

Network Fundamentals & Types of Network Attacks

Distributed
Denial of
Service Attacks

Botnets

Browser
Attacks

Brute Forcing

SSL
Compromise

Backdoors

ShellShock
Attacks

Miscellaneous
Attacks

Essential Terminologies

Threat	Vulnerability	Attack
An action or event that can potentially compromise security	Existence of a weakness , design or implementation error that can lead to an unexpected and undesirable event compromising the security of the system	An assault on the system security derived from an intelligent threat
A threat is a potential violation of security		An attack is any action violating security

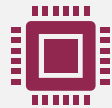
Network Security Concerns



Network Security is one of the primary concerns for **organization worldwide**



Potential threats to network security are evolving each day



Network security attacks are becoming technically more **sophisticated, better organised and harder to detect**



Organizations are failing to **defend themselves against rapidly increasing network attacks** due to **lack of network security skills**

Why Network Security Concerns Arise



Hardware or Software Misconfiguration

Insecure or poor design of the network

Inherent technology weaknesses

Careless approach of end users

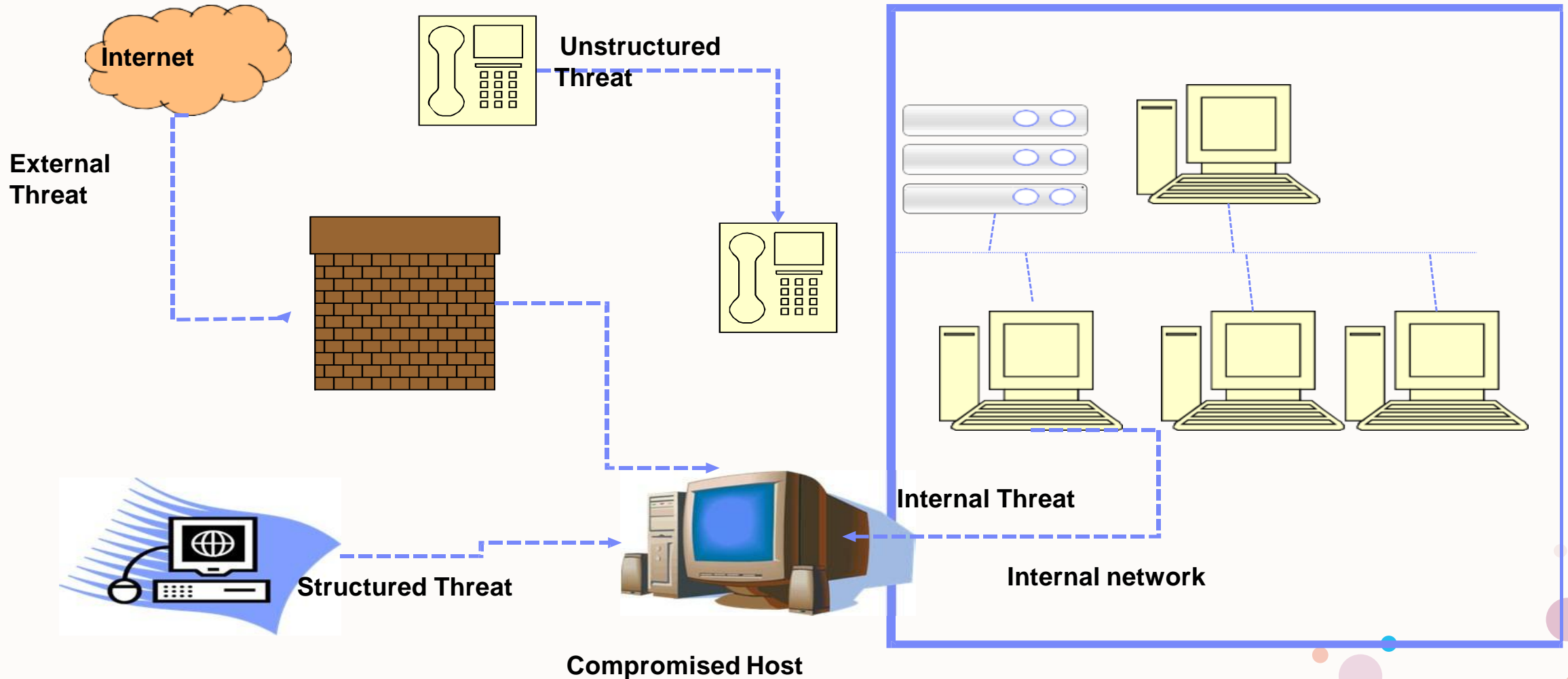
Intentional acts from end users



Types of Network Security Threats

Type of Threat	Origin of Threat
Internal Threats	Arise from internal employees with access to networks and other internal resources
External Threats	Arise from individuals who do not have direct access to the network
Unstructured Threats	Arise from Unskilled individuals who attack the network out of curiosity
Structured Threats	Arise from individuals who are highly motivated and technically competent

Different Types of network security threats

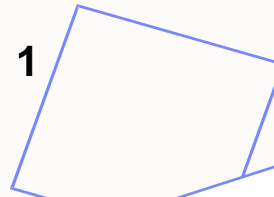


How does a Network Security Breach Affect Business Continuity

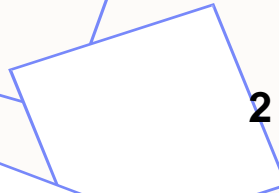
Disruption or even shutdown of the business



1



2



Loss of Productivity



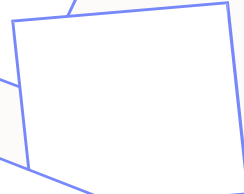
Loss of Privacy



3



4



Data Loss/Theft



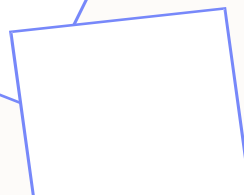
Legal Liability



5



6



Reputation Damage & loss of Consumer Confidence



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, Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (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

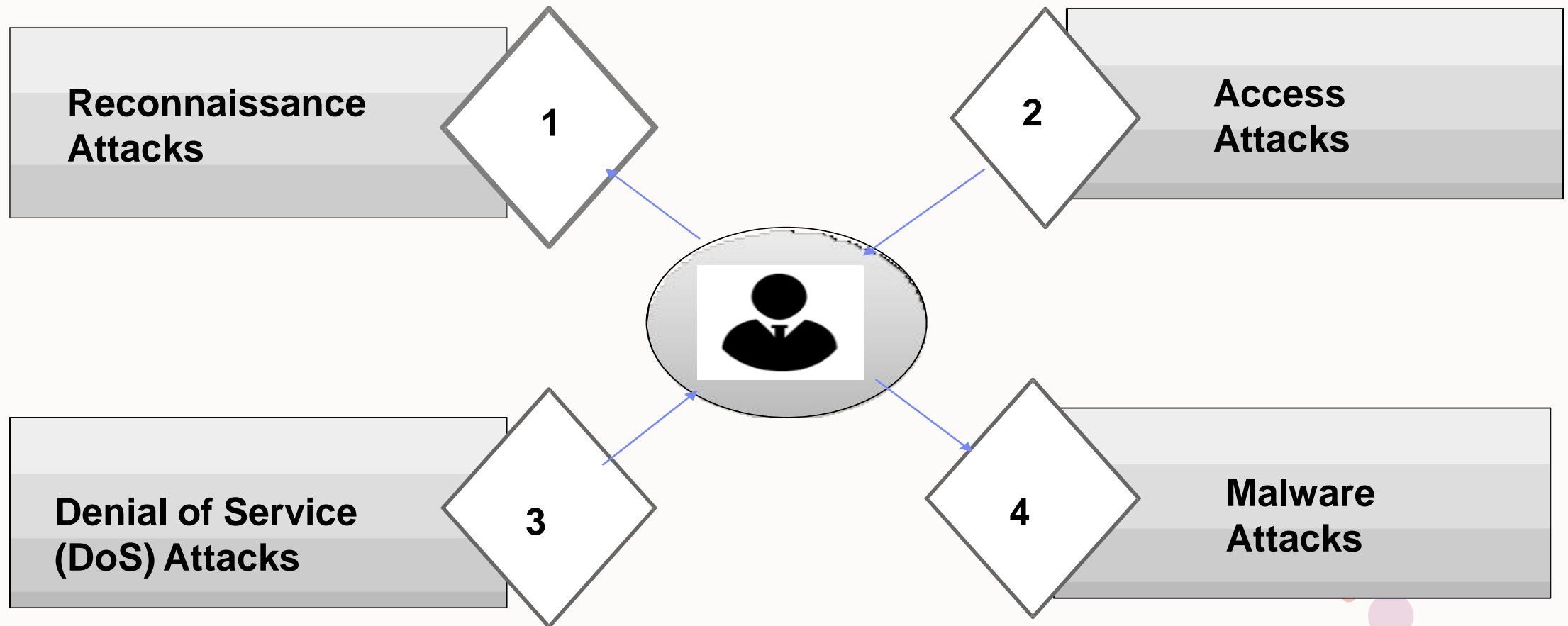
- RIP (Routing Information Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)

Types of Network Security Vulnerabilities: Security Policy

- Vulnerabilities due to weak security policy implementation & enforcement

Vulnerabilities	Description
Unwritten Policy	Unwritten security policy is difficult to implement and enforce
Lack of continuity	Lack of continuity in implementing and enforcing the security policy
Politics	Politics makes it difficult to implement a consistent security policy
Security Policy unawareness	Lack of awareness for the security policy

Network Security Attacks



The background features several large, overlapping circles with different patterns and colors. A large pink circle with a dense pattern of small blue dashes is in the top left. A light blue circle with a blue cross and a stylized flower in the center is in the top middle. A pink circle with white wavy lines is in the top right. A yellow circle with two strings of blue and white triangular bunting is in the bottom left. Scattered around these are smaller solid circles in pink, dark purple, and light blue.

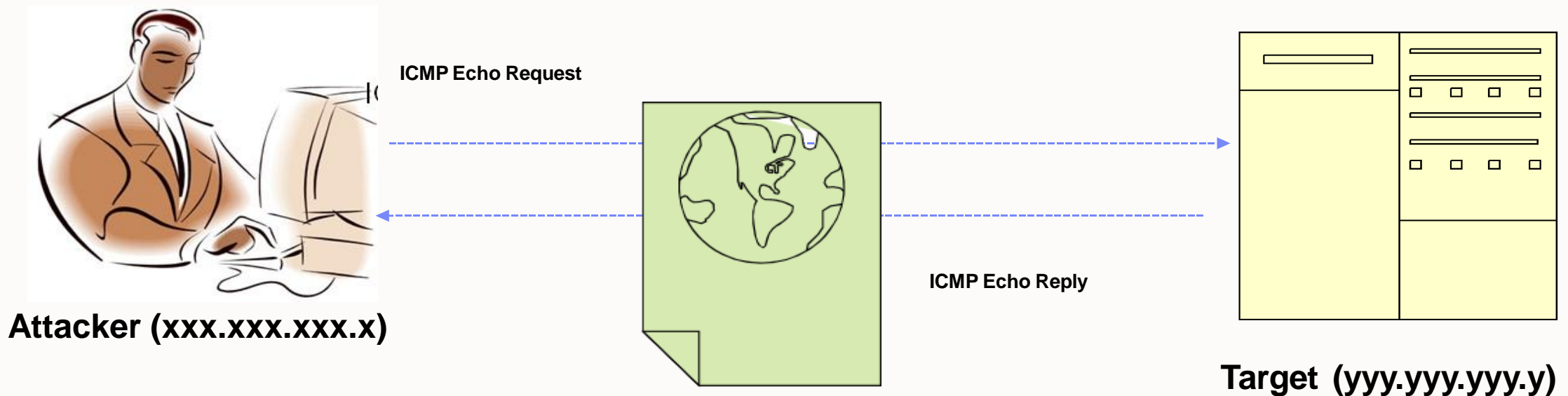
Reconnaissance Attacks

Reconnaissance Attacks

- In Reconnaissance Attacks, attackers make an attempt to discover the target network's information
- The aim of this attack is to gather all possible information about the target network
- Exploitation of the target network begins with reconnaissance
- Attackers gain the network information using different techniques such as :
 - Social Engineering
 - Port Scanning
 - DNS Footprinting
 - Ping Sweeping
- Network Information is obtained
 - using Reconnaissance Attacks :
 - Domain Name
 - Internal Domain Names
 - Network Blocks
 - IP Addresses of the Reachable Systems
 - Rogue Websites/Private Websites
 - TCP and UDP Services running
 - Access Control Mechanisms & ACL's
 - Networking Protocols
 - VPN Points
 - IDSes Running
 - Analog/Digital Telephone Numbers
 - Authentication Mechanisms
 - System Enumeration

Reconnaissance Attacks: ICMP Scanning

- An attacker sends an ICMP ECHO request to detect live hosts within a network
- They use tools such as NMAP to send ICMP ECHO requests





Reconnaissance Attacks: DNS Footprinting

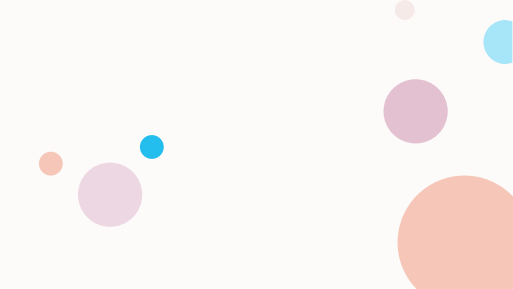
- An attacker gathers DNS information to determine the key hosts in the network and perform social engineering attacks.
- They use DNS interrogation tools to perform DNS Footprinting.
- DNS records provide important information about the location and type of servers.

Reconnaissance Attacks: Network Information Extraction using Nmap

- Nmap is a network discovery and security auditing tool.
- It is one of the most popular tools that hackers use for network discovery.
- 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.



Reconnaissance Attacks: Port Scanning

- Port scanning is the process of checking which services are running on the target computer
 - Involves sending a sequence of messages in an attempt to break in
 - Hackers may use various techniques to find open ports on the target
 - Hackers use Nmap to perform Port scanning
- 

Reconnaissance Attacks: Social Engineering

- **Social Engineering is the human side of breaking into a corporate network**
- **Social Engineering is nontechnical intrusion that relies heavily on human interaction**
- **It involves tricking other people to break normal security procedures**
- **Organizations are vulnerable to social engineering attacks even after implementing various technical network security measures**
- **Social Engineering attacks occur at two levels :**
 - **Physical**
 - **Psychological**

Access Attacks



Access Attacks

Password Attacks

Network Sniffing

Man in the Middle Attack

Replay Attack

Privilege Escalation

DNS Poisoning

DNS Cache Poisoning

ARP Poisoning

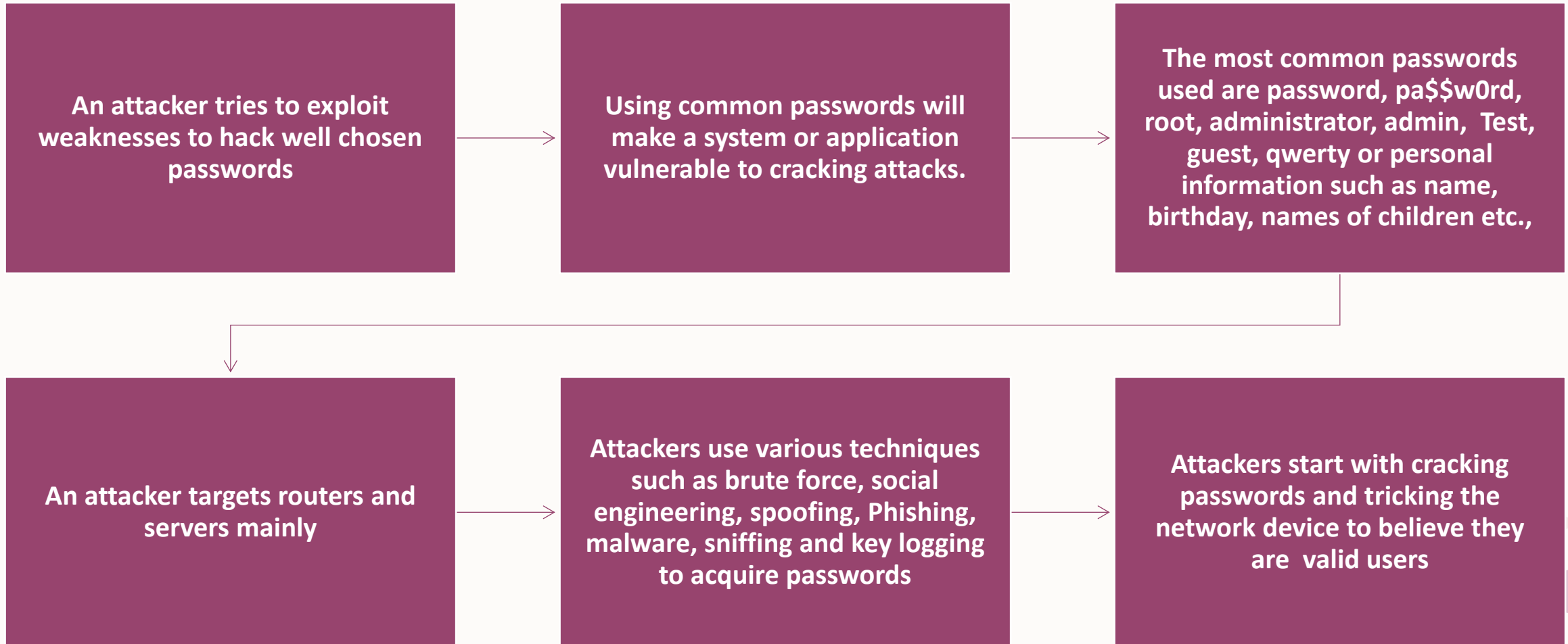
DHCP Starvation

DHCP Spoofing Attack

Switch Port Stealing

MAC Spoofing / Duplicating

Access Attacks : Password Attacks



Password Attack Techniques



Dictionary Attack

A dictionary file is loaded into the tracking application that runs against user accounts



Brute Forcing Attack

The program tries every combination of characters until the password is broken



Hybrid Attack

It works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password



Birthday Attack

It attracts cryptographic hash functions based on the probability that if a hashing process is used for creating a key, then the same is used for other keys

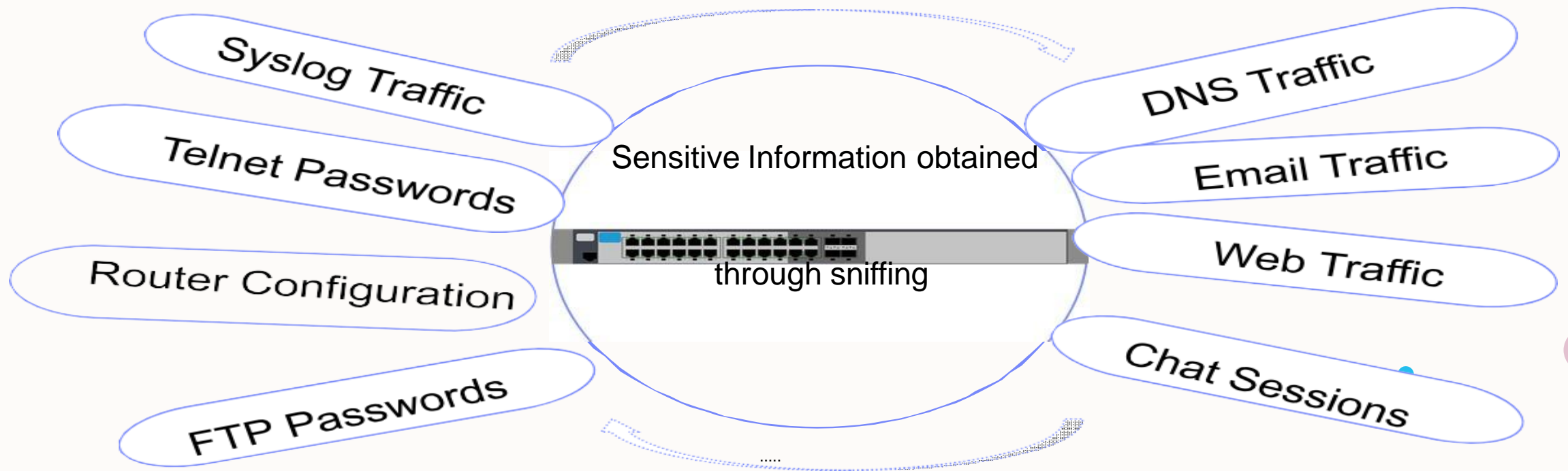


Rainbow Table Attack

It attacks rainbow tables that store precomputed hash values in plaintext

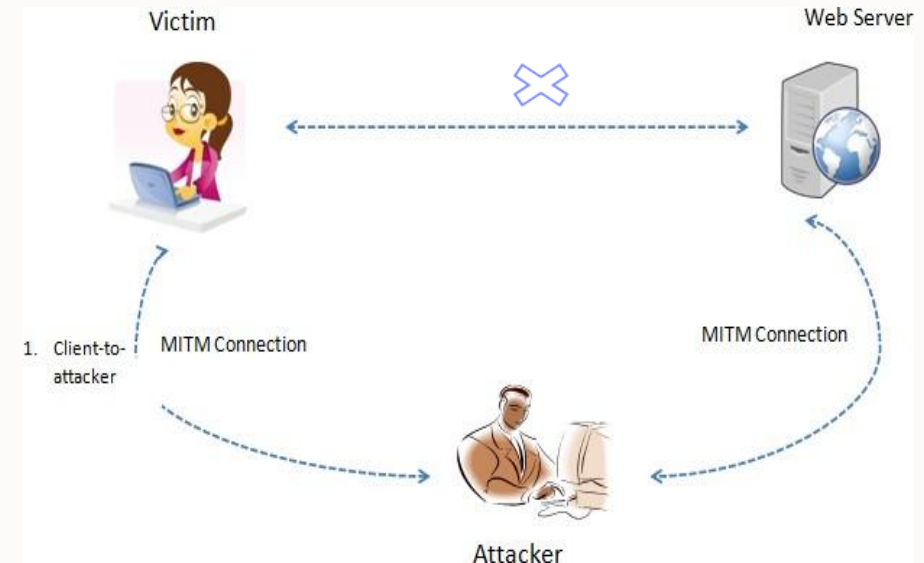
Access Attacks: Network Sniffing

- Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools
- Attackers use various sniffing utilities to sniff network traffic to gain sensitive information
- Organizations often leave their switch ports open
- Anyone in the same physical location can plug into the network using an ethernet cable



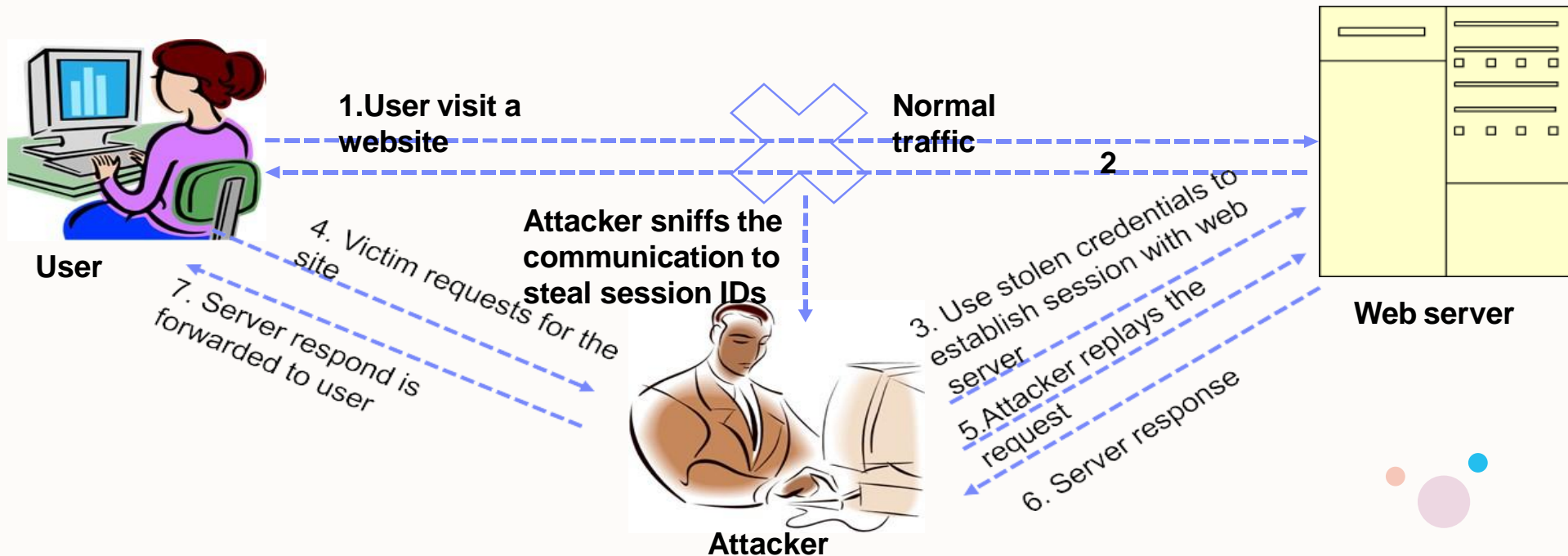
Access Attacks: Man in the Middle Attack

- In this attack, the intruder sets up a station in between the client and the server communication system to intercept messages being exchanged
- Attackers use different techniques to split the TCP connection into two connections
 - Client to attacker connection
 - Attacker to server connection
 - Interception of the TCP connection allows an attacker to read, modify and insert fraudulent data into the intercepted connection
 - In the case of an http transaction, the TCP connection between the client and the Server becomes the target



Access Attacks : Replay Attack

- A replay attack is an extension of the man in the middle attack that occurs after a two-way communication is intercepted
- A Hacker captures the data to obtain usernames and passwords
- Packets and authentication tokens are captured using a sniffer
- After the relevant information is extracted, the tokens are placed back onto the network to gain access

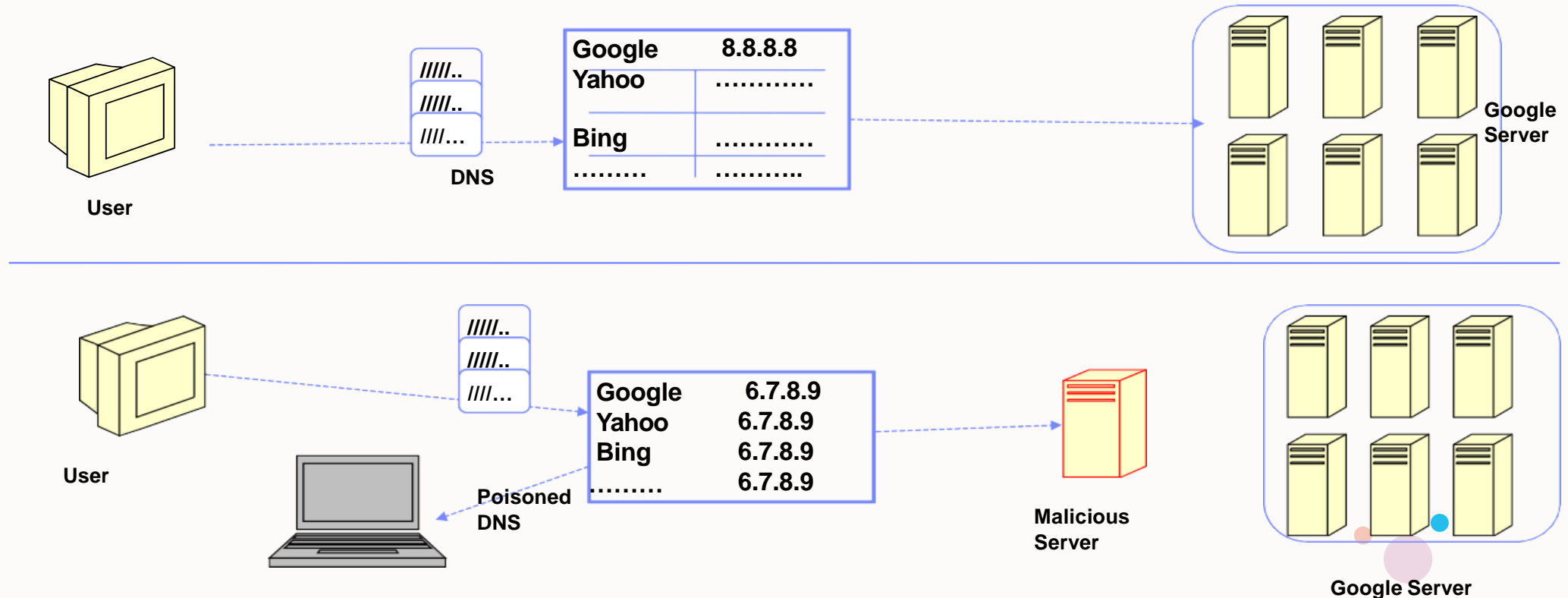


Access Attacks : Privilege Escalation

- A Hacker can gain access to a network using a non admin user account leading to gaining administrative privileges
- A Hacker performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs and configuration oversights in the Operating system and software applications to gain administrative access to the network and its associated applications
- These privileges allows a hacker to view private information, delete files, install malicious programs such as viruses, trojans, worms etc.,
- Types of Privilege Escalations
 - Vertical Privilege Escalations
 - Grant Higher privileges or higher level of access
 - Kernel level operations that permit unauthorized code to run
 - Horizontal Privilege Escalations
 - Use the same privileges or level of access while assuming the identity of another user

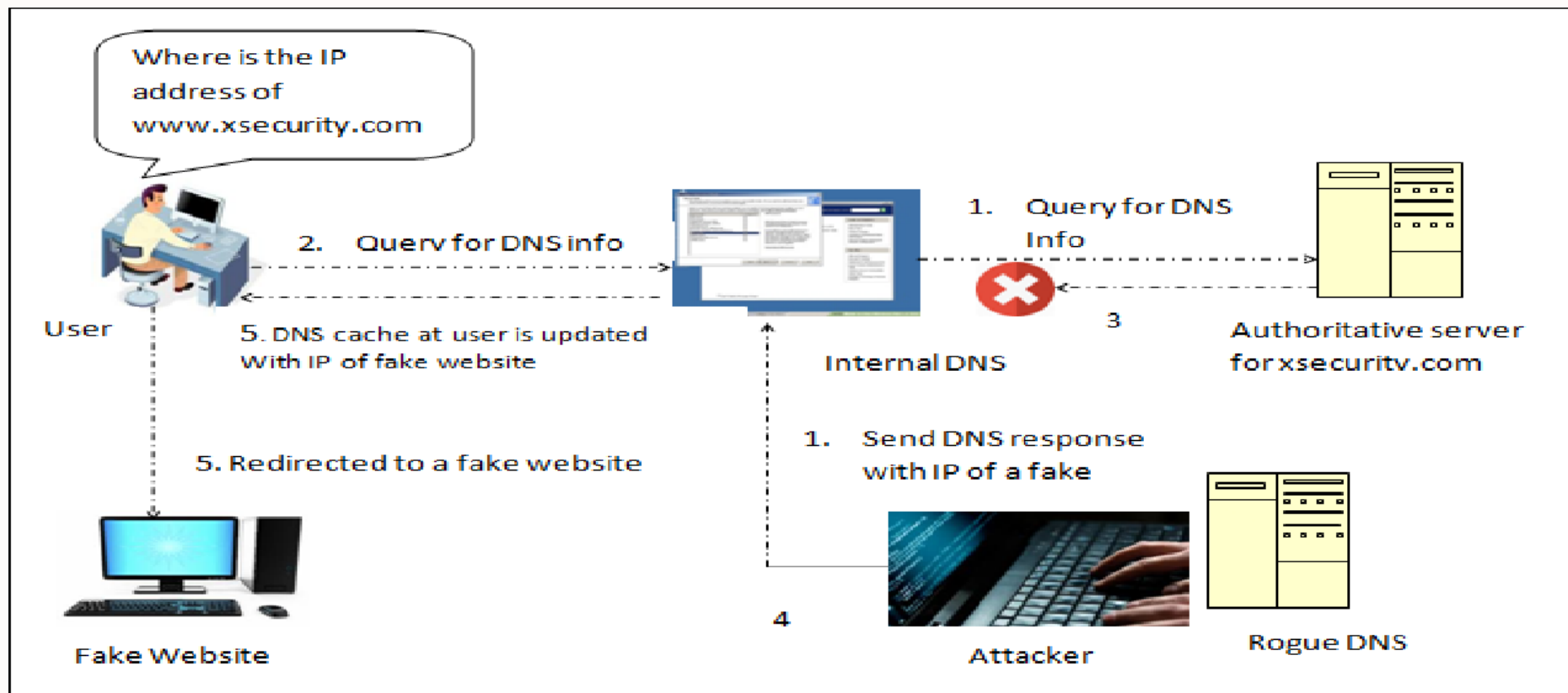
Access Attacks: DNS Poisoning

- Domain Name Server (DNS) poisoning is an unauthorized manipulation of IP addresses in the domain naming server cache
- The DNS holds domain name translations of the IP addresses for network devices
- A corrupted DNS redirects a user request to a malicious website to perform illegal activities.
- If a victim types www.google.com, the request is redirected to fake website www.goggle.com



Access Attacks: DNS Cache Poisoning

- DNS Cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site
- If the DNS resolver cannot validate that the DNS responses are coming from an authoritative source, it will cache the forged DNS entries locally and serve this forged DNS to users when someone makes the same DNS request

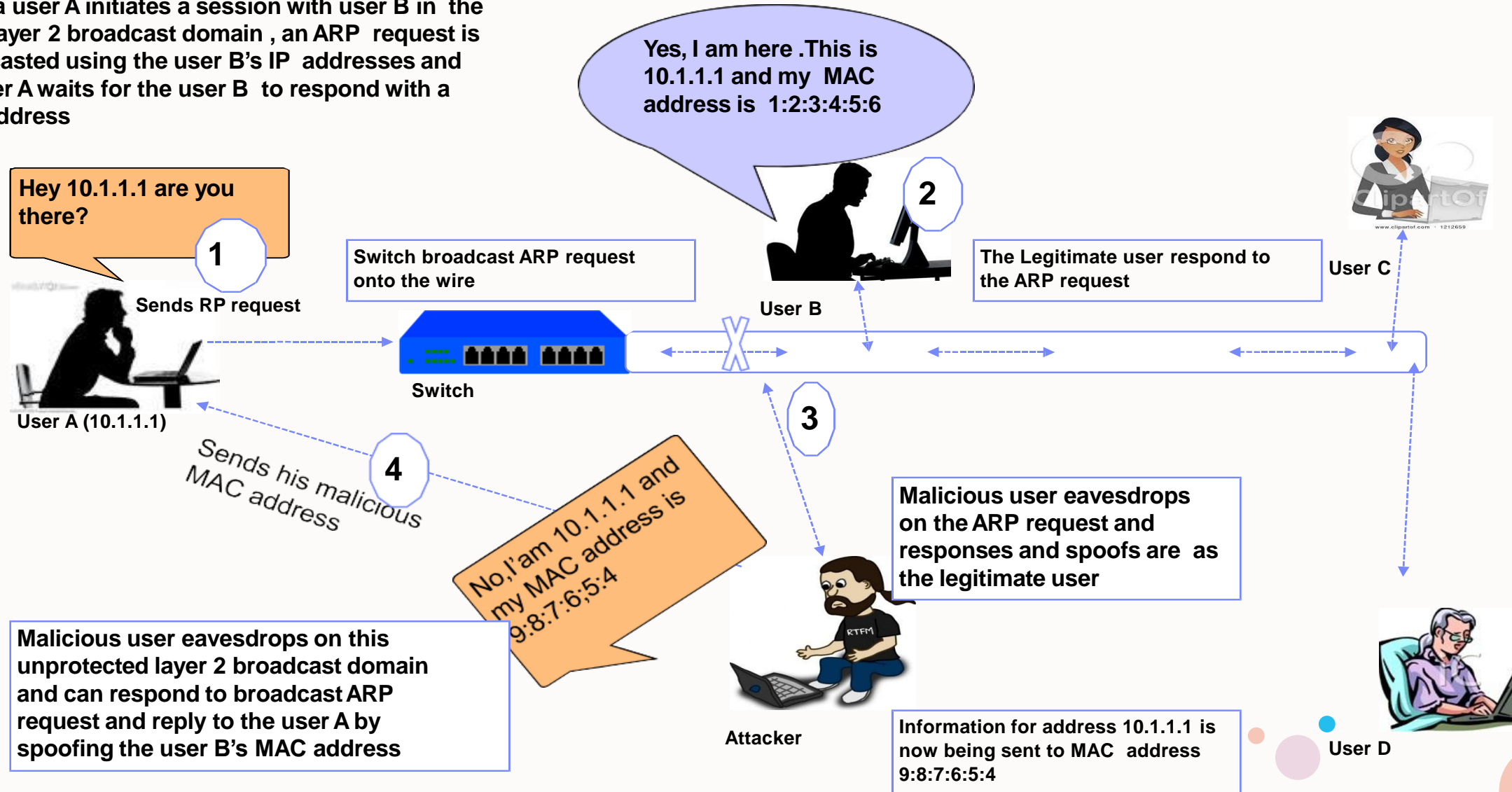


• Access Attacks: ARP Poisoning

- Address Resolution Protocol (ARP) is a protocol used for mapping an IP address to a physical machine address which is recognized in the local network
- ARP spoofing/poisoning involves sending a large number of forged entries to the target machine's ARP cache or overloading a switch

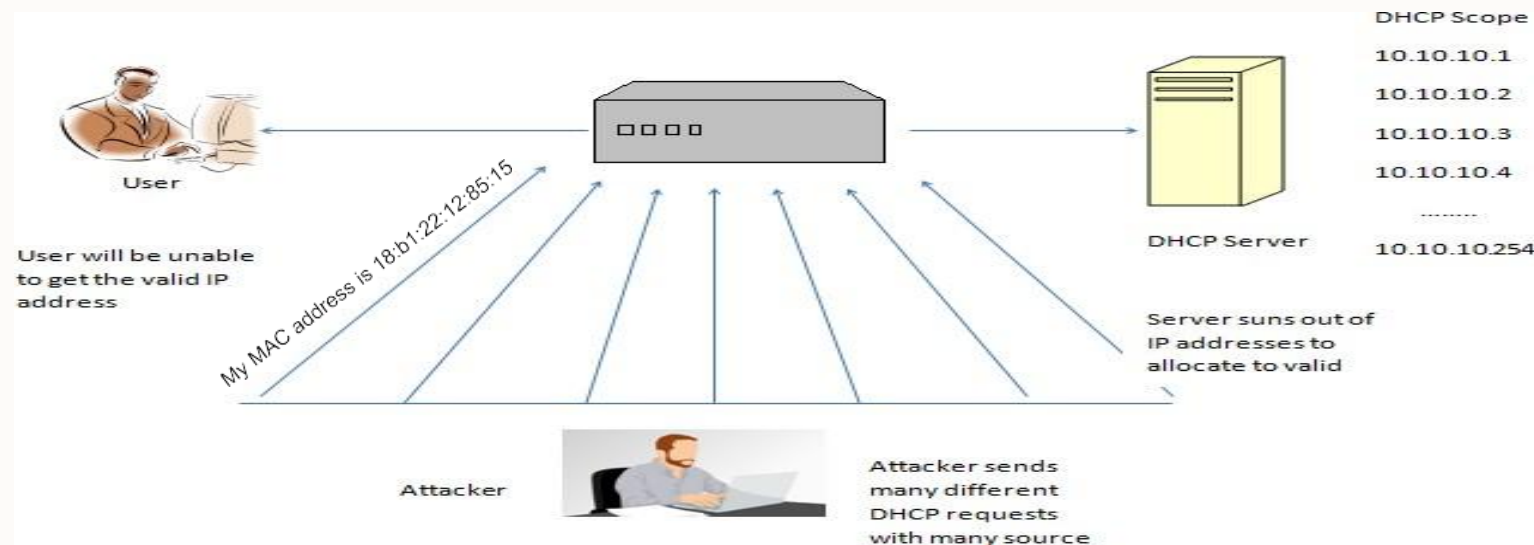
Access Attacks: ARP Poisoning

When a user A initiates a session with user B in the same layer 2 broadcast domain, an ARP request is broadcasted using the user B's IP addresses and the user A waits for the user B to respond with a MAC address



Access Attacks : DHCP Starvation

- Dynamic Host Configuration Protocol (DHCP) is a configuration protocol that assigns valid IP addresses to the host systems out of a preassigned DHCP pool
- DHCP starvation attack is a process of flooding DHCP servers with fake DHCP requests and using all the available IP addresses
- This results in a denial-of-service attack, where the DHCP server cannot issue new IP addresses to the genuine host requests
- New clients cannot get access to the network, resulting in a DHCP starvation attack
- **Yersinia** is the tool to perform the attack





DHCP CONNECTION HANDSHAKE



DHCP CLIENT

DHCP SERVER

Broadcasts Discover
Message

Recieve Discover
Message

Accepts the
Offered IP

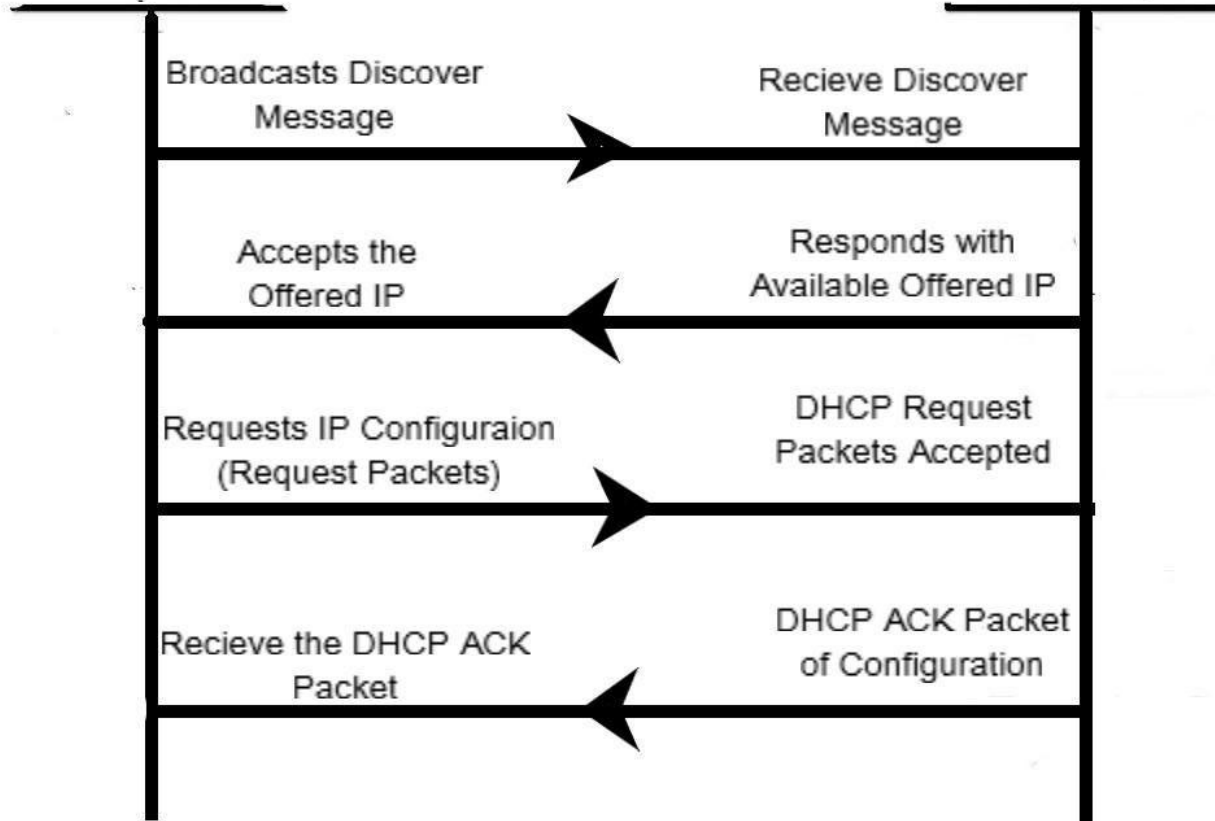
Responds with
Available Offered IP

Requests IP Configuraion
(Request Packets)

DHCP Request
Packets Accepted

Recieve the DHCP ACK
Packet

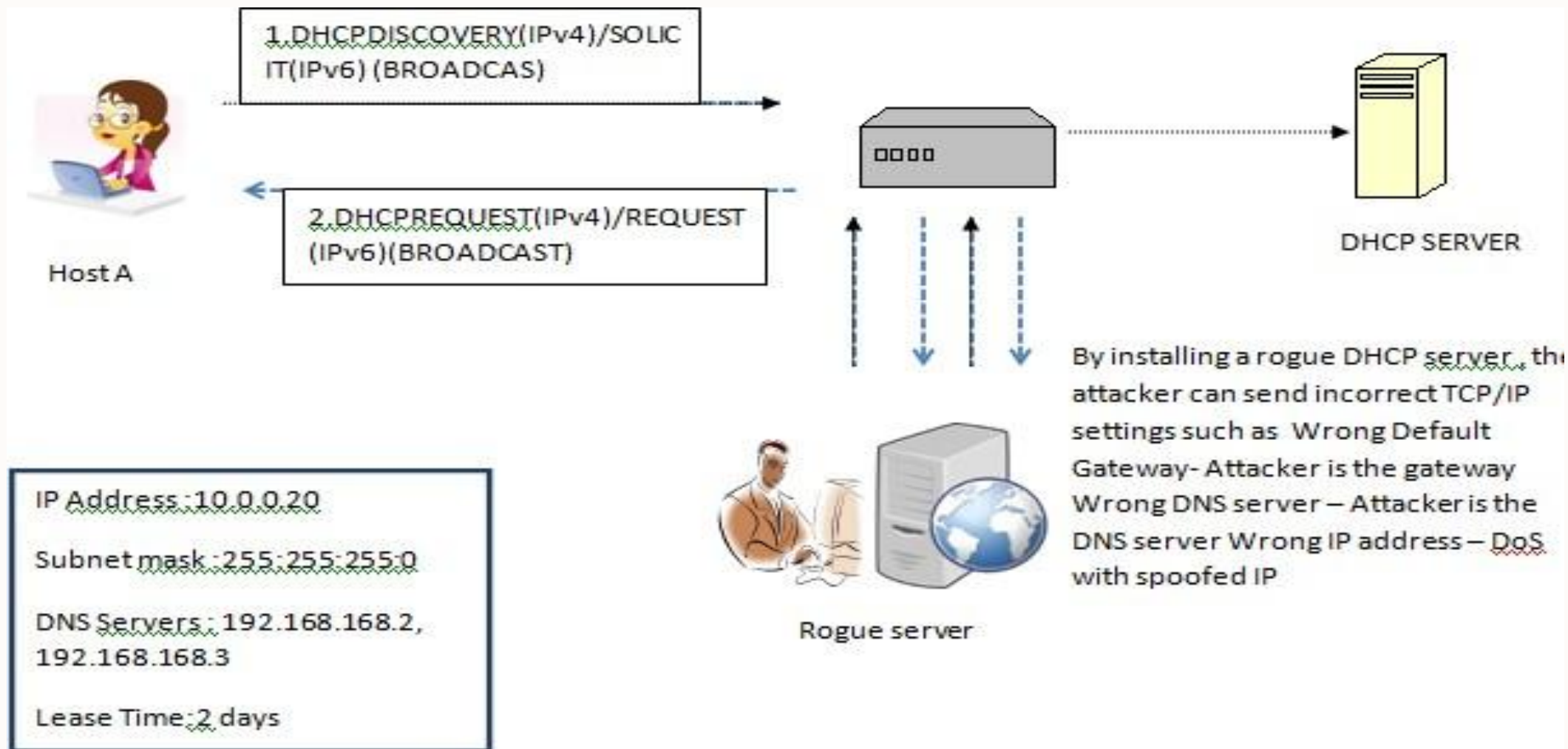
DHCP ACK Packet
of Configuration



Access Attacks : DHCP Spoofing Attack

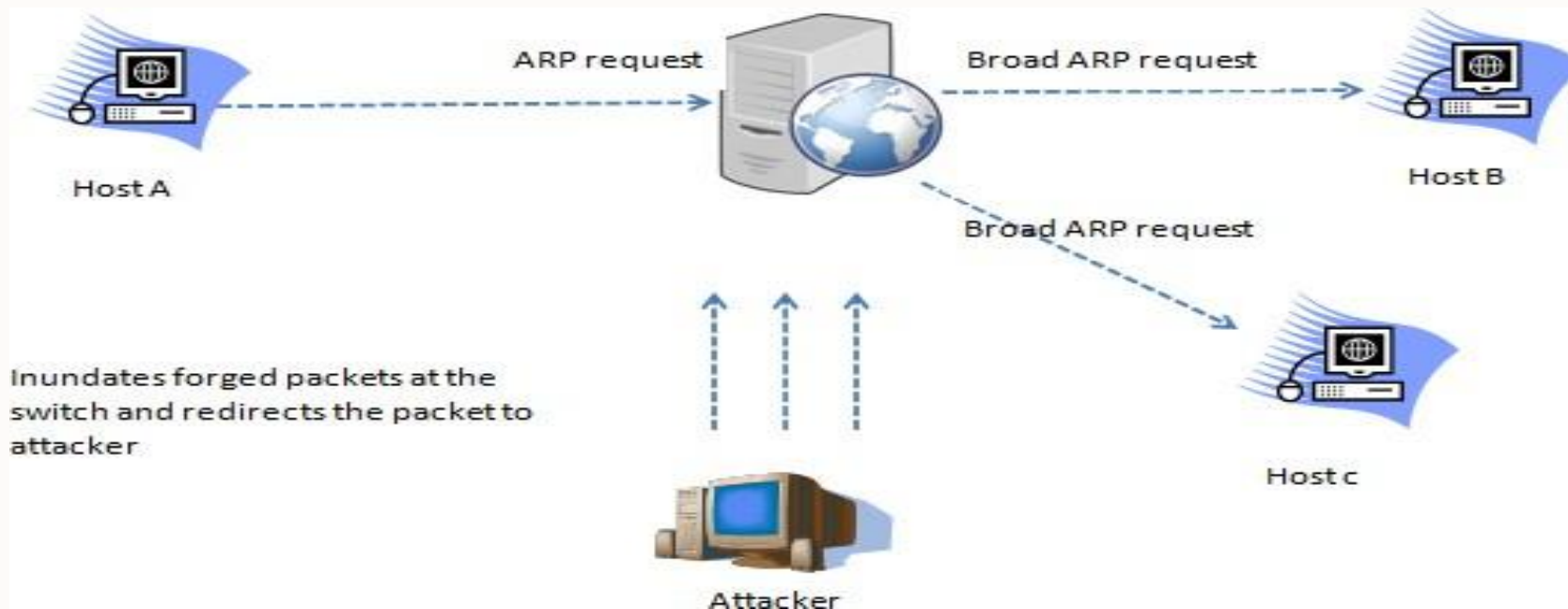
- DHCP servers assign IP addresses to the clients dynamically
- A Hacker places a rogue DHCP server between the client and the real DHCP server
- Whenever a client sends a request, the attackers rogue server intercepts the communication and acts as a valid server by replying with fake IP addresses
- By installing a rogue DHCP server, the hacker can send incorrect TCP/IP settings such as
 - Wrong default Gateway - Hacker is the gateway
 - Wrong DNS Server - Hacker is the DNS server
 - Wrong IP address - DoS with spoofed IP

Access Attacks : DHCP Spoofing Attack (CONT'D)



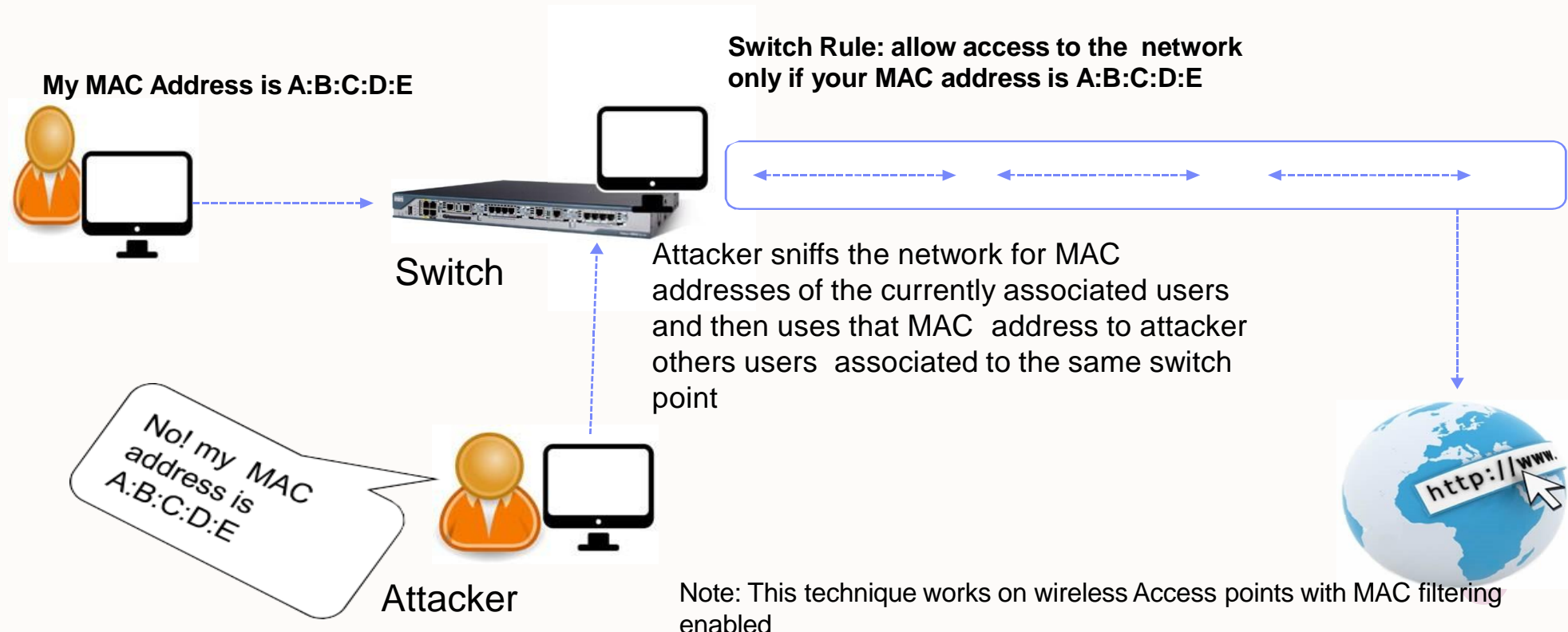
Access Attacks : Switch Port Stealing

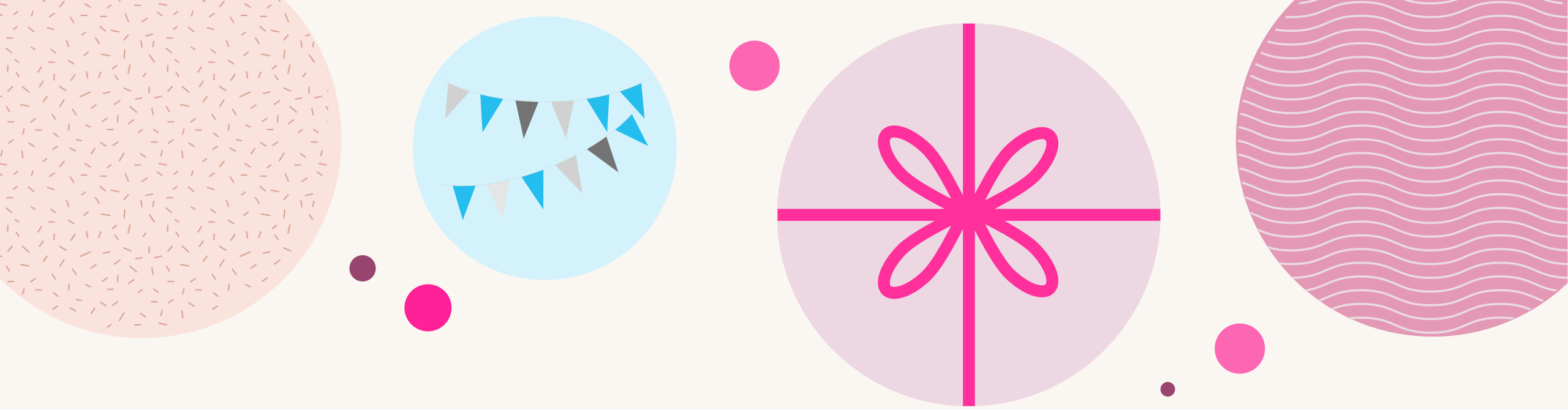
- It is a MiTM technique used to perform packet sniffing by exploiting the switch ports of a user
- Hackers flood the switch port with forged packets that contain victim's host spoofed MAC as source address and hacker's MAC as destination address
- This allows the switch port to send the traffic to the hacker instead of the intended recipients



Access Attacks : MAC Spoofing / Duplicating

- A MAC duplicating attack is launched by sniffing a network for MAC addresses of clients, which are actively associated with a switch port and reusing one of these addresses
- By intercepting the network traffic, the hacker replicates a legitimate user's MAC address to receive all the traffic intended for the specific user
- This attack allows a hacker to gain access to the network by faking another person's identity who is already on the network





Denial of Service (DoS) Attacks

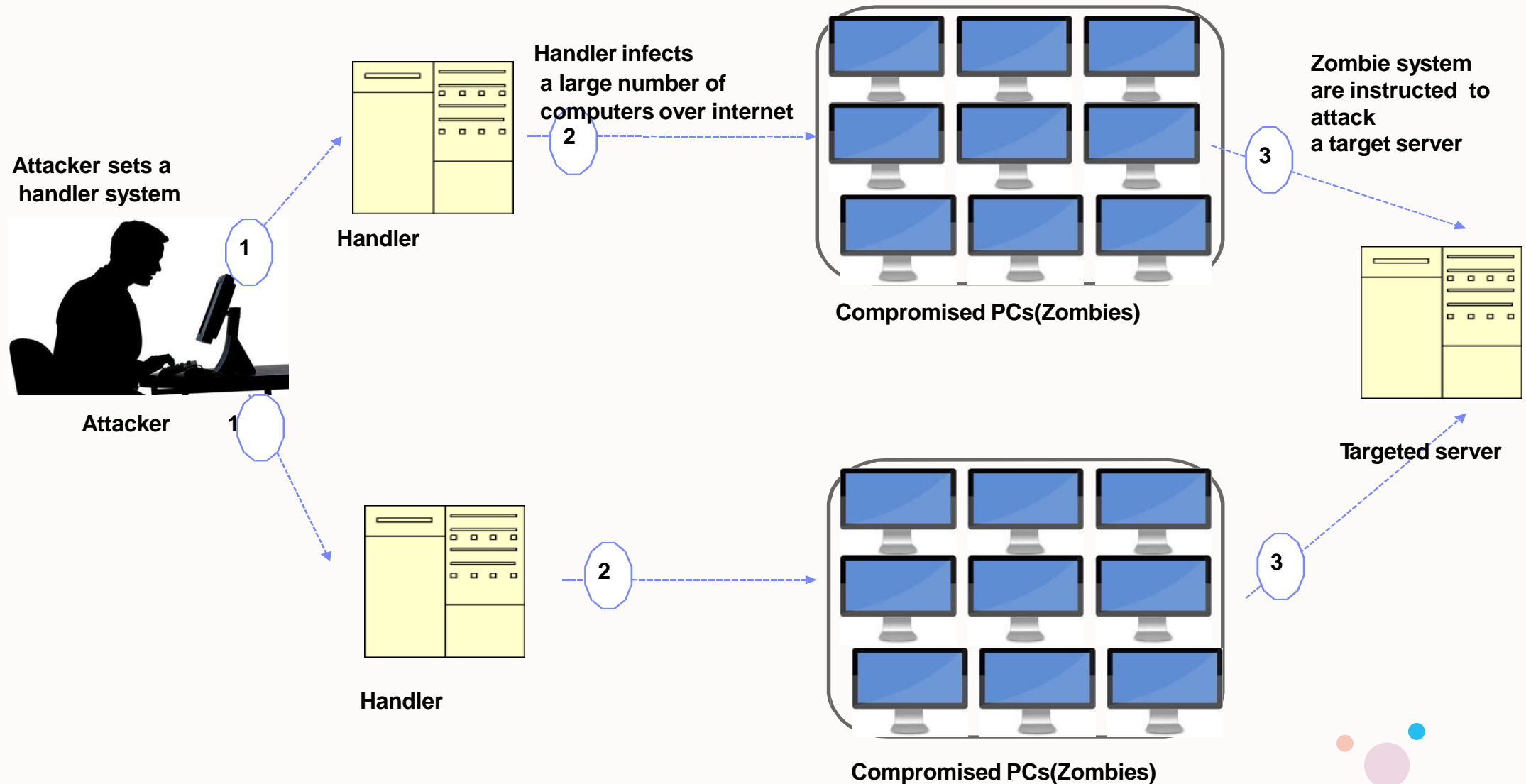
Denial of Service Attack (DOS)

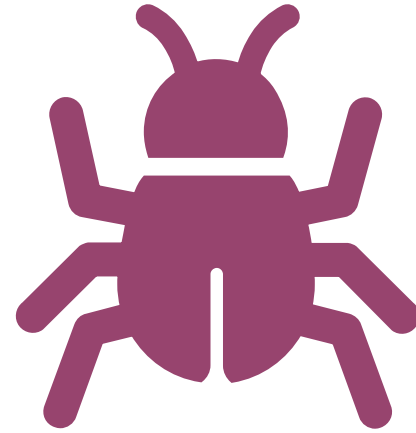
- The DOS attack makes resources unavailable for genuine users by sending a large number of service requests or exploiting vulnerabilities
- Techniques used by a hacker is sending malicious packets and exploiting already existing programming, logical and application vulnerabilities
- Organizations deploy IDS central logging servers exclusively to store IDS alert logs of all systems in a centralised manner
- If a hacker obtains the central log servers IP address, then they could slow it down or even crash it with a DOS attack
- After the server is shut down, attacks could go unnoticed because the alert data is no longer being logged
- Using this technique, hacker can :
 - Consume the device's processing power which allows attacks to go unnoticed
 - Cause the admin to take more time to investigate a large number of alarms
 - Fill up disk space providing no space or disrupt logged processes
 - Cause more alarms that are beyond handling capacity of the management systems, such as databases, ticketing systems etc.,
 - Cause the device to lock up

Distributed Denial of Service Attack: (DDoS)

- DDoS attack involves a multitude of compromised systems attacking a single target, thereby causing a denial of service for legitimate users
- DDoS attacks disable the whole network and hinder business operations causing financial loss and a bad reputation
- A Hacker uses botnets for exploiting vulnerabilities which exist in the target system and convert it to a bot master. Doing this will infect it with malware or even take control of other systems on the network
- Two Types of DDoS
 - Network Centric attack
 - Overloads a Service by consuming bandwidth
 - Application Centric attack
 - Overloads a service by sending flooded packets

Distributed Denial of Service Attack: (DDoS)





Malware Attacks

Malware Attacks

- Malware are software programs or malicious codes that install on a system without the user's knowledge
- It disrupts services, damages systems, gathers sensitive information etc.,
- Examples of malware include Virus, Trojan, Spyware, Rootkit, Backdoor etc.,

Virus

- A virus is a self-replicating program that attaches itself to another program, computer boot sector or a document

Trojan

- A program that appears to be good or useful software but contains hidden and harmful code

Adware

- Adware is a software program that tracks the User's browsing pattern for marketing purposes and to display advertisements

Malware Attacks

Spyware

- **Spyware is a piece of software code that extracts the user information and sends it to attackers**

Rootkit

- **Rootkit is a malicious software program that conceals certain activities from detection by the operating systems**

Backdoor

- **– Backdoors are programs that allow hackers to bypass the authentication checks, such as gaining administrative privileges without passwords**