Ethical Hacking

Session 2

Footprinting

Learning Objective

1. Define and describe footprinting methodology
2. Explain the objectives and the types of footprinting
3. Define and describe information gathering
4. List the footprinting tools
5. Describe Competitive Intelligence Gathering

Footprinting Methodology

Footprinting methodology:

- Is a methodology of gathering information of computer network and systems with the help of various computer security techniques.

- Helps to evaluate the IT infrastructure, network devices and information and plan ethical hacking of an IT business.

What is Footprinting? 1-5

Footprinting:

- Is a process of preparing a plan or map of networks and systems of an organisation.
- Also, provides information about the Internet, intranet, wireless and extranet systems that are part of network system.
- Is a process that starts by determining the scope of the system, device or application to gather information.

  After deciding the location, the non-intrusive methods can be used to gather the specific information.

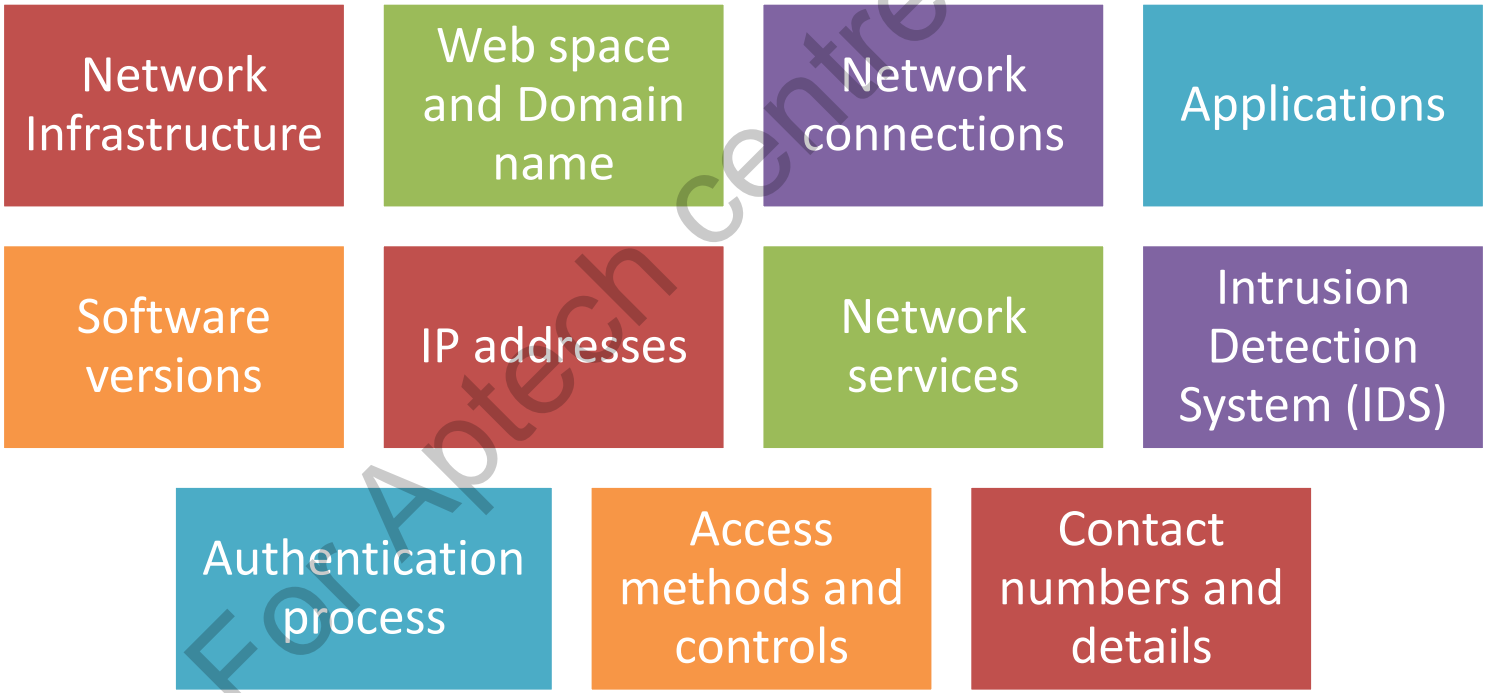
What is Footprinting? 2-5

- For example:
  - In order to carry out social-engineering attack, a hacker can use social networking Websites such as facebook.com or linkedin.com.
  - Hacker gets information about any person working in a company through this.

- During the footprinting phase, a hacker aims:
  - To search the information of network structure, system devices attached with the network, the type of data, data stored location, server details and so on.
  - To expose the information of system, application and version that are used in the systems to launch an effective attack on the target.

What is Footprinting? 3-5

- Examples of information which the hacker can gather at the primary step of footprinting are as follows:



What is Footprinting? 4-5

- After collecting the information, a hacker gets the knowledge of organisation's network structure.
- It helps the hacker to understand the location where the valuable information is stored.
- Thus, the hacker can plan to access the information from the system and the network of organisation.

What is Footprinting? 5-5

- Footprinting also:
  - Helps hacker to collect the information regarding a target without the help of aggressive reconnaissance techniques.
  - Helps hacker to collect and reuse valuable data without informing the target.
  - Provides useful data to the hacker to process it in other stages of hacking.

Objectives of Footprinting 1-2

- The most important objectives of footprinting include gathering following information of the target company:
  - Network information
  - System information
  - Organisational information

Objectives of Footprinting 2-2

- The objectives of footprinting are as follows:

For collecting network information	For collecting system information	For collecting organisational information
• Domain name • Internal domain names • Network blocks • IP addresses of the reachable systems • Rogue Website/Private Websites • TCP and UDP services running • Network protocols • VPN Points • ACLs • IDS running • Authentication mechanisms	• User and group names • System banners • Routing tables • SNMP information • System architecture • Remote system type • System names • Passwords	• Employee details • Organisational Website • Company directory • Address and phone numbers • Background of the organisation • News articles/press releases

Types of Footprinting

- Types of footprinting are:

Passive Footprinting

- Non-intrusive techniques help gather information about the target.
- Non-intrusive techniques gather information from the other sources.
- For example: Gathering information about a target organisation from Google cached pages is passive footprinting.

Active Footprinting

- Intrusive techniques (getting information directly from the target) help gather the required information.
- Information is gathered by directly accessing the target Website of the company.

Information Gathering 1-4

- There are many methods to gather the information, based on the target.
- Information gathering is an important phase in the hacking process.
- Some reconnaissance methodologies can help a hacker to obtain important information.

Information Gathering 2-4

- The two important phases in information gathering are:
  - footprinting
  - Scanning
- Footprinting method helps a hacker to gather maximum information.
- This gathered information can be accomplished by visiting:
  - Organisations Websites
  - Business papers
  - Economical database and so on

Information Gathering 3-4

- Seven stages in information gathering are:

1. Gathering initial information
2. Locating the network range
3. Recognizing active machines
4. Locate open ports/access points/applications
5. Finding operating systems
6. Fingerprinting services
7. Mapping the network source

Information Gathering 4-4

- In the footprinting stage, hackers:
  - Uncover some initial information and locate the network range.
  - Determine the active machines in the network and find the open ports and access points.
  - Detect the operating system and expose the services on the ports.
  - Map the networks in the organisation that help collect the overall information.

Google's Search Capability 1-6

- A hacker can search information manually, with the help of search engines such as Yahoo, Google, Bing and so on.
- Google:
  - Is one of the most widely used search engines on the Internet all over the world and is owned by Google Inc.
  - Helps its users by providing many keywords and more than 40 options to search with it's search features.
  - Displays the result page against the query search to its users.
  - Shows its features by Search Engine Optimization (SEO) pattern and patents. SEO helps users to increase ranking of their Web pages.

Google's Search Capability 2-6

- Google has developed various services along with its word search capability such as:
  - Weather forecasts
  - Market data
  - Synonym search
  - Time zones
  - Stock information
  - Book search
  - Earthquake information
  - Movie show times
  - Airports information
  - Sports scores
  - Public data

Google's Search Capability 3-6

- Some special features for numbers such as:
  - General calculations (3*4+sqrt(6)-pi/2)
  - Prices
  - Money/Unit conversions (10.5 cm in inches)
  - Area codes
  - Package tracking
  - Temperatures (50 Fahrenheit in Celsius)
  - Patents
  - language change options and so on

Google's Search Capability 4-6

- The users of Google Search gets more than 15 options to modify their searches and they areas follows:
  - Exclusion ('-xx')
  - Inclusion ('+xx')
  - Alternatives ('xx OR yy')
  - Wildcard matching ('*')

Google's Search Capability 5-6

The advantages of using Google to gather information are as follows:

- It shows only the information that is related with the search words.
- It searches location-wise information.
- It displays the search links with summarised content for each result.
- It keeps Web pages in the cache.

Google's Search Capability 6-6

- Hackers:
  - Use Google to gather preliminary information and find security loopholes.
  - Use Google search to gather information which is also called Google hacking.
  - Uses commands such as site, filetype, link, cache, intitle and inurl.
  - Search information from blogs, newsgroups and press notes.
  - May search some more information about system technologies, e-mail addresses, IP addresses, operating system and hardware used in the system and the network.
  - May also use advanced operators in Google to search specific links of the text in the search result.

Footprinting Tools 1-2

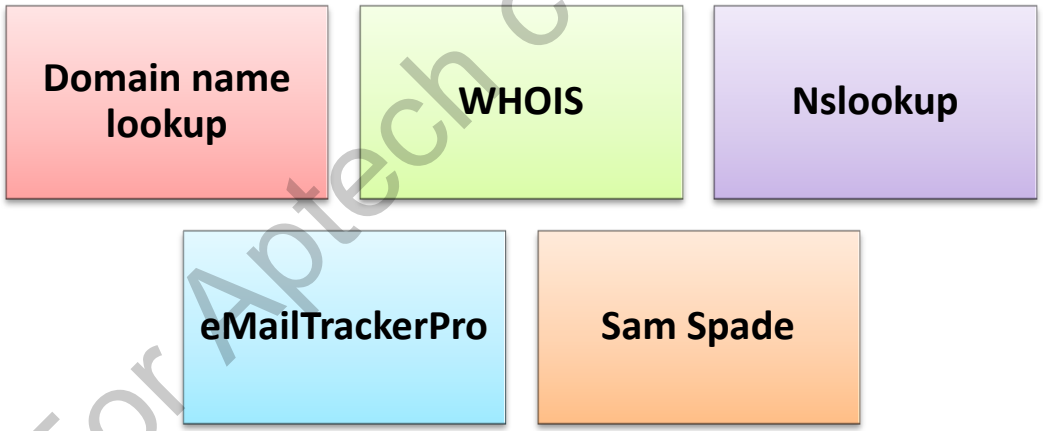
In footprinting, hackers:

- Locate information with the help of some hacking tools, applications or Websites.
- 'Footprint' the target or collect some important information.
- Can avoid the tools that are not suitable for hacking the specific network or systems.
- For example:

  If some specific Windows-based software is being used in an IT organisation, a hacker can avoid all the Windows-based hacking applications and use the suitable ones.

Footprinting Tools 2-2

- Footprinting not only indentifies the unwanted tools, but also increases the speed of the hacking process.
- Following are the tools used for footprinting and information gathering:



WHOIS 1-8

- WHOIS is a search tool that helps users to check registered domain names.
- To register a domain name of a business Website or portal, the Internet Corporation for Assigned Names and Numbers (ICANN) stores submitted personal contact information in the WHOIS database.
- After listing the domain name in the online directory, it will be publically available and anyone can search the registered domain name on the WHOIS tool.

WHOIS 2-8

- People search for the domain names in the WHOIS database for:
  - Checking expiration dates by the individuals
  - Transferring ownership by the registrars
  - Investigating criminal activity by authorities

- Network solutions should be in accordance with the requirements of WHOIS database determined by ICANN as an accredited domain names registrar.

WHOIS 3-8

- The network solution provides three options for WHOIS database listing, ensuring the customer's comfort to display their personal information and they are as follows:
  - **Public WHOIS Database Listing**
  - **Private WHOIS Database Listing**
  - **Enhanced Business Listing in WHOIS Database**

WHOIS 4-8

- **Public WHOIS Database Listing:**
  - Network solutions will provide public listing to the WHOIS database when a customer is comfortable with showing his information to the public listing and wants to avoid an extra fee towards private domain registration.
  - The Public WHOIS Database Listing includes:

WHOIS 5-8

- **Private WHOIS Database Listing:**
  - In public listing, personal information may be at the risk of hackers, data miners and spammers.
  - In this case, Network solutions offer private domain name registration to keep the customer's information safe.
  - Network solutions charge small amount fee and act as a proxy.
  - When the hackers look for a personal information and domain name registration, they will get the domain name information of the hosting company. The customer's information will be safe.

WHOIS 6-8

- **Enhanced Business Listing in WHOIS Database:**
  - Network Solutions also provides online business solutions for small scale businesses. Companies can get benefits by registering their advertisements in the WHOIS database.
  - More than 30 to 40 million people check their business domain names in the WHOIS database in a month and drive traffic to their businesses.
  - The customers can enhance their business listing by providing some more details pertaining to their business and they are as follows:

WHOIS 7-8

- Network Solutions provide various facilities to their customers by providing various options, where customers need to decide which service options they need for their businesses.

- The Internet Corporation for Assigned Names and Numbers (ICANN) ensures that one user should use only one specific domain name.

WHOIS 8-8

- **WHOIS:**
  - Is now available across various operating systems, hacking toolkits and on the Internet.
  - Was developed from the Unix operating system. WHOIS identifies registered domain names users.
  - Helps search the domain registration details of an individual or organisation.

Nslookup 1-2

- **Nslookup:**
  - Is a network administration command-line tool which tests and troubleshoots DNS servers. A hacker can install this tool along with the TCP/IP protocol by using Control Panel.
  - Helps the computer operating system to query the Domain Name System (DNS) in order to obtain the following:
    - Domain name
    - IP address mapping
    - Specific DNS record
- Does not use the DNS of the operating system's local DNS resolver library to perform its queries, but performs different actions to dig the details.

Nslookup 2-2

- To use Nslookup.exe:
  - install the TCP/IP protocol on the computer.
  - Specify a single DNS server while running the IPCONFIG/ALL command through a command prompt window.
- Nslookup.exe runs:

Interactive mode

- To run Nslookup.exe in interactive mode, type **nslookup** in the command prompt.

```
C:\> nslookup Default Server:
nameserver1.domain.comAddress:
10.0.0.1>
```

Non-interactive mode

- To return a piece of data, use non-interactive mode. The syntax for non-interactive mode is as follows:

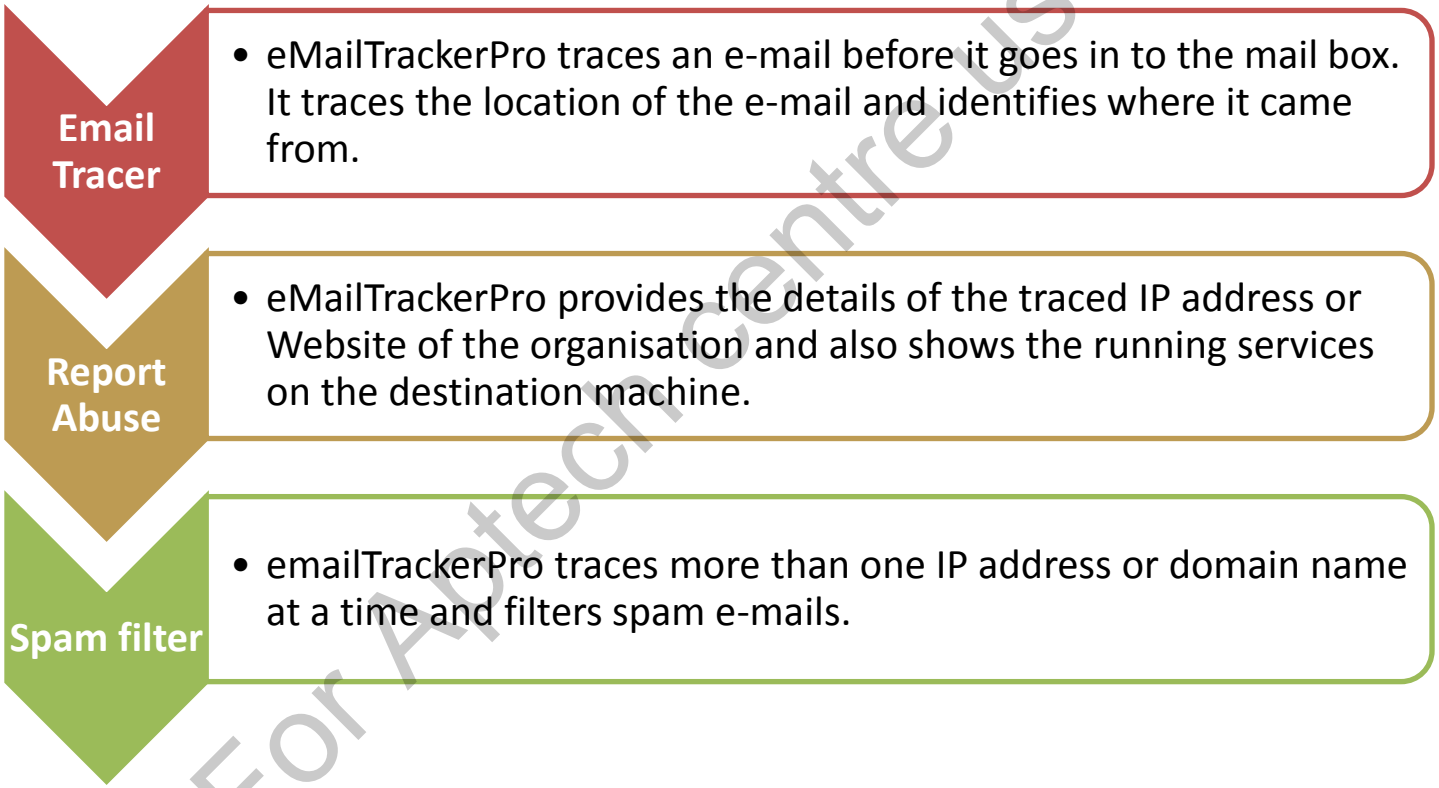
```
nslookup [-option] [hostname]
[server]
```

eMailTrackerPro 1-2

- **eMailTrackerPro**:
  - Is an e-mail tracer and spam filter tool. Spam is a nuisance and 97% e-mails received are spam.
  - Is usually harmless, but can sometimes contain viruses or tricky e-mails that will ask for personal details such as name, address, bank details and so on that leads to fraud.
  - Offers a spam filter, which scans each e-mail that is received and warns the user if there is any danger.
  - Has the ability to trace an e-mail using the e-mail header that stops spam e-mail before it reaches to the mail box.

eMailTrackerPro 2-2

- Following are the features of eMailTrackerPro tool:



ARIN 1-3

- **American Registry for Internet Numbers (ARIN)**:
  - Is the regional registry for Canada, the United States and many Caribbean and North Atlantic islands.
  - Is used as a Web based tool for information gathering such as WHOIS.
  - Provides services related to technical coordination and management of Internet number resources and distributes Internet number resources including IPv4 and IPv6 address space and AS numbers.
  - ARIN is also a database that includes static IP addresses and this database can be queried by using the WHOIS tool.
  - WHOIS search is available on ARIN Website, which searches the ARIN's database for any particular query.

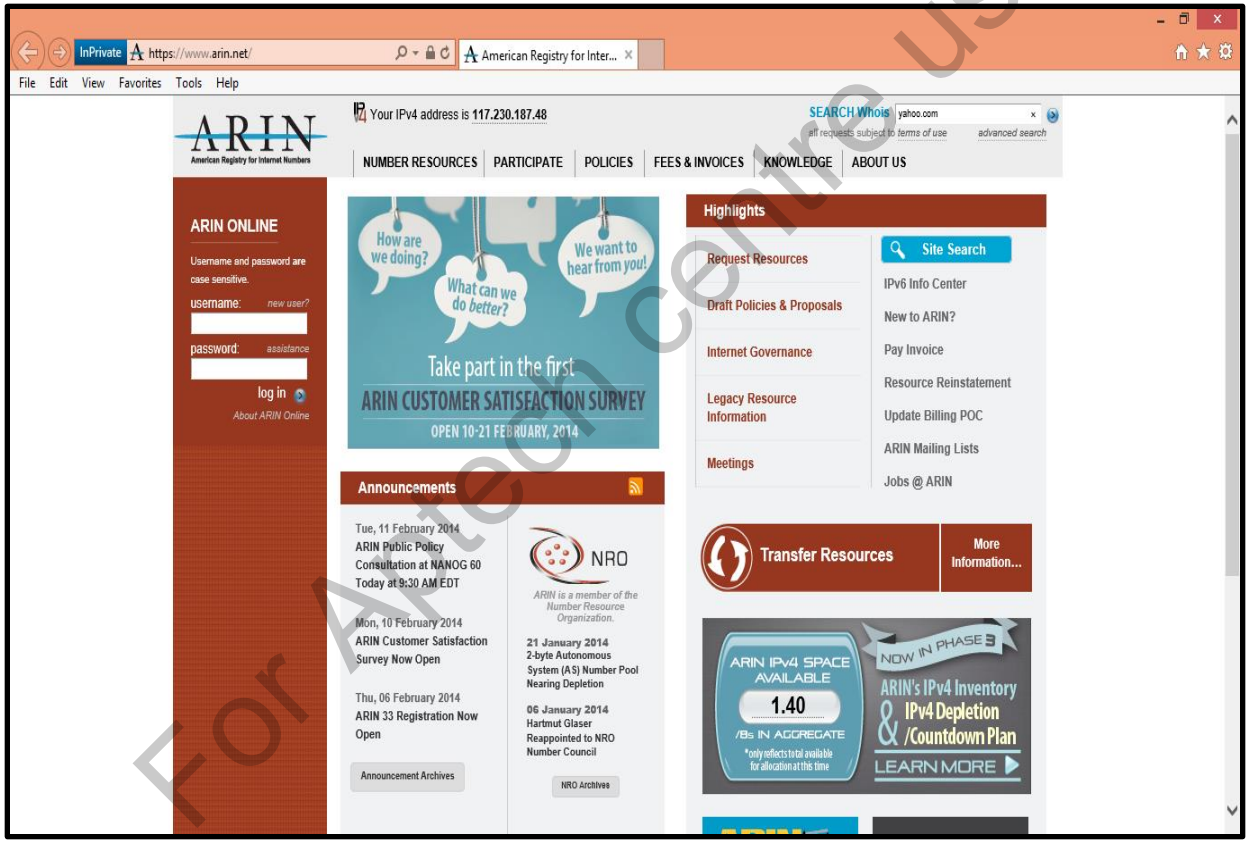
ARIN 2-3

- ARIN provides three types of services:

- An ethical hacker uses the ARIN WHOIS information to know the customer details, IP addresses and so on.
- A malicious hacker may use this ARIN information to attack the system of the organisation.
- Domain owners should be aware of these malicious hackers and keep the ARIN database safe.

ARIN 3-3

- The ARIN Web interface is shown in the figure:



Competitive Intelligence Gathering 1-2

- Competitive intelligence can be defined:

  "As information regarding competitor businesses' services and products, their marketing strategies and imparted technologies in their organisations."

- Competitive Intelligence Gathering:
  - Is a process to collect and analyse the information of competitor's products, services, administration and many aspects of the organisation.
  - Is also used to perform product or service comparisons between businesses and to know strategies of product and service positioning of the competitor.

Competitive Intelligence Gathering 2-2

- Ethical hackers can use Competitive Intelligence to analyse the gathered information and secure it for the organisation.

- Following are the online tools used for competitive intelligence gathering for the target Website:
  - SpyFu
  - KeywordSpy

- Both these tools give keywords for the Websites and are easy to use and the information gathering process cannot be detected by the potential target.

Countermeasures 1-3

- Identify and understand the type of the attacks before determining the countermeasures.
- Following are the practices of the countermeasures:
  - Configure routers such that they deny footprinting requests.
  - Configure Web servers to disable false protocols and stop information leakage.
  - Configure ‘fw config’ and lock the ports.
  - Configure IDS to avoid apprehensive traffic and pick up footprinting patterns.
  - Validate personal information before putting it on the Website.
  - Remove important information from the Website while footprinting again.
  - Restrict or avoid search engines from accessing a Web page.

Countermeasures 2-3

- Uses split-DNS and disable directory listing
- Installs patches on a daily or weekly basis
- Stops unwanted services and ports
- Changes passwords constantly using uppercase/lowercase/numbers/special characters
- Restricts physical and unofficial access of the systems
- Restrains unexpected inputs
- Takes backups and system checks regularly
- Educates employees about future attacks and risks
- Develops preventive strategies to avoid attacks
- Encrypts password protected data and keeps multiple copies on different systems
- Installs and performs security checks

Countermeasures 3-3

- Use Firewalls and intrusion detection systems to alarm the risks
- Develop and circulate the written security policy within the organisation

Summary 1-4

- Footprinting is a methodology of gathering information of computer network and systems with the help of various computer security techniques.
- Footprinting is also known as an information gathering process that helps gather system and network information.
- During the footprinting phase, a hacker aims to search the information of network structure, system devices attached with the network, the type of data, data stored location, server details and so on.
- Footprinting is about information gathering and there are many methods to gather the information, based on the target.

Summary 2-4

- Google search features helps its users by providing many keywords and more than 40 options to search.
- The Google search features has some special features for numbers such as general calculations (3*4+sqrt(6)-pi/2), prices, money/unit conversions (10.5 cm in inches) and so on.
- Domain name lookup, WHOIS, Nslookup, Sam Spade and eMailTrackerPro are some important tools used for footprinting and information gathering.
- WHOIS is a search tool that helps users to check the registered domain names.

Summary 3-4

- The Nslookup.exe runs in an interactive mode or in non-interactive mode.
- eMailTrackerPro is an e-mail tracer and spam filter tool. Spam is a nuisance and 97% e-mails received are spam.
- American Registry for Internet Numbers (ARIN) is the regional American Registry.
- ARIN provides three types of services: Registration, Organisation and Policy Development.
- 'Competitive intelligence' is information of the competitors' products, marketing and technologies.

Summary 4-4

- Competitive intelligence gathering is a method used for product or service comparisons between the two same businesses and to know strategies of product and service positioning of the competitors.
- SpyFu and KeywordSpy are the online tools used for competitive intelligence gathering for the target Website.
- To gather competitive intelligence, the EDGAR database is also used as a tool.
- It is important to identify and understand the type of attacks before determining the countermeasures.