.168.107.2): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.107.2 hping statistic ---
35 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

4.5 NETCAT

"Netcat is a tool that every security professional should be aware of and possibly have in their 'security tool box'. In May/June of 2000, insecure.org conducted a survey of 1200 Nmap users from the Nmap-hackers mailing list to determine their favorite security tools. Netcat was the second most popular tool, not including Nmap. A quick search on securityportal (www.securityportal.com) found 166 matches of netcat. Most of the matches describe or use netcat in some way. Netcat is a utility that is able to write and read data across TCP and UDP network connections. If you are responsible for network or system security it essential that you understand the capabilities of netcat" (13).

Netcat has many uses but one nifty feature is that it can be used as an extremely lightweight port scanner on both Unix and Windows platforms. I have included an example for the Unix platform to find out if port 80 was open and listening at somebody.com. According to the output below, port 80 is open and awaiting connections (good or otherwise).

-=[toolbox]=- -4:56pm- ~# nc -v -w 2 -z somebody.com 80
DNS fwd/rev mismatch: somebody.com != server.somebody.com
notarealdomain.org [x.x.x.40] 80 (?) open

Alternatively, a range of ports can be passed as an argument and this is illustrated in the example directly below:

```
-=[toolbox]=- -4:58pm- ~# nc -v -w 2 -z notarealdomain.org 1-80
DNS fwd/rev mismatch: notarealdomain.org != server.notarealdomain.org
notarealdomain.org [x.x.x.40] 80 (?) open
notarealdomain.org [x.x.x.40] 53 (?) open
notarealdomain.org [x.x.x.40] 25 (?) open
notarealdomain.org [x.x.x.40] 23 (?) open
notarealdomain.org [x.x.x.40] 22 (ssh) open
```

It appears that port 80, 53, 25 23, and 22 are open at notarealdomain.org.

A great paper about Netcat is available at the SANS Reading Room by Tom Armstrong at http://rr.sans.org/audit/netcat.php

Netcat has many other uses that can be both positive and extremely malicious. Be very sure that you know what you are doing when installing Netcat and as a general rule NEVER install it on a production host with external access. This would only make the job of an attacker that much easier.

5 VULNERABILITY TESTING

5.1 OVERVIEW

Vulnerability testing is serious business and only educated and trained professionals should be allowed to execute them. I have personally witnessed many organizations that had the best of intentions when they started their own penetration and vulnerability tests, but unfortunately in some cases they ended up taking a production asset off line because they didn't fully understand the tool they were using.

Nessus is probably one of the best, if not the best tool in its class for testing potential vulnerabilities of an online asset. The server portion currently must run on Unix or Linux and the client portion can run on Windows (see www.nessus.org for more details). In addition, many organizations utilize the command line option on the Unix platform so they can automate their tests on a regularly scheduled time. In this section I will demonstrate how to setup and configure automated tests via the command line. In addition, I will provide a sample report on a vulnerability test of a Windows 2000 Advanced Server that has been fully patched but no other modifications have been done. The report illustrates the need for organizations to develop "baseline standards" when rolling on key assets such as routers, switches, firewalls, servers, etc.

5.2 NESSUS

Nessus is available for download at http://www.nessus.org. In my lab I configured and installed Nessus on Solaris 8. This was a simple install and the following note outlines the procedure:

extract nessus-libraries-1.0.10
./configure
make
make install

extract libnasl-1.0.10
./configure
make
make install

extract nessus-core-1.0.10
./configure
make
make install

extract nessus-plugins-1.0.10
./configure
make
make install

run nessus-adduser from the /usr/local/sbin directory.

run nessusd –D as root.

Next I elected to run Nessus from the command line in order to take advantage of scripting opportunities. The following is the actual shell script that I used to scan the lab Win 2000 Advanced Server host (192.168.107.2).

I created a simple shell script called nessus_scan.sh

```
!#/bin/sh
nessus --output-type=html_graph --config-file=.nessusrc -V --batch-mode localhost 1241 labuser labpw targets rptfile
```

The output-type directive tells Nessus to output the results in HTML graph format.

The config-file switch tells Nessus the name of the configuration file to look at when starting up.

The –V switch tells Nessus to output to standard out so I can watch the progress.

Localhost and 1241 tell Nessus the host and port to run on.

Labuser is the username I setup with the nessus-adduser command.

Labpw is the password I configured for the user account.

The targets directive is the file that contains the IP address or addresses of the hosts in the scan. In my case the only address in the targets file is that of the Win 2000 Advanced Server.

Rptfile is the directory that Nessus will place the output into. Note: this directory must not currently exist or Nessus will fail when writing the output.

Next, I simply launched the shell script from the command line:
#-> ./nessus_scan.sh [ENTER]

Nessus completed the port scan and vulnerability tests configured in the .nessusrc configuration file. In order to take full advantage of the Nessus vulnerability tests you should log into the GUI interface and select the tests you would like Nessus to perform. In this example, I selected all plugins except dangerous. I then copied that .nessusrc file into the directly I launched the shell script from. In order to keep Nessus up to date with the latest plugins you can setup a cron job as root to execute /usr/local/sbin/nessus-update-plugins on a nightly basis. The plugins are stored in the /usr/local/lib/nessus/plugins directory. You can run a "ls –l | wc –l" command to check the number of plugins in the directory before running the update script. After the update if there were new plugins available you should see a higher number. Below is an example:

```
-=[toolbox]=- -11:02pm- /usr/local/lib/nessus/plugins# ls | wc -l
    921
```

Next I ran the nessus-update-plugins program.

```
-=[toolbox]=- -11:05pm- /usr/local/lib/nessus/plugins# ls | wc -l
    924
```

As of today there are 924 plugins for Nessus. This is comparable to any commercial vulnerability scanner!

5.3 SAMPLE PENETRATION REPORT

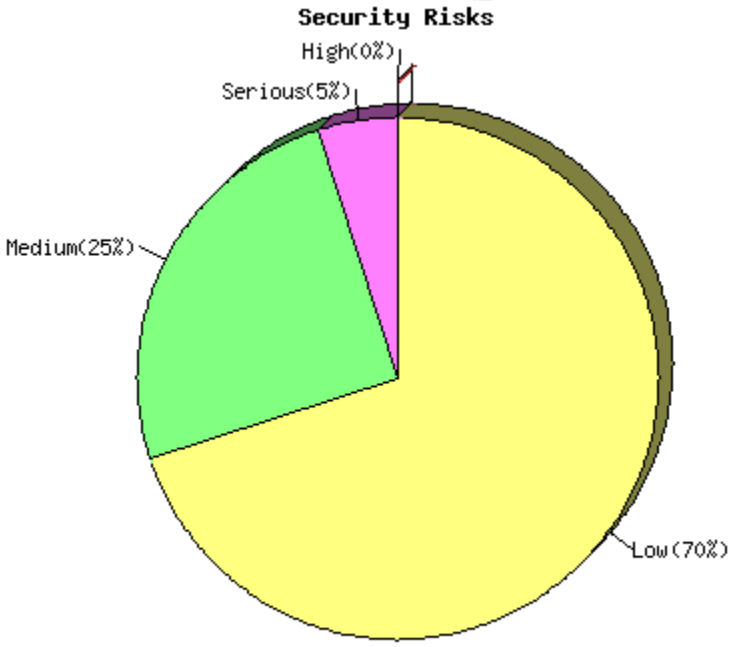
The Nessus Vulnerability report listed in this section is for the Windows 2000 Advanced Server (192.168.107.2) located in the lab DMZ. This report indicates the server is in need of immediate attention by a qualified professional. This report also tells us how vulnerable this server is and why it is imperative for organizations to fully understand the vulnerabilities they may be exposing themselves to. It is also important to understand that this report can not be taken at face value and the real value of the output of this report is to have a trained information security processional review the information. The professional would drill down into the details, eliminate any false positives, clean up redundant information and prepare a report that management could easily understand. The information in the native Nessus test is very valuable, but it does not eliminate the need for a trained professional.

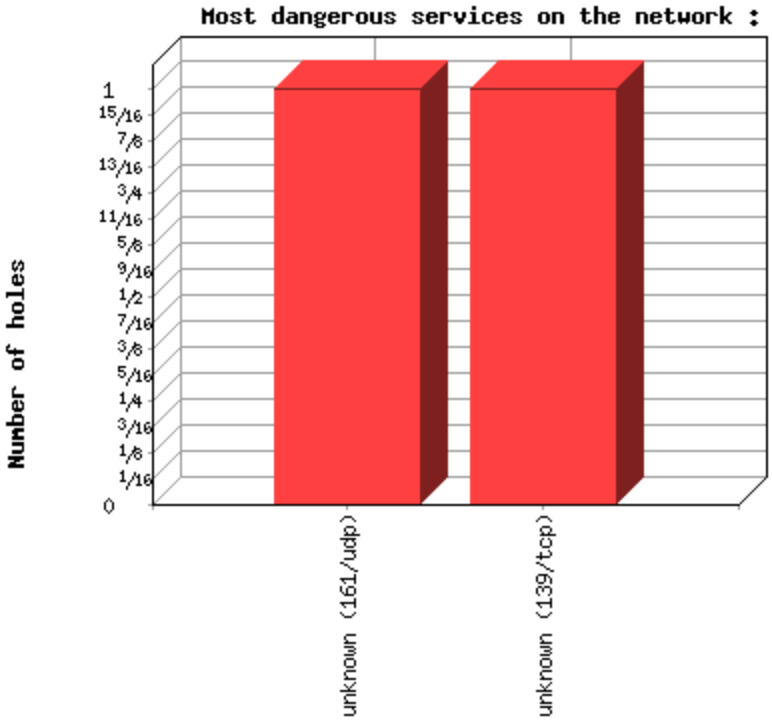
NESSUS REPORT

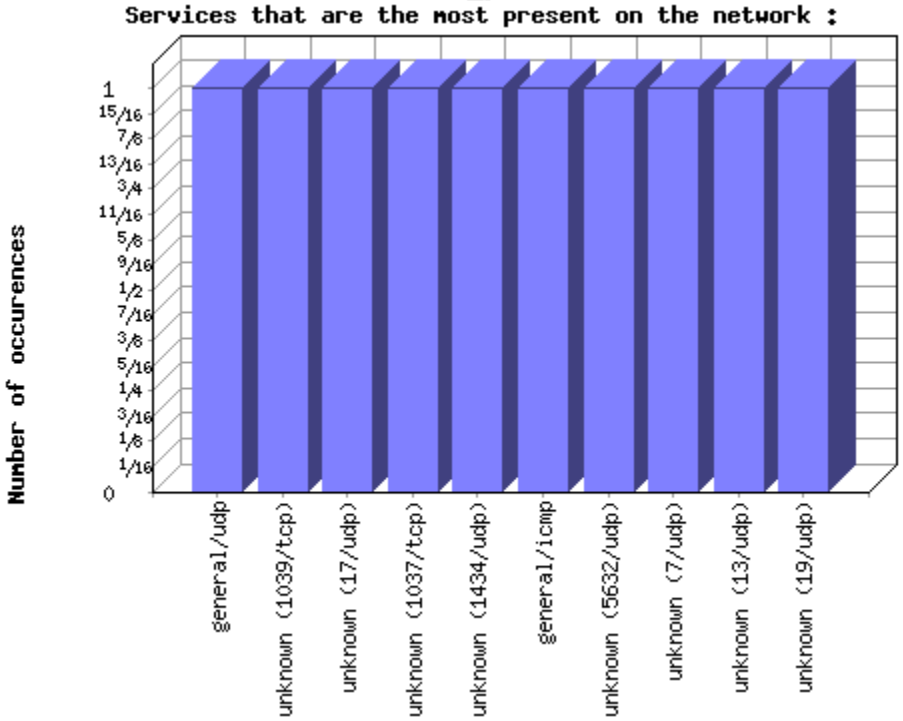
The Nessus Security Scanner was used to assess the security of 1 host

- **2 security holes have been found**
- **35 security warnings have been found**
- **42 security notes have been found**

PART I : GRAPHICAL SUMMARY :







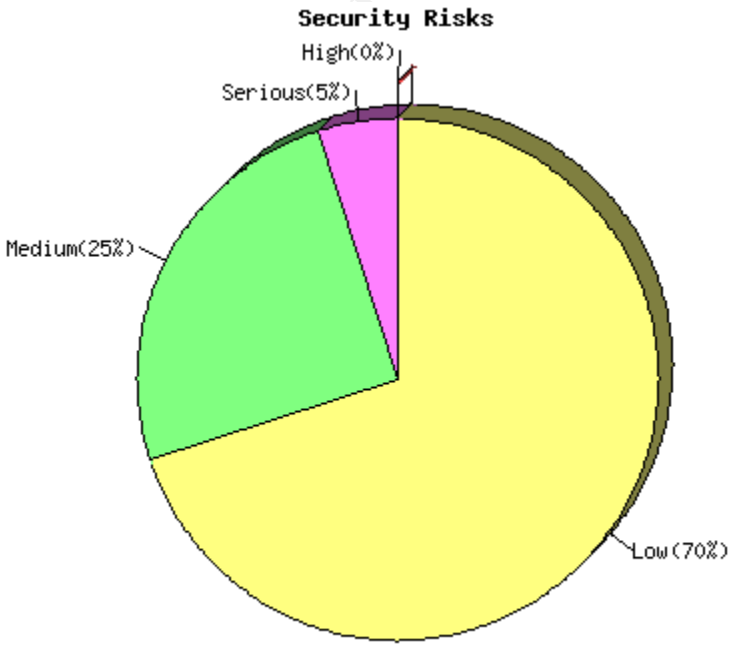
PART II. RESULTS, BY HOST :

192.168.107.2 **(found 2 security holes)**

This file was generated by Nessus, the open-sourced security scanner.

192.168.107.2

Repartition of the level of the security problems :



List of open ports :

- *unknown (7/tcp) (Security warnings found)*
- *unknown (9/tcp)*
- *unknown (13/tcp) (Security warnings found)*
- *unknown (17/tcp) (Security warnings found)*
- *unknown (19/tcp) (Security warnings found)*
- *unknown (21/tcp)*
- *unknown (25/tcp) (Security notes found)*
- *unknown (42/tcp)*
- *unknown (53/tcp) (Security warnings found)*
- *unknown (135/tcp) (Security warnings found)*
- *unknown (139/tcp) (Security hole found)*
- *unknown (443/tcp)*
- *unknown (445/tcp)*
- *unknown (515/tcp)*
- *unknown (548/tcp) (Security notes found)*
- *unknown (1025/tcp) (Security notes found)*
- *unknown (1027/tcp) (Security notes found)*
- *unknown (1029/tcp) (Security notes found)*
- *unknown (1034/tcp) (Security notes found)*
- *unknown (1036/tcp) (Security notes found)*
- *unknown (1038/tcp) (Security notes found)*
- *unknown (1433/tcp) (Security warnings found)*
- *unknown (1755/tcp)*
- *unknown (1965/tcp) (Security warnings found)*
- *unknown (3372/tcp)*
- *unknown (5631/tcp)*
- *unknown (6666/tcp)*
- *unknown (7778/tcp) (Security warnings found)*
- *unknown (8882/tcp)*
- *general/tcp (Security notes found)*
- *unknown (2032/tcp) (Security warnings found)*
- *unknown (2031/tcp) (Security warnings found)*
- *unknown (2030/tcp) (Security warnings found)*
- *unknown (2029/tcp) (Security warnings found)*
- *unknown (2027/tcp) (Security warnings found)*
- *unknown (2047/tcp) (Security warnings found)*
- *unknown (137/udp) (Security warnings found)*
- *unknown (161/udp) (Security hole found)*
- *unknown (19/udp) (Security warnings found)*
- *unknown (13/udp) (Security warnings found)*
- *unknown (7/udp) (Security warnings found)*
- *unknown (5632/udp) (Security warnings found)*
- *general/icmp (Security warnings found)*
- *unknown (1434/udp) (Security warnings found)*
- *unknown (1037/tcp) (Security notes found)*
- *unknown (17/udp) (Security warnings found)*

- *unknown (1039/tcp) (Security notes found)*
- *general/udp (Security notes found)*

Warning found on port unknown (7/tcp)

The 'echo' port is open. This port is not of any use nowadays, and may be a source of problems, since it can be used along with other ports to perform a denialof service. You should really disable this service.
Risk factor : Low
Solution : comment out 'echo' in /etc/inetd.conf
CVE : CVE-1999-0103

Information found on port unknown (7/tcp)

an echo server is running on this port

Warning found on port unknown (13/tcp)

The daytime service is running.
The date format issued by this service may sometimes help an attacker to guess the operating system type. In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service.
Solution : disable this service

Risk factor : Low
CVE : CVE-1999-0103

Warning found on port unknown (17/tcp)

The quote service (qotd) is running.

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17. When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. They will commence spewing characters at each other, slowing

the machines down and saturating the network.
Solution : disable this service
Risk factor : Low
CVE : CVE-1999-0103

Warning found on port unknown (19/tcp)

The chargen service is running.
The 'chargen' service should only be enabled when testing the machine.

When contacted, chargen responds with some random (something like all the characters in the alphabet in row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

An easy attack is 'pingpong' which IP spoofs a packet between two machines running chargen. They will commence spewing characters at each other, slowing the machines down and saturating the network.
Solution : disable this service
Risk factor : Low
CVE : CVE-1999-0103

Information found on port unknown (19/tcp)

Chargen is running on this port

Information found on port unknown (25/tcp)

Remote SMTP server banner :
0
0

Warning found on port unknown (53/tcp)

The remote name server allows recursive queries to be performed by the host running nessusd. If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do

this by using the instruction 'allow-recursion' in the 'options' section of your named.conf. If you are using another name server, consult its documentation.

Risk factor : Serious

Warning found on port unknown (135/tcp)

DCE services running on the remote can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host.
Solution : filter incoming traffic to this port.
Risk factor : Low

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000001ec.00000001' is running on this host
Type : ncalrpc
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000001ec.00000001' is running on this host
Type : ncalrpc
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000001ec.00000001' is running on this host
Type : ncalrpc
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000001ec.00000001' is running on this host
Type : ncalrpc
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000002f4.00000001' is running on this host
Type : ncalrpc
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (135/tcp)

The DCE Service 'LRPC0000042c.00000001' is running on this host
Type : ncalrpc
UUID : f706820d-511f-e80a-3007-6d740be8cee9

Information found on port unknown (135/tcp)

The DCE Service 'LRPC0000042c.00000001' is running on this host
Type : ncalrpc
UUID : 8e52b00d-a937-cfc0-1182-2daa51e40000

Information found on port unknown (135/tcp)

The DCE Service 'DHCPSERVERLPC' is running on this host
Type : ncalrpc
UUID : ffd0980d-126b-10a1-3698-3346c3f87453

Information found on port unknown (135/tcp)

The DCE Service 'DHCPSERVERLPC' is running on this host
Type : ncalrpc
UUID : 8217200d-3b5b-d0f6-11aa-d2c04fc32400

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000004b4.00000001' is running on this host
Type : ncalrpc
UUID : f52c280d-9f45-1a7f-10b5-2b082b2efa00

Information found on port unknown (135/tcp)

The DCE Service 'LRPC000004b4.00000001' is running on this host
Type : ncalrpc
UUID : 1109bf0d-e181-d1a4-11ab-54a0c91e9b00

Information found on port unknown (135/tcp)

The DCE Service 'ntsvcs' is running on this host
Type : ncalrpc
UUID : 7b91f80d-ff5a-11d0-a9b2-c04fb6e60000
Annotation : Messenger Service

Vulnerability found on port unknown (139/tcp)

It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants

the user the 'guest' access. To prevent null sessions, see MS KB Article Q143474. Note that thid won't completely disable null sessions, but will prevent them from connecting to IPC$
All the smb tests will be done as "/" in domain

Warning found on port unknown (139/tcp)

The domain SID can be obtained remotely. Its value is :
TLWORKGROUP : 48-0-0-0-0
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139
Risk factor : Low
CVE : CVE-2000-1200

Warning found on port unknown (139/tcp)

The host SID can be obtained remotely. Its value is :
CAZADOR : 5-21-602162358-884357618-1547161642
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139
Risk factor : Low
CVE : CVE-2000-1200

Warning found on port unknown (139/tcp)

The host SID could be used to enumerate the names of the local users
of this host. (we only enumerated users name whose ID is between 1000 and 1200 for performance reasons) This gives extra knowledge to an attacker, which is not a good thing : - Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_CAZADOR (id 1003)
- IWAM_CAZADOR (id 1004)
- DHCP Users (id 1005)
- DHCP Administrators (id 1006)
- WINS Users (id 1007)
- tlayton (id 1008)

Risk factor : Medium
Solution : filter incoming connections to port 139

Warning found on port unknown (139/tcp)

Here is the browse list of the remote host :

CAZADOR -

This is potentially dangerous as this may help the attack of a potential hacker by giving him extra targets to check for.
Solution : filter incoming traffic to this port
Risk factor : Low

Warning found on port unknown (139/tcp)

The following local accounts have never changed their password :
Administrator
NetShowServices

To minimize the risk of break-in, users should change their password regularly

Warning found on port unknown (139/tcp)

The following local accounts have never logged in :
Guest
Unused accounts are very helpful to hacker
Solution : suppress these accounts
Risk factor : Medium

Warning found on port unknown (139/tcp)

The following local accounts have passwords which never expire :
Administrator
Guest
NetShowServices

Password should have a limited lifetime
Solution : disable password non-expiry
Risk factor : Medium

Information found on port unknown (139/tcp)

The remote native lan manager is : Windows 2000 LAN Manager
The remote Operating System is : Windows 5.0
The remote SMB Domain Name is : TLWORKGROUP

Information found on port unknown (139/tcp)

The following local accounts are disabled :
Guest

To minimize the risk of break-in, permanently disabled accounts should be deleted
Risk factor : Low

Information found on port unknown (548/tcp)

This host is running an AppleShare File Services over IP.
Machine type: Windows NT
Server name: CAZADOR
UAMs: ClearTxt Passwrd/Microsoft V1.0/MS2.0
AFP Versions: AFPVersion 2.0/AFPVersion 2.1/AFP2.2

Information found on port unknown (1025/tcp)

A DCE service is listening on 192.168.107.2:1025 :
Type: ncacn_ip_tcp
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (1025/tcp)

A DCE service is listening on 192.168.107.2:1025 :

Type: ncacn_ip_tcp
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (1025/tcp)

A DCE service is listening on 192.168.107.2:1025 :
Type: ncacn_ip_tcp
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (1025/tcp)

A DCE service is listening on 192.168.107.2:1025 :

Type: ncacn_ip_tcp
UUID : 6b0ce00d-0b90-67c7-10b3-17dd01066200

Information found on port unknown (1027/tcp)

A DCE service is listening on 192.168.107.2:1027 :
Type: ncacn_ip_tcp
UUID : f706820d-511f-e80a-3007-6d740be8cee9

Information found on port unknown (1027/tcp)

A DCE service is listening on 192.168.107.2:1027 :
Type: ncacn_ip_tcp
UUID : 8e52b00d-a937-cfc0-1182-2daa51e40000

Information found on port unknown (1029/tcp)

A DCE service is listening on 192.168.107.2:1029 :

Type: ncacn_ip_tcp
UUID : ffd0980d-126b-10a1-3698-3346c3f87453

Information found on port unknown (1029/tcp)

A DCE service is listening on 192.168.107.2:1029 :
Type: ncacn_ip_tcp
UUID : 8217200d-3b5b-d0f6-11aa-d2c04fc32400

Information found on port unknown (1034/tcp)

A DCE service is listening on 192.168.107.2:1034 :
Type: ncacn_ip_tcp
UUID : abc2a40d-4d50-b357-409d-66ee4fd5fba0

Information found on port unknown (1036/tcp)

A DCE service is listening on 192.168.107.2:1036 :
Type: ncacn_ip_tcp
UUID : f52c280d-9f45-1a7f-10b5-2b082b2efa00

Information found on port unknown (1036/tcp)

A DCE service is listening on 192.168.107.2:1036 :
Type: ncacn_ip_tcp
UUID : 1109bf0d-e181-d1a4-11ab-54a0c91e9b00

Information found on port unknown (1038/tcp)

A DCE service is listening on 192.168.107.2:1038 :
Type: ncacn_ip_tcp
UUID : ad42800d-6b82-cf03-1197-2caa68870000

Information found on port unknown (1038/tcp)

A DCE service is listening on 192.168.107.2:1038 :

Type: ncacn_ip_tcp
UUID : fb5d700d-a48c-cf31-11a7-d8805f48a100

Information found on port unknown (1038/tcp)

A DCE service is listening on 192.168.107.2:1038 :
Type: ncacn_ip_tcp
UUID : a951d10d-0ebf-d32f-11bf-d1c04fa34900

Warning found on port unknown (1433/tcp)

It is possible that Microsoft's SQL Server is installed on the remote computer.
CVE : CAN-1999-0652

Warning found on port unknown (1965/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (7778/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Information found on port general/tcp

Nmap found that this host is running Windows Millennim Edition (Me), Win 2000, or WinXP

Information found on port general/tcp

Nmap only scanned 14999 TCP ports out of 65535.Nmap did not do a UDP scan, I guess.

Information found on port general/tcp

The plugin PC_anywhere_tcp.nasl was too slow to finish - the server killed it

Information found on port general/tcp

The plugin mstream_handler.nasl was too slow to finish - the server killed it

CVE : CAN-2000-0138

Information found on port general/tcp

The plugin port_shell_execution.nasl was too slow to finish - the server killed it

Information found on port general/tcp

The plugin subseven.nasl was too slow to finish - the server killed it

CVE : CAN-1999-0660

Warning found on port unknown (2032/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (2031/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (2030/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (2029/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (2027/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (2047/tcp)

The port was detected as opened by scanner but is now closed. The service was probably crashed by the scanner

Warning found on port unknown (137/udp)

. The following 8 NetBIOS names have been gathered :
INet~Services
IS~CAZADOR
CAZADOR
TLWORKGROUP
CAZADOR
TLWORKGROUP
TLWORKGROUP
__MSBROWSE__
. The remote host has the following MAC address on its adapter :
0x00 0xa0 0xc9 0x1f 0xc4 0x26

If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.

Risk factor : Medium

Vulnerability found on port unknown (161/udp)

SNMP Agent responded as expected with community name: public
CVE : CAN-1999-0517

Warning found on port unknown (161/udp)

It was possible to obtain the list of SMB users of the
remote host via SNMP :
Guest
An attacker may use this information to set up brute force attacks or find an unused account.

Solution : disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port

Risk factor : Medium

Warning found on port unknown (161/udp)

It was possible to obtain the list of network interfaces of the
remote host via SNMP :

. MS TCP Loopback interface
. Intel 8255x-based Integrated Fast Ethernet

An attacker may use this information to gain more knowledge about
the target host.
Solution : disable the SNMP service on the remote host if you do not use it, or
filter incoming UDP packets going to this port
Risk factor : Low

Warning found on port unknown (161/udp)

It was possible to obtain the list of Lanman shares of the remote host via SNMP :

. c

An attacker may use this information to gain more knowledge about
the target host.
Solution : disable the SNMP service on the remote host if you do not
use it, or filter incoming UDP packets going to this port
Risk factor : Low

Warning found on port unknown (161/udp)

It was possible to obtain the list of Lanman services of the
remote host via SNMP :
. Server
. Alerter
. Event Log
. Messenger
. Telephony
. DNS Client
. DNS Server
. DHCP Client
. DHCP Server
. MSSQLSERVER
. Workstation
. SNMP Service
. Plug and Play
. Print Spooler
. RunAs Service
. Task Scheduler
. Computer Browser
. Microsoft Search
. COM+ Event System
. IIS Admin Service
. Protected Storage

. Removable Storage
. IPSEC Policy Agent
. TCP/IP Print Server
. Logical Disk Manager
. FTP Publishing Service
. Simple TCP/IP Services
. Distributed File System
. License Logging Service
. Remote Registry Service
. pcAnywhere Host Service
. File Server for Macintosh
. Security Accounts Manager
. System Event Notification
. Print Server for Macintosh
. Remote Procedure Call (RPC)
. TCP/IP NetBIOS Helper Service
. Windows Media Monitor Service
. Windows Media Program Service
. Windows Media Station Service
. Windows Media Unicast Service
. Internet Authentication Service
. NT LM Security Support Provider
. Distributed Link Tracking Client
. World Wide Web Publishing Service
. Windows Management Instrumentation
. Distributed Transaction Coordinator
. Windows Internet Name Service (WINS)
. Simple Mail Transport Protocol (SMTP)
. Windows Management Instrumentation Driver Extensions

An attacker may use this information to gain more knowledge about the target host.
Solution : disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port
Risk factor : Low

Information found on port unknown (161/udp)

Using SNMP, we could determine that the remote operating system is : Hardware: x86 Family 6 Model 1 Stepping 9 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)

Warning found on port unknown (19/udp)

The chargen service is running.
The 'chargen' service should only be enabled when testing the machine.

When contacted, chargen responds with some random (something like all the characters in the alphabet in row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

An easy attack is 'pingpong' which IP spoofs a packet between two machines running chargen. They will commence spewing characters at each other, slowing the machines down and saturating the network.

Solution : disable this service

Risk factor : Low
CVE : CVE-1999-0103

Warning found on port unknown (13/udp)

The daytime service is running.
The date format issued by this service may sometimes help an attacker to guess the operating system type.

In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service.

Solution : disable this service
Risk factor : Low
CVE : CVE-1999-0103

Warning found on port unknown (7/udp)

The 'echo' port is open. This port is not of any use nowadays, and may be a source of problems, since it can be used along with other ports to perform a denial of service. You should really disable this service.

Risk factor : Low

Solution : comment out 'echo' in /etc/inetd.conf
CVE : CVE-1999-0103

Warning found on port unknown (5632/udp)

The NetBIOS hostname of the remote host was given by PC anywhere : CAZADOR

Warning found on port unknown (5632/udp)

PC Anywhere is running.

This service could be used by an attacker to partially take the control of the remote system.

An attacker may use it to steal your password or prevent your system from working properly.

Solution : disable this service if you do not use it.

Risk factor : Medium

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

Warning found on port unknown (1434/udp)

Here is the reply to a MS SQL 'ping' request :
rServerName;CAZADOR;InstanceName;MSSQLSERVER;IsClustered;No;Version;
8.00.194;tcp;1433;np;\CAZADORipeqluery;;

Information found on port unknown (1037/tcp)

A DCE service is listening on 192.168.107.2:1037 :

Type: ncacn_ip_udp
UUID : 7b91f80d-ff5a-11d0-a9b2-c04fb6e60000
Annotation : Messenger Service

Warning found on port unknown (17/udp)

The quote service (qotd) is running.

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.
Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17. When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. They will commence spewing characters at each other, slowing the machines down and saturating the network.
Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

Information found on port unknown (1039/tcp)

A DCE service is listening on 192.168.107.2:1039 :

Type: ncacn_ip_udp
UUID : a951d10d-0ebf-d32f-11bf-d1c04fa34900

Information found on port general/udp

For your information, here is the traceroute to 192.168.107.2 :
192.168.1.1
192.168.107.2

This file was generated by Nessus, the open-sourced security scanner.

6 OTHER SECURITY RELATED RESOURCES

Information Security News and Information	
Current Security Related News	http://www.atstake.com/security_news/
Security Focus News	http://www.securityfocus.com/
Phrack Magazine On-Line	http://www.phrack.com/
Security News Portal	http://www.securitynewsportal.com/index.shtml

Def Con	http://www.defcon.net/
CERT	http://www.cert.org/
Security Related Statistics	http://www.securitystatistics.com/
SANS	http://www.sans.org/newlook/home.php
Security Professionals Reference	http://www.cotse.com/
Visual Traceroute	http://wetelephant.cotse.com/tracetools.html

7 BIBLIOGRAPHY

1. SANS Defense In-Depth module 1, SANS Institute.

2. Hackers Beware, New Riders Publishing, 2002.

3. SANS/FBI Top 20 List, http://www.sans.org/top20.htm

4. CERT® Coordination Center, http://www.cert.org

5. Hacking Exposed, Osborne, McGraw-Hill, 2001

6. Nmap man page

7. Hping2 man page

8. Nessus – http://www.nessus.org

9. Counter Hack, Prentice Hall, 2002

10. Penetration Testing: The Third Party Hacker. http://rr.sans.org/penetration/third_party.php

11. http://www.pwcrack.com/Penetration_Testing/penetration_testing.html

12. ARIN Whois Database Search: http://www.arin.net/whois/arinwhois.html

13. Netcat – The TCP/IP Swiss Army Knife - http://rr.sans.org/audit/netcat.php

14. IDS Evasion - http://www.sans.org/newlook/resources/IDFAQ/fragments.htm

15. Freshmeat Link for Hping2 - http://freshmeat.net/projects/hping2/?topic_id=43,150

16. Hack I.T. , Pearson Education, 2002