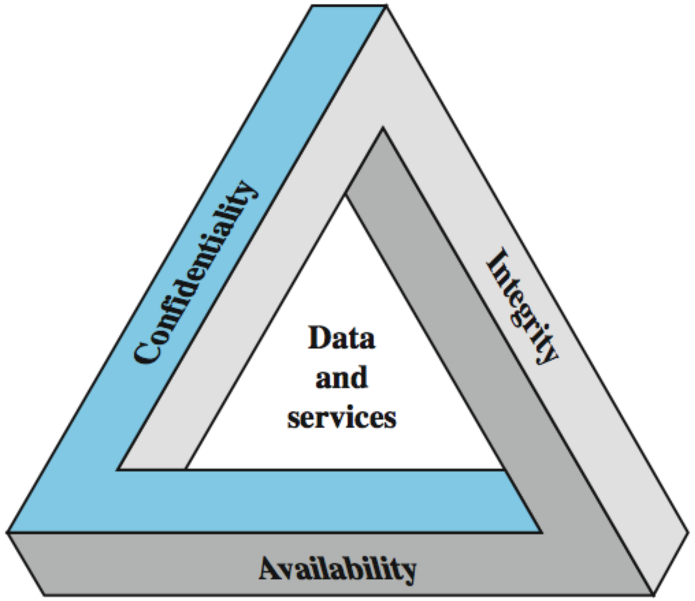
CHAP -1

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

- **Confidentiality** is roughly equivalent to Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- **Availability** means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

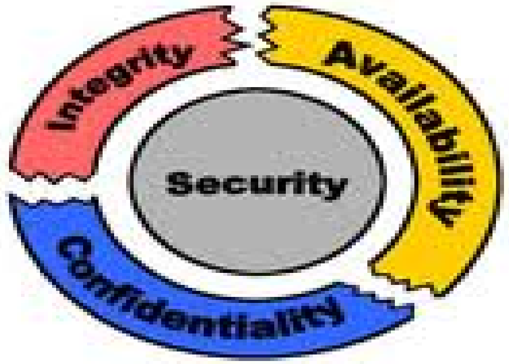


CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **Integrity**
  - **Data integrity**: assures that information and programs are changed only in a specified and authorized manner
  - **System integrity**: Assures that a system performs its operations in unimpaired manner
- **Availability**: assure that systems works promptly and service is not denied to authorized users

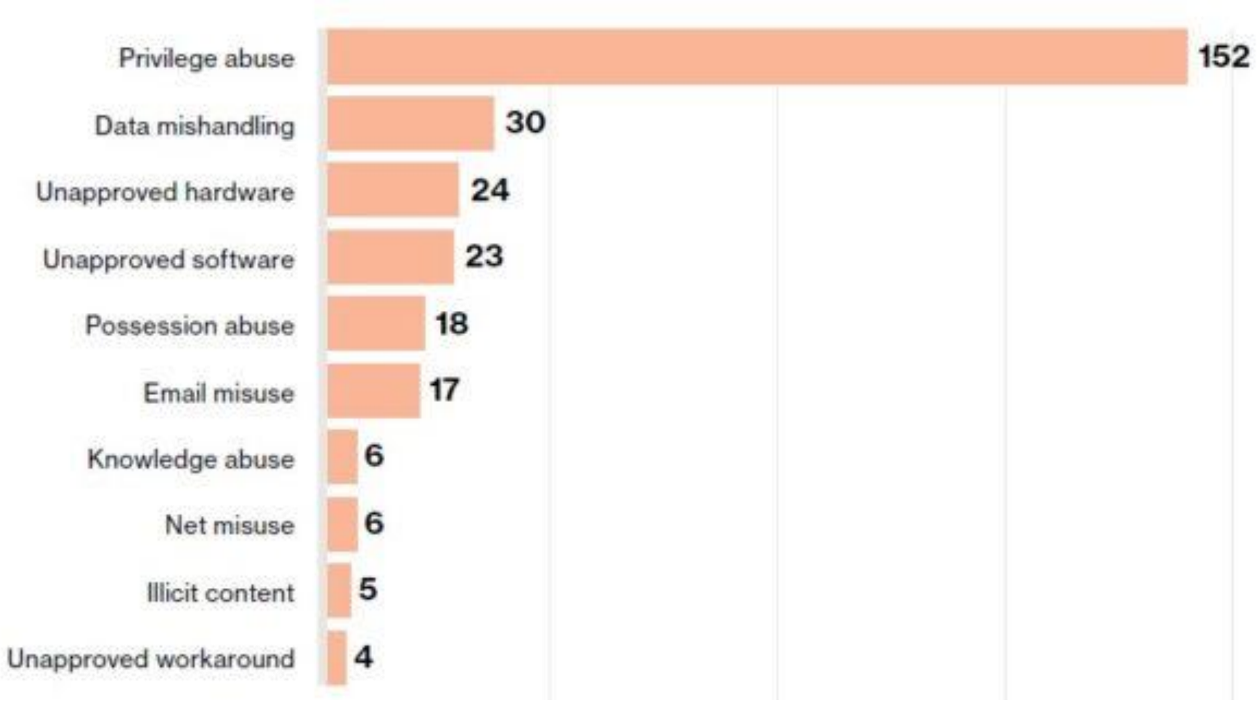
CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

- Confidentiality : Assurance that information is shared only among authorized persons or organizations.
- Integrity : Assurance that the information is authentic and complete. Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
- Availability : Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.



CYBERSECURITY RISK

- Cybersecurity risk is the probability of exposure, loss of critical assets and sensitive information, or reputational harm as a result of a cyber attack or breach within an organization's network. Across industries, cybersecurity must remain top of mind and organizations should work to implement a cybersecurity risk management strategy to protect against constantly advancing and evolving cyber threats.



WHAT IS A DATA BREACH?

- To define data breach: a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission.
- Anyone can be at risk of a data breach — from individuals to high-level enterprises and governments. More importantly, anyone can put others at risk if they are not protected.
- In general, data breaches happen due to weaknesses in:
  - Technology
  - User behavior

VULNERABILITY

- A vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system.
- Vulnerabilities are classified according to the asset class they are related to:-
  - **Hardware**:- Susceptibility to humidity/dust ; Unprotected storage; Over-heating.
  - **Software**:- Insufficient testing; insecure coding; lack of audit trail; Design flaw.
  - **Network**:- Unprotected communication lines; Insecure network architecture.
  - **Personnel**:- Inadequate recruiting process; Inadequate security awareness; insider threat
  - **Physical site:-** Area subject to natural disasters (e.g. flood, earthquake); interruption to power source
  - **Organizational**:- Lack of regular audits; lack of continuity plans;

THREATS

- A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber threats can originate from various actors, including corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers and disgruntled employees.
- A threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.
- Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
- A countermeasure is any step you take to ward off a threat to protect user, data, or computer from harm.
- Various Security threats:-
  - **Users**:- Identity Theft; Loss of Privacy; Exposure to Spam; Physical Injuries.
  - **Hardware**:- Power-related problems; theft; vandalism; and natural disasters.
  - **Data**:- Malwares; Hacking; Cybercrime; and Cyber-terrorism.

THREATS

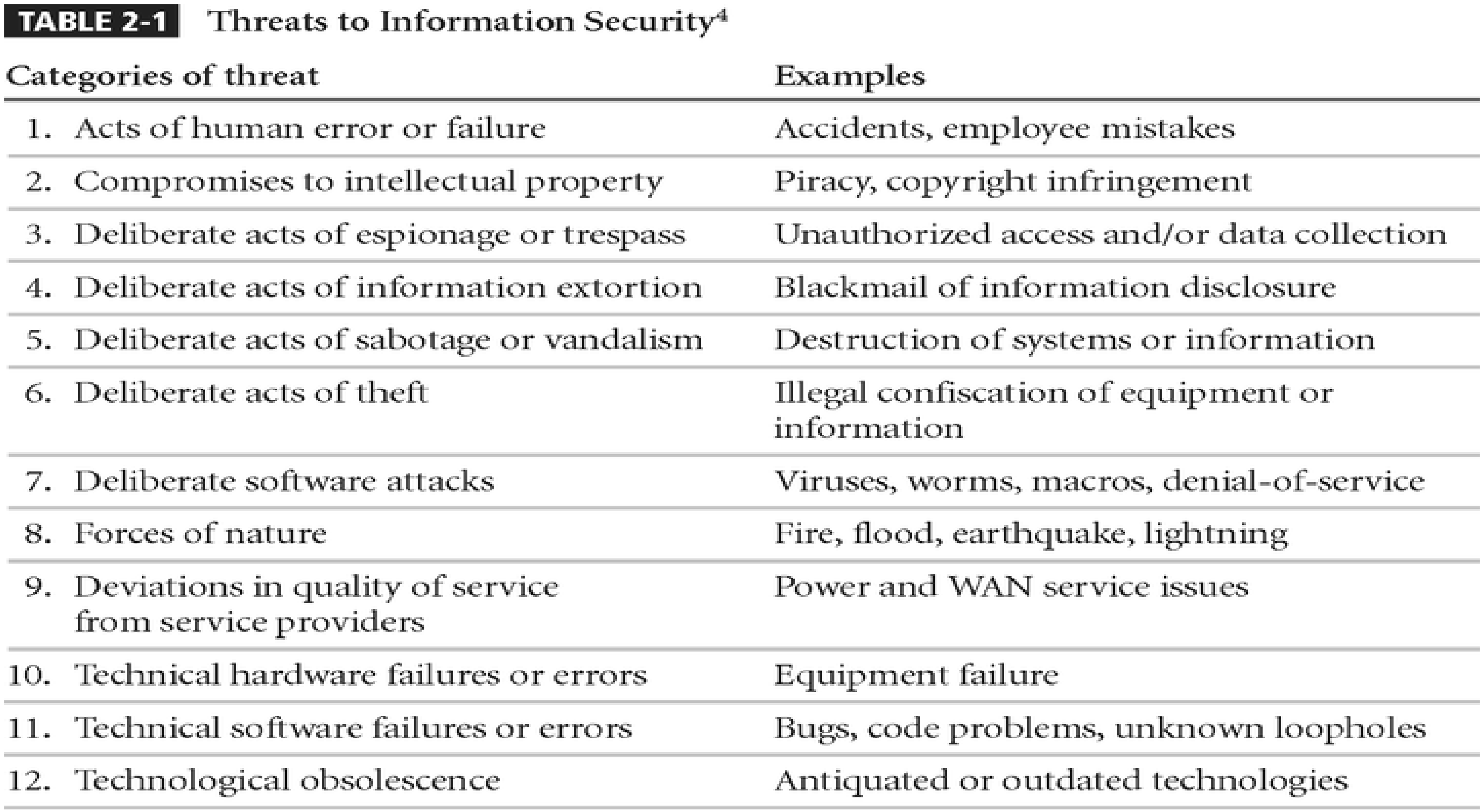


TABLE 2-1 Threats to Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

ATTACKS

- A cyber attack is an attempt to disable computers, steal data, or use a breached computer system to launch additional attacks. Cybercriminals use different methods to launch a cyber attack that includes malware, phishing, ransomware, man-in-the-middle attack, or other methods.
- A cyber attack is any attempt to gain unauthorized access to a computer, computing system.
- A cyber attack is a set of actions performed by threat actors, who try to gain unauthorized access, steal data or cause damage to computers, computer networks, or other computing systems. A cyber attack can be launched from any location. The attack can be performed by an individual or a group using one or more tactics, techniques and procedures (TTPs).

EXPLOIT

- An exploit is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations. When used, exploits allow an intruder to remotely access a network and gain elevated privileges, or move deeper into the network.
- In some cases, an exploit can be used as part of a multi-component attack. Instead of using a malicious file, the exploit may instead drop another malware, which can include backdoor Trojans and spyware that can steal user information from the infected systems.

Types of Attacks and Threats

MALWARE

1. **Malware -** is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:

- Blocks access to key components of the network (ransomware)
- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable

MALWARE

- Malware is so common that there is a large variety of modus operandi. The most common types being:

- **Viruses**—these infect applications attaching themselves to the initialization sequence. The virus replicates itself, infecting other code in the computer system. Viruses can also attach themselves to executable code or associate themselves with a file by creating a virus file with the same name but with an .exe extension, thus creating a decoy which carries the virus.

- **Trojans**—a program hiding inside a useful program with malicious purposes. Unlike viruses, a trojan doesn't replicate itself and it is commonly used to establish a backdoor to be exploited by attackers.

MALWARE

- **Worms**—unlike viruses, they don’t attack the host, being self-contained programs that propagate across networks and computers. Worms are often installed through email attachments, sending a copy of themselves to every contact in the infected computer email list. They are commonly used to overload an email server and achieve a denial-of-service attack.
- **Ransomware**—a type of malware that denies access to the victim data, threatening to publish or delete it unless a ransom is paid. Advanced ransomware uses cryptoviral extortion, encrypting the victim’s data so that it is impossible to decrypt without the decryption key.

MALWARE

- **Spyware**—a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user. The attacker can then use the information for blackmailing purposes or download and install other malicious programs from the web.

PHISHING

- Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information. Phishing is a common type of cyber attack that everyone should learn about in order to protect themselves.
- Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine. Phishing is an increasingly common cyberthreat.

MAN-IN-THE-MIDDLE (MITM)

- Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- Two common points of entry for MitM attacks:
- 1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor’s device and the network. Without knowing, the visitor passes all information through the attacker.
- 2. Once malware has breached a device, an attacker can install software to process all of the victim’s information.

DENIAL-OF-SERVICE ATTACK

- A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.
- DOS attacks work by flooding systems, servers, and/or networks with traffic to overload resources and bandwidth. This result is rendering the system unable to process and fulfill legitimate requests. In addition to denial-of-service (DoS) attacks, there are also distributed denial-of-service (DDoS) attacks.
- DoS attacks saturate a system's resources with the goal of impeding response to service requests. On the other hand, a DDoS attack is launched from several infected host machines with the goal of achieving service denial and taking a system offline, thus paving the way for another attack to enter the network/environment.

SQL INJECTION

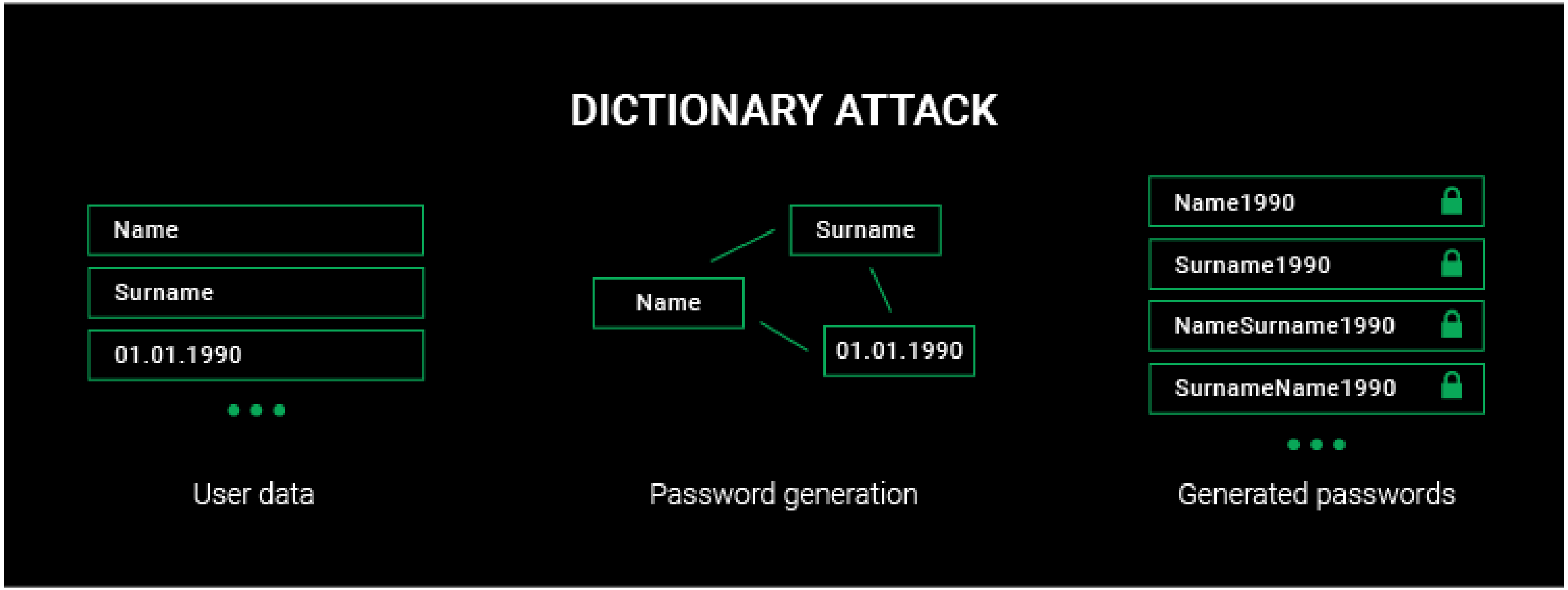
- A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.
- This occurs when an attacker inserts malicious code into a server using server query language (SQL) forcing the server to deliver protected information. This type of attack usually involves submitting malicious code into an unprotected website comment or search box. Secure coding practices such as using prepared statements with parameterized queries is an effective way to prevent SQL injections. When a SQL command uses a parameter instead of inserting the values directly, it can allow the backend to run malicious queries. Moreover, the SQL interpreter uses the parameter only as data, without executing it as a code.

PASSWORD ATTACK (BRUTE-FORCE ATTACK)

- Passwords are the most widespread method of authenticating access to a secure information system, making them an attractive target for cyber attackers. By accessing a person's password, an attacker can gain entry to confidential or critical data and systems, including the ability to maniuplate and control said data/systems.
- Password attackers use a myriad of methods to identify an individual password, including using social engineering, gaining access to a password database, testing the network connection to obtain unencrypted passwords, or simply by guessing.
- The last method mentioned is executed in a systematic manner known as a "brute-force attack." A brute-force attack employs a program to try all the possible variants and combinations of information to guess the password.

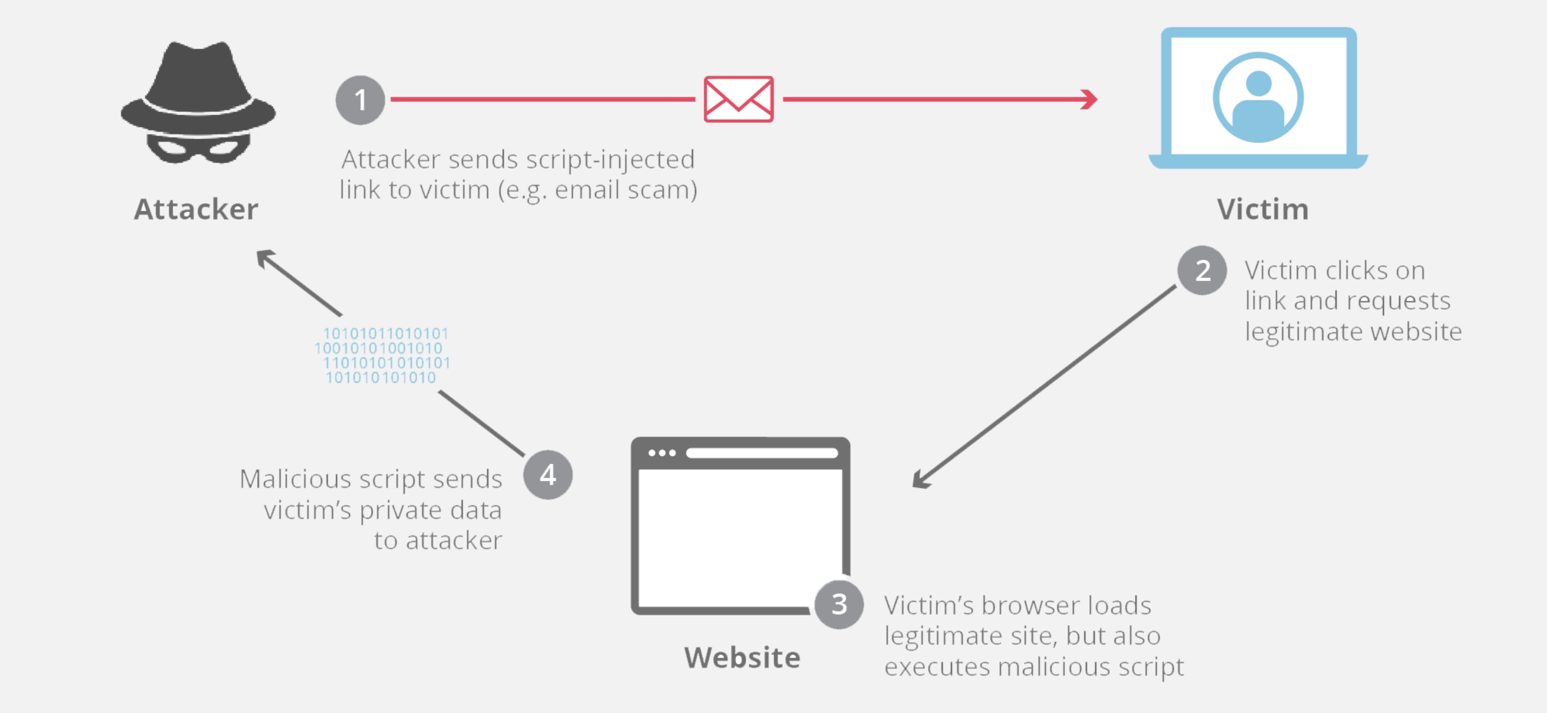
DICTIONARY ATTACKS

- This type of attack stored the list of a commonly used password and validated them to get original password.



CROSS-SITE SCRIPTING

- A cross-site scripting attack sends malicious scripts into content from reliable websites. The malicious code joins the dynamic content that is sent to the victim’s browser. Usually, this malicious code consists of Javascript code executed by the victim’s browser, but can include Flash, HTML and XSS.



1 Attacker sends script-injected link to victim (e.g. email scam)

2 Victim clicks on link and requests legitimate website

3 Victim’s browser loads legitimate site, but also executes malicious script

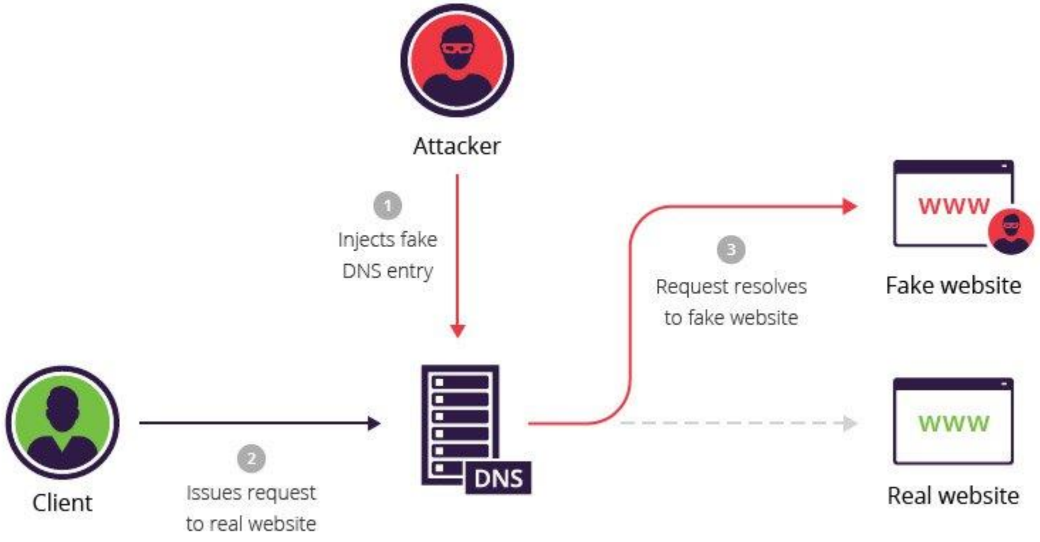
4 Malicious script sends victim’s private data to attacker

ROOTKITS

- Rootkits are installed inside legitimate software, where they can gain remote control and administration-level access over a system. The attacker then uses the rootkit to steal passwords, keys, credentials, and retrieve critical data.
- Since rootkits hide in legitimate software, once you allow the program to make changes in your OS, the rootkit installs itself in the system (host, computer, server, etc.) and remains dormant until the attacker activates it or it's triggered through a persistence mechanism. Rootkits are commonly spread through email attachments and downloads from insecure websites.

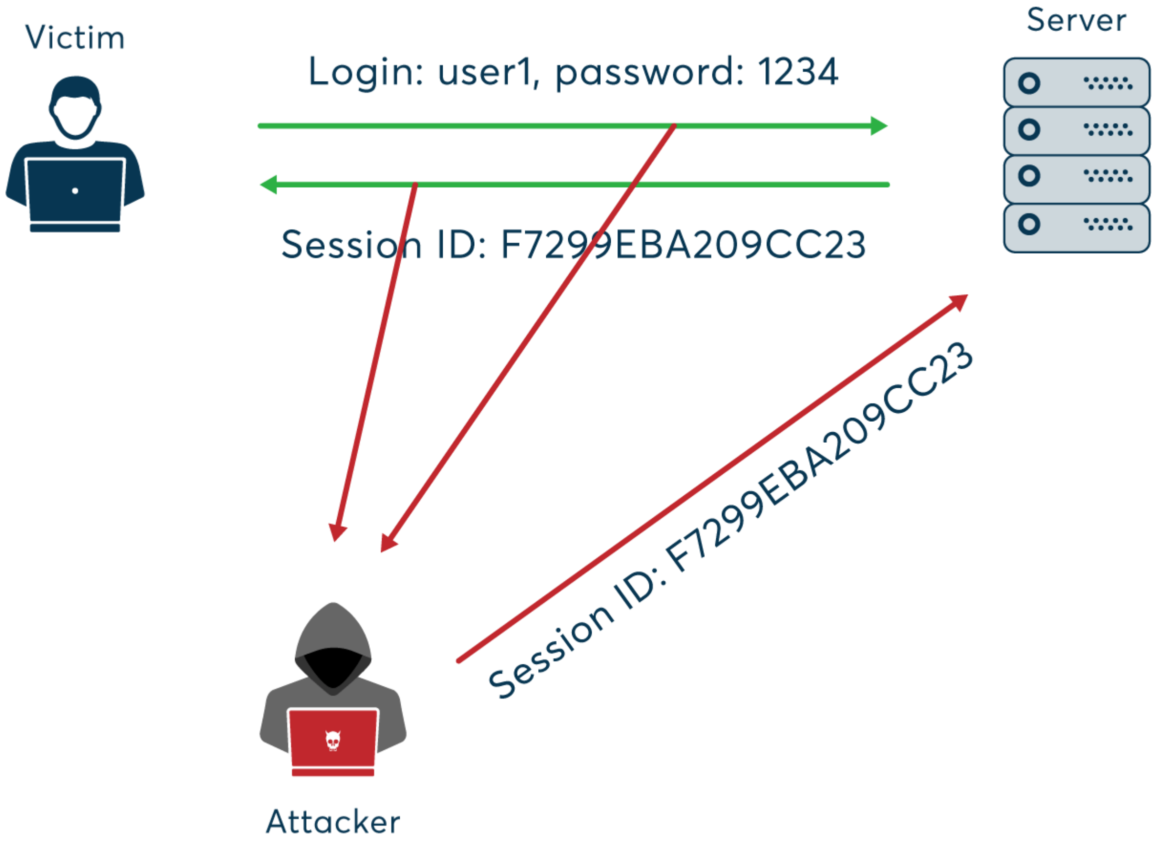
DNS SPOOFING

- Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.
- DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.



SESSION HIJACKING

- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.


Victim
Server
Login: user1, password: 1234
Session ID: F7299EBA209CC23
Session ID: F7299EBA209CC23
Attacker

URL INTERPRETATION AND FILE INCLUSION ATTACKS

- **URL Interpretation**
  - It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
  - The URL (Uniform Resource Locator) of a web application is the vector that makes it possible to indicate the requested resource. This article will show you how to protect yourself against URL manipulation attacks.
- **File Inclusion attacks**
  - A file inclusion vulnerability allows an attacker to access unauthorized or sensitive files available on the web server or to execute malicious files on the web server by making use of the 'include' functionality.
  - It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

FOOTPRINTING

- **Footprinting** means gathering information about a target system which can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system. There are two types of footprinting as following below.

1. **Active Footprinting:**
   Active footprinting means to perform footprinting by getting in direct touch with the target machine.
2. **Passive Footprinting:**
   Passive foot printing means collecting information of a system located at a remote distance from the attacker.

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

FOOTPRINTING

- **During this phase, a hacker can collect the following information −**
  - Domain name
  - IP Addresses
  - Namespaces
  - Employee information
  - Phone numbers
  - E-mails
  - Job Information

SOURCES OF FOOTPRINTING

1. **Social Media:**
   Most people has the tendency to release most of their information online. Hackers use this sensitive information in a big deal. They may create a fake account for looking real to be added as friend or to follow someone's account for grabbing their information.

2. **JOB websites:**
   Organizations share some confidential data in many JOB websites like monsterindia.com. For example, a company posted on a website : "Job Opening for lighttpd 2.0 Server Administrator". From this information can be gathered that an organization uses lighttpd web server of version 2.0 .

SOURCES OF FOOTPRINTING

3. Social Engineering:
There are various techniques that fall in this category. A few of them are:

1. **Eavesdropping –** Attacker tries to record personal conversation of the target victim with someone that's being held over communication mediums like Telephone.
2. **Shoulder Surfing –** In this technique Attacker tries to catch the personal information like Email id, password, etc; of the victim by looking over the victim's shoulder while the same is entering(typing/writing) his/her personal details for some work.

SOURCES OF FOOTPRINTING

4. Archive.org:
Archived version refers to the older version of the website which existed in a time before and many features of the website has been changed. archive.org is a website that collects snapshots of all the website at a regular interval of time. This site can be used to get some information that does not exist now but existed before on the site.

5. Using Neo Trace:
NeoTrace is a powerful tool for getting path information. The graphical display displays the route between you and the remote site, including all intermediate nodes and their information. NeoTrace is a well-known GUI route tracer program. Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.

SOURCES OF FOOTPRINTING

6. Who is:

This is a website which serves a good purpose for Hackers. Through this website information about the domain name, email-id, domain owner, etc; a website can be traced. Basically, this serves a way for Website Footprinting.

NMAP

- Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

PORT SCANNER

- Network scanning helps in assessing the complete IT infrastructure of an organization to identify existing loopholes and susceptibilities. Thorough scanning of the network helps quantify the risks and plan out the remediation process to address the issue.
- In other words, network scanning is important for the health of the network. It covers all devices, connecting points, filtering systems, active hosts, OS systems, and traffic. It also includes Port scanning, sensing TCP sequence numbers on active hosts, and discover UDP and TCP services on networks. It is always advisable to use advanced and intelligent network scanning tools for optimized results.

NETWORK SCANNERS

- A **port scan** is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system’s firewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

Thank you