Global Information Assurance Certification Paper

Footprinting
What Is It, Who Should Do It, And Why?

By: James P. McGreevy
GIAC User ID: mcgreev001
Security Essentials

ABSTRACT

Are you footprinting your systems? Or is an attacker doing it for you? Yes, footprinting can be good for you just like scanning. The process of footprinting is the first step in information gathering of hackers. To perform or thwart a successful attack, one needs to gather information. The hacker's intention is to learn about all aspects of the perspective organization's security posture, profile of their Intranet, remote access capabilities, and intranet/extranet presence (Scambray, McClure, and Kurtz 2001).

Footprinting is a necessary evil. What does that mean? Successful hackers are building their information database about your company's security weaknesses. Wouldn't be nice to know these weaknesses in advance to take proper action? Yes, it would be nice. Therefore, security personnel need to add footprinting to their already long task list. One has to remember that an organization's security is a process, not a technology. A good security system provides multiple layers of security. The system would be defined as "a collection of things or elements which, working together, produce a result not achievable by the things alone."[1] Hopefully, the suggestions in the text below make that task easier.

[1]Rechtin, Eberhardt, and Maier, Mark W., "The Art of Systems Architecting", CRC Press, 1997, p. 254.

OPEN SOURCE SEARCHING

Footprinting is the process of using various tools and technologies to understand and learn the best way to attack a target. Attackers find out as much as possible without actually giving themselves away. They find public information or appear as normal users. The attacker/hacker does a 'whois' lookup to find as much information as possible about the network along with the domain name. They might stroll through your DNS tables using nslookup, dig, or other utilities to do domain transfers to find the names of machines. The hacker/attacker browses other public information looking for the public web site and anonymous FTP sites. Specifically, hackers/attackers look for domain names, network blocks, particular IP addresses, networking protocols in use, internal domain names, IDSs (Intrusion Detection Systems), telephone numbers, ACLs (Access Control Lists), etc. Footprinting is necessary to identify the above listed items. Hackers use this information to attack. Security personnel can use it to strengthen their security stance.

Before one begins making tracks for the target, one may want to focus on smaller sections within the organization. Footprinting an entire company can be a daunting task and could lead to a frustrated security group who will have no idea where to start. Possibly begin in one department and broaden the process as time allows.

According to Scambray, McClure, and Kurtz, begin by studying the company's web page. See if it has too much information that hackers can use against you. They say to look for

- Locations
- Related companies
- Merger or acquisition news
- Phone numbers
- Contact names and email addresses
- Privacy or security policies indicating the types of security mechanisms in place
- Links to other web servers related to the organization

It may also be advantageous to read the HTML source code for comments. Take time to study this information. It is wise to copy the source code and save it to your system allowing you to thoroughly collect much data. Refer to these web sites to make the process easier: Wget (ftp://gnjilux.cc.fer.hr/pub/unix/util/wget/) for Unix and Teleport Pro (http://www.tenmax.com/teleport/home.htm) for Windows. FerretPRO is a search tool from FerretSoft (http://www.ferretsoft.com) that provides the ability to search many different search engines simultaneously. Other tools in the software allow searching IRC, USENET, email, and file databases looking for clues. Another free tool to search multiple search engines is http://www.dogpile.com. AltaVista or Hotbot are other tools with advanced searching abilities.

A security professional may want to ask these questions in deciding if what's out there could be used against the company.

- Are there news articles, press releases, etc that may provide information about the state of the company's security posture?
- What is on these sites about your company? (finance.yahoo.com or www.companysleuth.com)
- Are there any news stories out on the web relating to security incidents at your company?

Finally, Scambray, McClure, and Kurtz recommend using advanced search engines to uncover any information hackers might use. They advise searching for all sites that have links back to the target organization's domain. Sometimes these "other" sites are not secure. Hackers might use an EDGAR search to find out about a company's newest acquisition. The reason is companies scramble to connect new folks without following best practices for security leaving them open for attack.

It is difficult to protect your company's jewels from these types of information gathering tools. However, if you use these tools to locate weaknesses, act on those weaknesses, then you'll be a hero for another day. Check the Site Security Handbook (RFC 2196 http://www.ietf.org/rfc/rfc2196.txt) as a resource for many policy-related issues.

NETWORK ENUMERATION

Network enumeration is the process to identify domain names and associated networks. The first step is to identify the domain names and associated networks related to a

particular organization. The end result of performing enumeration is the hacker has the information they need to attack your system. The process is performing various queries on the many whois databases on the Internet. According to Scambray, McClure, and Kurtz, companies are listed with registrars and one would query these registrars for the information they seek. However, the hacker would need to know which registrar handles the company in question. There are five types of queries.

The first is the Registrar Query. This gives information on potential domains that match the target and associated information. One needs to determine the correct registrar so they could submit detailed queries to the correct database in steps. It is recommended to use wild cards to find additional search results. The second is Organizational Queries where the search of a specific registrar will give all instances of the target's name. The results show the many different domains associated with the target company. Thirdly, Domain Queries are based on organizational queries and could lead to the company's address, domain name, administrative contact and phone number, and domain servers. At this point, one would need to become a detective to analyze the information for clues that will provide more information. The administrative contact is an important piece of information since it will yield the person responsible for the Internet connection or firewall and it may list the fax and voice numbers. A hacker knowing these numbers new has a range to use his wardialer. This information could also lead to some social engineering opportunities. The security officer could place false information here to foil the hacker's attempt to use social engineering. The Network Query is the fourth method where one would use the American Registry for Internet Numbers (ARIN http://www.arin.net/) to discover the blocks owned by a company. It's handy to use the wildcard here as well. Last is the POC Query that lists the user's database handle. One tool I noticed was located at http://www.codeproject.com/internet/ipenum.asp and one would use this freeware to find the IP addresses a machine possesses.

What do you do with this information? The suggestion here is to develop countermeasures to protect the company. Scambray, McClure, and Kurtz suggest keeping the organization's domain information up to date, consider using a toll-free number, and use a fictitious administrative contact to trip the social engineer into exposing his intentions. They also suggest using secure solutions like password or PGP to authenticate a change to the domain information.

DNS INTERROGATION

Upon the completion of the above information gathering techniques, a hacker would begin to query the DNS. A common problem is system administrators allowing untrusted Internet users to perform a DNS Zone Transfer. Some tools to use to perform zone transfers include *nslookup*. To use *nslookup*, it has to be told to look up a specific DNS server that would have been found in one of the earlier steps. Also type *any* to pull any DNS records available for a complete list. Then use the ls option to list all associated records for the domain. Use the –d to list all records for the domain. The information listed may include interesting results a hacker can use against the company. The security officer can use this information to tighten the loose ends. One can determine the mail

exchange records by using host. Knowing where the mail is handled could lead to the discovery of the firewall network.

As a newbie to the world of security, I found several tools that are free for DNS Interrogation. These three tools were openly available out on the web and easy to use.

- http://www.zoneedit.com/lookup.html?ad=goto
- http://www.infobear.com/nslookup.shtml
- http://www.network-tools.com/

I did find that the University of Utah's DNS Services site has taken the tool off-line due to security concerns. I felt that was a point of interest.

How does one provide security against DNS Interrogation? Begin by trying these tools at your company and shoring up the problems found. Remember to reduce the amount of information available to the Internet. One should restrict zone transfers to authorized servers. Set your firewall or router to deny all unauthorized inbound connections to TCP port 53. Configure external name servers to provide information only about systems directly connected to the Internet. Finally, set the access control device or intrusion detection system to log this type of information as hostile activity. Another countermeasure according to Novak is to disable BIND so as not to leak DNS server versions of BIND. BIND versions 8.x have an options keyword that can do this. One of the ways that this can be completed is by altering the named.conf file as follows:

```
options {
        version "version unavailable";
        };
```

Novak continues to explain that you can put whatever text you feel is appropriate in the message that is displayed. Some sites even reply with the wrong version of BIND just to see what ensuing attack may look like after an unauthorized query for the version of BIND. Still another configuration would be to set external name servers to not list the internal networks they service. Finally, avoid using HINFO records since that allows identifying the target's operating system easier.

NETWORK RECONNAISSANCE

Traceroute may help the would-be hacker discover the network topology of a target network as well as access control devices. There is a GUI type available through VisualRoute (www.visualroute.com) or NeoTrace (http://www.neotrace.com/). The results can differ depending on what OS is being used. Unix sends the packets as UDP with the option of using the Internet Control Messaging Protocol with the –I switch. In Windows, the default behavior is to use ICMP echo request packets (ping). There are other switches available to help bypass access control devices. The –p *n* option of traceroute allows one to specify a starting UDP port number (*n*). The switch –S will stop port incrementation for traceroute version 1.4a5 (ftp://ftp.ee.lbl.gov/traceroute-1.4a5.tar.Z). This forces every packet to have a fixed port number. According to Zachary Wilson,

other recon type tools include ping sweeps, TCP Scans, UDP Scans, and OS Identification.

- **Ping Sweeps**-ping a range of IP addresses to find which machines are alive.
- **TCP Scans**-Probes for listening TCP ports looking for services. Scans can use normal TCP connections or stealth scans that use half-open connections or FIN scans. Scans can be sequential, randomized, or configured lists of ports
- **UDP Scans**-Scans that send garbage UDP packets to the desired port. Most machines respond with an ICMP "destination port unreachable" message meaning that no service is available.
- **OS Identification**-The process involves sending illegal or unusual ICMP or TCP packets. The system's response is unique to invalid inputs and allows one to figure out what the target machine is running.

Another tool called Traceloop is available at http://www.traceloop.com/. It's an interesting idea that lets you see what route your traffic takes on the /return/ path. By utilizing a large group of distributed test points anyone registered with the service can run traceroutes in both directions provided there is a client near the destination ISP. Traceloop is able to perform a round trip analysis of a specific route giving the user the whole picture. Traceloop can show both the outbound path from your network and the return path. According to Dashbit, reverse path analysis was cited by network operators as the biggest unmet need for diagnosing off-net problems.

Countermeasures that can be used to fight and identify network reconnaissance include many commercial network intrusion detection systems. If someone traceroutes your company, use RotoRouter to take the offensive (www.packetstormsecurity.com).

SUMMARY

According to Christine Orshesky, there is an increasing need for corporations to protect themselves from computer viruses and other things that bump around the on-line community. Denial of Service attacks and widespread virus infections have raised the issue of 'due care'. No longer is it reasonable to rely solely on the installation of anti-virus products to protect the on-line environment. A holistic approach that provides the corporation with an integrated and layered security posture is necessary to achieve protection – including policy, procedures, awareness, and technology. There are many devices available to the hacker to footprint your company's network. Use these tools to find the weaknesses before they do. Therefore, you can prepare an organized approach to your layered security stance.

FOR FURTHER INFORMATION

1. http://www.cert.org/incident_notes/ -Look here for a listing of incidents. Click on the links to find countermeasures.
2. http://www.samspade.org/ -Resolves an IP address or hostname.
3. http://www.sec.gov/ -EDGAR is listed here. EDGAR lists information about

laws and company's acquisitions. It also lists buyer's names, addresses, social security numbers, etc.

4. http://www.operationsecurity.com/ -A listing of helpful information regarding security.
5. http://www.operationsecurity.com/resource_db.php?viewCat=41 -Use these tools to find out what is out on the web about your company.
6. http://www.ibt.ku.dk/jesper/NTtools/ -Look here for enumeration tools.
7. http://www.operationsecurity.com/resource_db.php -Check out this site for DNS Interrogation tools.
8. http://www.itpapers.com/cgi/PSummaryIT.pl?paperid=22016&scid=275-*DNS Evasion Techniques and Beyond* by Judy Novak.

REFERENCES

Hale, Poynter, and Sample, *Holistic Security*, 2000. URL: http://www.jerboa.com/whitepapers/holisticsecurity.pdf

Novak, Judy, *DNS Evasion Techniques and Beyond* – February 2000. URL: http://www.itpapers.com/cgi/PSummaryIT.pl?paperid=22016&scid=275

Orshesky, Christine, *Corporations' Due Care*, September 2000. URL: http://www.virusbtn.com/vb2000/Programme/papers/orshesky.pdf

Scambray, J., Stuart McClure, and George Kurtz. *Hacking Exposed*. 2nd Edition. Osborne/McGraw-Hill Co., 2001. ISBN: 0-07-212748-1

Wilson, Zachary. *Hacking: The Basics*. 4 April 2001. URL: http://www.sans.org/infosecFAQ/hackers/hack_basics.htm