What is Footprinting?

Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.

Footprinting is the first step of any attack on information systems; attacker gathers publicly available sensitive information, using which he/she performs social engineering, system and network attacks, etc. that leads to huge financial loss and loss of business reputation.

Know Security Posture: Footprinting allows attackers to know the external security posture of the target organization.

Reduce Focus Area: It reduces attacker's focus area to specific range of IP address, networks, domain names, remote access, etc.

Identify Vulnerabilities: It allows attacker to identify vulnerabilities in the target systems in order to select appropriate exploits.

Draw Network Map: It allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break.

Objectives of Footprinting

Collect Network Information

Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.

- Footprinting is the first step of any attack on information systems; attacker gathers publicly available sensitive information, using which he/she performs social engineering, system and network attacks, etc. that leads to huge financial loss and loss of business reputation.

Know Security Posture:

- Footprinting allows attackers to know the external security posture of the target organization.

Reduce Focus Area:

- It reduces the attacker's focus area to a specific range of IP addresses, networks, domain names, remote access, etc.

Identify Vulnerabilities:

- It allows attacker to identify vulnerabilities in the target systems in order to select appropriate exploits.

Draw Network Map:

- It allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break.

Collect System Information

- User and group names
  - System banners
    - Routing tables
      - SNMP information
        - System architecture
          - Remote system type
            - System names
              - Passwords

Objectives of Footprinting (Continued)

Collect Organization's Information: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

Press releases

Footprinting through Search Engines

Attackers use search engines to extract information about a target such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks.

Search engine caches and internet archives may also provide sensitive information that has been removed from the World Wide Web (WWW).

Finding Company's Public and Restricted Websites

Search for the target company's external URL in a search engine such as Google, Bing, etc.

Restricted URLs provide an insight into different departments and business units in an organization.

You may find a company's restricted URLs by trial and error method or using a service such as http://www.netcraft.com

This is the netcraft result for yearup https://sitereport.netcraft.com/?url=http://www.yearup.org

Determining the Operating System

Use the Netcraft tool to determine the OSes in use by the target organization.

Then

Use SHODAN search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters.

Then

https://www.shodan.io/

Collect Location Information

Use Google Earth tool to get the physical location of the target.

Tools for finding the geographical location:

- Google Earth
- Google Maps
- Wikimapia
- National Geographic Maps
- Yahoo Maps
- Bing Maps

People Search: Social Networking Sites/People Search Services

Social networking sites are the great source of personal and organizational information.

Information about an individual can be found at various people search websites.

The people search returns the following information about a person or organization:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residencies
- Upcoming projects and operating environment

Footprinting through Job Sites

You can gather the company's infrastructure details job postings.

Look for these:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Monitoring Target Using Alerts

Alerts are the content monitoring services that provide up-to-date information based on your preference usually via email or SMS in an automated manner.

Examples of Alert Services:

- Google Alerts - http://www.google.com/alerts
- Yahoo! Alerts - http://alerts.yahoo.com
- Twitter Alerts - https://twitter.com/alerts
- Giga Alert - http://www.gigaalert.com

Information Gathering Using Groups, Forums, and Blogs

Groups, forums, and blogs provide sensitive information about a target such as public network information, system information, personal information, etc.

Register with fake profiles in Google groups, Yahoo groups, etc. and try to join the target organization's employee groups where they share personal and company information.

Search for information by Fully Qualified Domain Name (FQDN), IP addresses, and usernames in groups, forums, and blogs

Footprint Using Advanced Google Hacking Techniques

Query String: Google hacking refers to creating complex search queries in order to extract sensitive or hidden information

Vulnerable Targets: It helps attackers to find vulnerable targets

Google Operators: It uses advanced Google search operators to locate specific strings of text within the search results.

Google Hacking

Google supports several advanced operators that help in modifying the search:

- [cache:] Displays the web pages stored in the Google cache
- [link:] Lists web pages that have links to the specified web page
- [related:] Lists web pages that are similar to a specified web page
- [info:] Presents some information that Google has about a particular web page
- [site:] Restricts the results to those websites in the given domain
- [allintitile:] Restricts the results to those websites with all of the search keywords in the title
- [intitle:] Restricts the results to documents containing the search keyword in the title
- [allinurl:] Restricts the results to those with all of the search keywords in the URL
- [inurl:] Restricts the results to documents containing the search keyword in the URL

Collect Information through Social Engineering on Social Networking Sites

Attackers use social engineering trick to gather sensitive information from social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Attackers create a fake profile on social networking sites and then use the false identity to lure the employees to give up their sensitive information.

fake id generator

Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.

Attackers collect information about employee's interests by tracking their groups and then trick the employee to reveal more information.

Website Footprinting

Website Footprinting referes to monitoring and analyzing the target organization's website for information.

- Browsing the target website may provide:
  - Software used and its version
    - Operating system used
      - Sub-directories and parameters
        - Filename, path, database field name, or query
          - Scripting platform
            - Contact details and CMS details

Use Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug, etc. to view headers that provide:

- Connection status and content-type
  - Accept-Ranges
    - Last-Modified information
      - X-Powered-By information
        - Web server in use and its version
          - Examining HTML source provide:
            - Comments in the source code
              - Contact details of web developer or admin
                - File system structure
                - Script type

Examining cookies may provide:

- Software in use and its behavior
  - Scripting platforms used

Website Footprinting using Web Spiders

Web spiders perform automated searches on the target websites and collect specified information such as employee names, email addresses, etc.

Attackers use the collected information to perform further footprinting and social engineering attacks.

GSA Email Spider: http://email.spider.gsa-online.de

Web Data Extractor: http://webextractor.com

Mirroring Entire Website

Mirroring an entire website onto the local system enables an attacker to browse website offline; it also assists in finding directory structure and other valuable information from the mirrored copy without multiple requests to web server.

Web mirroring tools allow you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer.
wget -m

HTTrack Web Site Copier: http://www.httrack.com

SurfOffline: http://www.surfoffline.com

Email Tracking Tools

eMailTrackerPro: http://www.emailtrackerpro.com

PoliteMail: http://www.politemail.com

Email Lookup - Free Email Tracker: http://www.ipaddresslocation.org

Extracting DNS Information

Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks.

DNS records provide important information about location and type of servers.

DNS Interrogation Tools:

- http://www.dnsstuff.com
- http://network-tools.com
- https://dnsdumpster.com/

Locate the Network Range

Network range information assists attackers to create a map of the target network.

Find the range of IP addresses using ARIN whois database search tool.

You can find the range of IP addresses and the subnet mask used by the target organization from Regional Internet Registry (RIR).

Network Footprinting

The first thing you want to do is discover the network range (range of ipaddresses)

If you find an IP address of a server from a company- Enter that address in

www.arin.net

Start by trying this ip

54.164.59.97

Footprinting through Social Engineering

Social engineering is an art of exploiting human behavior to extract confidential information.

Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it.

Social engineers attempt to gather:

- Credit card details and social security number
    - Usernames and passwords
        - Security products in use
            - Operating systems and software versions
                - Network layout information
                    - IP addresses and names of servers

Social engineering techniques:

- Eavesdropping
    - Shoulder surfing
        - Dumpster diving
            - Impersonation on social networking sites

Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Eavesdropping:

- Eavesdropping is unauthorized listening of conversations or reading of messages.

- It is interception of any form of communication such as audio, video, or written.

Shoulder Surfing:

- Shoulder surfing is a technique, where attackers secretly observes the target to gain critical information

- Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.

Dumpster Diving:

- Dumpster diving is looking for treasure in someone else's trash.

- It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

WHOIS Lookup

WHOIS databases are maintained by Regional Internet Registries and contain the personal information of domain owners.

WHOIS query returns:

- Domain name details
    - Contact details of domain owner
        - Domain name servers
            - NetRange
                - When a domain has been created
                    - Expiry records
                        - Records last updated

Information obtained from WHOIS database assists an attacker to:

- Gather personal information that assists to perform social engineering

Regional Internet Registries (RIRs):

- AFRINIC (African Network Information Center)
    - ARIN (American Registry for Internet Numbers)
        - APNIC (Asia Pacific Network Information Center)
            - RIPE (Reseaux IP Europeens Network Coordination Centre)
                - LACNIC (Latin American and Caribbean Network Information Center)

Footprinting Tools

Footprinting Tool: Maltego

- Maltego is a program that can be used to determine the relationships and real world links between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files.

Footprinting Tool: Recon-ng

- Recon-ng is a Web Reconnaissance framework with independent modules, database interaction, built in convenience functions, interactive help, and command completion, that provides an environment in which open source web-based reconnaissance can be conducted.

Footprinting Tool: FOCA

- FOCA(Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans.
    - Using FOCA, it is possible to undertake multiple attacks and analysis techniques such as metadata extraction, network analysis, DNS snooping, proxies search, fingerprinting, open directories search, etc.

Tracking Email Communications

Email tracking is used to monitor the delivery of emails to an intended recipient.

Attackers track emails to gather information about a target recipient in order to perform social engineering and other attacks.

Get recipient's system IP address

Geolocation of the recipient

When the email was received and read

Whether or not the recipient visited any links sent to them

Get recipient's browser and operating system information

Time spent on reading the emails

Example bogus Email

Diagnostic information for administrators:
Generating server: eex1.YearUp.org

ebently@yearup.org
Remote Server returned '550 5.1.10 RESOLVER.ADR.RecipientNotFound; Recipient not found by SMTP address lookup'

Original message headers:

Received: from eex2.YearUp.org (172.17.53.235) by eex1.YearUp.org (172.17.53.230) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.1591.10; Wed, 11 Dec 2019 14:50:03 -0800 Received: from eex2.YearUp.org ([fe80::653f:644a:fd76:ee68]) by eex2.YearUp.org ([fe80::653f:644a:fd76:ee68%3]) with mapi id 15.01.1591.017; Wed, 11 Dec 2019 16:50:03 -0600 Content-Type: application/ms-tnef; name="winmail.dat" Content-Transfer-Encoding: binary From: "Goldman, Andy" <AGoldman@YearUp.org> To: "ebently@yearup.org" <ebently@yearup.org> Subject: test Thread-Topic: test Thread-Index: AQHVsHVTeXQC9uzsTUKC5DnMza3kag== Date: Wed, 11 Dec 2019 16:50:03 -0600 Message-ID: <83ba7eb4d0fb4cb1a5f2c04e9e67abd9@YearUp.org> Accept-Language: en-US Content-Language: en-US X-MS-Has-Attach: X-MS-TNEF-Correlator: <83ba7eb4d0fb4cb1a5f2c04e9e67abd9@YearUp.org> MIME-Version: 1.0 X-Originating-IP: [38.88.246.170] Return-Path: AGoldman@YearUp.org

Gather Information from Financial Services

Financial services provide useful information about the target company such as the market value of a company's shares, company profile, competitor details, etc.

- Google Finance
- Yahoo! Finance

Information on Employees

Employees present a giant target for you later in the process

Most of this type of data is in clear sight if you look for it.

Active Footprinting vs Passive Footprinting

Active Footprinting requires the attacker to touch the device, network or resource.

Passive Footprinting refers to measures to collect information from publicly accessible resources

- For example passive footprinting may be perusing websites or looking up public records while active footprinting would be running a scan against an IP you find in the network.
    - The vast majority of footprinting is passive

Passive Footprinting

Passive footprinting as defined by the EC-Council has nothing to do with lack of effort

It actually takes more effort then active footprinting

This is called Competitive Intelligence

- It is both time consuming and legal. It is customary to do intelligence on your competitors.

Where to Start

Start with the Companies website.

Some of the open source information you can find on a company's website is:

- Company history
- Directory Listings
- Current and Future Plans
- Technical Information

Directory listings become useful in social engineering. And you'd be surprised how much technical information some companies keep on their website.

Designed to put customers at ease, sometimes sites inadvertently give hackers a leg up by giving hackers the details of the makeup of their network

Active Footprinting

Social engineering is an active footprinting method which is an active footprinting method. Social engineering methods that involve interviewing, phone calls, face to face interactions and social media are active, whereas methods that don’t involve interviewing aren’t.

Search Engines

Search engines can provide a treasure trove of information for footprinting and if used properly won’t alert anyone looking at them

Google Earth and apps like it can provide location information and depending on when the pictures were taken, can show all types of intelligence

Often personal information like residential addresses and phone numbers of employees can be found on LinkedIn.com and Pipl.com

Google Hacking

Google Hacking involves manipulating a search string with additional specific operators to search for vulnerabilities

Right Now go to www.hackersforcharity.org/ghdb/

Also try entering this string

- allinurl: tsweb/default.html

More Google Hacks

Operator. Syntax. Description

filetype. filetype:type. Searches only for files of a specific type (Doc.xls etc…)

Index of. Index of/string displays pages with directory browsing enabled. For example the following will show directory listings containing passwd

“intitle:index of” passwd

Info. Info:string. Searches for pages that contain the string in the title. For example, the following will return the pages with the word login in the title”

Intitle: login

Search google hacks to find more examples

Examples

Pirating music is illegal. Just test the link

You can use a google hack to download music

Intitle: index of Nameofsong.mp3

Intitle: index of caro.mp3

To discover open vulnerabilities on a network that were found by Nessus Scan

Intitle:nessus Scan Report IBM

Other Tools

Web Spiders

Tools such as www.news.netcraft.com and www.webmaster-a.com/link-extractor-internal.php can help you see links that webmasters may not realize are even there

SEF (Social Engineering Framework)

www.paterva.com/web5/ are open source intelligence and forensics applications designed to demonstrate social engineering weaknesses for your environment

If you want to be a security engineer I won't explain any of this anymore. You can start exploring