Module 5

Footprinting/Reconnaissance

Ansh Bhawnani

Basics of Footprinting

Module 5

Basics of Footprinting

- Used for gathering possible information about a target computer system or network
- First step of a hacking process, Information Gathering
- Can be both passive and active.
- Finding information such as:
  - Domain name
  - IP Addresses
  - Namespaces
  - Employee information
  - Phone numbers
  - E-mails
  - Job Information

Types of Footprinting

- **Passive footprinting**
  - Collecting information without interacting with the target directly
  - Used when information gathering must not be detected by the target.
  - Through search engines or public records
- **Active footprinting**
  - Collecting information by interacting with the target directly
  - There is a chance that the target becomes aware of the information gathering.
  - Probing company's assets
  - Info more accurate and rapid

Objectives of Footprinting

- **Learn security posture**: Analyze the security posture of the target, find loopholes, and create an attack plan.
- **Identify focus area**: Using different tools and techniques, narrow down the range of IP addresses.
- **Find vulnerabilities**: Use the collected information to identify weaknesses in the target's security.
- **Map the network**: Graphically represent the target's network and use it as a guide during the attack.

Objectives of Footprinting

Collecting Network Information:

- Domain name
- Internal domain names
- Network blocks
- Active IP addresses
- Rogue websites/private websites
- TCP and UDP services running
- Access control mechanisms and ACLs
- Networking protocols
- VPN points
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms

Objectives of Footprinting

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

Objectives of Footprinting

- **Collecting Organizational 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

Types of Footprinting

Module 5

1. Footprinting through Search Engines

Module 5

Footprinting through Search Engines

- **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).

Footprinting through Search Engines

- **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.
  - Google hacking is a technique which attackers use to perform a complex search using a set of search operators and building complex queries, called Google Dorks.
  - You can also use NetCraft to find restricted URL's

Footprinting through Search Engines

- **Determining the Operating System:**
  - Use the Netcraft tool to determine the OSes in use by the target organization.
  - Use SHODAN search engine that lets you find specific computers or IoT devices (routers, servers, etc.) using a variety of filters.

Footprinting through Search Engines

- **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

Footprinting through Search Engines

- **Social Networking Sites/People Search Services:**
  - 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 Search Engines

Footprinting through Job Sites:

- You can gather company's infrastructure details job postings.
- Look for these:
  - Job requirements
  - Employee's profile
  - Hardware information
  - Software information

Footprinting through Search Engines

Monitor 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

Footprinting through Search Engines

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.

2. OSINT

Module 5

OSINT

- *Open Source Intelligence* is to gather information about a target using publicly available information.
- **OSINT Sources:**
  - Social media websites like Twitter, Facebook etc. hold a lot of user data.
  - Public facing web servers: Websites that hold information about various users and organizations.
  - Newsletters and articles.
  - Code repositories: Software and code repositories like Codechef, Github hold a lot of information but we only see what we are searching for.

OSINT

Objectives:

- Identification of IP addresses, subdomains, ports and services that can increase our attack surface.
- Identification of technologies used, application platform and other infrastructure details
- Identification of sensitive information for e.g. API keys, AWS S3 buckets, leaked credentials, etc.
- Other data includes identification of Log files, Backup files, Database files, Client-side code, Javascript libraries and Configuration files

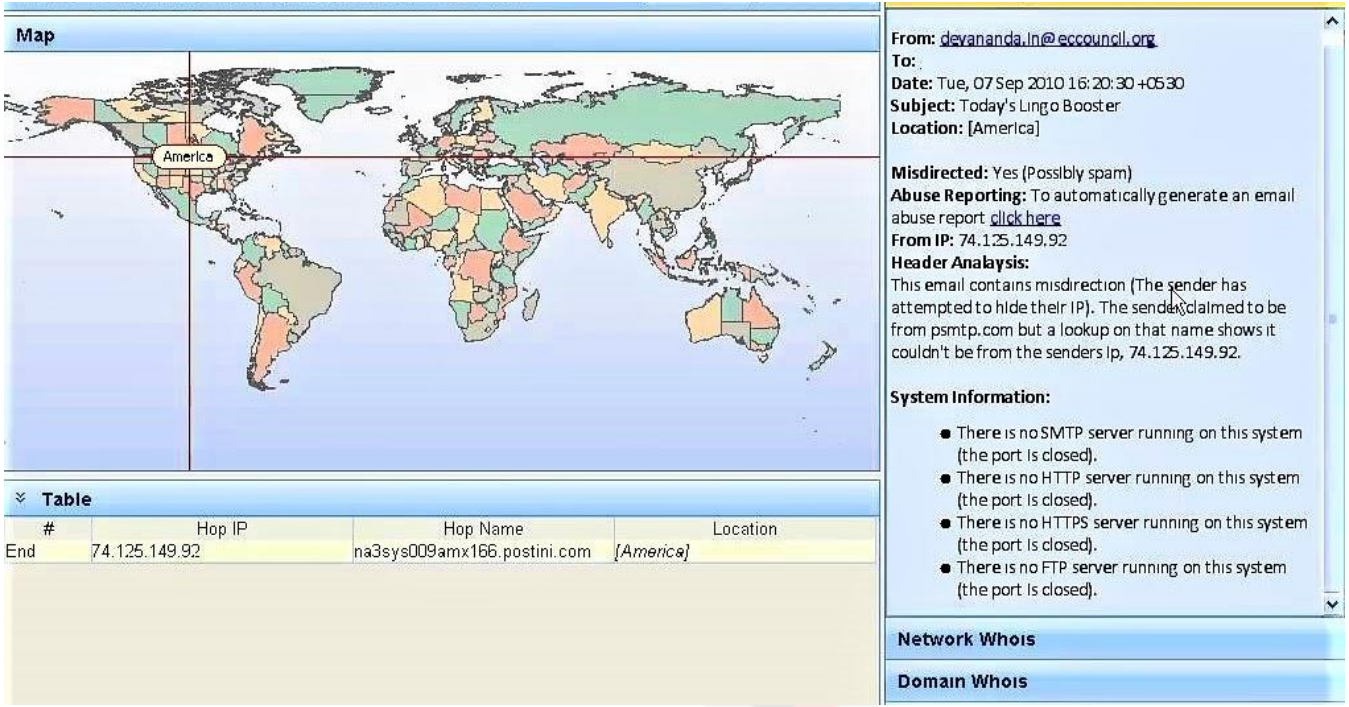
3. Email Footprinting

Module 5

Email Footprinting

- **Tracing Email Communications:**
  - Sender's Email
  - Sender's Name
  - Sender's Physical Location
  - Path through which email travelled
  - Sender's IP Address
  - Active Ports of sender

Email Footprinting



Email Footprinting

```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7cs[redacted]
        Sat, 1 Jun 2013 21:24:01 -0700 ([redacted])
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted] designates 10.224.205.137 as permitted
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; sp[redacted] in of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.mail[redacted]com; dkim=pass
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
        by 10.224.205.137 with SMTP id fq9mr8578570qab.39.1[redacted]ps = 1);
        Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:in-reply-to:referenc[redacted]bject:from:to
         :content-type;
        bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1[redacted]
        b=KguZLTLfg2+QZXzZKex1NnvRcnD/+P4+Nk5NKSPtG7uHXDsfv/hGH46e2P+75MxDR8
         blPK3eJ3Uf/CsaBZWDIT0XLaK0AGrP3BOt92MCZFxeUUQ9uwL/xHALSnkeUIEEeKGqOC
         oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqtlfP
         ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNGslKxcO7xQjeZuw+HWK/vR6xChDJapZ4
         K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuPl6yS/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
         /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9m[redacted]1040318;
 Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Sat, [redacted]700 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber[redacted]@mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4Ber[redacted]2MtV0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAMSvoXT0qEjnFW8WJdSzQhNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ::: [redacted] OLUTIONS :::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]an@gmail.com,
        [redacted]OLUTIONS <[redacted]tions@gm[redacted]ed <[redacted]_er@yahoo.com>,
```

The address from which the message was sent

Sender's IP address

Sender's mail server

Date and time received by the originator's email servers

Authentication system used by sender's mail server

Date and time of message sent

A unique number assigned by mr.google.com to identify the message

Sender's full name

Email Footprinting

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
- Whether or not the recipient visited any links sent to them
- Get recipient's browser and operating system information
- When the email was received and read

4. Website Footprinting

Module 5

Website Footprinting

- Website Footprinting refers 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

Website Footprinting

- **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

Website Footprinting

- **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
- **Website Footprinting using Web Spiders:**
  - Web spiders perform automated searches on the target websites

Website Footprinting

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.

5. Footprinting Using Google

Module 5

Footprinting Using Google

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.

Footprinting Using Google

Google Advance Search Operators

- [**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
- [**intitle:**] Restricts the results to documents containing the search keyword in the title
- [**allintitle:**] Restricts the results to those websites with all of the search keywords in the title
- [**inurl:**] Restricts the results to documents containing the search keyword in the URL

6. Competitive Intelligence

Module 5

Competitive Intelligence

Competitive Intelligence Gathering

- Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet.
- Competitive intelligence is non-interfering and subtle in nature.
- Essential part of your business marketing research plan for striving in the market and staying ahead of your rivals

Competitive Intelligence

Sources of Competitive Intelligence

- Company websites and employment ads
- Search engines, Internet, and online DB
- Press releases and annual reports
- Trade journals, conferences, and newspaper
- Social engineering employees
- Product catalogues and retail outlets
- Analyst and regulatory reports
- Customer and vendor interviews
- Agents, distributors, and suppliers

Competitive Intelligence

- **Monitoring Website Traffic of Target Company**
  - Attacker uses website traffic monitoring tools
  - Total Visitors, page views, bounce rate, live visitor map, site ranking
- **What Are the Company's Plans?**
- **When Did this Company Begin? How Did it Develop?**
  - When did it begin?
  - How did it develop?
  - Where is it located?
  - Who leads it?

Competitive Intelligence

Tracking Online Reputation of the Target

- Track company's online reputation
- Collect company's search engine ranking information
- Obtain email notifications when a company is mentioned online
- Track conversations
- Obtain social news about the target organization

7. DNS Footprinting

Module 5

whois

- WHOIS databases is managed by Regional Internet Registries and is a listing of all registered domains and contain the personal information of domain owners.
- Managed by International Corporation for Assigned Names and Numbers (ICANN)
- Protects domain registrants by prohibiting the use of WHOIS listings for marketing or spam purposes
- Poses a security risk on personal information when not properly configured

whois

- **WHOIS query returns**:
  - Domain name details
  - Contact details of domain owner, email and phone number
  - Domain name servers
  - When a domain has been created
  - Expiry records
  - Records last updated

whois

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

DNS Footprinting

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.
- Know about the network blocks those IP addresses belong to and other servers that may be in those network blocks

DNS Footprinting

Record	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

8. Network Footprinting

Module 5

Network Footprinting

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).

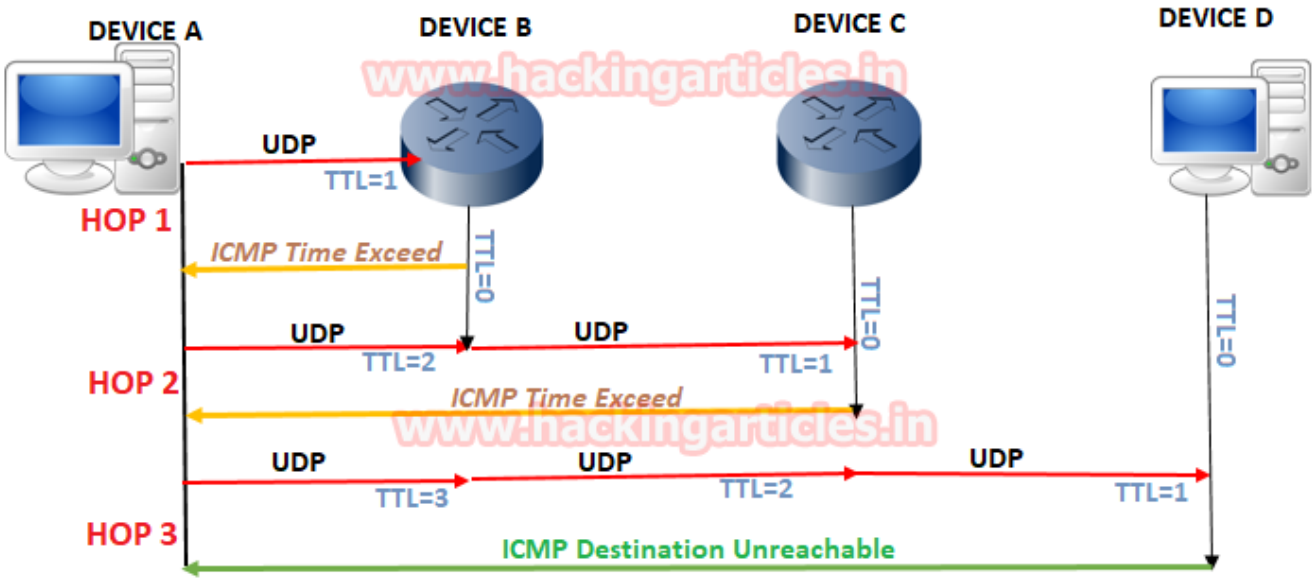
Network Footprinting

Network Footprinting Information:

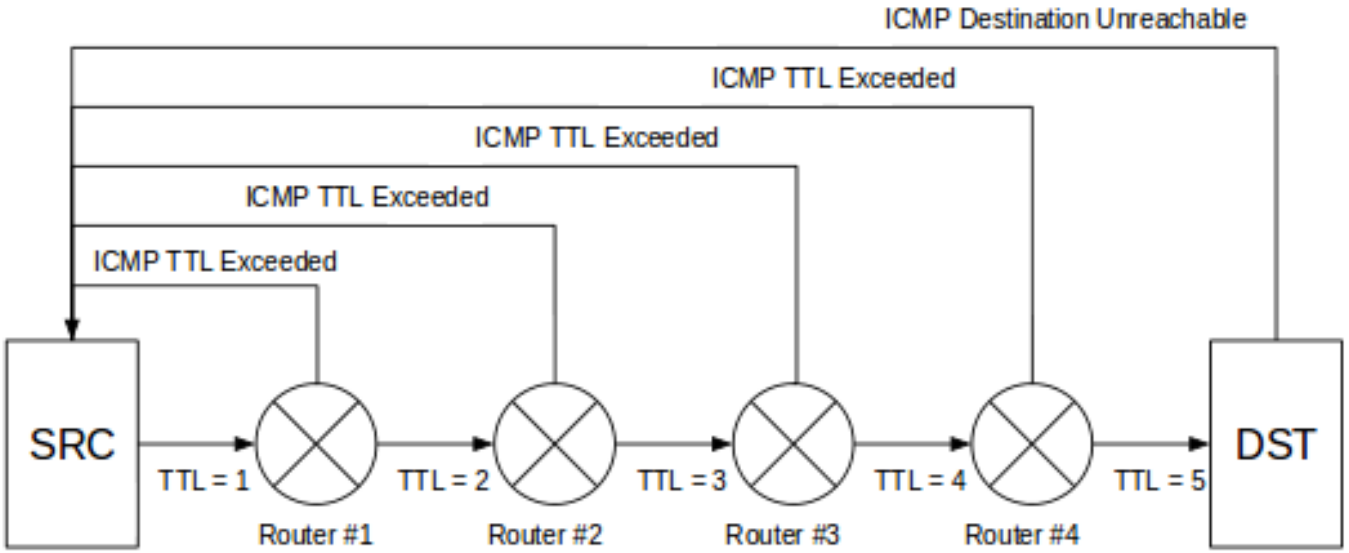
- Network address ranges
- Host names
- Exposed hosts
- Applications exposed on those hosts
- Operating System and application version information
- Patch state of the host and the applications
- Structure of the applications and back-end severs
- Implementation details the sys admin posted to newsgroups or told a reporter about

Network Footprinting

Working of Traceroute



Network Footprinting



Network Footprinting

Traceroute Analysis:

Hop #	RTT 1	RTT 2	RTT 3	Name/IP Address
10	81 ms	74 ms	74 ms	205.134.225.38

Network Footprinting

Traceroute Analysis:

```
C:\Users\anshb>tracert bitten.tech

Tracing route to bitten.tech [104.28.31.26]
over a maximum of 30 hops:

  1     3 ms    <1 ms    <1 ms  192.168.1.1
  2    82 ms    57 ms    56 ms  abts-mp-dynamic-001.224.70.182.airtelbroadband.in [182.70.224.1]
  3    55 ms    57 ms    54 ms  125.21.0.105
  4   120 ms   122 ms   116 ms  182.79.146.196
  5   117 ms   115 ms   117 ms  13335.sgw.equinix.com [27.111.228.132]
  6   117 ms   117 ms   116 ms  104.28.31.26

Trace complete.
```

9. Footprinting with Social Engineering

Module 5

Footprinting with 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.

Footprinting with Social Engineering

- **Social engineers attempt to gather**:
  - **Eavesdropping**:
    - Unauthorized listening of conversations or reading of messages.
    - It is interception of any form of communication such as audio, video, or written.

Footprinting with Social Engineering

Footprinting with Social Engineering

Footprinting with Social Engineering

- **Social engineers attempt to gather**:
  - **Shoulder surfing:**
    - 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.

Footprinting with Social Engineering

Footprinting with Social Engineering

- **Social engineers attempt to gather**:
  - **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.

Footprinting with Social Engineering

- **Social engineering techniques**:
  - Credit card details and social security number
  - User names and passwords
  - Security products in use
  - Operating systems and software versions
  - Network layout information
  - IP addresses and names of servers

Footprinting Countermeasures

Module 5

Footprinting Countermeasures

- Restrict the employees to access social networking sites from organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogues, etc.
- Limit the amount of information that you are publishing on the website/Internet

Footprinting Countermeasures

- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services
- Enforce security policies to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
- Disable directory listings in the web servers

Footprinting Countermeasures

- Educate employees about various social engineering tricks and risks
- Opt for privacy services on Whois Lookup database
- Avoid domain-level cross-linking for the critical assets
- Encrypt and password protect sensitive information
- Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns

HACKING

Is an art, practised through a creative mind.