Network Security Threats, Vulnerabilities, and Attacks

Module 02

Network Security Threats, Vulnerabilities, and Attacks

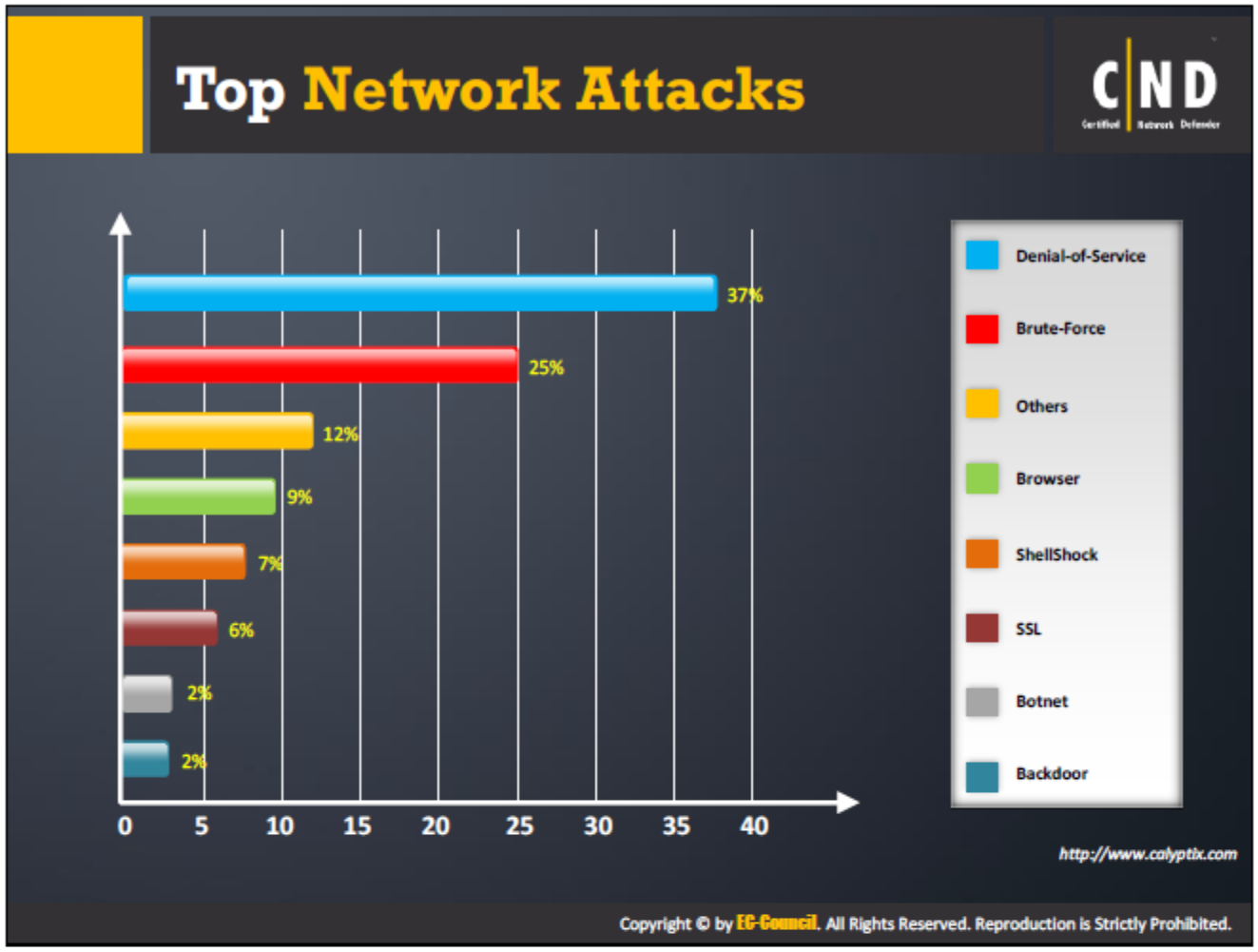
Module 02

C|ND
Certified Network Defender

Certified Network Defender

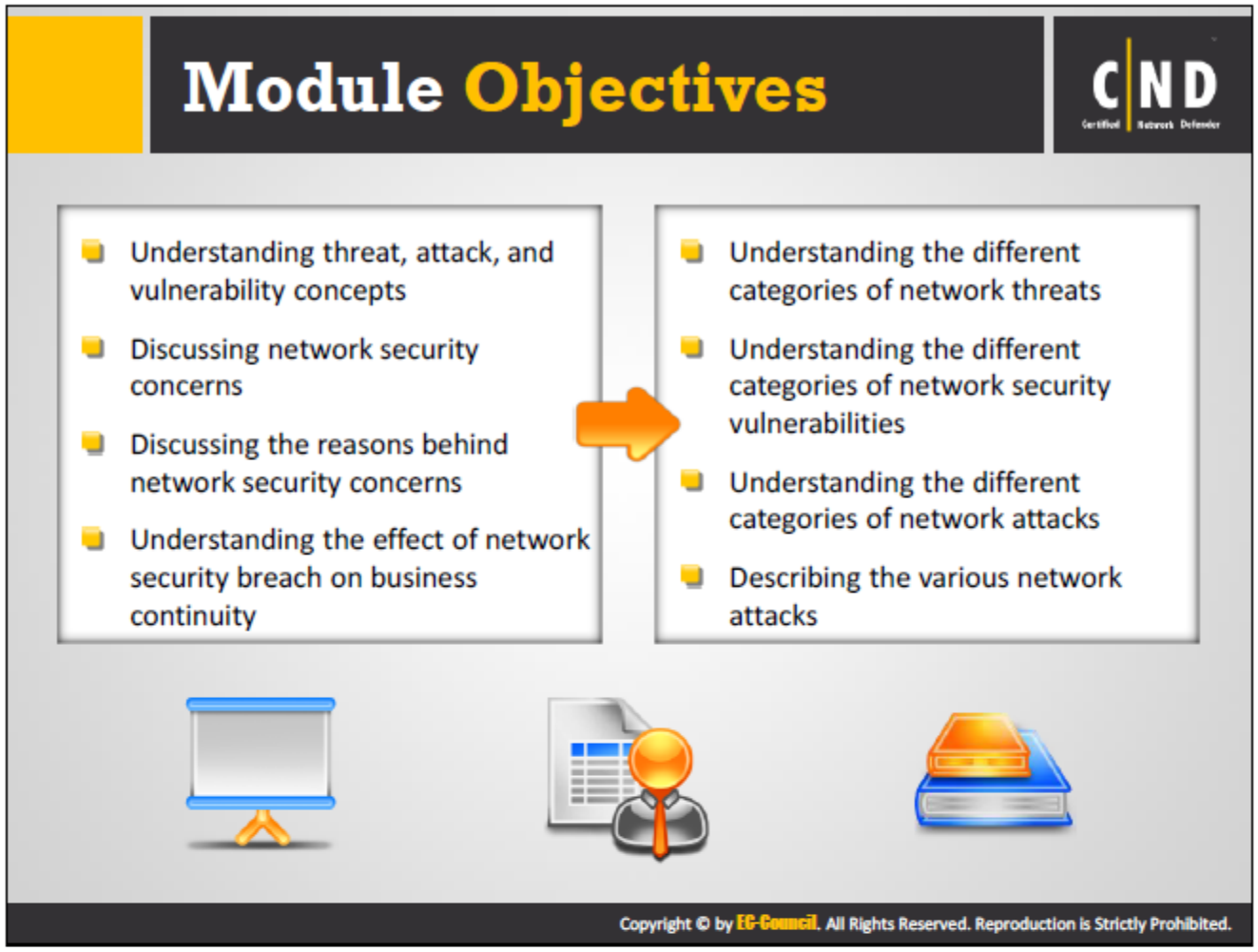
Module 02: Network Security Threats, Vulnerabilities, and Attacks

Exam 312-38

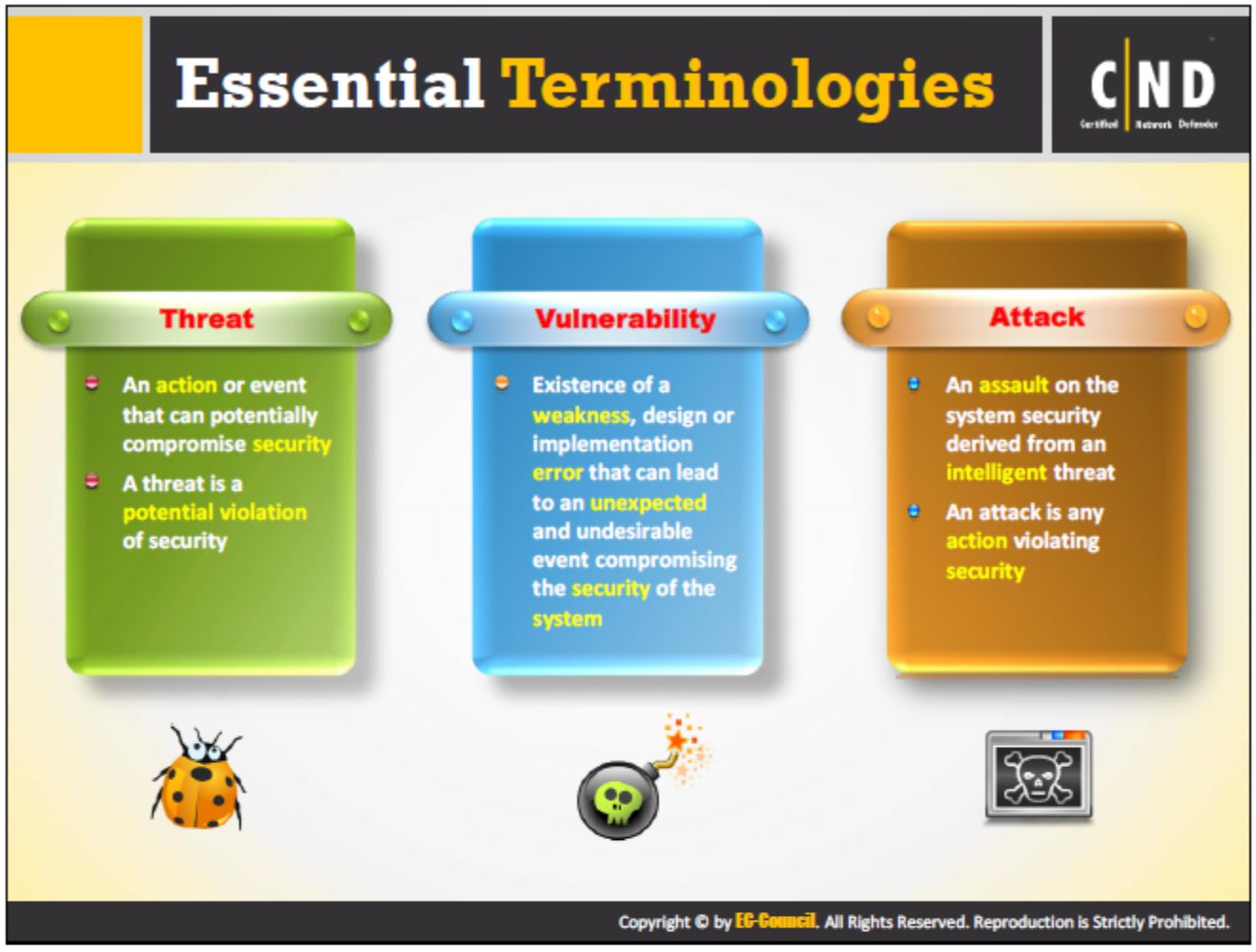


According to the latest Threat Report from McAfee Labs, the statistics for the most common network attacks detected are shown in the chart. The chart aggregates data from the company's network of millions of sensors across the globe. According to the report, Denial of Service attacks (DoS) top the list and is the most targeted attack towards the organization's network. DoS attacks are very common, accounting for more than one-third of all network attacks reviewed in the report. Attempts of brute forcing passwords are also significantly performed to gain unauthorized access to network resources. Browser-based attacks target end users who are browsing the Internet. The attacks may encourage them to unwittingly download malware disguised as a fake software update or application. Malicious and compromised websites can also force malware onto visitor's systems. Attackers are also exploiting vulnerabilities found in Bash, a common command-line shell for Linux and Unix systems in order to install malware that sends spam campaigns and DDoS attacks. SSL attacks aim to intercept data that is sent over an encrypted connection. A successful attack enables access to the unencrypted information. SSL attacks account for 6% of all network attacks analyzed.

Source: *http://www.calyptix.com*



This module discusses the various network threats, vulnerabilities, and attacks that an attacker can carry out to compromise network security. The module will teach you the different types of network threats, why they arise, possible ways through which they come from, etc. The module also discusses the different level of attacks that are carried out against the network and the types of vulnerabilities that exist in the network.



In the field of information security, Internet and computer security people often use the following terms interchangeably: threats, vulnerabilities and attacks. Many people confuse these terms. However, they are different and have a distinct meaning even though they are interrelated. Therefore, it is necessary to understand and differentiate between them.

Threat

Threat is a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization. A threat can affect the integrity and availability factors of an organization. The impact of threats is very high and it can affect the existence of the physical IT assets in an organization. The existence of threats may be accidental, intentional or due to the impact of some other action.

Vulnerability

Vulnerability is the existence of a weakness, design, or implementation error that, when exploited, leads to an unexpected and undesired event compromising the security of the system. Simply put, a vulnerability is a security loophole that allows an attacker to enter the system by bypassing various user authentications.

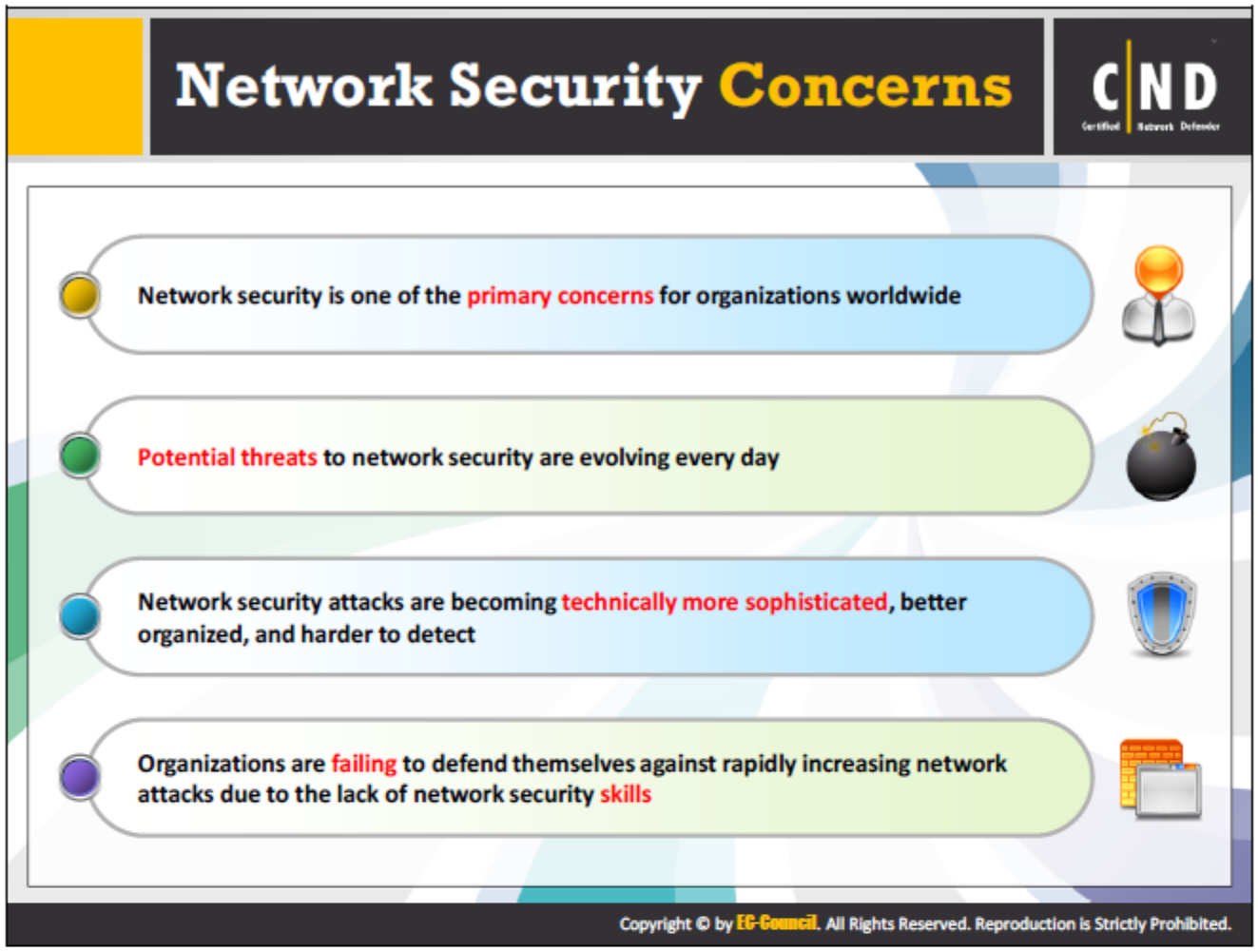
Attack

An attack is an action taken towards breaching an IT system's security through vulnerabilities. In the context of an attack on a system or network. It also refers to malicious software or

commands that can cause an unanticipated behavior of legitimate software or hardware because attackers take advantage of the vulnerabilities.

For example,

- **Threats to Input Validation cause an application to be exploited using:**
  - Buffer overflows
  - Cross-site scripting
  - SQL injection
  - Canonicalization attacks
  - Query string manipulation
  - Form field manipulation
  - Cookie manipulation
  - HTTP header manipulation
- **Vulnerabilities in Input Validation:**
  - Lack of validation on user inputs
  - Use of non-validated user inputs directly to generate SQL queries
  - Relying solely on client-side validation
  - Performing input validation based on known bad patterns
- **Attacks to Input Validation can be:**
  - Exploiting input validation vulnerabilities to perform a Buffer overflow attack, Cross-site scripting attack, SQL injection attack, Canonicalization attacks, Query string manipulation, Cookie manipulation, etc.



The attacks on the network are increasing at a fast rate. Constant attacks in the network is a major issue in the computing world. Organizations are raising funds for securing the network security. Network security concerns affect the availability, confidentiality and integrity of the information present in an organization. Attackers are exploiting loopholes existing in security related technologies. Administrators need to be more vigilant toward the newer attacks that can occur in the network. Network administrators need to categorize the type of attacks occurring in the network.

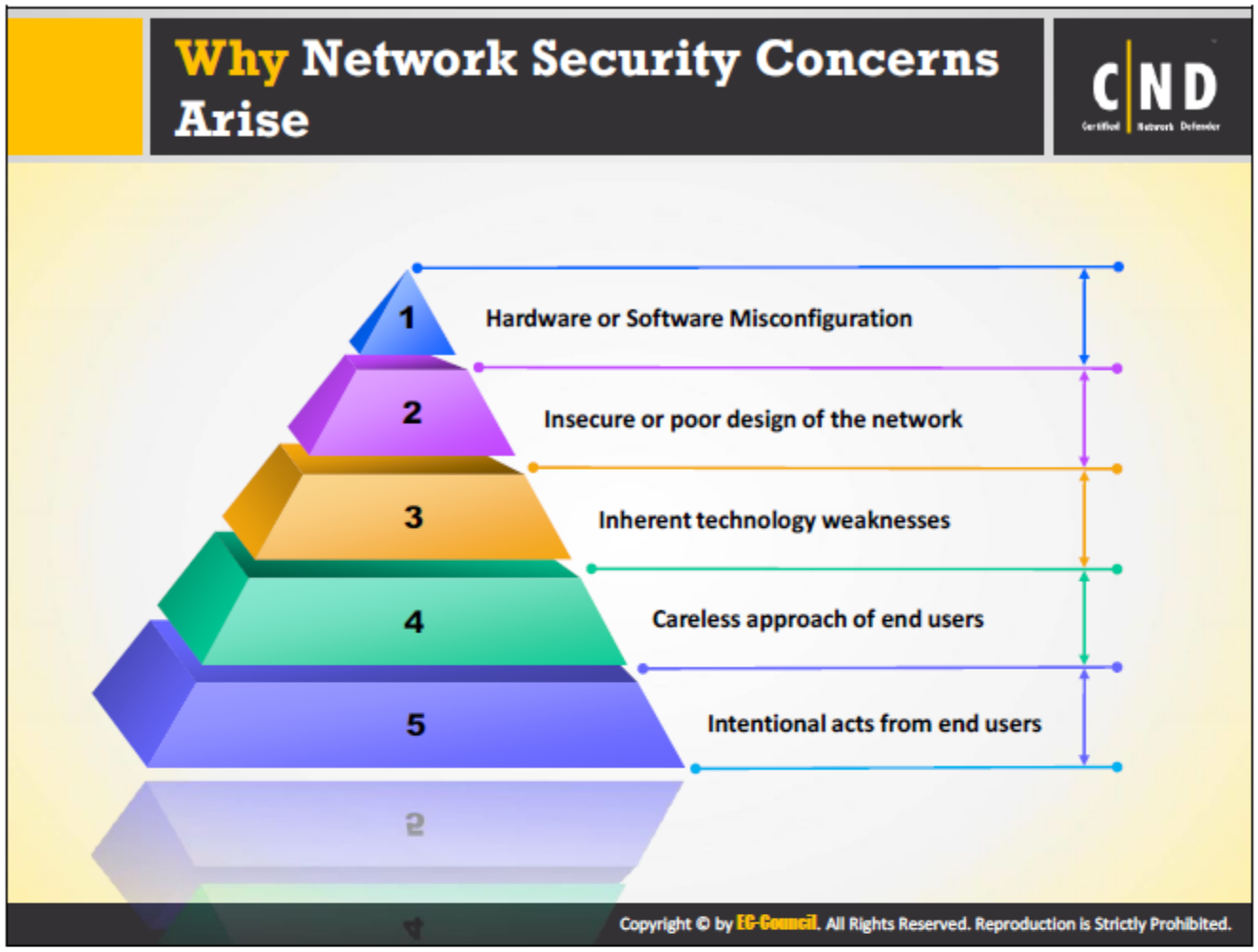
Designing and implementing a network is an easy task, but, maintaining the security of the network is a difficult task. Attackers are using various exploitation tools to gain access to the network and its resources.

The organization's network can also be at risk for different types of attacks from the inside. The employees of an organization can at times pose a threat to the security of the company's network. Insider threats can be more dangerous than external ones.

Attackers perform network attacks to take control of a computer, for curiosity and excitement, for publicity and fame, for financial gains, to spy or corporate espionage, get information about the organization and to disrupt the proper working of an application or service.

The organization needs to implement tasks that monitor and identify the attacks in the network on a daily basis. The sharing of information and resources across the computers in a network can attract intruders wanting to gain access to that information. The organization may consider taking certain protective steps to prevent any kind of unauthorized access to its network.

Administrators can locate the various areas of continuous attacks, thereby assisting the organization in planning for security.



Hardware or software misconfiguration

Security loopholes are created from an insecure configuration of the hardware or software in the network. For example, a misconfigured or the use of an unencrypted protocol may lead to network intrusions resulting in a leak of sensitive information. Misconfiguration of hardware may allow attackers to gain access to the network or system. Misconfiguration of software may allow attackers to gain unauthorized access to the applications and data.

Insecure or poor design of network

An improper and insecure design of the network may incur a variety of threats and the probability of data loss. For example, if firewalls, IDS and virtual private network (VPNs) technologies are not implemented securely they will expose the network to different threats.

Inherent technology weakness

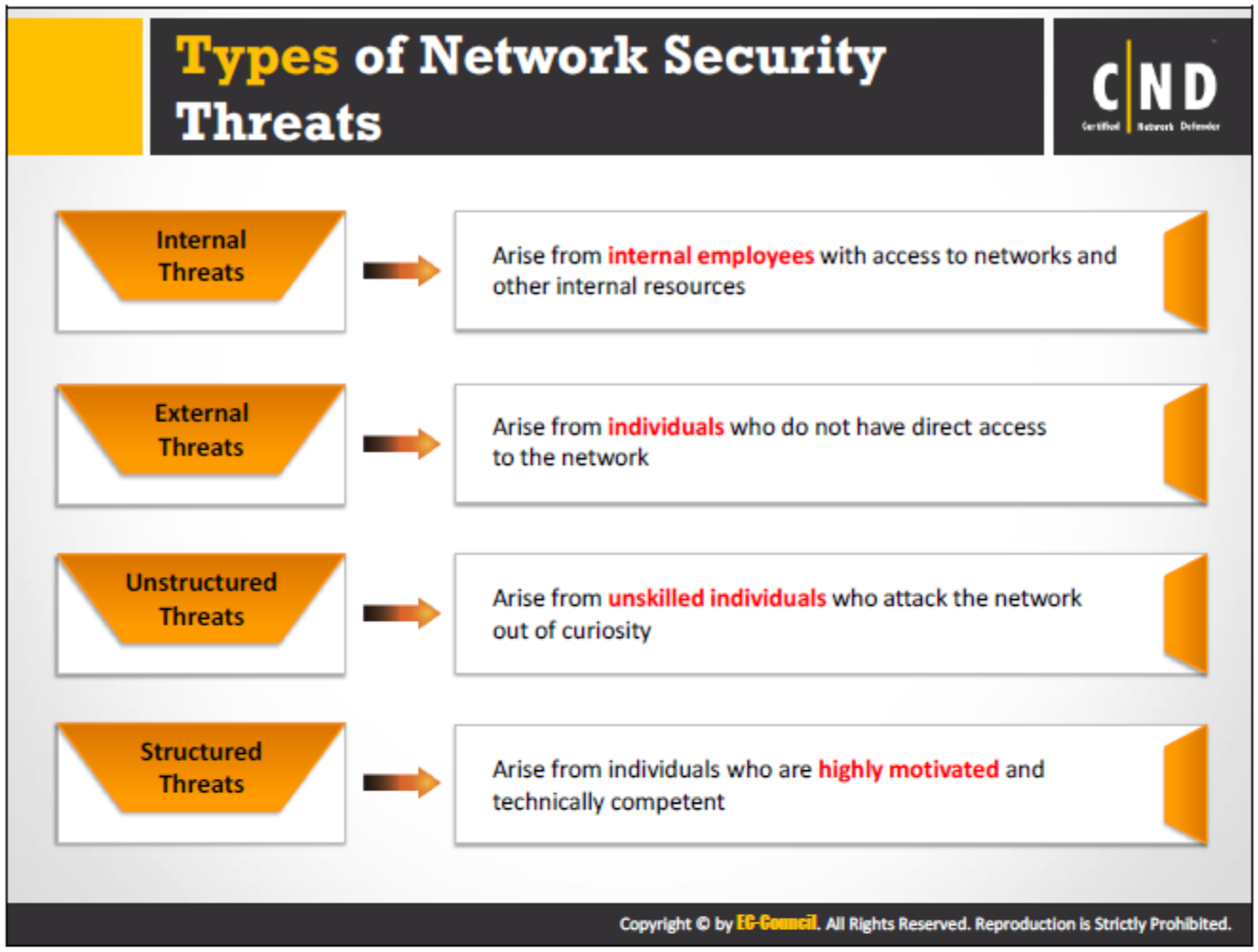
If the hardware or software is not capable of defending the network against certain types of attacks, then it will be vulnerable to those attacks. Many hardware, applications or web browsers are more prone to attacks such as denial-of-service or MITM attacks. If an old version of a web browser is running on the system, those systems have a higher chance of being vulnerable to distributed attacks. If the systems are not updated, a small Trojan attack will force the user to clean the entire machine. Cleaning a machine often leads to data loss.

End-user carelessness

End user carelessness creates a huge impact to network security. Human behavior is more susceptible to various types of attack and tends to lead to more serious attacks on the network including data loss, information leakage, etc. Intruders gain sensitive information through various social engineering techniques. If users share account information or login credentials, this leads to the loss of data or exploitation of the information. Connecting systems to an unsecure network can also lead to attacks from a third party.

Intentional end-user acts

If an ex-employee, still has access to a shared drive, it can be misused to leak the company's sensitive information. This type of act is called an intentional end-user act. Such acts lead to heavy losses to the company and data.



There are basically two types of threats to the network.

- Internal
- External

Internal Threats

Around 80% of the computer and Internet-related crimes are insider attacks. These are performed by insiders within the organization such as disgruntled employees, negligent employees, etc., and harms the organization intentionally or unintentionally (by accident). Most of these attacks are performed by privileged users of the network.

The reasons behind insider attacks could be revenge, disrespect, frustration, or lack of security awareness. Insider attacks are more dangerous compared to external attacks because insiders are familiar with the network architecture, security policies and regulations of the organization. Additionally, the security inside is not has strong because organizations focus on protection from external attacks.

External Threats

External attacks are performed by exploiting vulnerabilities already existing in the network. The attacker does it for the sake of curiosity, financial gain or reputation damage to the target organization. External attackers can be any user who is well-versed with attacking techniques or a group of users who work together to support a cause or political motive, by competitor companies to create corporate espionage, by countries for surveillance, etc. Attackers

performing external attacks have a predefined plan, use specialized tools and techniques to successfully penetrate the network.

The external attack depends on which weakness exists and then it is exploited to perform the attacks. These attacks are performed without the assistance of insider employees. Some of the external attacks include application and virus-based attacks, password-based attacks, instant messaging-based attacks, network traffic-based attacks, and operating system based attacks.

External threats are classified into two types. They are a structured and an unstructured external threat.

Structured External Threat

Structured external threats arise from highly skilled individuals who quickly identify vulnerabilities which exist and can write exploits on their own to compromise the network. These individuals or groups of individuals are often involved in major fraud and theft cases.

Unstructured External Attacks

Unstructured external threats arise from inexperienced individuals who use readily available hacking tools and scripts to perform the attack. This type of attack is generally executed with the intent of testing their hacking skills and poses serious harm to the organization.

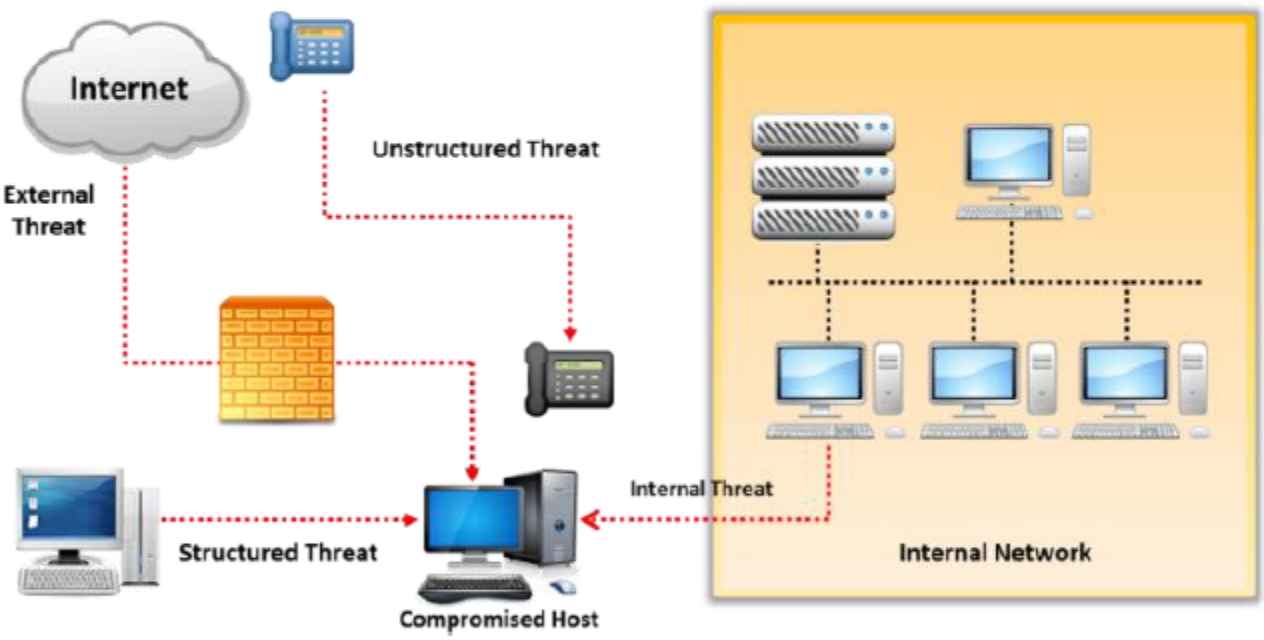
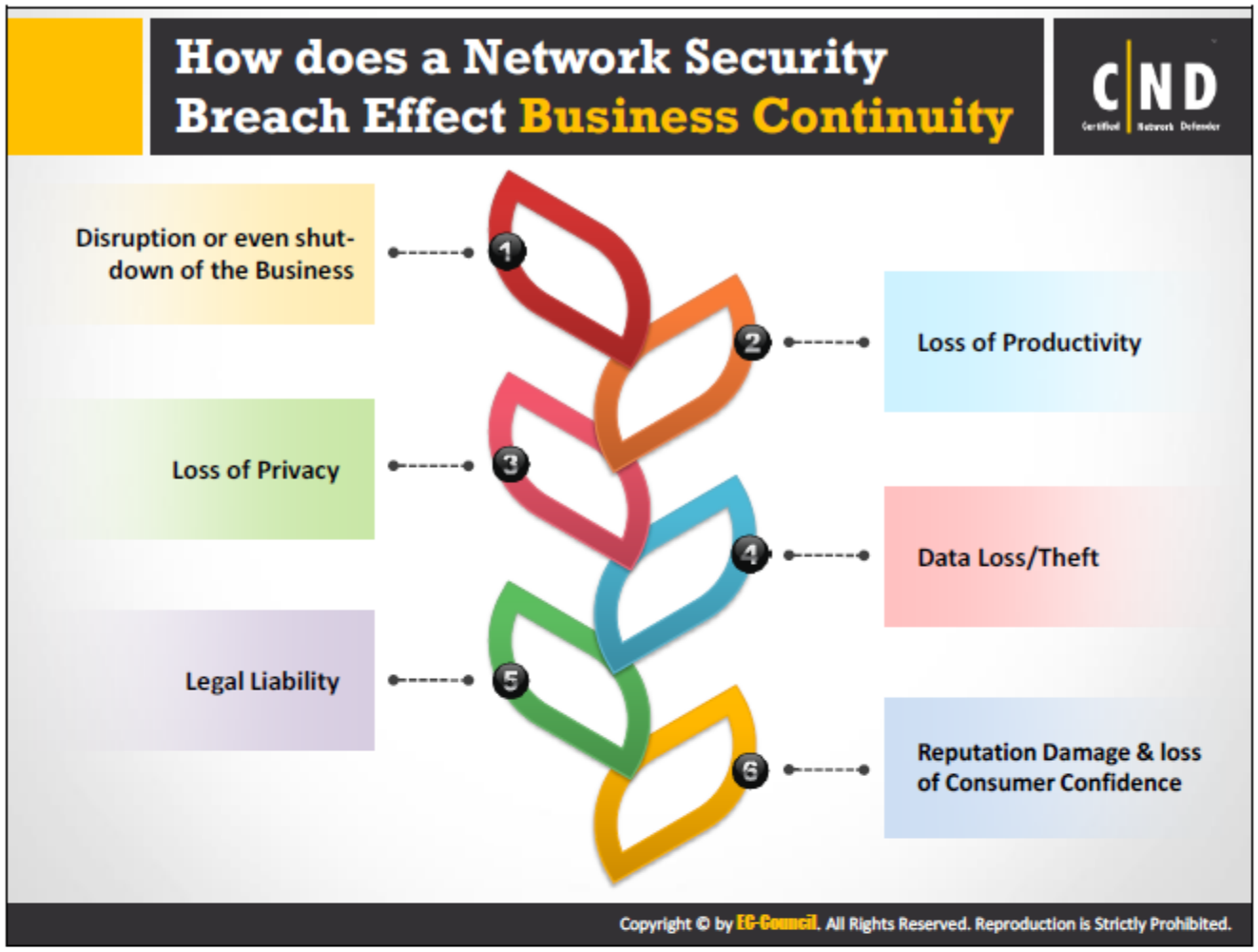


FIGURE 2.1: Different types of network security threats



Disruption of Business

Any type of attack on a business can bring the entire business process to a standstill. The breach in security leads to a loss of critical business and user information.

Loss of Productivity

An exploited business network has to undergo a lot of production losses. The loss incurred due to an attack has to be recovered either through data backups or the user has to rework the data. Recovery of data after a network attack is a time-consuming process.

Loss of Privacy

Due to a leak of all the confidential data, the organization has to face heavy losses of their private data, which also leads to legal issues for them.

Theft of Information

An attack on the network leads to a raid of the information by attackers. A raid of personal and professional information of the company's employees through such attacks affects those employees directly. If the attacks get into a customer database, then their customers are affected and this leads to huge problems.

Legal Liability

A case can be filed against the attackers. These laws differ between countries. With proper evidence of the incident an organization can file a legal lawsuit if their security is breached. The same is true for customers. If their private and personal information is stolen, such as credit card numbers, social security numbers and addresses are stolen, depending on the circumstances, they may also have the right to bring a lawsuit against the company.

Damage to reputation and consumer confidence

Once an attack has been detected and identified on an organization, it is difficult to gain customer confidence again. The reputation of the organization is at stake.

Types of Network Security Vulnerabilities: Technological

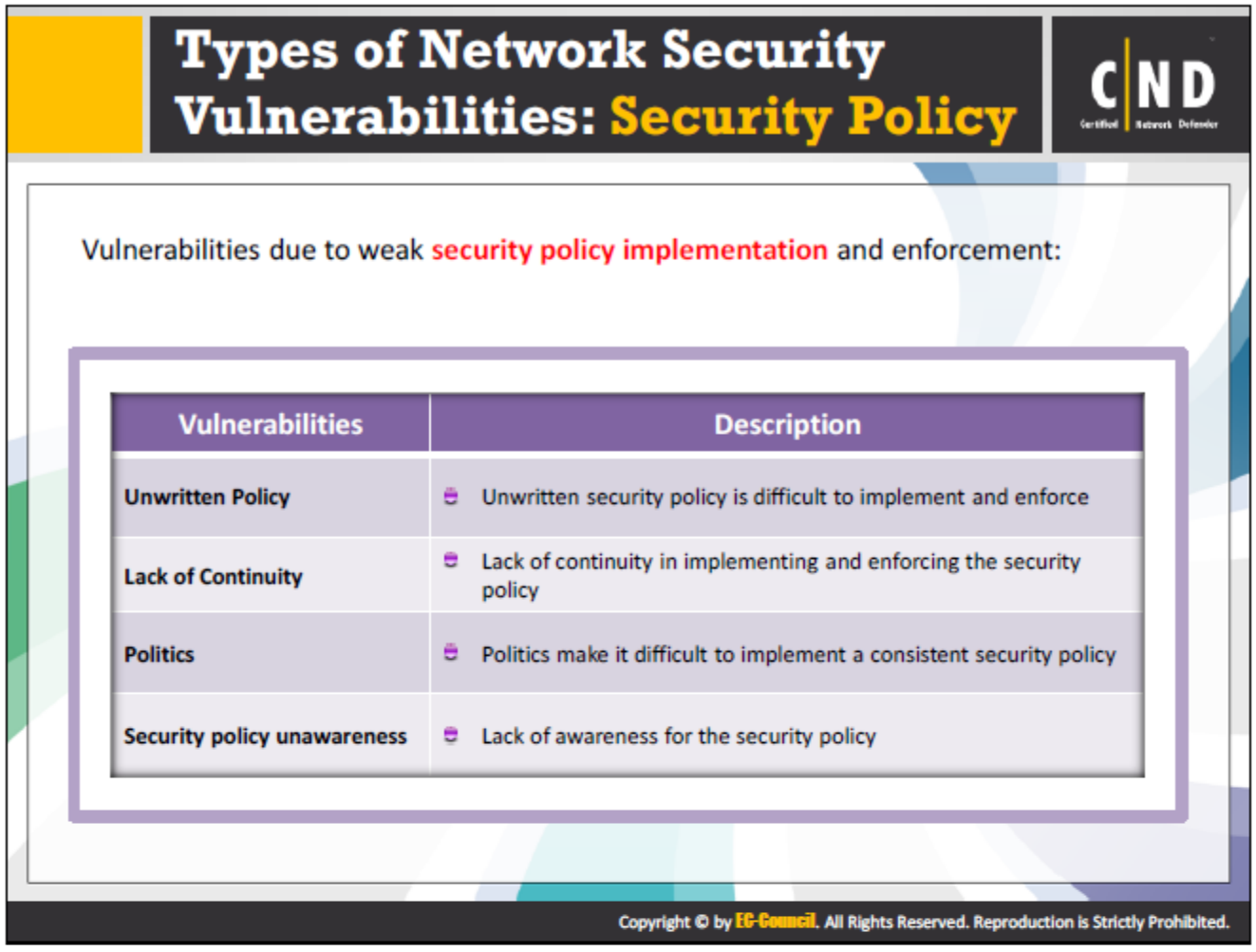
Vulnerabilities that exist in the TCP/IP protocol, operating system, and network devices:

Vulnerabilities	Description
TCP/IP protocol vulnerabilities	HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	An OS can be vulnerable because: - It is inherently insecure - It is not patched with the latest updates
Network Device Vulnerabilities	Various network devices such as routers, firewall and switches can be vulnerable due to: - Lack of password protection - Lack of authentication - Insecure routing protocols - Firewall vulnerabilities

Types of Network Security Vulnerabilities: Configuration

Vulnerabilities that exist due to the misconfiguration of computing and network devices:

Vulnerabilities	Description
User account vulnerabilities	Arising from the insecure transmission of user account details over the network such as usernames and passwords
System account vulnerabilities	Arising from setting weak passwords to system accounts
Internet service misconfiguration	Misconfiguring internet services can pose serious security risks. For example. Enabling JavaScript and misconfiguring IIS, Apache, FTP, Terminal services, etc., can create security vulnerabilities in the network
Default password and settings	Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	Misconfiguring the network device itself



A network security breach can occur because of the following vulnerabilities:

Technological vulnerabilities

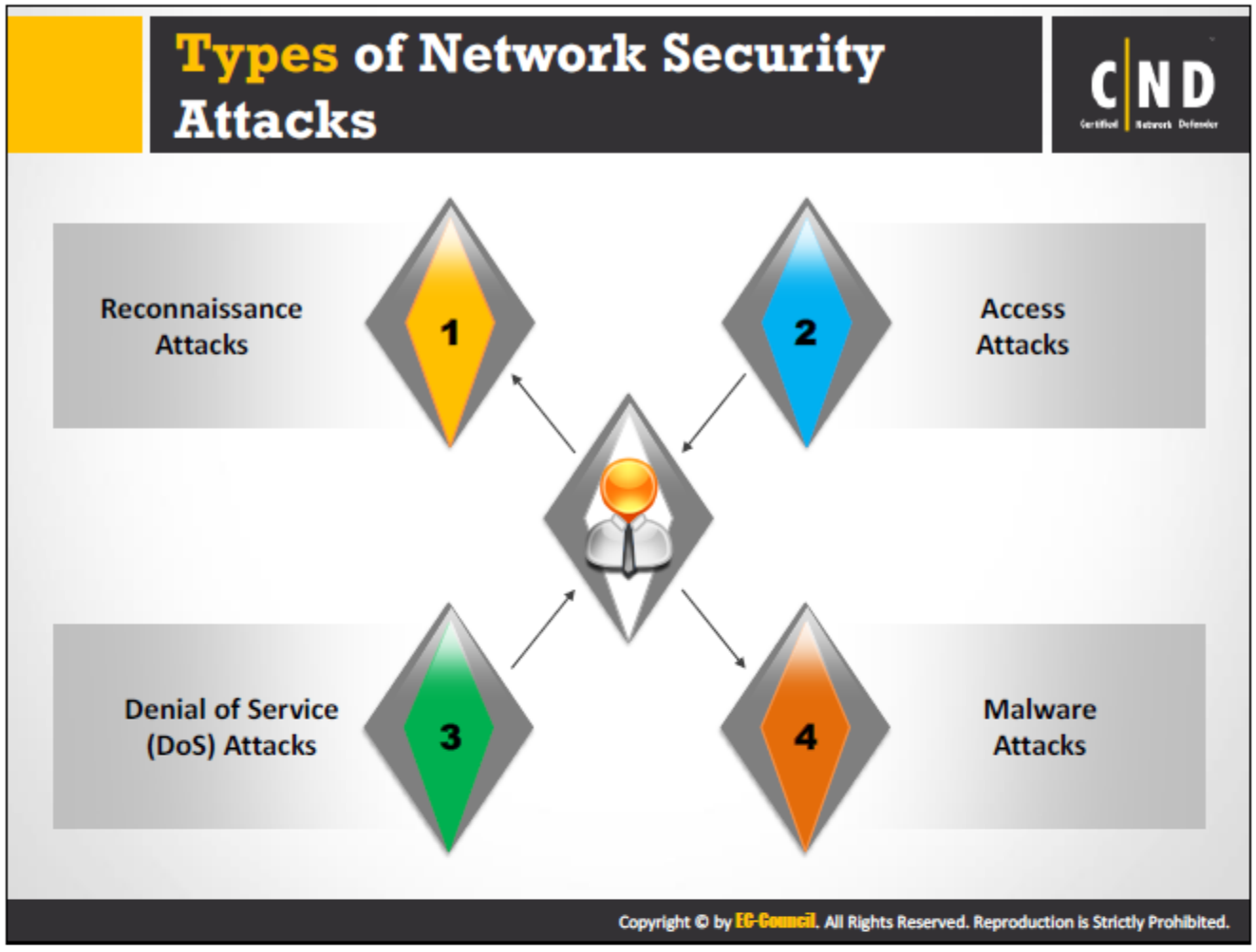
A technological vulnerability exists due to the inherent weakness in the operating system, printers, scanners or other networking equipment. Attackers can detect loopholes in protocols, like, SMTP, FTP and ICMP. Attackers detect the lack of authentication in networking equipment like switches and routers leading to an intrusion. Regular security audits by the network administrator or information security officer will help keep track of any irregular activities on the network.

Configuration vulnerabilities

Configuration vulnerabilities exist due to the misconfiguration of computing and network devices. It exists when an administrator configures a user account or the system services insecurely, leaving the default settings, improper password management, etc.

Security policy vulnerabilities

Security policy vulnerabilities exist when there is an improper drafting and enforcement of the security policies in the organization. Lack of appropriate policy enforcement may lead to unauthorized access to network resources. If an administrator fails to regularly, monitor and audit the activities it will be easy for attackers to exploit the system.



Organizations are facing challenges in maintaining the security of their network, as the number of attacks on a network is growing day by day. Attackers or hackers are finding new ways of getting into networks. The motive behind the attacks differ from based on the objective of each attacker. Some attackers want to steal the hardware and software, while others perform actions that reduce the bandwidth of the network resources and others are after customer data. The network administrator on the other hand needs to be highly efficient in identifying these attacks and have knowledge on what each of these different types of attacks are.

Typical network attacks are broadly classified into:

Reconnaissance attacks

The reconnaissance attack refers to a technique in which the attackers gather information about the network and organization, helping them perform attacks easier. Gathering information about a network allows attackers to recognize any potential weaknesses it may have.

Access Attacks

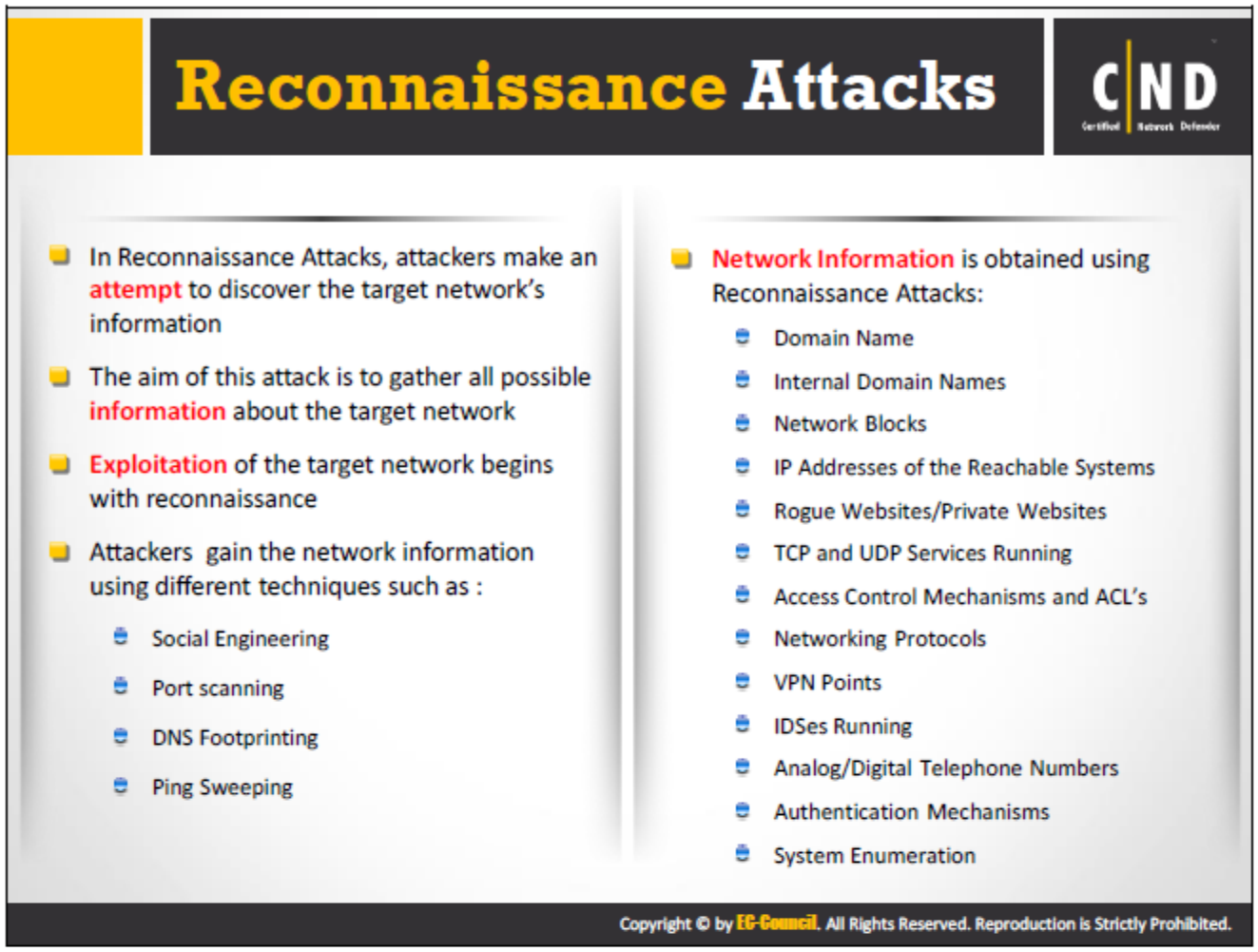
After gaining information about the target network, attackers then try to gain access by using various exploitation techniques. These are the attempts made towards gaining access to the system or network. This is called an access attack and it includes gaining unauthorized access, brute force, privilege escalations, man-in-the-middle, etc.

Denial-of-service

In the denial-of-service attack, attackers attempt to deny certain services available to customers, users and/or the organization. The DoS attack does not lead to any loss or theft of any information, but can affect the organization financially due to the downtime. The DoS attacks affect the files and other sensitive information stored in a system, as well as affect the working of any website. Websites are brought down using this method.

Malware attacks

Malware attacks affect the system or network either directly or indirectly. They cause an adverse impact on how the network functions. Malware is a program or a file that poses a threat to a computer system. The different types of malware include Trojans, Viruses and Worms.



In Reconnaissance attacks, attackers make an attempt to discover all the possible information about a target network, including information systems, services and vulnerabilities which may exist in the network.

The major objectives of a reconnaissance attack include collecting the target's network information, system information, and the organizational information. By carrying out reconnaissance at various network levels, the attacker gains information such as network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, and access control mechanisms. With a reconnaissance attack, the attacker collects information such as employee names, phone numbers, contact addresses, designation, and work experience, etc. Which leads to social engineering and other phases of the intrusion into the corporate network.

Collecting Network Information

An attacker performs a *whois* database analysis, trace routing, etc. to gather network information. Thereafter the attacker may gain access to sensitive data or may attack the network.

Collecting System Information

Prior to performing an attack, an attacker identifies the vulnerabilities to exploit in order to gain access to a system. Once the attacker gains system access, they can use various tools and

utilities to perform illegal activities such as stealing sensitive data, attacking other systems, sending forged emails from the system and deleting data.

Collect Organization's Information

An attacker obtains information about an organization from its website. In addition, they can query the target's domain name against the *whois* database and get valuable information such as location, people's names, phone numbers, etc. The information can then identify key employees in the company and using this they launch social engineering attacks to extract sensitive data about the organization.

Types of reconnaissance attack

Reconnaissance attacks can be active or passive.

- **Active reconnaissance attacks**

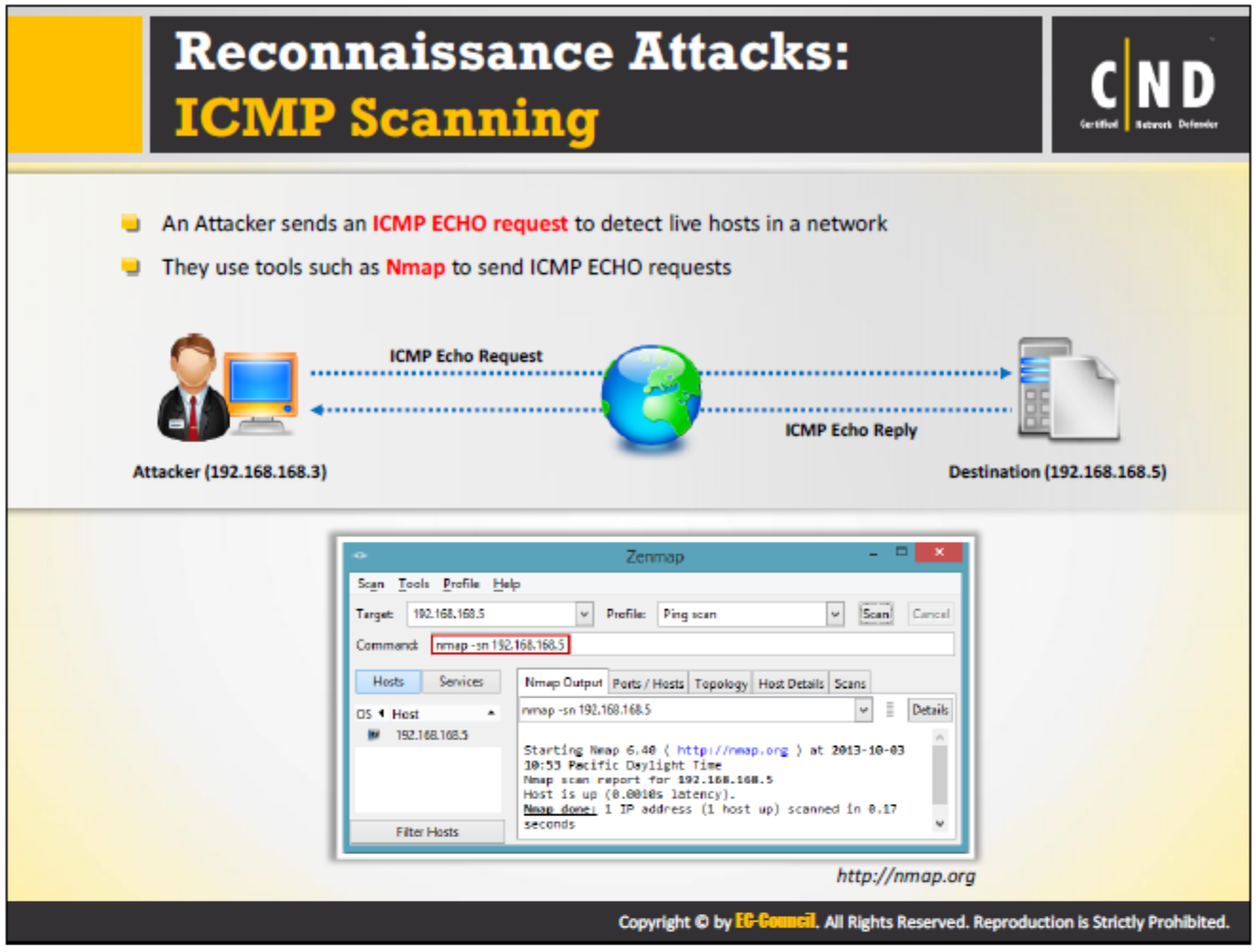
  Active reconnaissance attacks mostly include port scans and operating system scans. Here, the attacker uses tools to send packets to the target system. For example, the traceroute tool helps gather all the IP addresses for the routers and firewalls. The attacker also gathers more information regarding the services running on the target system.

- **Passive reconnaissance attacks**

  Passive reconnaissance attacks use the method of gaining information from the traffic. Here, the attackers perform sniffing that helps them gain all the details regarding the weaknesses in the network. The attackers use various tools to gain information about the target.

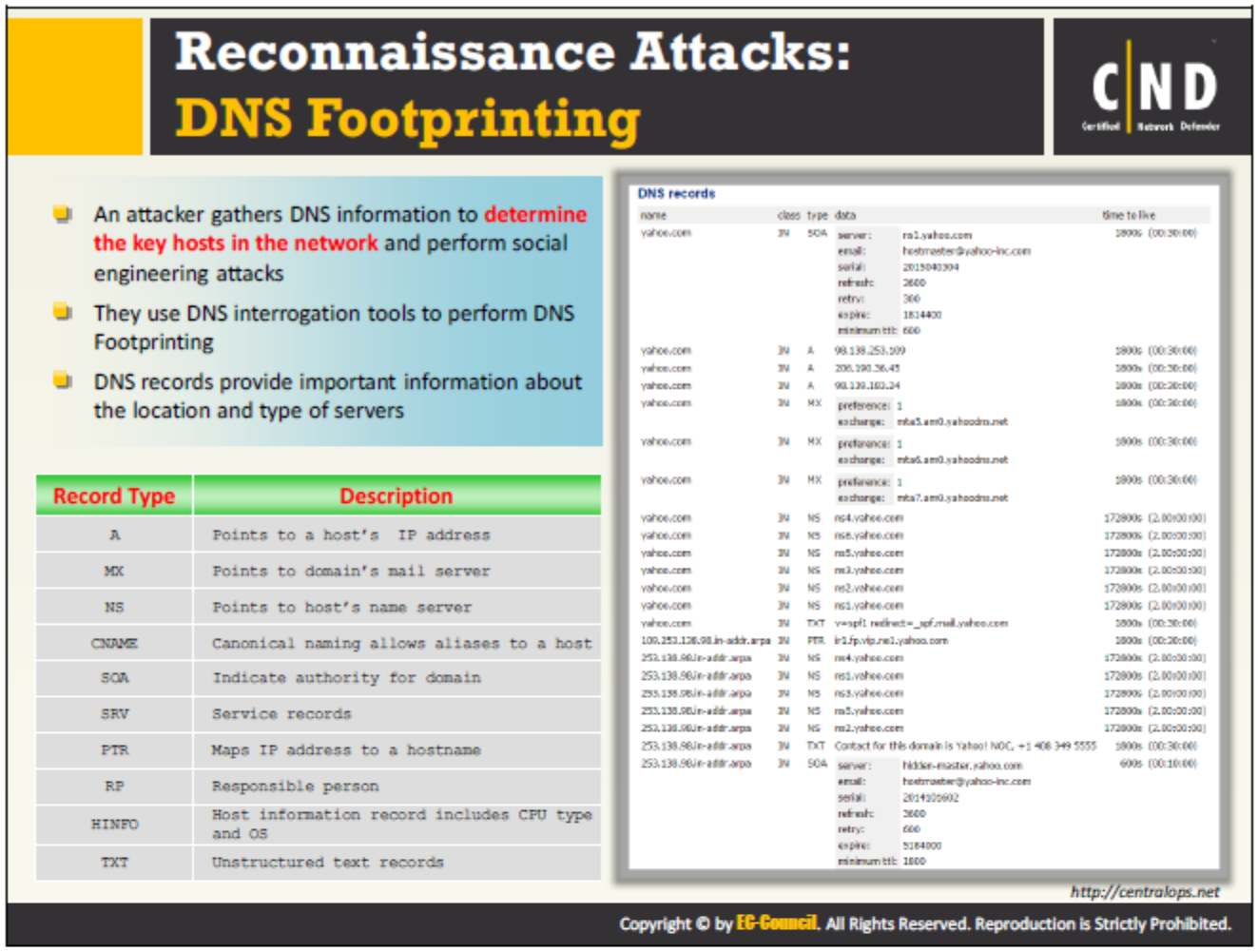
Example of Reconnaissance attacks includes

- **Packet sniffing:** Packet sniffing monitors every packet that passes through a network. Through various packet sniffing tools, attackers capture usernames, passwords, and other user information. The user information is available in plain text, on protocols like Telnet and HTTP. Packet sniffing can map the network and can break into the target computer.
- **Port scanning:** Port scanning gives attackers access to any open ports on the target machine. Once the access is possible, the intrusion is done.
- **Ping sweeping:** Ping sweeping is the technique which helps to locate the open/live port in a network through an ICMP request. A well configured ACL can prevent ping sweeping in the network.
- **DNS Footprinting:** DNS Footprinting is possible with the help of a DNS query consisting of DNS lookup and *whois*. The queries provide information about the specific domain and the IP address.
- **Social Engineering:** Social engineering is a technique, where targets, unknowingly share their credentials or personal information on the network. Attackers use this information to attack the target.



During ICMP scanning, the attacker sends ICMP packets to the system to gather all necessary information about it. ICMP scanning helps an attacker determine what hosts are running in a network. They are detected by pinging them with the help of scanning tools such as NMAP. NMAP uses the -P option to ICMP-scan in parallel, which can happen very quickly.

The Internet Control Message Protocol (ICMP) scanning technique works on one host system at a time. It sends ICMP ECHO Requests to a single host using the ping utility or third party tools. If the host is live, it will return an ICMP ECHO Reply. This technique also locates the active devices or determines if ICMP is passing through a firewall.

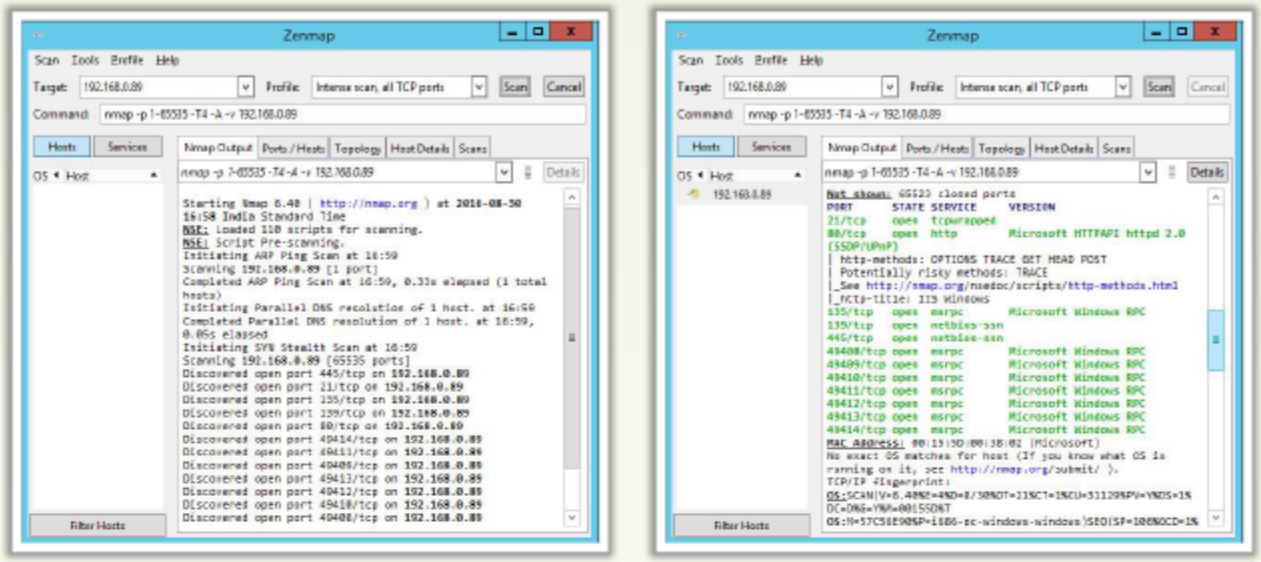


DNS footprinting reveals information about DNS zone. DNS zone data includes the DNS domain names, computer names, IP addresses, and much more about a particular network. An attacker uses the DNS information to determine key hosts in the network, and then performs social engineering attacks to gather even more information.

When the attacker queries the DNS server using the DNS interrogation tool, the server responds with a record structure that contains information about the target DNS. DNS records provide important information about the location and type of servers.

Reconnaissance Attacks: Network Information Extraction using Nmap Scan

- An attacker uses Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems and OS versions



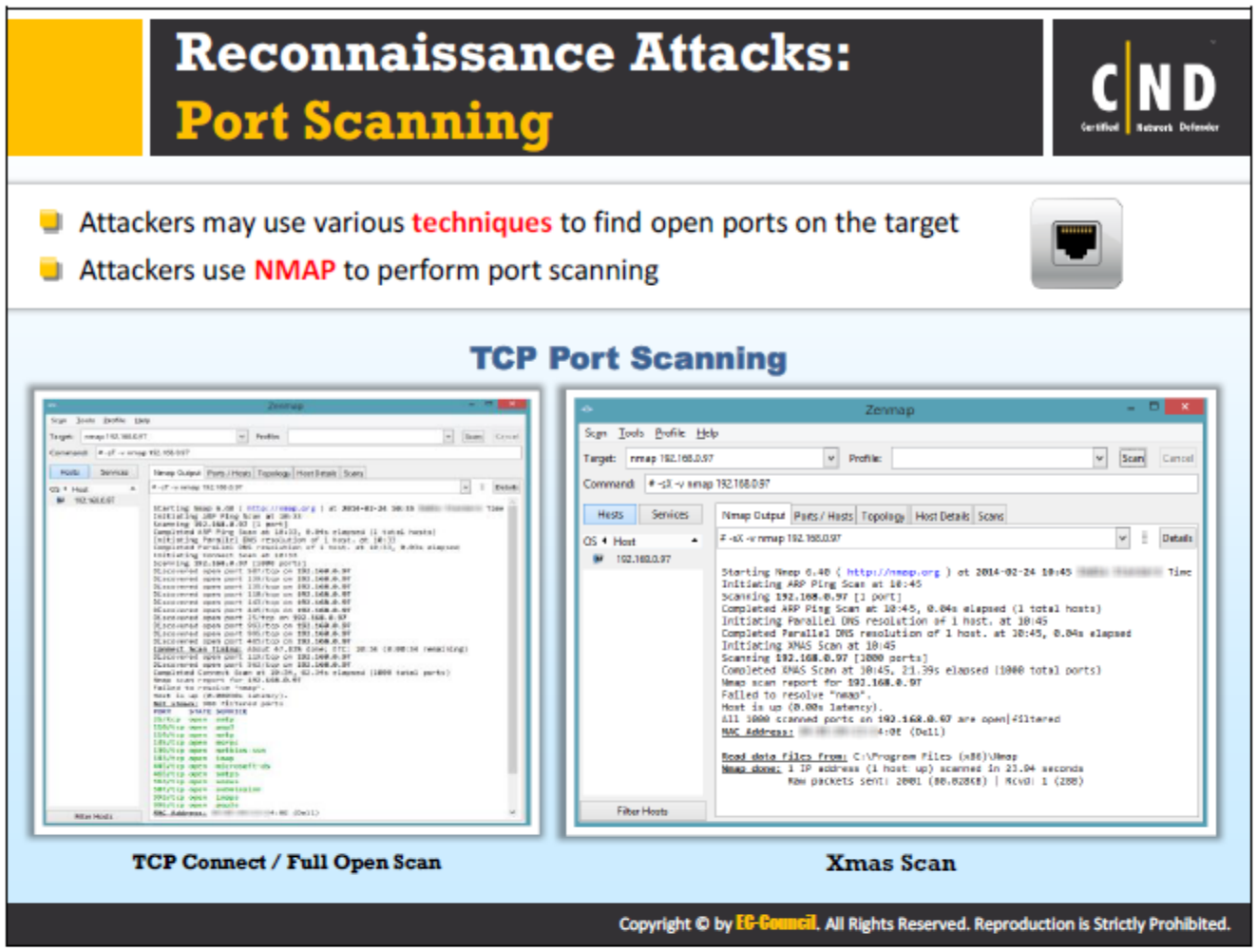
http://nmap.org

Nmap is a network discovery and security-auditing tool and is one of the most popular tools attackers use for network discovery. An attacker mostly uses the Nmap utility to extract all the necessary information from the target.

Attackers use Nmap to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

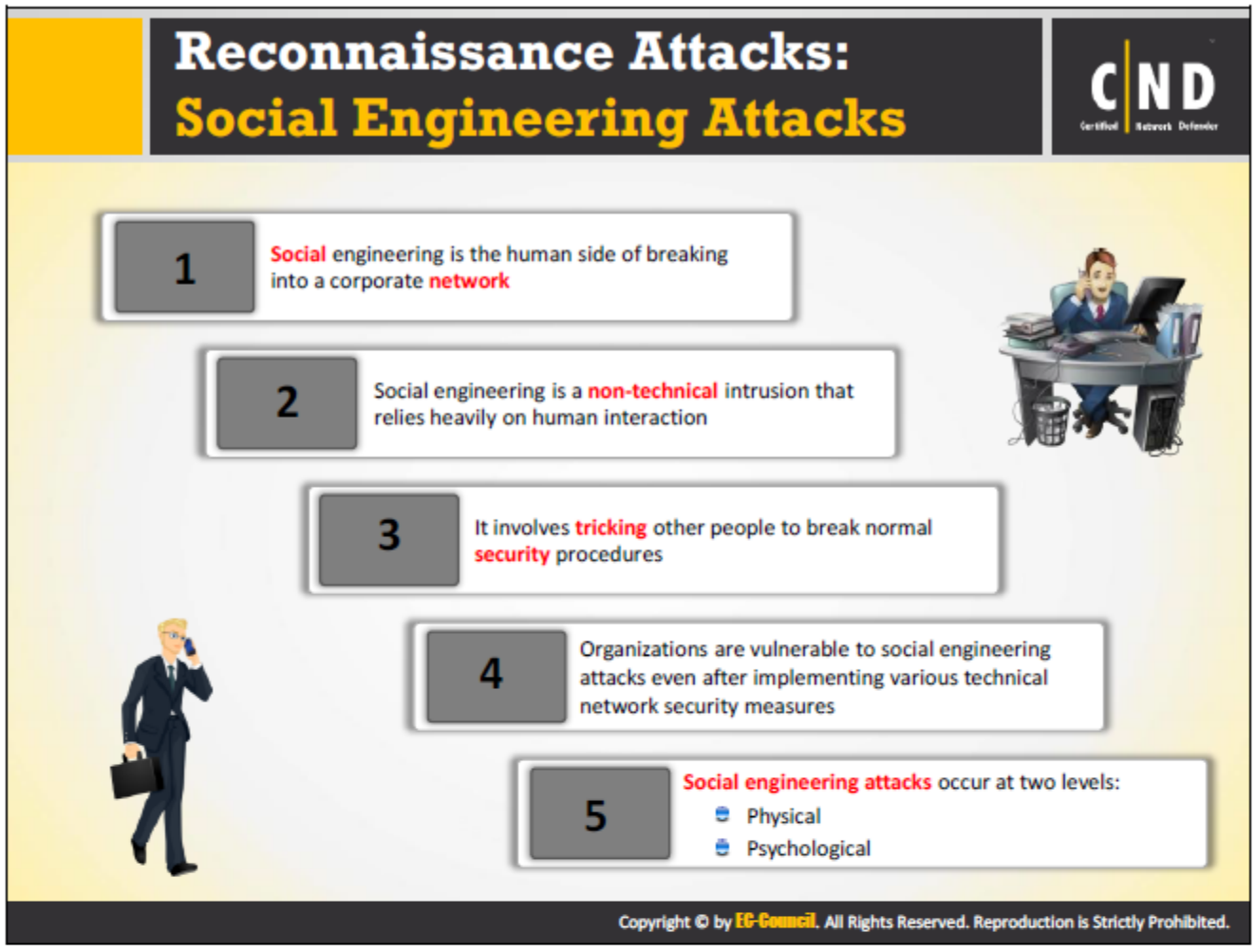
Network administrators also find this tool useful for security auditing tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Source: *http://nmap.org*



Port scanning is the process of checking what services are running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a listening state. The listening state provides information about the operating system and the application currently in use. Sometimes, active services that are listening may allow unauthorized users access to misconfigured systems or software that is running with vulnerabilities. Port scanning techniques help to identify and list all the open ports on a targeted server or host.

Attackers use various port scanning utilities tools such as NMAP, Netscan Tools Pro, SuperScan and PRTG Network monitor to detect open ports on the target. These tools help an attacker probe a server or host on the target network for open ports. Open ports are the doorways through which malware get on a system.



Social engineering is the art and science of convincing (tricking) people to provide personal or business information. This is one way an intruder chooses to step into an organization. Intruders gain unauthorized access through developing trust relationships with employees.

Social engineering refers to the method of influencing and persuading people to reveal sensitive information in order to perform some malicious action. With the help of social engineering tricks, attackers can obtain confidential information, authorization details, and access details of people by deceiving and manipulating them. They can find out what people are on vacation or going on vacation. Where they work, the security measures in place or simply listening to the employees talk about their work day.

Attackers can easily breach the security of an organization using social engineering tricks. All security measures adopted by the organization are in vain when employees get "social engineered" by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam email, and bragging in front of co-workers. Even answering questions on a phone call can lead to social engineering. Employees must be trained properly to recognize these tricks and taught how to counter them when necessary.

Prior to performing a social engineering attack, an attacker gathers information about the target organization from various sources such as:

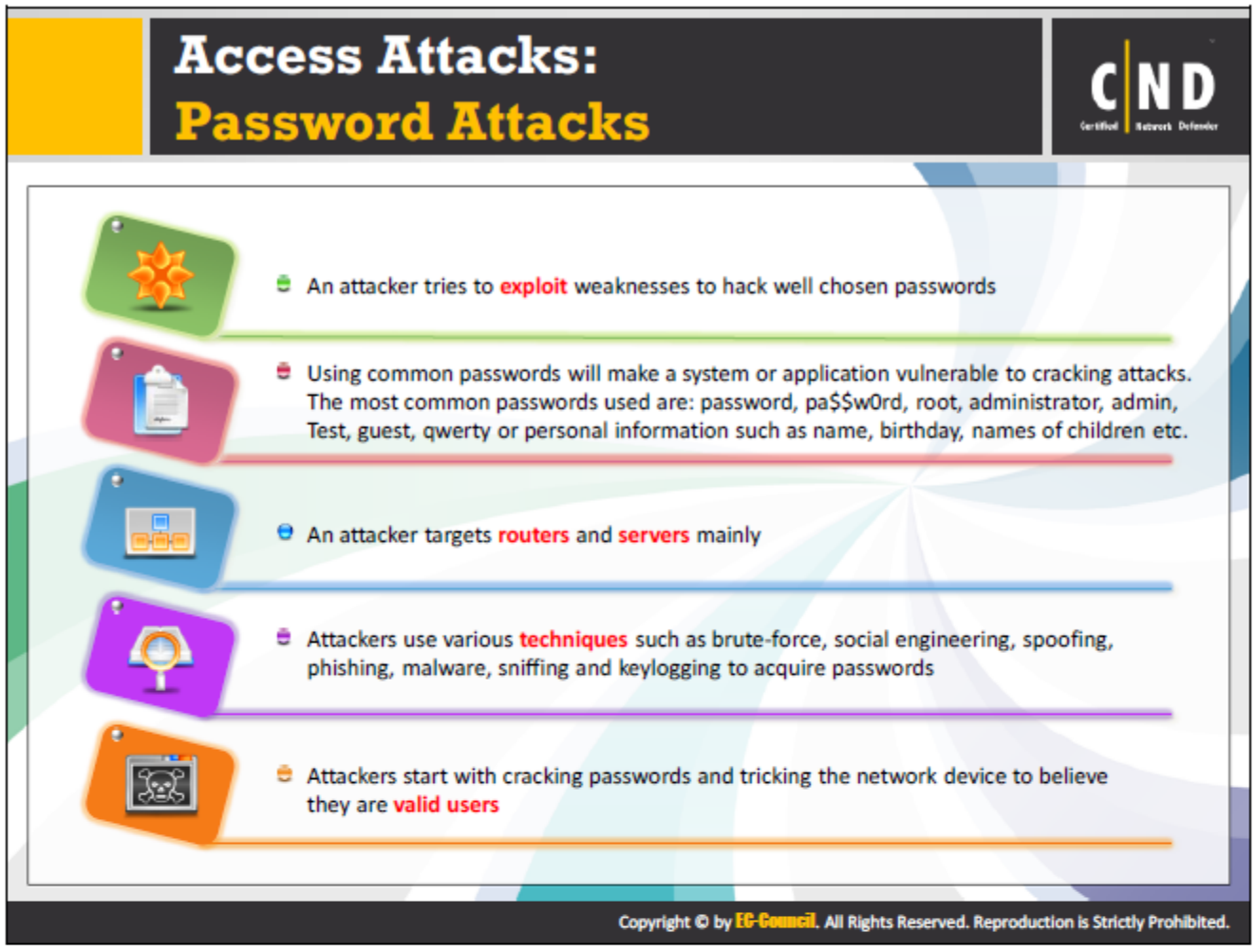
- Official websites of the target organization, where they reveal employee IDs, names, and email addresses.

- Advertisements of the target organization through the type of print media required for high-tech workers trained in oracle databases or UNIX servers.
- Blogs, forums, etc. in which employees reveal basic personal and organizational information.

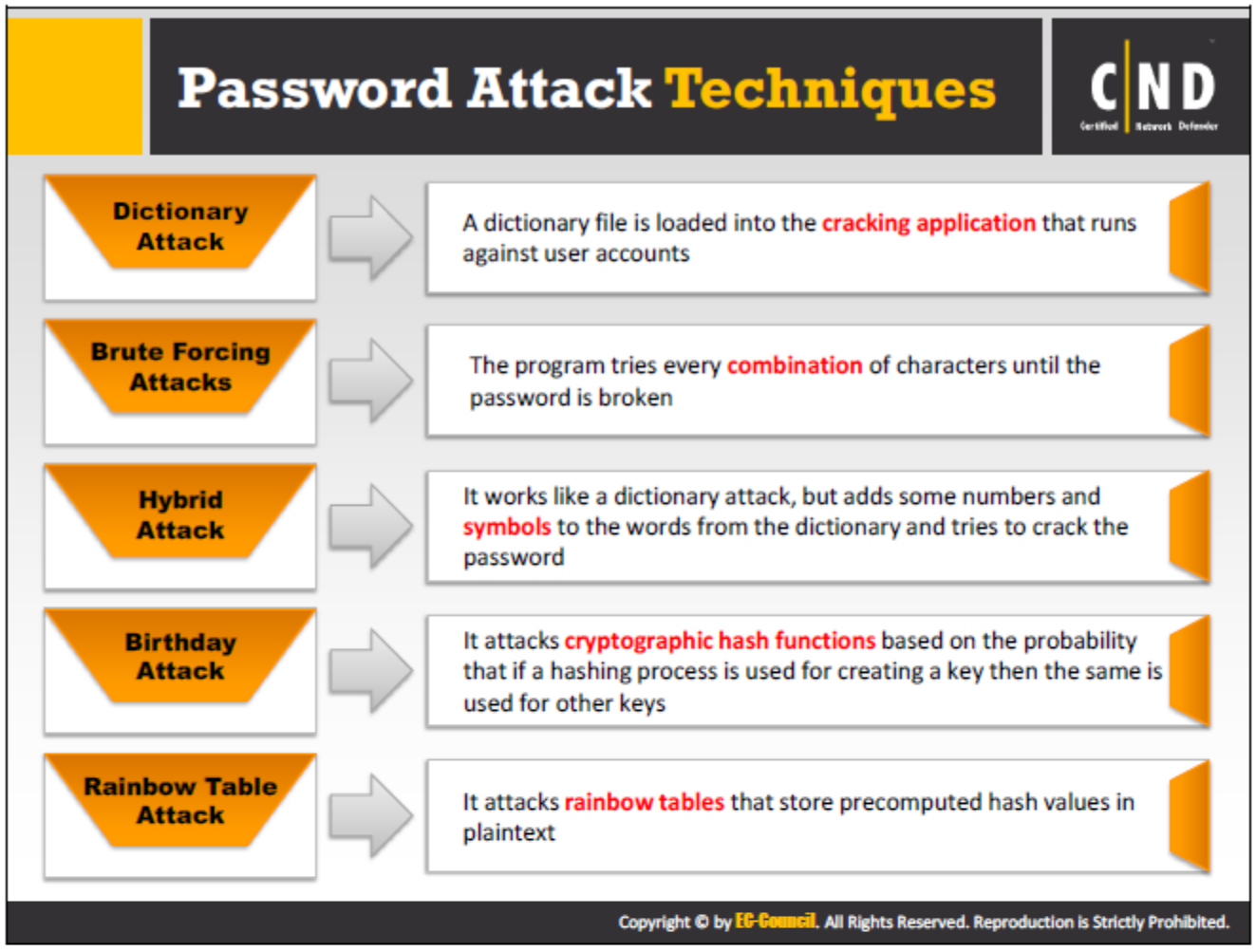
After gathering enough information about the target organization, an attacker tries to perform a social engineering attack through various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and so on.

Despite having security policies in place, attackers can compromise an organization's sensitive information by means of social engineering as it targets the weakness of people.

Social engineering attacks are classified into two types. They are either human-based or computer-based. In human-based attacks, the physical presence of intruders is required to extract personal information from the targeted people. In computer-based attacks, intruders extract the user's credentials remotely by operating on other systems.



Password attacks are performed to gain unauthorized access or to get control over a target computer system. Attackers perform password attacks to steal secrets, make slight modifications to websites, steal credit card details, get privileges, etc. Generally, passwords are used to authenticate users with a system. Attackers try to gain these user passwords with different techniques and authenticate with the system to enjoy the privileges the normal user has. Attackers perform different techniques to crack the passwords of servers and routers and get access to the targeted resource.



An attacker may use different types of techniques to crack passwords. Those are:

Dictionary Attack

The dictionary attack is an attempt to crack a user's password by making a guess. Attackers can guess passwords using a manual or an automated approach. This attack tries to match the most occurring words or commonly used words in day to day life. The most common passwords found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, date of birth, children names, addresses and hobbies.

Most of users create passwords with the names of birds, famous names and places, etc. These types of passwords are detected by dictionary attacks. Attackers prepare a dictionary of the most commonly used words that are likely to be used as a password and use all the possible entries to break the password. Dictionary attacks are relatively faster than brute force attacks.

Most networks are not configured with lengthy and complex passwords. So it is easy for attackers to guess weak passwords and gain access to a network. Passwords that are not case sensitive are easily guessed by attackers. For example, LAN manager authentication is case insensitive. So the attacker doesn't need to consider whether the password is uppercase or lowercase. There are many tools that automate the process instead of typing password after password.

Brute Forcing Attack

In brute force password cracking, large number of guesses are performed in order to successfully gain a password of the target system. It involves checking all combinations of characters until the correct password is found. Brute-force attacks are best suitable for gaining passwords which are small or not very complex. If there is a long and complex password, the dictionary attack is faster than the brute-force attack. This is due to the time lag taken by the brute-force attack to gain the correct combination for the password. Brute-force attacks are time and resource consuming. The effectiveness of the brute-force attack depends on the password being cracked.

Hybrid Attack

It works like a dictionary attack, but adds numbers and symbols to the words and tries to crack the password. These attacks generalize common things people do to make their passwords hard to guess. The hybrid attacking tool starts guessing a dictionary term and creates other guesses by appending or prepending the characters to the dictionary term. It appends or prepends with dates, numbers, alphanumeric characters, etc., to break the password.

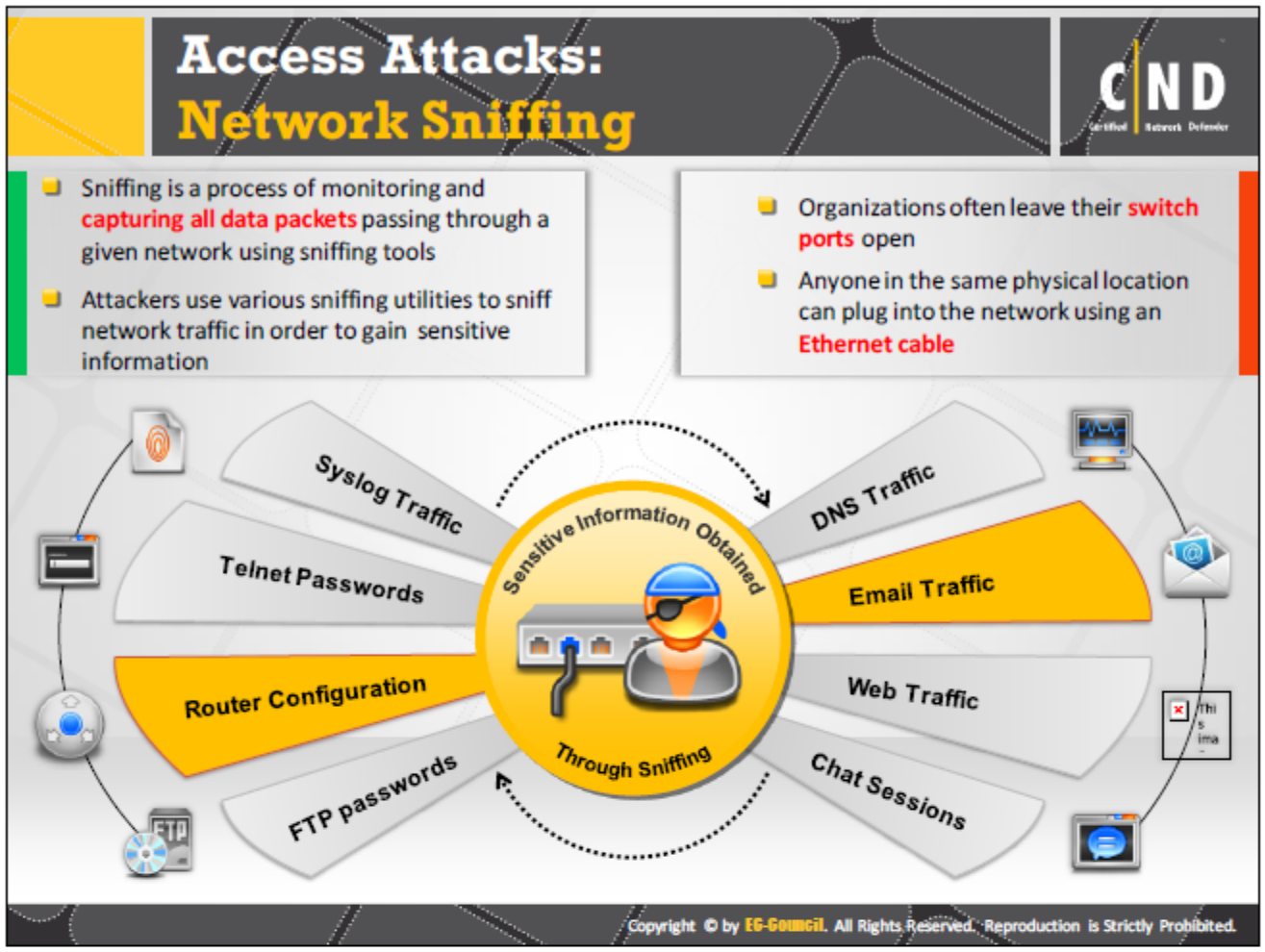
Birthday Attack

The birthday attacks use techniques that solve a class of cryptographic hash functions. The birthday attack falls under the section of brute-force attacks. The logic of a birthday attack depends on the birthday problem that is explained as follows: A probability problem that states if there are 23 people in a room, the probability of at least two people having the same date of birth is more than 0.5. Attackers try to get the birth date of the target employee to crack the password. It is because some users create passwords with their birth date. Attackers use different methodologies such as probability analysis to get birth dates.

Similarly, in a birthday attack, it is likely to achieve equal values when different input values are applied to a hash function. The attack depends on the occurrence of the number of collisions that can occur when applying different values to a hash function.

Rainbow Table Attack

Rainbow table is a huge set of hashes (encoded codes) that are pre-matched to possible plaintext passwords. Rainbow tables are used by password cracking software to breach network security. All computer systems that require authentication, store user accounts and passwords in the database in encrypted form. If the attacker gains access to password database, password cracking software compares the rainbow table's list of hashes with hashed passwords in the database. The Rainbow table maps plain text passwords with hashes that are exploited by attackers to access the network as a valid user.



Sniffing involves capturing, decoding, inspecting and interpreting the information inside a packet on a TCP/IP network. The purpose is to steal information, usually user IDs, passwords, network details, credit card numbers, etc. Sniffing is generally referred to as a "passive" type of attack, where the attacker can be silent/invisible on the network. This makes it difficult to detect, and it is a dangerous type of attack. The TCP/IP packet contains vital information required for two network interfaces to communicate with each other. It contains fields such as source and destination IP addresses ports, sequence numbers and the protocol type.

There are three ways to sniff a network:

Internal sniff

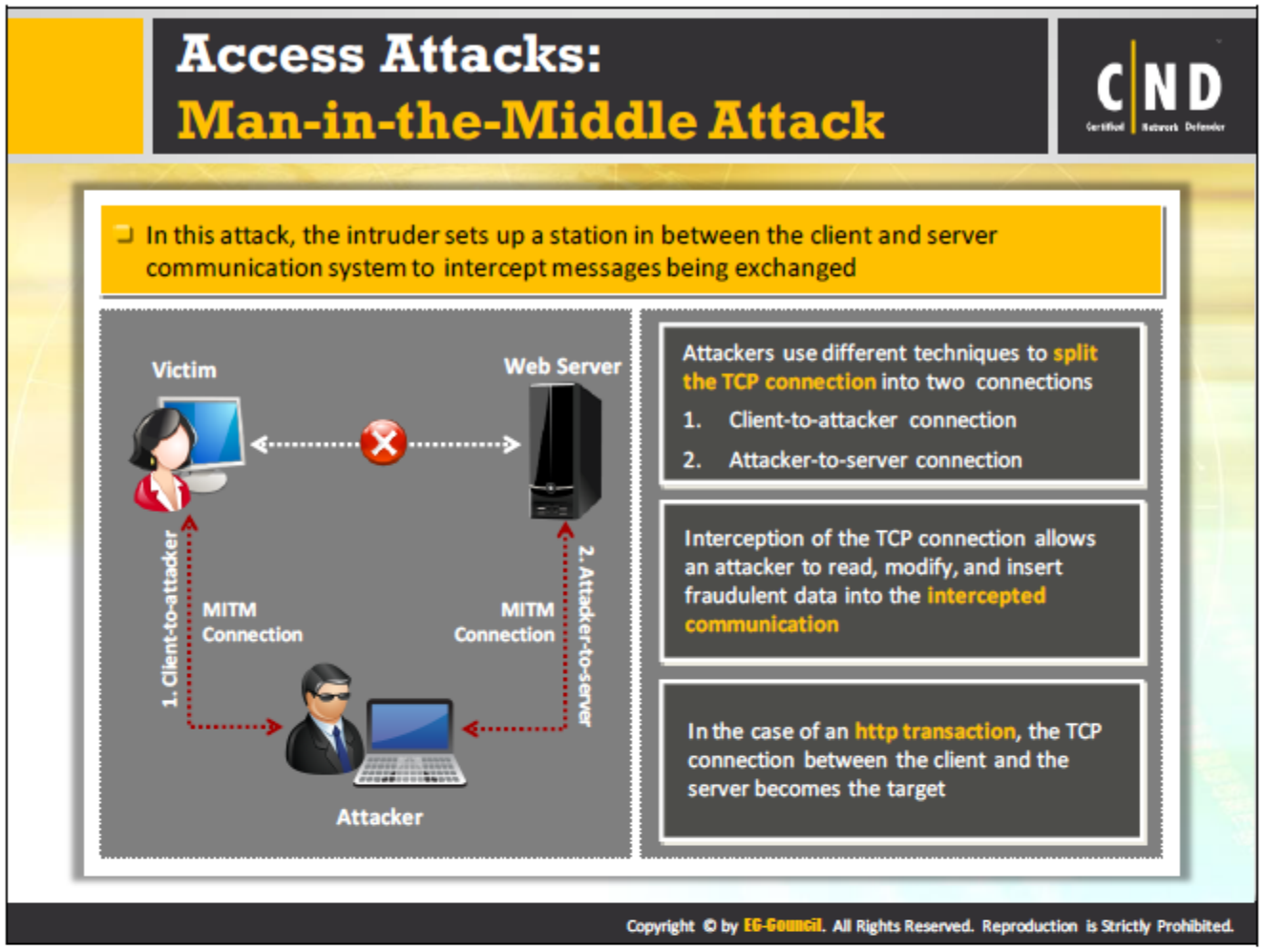
A person (who may be an employee of the firm) who is already hooked up to the internal LAN can run tools to directly capture network traffic.

External sniff

A hacker outside the target network can intercept packets at the firewall level and steal the information.

Wireless sniff

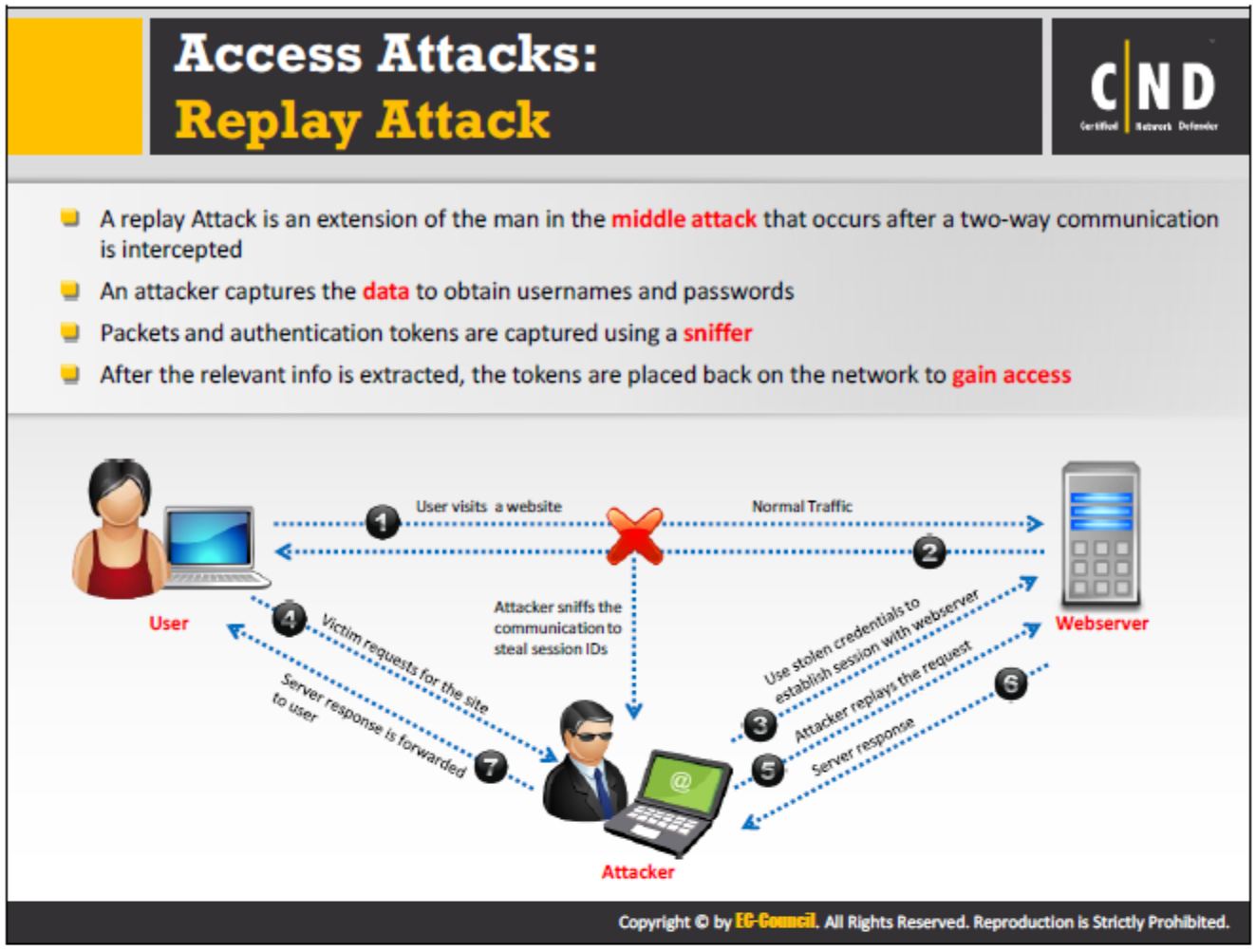
Regardless of where the hackers are located on the network being sniffed, wide usage of wireless networks has made it easy to sit near the network and penetrate it to get information.



A man-in-the-middle attack (also known as MiTM) is a type of attack in which attackers intrude into an existing connection between two systems to intercept the messages being exchanged and to inject fraudulent information. It involves snooping on a connection, intruding into a connection, intercepting messages, and modifying the data. It is basically a type of eavesdropping attack where communication between two parties is monitored or modified by a third unauthorized party. With the help of a MiTM attack, an attacker can exploit the real-time processing of transactions, conversations or transfer of other data. MiTM is a form of a session hijacking attack.

- Communication susceptible to MiTM attacks:
  - Login functionality
  - Unencrypted
  - Financial sites

MiTM attack is often found in telnet and wireless technologies. It is not easy to implement such attacks due to the TCP sequence numbers and speed. This method is relatively hard to perpetrate and can be broken sometimes by invalidating the traffic.



The replay attack is an extension of the MITM attack in which the attacker replays the information gained from the communication between two parties. The attacker gains the token used for validating the users accessing the webserver by eavesdropping. And later replays the token to the server after modifications or deletions thereby gaining access to the session. The attacker then sends the server response to the user.

In the replay attack, the attacker eavesdrops on the confidential information such as credentials or Session ID or any key that the attacker can later use with the receiver in the pretext of the sender. It is one of form of a MiTM attack.

For example, suppose user A sends a secret key to user B as a part of an identity verification. Then attacker C performs eavesdropping and gains the required information. Attacker C can later use this secret key to send information to user B in the pretext of user A. Then user B accepts the message as it is properly encrypted.

To perform the replay attack, the attacker needs to get an intermediary control between the sender and the receiver or achieve an access to the local machine of the sender. Packets are captured using a sniffer. After the relevant information is extracted, the packets are placed back on the network.

There are many ways to prevent the occurrences of any replay attack. The sender and the receiver can use one-time passwords that expire after a certain period of time. The receiver can validate the sender by matching the password provided by the sender. Even when the attacker gets the one-time password and initiates a connection with the receiver, the receiver might

send another one-time password different from what the attacker gathered. The attacker sent the one–time password he previously gathered and it does not match the password sent by the receiver. Timestamping is another method used to avoid replay attacks. Users can neglect the messages sent a very long time ago.

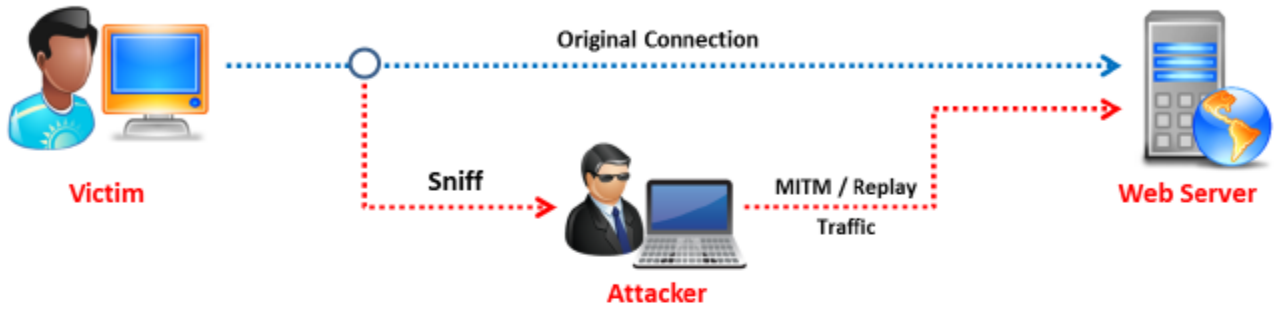
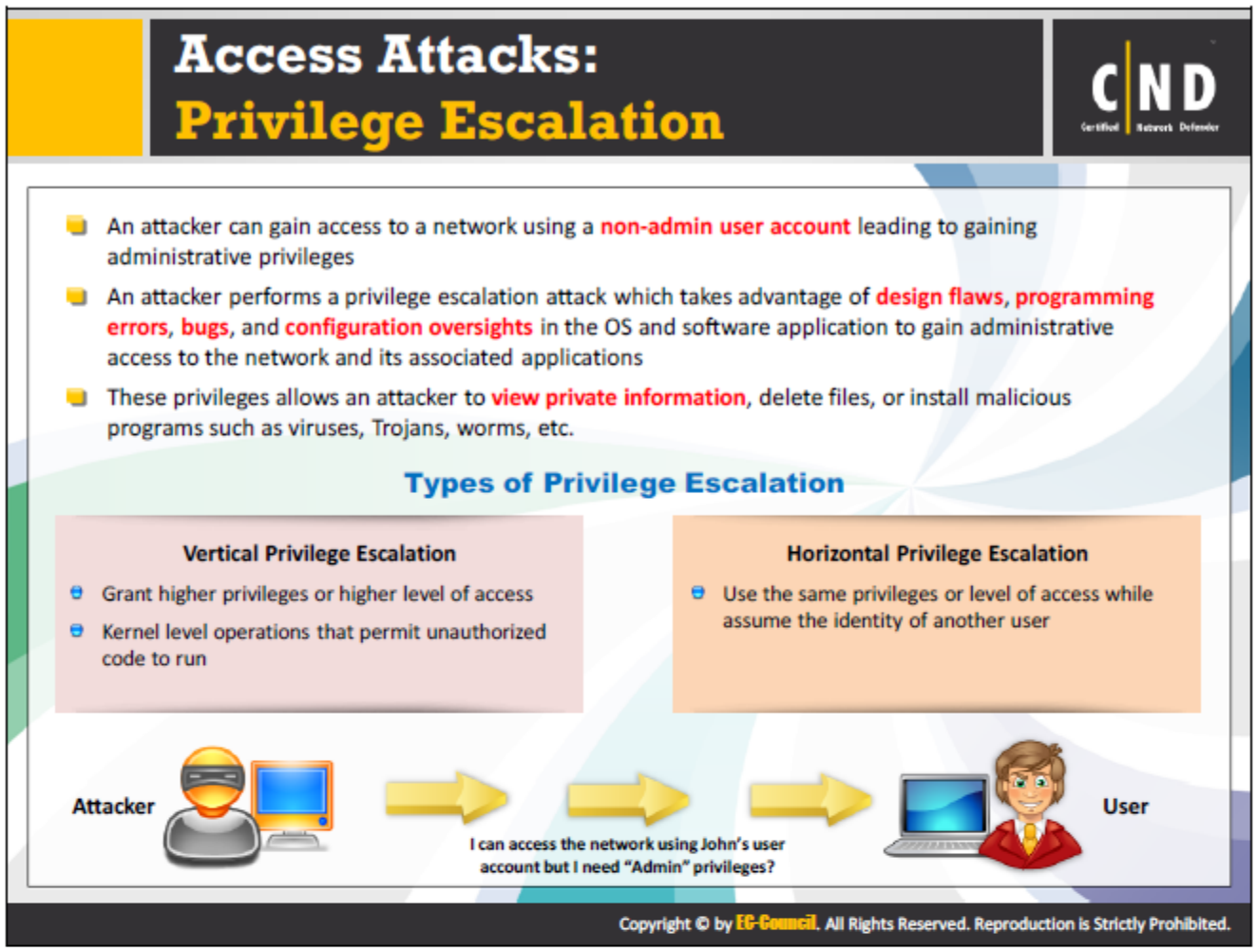


FIGURE 2.2: Replay Attack



In a privilege escalation attack, the attacker gains access to the network and the associated data and applications by taking advantage of defects in the design, software application, poorly configured operating systems, etc. Once an attacker has gained access to a remote system with a valid user name and password, they will attempt to increase their privileges. The attacker uses a method of escalating the user account to another increased privileges, such as administrator privileges.

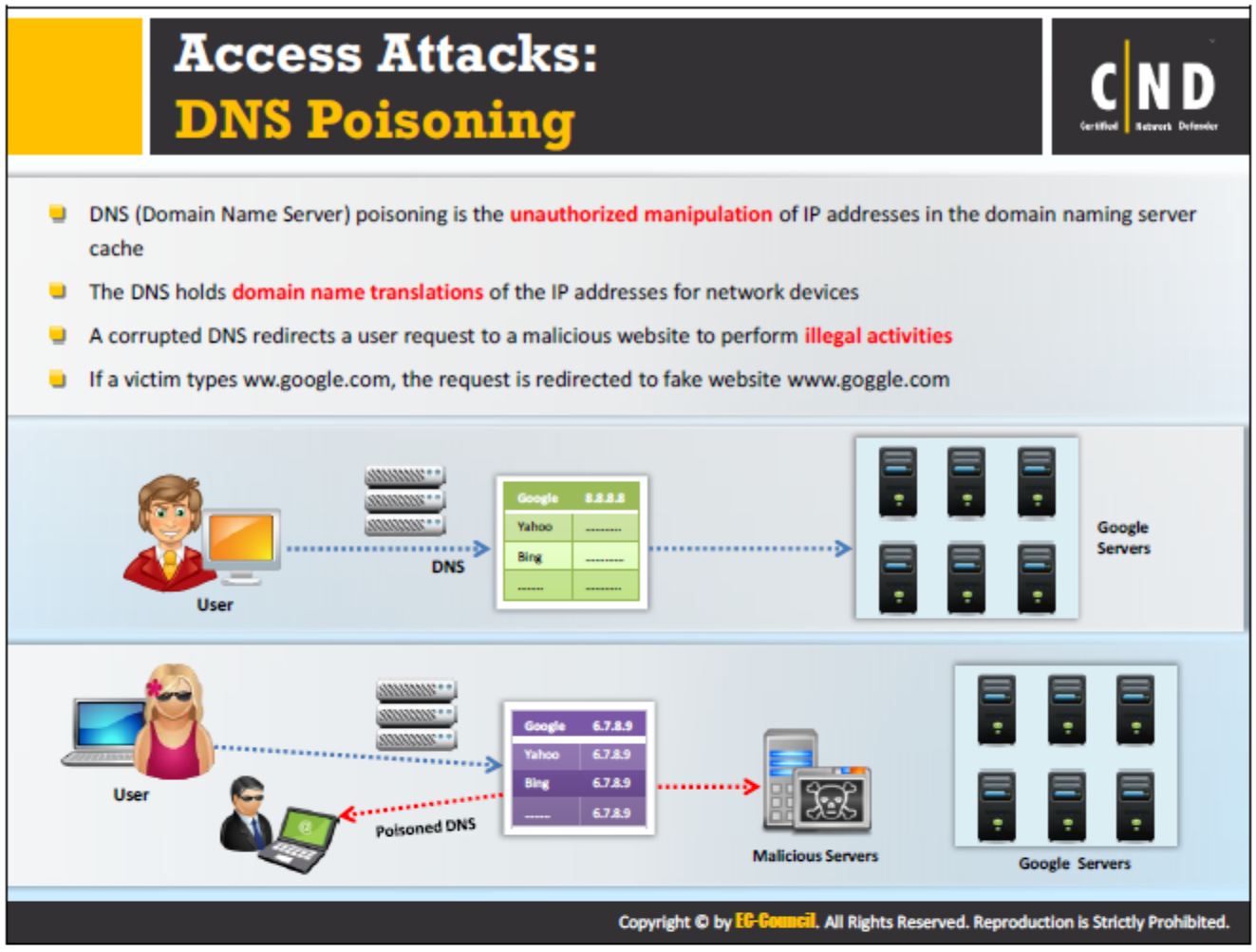
An attacker does privilege escalation to perform unauthorized access and privileged operation on the network or system. An admin account can access more and do more in a network than a regular user. Basically, privilege escalation takes place in two forms. There is vertical privilege escalation and horizontal privilege escalation.

Horizontal Privilege Escalation

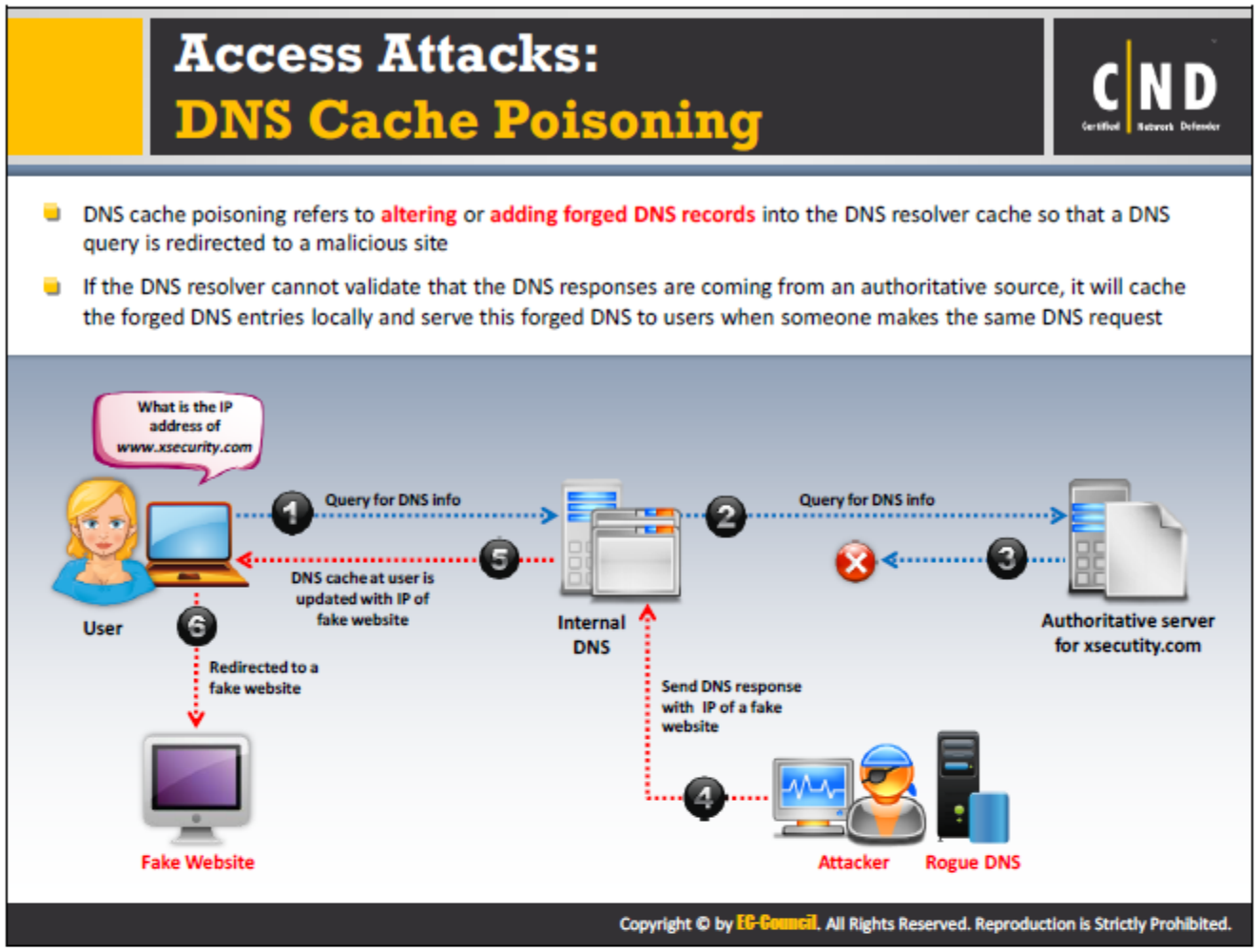
In horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.

Vertical Privilege Escalation

In vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of the user with higher privileges, such as application or site administrators. For example, someone performing online banking can access the site with administrative functions.

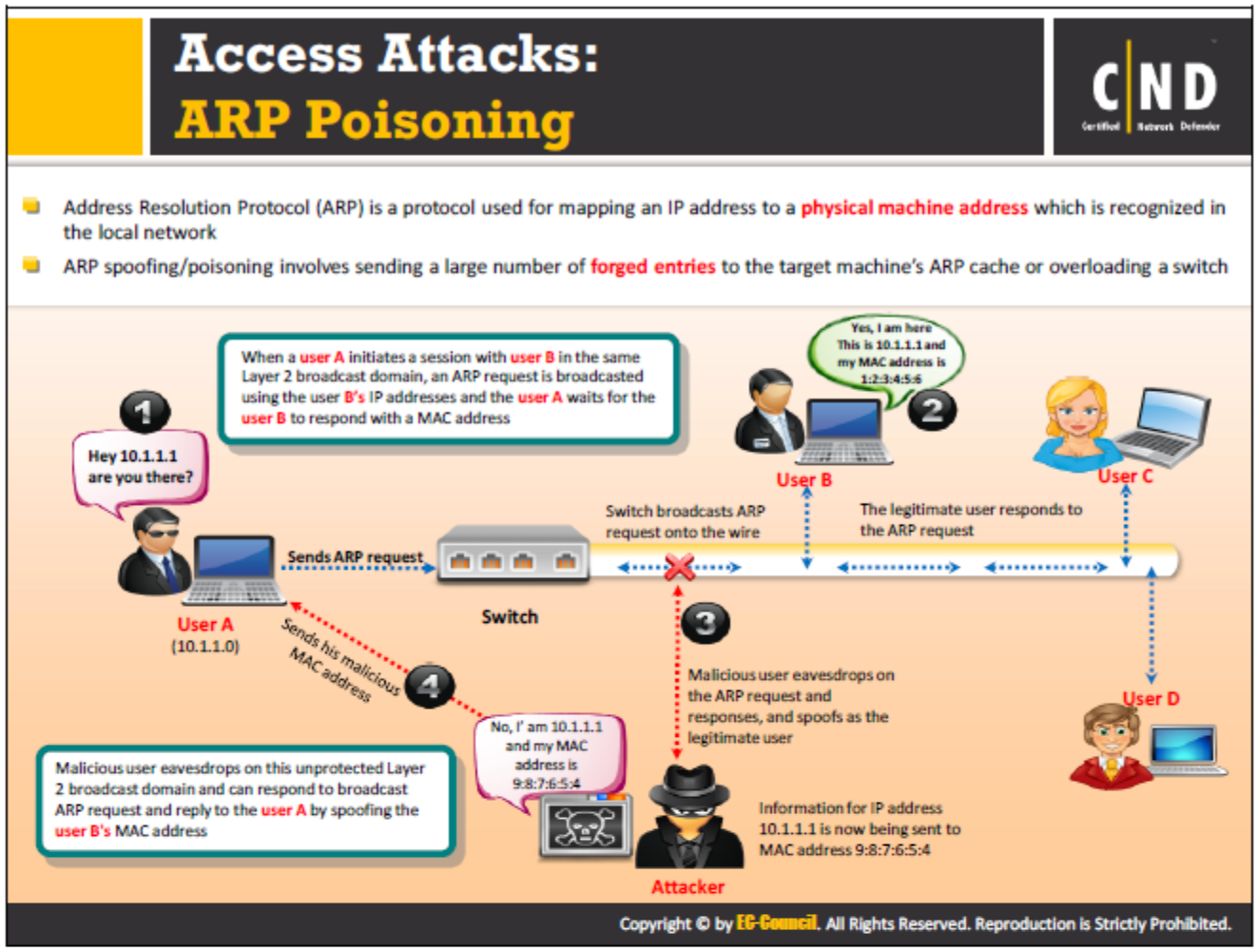


DNS poisoning is a process in which the user is misdirected to a fake website by providing fake data to the DNS server. The website looks similar to the genuine site, but it is controlled by the attacker. It is also called a DNS spoofing attack in which the attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker performs this type of attack by manipulating the DNS table entries in the DNS system. Suppose the victim wants to access the website 123.com, the attacker manipulates the entries in the DNS table in such a way that the victim is being redirected to the attacker's server instead. This can be done by changing the IP address of 123.com to the attacker's malicious server IP address. The victim connects to the attacker's server without their knowledge. Once the victim connects to the attacker's server, the attacker can compromise the victim's system and steal data.



The DNS system uses cache memory to hold the recently resolved domain names. It is populated with recently used domain names and respective IP address entries. When the user request is received, the DNS resolver first checks the DNS cache; if the domain name that the user requested is found in the cache, then the resolver sends its respective IP address quickly. Reducing the traffic and time of for DNS resolving.

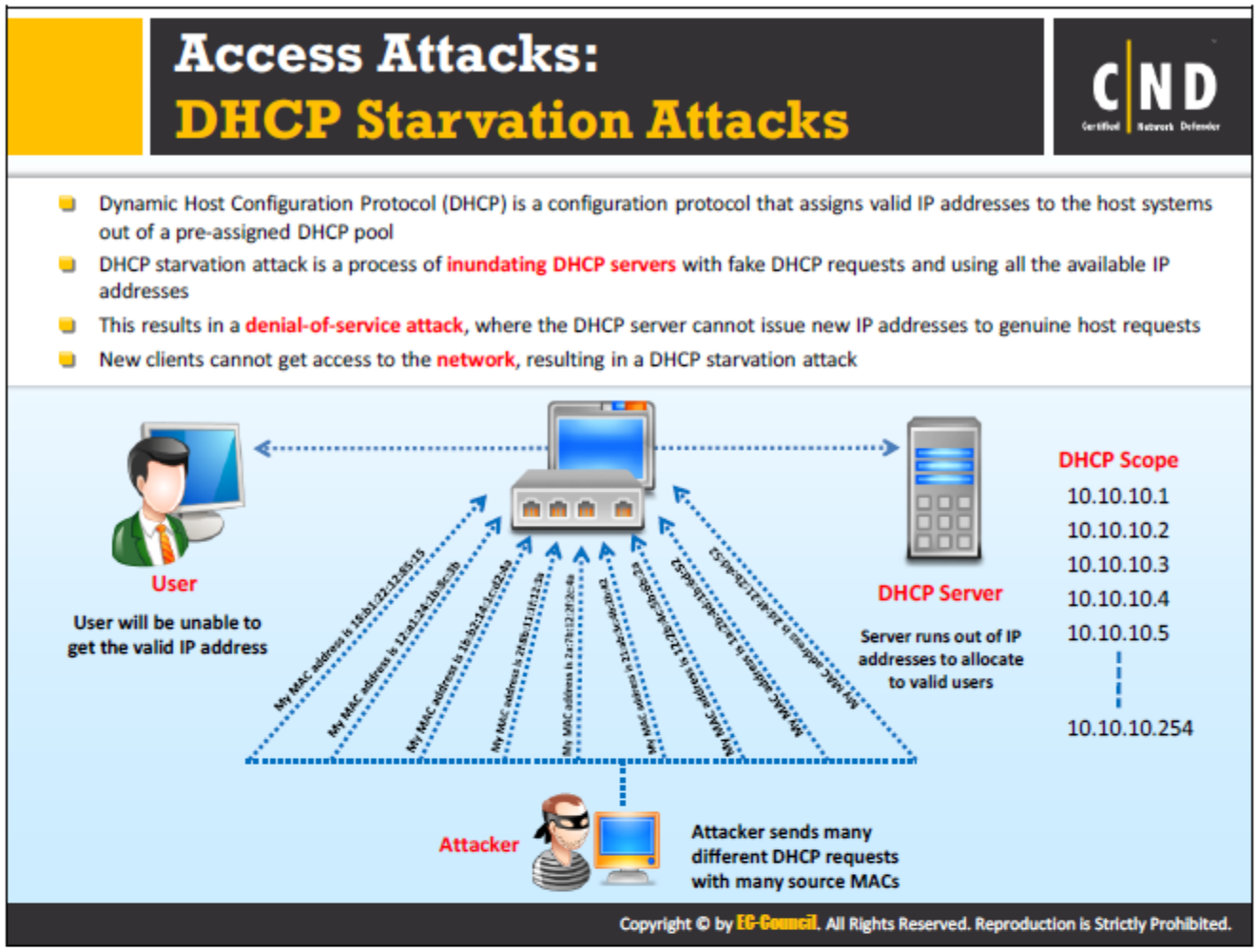
Attackers target the DNS cache and make changes or add entries to it. The attacker replaces the user-requested IP address with the fake IP address. Then, when the user requests the domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poisoned) entry. The victim is redirected to the attacker's fake server instead of the authorized server.



ARP poisoning is an attack in which the attacker tries to associate their own MAC address with the victim's IP address so that the traffic meant for that IP address is sent to the attacker. ARP (Address Resolution Protocol) is a TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by the data link protocol. Using this protocol, you can easily get the MAC address of any device within a network. Apart from the switch, the host machines also use the ARP protocol for getting MAC addresses. ARP is used by the host machine when a machine wants to send a packet to another device and it has to mention the destination MAC address in the packet sent. In order to write the destination MAC address in the packet the host machine should know the MAC address of the destination machine. The MAC address table (ARP table) is maintained in several places even in the operating system.

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an ARP request, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. In fact, many operating systems implement ARP so trustingly that devices that have not made an ARP request still accept ARP replies from other devices.

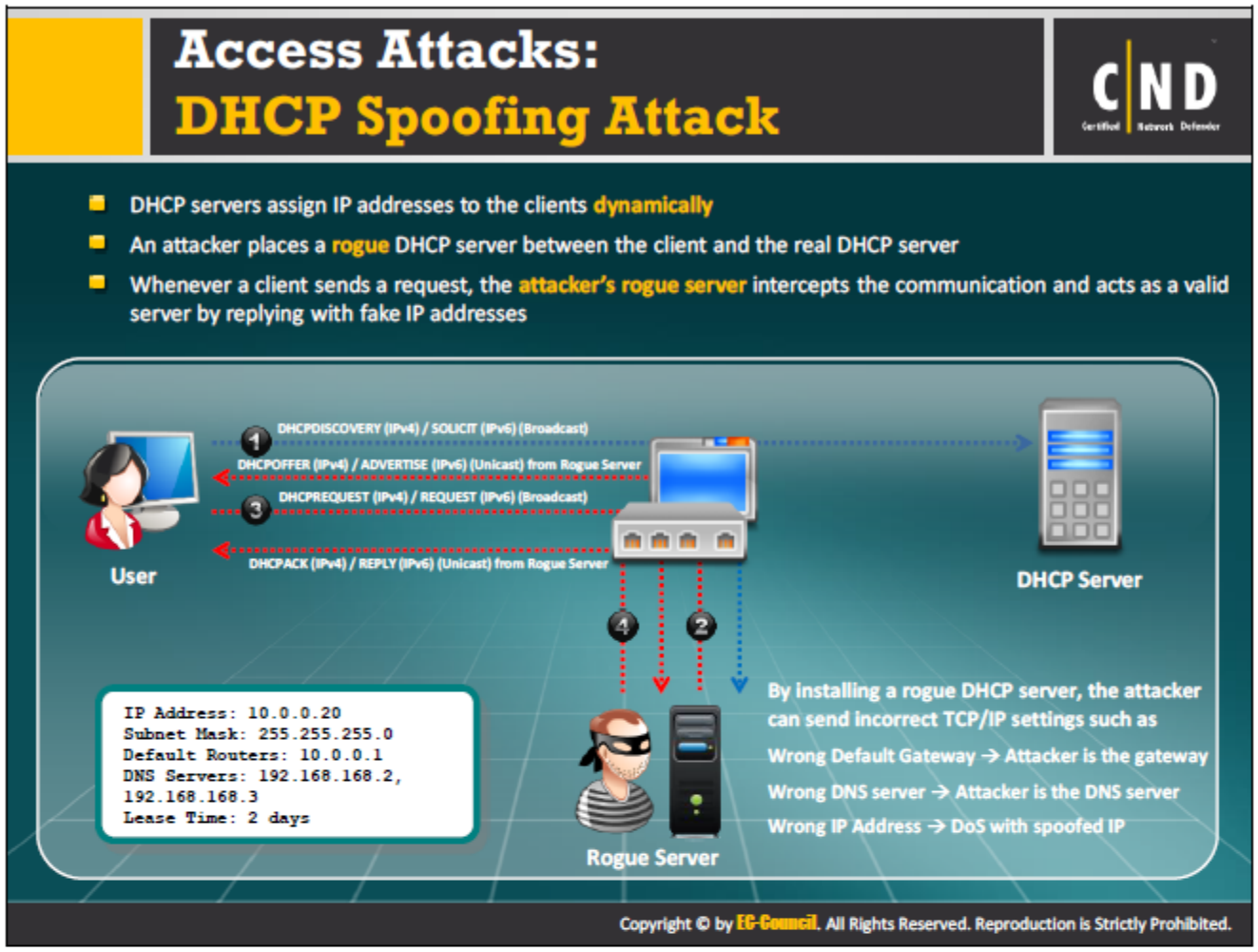
An attacker can craft a malicious ARP reply that contains an arbitrary IP and MAC address. Since the victim's computer blindly accepts the ARP entry into its ARP table, an attacker can force the victim's computer to think that the IP is related to the MAC address they want. An attacker can then broadcast their fake ARP reply to the victim's entire network.



In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a denial of service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network.

In a DHCP starvation attack, the attacker can broadcast a number of DHCP requests with spoofed MAC addresses. Sending many DHCP requests can consume the address space in the DHCP server. The DHCP starvation attack is similar to the Synchronization (SYN) flood attack. The victim network suffers a starvation of DHCP resources as the attackers are continuously broadcasting fake DHCP requests. The attackers can also place a rogue DHCP server in their system and respond to the DHCP requests from the victims or users. In the DHCP starvation attack, the attacker continuously sends many DHCP requests with fake MAC addresses. These request IP addresses from the DHCP server. The attacker continues the process until their request has completely utilized the space available in the DHCP server, disabling the victim from gaining an IP address. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Gobbler.

Port security is a method used in preventing the DHCP starvation attack. It limits the number of MAC addresses that can access the port. Only those MAC addresses having permission to access the port can send forward the packets. DHCP snooping is another method available in preventing the DHCP starvation attack. It filters the untrusted DHCP messages. The DHCP snooping is a Cisco catalyst switch feature that determines the port that can respond to the DHCP requests.

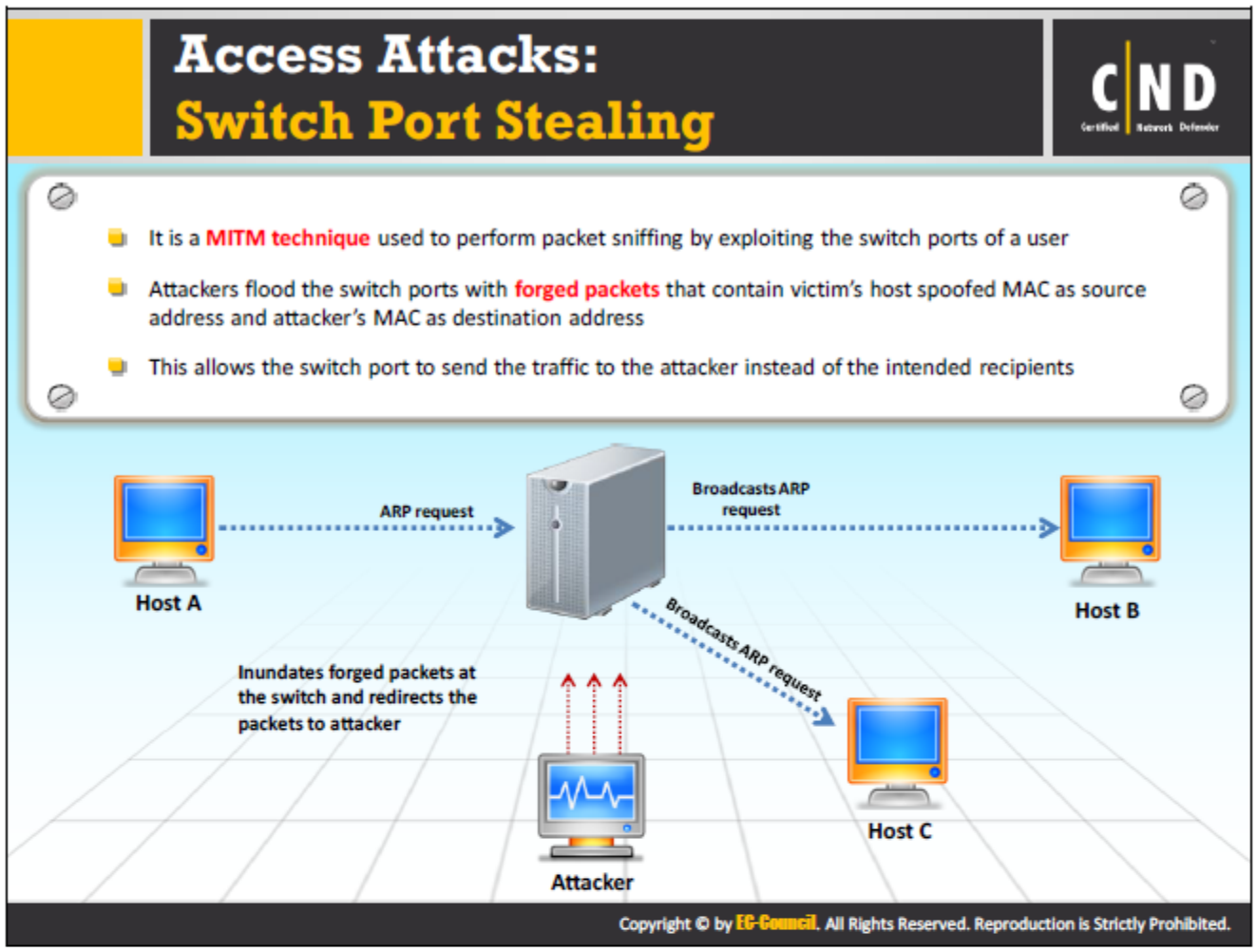


A DHCP Spoofing attack is also known as a rogue DHCP server attack. In a rogue DHCP server attack, an attacker will introduce a rogue server in the network. This rogue server has the ability to respond to client's DHCP discovery requests. Though both the servers respond to the request, i.e., the rogue server and the actual DHCP server, the server that responds first will be taken by the client. If the rogue server gives the response earlier than the actual DHCP server, the client takes the response from the rogue server instead. The information provided to the clients by this rogue server can disrupt their network access, causing a DoS.

The DHCP response from the attacker's rogue DHCP server may assign the IP address of an attacker as a client's default gateway. As a result, all the traffic from the client will be sent to the attacker's IP address. The attacker then captures all the traffic and forwards this traffic to the appropriate default gateway. From the client's viewpoint, they think that everything is functioning correctly. This type of attack cannot be detected by the client for a long period of time.

Instead of using the standard DHCP server, the client can use a rogue DHCP server. The rogue server directs the client to visit fake websites for the purpose of gaining their credentials.

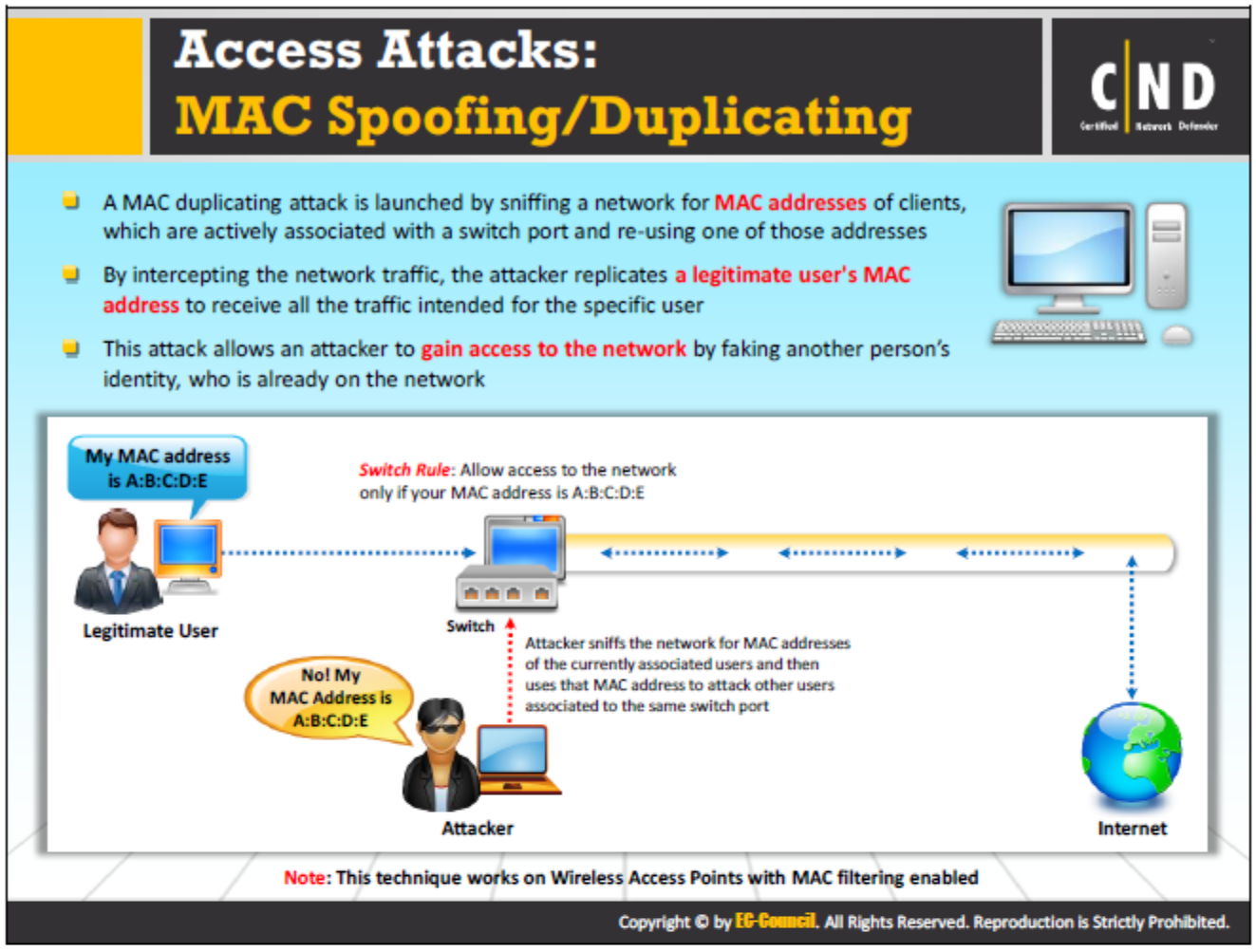
To mitigate a rogue DHCP server attack, set the interface to which that rogue server is connected to as untrusted. That action will block all ingress DHCP server messages from that interface.



Switch port stealing is a sniffing technique used by an attacker who spoofs both the IP address and MAC address of the target machine. Using a port stealing attack, attackers steal traffic destined to a specific port of an Ethernet switch. It allows an attacker to sniff the packets that were originally destined for another computer.

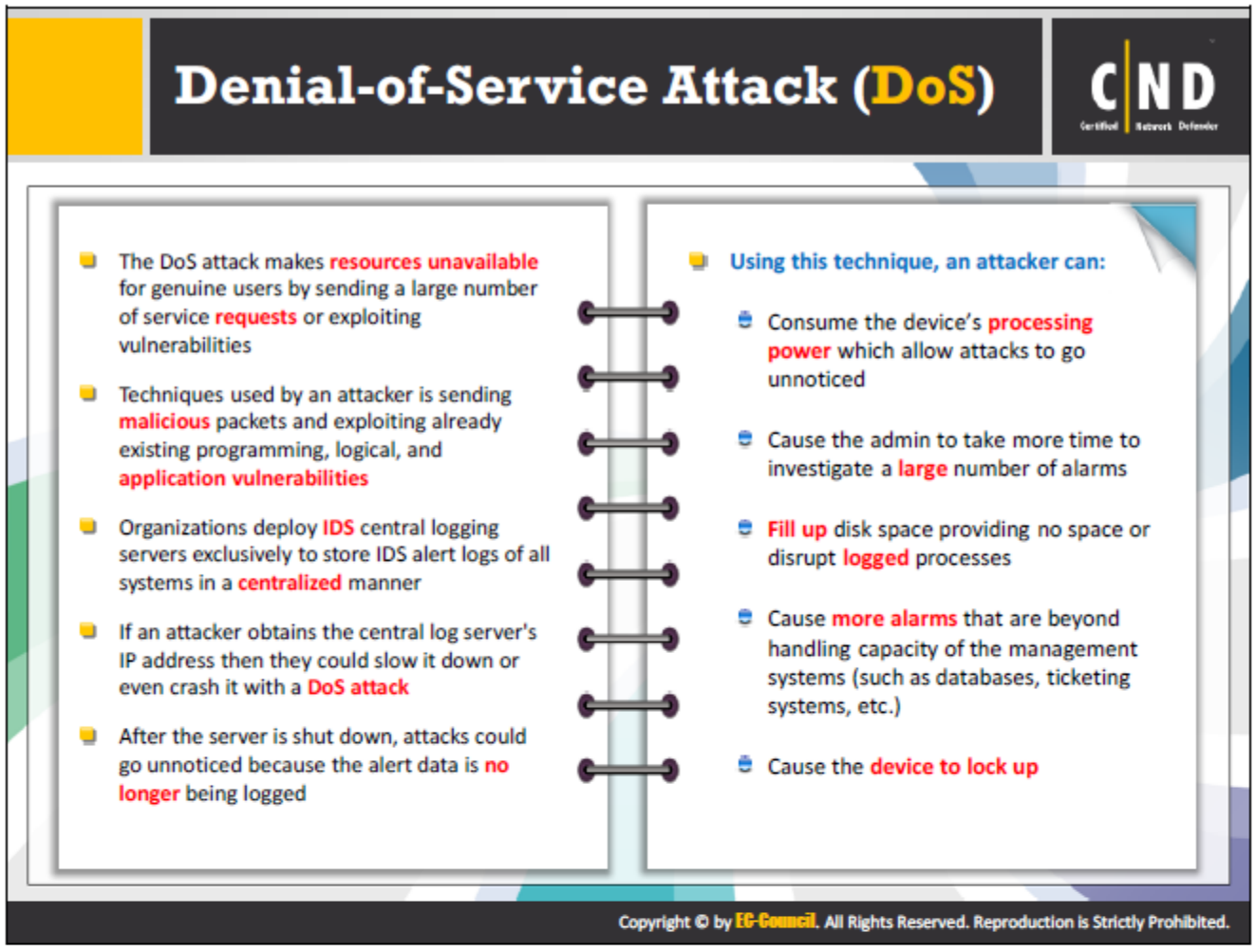
An attacker takes advantage of a switch's incapability of updating its address table dynamically. Ethernet switches learn and maintain information about who is connected to the port. This information includes IP and Mac addresses of the computers connected to the network. The switch is supposed to update this information dynamically. However, the switch is still static in a real network environment. For example, if computer connected to a particular port is moved to another port, the switch's address table entry will still point to the same computer only.

A MiTM technique is used to perform packet sniffing by exploiting the switch ports of a user. Attackers flood the switch ports with forged packets that contain the attacker's MAC address as the source address which is identical to the victim's host spoofed MAC and destination addresses. This allows the switch port to send traffic to the attacker instead of to the intended recipients.



Spoofing attacks allow attackers to spread malware, bypass authentication checks, or steal sensitive information. The attacker pretends to be a legitimate user on a network and gets access to restricted resources in order to perform malicious activities.

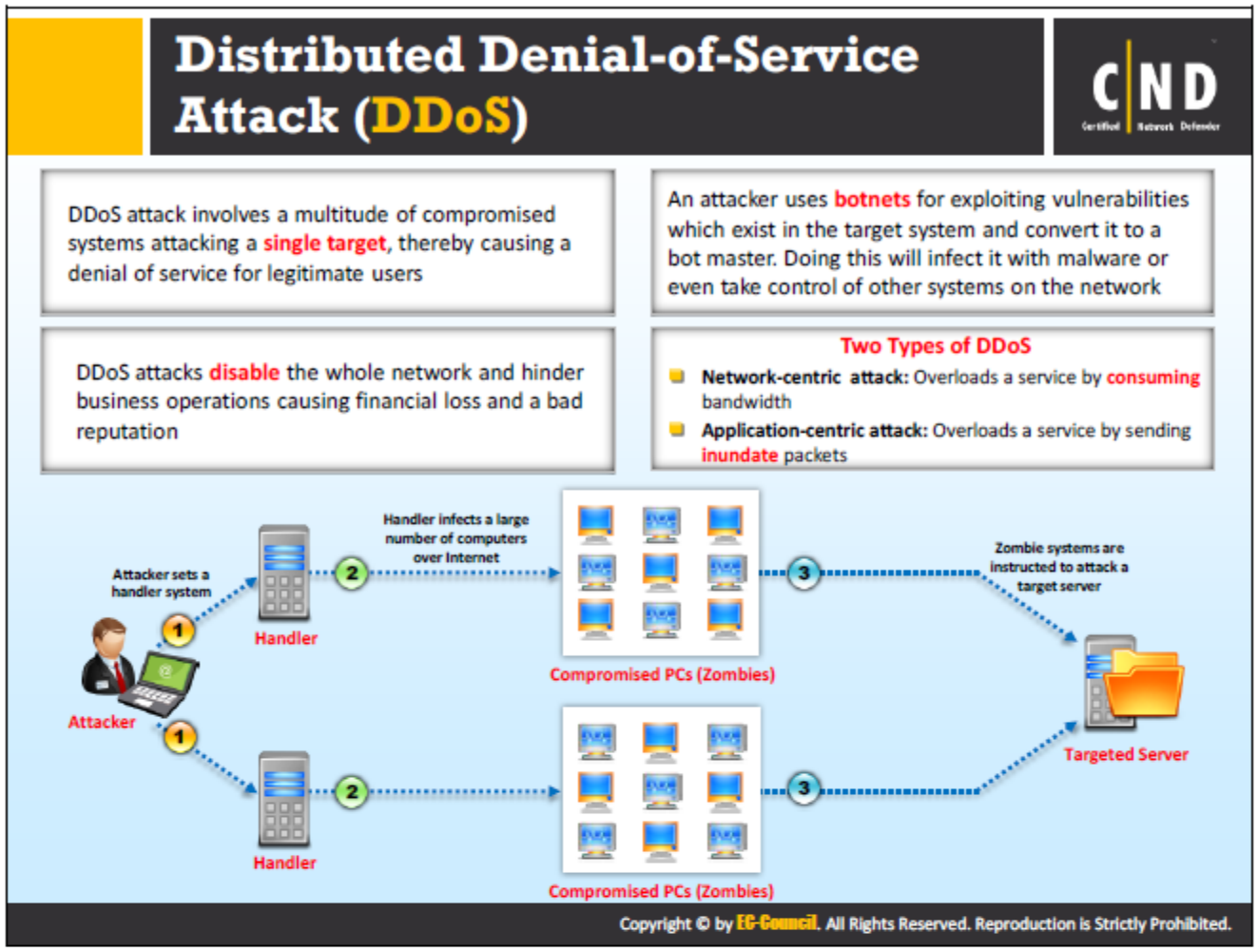
MAC duplicating refers to spoofing the MAC address with the MAC address of a legitimate user on the network. It involves sniffing a network for the MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs their own MAC address with the MAC address of the legitimate client. If the spoofing is successful, the attacker can receive all the traffic destined for the client. An attacker gains access to the network and will take over someone's identity who is already on the network.



Denial-of-service (DoS) is an attack that prevents authorized users from accessing a computer or network. DoS attacks target the network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, depriving legitimate users of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available operating system resources, so that the computer cannot process legitimate user requests.

Consider a company (Target Company) that delivers pizza upon receiving a telephone order. The entire business depends on telephone orders from customers. Suppose a person intends to disrupt the daily business of this company. If this person came up with a way to keep the company's telephone lines engaged in order to deny access to legitimate customers, the Target Company would lose business.

DoS attacks are similar to the pizza company situation. The objective of the attacker is not to steal any information from the target. It is to render its services useless. In this process, the attacker compromises many computers (called zombies) and virtually controls them. The attack involves deploying the zombie computers against a single machine to overwhelm it with requests and finally crash the target in the process.

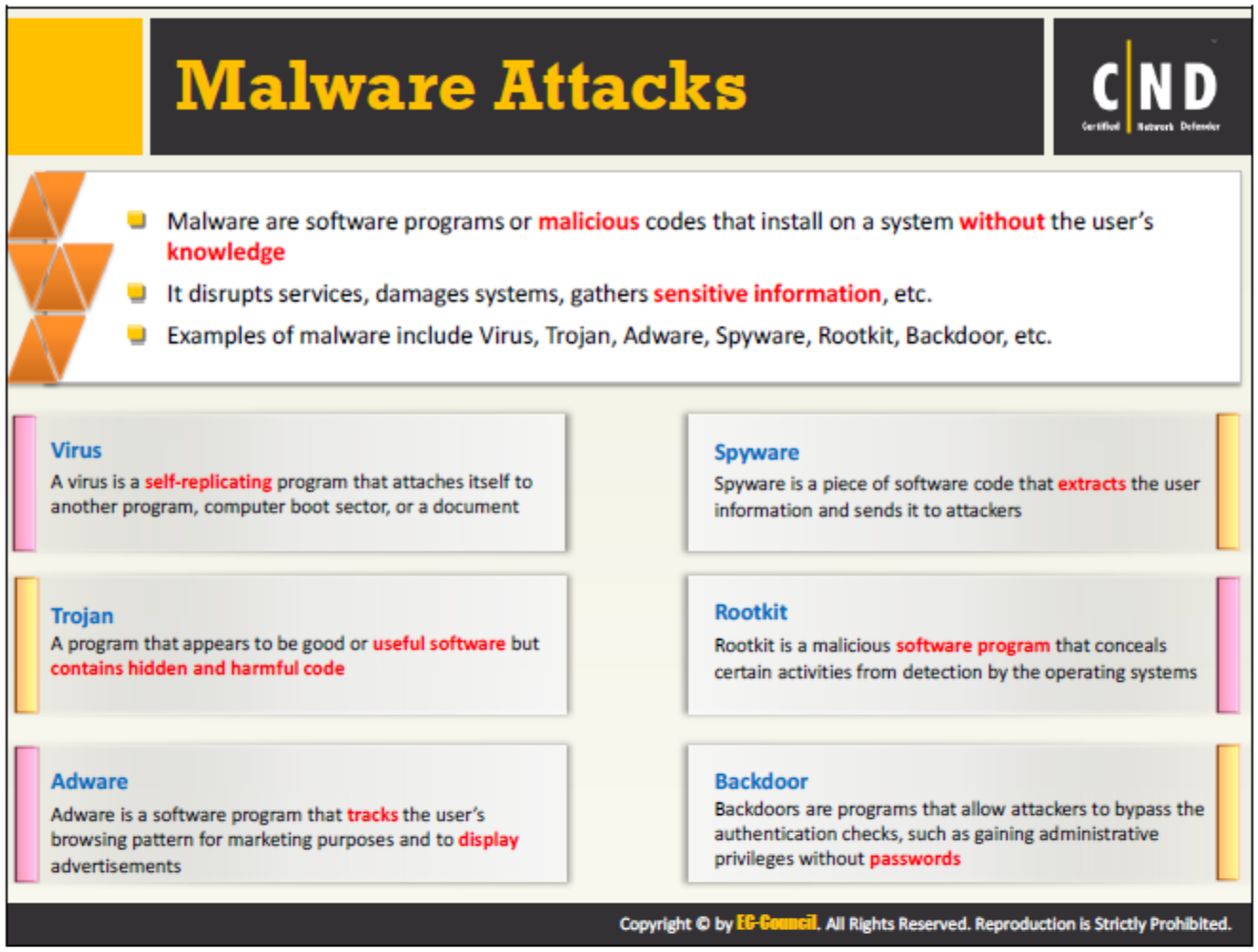


A distributed denial-of-service (DDoS) attack is a large-scale, coordinated attack on the availability of services on a target's system or network resources. Launched indirectly through many compromised computers on the Internet.

The services under attack are those of the "primary target," while the compromised systems used to launch the attack are often called the "secondary target." The use of secondary targets in performing a DDoS attack provides the attacker with the ability to wage a larger and a more disruptive attack, while making it more difficult to track them.

As defined by the World Wide Web Security FAQ: "A Distributed Denial-of-Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial-of-service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms."

If left unchecked, more powerful DDoS attacks could cripple or disable essential Internet services in minutes. DDoS attacks can be very dangerous because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of DDoS includes loss of goodwill, disabled network, financial loss, and disabled organizations. They are also used as decoys. Attacks use DDoS attacks to crash systems, while they then attack the real target. Administrators are busy with the DDoS and may not notice the real attack until it is too late.



Malware

Malware is a piece of malicious software that is designed to perform activities as intended by the attacker without user consent. It appears in the form of an executable code, active content, scripts or other forms of software. The attacker compromises system security, intercepts computer operations, gathers sensitive information, modify, delete or add content to a website, take control of a user's computer, etc. It is used against government agencies or corporate companies to extract highly confidential information.

Virus

A virus is a type of program that can duplicate itself by making copies of itself. The major criteria for categorizing a piece of executable code as a virus is that it replicates itself through hosts. A virus can only spread from one PC to another when its host is taken to the uncorrupted computer. For example, by a user transmitting it over a network or executing it on a removable media. Viruses can spread the infection by damaging files in a file system. Viruses are sometimes confused as worms. A worm can spread itself to other computers without the intent of the host. A majority of PCs are now connected to the Internet and to local area networks, increasing their spread. The virus spreads through the computer by itself and infects the file from one computer to another computer using a host. It reproduces its own code while enclosing other executables and spreads throughout the host. Some viruses reside in the memory and may infect programs through the boot sector. A virus can also be in an encrypted form infecting files in a symbolic form.

Armored Virus

An armored virus is a type of computer virus that is specifically coded with different mechanisms to make its detection difficult. It fools antivirus programs, making them believe the armored virus is located somewhere else in memory and making it difficult to detect and remove. There is another kind of armor that is implemented with complicated and confusing code, whose purpose is to hide the virus from being detected as well as develop a countermeasure. This mechanism makes it difficult for researchers to disassemble the virus. Therefore, it propagates longer before researchers find a countermeasure. It affects target users similar to a normal virus.

Trojan

A Trojan is a malicious program that masquerades as legitimate software. A Trojan horse attack is termed as a serious threat to system security. A victim may be under attack from the trojan, but they could also be used as an intermediary to attack others (without the knowledge of the victim). Most Trojans consist of two parts: server and a client. A server is a program that gets installed on the infected system. The client is also a program that is located on the attacker's computer. Both the server and client are used to establish a connection between the attacker and a victim's system via the Internet.

In the computer world, a Trojan can be described as a hateful security-breaching program that is impersonates an application and is illegal. For example, if the user downloads what appears to be a movie or a music file and then clicks on the file to open it, the file will instead unleash a dangerous program that erases the disk.

Trojan horses can also access the programs remotely. It can delete files, send files to the intruder, modify the files, installs other programs that provide unauthorized network access and execute privilege-elevation attacks. A Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If a Trojan compromises a system in a shared network, the attacker records user names and passwords or other sensitive information as it navigates across the network.

Adware

Adware is a software program that tracks the user's browsing patterns for marketing purposes and displaying advertisements. It collects the user's data, such as what types of Internet sites the user visits in order to customize the adverts that are relevant to the user. Legitimate software is embedded with adware programs to generate revenue. Adware is considered as a legitimate alternative provided to customers who do not wish to pay for software. Software developers look to adware as a way to reduce development costs and increase profits. It enables software developers to offer software at no cost or at a reduced price. Software developers are motivated to design, maintain and upgrade their software product and generate revenues using adware. It has become a large platform with millions of users and has attracted attackers looking to perform attacks through exploiting adware.

Legitimate adware requests a user's permission before collecting user data. If a legitimate adware is used and you remove or uninstall it, the ads should disappear. Further, there is an

option to disable ads by purchasing a registration key. When user data is collected without a user's permission, it is malicious and termed as spyware. It should be avoided for privacy and security reasons. Malicious adware gets installed on a computer using cookies, plug-ins, file sharing, freeware and shareware. It consumes more bandwidth, exhausts CPU resources and memory. Attackers perform spyware attacks and collect information from the target user's hard drive, the websites visited or keystrokes typed in order to misuse and perform fraud.

Common adware programs include toolbars on a user's desktop or those that work in conjunction with the user's web browser. Adware performs advanced searching of the web or a user's hard drive and may provide better organization of bookmarks and shortcuts. Adware typically requires an Internet connection to run. There is more advanced adware that includes games and utilities that are free to use but users need to watch advertisements until the program opens. For example, while watching "YouTube videos", users need to wait until the ad is completed before watching the video.

Spyware

Spyware is a piece of software code that extracts the user's information and sends it to attackers. It enables pop-up advertisements to appear, modifies computer settings, redirects users to fake webpages or changes the home page of the browser. Users are not really aware of spyware being installed on their computer. Most of the time, spyware is used to track cookies and display unwanted pop-up ads. Its presence is hidden from the user and it is difficult to detect. Keylogger is a type of spyware used by attackers to record keystrokes entered by the user.

Spyware infects a user's system when they visit a fake website containing malicious code which is controlled by the spyware author. This malicious code forces the spyware download and its installation. It also gets infected by manipulating loop holes in the browser or software, by binding itself with trusted software, etc. Once the spyware is installed, it monitors the user's activities on the Internet. It gathers information such as usernames, passwords, bank account details, credit card numbers, etc., and sends it to the attacker.

When a system is infected by spyware, its performance degrades. It disables the software firewall, antivirus software, reduces browser security settings and makes it more vulnerable to attacks. Applications will freeze, failure to boot, etc. Spyware that interferes with networking software makes it difficult to connect to the Internet. It steals information from users by utilizing the target computer's memory resources and bandwidth allocated for an Internet connection. Since spyware uses memory and system resources, there are chances of system crashes.

Rootkits

Rootkit is a software program that hides its activities from detection and performs malicious activities to get privileged access to a target computer. It hides the fact that the operating system is compromised by the attackers. A successful rootkit can potentially remain in place for years if it remains undetected. Rootkits are used to hide viruses, worms, bots, etc., and it is difficult to remove them. Malware that is hidden by rootkits are used to monitor, filter or steal

sensitive information and resources, change the configuration settings of the target computer and other potentially unsafe actions.

Rootkits are installed by attackers after gaining administrative access either by manipulating a vulnerability or cracking a password. The attacker gets full control over the target system, they can modify files and existing software that detects rootkits.

Rootkits are activated each time the system is rebooted. It gets activated before the operating system completes booting. So it is difficult to detect the presence of a rootkit. Rootkits install hidden files, processes, hidden user accounts, etc., in the system's operating system to perform malicious activities. It intercepts the data from terminals, keyboard and network connections and allows the attacker to extract sensitive information from the target user. Rootkits gather user's sensitive information such as usernames, passwords, credit card details, bank account details, etc., in order to misuse the information to commit fraud or other illegal activities.

Backdoors

Attackers create backdoors to compromise the security of the target systems and gain access to a network illegitimately. Attackers insert small programs that bypass the authentication check such as gaining administrative privileges without passwords. The attacker installs programs and controls the victim's computer remotely. Attackers use backdoors to get access to a network and keep returning by using the same exploit.

It is difficult for the system administrators to block access to attackers using backdoors. Even if the system administrator detects a backdoor attack and changes the password, the attacker is still able to get access to the resources of the infected system. If the attacker believes that system administrator detected access, then they can simply choose to locate another vulnerability to avoid being detected. Backdoors are not logged and appear as if no one is online, while the attacker continues to use the infected machine.

Password cracking is a common type of backdoor attack used to breach network security and systems connected to the network. Accounts that are unused or not used frequently are exploited by attackers to perform backdoor attacks. Password crackers detect the accounts with weak passwords and create an access point by changing the password. System administrators are not able to identify fragile accounts because the accounts with modified passwords do not appear and they believe that everything is operating normally. System administrators find it difficult to determine which accounts are not used in order to lock them.

Logic Bomb

A logic bomb is a piece of software code that performs a malicious action when a logic condition is satisfied. For example: Crashing a program on specific date using. When a logic bomb explodes, it is designed to display an unauthentic message, delete data or completely reformat hard drives, send sensitive information to untrusted parties, disable a network for a certain length of time and cause harm to the target computer. Malicious software such as a virus, use logic bombs to spread before being noticed.

Logic bombs are used to demand money for software by developing a code that makes the software a trial version. After a specific number of days, the user has to pay a specified amount

to continue to use the software. Logic bombs are used to blackmail target users. If the demand is not met, the logic bomb explodes into the computer network and corrupts, deletes data or performs malicious activities as intended by attackers.

Attackers use the combination of spyware and a logic bomb to steal the identity of a target user. Spyware allows attackers to install keyloggers secretly and capture the keystrokes. A logic bomb is designed to wait until the targeted user visits a website requiring a login with their username and password. It then triggers the logic bomb to execute a key logger to capture the user credentials and send it to the remote attacker.

Botnets

A botnet is a collection of compromised computers connected to the Internet to perform a distributed task. Attackers distribute malicious software that turns a user's computer into bots. A bot refers to a program or an infected system that performs repetitive work or acts as an agent or as a user interface to control other programs. The infected computer performs automated tasks without the user's permission. Attackers use bots to infect a large number of computers. Cyber-criminals who control bots are called a botmaster. Bots spread across the Internet and search for vulnerable and unprotected systems. When it finds an exposed system, it quickly infects and reports back to the botmaster.

Attackers use botnets to distribute spam emails, carry out denial-of-service attacks and automated identity theft. A computer part of a botnet might slow down its performance. Botmasters use infected computers to perform various automated tasks. They instruct the infected systems to send viruses, worms, spam, spyware, etc. Botmasters steal personal and private information from the target users such as credit card numbers, bank details, usernames, passwords, etc. Botmasters launch DoS attacks on a specific target user and extort money to regain control over the compromised resources. Botmasters use bots to boost web advertising billings by automatically clicking on internet ads.

Bots enter a target system using a payload in a Trojan horse or similar malware. It infects the target system through drive-by-downloads, or by sending spam mails that are embedded with malicious content.

Ransomware

Ransomware is a type of malicious software that locks or encrypts valuable files available in the victim's computer until a ransom is paid. Unlike other malware it does not hide, it displays a message on the infected system that "your files are taken away for ransom and you need to pay money in order to decrypt it". It redirects victims to different sites and provides information regarding how to make payment to recover the data back. During payment, attackers often collect credit card details that may result in further financial losses. Moreover, there is no guarantee the data will be recovered, even if the payment is made.

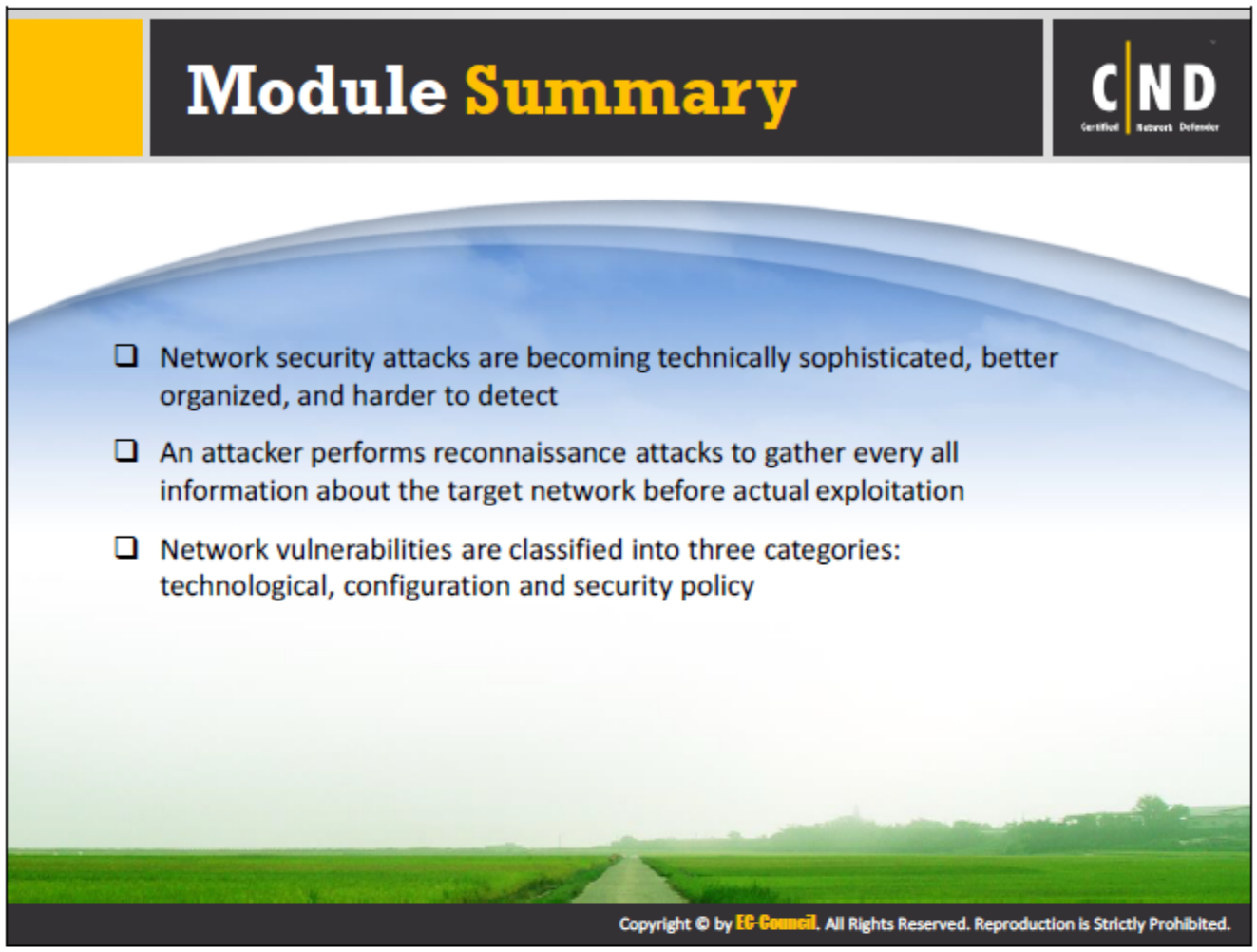
Ransomware gets installed when a user clicks on a malicious link in an email attachment or instant message or on a social networking site. It gets installed even when the user visits an infected site or clicks on an infected pop-up advertisement. Ransomware demands are displayed either in a text file or on a web page in the browser.

This type of malware takes advantage of a victim's embarrassment, surprise or fear to satisfy the ransom demands. For example, attackers put time pressure on a victim stating that their data gets destroyed every 30 minutes if they do not make a payment. If the payment is not done within the time span, the files cannot be recovered. Other ransomware forces users to purchase a product to recover the data back. Some ransomware tricks or embarrasses users to pay the ransom by stating they have been watching illegal content and must pay a fine.

Polymorphic malware

Polymorphic malware is a destructive and intrusive malware code that changes its signature to avoid pattern matching detection by antivirus programs. The functionality remains the same even though its signature changes. For example, a spyware program working as a keylogger continues to perform the same action, even if its signature changes. If a polymorphic malware is detected and its signature is added to a downloadable database for an antivirus program, it fails to detect the same malware with the modified signature.

Polymorphic malware code (payload) is encrypted in order to hide and make it difficult to read by antivirus programs. Polymorphic behavior is gained by malware when the mutation engines are bundled with another payload such as viruses, worms, or Trojans. It allows different subversions of the same code but with the same functionality. It modifies the file names, encrypts the data with variable keys, compresses the files etc.



The module has addressed various network security concerns that affect an organization's business continuity. The module described various types of network threats, vulnerabilities and attacks. With this module, students know and understand how an attacker exploits and compromises the security of the network.