FOOTPRINTING:INTRODUCTION

Footprinting involves investigating system with the purpose of attacking and compromising the systems. It helps to collect data both actively and passively about the intended target of evaluation. Spending a good amount of time learning about your target before you start launching attacks and strikes against it will allow for more precise targeting and more accurate and productive actions.

Steps of Ethical Hacking

Phase 1: Footprinting → The goal is to gather as much information as is reasonable and useful about a potential target with the objective of getting enough information to make later attacks more accurate. Information that can be gathered during this phase includes the following:

→IP address ranges
→Namespaces
→Employee information
→Phone numbers
→Facility information
→Job information

Phase 2: Scanning → It focuses on an active engagement of the target with the intention of obtaining more information. The scanning of any network **helps locate the active hosts in a network which helps in planning the later attack.** Footprinting helps identify potential targets, but not all may be viable or active hosts. During this phase tools such as these are used:

→Pings
→Ping sweeps
→Port scans
→Tracert

Phase 3: Enumeration → enumeration is the step before actually hacking the system. Enumeration is the systematic probing of a target with the goal of **obtaining user lists, routing tables, and protocols from the system.** Information such as shares, users, groups, applications, protocols, and banners all proved useful in getting to know your target, and this information is carried forward into the attack phase. The information gathered during phase 3 typically includes, but is not limited to, the following:

→Usernames
→Group information
→Passwords
→Hidden shares
→Device information
→Network layout Protocol information
→Server data
→Service information

Phase 4: System Hacking → This is a much more complex phase than previous 3 phases. It cannot be completed in just one step. It involves a methodical approach that **includes cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, concealing evidence, and then pushing into a complex attack.**

What is Footprinting?

Footprinting, or reconnaissance, is a method of observing and collecting information about a potential target with the intention of finding a way to attack the target. Footprinting looks for information and later analyzes it, looking for weaknesses or potential Footprinting generally entails the following steps to ensure proper information retrieval:

1. Collect information that is **publicly available about a target** (for example, host and network information).
2. As certain the **operating system(s) in use** in the environment, including web server and web application data where possible.
3. Issue queries such **as Whois, DNS, network, and organizational queries.**
4. **Locate existing or potential vulnerabilities or exploits** that exist in the current infrastructure that may be conducive to launching later attacks.

Why perform Footprinting?

Footprinting helps gather information and strategize our hacks. Using this we can choose the least resistance path of the hack. If done by a skilled, inventive, and curious party (you!), the amount of information that can be passively gathered is staggering. Expect to obtain information such as this:
1>Information about an **organization's security posture and where potential loopholes may exist.** This information will allow for adjustments to the hacking process that make it more productive.
2>A database that paints a detailed picture with the maximum amount of information possible about the target. This may be from an application such as a web application or other source.
3>A network map using tools such as the Tracert utility to construct a picture of a target's Internet presence or Internet connectivity. Think of the network map as a roadmap leading you to a building; the map gets you there, but you still have to determine the floor plan of the building.

Goals Of The Footprinting Processes

What we are looking for? and what will we have in the end? Are the two important questions we should ask before doing the Footprinting. We may expect to have following information at the end(the below list is a limited list and we can expect much more than this):

→Network information
→Operating system information
→Organization information, such as CEO and employee information, office information, contact numbers, and email
→Network blocks
→Network services
→Application and web application data and configuration information →System architecture
→Intrusion detection and prevention systems
→Employee names
→Work experience

NETWORK INFORMATION

Much of the network information that is useful to you in starting the initial phase of an attack is readily available or can be easily obtained with little investigation. During the Footprinting phase, keep your eyes open for the following items:

→Domain names the company uses to conduct business or other functions, including research and customer relations
→Internal domain name information
→IP addresses of available systems
→Rogue or unmonitored websites that are used for testing or other purposes
→Private websites
→TCP/UDP services that are running
→Access control mechanisms, including firewalls and ACLs
→Virtual private network (VPN) information
→Intrusion detection and prevention information as well as configuration data
→Telephone numbers, including analog and Voice over Internet Protocol (VoIP)
→Authentication mechanisms and systems

OPERATING SYSTEM INFORMATION

The operating system is one of the most important areas you must gain information about. When browsing information on job sites or gathering information from elsewhere, look closely to see if anything you obtain can give you clues to what is running. For example, job postings that ask for experience on Office 2016 or Internet Explorer 9 could go a long way toward narrowing down the OSs present in the environment.

→User and group information and names
→Operating system versions
→System architecture
→Remote system data
→System names
→Passwords

ORGANIZATION DATA

Not all information is technical, so look for information about how an organization works. Information that provides details about employees, operations, projects, or other details is vital. Expect to encounter this information in many locations such as the company's own website, discussion groups, financial reports, and other locations. This information includes the following:

→Employee details
→Organization's website
→Company directory
→Location details
→Address and phone numbers
→Comments in HTML source code
→Security policies implemented
→Web server links relevant to the organization
→Background of the organization
→News articles and press releases

Terminologies in Footprinting

Open source and Passive Information Gathering

open source or passive information gathering is the **least aggressive**. The process relies on obtaining information from those sources that are **typically publicly available**. Potential sources include **newspapers, websites, discussion groups, press releases, television, social networking, blogs, and innumerable other sources.** With a skilled and careful hand, it is more than possible to gather operating system and network information, public IP addresses, web server information, and TCP and UDP data sources, just to name a few.

Active Information Gathering

It involves engagement with the target through techniques such as social engineering. A savvy attacker engages employees under different guises under various pretenses with the goal of socially engineering an individual to reveal information.

Passive Information Gathering

It is **less aggressive** and overt than active information gathering. Whereas active information gathering requires much more direct engagement with the target, passive does not. Passive uses methods that **gather information indirectly about a target** from other sources. These sources include **websites, job postings, social media, and other types of sources.** Typically, the information-gathering process will start passively.

Pseudonymous Footprinting

It involves **gathering information from online sources that are posted by someone** from the target but under a different name or in some cases a pen name. Under normal conditions this technique can be **used to get unsuspecting parties to contact you.** Using the name of someone within the company (whom you may have never met face to face) but from another office or location can be an easy way to entrap someone and gain useful information.

Internet Footprinting

Here we mainly use internet techniques such as Google Hacking, Google apps to identify security holes in website's configuration and computer code) and other methods to find out what your target wants to hide (or doesn't know is public information) that a malicious party can easily obtain and use.

Threats introduced by Footprinting

Social Engineering→ One of the easiest ways to gain information about a target or to get information in general is to just ask for it. When asking doesn't work, you can try manipulating people with the goal of getting that gem of information that can give you useful insight.
Network and System Attacks→ These are designed to gather information relating to an environment's system configuration and operating systems.
Information Leakage→ This one is far too common nowadays; **organizations frequently have become victims of data** and other company secrets slipping out the door and into the wrong hands.
Privacy Loss→ Another one that is common—all too common, sadly—is privacy loss. Remember that gaining access to a system isn't just about controlling an environment; it could also be a way to gather private and personal information within it. If you happen to be the target of such an attack, you may easily find yourself running afoul of laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or Sarbanes- Oxley, to name a couple.
Revenue Loss→ Loss of information and security related to online business, banking, and financial-related issues can easily lead to lack of trust in a business, which may even lead to closure of the business itself. Remember that aside from the financial loss in fines, penalties, and lawsuits, customers are prone to take their business elsewhere if they don't feel it is safe.

The Footprinting Processes

It's important to log all kind of data we gather irrespective of how insignificant it looks at the time.

Using Search Engines

Search engines such as google or bing can help in collecting lot's of information through a SERP(Search Engine Result Page). A search can easily provide even more details such as names of security personnel, brand and type of firewall, and antivirus protection, and it is not unheard of to find network diagrams and other information.

Google hacking

Google hacking is not anything new and has been around for a long time, it just isn't widely known by the public. Here we use advanced operators rather than be at the whim of search engine. With Google hacking it is possible to obtain items such as passwords, certain file types, sensitive folders, logon portals, configuration data, and other data.
Cache:→ Displays the version of a web page that Google contains in its cache instead of displaying the current version.
    Syntax: cache:<website name>
Link:→ Lists any web pages that contain links to the page or site specified in the query.
J   ***Syntax***: link:<website name>
Info:→ Presents information about the listed page.
    Syntax: info:<website name>
Site:→ Restricts the search to the location specified.
    Syntax: <keyword> site:<website name>
Allintitle:→ Returns pages with specified keywords in their title.
    Syntax: allintitle: <keywords>
Allinurl:→ Returns only results with the specific query in the URL.
    Syntax: allinurl: <keywords>
a very good resource is the Google Hacking Database (GHDB). This website (www.exploit-db.com/google-dorks/) has been maintained for a very long time; there you will find the operators described here along with plenty of new ones.
Use the google hacking after you have done some reconnaissance, because if you have some initial information then you can search effectively.

To use a search engine effectively for footprinting, always start with the basics. The very first step in gathering information is to begin with the company name. Enter the company name and take note of the results, because some interesting ones may appear.

Note:→ It is also worth your time to look beyond the first 3-5 pages of results because you can miss information that may be valuable. Studies have shown that most users look at only the first 3-5 pages before stopping and trying another search. Look closely!

Tip:→ In some cases you may find that the information you wanted or hoped for was on a website that has long since been removed, but you are in luck in this case. Thanks to Archive.org (also known as The Wayback Machine), you can find archived copies of websites from which you can extract information.

Netcraft Actually a suite of related tools, Netcraft lets you obtain web server version, IP address, subnet data, OS information, and subdomain information for any URL. Remember this tool—it will come in handy later. Netcraft can also reveal the subdomains of a target by simply entering the domain name the right way. Make sure that you enter a target as domainname.com and not www.domainname.com. For example, use Microsoft.com instead of www.microsoft.com for the target. The result will be the main domain plus all the subdomains associated with it. It helps to find **beta versions of company websites, company extranets, and plenty of other items companies would have rather kept hidden.**

Link Extractor This utility locates and extracts the internal and external URLs for a given location.

Public and Restricted Websites Websites that are intended not to be public but to be restricted to a few can provide you with valuable information. Because restricted websites—such as technet.microsoft.com and developer.apple.com—are not intended for public consumption, they are kept in a subdomain that is either not publicized or that has a login page.

Location and Geography

Physical information about location of office and personnel is a vital information. knowing a company's physical location can aid in dumpster diving, social engineering, and other efforts.

Google Earth→ This popular satellite imaging utility has been available since 2001, and since that time it has gotten better with access to more information and increasing amounts of other data. Also included in the utility is the ability to look at historical images of most locations, in some cases back more than 20 years.

Google Maps→ Google Maps provides area information and similar data. Google Maps with Street View allows you to view businesses, houses, and other locations from the perspective of a car. Using this utility, many people have spotted things such as people, entrances, and even individuals working through the windows of a business.

Webcams→ These are very common, and they can provide information on locations or people.

Eg: intitle:"live view" intittle:axis

People Search→ Many websites offer information of public record that can be easily accessed by those willing to search for it. It is not uncommon to come across details such as phone numbers, house addresses, email addresses, and other information depending on the website being accessed. Some really great examples of people search utilities are Spokeo, ZabaSearch, Wink, and Intelius

NOTE: PHYISICAL INFORMATION IS IMPORTANT IN CASE OF PHYSICAL SECURITY

SOCIAL NETWORKING AND INFORMATION GATHERING

A large number of people who use these services provide updates on a daily basis. You can learn not only what an individual is doing but also all the relationships, both personal and professional, that they have. Because of the openness and ease of information sharing on these sites, a savvy and determined attacker can locate details that ought not to be shared. We can collect data such as project data, vacation information, working relationships, and location data. Using these data and social engineering we can build a sense of trust.

Some popular social networking services that are worth scouring for information about your target may be the ones that you are already familiar with:

Facebook→ The largest social network on the planet boasts an extremely large user base with a large number of groups for sharing interests. Facebook is also used to share comments on a multitude of websites, making its reach even farther.

Twitter→ Twitter has millions of users, many of whom post updates several times a day. Twitter offers little in the way of security, and those security features it does have are seldom used. Twitter users tend to post a lot of information with little or no thought as to the value of what they are posting.

Google+→ This is Google's answer to the popular Facebook. Although the service has yet to see the widespread popularity of Facebook, there is a good deal of information present on the site that you can search and use.

LinkedIn→ One of my personal favorites for gathering information is LinkedIn. The site is a social networking platform for job seekers, and as such it has employment history, contact information, skills, and names of those the person has worked with.

Instagram→ This social media service allows the sharing of photos online. The service is extremely popular and is used by a large number of people worldwide. Figure 4.3 shows a screenshot of Instagram.

Introduction to **EchoSEC**

One of the most exciting and interesting products for extracting information from social media is a relatively new service known as Echosec. Echosec, found at **www.echosec.net**, is a service that allows you to search social media and takes **advantage of location services to show where the postings originated. Simply put, this means that you can pick a spot on a map using a selection box, or type in an address or name, and view everything that has been posted from that location. You can search by username or keyword as well and then even go a step further and filter the search by date range**. The easiest and most obvious way would be to enter the address of the company and/or select a box around the address and see what appears. Since a lot of people post information to social media regularly, it is possible to get information in and around a workplace. This could score valuable information about who is in the organization, where they are, what they are doing, and the like; you may even get extra lucky and see where employees are going for lunch that day so you can "meet" them there.

Maltego

Another valuable tool for visualizing information in social media (as well as other sources) is called Maltego. Maltego is available at www.paterva.com, where both a free version and a paid version are available.

Financial Services and Information Gathering

Popular financial services such as **Yahoo! Finance, Google Finance, and CNBC** provide information that may not be available via other means. This data includes company officers, profiles, shares, competitor analysis, and many other pieces of data. Gathering this information may be incredibly easy. Using this data we can esily launch a phsing and a spear phising attack.

Job posting in information gathering

If you visit a job posting site and find a company that you are targeting, you simply need to investigate the various postings to see what they are asking for. It is not uncommon to find information such as infrastructure data, operating system information, and other useful facts. A quick perusal through job sites such as Monster.com, Dice.com, or even Craigslist.com can prove valuable. This information is essentially free, because there is little investment in time or effort to obtain it in many cases. When analyzing job postings, keep an eye out for information such as this:

Job requirements and experience Employer profile

Employee profile

Hardware information (This is incredibly common to see in profiles; look for labels such as Cisco, Microsoft, Juniper, Checkpoint, and others that may include model or version numbers.)

Software information

Emails

emails are important in any organization for communication. One tool that is very useful for this purpose is **PoliteMail (www.politemail.com)**, which is designed to create and track email communication from within Microsoft Outlook. This utility can prove incredibly useful if you can obtain a list of email addresses from the target organization. Once you have such a list, you can then send an email to the list that contains a malicious link. When the email is opened, PoliteMail will inform you of the event for each individual. Another utility worth mentioning is **WhoReadMe (http://whoreadme.com)**. This application lets you track emails and also provides information such as operating system, browser type, and ActiveX controls installed on the system.

NOTE: *Don’t forget that by searching discussion groups and other resources on*

Google you may very well find emails posted that can also yield useful information.

Competitive Analysis

The reports created through competitive analysis provide information such as product information, project data, financial status, and in some cases intellectual property. Good places to obtain competitive information are the following:

EDGAR (the Electronic Data-Gathering, Analysis, and Retrieval system) contains reports publicly traded companies make to the Securities and Exchange Commission (SEC). Learn more at www.sec.gov/edgar.shtml.

LexisNexis maintains a database of public record information on companies that includes details such as legal news and press releases. Learn more at **www.lexisnexis .com/en-us/home.page**.

BusinessWire (www.businesswire.com/portal/site/home/) is another great resource that provides information about the status of a company as well as financial and other data. **CNBC (www.cnbc.com)** offers a wealth of company details as well as future plans and in-depth analysis.

When analyzing these resources, look for specific types of information that can prove insightful, such as the following:

1>When did the company begin? How did it evolve? Such information gives insight into their business strategy and philosophy as well as corporate culture.

2>Who are the leaders of the company? Further background analysis of these individuals may be possible.

3>Where are the headquarters and offices located?

NOTE: IF YOU DON’T GET MUCH INFORMATIONA BOUT ANY COMPANY THEN TRY TO LOOK WHAT THE COMPETITORS KNPWS AS SOMETTIMES COMPETTITORS KNOW MORE THAN THE PUBLIC.

Gaining Network Information

1) **Whois**
   This utility helps you gain information about a domain name, including ownership information, IP information, netblock data, and other information where available. The utility is freely available in Linux and Unix and must be downloaded as a third-party add-on for Windows
2) **Ping** Utilizing ICMP, this utility is used to determine not only if a host is reachable, but also if it is up or down.

3) **Nslookup** This utility is used to query DNS servers and gain information about various parts of the DNS namespace or individual hosts. The name stands for Name Server Lookup, which accurately describes its role. On the Unix and Linux platforms the DIG command is used to perform the same function as nslookup. Here mx is for mail server and ns is for name servers.
4) **Tracert** This utility is designed to follow the path of traffic from one point to another, including points in between. The utility provides information on the relative performance and latency between hops. Such information can be useful if a specific victim is targeted because it may reveal network information such as server names and related details. The utility is freely available for all Oss

Social Engineering: the Art of Hacking Humans

Inside the system and working with it is the human being, which is frequently the easiest component to hack. Human beings tend to be, on average, fairly easy to obtain information from.

Eavesdropping This is the practice of covertly listening in on the conversations of others. It includes listening to conversations or just reading correspondence in the form of faxes or memos. Under the right conditions, you can glean a good amount of insider information using this technique.

Phishing Phishing is the process of sending emails to a group of email addresses and

making the message look legitimate enough that the recipient will click a link in the email. Once the victim clicks the link, they are typically enticed into providing information of a personal nature under a pretense such as their bank requesting personal data to reset their account or such. In practice as a penetration tester, you would use methods such as **spear phishing or whaling.** Spear phishing means that you would only send phishing emails to an individual company or organization and make the email look like it comes from some vendor or person they work with to get them to provide info**. Whaling targets only those within an organization who are almost certain to have valuable information and works using the same methods.**

Shoulder Surfing This is the act of standing behind a victim while they interact with a computer system or other medium while they are working with secret information. Shoulder surfing allows you to gain passwords, account numbers, or other secrets.

Dumpster Diving This is one of the oldest means of social engineering, but it’s still an effective one. Going through a victim’s trash can easily yield bank account numbers, phone records, source code, sticky notes, CDs, DVDs, and other similar items. All of this is potentially damaging information in the wrong hands.