Footprinting: What is it and How Do You Erase Them

By
Eddie Sutton

Abstract

Footprinting is one of a hacker's best friends. In this paper I will discuss just exactly what footprinting is, how it affects your privacy, and how to erase your footprints. Footprinting can cause severe damage to a business and your personal life. I t can also be beneficial for you and your business. I will show you how it can be a necessary evil for you so you can protect your computer life.

Introduction

The systematic and methodical Footprinting of an organization enables attackers to create a complete profile of an organization's security posture. By using a combination of tools and techniques coupled with a healthy dose of patience, attackers can take an unknown entity (for example XYZ Organization) and reduce it to specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the internet, as well as many other details pertaining to its security posture. Although there are many types of Footprinting techniques, they are primarily aimed at discovering information related to the following environments: Internet, intranet, remote access, and extranet. (the book)

What is footprinting?

Footprinting is the first and most convenient way that hackers use to gather information about computer systems and the companies they belong to. The purpose of footprinting is to learn as much as you can about a system, its remote access capabilities, its ports and services, and the aspects of its security.

In order to perform a successful hack on a system, it is best to know as much as you can, if not everything, about that system. While there is nary a company in the world that isn't aware of hackers, most companies are now hiring hackers to protect their systems. And since footprinting can be used to attack a system, it can also be used to protect it. If you can find anything out about a system, the company that owns that system, with the right personnel, can find out anything they want about you. (http://web.textfiles.com/hacking/footprinting.txt)

In computers, footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited. (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci546674,00.html)

Footprinting is the means by which hackers target an organization and use a remote access process to garner proprietary information relevant to organization's Internet and network processors. They also access the organizational profiles for the purpose of mapping out the target organization's security stance. Footprinting employs a "who is" queries technique which produces employee names, phone numbers, and other information upon request from the hacker.

Areas targeted by computer hackers are (a) Domain Name Systems (DNS) and Internet protocols (IP) in order to extract addresses; (b) Firewalls designed to protect systems from external intrusion; and (c) Quick steps normally associated with corporate acquisitions and dispositions and subsequent broadcasting of this acquisition information on the Internet, Intranets, and mass media. When companies acquire other companies or dispose of subsidiaries, several documents are produced which become public information that are of target interest to intruders. These documents are usually created through legal processes secondary to the acquisition process. (http://www.bcte.ecu.edu/ACBMITEC/p2002/lomodavid.htm)

Why is footprinting necessary

As a necessary evil for businesses as well as individuals, footprinting is necessary to systematically and methodically ensure that all pieces of information related to the aforementioned technologies are identified. Without a sound methodology for performing this type of reconnaissance, you are likely to miss key pieces of information related to a specific technology or organization. Footprinting must be performed accurately and in a controlled fashion. (The book)

Businesses must do this to see what and where their vulnerabilities are so they can address them and make changes in the business policy. Footprinting for a non-computer based company is almost more important to address than a computer based company. The main reason for this would be the fact that hackers will certainly try, what they think to be, a non computer educated company first. This is why a business owner

must invest in his or her Information Technology department so he can be proactive and not reactive. If he waits it is like closing the barn door after the horse has gotten out. Some information, if placed in to the wrong hands, will cripple a company.

How to footprint and what Hackers look for

The attacker first identifies the various domain names that he's interested in exploiting. He then performs a footprint analysis of the target to gather as much information as possible through publicly available sources. The footprint analysis gives the hacker an indication of how large the target might be, how many potential entry points exist, and what, if any, security mechanisms might exist to thwart the attack. During a footprint analysis, the hacker attempts to discover all potentially related information that may be useful during the attack. This information includes: Company names Domain names Business subsidiaries Internet Protocol (IP) networks Phone numbers Hackers pay particular attention to potential entry points that might circumvent the "front door." (http://www.shavlik.com/whitepapers/hacker.pdf)

The first step in attacking any network is to figure out what to attack, to develop a "footprint" of the target network. There are many techniques for this. For a full discussion, see one of the excellent books in the "Hacking Exposed" series. The basic goal is to learn more about the network. There is a lot to discover, including, but not limited to, the following: Network address ranges, Host names, Exposed hosts, applications exposed on those hosts, OS and application version information patch, state of the host, and the applications structure of the applications and back-end severs

implementation details the system administrator posted to newsgroups or told a reporter about. (http://www.informit.com/articles/article.asp?p=397660&seqNum=4&rl=1)

The first item of business is to determine the scope of your footprinting activities. Are you going to footprint the entire organization, or limit your activities to certain subsidiaries or location? One thing that hackers can usually disregard that you must pay particular attention to is what we techies affectionately refer to as layers eight and nine of the seven layer OSI Model-Politics and Funding. The amount of information that is readily available about you, your organization, its employees, and anything else you can image is nothing short of amazing. So what are the needles in the proverbial haystack that we are looking for, company web pages, related organizations, location details, phone numbers, contact names, e-mail addresses, and personal details current events (Mergers, acquisitions, layoffs, rapid growth, etc.) privacy and security policies, archived information, disgruntled employees, search engines, Usenet, and resumes, other information of interest. Current events are often of significant interest to attackers. Mergers, acquisitions, scandals, layoffs, rapid hiring, reorganizations, outsourcing, extensive use of temporary contractors, and events may provide clues, opportunities and situations that didn't exist before. (The book)

To break this down a little further, lets get in to what exactly hackers are looking for and what tools they are using against you. Port scanners are used to determine which hosts are alive on the Internet, which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports are listening on each system, and the operating system that is installed on each host. Trace routes are performed to help identify the relationship

of each host to every other and to identify potential security mechanisms between the attacker and the target. Nslookup is a command line tool in Windows NT 4.0, Windows 2000, and Windows XP that can be used to perform DNS queries and zone transfers. Tracert is a command line tool used by hackers to create network maps of the target network presence. After the port scanning and trace routing is finished, attackers create a network map that represents their understanding of the target's Internet footprint. This map is used for the second phase of the attack: information enumeration. The SamSpade.org Web interface that performs Whois lookups, forward and reverse DNS searches, and trace routes. Nmap is a Unix-based port scanner and ScanLine is a Windows NT-based port scanner. (http://www.shavlik.com/whitepapers/hacker.pdf)

When dealing with FTP, Web or mail servers you have to be very careful as to whom you let in. Hackers will try to determine what version of Web, File Transfer Protocol (FTP), or mail server is running by connecting to the listening TCP and UDP ports and sending random data to each. Contact names and e-mail addresses are particularly useful items. Most organizations use some sort of derivative of the employee's name for their username and e-mail address.

Other personal details can be readily found on the internet using any number of sites like http://www.peoplesearch.com, which can give hackers personal information ranging from home phone numbers and addresses to social security numbers, credit history and criminal records among other things. Many services respond to this random data with a banner, data that identifies the running application and potentially version

information. Hackers will cross-reference this information to vulnerability databases such as SecurityFocus to look for possible exploits. Netcat (listed under Network Utility Tools) is the hacker's Swiss army knife. Used for banner grabbing and port scanning, among other things. Epdump/Rpcdump Tools to gain information about remote procedure call (RPC) services on a server. Getmac (Windows NT resource kit) Windows NT command to obtaining the media access control (MAC) Ethernet layer address and binding order for a computer running Windows NT 4.0, Windows 2000, or Windows XP. DumpSec is a security auditing program for Windows NT systems. It enumerates user and group details from a chosen system. This is the audit and enumeration tool of choice for Big Five auditors (PricewaterhouseCoopers, Ernst & Young, KPMG, Arthur Andersen, and Deloitte & Touche) and hackers alike. (http://www.shavlik.com/whitepapers/hacker.pdf)

Companies web pages are also prey to footprinting hackers. Perusing the target organization's web page will often get you of to a good start. Many times, a web site will provide excessive amounts of information that can aid attackers. In addition, try reviewing the HTML source code for comments. Be sure to investigate other sites beyond the main "www" sites as well. Many organizations have sites to handle remote access to internal resources via a web browser. VPN's are very common in most organizations as well, so looking for sites like http://vpn.company.com or http://company.com/vpn will often love sites designed to help end users connect to their companies' VPNs. You may find VPN vendor and version detail as well as detailed instructions on how to download and configure the VPN client software. Be on the lookout for references or links to other organizations that are somehow related to the

target organization. Even if an organization keeps a close eye on what it posts about itself. (The book)

Let's talk about addresses, physical and logical. A physical address can prove very useful to a determined attacker. It may lead to dumpster diving, surveillance, social engineering, and other nontechnical attacks. Physical addresses could lead to unauthorized access to buildings, wired and wireless networks, computers etc. It is even possible for the attackers to attain detailed satellite imagery of your location from various sources on the internet. Attackers can use phone numbers to look up your physical address via sites like http://www.phonenumber.com, http://www.411.com, and http://yellowpages.com. My personal favorite is http://wwwkeyhole.com. (The book)

Logical addresses or IP addresses as they are known as in the computer world are destined to be hacked. The first step is to find the logical locations for the networks of interest. We are performing a penetration test of victimsrus.com, so we start by looking up what networks are registered to who ever they want to hack. Doing so is really simple, since address ranges are public records. You can just go to http://www.samspade.org and type in the address and press Enter. Out will come all kinds of useful information about the address ranges of the domain, including contact personnel and so on.
(http://www.informit.com/articles/article.asp?p=397660&seqNum=4&rl=1)

However, perhaps even more interesting than the publicly registered address ranges for the victim is any information on networks possibly connected to the target network. For example, there may be an extranet located at extranet.whatever.com. This extranet is not publicized as well as the core domain, so it is a good bet it is not secured as well as the main public network. In addition, you may know that some other company is a business partner of whatever.com. They may very well have direct links into whatever.com. If so, it may be easier to attack them and jump from there to whatever.com. Keep in mind the first principle of successful attacks: Sometimes the shortest path to your goal is not through the front door. (http://www.informit.com/articles/article.asp?p=397660&seqNum=4&rl=1)

Attackers are as lazy as everyone else. Why make things more difficult and attack a well-defended network or host when you can take the simple approach and attack a poorly defended one and then take over the well-defended one from the back. (http://www.informit.com/articles/article.asp?p=397660&seqNum=4&rl=1)

ICANN is a technical coordination body for the Internet. It was created in October 1998 by a broad coalition of the Internet's business, technical, academic, and user communities. ICANN is assuming responsibility for a set of technical functions previously performed under U.S. government contract by The Internet Assigned Numbers (IANA).

Specifically, ICANN coordinates the assignment of the following identifiers that must be globally unique for the Internet to function:

- Internet domain names
- IP address numbers
- Protocol parameters and port numbers

In addition, ICANN coordinates the stable operation of the Internet's root DNS server system.

So, with all of this centralized management in place, mining for information should be as simple as querying a central super-server farm somewhere, right? Not exactly, while the management is fairly centralized, the actual data is spread across the globe in numerous WHOIS servers for technical and political reasons. To further complicate matters, the WHOIS query syntax, type of permitted queries, available data, and the formatting of the results can vary widely from server to server. Furthermore, many of the registrars are actively restricting queries to combat spammers, hackers, and resource overload, and to top it all off, information for .mil and .gov have been pulled from public view entirely due to national security concerns. (The book)

How to Fight Footprinting

1. Place offline any information that has the potential to identify and compromise your organization's security such as access to business plans, formulas, and proprietary documents.

2. Determine the level of information that is necessary for the public about your organization and make only that piece available on the network.

3. Visit your organization on the Web to determine current insecurities and the attributes for protection.

4. Run a ping sweep on your organizational network to see results.

5. Familiarize yourself with the American Registry for Internet Numbers (ARIN) to determine network blocks.

Tracking the hacker is a valuable method of ensuring safety of proprietary information in your organization. (http://www.bcte.ecu.edu/ACBMITEC/p2002/lomodavid.htm)

Here is a list of ten other ways to defend against a Footprinting attack.

Top Ten Ways to Secure Against Attack:

Defending your network against attack requires constant vigilance and education. Although there is no recipe for guaranteeing the absolute security of your network, the following ten practices represent the best insurance for your network.

1. Keep patches up to date by installing weekly or daily if possible. Buffer overflow and privilege escalation attacks can usually be prevented by keeping patches up-to-date. Check your vendor's site daily for new patch releases and monitor the Computer Emergency Response Team's site, http://www.cert.org, for information on the latest vulnerabilities.

2. Shut down unnecessary services/ports. Review your installation requirements by eliminating unnecessary services and applications. Perform a post-installation lockdown and hardening of the machine. Lance Spitzner, Senior Security Architect for Sun

Microsystems, Inc. authors a useful site, http://www.enteract.com/~lspitz, with more information.

3. Change default passwords by choosing strong passwords that utilize uppercase/ lowercase/ numbers/special characters. Some database applications create a database administrator account with no password. To protect against this vulnerability, test the accounts after install, and if no password is found on any account, disable the account or set a strong password. Weak passwords are not much better than no password at all. Examples of weak passwords include the user's name, birth date, or a dictionary word. Educate your administrators and users about the importance of strong passwords. A strong password should contain upper and lower case letters, as well as numbers and special characters (!, #, $, etc). A strong password should also be at least 7-8 characters in length, depending on operating system. Many operating systems provide means for requiring complex passwords, when enabled. More extreme countermeasures include one-time password mechanisms.

4. Control physical access to systems. Protecting physical access to computer systems is as important as protecting computer access. Be sure employees lock down consoles when not in use—an unlocked desktop screen can instantly allow a hacker access to the network as a privileged user. A hacker may also gain access to the network via a network jack in a conference room or any non-restricted area. Data centers and network closets should be treated with vigilance as well. Even a locked door may not be enough protection in the face of a determined attacker. Alarms, video cameras, raised floors, security guards, customer accessible cages, biometric scans, and ID cards may be necessary to adequately defend against network attacks.

5. Curtail unexpected input. Some Web pages allow users to enter usernames and passwords. These Web pages can be used maliciously by allowing the user to enter in more than just a username. Username: jdoe; rm -rf / This might allow an attacker to remove the root file system from a UNIX Server. Programmers should limit input characters, and not accept invalid characters such as |; < > as possible input.

6. Perform backups and test them on a regular basis.

7. Educate employees about the risks of social engineering and develop strategies to validate identities over the phone, via e-mail, or in person.

8. Encrypt and password-protect sensitive data. Data such as Web accessible e-mail should be considered sensitive data and should be encrypted. This will discourage any type of sniffer program or exposure of sensitive company data.

9. Implement security hardware and software. Firewalls and intrusion detection systems should be installed at all perimeters of the network. Viruses, Java, and ActiveX can potentially harm a system. Anti-virus software and content filtering should be utilized to minimize this threat.

10. Develop a written security policy for the company.

(http://www.atapusa.org/downloads/hacking.pdf)

These methods will help to lessen attacks of footprinting, which lead to your computer or your company being hacked. With that said, a company has to stay vigil at all times due to new methods of intrusion being developed almost daily.

Conclusion

The information stated above hopefully has helped you understand the nature of what Footprinting is, what hackers look for to Footprint, and how to defend against it. I, myself, learned a great deal above the subject while doing the research. I feel you must defend against Footprinting for the defense of your network. Try Footprint your own computer or company's computer, if you have the OK to do so, and see what you can learn from it. I believe you will be quite surprised at what you find.

Resources

Schultze, E. (2002, March7). Thinking Like a Hacker Retrieved November 1, 2005, from Thinking Like a Hacker Web Site: http://www.shavlik.com/whitepapers/hacker.pdf

Caffeine20. (2002, November 11). Footprinting your target Retrieved October 28, 2005 from Antionline Web Site: http://www.antionline.com/showthread.php?s=&threadid=236722

Riley, S. and Johansson, J. (2005 July 1) Anatomy of a Hack-The Rise and Fall of Your Network Retrieved on October 28, 2005 from Footprinting Web Site: http://www.informit.com/articles/article.asp?p=397660&seqNum=4&rl=1

Nachenburg, C. (2005) Hacking A Computer Science Guide Retrieved on October 28, 2005 from Book Rags Web Site: http://www.bookrags.com/sciences/computerscience/hacking-csci-03.html

Velocity M. (2005) Footprinting and the Basics of Hacking Retrieved on October 29, 2005 from Web.textedfiles.com Web Site: http://web.textfiles.com/hacking/footprinting.txt

Anonymous, (2005) Week 2: Footprinting Retrieved on October 28, 2005 from gaia.ecs.csus.edu Web Site: http://gaia.ecs.csus.edu/~ghansahi/classes/notes/196n_at_def_notes/lectures/wk02.ppt#16

Velocity, M. (2002 February 13). What is Footprinting Retrieved on October 28, 2005 from Footprinting: The Basics of Hacking Web Site: http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=5359&mode=thread&order=0&thold=0

Mittens, M. (2004 March 18) WarGames: Steps to an Attack Retrieved on October 27, 2005 from WarGames: How To Part 2 from Web Site: http://www.governmentsecurity.org/archive/t7354.html

HellBound (2004 April 11) Advanced Footprinting Retrieved on October 28, 2005 from knowledge-bank.cauniversity Web Site: http://knowledge-bank.cauniversity.org/?file=kb.php&action=view&id=322

HellBound (2004 April 11) Basic Footprinting Retrieved on October 28, 2005 from knowledge-bank.cauniversity Web Site: http://knowledge-bank.cauniversity.org/?file=kb.php&action=view&id=323

McClure, S, Scambray, J, Kurtz, G (2005) Hacking Exposed 5th Edition Footprinting pp(5-77), McGraw Hill Osbourne

David, E. (2005) Track and Thwart Computer Hacking Retrieved on October 1, 2005 from Track and Thwart Computer Hacking Web Site: http://www.bcte.ecu.edu/ACBMITEC/p2002/lomodavid.htm

Dawg, S (2005) “Footprinting” a System Retrieved on October 1, 2005 from Hacking 101 from Web Site: http://www.binrev.com/magazine/1.1/Hacking%20101.pdf

Anonymous (2001 April 23) Footprinting Retrieved on October 1, 2005 from searchSecurity Definitions from Web Site: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci546674,00.html

McGreevy, J. (2002) Footprinting What is it, Who should do it, and Why Retrieved on October 1, 2005 from Sans.org Web Site: http://www.sans.org/rr/whitepapers/auditing/62.php

Berkowitz, B. (2002) Information Warfare: Time to Prepare Retrieved on October 1, 2005 from issues.org Web Site: http://www.issues.org/17.2/berkowitz.htm

Raggo, M. (2002) Defending Against an Attack Retrieved on November 2, 2005 from Hacking and Network Defense Web Site: http://www.atapusa.org/downloads/hacking.pdf

Niederhoffer, M. (2002 August) Internet Security and CPA Retrieved on November 2, 2005 from The CPA Journal Web Site: http://www.nysscpa.org/cpajournal/2002/0802/dept/d087102a.htm

Redwine, S. (2002) Dissecting Trust and the Assurance-Violation Dynamic Retrieved on November 2, 2005 from Dissecting Trust and the Assurance-Violation Dynamic Web Site: http://csdl2.computer.org/comp/proceedings/hicss/2003/1874/09/187490331b.pdf

Bishop, M. (2000) UNIX Security Tools: Use and Compare Retrieved on November 2, 2005 from USENIX Tech Annual Conference from Web Site: http://www.usenix.org/publications/library/proceedings/usenix2000/tutsun.html