Global Information Assurance Certification Paper

Building a Security Toolkit
Trevor Goering
June 25, 2001

Introduction

Although the numbers of IT security professionals are growing there is still the consensus that there are not enough available. This has probably been a key factor in the success and growth of Managed Security Service Providers (MSSP) companies. However the cost associated with many of the MSSP's bring up the questions as to what services if any can be done in house. The decision as to what security services that can be performed in-house and what need to be out source should be a concern of any company or manager. Many MSSP, have been successful because they have multiple personnel with unsurpassed experience and knowledge in the IT security field. However not everyone can afford that level of expertise. The purpose of this paper is to help those who are considering performing their own security assessment with a framework toward developing a security toolkit.

Know Your Enemy, Know Thy Self

"Military tactics are like flowing water. Flowing water always moves from high to low, and military tactics always avoid the enemy's strong points and attack his weak points. Whereas the course of flowing water is decided by the different landforms, the way to win victory in a battle is decided by altering the tactics according to enemy's changing situation." Sun~Tzu

In order to effectively protect your network and resources you need to understand your attacker, their tools and the strength of the Black Hat community. Secondly, know your own vulnerabilities. The low hanging fruit can be the most attractive, recognize your weakness and become familiar with the tools that will exploit and defend them. Having this information as well as a good understanding of your environment will be crucial to adequately assessing your level of risk at any point in time or as new vulnerabilities emerge. All to often-effective security practices come second to productivity and the flow of business. Staying current by subscribing to newsletters, review bulletin boards or any of the many other ways to stay up to date will arm you with the necessary information to possibly change policy if need be.

Get it in Writing

Before you begin to either collect tools or audit your network it is very important that measures are set up to protect yourself. I'm talking of course about policies and work orders. Make sure policies exist that answer the elementary questions of why, how and when. These are all questions that will most likely need to be answered to a higher authority before you begin. Before you begin researching or collecting tools see if there are policies restricting the use of certain tools or techniques such as freeware, denial of service attacks or Trojans. While the use of vendor only tools does have its

disadvantages like cost and feasibility in an attack. They are often more secure than freeware pulled off of an UN-trusted website. In addition there may be a policy in place stating that freeware has to be tested thoroughly before it can be used on a live network. It must not be assumed that in the case that there are no policies in conjunction with penetration testing or risk assessment that you have free reign to use any tools and techniques you see fit. If the policies are not in place to justify and protect your actions it is imperative that they be put in place before you begin. Keep in mind that you are testing your security posture and that it is very possible that you are susceptible to a given vulnerability and even exploit that vulnerability.

Types of Tools

The majority of tools fall under the following categories: Foot printing, Scanning, Enumeration, Access and Denial of Service. Your operating system, objectives and security policy will dictate which if not all the categories of tools that you need or are authorized to use.

Foot printing

Foot printing is the process in which information is gathered to get a better understanding of a target. In this case one would attempt to locate any technical information open to the Internet about their organization.

WHOIS – This is service by which registration information can be obtained from a Network Information Center (NIC) database.

Usenet – This is a discussion service found at http://www.deja.com. Often users will post messages revealing information that could be used in an attack. Any discussion group or service can potentially provide the same information particularly vendor discussion groups or those oriented around networking or security.

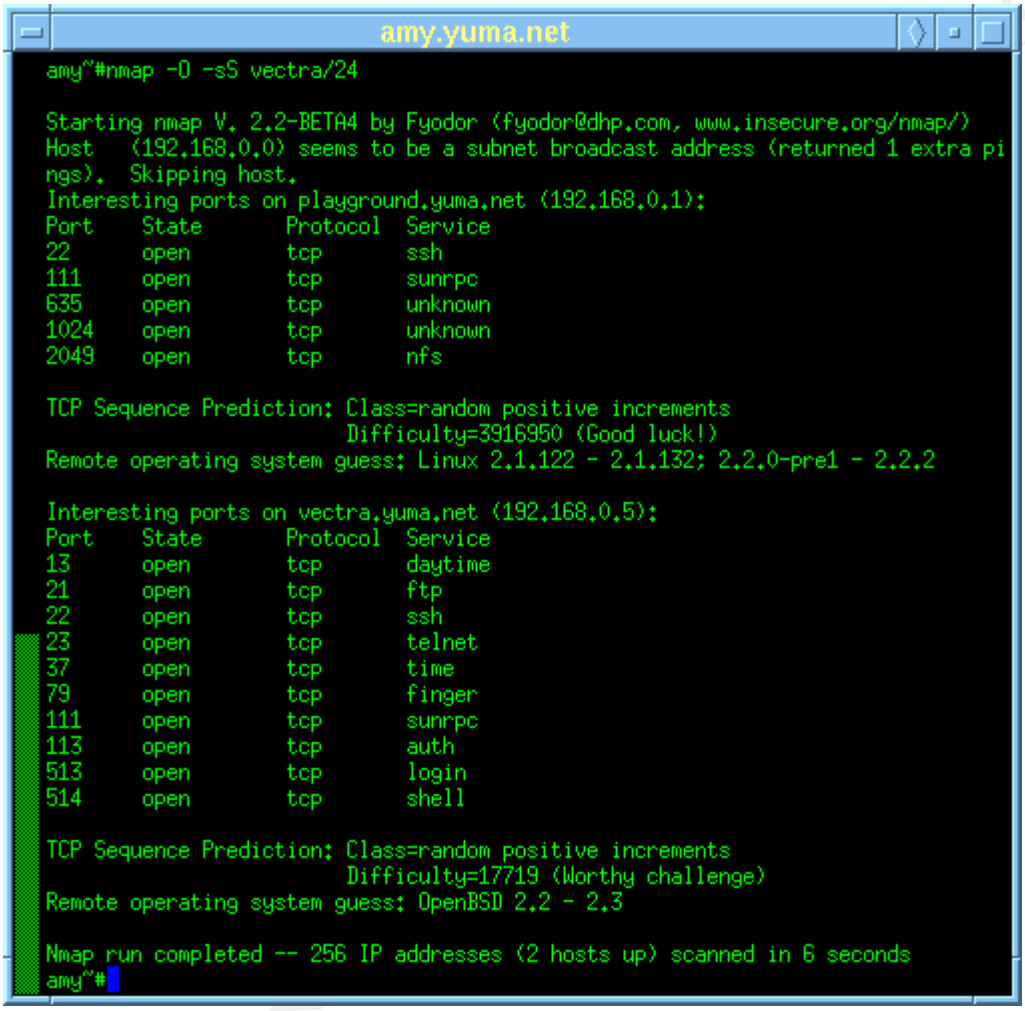
Search Engines – Don't count out good old search engines. Information regarding business mergers as well as layoffs may bring about unforeseen vulnerabilities, whether it being network migration related, information from a former employee or a lack of resources and expertise.

Scanning

Scanning is when a survey is performed to determine what hosts and services are alive in a certain network block or IP range.

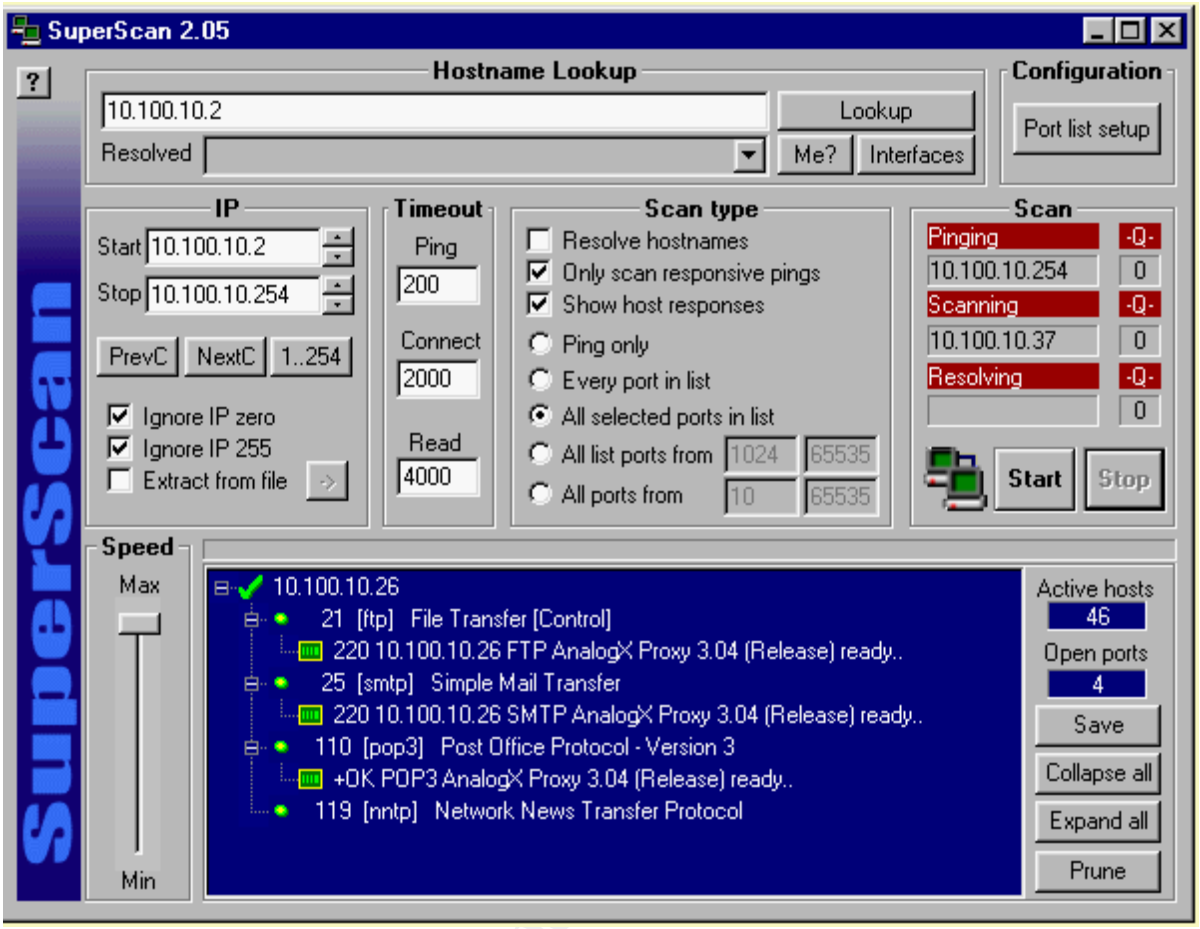
Nmap – Although there are many other scanners available Nmap is a must. It's versatility and cost has made Nmap perhaps the most popular network exploration or security-auditing tool available. It offers a wide range of scanning options and even includes stealth, TCP/IP fingerprints for remote operating system detection. Nmap has received numerous accolades from been named "Security Product of the Year" by Info

World and Codetalker Digest to praise in numerous computer magazines and websites such as Network World, Wired, 2600, Computer World, SANS, the CIO Institute Bulletin, and Phrack. It is currently the 13th most popular download (out of 9,000+) on the Freshmeat.Net software index. For more information check out **Nmap - The Tool, It's Author and It's Implications by** Brent Deterring in the SANS reading room or www.insecure.org. If you aren't using UNIX Nmap is a great reason to start.



Available at http://www.insecure.org/

SuperScan – Don't know any UNIX? Try SuperScan by the folks at Foundstone, Inc. This GUI application also provides a variety of scanning options. It also comes with some sneaky feature that enables you to control the speed of your scan, a progress meter, set timeout time for pings and hostname resolve. It even comes with a very useful help file.



Fscan – While you're at Foundstone's site taking a look at SuperScan see Fscan a command line scanner that scans both UDP and TCP. Below are some of the options available to you from Fscan.

-?/-h - shows this help text
-a - append to output file (used in conjunction with -o option)
-b - get port banners
-c - timeout for connection attempts (ms)
-d - delay between scans (ms)
-e - resolve IP addresses to hostnames
-f - read IPs from file (compatible with output from -o)
-i - bind to given local port
-l - port list file - enclose name in quotes if it contains spaces
-n - no port scanning - only pinging (unless you use -q)
-o - output file - enclose name in quotes if it contains spaces
-p - TCP port(s) to scan (a comma separated list of ports/ranges)
-q - quiet mode, do not ping host before scan
-r - randomize port order
-t - timeout for pings (ms)
-u - UDP port(s) to scan (a comma separated list of ports/ranges)

-v - verbose mode
-z - maximum simultaneous threads to use for scanning

Available at http://www.foundstone.com/rdlabs/tools.php

Enumeration

Enumeration takes footprinting a step further; Enumeration is typically used to obtain information on valid account names, network resource, shares and applications. Although much of the information obtained through enumeration may appear harmless once any of these are found it is not too difficult to crack the password or find vulnerability associated with operating system shares or production applications.

Winfingerprint – Winfingerprint is a Win32 based security tool that is able to determine OS, enumerate users, groups, shares, transports, services, event log, service pack and hotfix level, and date and time. Winfingerprint takes advantage of Windows null sessions; default unauthenticated session to a Windows NT box. If the network administrator has not disabled this default setting a hacker could obtain vital information on both users and shares.

Available at http://www.technotronic.com/winfingerprint

Access

Unauthorized access is typically obtained in two ways, with a valid username and password or by escalating existing user privileges. Although it's a long-established hacker technique, guessing fixed passwords still remains a concern thanks to human error and the technique lack of prejudice towards applications or operating systems.

LC3 – @stake has released LC3 its latest version of the very popular password auditing a recovery tool L0phtcrack. LC3 is an excellent Windows NT and Windows 2000 tool that provides excellent statistics for reporting such as the time frame it took to crack each account. It also offers several ways to obtain encrypted passwords. I find this especially useful when full disclosure of my audit can't be divulged at that time.

Available at http://www.@stake.com/research/index.html

Pandora – I only recently just got involved with Novell NetWare and this is the only tool that I have used to date. However if you have to audit NetWare accounts it is worth taking a look at. Although in my opinion it is not as comprehensive as the other is two it does work.

Available at http://www.nmrc.org/

Whisker – A large number of privilege escalations are performed on web servers. Whisker is a tool developed and maintained by Rain Forest Puppy is designed to check

a website for known vulnerable CGI scripts. In addition to the long list of signatures that it checks against Whisker can also be configured to avoid intrusion detection systems or other web scanning applications. Whisker also is efficient enough to not run vulnerabilities not associate with the webserver it is scanning.

Available at http://www.wiretrip.net/

Denial of Service

Think carefully before deciding if you really want to perform a denial of service attack against your network. As mentioned above check to see if denial of service attacks violates or is even mentioned in you security policy. While it can be used constructively to test firewall, intrusion detection configurations or incident response procedures, the down side of using a denial of service tool is fairly obvious. An alternative to consider may be to search for DDos tools on your systems ensuring that you are not contributing to denial of service attack. In addition to inspecting ports that are listening the FBI has produced a DDos detection tool to locating DDos services.

Find_DDos – Due to the number of DDos incidents reported in the last few years the National Infrastructure Protection Center (NIPC) a division of the FBI developed a tool to detect DDos tools on Solaris on an SPARC platform and Solaris and Linux on an Intel platform. Find_ddos version 4.2 currently detects mstream, tfn2k client, tfn2k daemon, trinoo daemon, trinoo master, tfn daemon, tfn client, stacheldraht master, stachedraht client, stachelddraht daemon, trn-rush client, trinity v3 daemons and memphisdraht clients.

Available at http://www.nipc.gov/warnings/advisories/2000/00-055.htm

Summary

There are many more vendors and free tools available. Take the time to assess your risk assessment objectives and research which tools are best for you. There is more to penetration testing or risk assessment than just the technical aspect when performing one on your own or for the first time. This sort of project demands technical skills, written skills, organizational skills and experience. This is one reason many managed security service providers have been so successful. However, the increase in books, training and accessibility to hackers over the last few years can help you put some of the MSSP knowledge into your hands. Software such as VMware workstation in which operating systems and applications run inside virtual machines, is an excellent learning tool for testing in a safe environment until your ready to go live. A successful assessment is all in the planning.

References

1. Insecure.org, "Top 50 Security Tools"
URL: http://www.insecure.org/tools.html (August 2000)

2. Oubug, “Tools of the Trade”
URL: http://www.collusion.org/article.cfm?ID=247 (November 2000)

3. Oubug & Characterdisorder, "Tools of the Trade II"
URL: http://www.collusion.org/article.cfm?ID=260 (December, 2000)

4. Scrambray, Joel. McClure, Stuart. Kurtz, Gerorge. Hacking Exposed Network Security Secrets & Solutions 2nd Edition, McGraw-Hill Professional Publishing (October, 2000)

5. Spitzner, Lance “Know Your Enemy”
URL: http://kracked.com/~felons/pub/security/spitzner-papers/enemy.html?clkd=iwm (August, 1999)

6. Fennelly, Carole “Hacker’s toolchest – Techniques and tools for penetration testing”
URL: http://www.itworld.com/Man/3887/swol-05-security/pfindex.html (May 2000)

7. Shipley, Greg. “Tools from the Underground”
URL:
http://www.networkcomputing.com/shared/printArticle?article=nc/1110/110ws1full.html
(May, 2000)