

Ethical Hacking - Overview

SAMARENDRANATH

Introduction

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them.

Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Types of Hacking

Website Hacking – Hacking a website means taking unauthorized control over a web server and its associated software, such as databases and other interfaces.

Network Hacking – Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. to harm the network system and hamper its operation.

Email Hacking – It includes getting unauthorized access to an Email account and using it without taking the consent of its owner.

Types of Hacking

Ethical Hacking – Ethical hacking involves finding weaknesses in a computer or network system for testing purposes and finally getting them fixed.

Password Hacking is recovering secret passwords from data stored in or transmitted by a computer system.

Computer Hacking is stealing computer IDs and passwords by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

To recover lost information, especially in case you lost your password.

To perform penetration testing to strengthen computer and network security.

To put adequate preventative measures in place to prevent security breaches.

To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

- Massive security breach.
- Unauthorized system access to private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Purpose of Hacking

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

Hacker Types

White Hat Hackers

White Hat hackers are also known as Ethical Hackers. They never intend to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and is one of the most demanding jobs in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Hacker Types

Black Hat Hackers

Black Hat hackers, also known as crackers, hack to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent, which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Hacker Types

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for fun and exploit a security weakness in a computer system or network without the owner's permission or knowledge.

They intend to bring the weakness to the attention of the owners and get appreciation or a little bounty from the owners.

Miscellaneous Hackers

Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under sensitive information.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term Blue Hat to represent security briefing events.

Miscellaneous Hackers

Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

Script Kiddie

A script kiddie is a non-expert who breaks into computer systems using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term Kiddie.

Miscellaneous Hackers

Neophyte

A neophyte, "n00b", "newbie," or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

Terminologies

Adware – Adware is software designed to force pre-chosen ads to display on your system.

Attack – An attack is an action that is done on a system to get its access and extract sensitive data.

Back door – A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

Bot – A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.

Terminologies

Botnet – A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.

Brute force attack – A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.

Buffer Overflow – Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

Clone phishing – Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

Terminologies

Cracker – A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.

Denial of service attack (DoS) – A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

DDoS – Distributed denial of service attack.

Terminologies

Exploit Kit – An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.

Exploit – Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.

Firewall – A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.

Terminologies

Keystroke logging – Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Key loggers are usually secreted onto a device using a Trojan delivered by a phishing email.

Logic bomb – A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.

Malware – Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

Terminologies

Master Program – A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

Phishing – Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.

Phreaker – Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long distance phone calls or to tap phone lines.

Rootkit – Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

Terminologies

Shrink Wrap code – A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.

Social engineering – Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.

Spam – A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.

Spoofing – Spoofing is a technique used to gain unauthorized access to computers, where by the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

Terminologies

Spyware – Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

SQL Injection – SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution(e.g. to dump the database contents to the attacker).

Threat – A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.

Terminologies

Trojan – A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be the redesigned with an intention to destroy files, alter information, steal passwords or other information.

Virus – A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Vulnerability – A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

Worms – A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Terminologies

Cross-site Scripting – Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into webpages viewed by other users.

Zombie Drone – A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

Tools

NMAP

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing.

Nmap was originally designed to scan large networks, but it can work equally well for single hosts.

Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine –

- what hosts are available on the network,

- what services those hosts are offering,

- what operating systems they are running on,

- what type of firewalls are in use, and other such characteristics.

Tools

Metasploit

Metasploit is one of the most powerful exploit tools. It's a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions – commercial and free edition. Metasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations –

- Conduct basic penetration tests on small networks

- Run spot checks on the exploitability of vulnerabilities

- Discover the network or import scan data

- Browse exploit modules and run individual exploits on hosts

Tools

Burp Suit

Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

Tools

Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range. It can be freely copied and used anywhere. In order to increase the scanning speed, it uses multithreaded approach, wherein a separate scanning thread is created for each scanned IP address.

Angry IP Scanner simply pings each IP address to check if it's alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be saved to TXT, XML, CSV, or IP-Port list files. With help of plugins, Angry IP Scanner can gather any information about scanned IPs.

Tools

Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It helps in easy recovery of various kinds of passwords by employing any of the following methods –

sniffing the network,

cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks,

recording VoIP conversations,

decoding scrambled passwords,

recovering wireless network keys,

revealing password boxes,

uncovering cached passwords and analyzing routing protocols.

Tools

Ettercap

Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

Tools

EtherPeek

EtherPeek is a wonderful tool that simplifies network analysis in a multiprotocol heterogeneous network environment. EtherPeek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes.

EtherPeek proactively sniffs traffic packets on a network. By default, EtherPeek supports protocols such as AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets.

Tools

SuperScan

SuperScan is a powerful tool for network administrators to scan TCP ports and resolve host names. It has a user friendly interface that you can use to –

- Perform ping scans and port scans using any IP range.

- Scan any port range from a built-in list or any given range.

- View responses from connected hosts.

- Modify the port list and port descriptions using the built in editor.

- Merge port lists to build new ones.

- Connect to any discovered open port.

- Assign a custom helper application to any port.

Tools

QualysGuard

QualysGuard is an integrated suite of tools that can be utilized to simplify security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for IT systems and web applications.

QualysGuard includes a set of tools that can monitor, detect, and protect your global network.

Tools

WebInspect

Web Inspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web application layer.

It can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

LC4

LC4 was formerly known as L0phtCrack. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.

LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

Tools

LANguard Network Security Scanner

LANguard Network Scanner monitors a network by scanning connected machines and providing information about each node. You can obtain information about each individual operating system.

It can also detect registry issues and have a report set up in HTML format. For each computer, you can list the netbios name table, current logged-on user, and Mac address.

Tools

Network Stumbler

Network stumbler is a Wi-Fi scanner and monitoring tool for Windows. It allows network professionals to detect WLANs. It is widely used by networking enthusiasts and hackers because it helps you find non-broadcasting wireless networks.

Network Stumbler can be used to verify if a network is well configured, its signal strength or coverage, and detect interference between one or more wireless networks. It can also be used to non-authorized connections.

Tools

ToneLoc

ToneLoc stands for Tone Locator. It was a popular war dialing computer program written for MS-DOS in the early 90's. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code.

Malicious hackers use the resulting lists in breaching computer security - for guessing user accounts, or locating modems that might provide an entry-point into computer or other electronic systems.

It can be used by security personnel to detect unauthorized devices on a company's telephone network.

Skills

- Password guessing and cracking
- Session hijacking
- Session spoofing
- Network traffic sniffing
- Denial of Service attacks
- Exploiting buffer overflow vulnerabilities
- SQL injection

Basic Skills

Computer Hacking is a Science as well as an Art. Like any other expertise, you need to put a lot of effort in order to acquire knowledge and become an expert hacker. Once you are on the track, you would need more effort to keep up-to-date with latest technologies, new vulnerabilities and exploitation techniques.

An ethical hacker must be a computer systems expert and needs to have very strong programming and computer networking skills.

An ethical hacker needs to have a lot of patience, persistence, and perseverance to try again and again and wait for the required result.

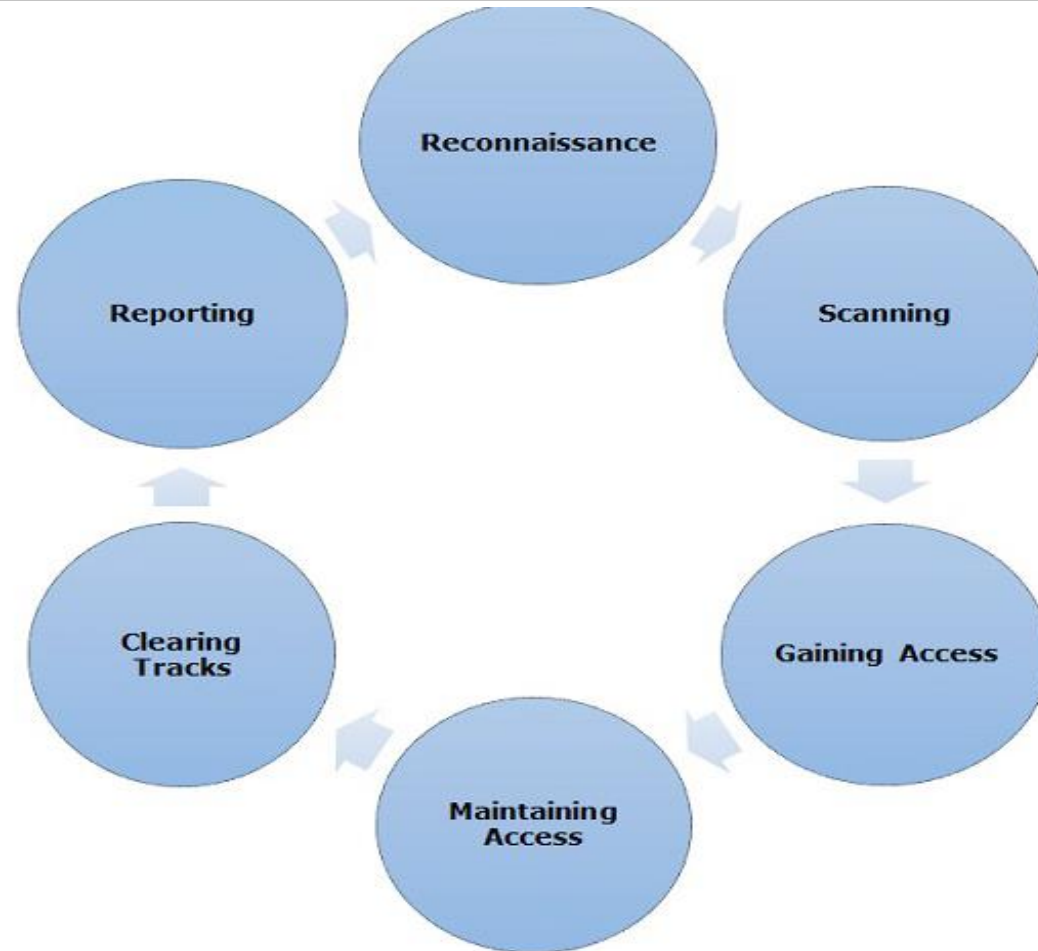
Additionally, an ethical hacker should be smart enough to understand the situation and other users 'mind-set in order to apply social engineering exploits. A good ethical hacker has great problem-solving skills too.

Note

You need to stay as a White Hat Hacker which means you need to work within given boundaries. Never intrude or attack any computer or network without a required permission from the authorities.

As a final note, it is highly recommended that you refrain from engaging yourself in black hat hacking which may spoil your entire career.

Ethical Hacking - Process



Process

Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Process

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Process

Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Reconnaissance

Information Gathering and getting to know the target systems is the first process in ethical hacking.

Reconnaissance is a set of processes and techniques (Foot printing, Scanning & Enumeration) used to covertly discover and collect information about a target system.

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below –

Gather initial information

Determine the network range

Identify active machines

Discover open ports and access points

Fingerprint the operating system

Uncover services on ports

Map the network

Reconnaissance

Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Passive Reconnaissance

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Foot printing

Foot printing is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Foot printing could be both passive and active. Reviewing a company's website is an example of passive foot printing, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Foot printing is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

Footprinting

A hacker can collect the following information –

Domain name

IP Addresses

Namespaces

Employee information

Phone numbers

E-mails

Job Information

Domain Name Information

You can use <http://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.



The image shows a screenshot of the WHOIS Lookup website. At the top, the text "WHOIS Lookup" is displayed in a large, bold, orange font. Below this, the text "Search domain name registration records" is shown in a smaller, grey font. There is a search input field with a light blue border and a green search button to its right. The input field contains the placeholder text "Enter Domain Name or IP Address". The search button is green and features a magnifying glass icon followed by the word "SEARCH" in white capital letters. Below the input field, there is a line of text providing examples: "Examples: qq.com, google.co.in, bbc.co.uk, ebay.ca".

WHOIS Lookup

Search domain name registration records

Enter Domain Name or IP Address

Q SEARCH

Examples: qq.com, google.co.in, bbc.co.uk, ebay.ca

This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: <http://whois.educause.edu>

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail. The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

Domain Name: MANIPAL.EDU

Registrant:

Manipal Academy of Higher Education
Madhav Nagar
Manipal, Karnataka 576184
India

Administrative Contact:

Domain Admin
Manipal Academy of Higher Education
Madhav Nagar
Manipal, Karnataka 576184
India
+91.8282571281
kathir.kanath@manipal.edu

Technical Contact:

Domain Admin
Manipal Academy of Higher Education
Madhav Nagar
Manipal, Karnataka 576184
India
+91.8282571281
kathir.kanath@manipal.edu

Name Servers:

NS-759.AWSDNS-38.NET
NS-1945.AWSDNS-51.CO.UK
NS-1843.AWSDNS-82.ORG
NS-285.AWSDNS-35.COM

Domain record activated: 27-Sep-1999
Domain record last updated: 17-Aug-2023
Domain expires: 31-Jul-2024

Finding IP Address

You can use ping command at your prompt. This command is available on Windows as well as on Linux OS.

\$ping manipal.edu

```
Microsoft Windows [Version 10.0.19045.3324]
(c) Microsoft Corporation. All rights reserved.

C:\Users\samar>ping manipal.edu

Pinging manipal.edu [13.33.146.28] with 32 bytes of data:
Reply from 13.33.146.28: bytes=32 time=51ms TTL=246
Reply from 13.33.146.28: bytes=32 time=97ms TTL=246
Reply from 13.33.146.28: bytes=32 time=61ms TTL=246
Reply from 13.33.146.28: bytes=32 time=93ms TTL=246


Ping statistics for 13.33.146.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 97ms, Average = 75ms

C:\Users\samar>
```

Finding Hosting Company

Once you have the website address, you can get further details using the [ip2location. Com](http://ip2location.com) website.

Following is the example to find out the details of an IP address –

Permalink	https://www.ip2location.com/13.33.146.28
<input checked="" type="checkbox"/> IP Address	13.33.146.28
<input checked="" type="checkbox"/> Country	 India [IN]
<input type="checkbox"/> Region	Tamil Nadu
<input type="checkbox"/> City	Chennai
<input type="checkbox"/> Coordinates of City	13.087898, 80.278479 (13°5'16"N 80°16'43"E)
<input type="checkbox"/> ISP	Amazon.com Inc.
<input type="checkbox"/> Local Time	20 Aug, 2023 07:56 PM (UTC +05:30)
<input type="checkbox"/> Domain	amazon.com
<input type="checkbox"/> Net Speed	(COMP) Company/T1
<input type="checkbox"/> IDD & Area Code	(91) 044
<input type="checkbox"/> ZIP Code	600009
<input type="checkbox"/> Weather Station	Madras (INXX0075)
<input type="checkbox"/> Mobile Carrier	-
<input type="checkbox"/> Mobile Country Code - MCC	-
<input type="checkbox"/> Mobile Network Code - MNC	-
<input type="checkbox"/> Elevation	13m
<input type="checkbox"/> Usage Type	(DCH) Data Center/Web Hosting/Transit
<input type="checkbox"/> Address Type	Anycast
<input type="checkbox"/> Category	Data Centers
<input type="checkbox"/> District	Chennai
<input type="checkbox"/> ASN	AS16509 Amazon.com Inc.

Bots

You can easily lookup an IP address on the below channels using the below commands.

Slack Bot

IP2Location Slack Bot	/ip2location 13.33.146.28
IP2Proxy Slack Bot	/ip2proxy 13.33.146.28

Reddit Bot

IP2Location Reddit Bot	u/ip2location_bot 13.33.146.28
IP2Proxy Reddit Bot	u/ip2proxy_bot 13.33.146.28

Telegram Bot

IP2Location Telegram Bot	ip2location 13.33.146.28
IP2Proxy Telegram Bot	ip2proxy 13.33.146.28

IP Address Notification

Would you like to receive an email notification if the results for the IP address 13.33.146.28 change? Sign up for notification [here](#).

Note

If a computer system or network is linked with the Internet directly, then you cannot hide the IP address and the related information such as the hosting company, its location, ISP, etc. If you have a server containing very sensitive data, then it is recommended to keep it behind a secure proxy so that hackers cannot get the exact details of your actual server. This way, it will be difficult for any potential hacker to reach your server directly.

Another effective way of hiding your system IP and, ultimately, all the associated information is to go through a Virtual Private Network (VPN). If you configure a VPN, then the whole traffic routes through the VPN network, so your true IP address assigned by your ISP is always hidden.

IP Address Ranges

Small sites may have a single IP address associated with them, but larger websites usually have multiple IP addresses serving different domains and sub-domains.

You can obtain a range of IP addresses assigned to a particular company using the American Registry for Internet Numbers (ARIN).



History of the Website

It is very easy to get a complete history of any website using www.archive.org



Fingerprinting

The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be –

Active Fingerprinting – Active fingerprinting is accomplished by sending specially crafted packets to a target machine, noting its response, and analyzing the gathered information to determine the target OS. In the following section, we have given an example to explain how you can use the NMAP tool to detect the OS of a target domain.

Passive Fingerprinting – Passive fingerprinting is based on sniffer traces from the remote system. Based on the packets' sniffer traces (such as Wireshark), you can determine the remote host's operating system.

Fingerprinting

We have the following four important elements that we will look at to determine the operating system –

TTL – What the operating system sets the Time-To-Live on the outbound packet.

Window Size – What the operating system sets the Window Size at.

DF – Does the operating system set the Don't Fragment bit.

TOS – Does the operating system set the Type of Service, and if so, at what.

Basic Steps

Before attacking a system, it is required that you know what operating system is hosting a website. Once a target OS is known, it becomes easy to determine which vulnerabilities might be present to exploit the target system.

```
nmap -O -v manipal.edu
```

Port scanning

```
nmap -sT -p 443 manipal.edu
```

Ping Sweep

A ping sweep is a network scanning technique that you can use to determine which IP address from a range of IP addresses maps to live hosts. Ping Sweep is also known as ICMP Sweep.

You can use the `fping` command for ping sweep. This command is a ping-like program that uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up.

`fping` is different from `ping` in that you can specify any number of hosts on the command line or specify a file containing the lists of hosts to ping. If a host does not respond within a certain time limit and/or retry limit, it will be considered unreachable.

Note

To disable ping sweeps on a network, you can block ICMP ECHO requests from outside sources. This can be done using the following command, which will create a firewall rule in iptable.

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

DNS Enumeration

Domain Name Server (DNS) is like a map or an address book. In fact, it is like a distributed database that is used to translate an IP address 192.111.1.120 to a name www.example.com and vice versa.

DNS enumeration is locating all the DNS servers and their corresponding records for an organization. The idea is to gather as much interesting details as possible about your target before initiating an attack.

You can use the nslookup command on Linux to get DNS and host-related information. In addition, you can use the following DNSenum script to get detailed information about a domain –

DNSenum.pl

Ethical Hacking - Sniffing

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools.

It is a form of “tapping phone wires” and getting to know about the conversation. It is also called wiretapping applied to computer networks.

Sniffing allows you to see all sorts of protected and unprotected traffic.

In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

DNS Enumeration

DNSenum script can perform the following important operations –

Get the host's addresses

Get the nameservers

Get the MX record

Perform axfr queries on nameservers.

Get extra names and subdomains via Google scraping

Brute force subdomains from file can also perform recursion on a subdomain that has NSrecords

Calculate C class domain network ranges and perform whois queries on them

Perform reverse lookups on netranges

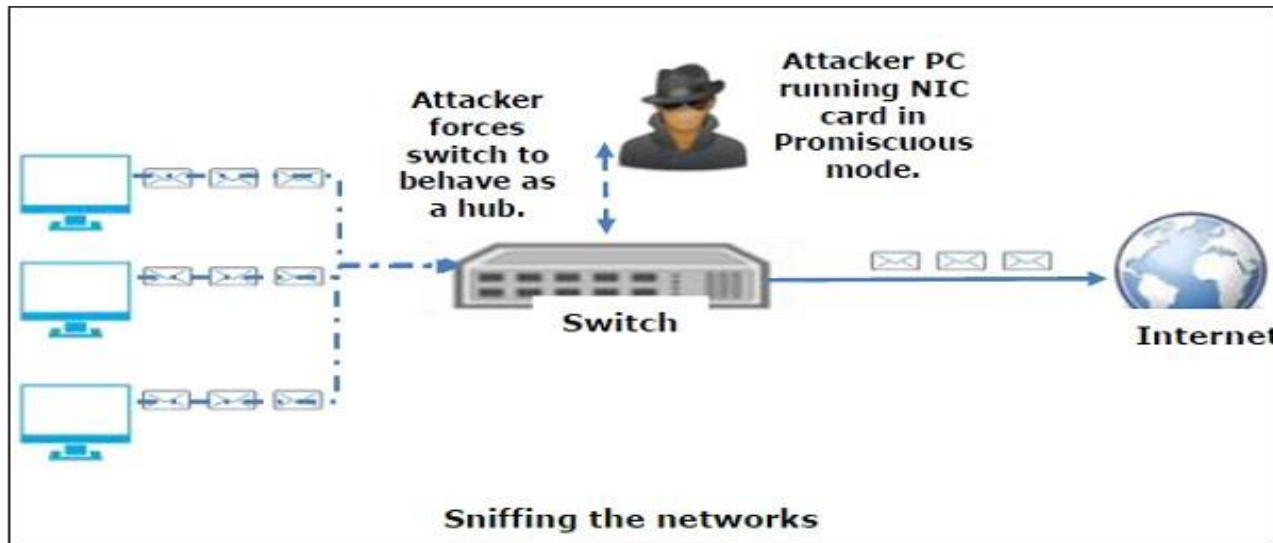
What can be sniffed?

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

How it works

A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, particularly network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC.



Types of Sniffing

Passive Sniffing

In passive sniffing, the traffic is locked but not altered in any way.

Passive sniffing allows listening only. It works with Hub devices.

On a hub device, the traffic is sent to all the ports.

In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

Types of Sniffing

Active Sniffing

In active sniffing, the traffic is locked and monitored and may also be altered in some way as determined by the attack.

Active sniffing is used to sniff a switch-based network.

It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table.

CAM keeps track of which host is connected to which port.

Active Sniffing Techniques

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

Protocols which are affected

HTTP – It is used to send information in clear text without encryption and, thus, a real target.

SMTP (Simple Mail Transfer Protocol) – SMTP is utilized in the transfer of emails. This protocol is efficient but does not include any protection against sniffing.

NNTP (Network News Transfer Protocol)– It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.

POP (Post Office Protocol) – POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.

Protocols which are affected

FTP (File Transfer Protocol) – FTP is used to send and receive files but does not offer any security features. All the data is sent as clear text that can be easily sniffed.

IMAP (Internet Message Access Protocol) – IMAP is the same as SMTP in its functions, but it is highly vulnerable to sniffing.

Telnet – Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and can be easily sniffed.

Hardware Protocol Analyzers

Hardware protocol analyzers monitor and identify malicious network traffic generated by hacking software installed in the system.

They capture a data packet, decode it, and analyze its content according to certain rules.

Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

Lawful Interception

Lawful Interception (LI) is legally sanctioned access to communications network data such as telephone calls or email messages.

LI must always be in pursuance of a lawful authority for analysis or evidence.

LI is a security process in which a network operator or service provider permits law enforcement officials to access the private communications of individuals or organizations.

Sniffing Tools

BetterCAP – BetterCAP is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS, and TCP traffic in real time, sniff for credentials, and much more.

Ettercap – Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly, and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

Sniffing Tools

Wireshark – It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.

Tcpdump – It is a well-known command-line packet analyzer. It allows intercepting and observing TCP/IP and other packets during transmission over the network. Available at www.tcpdump.org.

WinDump – A Windows port of the popular Linux packet sniffer tcpdump, a command-line tool perfect for displaying header information.

OmniPeek – Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.

Sniffing Tools

Dsniff – A suite of tools designed to perform sniffing with different protocols intending to intercept and reveal passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.

EtherApe – It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.

MSN Sniffer is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.

NetWitness NextGen – It includes a hardware-based sniffer, along with other features, designed to monitor and analyze all traffic on a network. The FBI and other law enforcement agencies use this tool.

ARP Poisoning

Address Resolution Protocol (ARP) is a stateless protocol for resolving IP addresses to machine MAC addresses.

All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses.

ARP Poisoning is also known as ARP Spoofing.

How ARP works

When one machine needs to communicate with another, it looks up its ARP table.

The ARP_request is broadcast over the network if the MAC address is not found in the table.

All machines on the network will compare this IP address to the MAC address.

If one of the machines in the network identifies this address, it will respond to the ARP_request with its IP and MAC address.

The requesting computer will store the address pair in its ARP table, and communication will take place.

What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine.

ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.

The switch is set in forwarding mode, and after the ARP table is flooded with spoofed responses, the attackers can sniff all network packets.

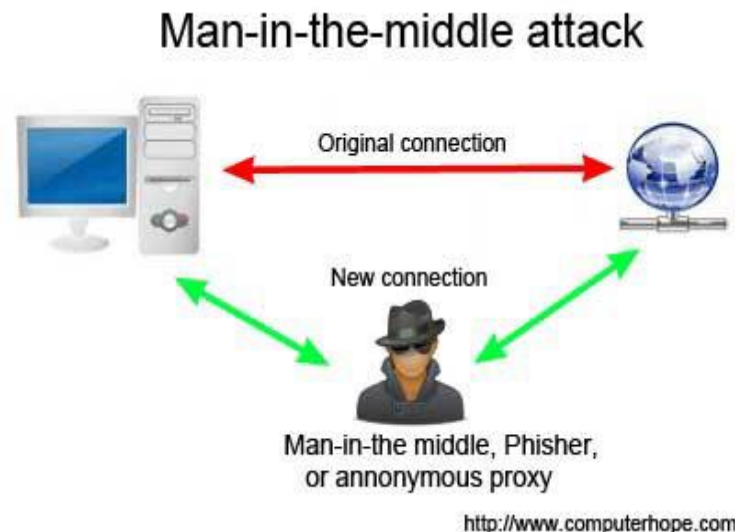
Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning.

ARP poisoning uses Man-in-the-Middle access to poison the network.

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sending messages between them.

In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.



DNS Poisoning

DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not.

It results in the substitution of false IP addresses at the DNS level where web addresses are converted into numeric IP addresses. It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls.

An attacker can create fake DNS entries for the server which may contain malicious content with the same name.

Defenses against DNS Poisoning

Use a hardware-switched network for the most sensitive portions of your network in an effort to isolate traffic to a single segment or collision domain.

Implement IP DHCP Snooping on switches to prevent ARP poisoning and spoofing attacks.

Implement policies to prevent promiscuous mode on network adapters.

Be careful when deploying wireless access points, knowing that all traffic on the wireless network is subject to sniffing.

Encrypt your sensitive traffic using an encrypting protocol such as SSH or IPsec.

Defenses against DNS Poisoning

Port security is used by switches that can be programmed to allow only specific MAC addresses to send and receive data on each port.

IPv6 has security benefits and options that IPv4 does not have.

Replacing protocols such as FTP and Telnet with SSH is an effective defense against sniffing. If SSH is not a viable solution, consider protecting older legacy protocols with IPsec.

Virtual Private Networks (VPNs) can effectively defend against sniffing due to their encryption.

SSL is a great defense, along with IPsec.

.

Social Engineering

Social engineering is a manipulation technique that exploits human error to obtain private information or valuable data.

The human hacking scams entice unsuspecting users **to disclose data, spread malware infections**, or give them access to **restricted systems**.

Attacks can occur **online, in-person**, and by other interactions.

Social engineering scams are based on how people think and act.

Social Engineering

Hackers try to exploit the user's knowledge.

Thanks to technology's speed, many consumers and employees are not aware of specific threats such as drive-by downloads.

Users cannot realize the value of personal data like **phone number**.

Many users are unsure of how best to protect themselves and their confidential information

Goals

Social engineering attackers have two goals:

Subversion: Interrupting or corrupting data due to loss or inconvenience.

Theft: Obtaining valuable items such as **information** or **access**

How does social engineering work?

Most social engineering attacks depend on real communication between attackers and victims.

Instead of using **brute force methods** to breach the data, the attacker prompts the user to compromise.

Social Engineering attack cycle

The attack cycle gives the criminals a reliable process to deceive you.

- Prepare by gathering background information on a large group.
- Infiltrate by building trust, establishing a relationship or starting a conversation.
- Establish the victim once more to confront the attack with confidence and weakness.
- Once the user takes the desired action, release it.

Many employees and consumers are unaware that certain information can give hackers access to **multiple networks** and **accounts**.

By sending messages for IT support personnel as legitimate users, they grab your details - such as **name, date of birth** or **address**.

It is a simple matter to reset the password and get almost unlimited access.

They can steal money, spread social engineering malware, and many more.

Characteristics

Social engineering attack center on the attacker's use of persuasion and confidence.

High emotions: Emotional manipulation gives attackers the upper hand in any conversation. The below feelings are used equally to explain to you.

Fear

excitement

Curiosity

Anger

Crime

Sadness

Time-sensitive occasions or requests are other reliable tools in an attacker's arsenal.

Characteristics

Confidence: Credibility is invaluable and necessary for a social engineering attack. If the attacker is lying to us, confidence plays an important role.

They have done enough research to prepare a narrative for us that is easy to believe and is unlikely to reduce suspicion.

In many cases, attackers use more methods of social engineering to gain network and computer access.

For example, a hacker can often "shoulder surf" a large office building and public food court of users working on their tablet or laptop.

Attackers can hack your passwords and usernames without sending an email or writing a single line of virus code.

Types of Social Engineering Attacks

Phishing Attacks

Phishing attackers pretend to a trusted institution or person in an attempt to convince you to uncover personal data and valuables. Attacks by using phishing are targeted in two ways:

Spam phishing is a widespread attack for some users. The attacks are non-personal and try to capture any irresponsible person.

Phishing and **whaling** use personal information to target particular users. The whaling attacks are aimed at high-profile individuals such as celebrities, upper management and higher government officials.

Whether it is direct communication or by a fake website, anything you share goes directly into the **seamster's pocket**.

You can also be fooled into the next stage of the phishing attack malware download. The methods used in phishing are unique methods of delivery.

Voice phishing (Wishing) phone calls can be an automated messaging system recording all your inputs. The person can speak with you to build trust.

SMS phishing (SMS) texts or mobile app messages may indicate a web link or follow-up via a web link or phone number. A web link, phone number, or malware attachment may be used.

Angler phishing takes place on social media, where the attacker mimics the customer service team of a trusted company. They interrupt your communication with a brand and turn the conversations into private messages, where they escalate the attack.

Search engine phishing attempts to place links to fake websites at the top of any search results.

The advertisements will be paid or use valid optimization methods to manipulate search rankings.

The links are given in **email, text, social media messages** and **online advertisements**.

In-session phishing appears as an interruption to the **normal web browsing**.

For example, you can see fake **pop-ups** on the webpages you are currently viewing.



Baiting Attack

Baiting abuses your natural curiosity of exposing yourself as an attacker. The potential for something exclusive is used to exploit us. An attack involves infecting us with malware. Popular methods of baiting are:

USB drives are left in public places, such as libraries and parking lots.

Email attachment with details with free offer.

Physical Breach Attack

Physical violations include attackers, who would otherwise present themselves as legitimate to access unauthorized areas or information.

This type of attack is common in enterprise environments, like the **government, businesses, or other organizations**.

Attackers pretend to be a representative of a trusted vendor for the company. Some attackers may have recently been fired in retaliation against their former employers.

They obscure their identity but are reliable enough to avoid questions. It requires little research on the part of the attacker and involves high risk.



Preceding Attack: Trusting uses a misleading identity as a "trust" to establish trusts, such as applying directly to a vendor or facility employee.

The approach requires the attacker to interact with you more actively. Once exploited, they are convinced that you are legitimate.


Access tailgating attack: Tailgating or piggybacking is the act of **trapping** any authorized staff member in a **restricted-access area**.

Quid pro quo Attack

The term quid pro quo roughly means "**a favor for a favor**," which refers to exchanging your information for some reward or other compensation in exchange for phishing.

Offer to participate in giveaways or research studies may make you aware of this type of attack.

Exploitation comes from making you happy for something valuable that comes with little investment on your end. However, the attacker does not reward your data for you.



DNS Spoofing and Cash Poisoning Attack

DNS spoofing manipulates your browser and web server to visit malicious websites when you enter a valid URL.

DNS cache poisoning attacks infect our device with valid URLs or routing instructions for multiple URLs to connect to fake websites.

Scareware Attack

Scareware is a form of malware that is used to scare you into taking action.

The deceptive malware uses dangerous warnings that report fake **malware infections** or claim that your accounts have been compromised.

Water Hole Attack

Watering hole attacks infect popular web pages with malware to affect multiple users at the same time.

Carefully planning on the part of the attacker is required to find vulnerabilities of the specific sites.

Unusual Social Engineering Methods

Fax-based Phishing: When a bank's customers receive a fake email that claims to be from the bank - asking the customer to confirm their access code - by regular email.

The customer was asked to print out the form in an email, fill in their details and fax the form to the cyber **criminal's** telephone number.

Traditional Mail Malware Delivery: Cybercriminals use a **home-delivery** service to deliver **CDs** infected with **Trojan** spyware in Japan.

The disc was delivered to customers of a Japanese bank. The addresses was firstly stolen from the **bank's database**.

Examples of Social Engineering Attacks

Worm Attack

Cybercriminal aims to get the **user's attention** to the link or infected file - and then allure the user to **click** on it.

In 2000, the Lavalier worm overloaded on the email servers of many companies. The victims received an email inviting them to open an attached love letter. When she opened the attached file, the worm copied all the contacts in the **victim's address book**.

In January 2004, the Mydoom email worm, which appeared on the Internet, used texts that mimicked mail servers' technical messages.

Peer-to-Peer (P2P) Network Attack

P2P networks are used to distribute malware. A worm or any Trojan virus will appear on the **P2P** network; its name will attract attention and allow users to download and launch the file. **For example:**

AIM and AOL Password Hacker.exe

Microsoft CD Key Generator .exe

Play station emulator crack.exe



How to Solve any Social Engineering Attack

To avoid social engineering, you have to practice self-awareness. Always slow down and think before you do anything or react.

Have my feelings increased? When you are particularly curious, scared, or excited, you are less likely to evaluate your actions' results.

If your emotional state is advanced, consider it a red flag.

Did the message come from a valid sender? Carefully inspect email addresses and social media profiles when receiving suspicious messages.

There could be characters that mimic others, such as "torn@example.com" instead of "tom@example.com."

Fake social media profiles that mimic your friend's photo, and many details are also standard.

Has my friend sent me the message? It is always good to ask the sender if they were the actual sender of the message in question.

They can be hacked, and they may not be detected, or someone may impersonate their accounts.

Are attachments or links suspicious? If a link or filename appears unclear or odd in a message, rethinking the entire communication's authenticity.

Besides, consider when the message itself raises an odd reference, time, or other red flags.

Can this person prove his identity? It applies both **in-person** and **online**, as physical violations require that you ignore the attacker's identity.

Ways to Protect From Social Engineering

Secure communication and account management habits

Online communication is where you are insecure. Social media, email and text messages are common goals, but you want to inter-person.

Never click on any email or message link.

Use multi-factor authentication. When only passwords are used to secure them, online accounts are more secure.

Multi-factor authentication adds additional layers to verify its identity at account login.

These "factors" may have biometrics such as **fingerprints** or **facial recognition** or passcodes sent via text message.

Use a strong password. Each of your passwords must be unique and complex. You are using several types of characters, including uppercase, numbers, and symbols.

Also, you can opt for the more extended password option.

You may want to use Password Manager to store and remember them securely to manage all your custom passwords,.

Avoid sharing your schools, pets, place of birth, or other personal details.

You will make it harder for the criminal to crack your account.

Be very conscious of making online friendships.



Secure Network Usage Habits

Compiled online networks may be another point of exploited vulnerability for background research. To avoid you using your data, take protective measures for any network you connect to.

Never let strangers connect to the main **Wi-Fi** At **home** or **workplace**, access to guest Wi-Fi connections should be provided. It allows secure and secure access to your primary encrypted, password-protected connection.

Never let strangers connect to your personal Wi-Fi network. At home or work, access to guest Wi-Fi connections should be provided.

Always use a Virtual Private Network (VPN). VPNs are services that provide you with a private, encrypted "**tunnel**" over the Internet connection.

Protect all the networked devices and services.

Safe Device Use Habits

Protect your mobile phone, tablet and other computer devices with the below points:

Use comprehensive Internet security software. If the social strategy succeeds, malware infection is an expected outcome.

To counter rootkits, Trojans and bots, it is essential to employ high-quality Internet security solutions to eliminate infections and help track their source.

Never keep your devices insecure in public.

Please keep all your software updated as soon as it becomes available. Quick updates give your software the necessary security fixes.

When you skip or delay an update to the operating system or applications, you leave a security holes to target hackers.

Social engineering is dangerous because it relies on human error rather than weaknesses in operating systems.