## Aim

To elaborate on the meaning and nature of ethical hacking and the various concepts of ethical hacking

## Instructional Objectives

After completing this chapter, you should be able to:

- Explain the scope and concept of ethical hacking
- List the skills required for an ethical hacker
- Explain the various types of penetration testing
- Describe the various steps of ethical hacking
- Outline the steps involved in footprinting
- Explain the process of scanning

## Learning Outcomes

At the end of this chapter, you are expected to:

- Define ethical hacking
- Describe the scope of ethical hacking in the Information Security domain
- Apply the most appropriate type of penetration testing to a system, in order to gather information
- Outline the steps to develop a footprint of an organisation's network and systems

## 1.1.1 Introduction

In the world of information security professionals, ethical hackers, still remain a mystery to most of us who are interested in perceiving a career in the world of IT security. All we understand and interpret in a broad sense is that ethical hackers help individuals and organizations in analysing the security strategies of their services or products by conducting a detailed study about the vulnerabilities that exist in the system and anticipating attacks by hackers.

But how exactly do they do this? What are the tools and techniques used by ethical hackers? How do they report their findings to present before their client? And, most importantly, how can one become an ethical hacker? This chapter is your chance to find out the answers to all these questions.

### (i) Hacktivism

Hacktivism may be defined as *'The Act of Hacking', by individuals who are called 'hackers',* who gain unauthorised access to any computer system. If we look at the history of hacking or hackers, we realise that it did not start as an act to cause damage or loss to an individual or an organization. A hacker was someone who had the natural instincts and the curiosity to learn as much as possible about computer systems. By 'hacking' into a computer system, the intention of the hacker was merely to develop or improve the software in order to enhance the performance of said software.

Organizations are baffled with the kind of threats that they might face and are imposed with the daunting task of protecting their information system. At one point, a firewall or intrusion detection system took care of these threats. The rising complexities and the mammoth infrastructure demands precise security steps to be executed by a specialist, which will predict any kind of possible attack in any form or magnitude and protect the organisation.

### (ii) Definition of Ethical Hacking

Ethical Hacking may be defined as the *"Process of gaining authorized access in to an Information System of an Organization or individual, in order to identify and evaluate the possible threats to it".*

An ethical hacker is an information security professional who will use his knowledge and skills to evaluate the security of a system to protect it from possible attacks by a hacker.

Simply put, an ethical hacker is "*a hacker with no harmful intentions but someone who has been enlisted with the responsibility of safeguarding information system*". An ethical hacker will always work in a real-time environment - the outcome of such a process is not only applicable today, but also in the future.

## (iii) History of Hacking

If we look at the history of hacking or hackers, we realise that it did not start as an act to cause damage or loss to an individual or an organization. A hacker was someone who was interested in learning about the nitty-gritties of a computer system. By 'hacking' into a computer system, the intention of a hacker was merely to develop or improve the software to enhance it's the performance.

Over the years, we witnessed variations in the definitions of hackers and crackers, as they started using offensive skills to wage attacks on computer systems. Let us look at some of the most famous hackers and what they did:

- Kevin Mitnick was described by US Department of Justice as the "*most wanted computer criminal in the United States history*", hacked into the network of the Digital Equipment Corporation and the National Defence Warning System; he also stole corporate secrets.

- Jonathan James made headlines as he was still a minor when he successfully hacked into the network of giant organizations in the US such as Bell South, Miami-Dade, the US Department of Defence and NASA.

- Albert Gonzaleez was the leader of the Shadow Crew, a hacking outfit. The group was involved in hacking credit and ATM cards and even passport fraud; they also used health insurance cards and birth certificates to commit identity theft.

- Kevin Poulsen had incredible knowledge about the telephone system, which he used to gain access into a radio station's phone lines. After declaring himself as a winning caller, he got a Porsche. He also hacked into various US federal systems.

**Some incidents of hacking that made headlines around the world have been listed below for your knowledge:**

- **1960s** – Students of MIT hacked into main frame computer systems using space war game for the purpose of learning more about mainframe computing systems.

Around the same time, John Drapers and others invented what was called a 'blue box' that generated frequencies that could be used for making long distance phone calls, for free.

- **1980s** – Birth of hacking clubs.
- **1982** – Members of a hacking club called the 414 Gang hacked into the medical records of a local hospital.
- **1986** – Attack on the US classified computer systems by hackers from the Chaos Computer Club.
- **1988** – Robert Tappan Morris who was a student at Cornell University, wrote a program that resulted in the Morris Internet worm, causing a Denial of Service attack on a large scale on the internet.
- **1990** – Hacking spree by Kevin Poulson. In 1990 the station ran the "Win a Porsche by Friday" contest, with a $50,000 Porsche given to the 102nd caller. Kevin and his associates, stationed at their computers, seized control of the station's 25 telephone lines, blocking out all calls but their own. Then he dialed the 102nd call - and later collected his Porsche 944.
- **1995** – Kevin Mitnick was arrested for multiple hacking activities.
- **1995** – Vladimir Levin, a Russian hacker carried out electronic transfers of huge amounts of up to 10 million that led to the international robbery over a network.
- **2000** – Yahoo!, Amazon.com and ZDNet suffered from hacking attacks.
- **2000** – The internal network at Microsoft was hacked.

**The scope of an ethical hacker has been outlined below:**

- An ethical hacker tries to impersonate the intent and actions of a hacker but without causing any damages to the information system.
- An ethical hacker operates with legal permissions obtained by the organization or the individual they are working for.

- The job description of an ethical hacker is to look for information sought by a hacker, to study the possible ways a hacker may access a system and ways to cover a hacker's track without being noticed.

- To perform with precision, an ethical hacker looks for information about the information system such as network layout, physical security, users, databases and software.

## Self-assessment Questions

1) A person who gains access to information via communication systems such as credit card information, attack PBXs or is able to make calls free of cost illegally, is called a/an

   a) Hacker
   b) Ethical hacker
   c) Whacker
   d) Phreaker

2) A nation is said to be under ________________if there has been a major attack on the infrastructure of a nation such as on financial centres, transport hubs or power plants.

   a) Threat
   b) A virus attack
   c) Cyber terrorism
   d) Hacktivism

3) What is the definition of Steganography

   a) Attacking computer systems with an intention to weaken the economic or military strength of a nation.
   b) The practice of concealing messages or information within other non-secret text or data.
   c) Operating in a double blind environment to ethically hack into an organization.
   d) The study of technology and the tools required to be an expert ethical hacker

4) A computer system or a software that goes through a security evaluation is called a

   a) Target
   b) Security threat
   c) Risk
   d) Target of evaluation

## 1.1.2 Skills Required for an Ethical Hacker

- In any organization, one may find computers with different types of operating systems such as Windows, Unix, Linux or Macintosh. Hence, an ethical hacker must be acquainted with the various features and operations of any OS.

- Good knowledge in computer networking.

- Familiarity with various types of hardware and devices.

- Sound knowledge in the information security domain with hands-on experience in administering security measures on a computer or in a network.

## 1.1.3 Important Terms used in Ethical Hacking

Let us now look at some of the important terms we often come across in ethical hacking, along with their meanings. These words also form the foundation for information security.

1. **Confidentiality:** Non-disclosure of information to either unauthorised persons or processes.

2. **Integrity:** To make sure that data or information is real, accurate and safe from the reach of unauthorised users.

3. **Availability:** Availability is important for security systems from hackers, for ensuring the authorised persons that they are provided with uninterrupted and timely access to the data.

**Note:** These three terms form what is called as the **CIA triad.**

**Other terms that are applicable to information security and the hacking world are:**

1. **Threat:** An activity or occurrence that is capable of causing potential damage to information systems or networks.

2. **Vulnerability:** A weak point or a loophole which turns out to be an entry point for a threat to enter and exploit the system. Vulnerabilities can be found in operating systems, programs, networks or hardware.

3. **Risk:** The probability of a possible threat becoming successful.

4. **Attack:** The very result of a threat which has materialised.

5. **Exploit:** Using the vulnerability of a system or a network so that it is open to attacks.

## Self-assessment Questions

5) If confidentiality and integrity constitute of two factors in a CIA triad, ________________is the third.

   a) Accessibility  b) Authentication

   c) Availability  d) Authorisation

6) The term used for the protection of an individual's information that is identifiable is called ____________________.

   a) Identification  b) Privacy

   c) Authentication  d) Evaluation

7) The weakness within the system that attracts the attention of a hacker for a possible attack is called a

   a) Virus  b) Worm

   c) Trojan  d) Vulnerability

8) Two reconnaissance methods in hacking are

   a) Proactive and reactive  b) Open and close

   c) Active and passive  d) Black box and white box

## 1.1.4 Security Testing

In the section about CIA triad, we have learnt the definition and importance of significant words. In order to test an information security system for these traits, one has to conduct a thorough examination of the system, studying various parameters and exposing vulnerabilities. The findings from such a report is very useful in building a secure system. This type of investigation is called security testing.

### (i) Definition

Security testing may be defined as *"a process that is used to determine that the security features of a system are implemented as par design"*.

**It consists of the following:**

1. **Hands-on Functional Testing:** This is done on behalf of the actual user, who intends to use the product or service being tested for what it is actually used for. This means, that the tester has to think and act like a legitimate user of the product.

2. **Penetration Testing:** This can be defined as the method of testing a computer or a network to identify the vulnerabilities present in the system/network.

3. **Verification:** This is the process of evaluating a product in the development stage, against specified requirements.

The most important and widely used among the various types of security testing is penetration testing; we will be restricting our discussion about security testing to only this, in our book.

### (ii) Types of Security Testing

There are three types of penetration testing:

1. No Knowledge testing or Black Box testing
2. Full Knowledge testing or White Box testing
3. Partial Knowledge testing or Grey Box testing

**Let us take a look at each type of penetration testing and compare their features.**

### Black Box Testing:

- It is assumed that an ethical hacker has no knowledge of the internal structure of the system/network that he is hacking. This test is used in cases where a possible attack may come from an unknown presence, who is completely unaware of the system and is able to gain access to the information on the network/servers.
- As no information about the system or the network is shared with the ethical hacker, it is his responsibility to collect all the required information about the system he is hacking into from other sources, prior to executing an attack.
- The fact that an ethical hacker will be penetrating their network, is not made known to everyone in the network security team. This helps in monitoring their reaction in a real-time scenario.

### White Box Testing

- An ethical hacker and his team will have extensive knowledge about the entire information system that they are going to be hacking into.
- They will have prior access to internal network assets, physical security measures and security protocols.
- A hacker will use controlled and deterministic methods to gain access to exact information or data that he is looking for.

Grey Box testing is a combination of both Black and White box testing, in which only the required information is shared with the ethical hacker and only a section of the system that needs investigation is allowed access to. Therefore, an ethical hacker must still research and what needs to be done.

### No Knowledge Testing or Black Box Testing

In this type of testing, *"an ethical hacker performing the action has no knowledge about the system being attacked. His intention is merely to simulate an external hacking or a Cyber-attack."*

**According to Paul Midian, there are five stages in Black Box testing and they are:**

1. Initial reconnaissance
2. Service determination
3. Enumeration
4. Gaining access
5. Privilege escalation

**Some of the important features factors about White Box testing have been listed below. White Box testing is:**

- Deterministic in nature.
- Demands lesser time and resources and thereby economical.
- A fast and efficient method of testing Moreover,
- In most of large organizations, there is a high level of dependency on partner systems/ other systems within the organization that have different security levels or protocols. There are possibilities that a client is unaware of the entire situation and hence is unable to educate the ethical hacker in this type of situation.
- In order to collect the information needed to conduct White Box testing, an ethical hacker needs complete support from:
    - Higher management
    - Technical support
    - Human resource/legal department of the organization

Grey Box testing may also be referred to as Hybrid testing as it incorporates features of both Black and White Box testing. Some of the important points to remember here are:

- One ethical hacker is operating from outside the network, preparing for a black box reconnaissance attack.
- Another person from inside the network is providing all the information to the former.

- The organization will decide and share only the relevant information with the hacking team.

There must be a communication protocol between those on the outsider and whoever is on the inside. If this is compromised at any point of time during the testing, the hackers will usually switch to a different plan.

### Comparison between Black Box Testing and White Box Testing

There are limitations to each type of testing. One of the most jarring limitations are the possibility of vulnerabilities going unnoticed by the attack team, especially in white box testing, because all the resources are open in front of them. Preparing a detailed checklist and following systematic methods will overcome these limitations on a good level.

**Let us take a look at the comparison between White and Black Box testing:**

*Table 1.1.1: Black Box Testing vs. White Box Testing*

| Black Box Testing | White Box Testing |
|---|---|
| The professional is unaware of the configurations of the system or the network he is hacking. | All the required information about the system, network, security protocols, users, databases etc.is provided to the professional, beforehand. |
| Test approaches are open-ended as the situation is unknown. | Test results are more specific and leading towards a certain conclusion. |
| As the tester works under unknown conditions, the whole testing procedure is going to utilise more resources and time, which costs more money. | This takes lesser time, resources and money. |
| There is almost nil or minimum communication between the tester and the development community, who can patch up vulnerabilities as and when they have been identified by the testers. | The developer community is in constant contact with the testers. Therefore, most of the vulnerabilities are generally eliminated in the design phase itself. |
| This is suitable for development companies that do not want to disclose the product or service that is being tested. | This is suitable for small or medium-sized companies with limited infrastructure or budget allocation for penetration testing. |

## Self-assessment Questions

9) Black box testing, White box testing and Grey box testing are the three types of Security testing. Among this, Grey box testing is also called as _______________

    a) Penetration testing b) Hybrid testing
    c) Reconnaissance d) None of the above

10) Assume that a company 'Trigent Information Systems' has decided to employ a team of ethical hackers to investigate their security protocols concerning the development of a new product. What is the ideal penetration testing type in this situation?

    a) Black box testing b) White Box testing
    c) Grey box testing d) Hybrid testing

## 1.1.5 Process of Malicious Hacking

Malicious hacking refers to the forced attempt by an individual, who we may call 'a hacker', on a computer system or a network, to steal information – either personal or corporate, or to render the system non-functional and non-reachable to its legitimate users. Malware attacks and social engineering are the two most commonly used methods by which a hacker can accomplish his intentions. In the following chapter, we are going to learn more about malicious hacking in terms of the various steps involved in this, the types of attacks and so on.

### (i) The Five Steps

1. **Reconnaissance:** Active and passive

2. **Scanning**

3. **Gaining access:** This has four levels - operating system, application, network and denial of service

4. **Maintaining access:** To perform the following actions:

    a) Uploading programs or data

    b) Downloading programs or data

    c) Modifying programs or data

5. Covering tracks, clearing tracks and installing back doors.

**The diagram show below will help you remember these steps easily:**

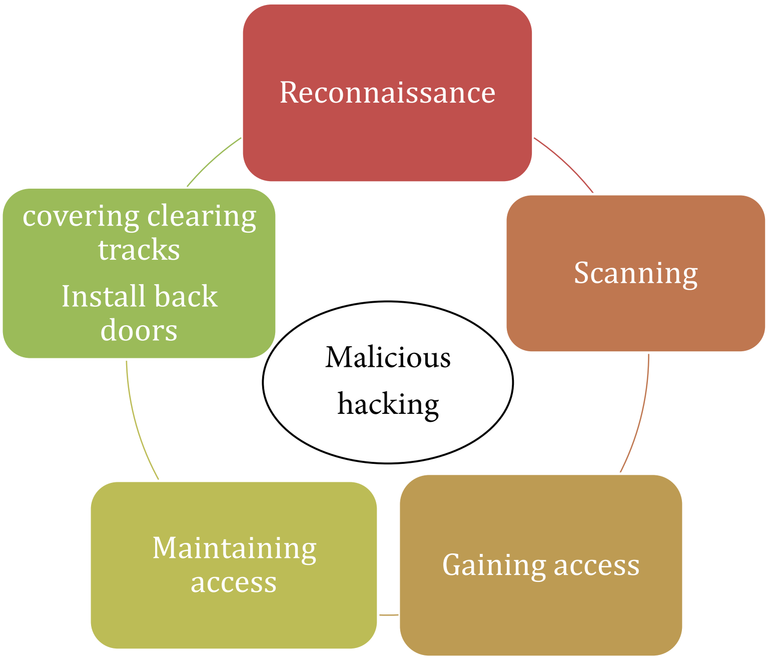


*Figure 1.1.1: Steps in Malicious Hacking*

Each of these steps have been briefly explained for your knowledge.

### Reconnaissance

Reconnaissance may be defined as the *'process of gathering data or preliminary inspection of an area of interest over a short period of time'.* In this stage, an attacker collects as much information about the target system via various means. He may do so by 'active' reconnaissance that involves 'probing' the network using technology and tools to collect information about an operating system, network configurations or protocols, open ports and so on. The second method, 'passive' reconnaissance, is where tasks are accomplished by using tools such as 'sniffers' (*i.e.*, if an intruder is able to get his hands of data packets, it is as good as hacking information from the sender. This is called as Sniffing.). If we compare the risk level experienced by organizations during each step of malicious hacking, one may call it 'notable' in Reconnaissance phase.

### Scanning

In this step, a hacker gains access to more detailed information based on the data collected during the reconnaissance phase. This includes user accounts, entry points into an application, security measures such as intrusion detection system, etc. It is also possible, by means of scanning tools such as vulnerability scanners, ports scanners and war diallers, to monitor register entries corresponding to the operating system in order to gauge if any patches have been installed. Retrieval of this kind of information is called as enumeration.

**Some of the tools used for scanning have been mentioned below:**

**Nmap:** This tool is used to identify network computers and operating systems. It also identifies open ports and applications installed or running on the target system and their different versions. All these actions help in investigating the standard security measures implemented on a network/system.

**Nessus:** This detects local flaws and missing patches if any and detects vulnerabilities present in a network host.

If you recall from what we read earlier about reconnaissance, we referred to the risk level to the organization as notable; however, in the scanning phase, it becomes 'high'. To an extent, the risk can be lowered by turning off all those applications and ports that are not required.

## Gaining Access

This is the actual attack phase; hence the risk level is considered as the 'highest'. The attacker has been successful in hacking the system and he now enjoys access to the operating system, network and other valuable and sensitive information. The type of attack may be a denial of service attack, buffer overflow or web-application based. It is also possible for the attacker to grant himself the highest level of access (similar to that of a system administrator) to the system. With these kinds of rights, a hacker can access even the most sensitive areas of the entire information system.

## Maintaining Access

The intentions of the hacker will not be satisfied by merely acquiring access to the target system. He has to maintain that access long enough to infect the system. In order to retain the rights over the system he has successfully hacked, he may have to modify the vulnerability that allowed him this access. By doing so, he can make sure that no other hackers can attack the same system. Some of the activities that take place in the background during this phase have been mentioned below:

- Downloading password files that may later be used to re-enter the same system.

- Installing Trojan horses and rootkits.
- Installing sniffers to monitor and log keystrokes of a user.

The last step in the whole process of malicious attack is to understand how to cover and clear tracks and install back doors.

### Covering, Clearing Tracks and how to install Back Doors

It is in the best interest of the hacker to erase his fingerprints from the scene. Rootkits to an extent does the job, but a hacker can modify log files to hide all those programs or applications that he has installed, from the view of the computer system. To hide directories, programs or file attributes, tunnelling, steganography and alternate data streams (ADS) are some of the methods that can be used to mask data.

## (ii) Outcome of Ethical Hacking

Considering the investment in money, time and resources, an organization is willing to make towards its Information Security department and professionals, the output of such an effort needs to be valuable to the organisation. The outcome of an ethical hacking investigation is a detailed report that comprises of:

- Background of events that has initiated the ethical hacking.
- Description of the steps performed and its results. This will also help the company compare it with the intended output and decide if the task has been accomplished to the client's satisfaction.
- Vulnerabilities and its remediation details are the most important and sensitive information of the whole assignment and will be handed over to the client directly without any leaks in sensitive information.

## Self-assessment Questions

11) In what is called as the actual attack phase, the hacker can gain access to a system at four levels. Operating system, application, network and ______________.

    a) Physical layer b) Denial of service

    c) Transport layer d) Penetration layer

12) Nessus used to identify network computers and operating systems.

    a) True b) False

13) Nmap and Nessus are examples of _____________.

    a) Security scanning tools b) Worms

    c) Malware d) Sniffers

14) Which is one feature of Windows NTFS, that lets the hacker hide rootkits or hacker tools in a system that can be executed without being noticed by System administrator.

    a) Alternate Data Stream b) Advanced Design System

    c) Active Directory Service d) None of the above

## 1.1.6 Footprinting

In the earlier section of this chapter, we learnt about Reconnaissance and its types. At times, the terms reconnaissance and footprinting are used alternatively to mean the same thing. Footprinting is a method used by a hacker to collect information about the organization, without its knowledge. This information is then used to create what is called as a blue print of the security details of a company.

In a definition by the **EC-Council**, there are 7 steps in the footprinting process and it is very important to understand these as they form the foundation for the ethical hacking process:

1. Information gathering
2. Network range determination
3. To identify active machines
4. Finding active ports and access points
5. Finding operating systems

6. Fingerprinting
7. Network mapping

Although, it is a common practise to perform these steps in this order, there may be exceptions.

### Outcome of Footprinting

Information collected from footprinting adds significant value to information security professionals who are representing either an organization or an individual, towards maintaining the integrity of the information. It is mandatory for organizations to conduct footprinting of their company, which helps reveal vulnerabilities present within and around the system and lets them design security parameters to countermeasure any possible attack from outside as well as from the inside.

**The information collected from footprinting may contain the following:**

- Domain name and internet domain names
- Network blocks
- IP addresses of the systems
- Name and version of the OS used on the target
- Web server version
- Information about any TCP/UDP services running on the target
- Location of VPN points
- Telephone numbers - Analogue/Digital
- Details of authentication programs
- Access Control Lists or ACLs

## (i) Gathering Information

Also known as the documentation phase, this involves collecting all possible information about the target network via various means. Various techniques are used for gathering information and each of them have a different source. The below table gives detailed information about every technique and source of information gathered in footprinting.

*Table 1.1.2: Information Gathering Techniques*

| Technique | Source of information |
|---|---|
| Open source or active information gathering. | Publicly accessible sources. |
| Active information gathering. | Social engineering, on-site visits and questionnaires. |
| Pseudonymous footprinting. | Information collected, may be published under a false name for safeguarding privacy. |
| Organizational or private footprinting. | Web-based calendars or company's email services. |
| Internet footprinting. | Internet. |
| Competitive footprinting. | Facts about the company's establishment, growth plans, resource planning and positioning and etc. |
| Whois footprinting | A hacker is able to name and gather the IP information of devices on the target network by hacking the DNS server. WsPingPro and Sam Spade can be used to perform  in Windows environment |
| Network footprinting. | Active footprinting - conducted through social engineering<br>Passive footprinting - conducted through an organization's website |
| Website and e-mail footprinting. | A mirror image of an organization's website is crated and phone numbers, e-mails or names are retrieved. |
| Google hacking. | Uses advanced operators in Google search. |

Internal or external URL of an organization – Google, blogs or discussion forums are a very valuable information source for hackers. Internal URL's can at times, provide a great deal of information about the internal architecture, hierarchy and positioning of the company and its strategies. Websites such as those mentioned below, are useful to find out more about an organisation information for hackers:

- http://news.netcraft.com
- http://www.webmaster-a.com/link-extractor-internal.php

### Footprinting through Search Engines

The attacker may use a search engine such as Google or Bing, to collect information such as technology platforms, employee information and intranet portals of the target. The advantage of using a search engine instead of reading about this information on the web is that even information that has been classified as sensitive and thus omitted by the web will be displayed in a search engine. Google Earth is one such resource that can be used to scout for location information about a target.

Analytical skills are essential for every hacker or information security professional as the results you get on a search engine greatly depends on keywords and other techniques that you use for searching and interpreting results. It is always recommended to use complex keywords which will help in getting the intended result rather usual or normal keywords that give you thousands of results.

**Some of the techniques that are used for searching include:**

- Extracting archived or mirrored websites.
- People search.
- **Competitive intelligence:** To identify, collect, analyse, verify and make use of important details about your competitor company, using the internet. This will help you conduct a comparative study of your product or service with a similar entity from your competitor in terms of market positioning, sales, revenue and so on.

### Whois

The output of this utility provides information such as what has been mentioned below, with respect to the target:

- Domain with which the target is registered.

- Contacts for technical as well as administrative aspects of the target system such as ownership, address, phone numbers, location and so on.

- The company's domain servers.

Information about who assigns domain names and how it is maintained in the database as well as updated has been mentioned below.

Based on the geographical location of the organization, there are 5 Regional Internet Registries (RIRs) that are responsible for associating domain names with IP addresses. They are:

*Table 1.1.3: RIRs and Regions*

| Region | RIRs |
|---|---|
| North America | American Registry for Internet Numbers (ARIN) |
| Europe, Middle East and Central Asia | RIPE Network Coordination Centre (RIPE NCC) |
| Asia-Pacific | Asia-Pacific Network Information Centre (APNIC) |
| Latin America and Caribbean | Latin American and Caribbean Internet Address Registry (LACNIC) |
| Africa | African Network Information Centre (AfriNIC) |

All these RIRs allow Whois searches on their database to retrieve the information. While we have RIRs to delegate resources to local customers, following the regional policy, it is the Internet Corporation for Assigned Names and Numbers or ICANN that delegates the required internet resources to these RIRs.

The statistics mentioned below show a part of the RIPE (Réseaux IP Européens) Network Coordination Centre Whois for BBC (British Broadcasting Corporation).

| | |
|---|---|
| person | Brandon Butterworth |
| address | British Broadcasting Corporation |
| address | BBC Centre House |
| address | 56 Wood Lane |
| address | London |
| address | W12 7SB |
| address | England, GB |
| phone | +44 3030409777 |
| fax-no | +44 2088115515 |
| e-mail | brandon@rd.nnc.co.uk |
| nic-hdl | BB231 |
| mnt-by | BBC-MNT |
| created | 1970-01-01T00:00:00Z |
| last-modified | 2010-12-13T13:54:56Z |
| source | RIPE |

*Figure 1.1.2: RIPE Network Coordination Centre Whois for BBC*

There is no in-built Whois client in a Windows operating system. Therefore, users can use any third-party utility that is available in the market. Some of them are mentioned below for your reference:

1. www.samspade.org
2. www.dnsstuff.com
3. www.allwhois.com

**Other Whois lookup tools for your reference:**

1. SmartWhois from TamoSoft can be downloaded from http://www.tamos.com/products/smartwhois/ - SmartWhois is a network information utility tool which can fetch information about the owner of the target domain, the year in which the domain was registered and in whose name and the person who owns the IP address block
2. http://netcraft.com
3. http://www.whois.net
4. http://www.iptools.com

## DNS Footprinting

As previously mentioned, this method refers to the process of extracting a target's DNS Zone information from the server, in turn leading to naming and IP information for resources found within the network. Before dwelling on the details of DNS footprinting, let us first define DNS.

DNS stands for Domain Name System, which is associated with either internet or private network that translated domain names to IP addresses. The primary objective of DNS footprinting is to retrieve all DNS servers and any corresponding records of the target organization or computer system. When we come to footprinting using DNS, we should realise that an organization may have an internal or external DNS servers, that can give out information such as usernames, system names, IP addresses and so on.

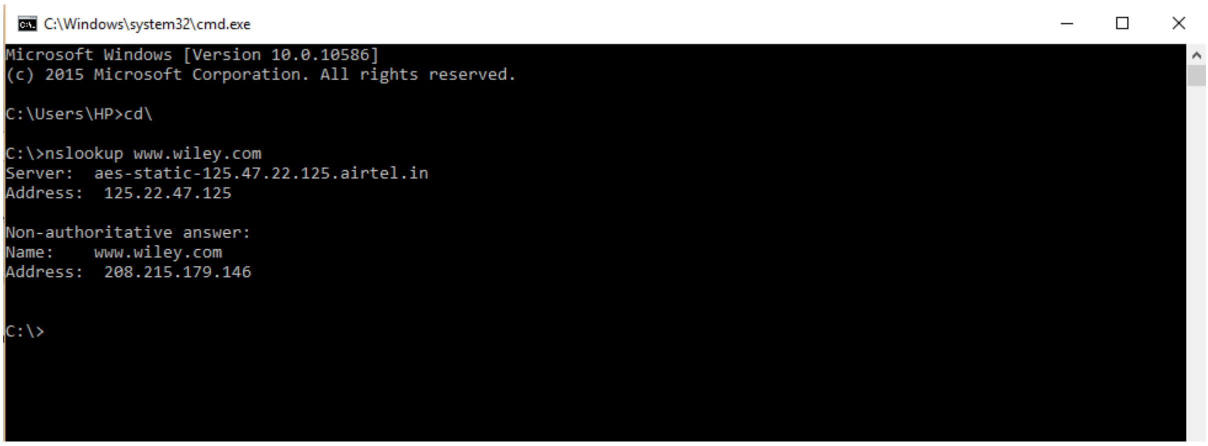
Some of the tools that can be used for DNS footprinting are NSlokup, DNSstuff, ARIN and Whois. ARIN and Whois have already been described. Now, we will take a look at NSlookup.

**Some of the DNS interrogation tools have been mentioned below:**

- http://www.dnsstuff.com
- http://network-tools.com
- http://www.checkdns.neSt
- http://www.iptools.com

## Nslookup

Nslookup is a program which is used to query internet domain name servers. With the output from this program, one can identify a target's DNS Infrastructure, IP address and the IP of the mail server. Nslookup client is available in both for Windows and Linux operating systems and in Windows can be accessed via command prompt by typing nslookup.



C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\HP>cd\

C:\>nslookup www.wiley.com
Server:  aes-static-125.47.22.125.airtel.in
Address:  125.22.47.125

Non-authoritative answer:
Name:    www.wiley.com
Address:  208.215.179.146


C:\>
```

*Figure 1.1.3: nslook for wiley*

**Other tools that are available are:**

1. **DIG: Domain Information Groper –** It is used to query DNS servers or to simulate a DNS resolver or a name server. Another use of this tool is in network troubleshooting.

2. **SpiderFoot:** This is a domain footprinting tool that gives information about subdomains, affiliates, web server versions, email addresses and so on by searching Google, Netcraft, DNS and other websites.

### Open Source Searching

A fair amount of valuable information about a target, such as a company's location, email addresses and phone numbers, partner company details, news about latest product launches and even certain privacy policies may be researched from their website, press releases, newsletters, employee blogs or their job postings. This kind of information is available easily to hackers and they do not need to use any utility or tools.

Up to now, we have seen, various utilities and procedures to gather information about the target. The next step that constitutes of footprinting is to not locate the network range. Let us take a look at some of the methods to do this in the following sections.

## (ii) Locating the Network Range

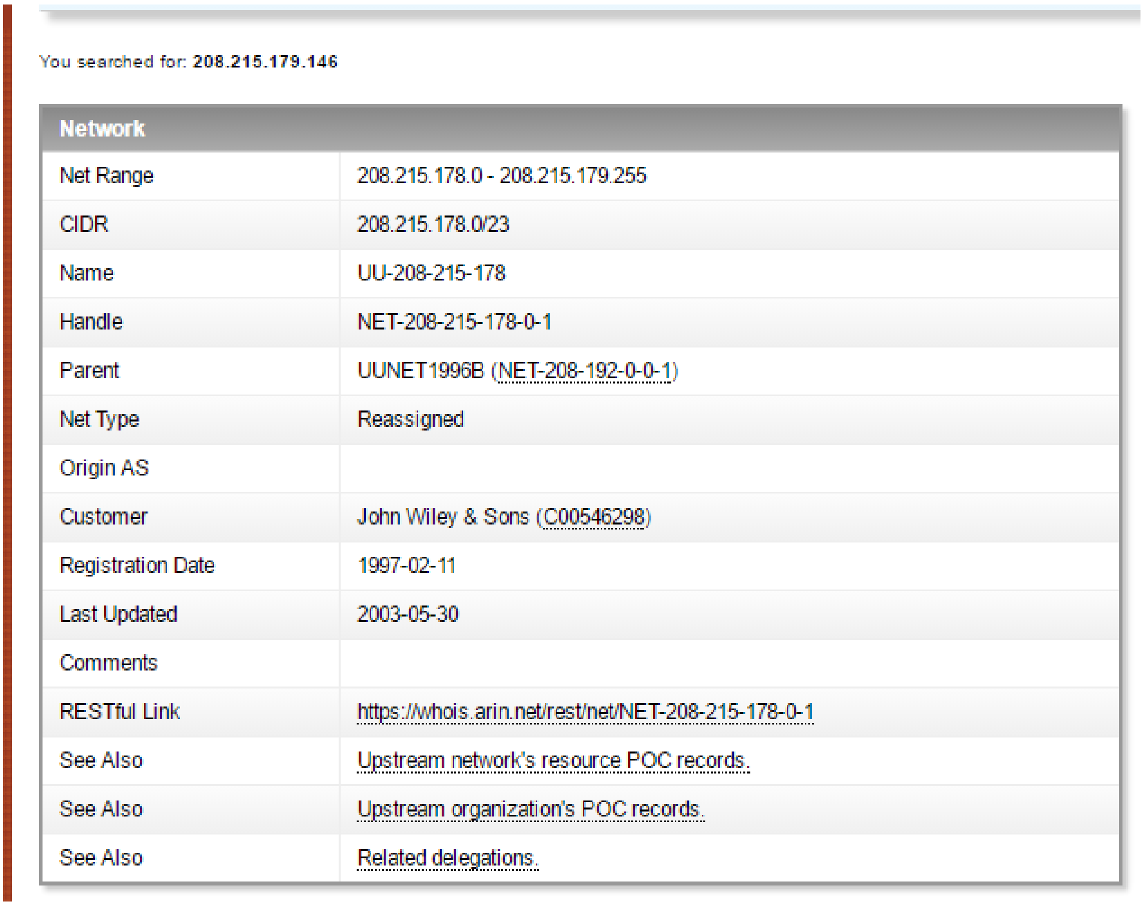
After having studied the first phase in footprinting which was 'information gathering', let us now proceed to learn about how to locate the network range of the target system.

In this phase, the aim of the hacker will be to identify the range of IP addresses which are used by the target system, along with its subnet mask. Knowing these will pave its way for the scanning and enumeration processes.

Similar to Nslookup and Whois utilities, there are other utilities that can be used to find IP addresses and subnet masks, such as:

- **ARIN** (American Registry for Internet Numbers)
- **Trace route** and TTL

Let us assume that you know the IP address of the target's web server (***For example,*** www.wiley.com, from Nslookup, Refer Fig 1.1.4) and it is 208.215.179.146. Let us now enter this IP address in www.arin.net and see the result.



You searched for: **208.215.179.146**

| Network | |
|---|---|
| Net Range | 208.215.178.0 - 208.215.179.255 |
| CIDR | 208.215.178.0/23 |
| Name | UU-208-215-178 |
| Handle | NET-208-215-178-0-1 |
| Parent | UUNET1996B (NET-208-192-0-0-1) |
| Net Type | Reassigned |
| Origin AS | |
| Customer | John Wiley & Sons (C00546298) |
| Registration Date | 1997-02-11 |
| Last Updated | 2003-05-30 |
| Comments | |
| RESTful Link | https://whois.arin.net/rest/net/NET-208-215-178-0-1 |
| See Also | Upstream network's resource POC records. |
| See Also | Upstream organization's POC records. |
| See Also | Related delegations. |

*Figure 1.1.4: Output for an IP address from www.arin.net*

The first line from our output states the IP address range of the target system, which helps a hacker to restrict his search to this range, during scanning.

### Traceroute

This is a method by which we can identify active machines in the network. It uses the path travelled (by packet) from the source to the destination computer, to arrive at the conclusion. This utility is called Tracert in Windows and it uses Internet Message Control Protocol (ICMP); the Linux version uses UDP.

ICMP is one of the most important protocols in the IP family, which is used by most routers in order to communicate error information in case of failure to deliver packets. Network administrators use ICMP for troubleshooting network connections using pong or Trace route.

With the help of ICMP echo packets, Traceroute displays the Fully Qualified Domain Name (FQDN) and IP addresses of every gateway right up to the remote host. The steps can be explained as shown below:

1. Traceroute sends a packet to a destination computer with a TLL value 1.
2. The first router encountered, will decrement the TTL value by 1. If the resulting TTL value is zero, that packet will be discarded and it sends a message to the originating host, informing Traceroute about this status.
3. Upon receiving this message, Traceroute will record the IP address and DNS name of this router before sending another packet, this time with TTL value 2.
4. This packet will go through successfully at the first router (as it will deduct 1 from TTL value which is 2 and the result is not zero) and will get discarded at the second router as it deducts 1 from TTL (whose value is now 1) and the result is zero.
5. The second router will now send a message to the originating host with the status, upon receiving which, Traceroute will record the IP address and DNS name of the second router.
6. This process will continue, with Traceroute sending packets each time with incremental TTL values, until the target is reached or when Treaceroute decides that the target is unreachable.
7. Apart from recording the IP address and DNS name of routers en path to target, Traceroute also records the time it takes for each packet to make a round trip around each router.

### Traceroute Analysis

The intention of the attacker in conducting a Traceroute analysis is to retrieve information such as network topology, trusted routers and firewall positioning. Once a hacker gets the result of a Traceroute, he will be able to draw the network diagram, which will further help him to strategize his plan better.

For illustration purposes, we shall consider a result from a Traceroute operation. It is important to note that an attacker may have to perform several Traceroute operations to arrive at this result.

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1z
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

**The resulting network diagram for the above Traceroute analysis would look like this:**

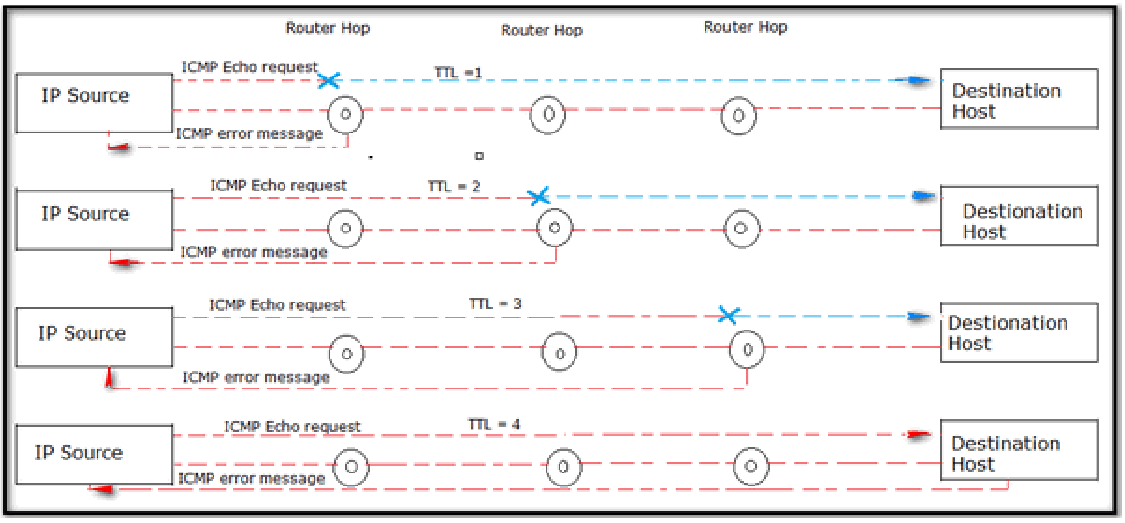
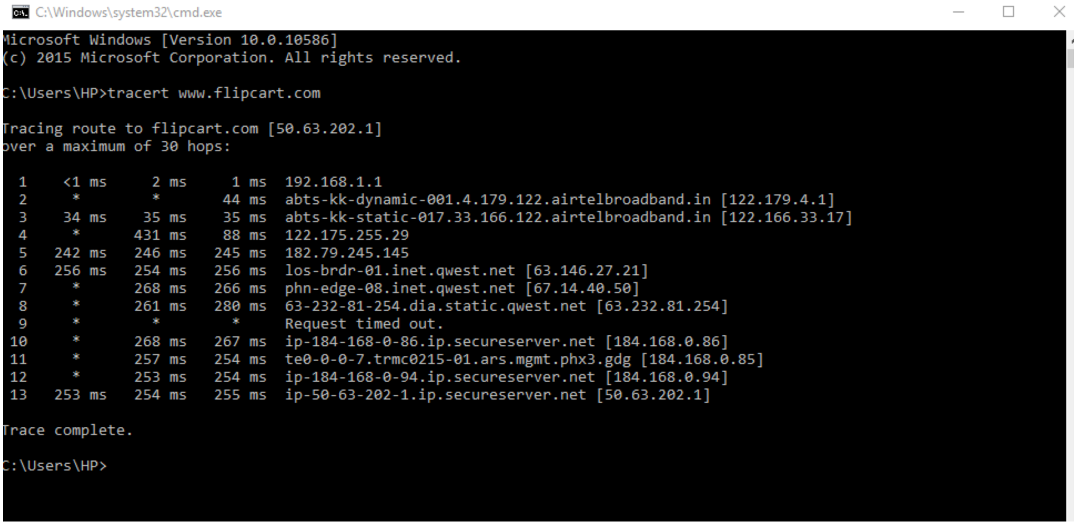


*Figure 1.1.5: Traceroute Analysis*

**Taking another example of Traceroute output for www.flipcart.com from a computer.**



```
icrosoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

:\Users\HP>tracert www.flipcart.com

racing route to flipcart.com [50.63.202.1]
ver a maximum of 30 hops:

  1    <1 ms     2 ms     1 ms  192.168.1.1
  2     *        *       44 ms  abts-kk-dynamic-001.4.179.122.airtelbroadband.in [122.179.4.1]
  3    34 ms    35 ms    35 ms  abts-kk-static-017.33.166.122.airtelbroadband.in [122.166.33.17]
  4     *      431 ms    88 ms  122.175.255.29
  5   242 ms   246 ms   245 ms  182.79.245.145
  6   256 ms   254 ms   256 ms  los-brdr-01.inet.qwest.net [63.146.27.21]
  7     *      268 ms   266 ms  phn-edge-08.inet.qwest.net [67.14.40.50]
  8     *      261 ms   280 ms  63-232-81-254.dia.static.qwest.net [63.232.81.254]
  9     *        *        *     Request timed out.
 10     *      268 ms   267 ms  ip-184-168-0-86.ip.secureserver.net [184.168.0.86]
 11     *      257 ms   254 ms  te0-0-0-7.trmc0215-01.ars.mgmt.phx3.gdg [184.168.0.85]
 12     *      253 ms   254 ms  ip-184-168-0-94.ip.secureserver.net [184.168.0.94]
 13   253 ms   254 ms   255 ms  ip-50-63-202-1.ip.secureserver.net [50.63.202.1]

race complete.

:\Users\HP>
```

*Figure 1.1.6: Executing Traceroute for flipcart.com*

The output of Traceroute can be interpreted to reveal vital information, about the path travelled by packets along with,

- How many routers are used in the network and their names.
- Geographical location of the router.
- Target's DNS entries.
- Network affiliations of the target.

Command prompt is not the only utility to run Traceroute. There are other applications that can be used that add a visual interface for results.

1. **Neo Trace:** This tool displays the route taken by the packets to travel from host to destination and nodes present in that path on the internet.
2. **Visual Route (http://www.visualroute.com/):** This tool is used to perform full hope traceroute, reverse tracing, giving hope response time, packet loss reporting, performing reverse DNS, ping plotting, port probing, network scanning etc.
3. **Ping Plotter (https://www.pingplotter.com/):** This is a network troubleshooting tool that provides results in a graphical manner which is easy to interpret and act upon rather a pure mathematical result set.

# Self-assessment Questions

15) What is the full form of ICANN?

  a) International Congress for Assigned Names and Numbers

  b) Internet Company for Assigned Names and Numbers

  c) International Commission for Assigned Names and Numbers

  d) Internet Corporation for Assigned Names and Numbers

16) One of the options given below is not a site that provides comprehensive Whois information. Which is it?

  a) www.dnsstuff.com    b) www.internic.net

  c) www.ripe.net    d) www.geektools.come

17) Which of these is not truein case of Whois

  a) Used to search the internet for domain ownership details

  b) Primary tool used to navigate RIRs and query the DNS

  c) Program used to find additional IP Addresses of a target

  d) www.samspade.org is a third-party utility that offers Whois

18) The command line syntax to query ‘Google’ using Nslookup will be.

  a) www.google.com    b) Nslookup www.google.com/

  c) Nslookup www.google.com    d) None of the above

19) The first step in the information gathering process is:

  a) Ping the domain name to find IP address

  b) Traceroute, to trace the path travelled by the packet to reach the target computer

  c) Whois, to query the DNS

  d) Nslookup to query internet domain name servers for additional IP addresses of a target

## 1.1.7 Scanning

Scanning may be defined as the *"investigation of an information system or network to identify any lapses in its security, using tools and techniques."*

### (i) Goal of Scanning

The goal of scanning is to discover open ports and applications that are vulnerable to hacking.

#### Steps in a Scanning Phase

1. To identify active machines.
2. To discover services actively running on the target, including TCP and UDP services.
3. To identify the operating system.
4. To use active and passive fingerprinting.

**Each one of these methods are explained in the following sections:**

#### Identifying Active Machines

This stage provides valuable information for the following reasons:

1. It provides precise and up-to-date details about the network and its surroundings that is very important for a hacker to plan his attack.
2. Defines the jurisdiction of a hacker.
3. Helps to take stock of the systems that are accessible on a target network.

Traceroute and ping are the two methods used to identify active machines. Let us look into each of these.

Traceroute has already been covered in the footprinting section of this book. We will now look at how Ping works.

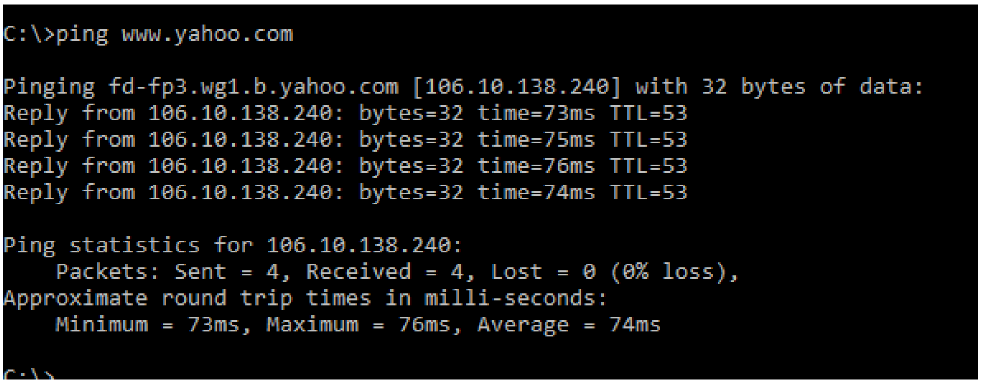
#### Ping

This helps us to:

1. Identify active machines on the network.
2. Identify the speed at which a packet travels from sender to receiver on a network.

3. Helps to analyse network traffic.

**Let us look at the results from a Ping test for www.yahoo.com from a computer.**



```
C:\>ping www.yahoo.com

Pinging fd-fp3.wg1.b.yahoo.com [106.10.138.240] with 32 bytes of data:
Reply from 106.10.138.240: bytes=32 time=73ms TTL=53
Reply from 106.10.138.240: bytes=32 time=75ms TTL=53
Reply from 106.10.138.240: bytes=32 time=76ms TTL=53
Reply from 106.10.138.240: bytes=32 time=74ms TTL=53

Ping statistics for 106.10.138.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 73ms, Maximum = 76ms, Average = 74ms

C:\>
```

*Figure 1.1.7: Ping Test for yahoo.com*

As it is not just one machine that the hacker has to identify in a network but all of them, trying a ping command on them individually can be a very time-consuming task. Hence, a technique called ping sweeps is used to ping a batch of devices at a time.

Apart from a ping command, there are other utilities that can be used such as WS, Pingpro Pack and Net Scantools.

Identifying open ports and services is the second phase of scanning and has been explained below:

**Some of the techniques used in this method are:**

1. Port scanning
2. Banner grabbing
3. War dialling
4. War walking

## Port Scanning

This is used by both system administrators and hackers to figure out which ports are open and to find out what are services/applications are running on the target device. This is done by connecting to TCP and UDP ports and then sending a data packet.

Any system will have 65, 535 ports and each one will have its own TCP and UDP ports, through which a hacker can gain access to the target, if found vulnerable to his attacks. By identifying the port numbers, the attacker can tell which services are running on the target's system/network. The website http://whatismyipaddress.com/port-listgives a list of port numbers.

An attacker uses the port-scanning method to differentiate between active and inactive hosts because he does not need to look at inactive hosts and can concentrate on the active ones instead.

## (ii) Scanning Types

1. **SYN or Stealth Scan:** An attacker sends a SYN packet to the target and if a SYN/ACK is received, this means that the port is listening and a connection to the target would be established. If the port is either inactive or closed, an RST is received. This type of scan is the most preferred as most Intrusion Detection Systems don't treat it as an attack.

2. **XMAS:** This scan works only on the target system that follows RFC 793 implementation of TCP/IP. XMAS scans send a packet with FIN, URG and PSH flags set. The scan receives no response if the port is open and receives RST/ACK signal if the port is closed.

3. **FIN:** This is identical to XMAS but the packet only has a FIN flag set.

4. **NULL:** This is also similar to XMAS, but has certain limitations. The packet sent has no flags set.

5. **IDLE:** Using a fake IP address, this sends a SYN packet to a target. The status of the port can be determined depending on the response.

### Determining the Operating System

1. By examining Telnet banners or its File Transfer Protocol (FTP Servers), once the connections are made to these services.

2. TCP/IP Stack Fingerprinting: This takes advantage of differences in the way TCP/IP is implemented by an operating system and device vendors.

3. TCP Initial Sequence Number Sampling: This interprets the pattern of sequences of numbers from the response sent by the target.

## (iii) Scanning Tools

Scanning tools are used by both, attackers and system administrators, for either attacking or detecting malicious attacks, respectively.

**Some of the tools used for scanning are:**

1. **HPing:** A network analysis tool that allows the scanner to gather information from the packet's response.

2. **Nessus:** Security auditing tool for Linux.

3. **NMap:** This is a very important tool and it is recommended to have hands-on experience when working with this tool.

4. **Snort:** Used for network sniffing.

5. **Tcpview:** Used to find out what application – port pairing on windows platforms.

6. SAINT

7. VLAD the Scanner

## Self-assessment Questions

20) What are the utilities used for identifying active machines on a network?

a) Ping and Traceroute　　b) Nslookup and Whois

c) Net view and Nbtscan　　d) None of the above

21) Which of the below options best define a Ping Sweep?

a) Detecting live machines on the target network

b) Identifying the operating system

c) The process where a ping is executed on a batch of devices

d) Identifying specific applications

22) A port can be found in either an ‘open’, ‘closed’ or _________ state.

a) Filtered　　b) Active

c) Inactive　　d) Nulls

23) TCP/IP stack fingerprinting exploits the fact that the ___________ protocol is implemented differently by an operating system and a vendor.

a) UDP　　b) POP3

c) SNMP　　d) TCP/IP

24) _________ is a free security auditing tool for Linux.

a) HPing　　b) Legion

c) Nessus　　d) NMap

## Summary

- Ethical hacking may be defined as the "Process of gaining authorized access in to an Information System of an Organization or individual, in order to identify and evaluate the possible threats to it".
- Confidentiality, integrity and availability form what is called the CIA triad.
- Threat is an activity or occurrence that is capable of causing potential damage to an information system or networks.
- Black Box testing, White box testing and Grey box testing are the three types of security testing.
- Black box testing is suitable for organizations that do not want to disclose any information about their unreleased product, but still want to test their security parameters for the same.
- A malicious attack can occur at the operating system level, application level, network level or denial of service.
- Nmap and Nessus are most widely used scanning tools.
- Steganography may be defined as the science of hiding information.
- Port scanning is a method used to find out which ports are open and what applications and services are running on the target.
- Apart from scanning tools that are available on the internet for no cost, there are also commercial scanning tools developed by vendors which have enhanced features and technical support.

## Terminal Questions

1. What are the five steps in the process of malicious hacking? Explain them briefly.
2. Explain the process involved in malicious hacking.
3. What are the various factors to be considered while conducting a penetration test for an organization?

# Answer Keys

| Self-assessment Questions | |
|---|---|
| Question No. | Answer |
| 1 | d |
| 2 | c |
| 3 | b |
| 4 | d |
| 5 | c |
| 6 | b |
| 7 | d |
| 8 | d |
| 9 | b |
| 10 | a |
| 11 | b |
| 12 | b |
| 13 | a |
| 14 | a |
| 15 | d |
| 16 | e |
| 17 | c |
| 18 | c |
| 19 | c |
| 20 | a |
| 21 | c |
| 22 | a |
| 23 | d |

# Activity

**Activity Type:** Online **Duration:** 45 Minutes

**Description:**

1. Assume that you are a part of an ethical hacking team that recently conducted a white box testing for a firm and you have your results with you. Prepare a report to present your facts before the firm using one of the templates available on the internet or a sample report.

   You may make the necessary assumptions as applicable

2. Use three of the many available third-party Whois utilities and run diagnostics for a specific domain name in all three. Make a report of the output and compare them.

   You may use www.samspade.org, www.dnsstuff.comorwww.allwhois.com