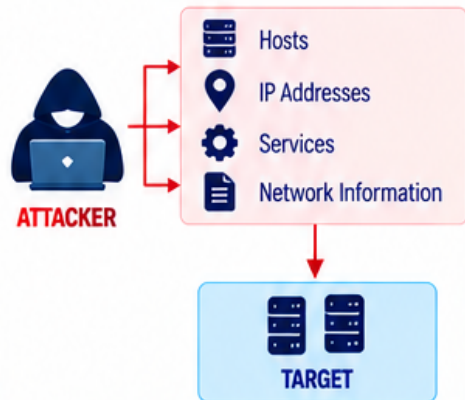


RECONNAISSANCE

Attackers collect information about a target before attempting further attacks.

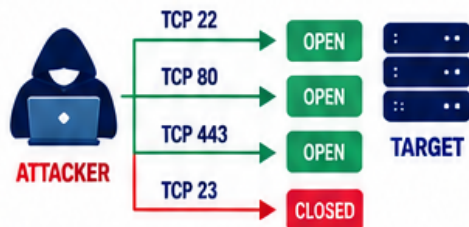


Type	Description
Passive Reconnaissance	Collect information without direct interaction (e.g. open sources)
Active Reconnaissance	Directly interact with target (e.g. scan, probe, query services)

Reconnaissance helps the attacker identify potential vulnerabilities and plan further attacks.

PORT SCANNING

Port scanning identifies reachable ports and services on a target.

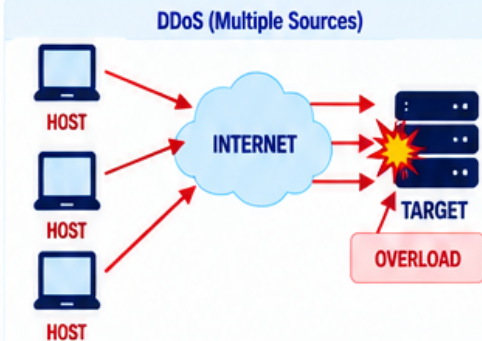


Scan Type	Description	Example Tool
TCP Connect Scan	Completes full TCP connection	nmap
SYN Scan	Half-open scan (faster, stealthier)	nmap
UDP Scan	Checks UDP ports	nmap
Service / Version Detection	Identifies running services and versions	nmap
OS Detection	Tries to identify the target operating system	nmap

Open ports can reveal exposed network services, which may be targeted in further attacks.

DoS / DDoS

A Denial-of-Service attack attempts to make a service unavailable by exhausting resources or disrupting normal operation.



Type	Description	Goal
DoS	One attack source	Disrupt availability
DDoS	Multiple distributed sources (e.g. botnet)	Overwhelm target resources

DoS/DDoS attacks can target network devices, servers or specific applications.

SPOOFING

Spoofing involves falsifying identity or addressing information.

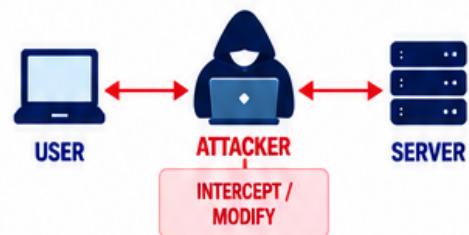


Type	Description
IP Spoofing	Fake source IP address
MAC Spoofing	Fake MAC address
Email Spoofing	Fake sender email address
DNS Spoofing	Fake DNS information
ARP Spoofing	Fake ARP information

Spoofing can be used to bypass filters, impersonate trusted systems or hide the real source of an attack.

MAN-IN-THE-MIDDLE ATTACK

A MITM attacker positions itself between communicating parties.



Technique	Description
Passive MITM	Observe communication (eavesdropping)
Active MITM	Modify traffic in transit
Common Targets	Unencrypted protocols, insecure networks, weak authentication

The attacker may steal information, inject malicious data or redirect traffic when protections are insufficient (e.g. no encryption, invalid certificates).

ARP SPOOFING

ARP spoofing sends forged ARP information to manipulate IP-to-MAC mappings on a local network.



Effect	Description
Traffic Redirection	Redirects traffic through attacker
Session Hijacking	Intercepts unencrypted traffic
MITM Attacks	Enables further attacks

ARP spoofing can allow the attacker to intercept, modify or drop traffic on the local network.

DNS SPOOFING

DNS spoofing can redirect a user toward an incorrect destination by providing false DNS information.



Type	Description
DNS Cache Poisoning	Injects false DNS records
DNS Spoofing	Provides incorrect DNS responses
DNS Redirection	Sends users to malicious websites
Pharming	Redirects users without changing DNS settings

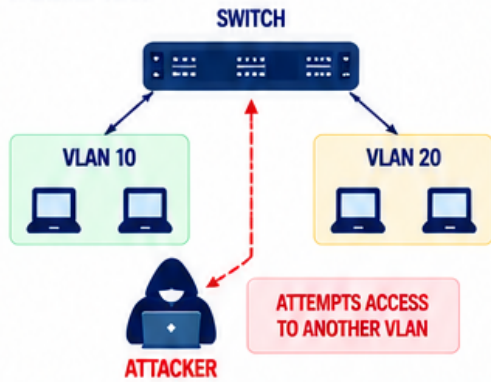
Users may believe they are connecting to the legitimate destination, which can lead to credential theft or malware infection.



Always verify and test security configurations in a lab environment before applying them to a production network.

VLAN HOPPING

VLAN hopping attempts to gain access to traffic in another VLAN.

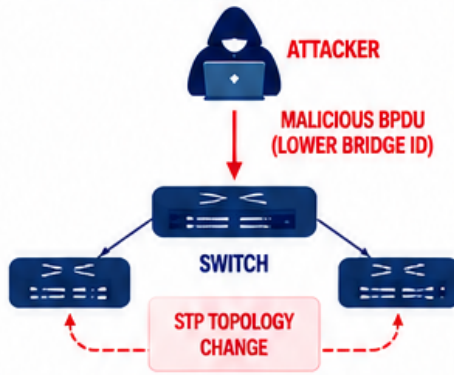


Attack Method	Description
Switch Spoofing	Attacker sends fake DTP messages to become a trunk.
Double Tagging	Attacker uses 802.1Q double tagging to access another VLAN.
Misconfiguration	Exploits improperly configured trunk ports or native VLANs.

Successful VLAN hopping can allow the attacker to access and capture traffic from other VLANs.

STP ATTACK

An attacker may send manipulated BPDUs to influence the Spanning Tree topology.

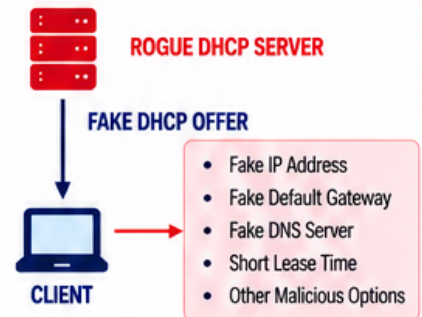


Attack Type	Description
Root Bridge Attack	Become the root bridge by sending superior BPDUs.
Topology Manipulation	Influence traffic paths and intercept traffic.
Disruption	Cause instability or loop conditions in the network.

STP attacks can allow the attacker to intercept, modify or drop traffic by controlling the Layer 2 topology.

ROGUE DHCP SERVER

An unauthorized DHCP server can provide clients with malicious network parameters.



Parameter	Malicious Effect
Default Gateway	Redirect traffic through attacker (Man-in-the-Middle)
DNS Server	Redirect users to malicious websites (DNS spoofing)
IP Configuration	Place client in attacker-controlled network

A rogue DHCP server can redirect client traffic, enabling further attacks such as MITM or DNS spoofing.

ROGUE ACCESS POINT

A rogue or malicious AP can imitate or expose a wireless network.

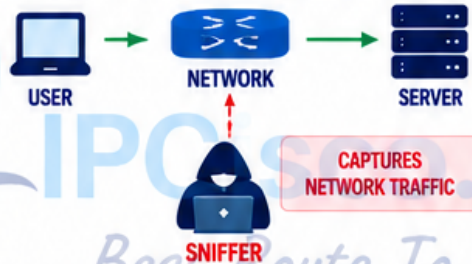


Attack Type	Description
Evil Twin	Fake AP with the same or similar SSID as a legitimate network.
Rogue AP	Unauthorized AP connected to the network (malicious or accidental).
Traffic Interception	Captures user traffic and credentials.

Users may unknowingly connect to the rogue AP, exposing their traffic and credentials to the attacker.

TRAFFIC SNIFFING

Sniffing captures network traffic visible to an attacker.

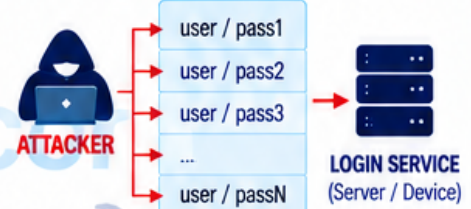


Capture Method	Description
Shared Network	Capture traffic on a shared segment (e.g. hub, SPAN, promiscuous mode).
ARP Spoofing	Redirect traffic to attacker for sniffing.
MITM	Position between devices to capture traffic.

Unencrypted traffic may expose sensitive information such as credentials, session tokens or internal data.

BRUTE-FORCE ATTACK

A brute-force attack repeatedly attempts credentials to gain access.

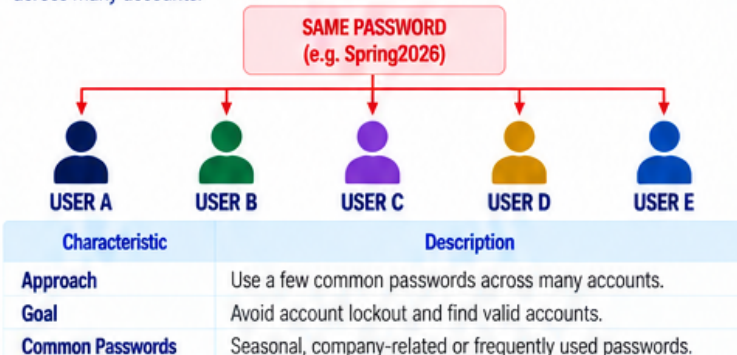


Target	Common Examples
Network Devices	SSH, Telnet, HTTP, HTTPS
Applications	Web Login, VPN, Email
Protocols	FTP, RDP, SMB, Database

The attacker tries many credential combinations until a valid one is found.

PASSWORD SPRAYING

Password spraying tries a small number of common passwords across many accounts.



Characteristic	Description
Approach	Use a few common passwords across many accounts.
Goal	Avoid account lockout and find valid accounts.
Common Passwords	Seasonal, company-related or frequently used passwords.

Unlike brute force, password spraying distributes attempts across multiple accounts, reducing the chance of lockout.

QUICK ATTACK MAP

Attack	Main Target	Goal / Impact
VLAN Hopping	VLAN Segmentation	Access traffic in another VLAN
STP Attack	Layer 2 Topology	Control topology / intercept traffic
Rogue DHCP	IP Configuration	Provide malicious network parameters
Rogue AP	Wireless Users	Attract users and intercept traffic
Sniffing	Network Traffic	Capture sensitive information
Brute Force	Credentials	Find valid username / password
Password Spraying	Multiple Accounts	Gain access using common passwords

These attacks can be used individually or together as part of a larger attack chain. Proper configuration, monitoring and security controls can help prevent and detect them.

Always verify and test security configurations in a lab environment before applying them to a production network.