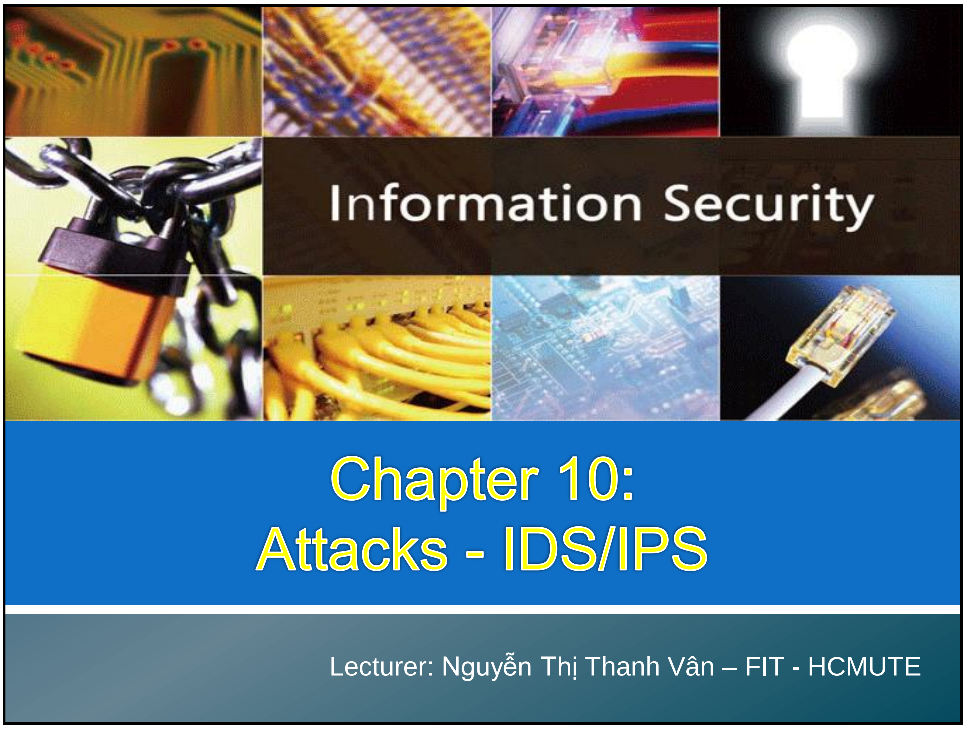
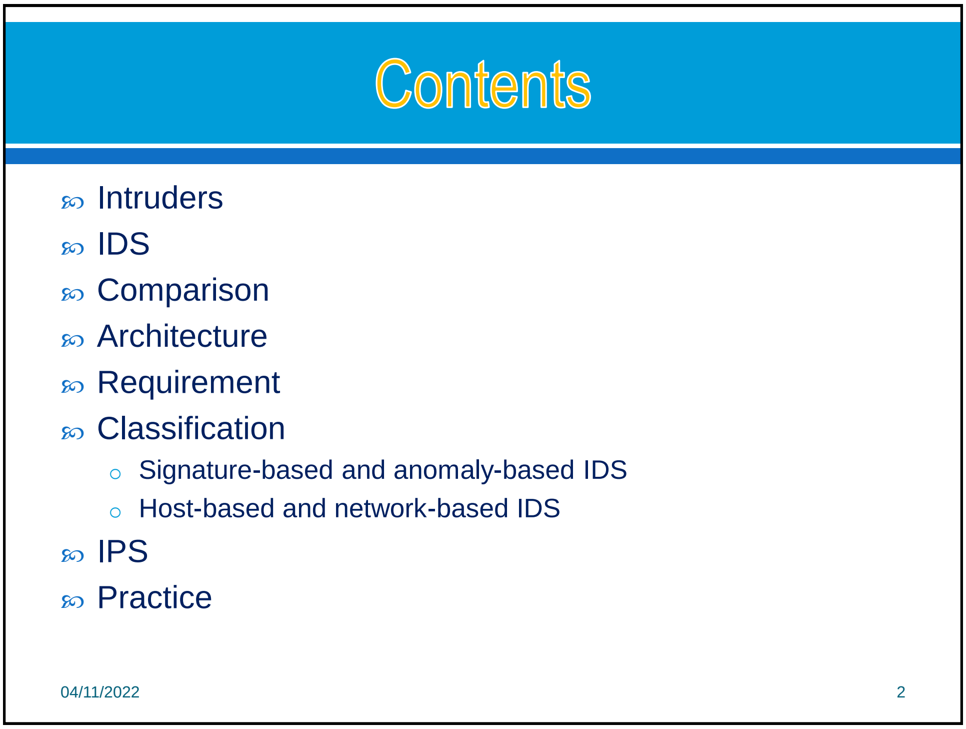


Information Security

Chapter 10: Attacks - IDS/IPS

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE



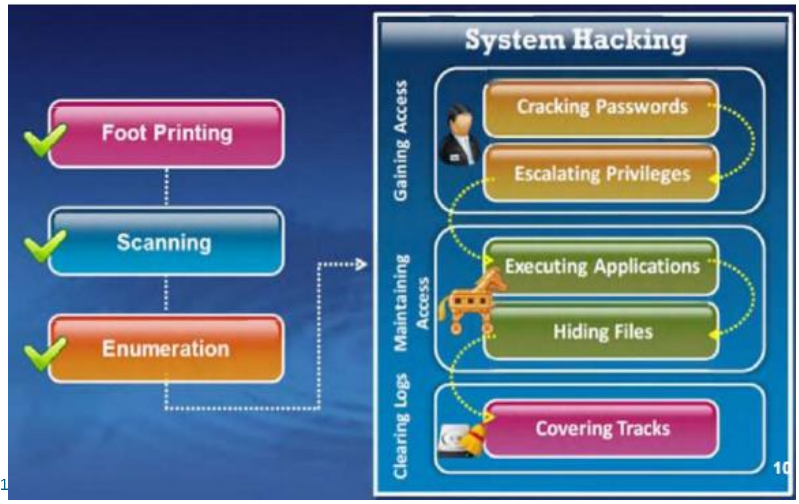
Contents

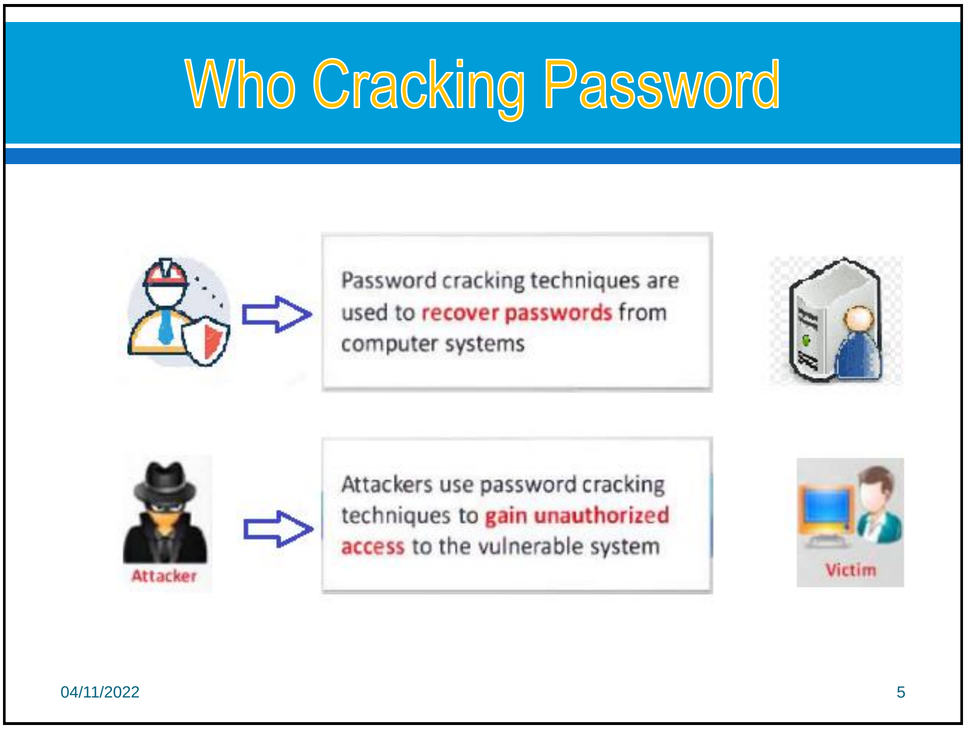
- Intruders
- IDS
- Comparison
- Architecture
- Requirement
- Classification
  - Signature-based and anomaly-based IDS
  - Host-based and network-based IDS
- IPS
- Practice

Attacks

- Crack password
  - Dictionary attack
  - Brute Force Attack
  - Hybrid Attack
  - Syllable Attack
  - Rule-Based Attack
- Denied Of Services:
  - Spoofing: SYN, source address
  - Flooding: SYN TCP, UDP, ICMP
  - Distributed DOS attacks
  - Reflection . Amplification: DNS. SMURF
  - Over bufferFlow
- TCP Attack
- Packet Sniff
- Session Hijacking
- Social attack
- Google Bomb

System Hacking Methodology



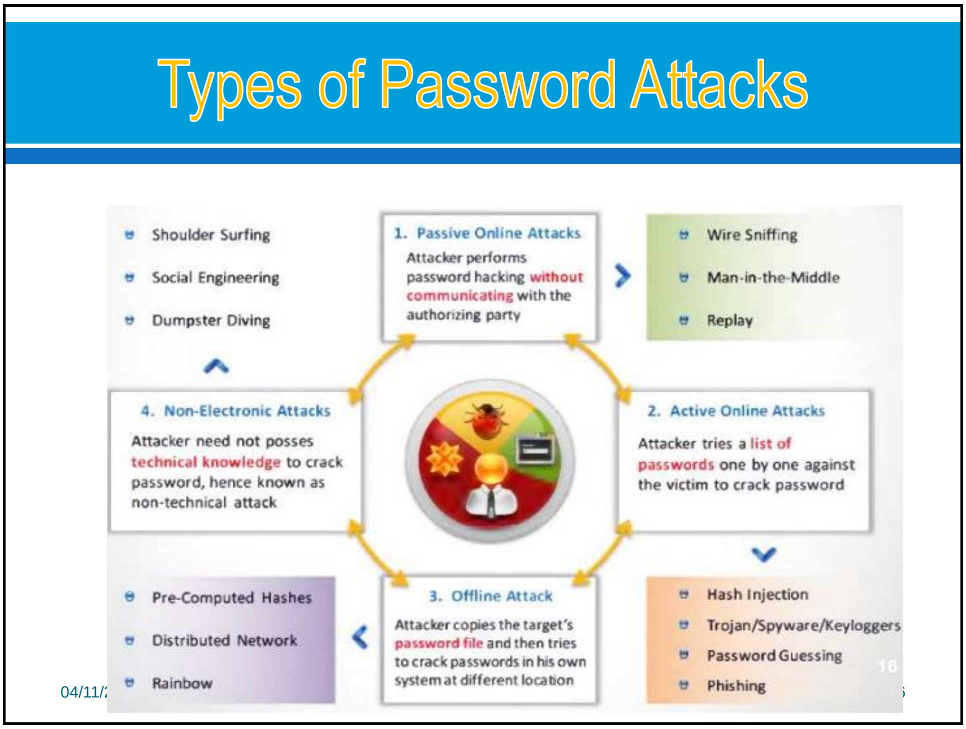


Who Cracking Password

Password cracking techniques are used to recover passwords from computer systems

Attackers use password cracking techniques to gain unauthorized access to the vulnerable system

04/11/2022 5



Types of Password Attacks

1. Passive Online Attacks

Attacker performs password hacking without communicating with the authorizing party

- Wire Sniffing
- Man-in-the-Middle
- Replay

2. Active Online Attacks

Attacker tries a list of passwords one by one against the victim to crack password

- Hash Injection
- Trojan/Spyware/Keyloggers
- Password Guessing
- Phishing

3. Offline Attack

Attacker copies the target's password file and then tries to crack passwords in his own system at different location

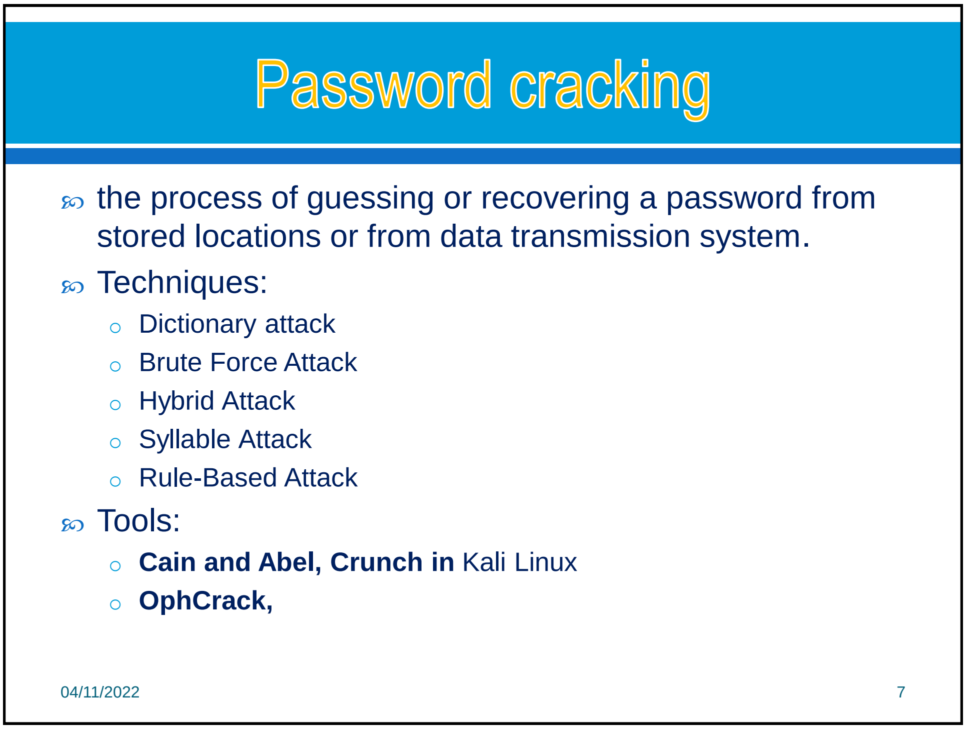
- Pre-Computed Hashes
- Distributed Network
- Rainbow

4. Non-Electronic Attacks

Attacker need not posses technical knowledge to crack password, hence known as non-technical attack

- Shoulder Surfing
- Social Engineering
- Dumpster Diving

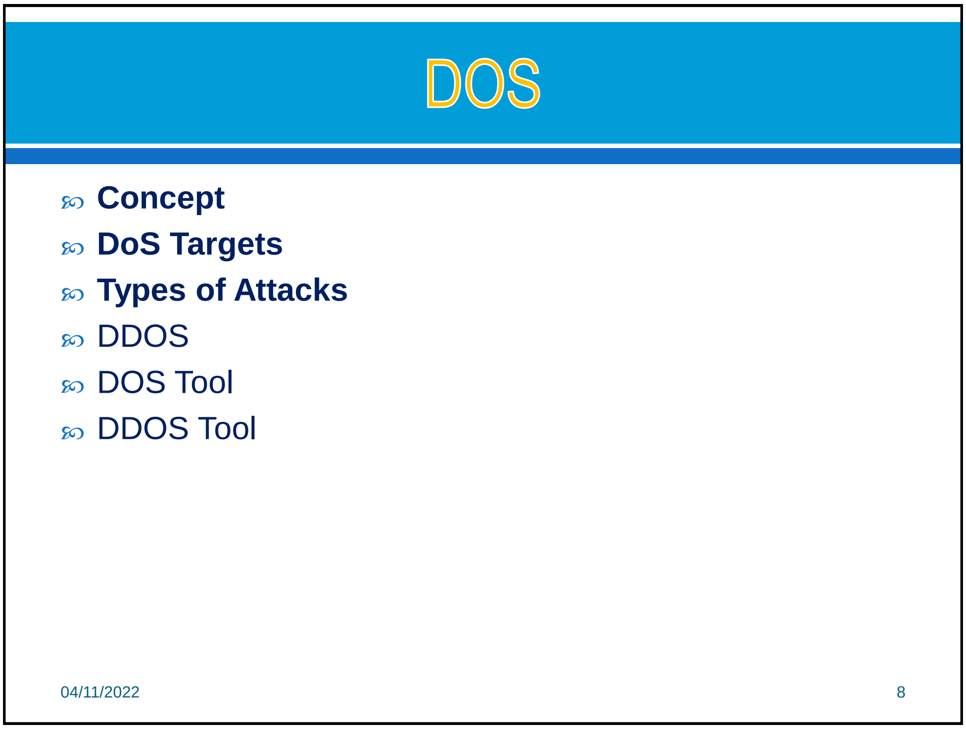
04/11/2



Password cracking

- the process of guessing or recovering a password from stored locations or from data transmission system.
- Techniques:
  - Dictionary attack
  - Brute Force Attack
  - Hybrid Attack
  - Syllable Attack
  - Rule-Based Attack
- Tools:
  - **Cain and Abel, Crunch in** Kali Linux
  - **OphCrack,**

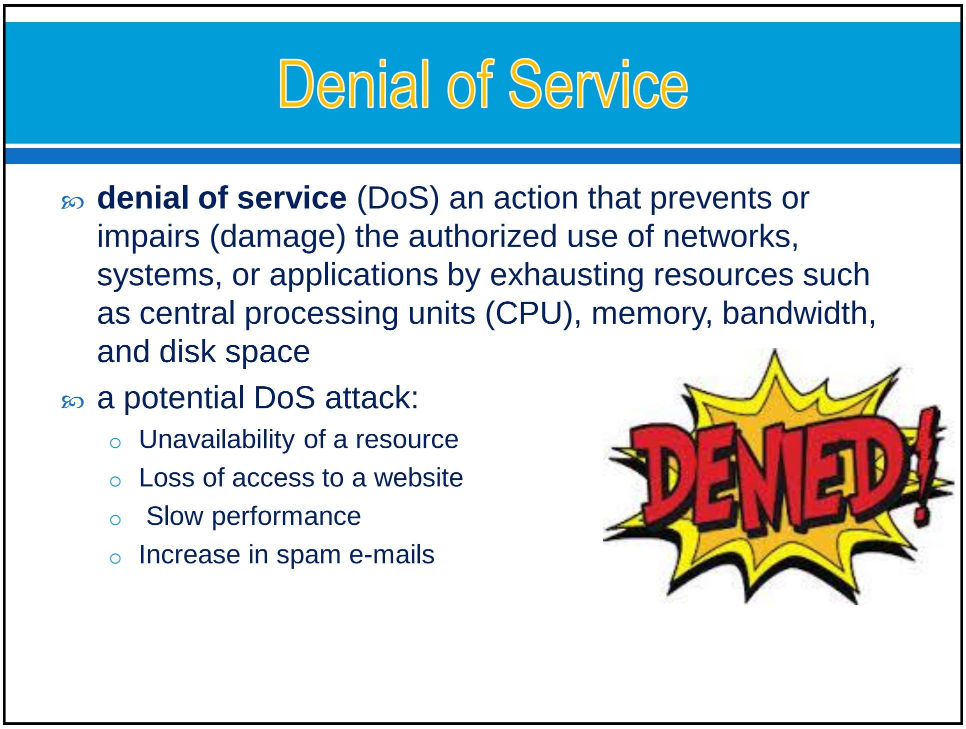
04/11/2022 7



DOS

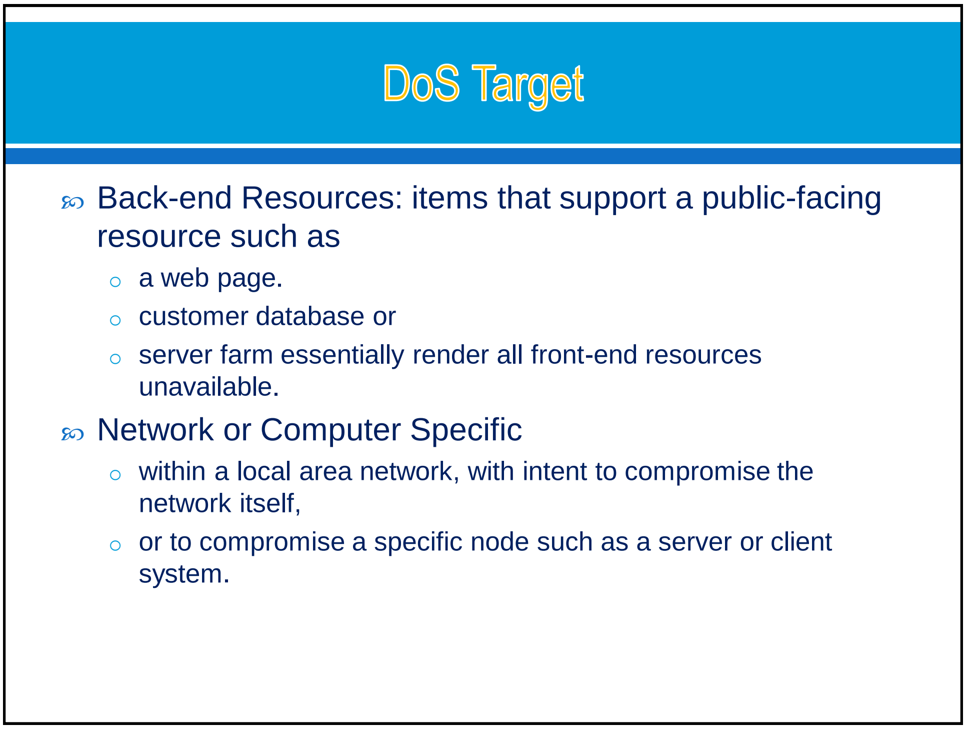
- **Concept**
- **DoS Targets**
- **Types of Attacks**
- DDOS
- DOS Tool
- DDOS Tool

04/11/2022 8



Denial of Service

- **denial of service** (DoS) an action that prevents or impairs (damage) the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space
- a potential DoS attack:
  - Unavailability of a resource
  - Loss of access to a website
  - Slow performance
  - Increase in spam e-mails



DoS Target

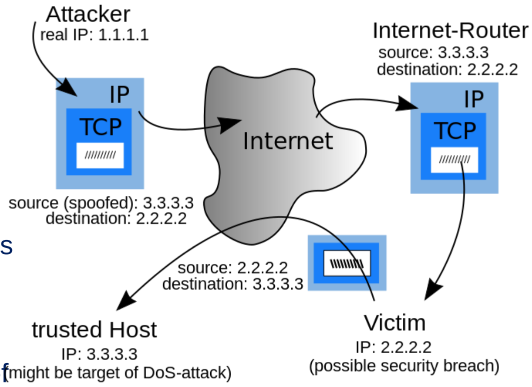
- Back-end Resources: items that support a public-facing resource such as
  - a web page.
  - customer database or
  - server farm essentially render all front-end resources unavailable.
- Network or Computer Specific
  - within a local area network, with intent to compromise the network itself,
  - or to compromise a specific node such as a server or client system.

DOS types

- Many different kinds of DoS attacks
  - Spoofing: SYN, source address
  - Flooding: SYN TCP, UDP, ICMP
  - Distributed DOS attacks
  - Reflection
  - Amplification
  - SMURF
  - Teardrop
  - Ping of Death

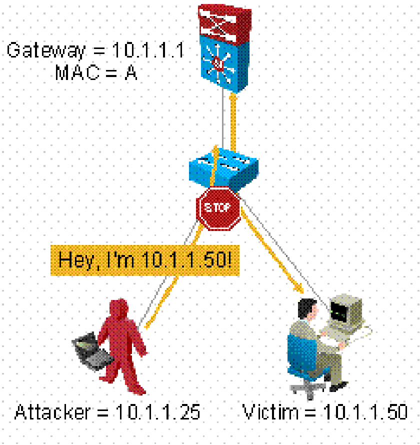
Spoofing: Source Address

- use fake source addresses
- generate large volumes (number) of packets
- directed at target
- with different, random, source addresses
- cause same bottleneck
- responses are scattered across Internet
- real source is much harder to identify
- used in many types of denial of service attacks



Protects Against Spoofed IP Addresses

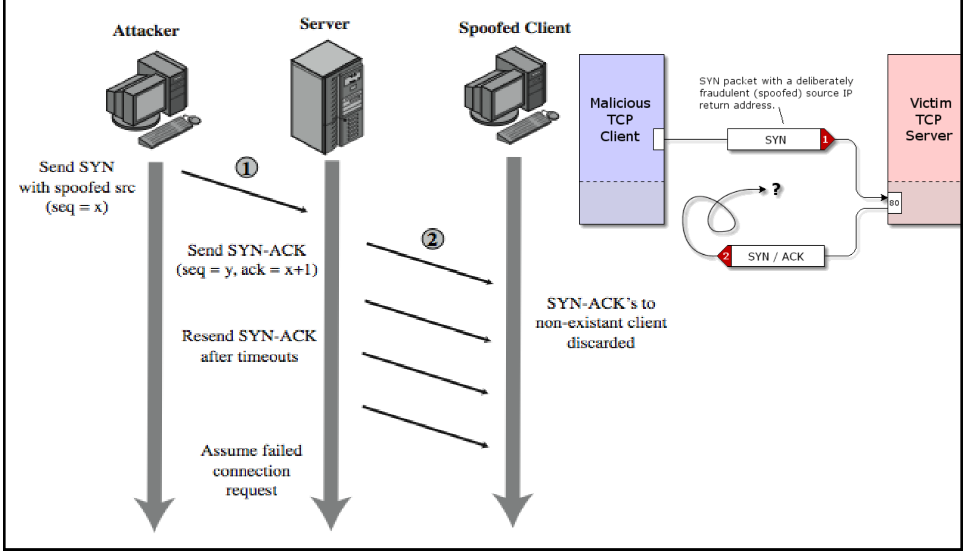
- **IP Source Guard:** Cisco IOS Software feature for Catalyst switches



Spoofing: SYN

- A SYN spoofing attack exploits on the targeted server system.
- The attacker generates a number of SYN connection request packets with forged source addresses.
- Operation at Server
  - records the details of the TCP connection request,
  - sends the SYN-ACK packet to the claimed source address,
  - resend the SYN-ACK packet a number of times before finally assuming the connection request has failed, and deleting the information saved concerning it.

SYN Spoofing Attack



SYN Spoofing Attack

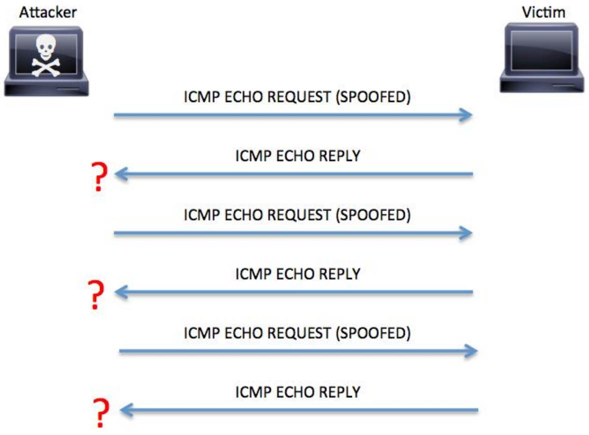
- attacker often uses either
  - random source addresses
  - or that of an overloaded server
  - to block return of (most) reset packets
- has much lower traffic volume
  - attacker can be on a much lower capacity link

Types of Flooding Attacks

- classified based on network protocol used
- ICMP Flood
  - uses ICMP packets, eg echo request
  - typically allowed through, some required
- UDP Flood
  - alternative uses UDP packets to some port
- TCP SYN Flood
  - use TCP SYN (connection request) packets
  - but for volume attack

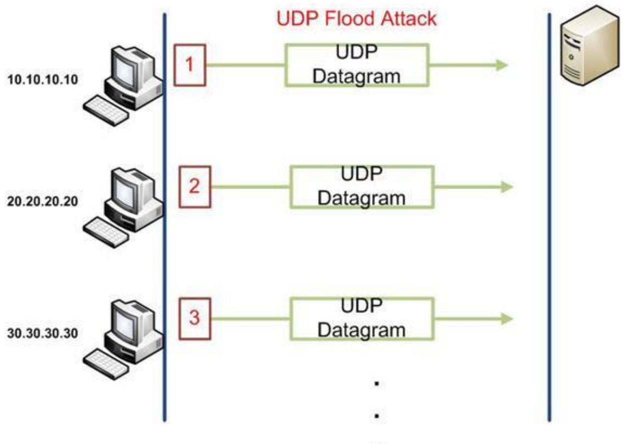
ICMP Flood

- uses an ICMP packet, such as ICMP echo request packets in a ping flood
- Tool: hping


Attacker
Victim
ICMP ECHO REQUEST (SPOOFED)
ICMP ECHO REPLY
?
ICMP ECHO REQUEST (SPOOFED)
ICMP ECHO REPLY
?
ICMP ECHO REQUEST (SPOOFED)
ICMP ECHO REPLY
?

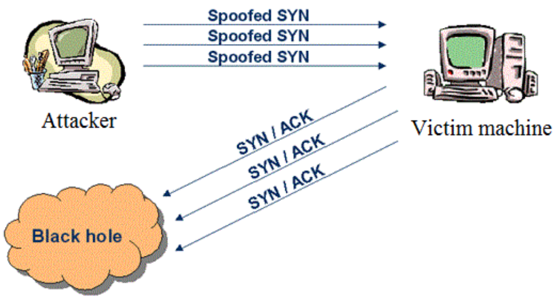
UDP Flood

- the IP packets that the attacker uses against its victim contain UDP datagrams of different sizes



TCP SYN Flood

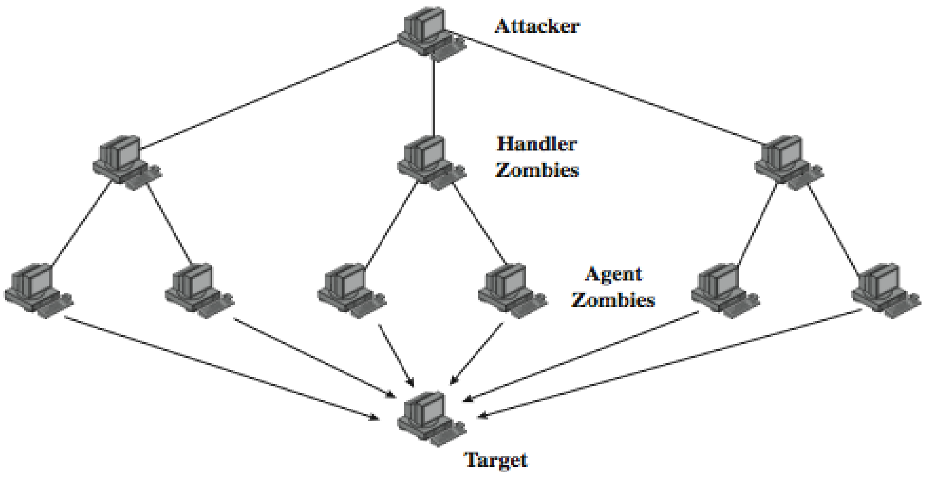
- SYN Packets with random source IP addresses
- flood the server with TCP SYN segments without acknowledging
- No further connections possible

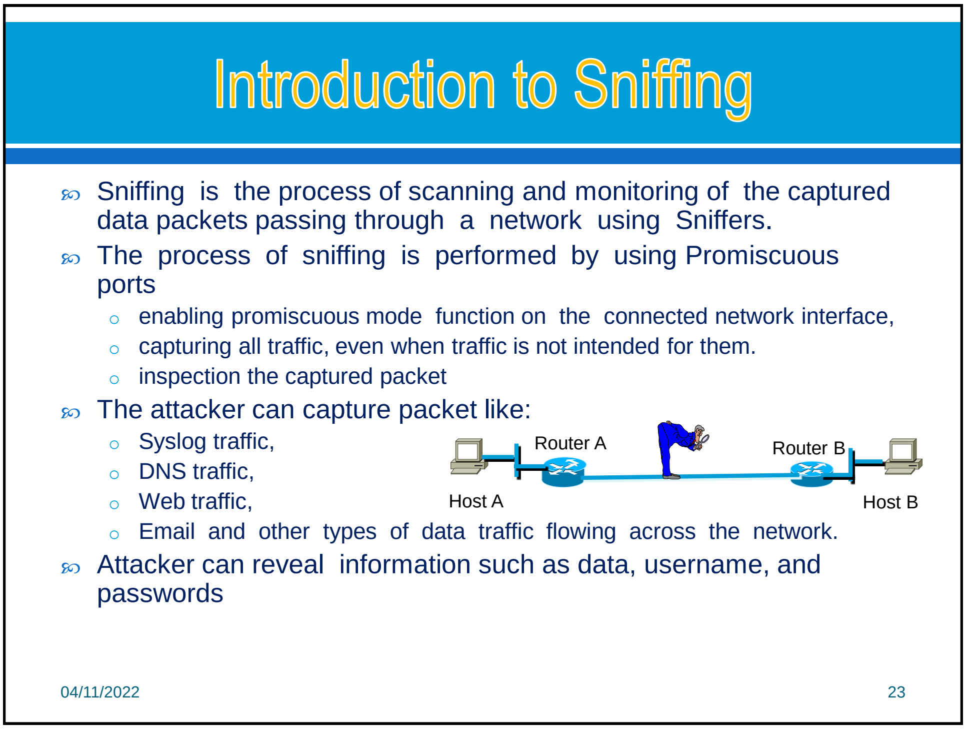


DDOS: Distributed Denial of Service

- Same techniques as regular DoS, but on a much larger scale
- multiple systems allow much higher traffic volumes to form a Distributed Denial of Service (DDoS) Attack
- often compromised PC's / workstations
  - zombies with backdoor programs installed
  - forming a botnet
- e.g.
  - Tribe Flood Network (TFN), TFN2K
  - Sub7Server Trojan and IRC bots
    - Infect a large number of machines with a "zombie" program
    - Zombie program logs into an IRC channel and awaits commands

DDoS Control Hierarchy

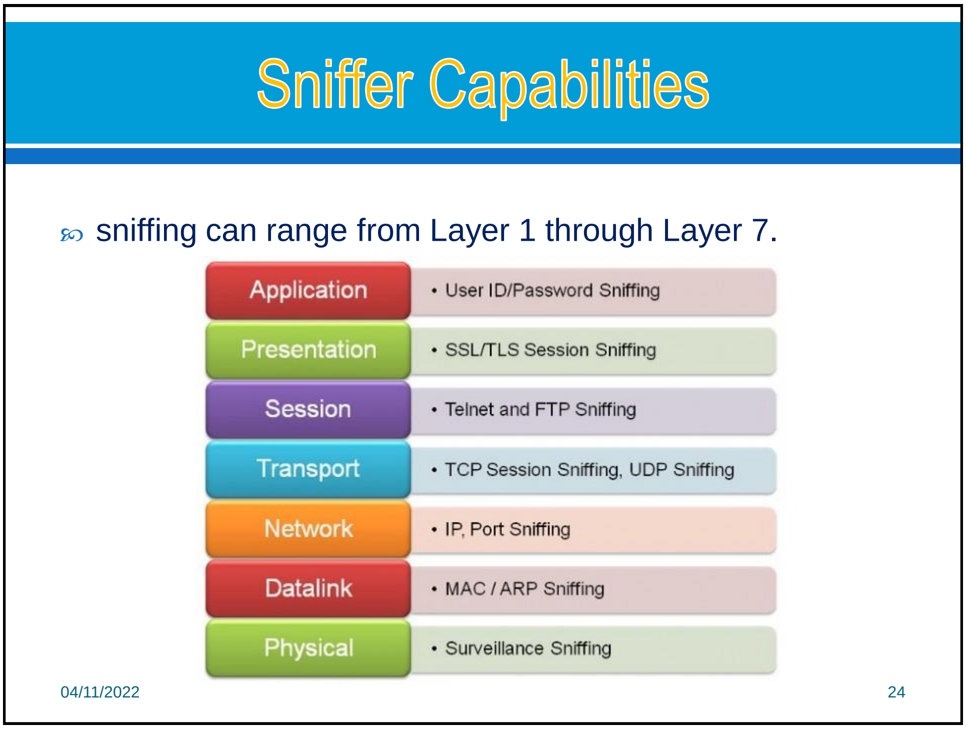




Introduction to Sniffing

- Sniffing is the process of scanning and monitoring of the captured data packets passing through a network using Sniffers.
- The process of sniffing is performed by using Promiscuous ports
  - enabling promiscuous mode function on the connected network interface,
  - capturing all traffic, even when traffic is not intended for them.
  - inspection the captured packet
- The attacker can capture packet like:
  - Syslog traffic,
  - DNS traffic,
  - Web traffic,
  - Email and other types of data traffic flowing across the network.
- Attacker can reveal information such as data, username, and passwords

04/11/2022 23

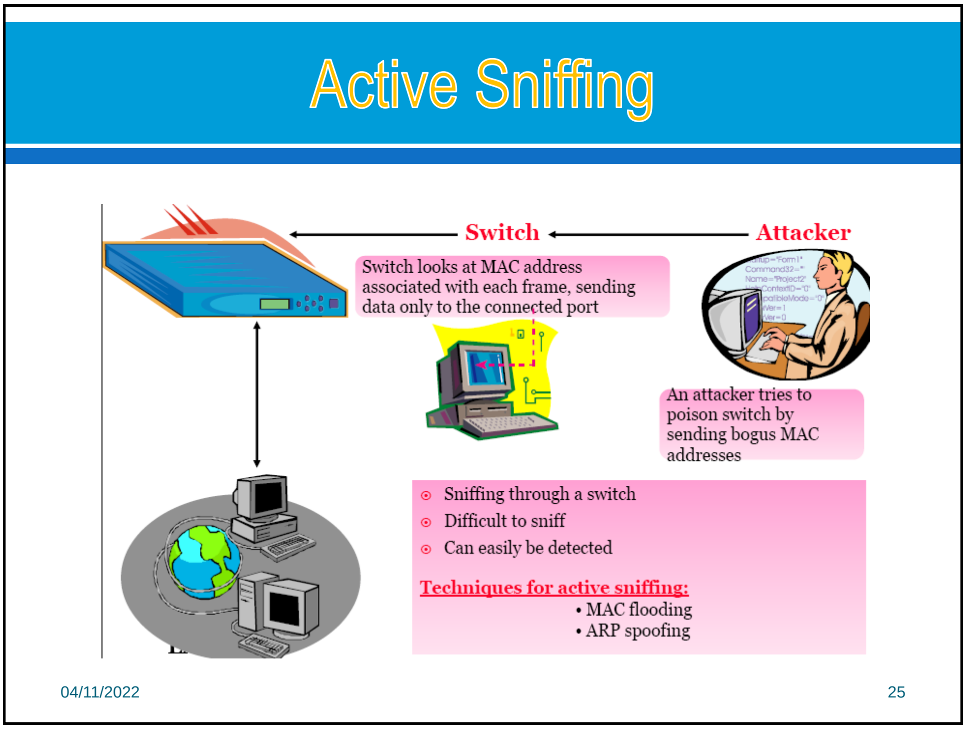


Sniffer Capabilities

- sniffing can range from Layer 1 through Layer 7.

Application	• User ID/Password Sniffing
Presentation	• SSL/TLS Session Sniffing
Session	• Telnet and FTP Sniffing
Transport	• TCP Session Sniffing, UDP Sniffing
Network	• IP, Port Sniffing
Datalink	• MAC / ARP Sniffing
Physical	• Surveillance Sniffing

04/11/2022 24



Active Sniffing

Switch

Attacker

Switch looks at MAC address associated with each frame, sending data only to the connected port

An attacker tries to poison switch by sending bogus MAC addresses

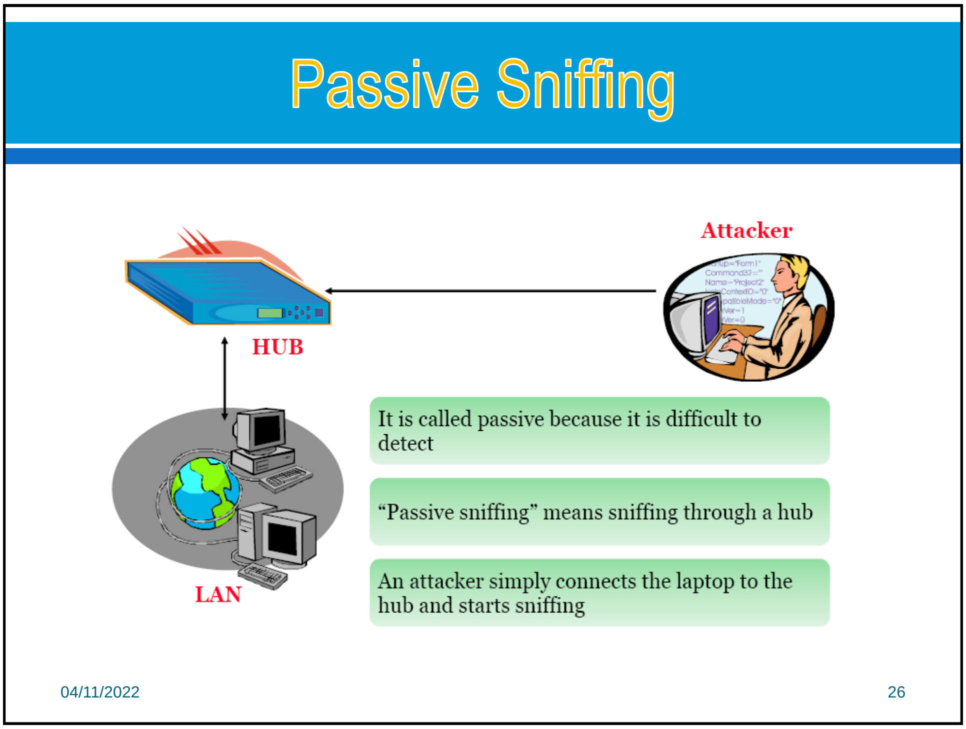
- Sniffing through a switch
- Difficult to sniff
- Can easily be detected

Techniques for active sniffing:

- MAC flooding
- ARP spoofing

04/11/2022

25



Passive Sniffing

Attacker

HUB

LAN

It is called passive because it is difficult to detect

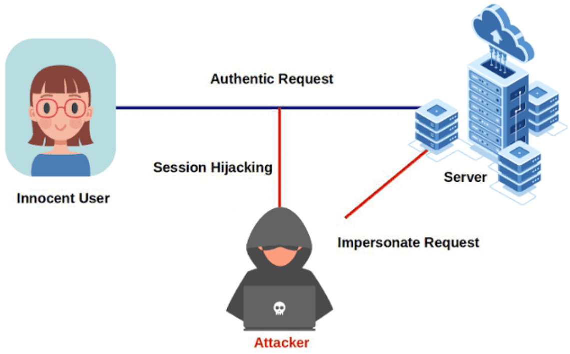
“Passive sniffing” means sniffing through a hub

An attacker simply connects the laptop to the hub and starts sniffing

04/11/2022

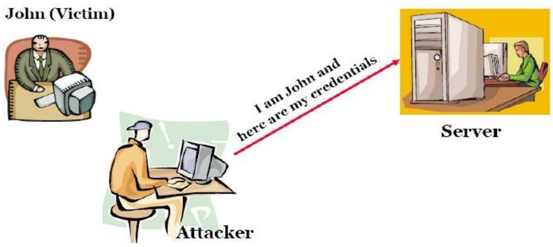
26

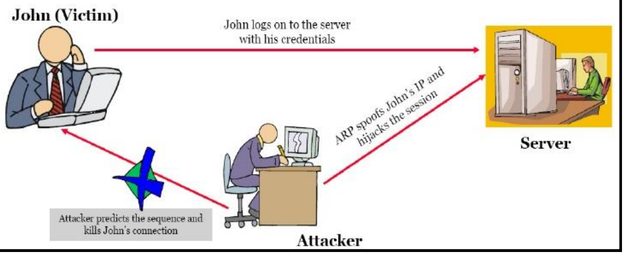
Session Hijacking

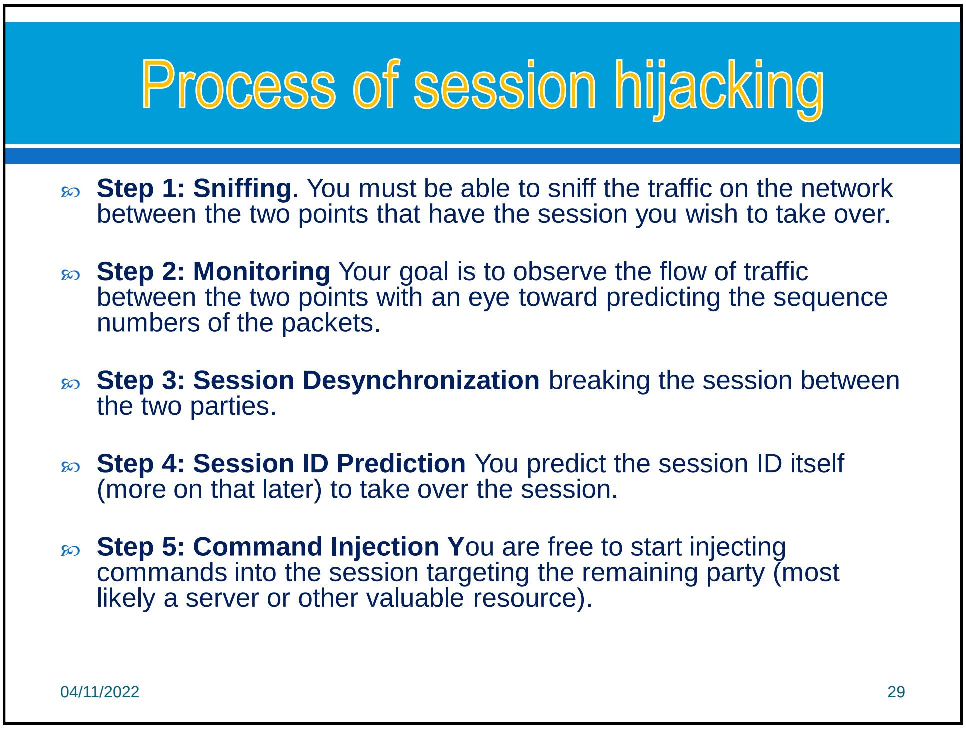


Spoofing vs Hijkacking

- Spoofing:
  - attacker does not actively take another user offline to perform the attack
  - Pretends to another user
- Hijacking:
  - attacker takes over a existing session
  - relying on the legitimate user to make a connection and authentication

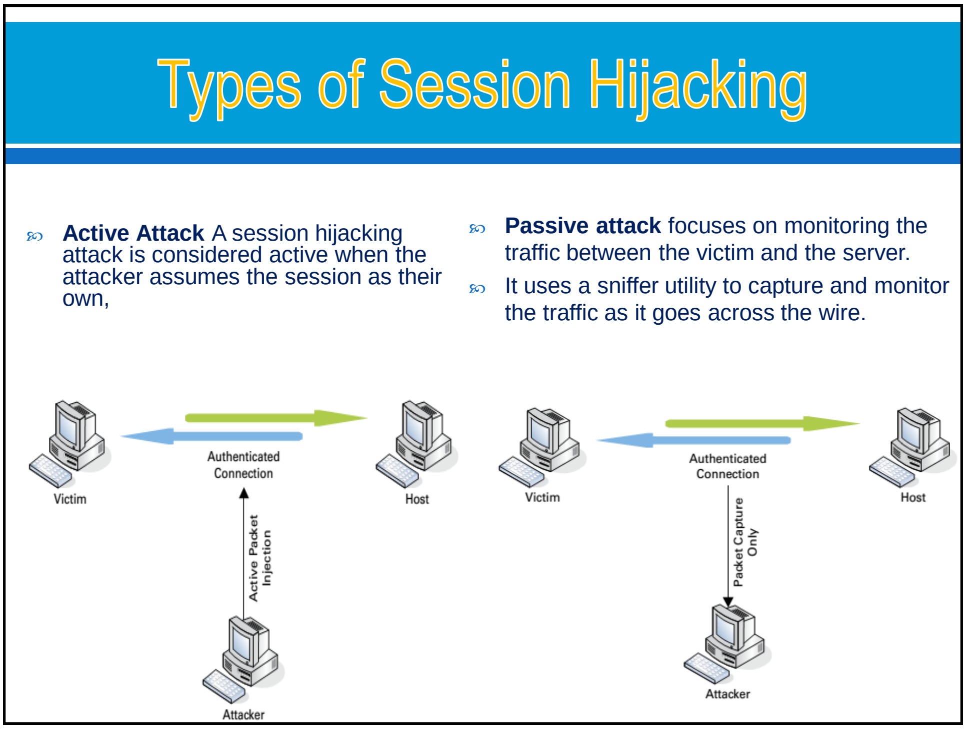



John (Victim)
John logs on to the server with his credentials
ARP spoofs John's IP and hijacks the session
Server
Attacker predicts the sequence and kills John's connection
Attacker



Process of session hijacking

- **Step 1: Sniffing**. You must be able to sniff the traffic on the network between the two points that have the session you wish to take over.
- **Step 2: Monitoring** Your goal is to observe the flow of traffic between the two points with an eye toward predicting the sequence numbers of the packets.
- **Step 3: Session Desynchronization** breaking the session between the two parties.
- **Step 4: Session ID Prediction** You predict the session ID itself (more on that later) to take over the session.
- **Step 5: Command Injection Y**ou are free to start injecting commands into the session targeting the remaining party (most likely a server or other valuable resource).



Types of Session Hijacking

- **Active Attack** A session hijacking attack is considered active when the attacker assumes the session as their own,

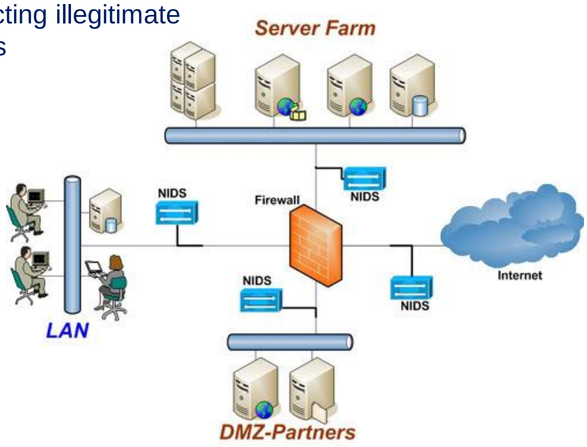
- **Passive attack** focuses on monitoring the traffic between the victim and the server.
- It uses a sniffer utility to capture and monitor the traffic as it goes across the wire.

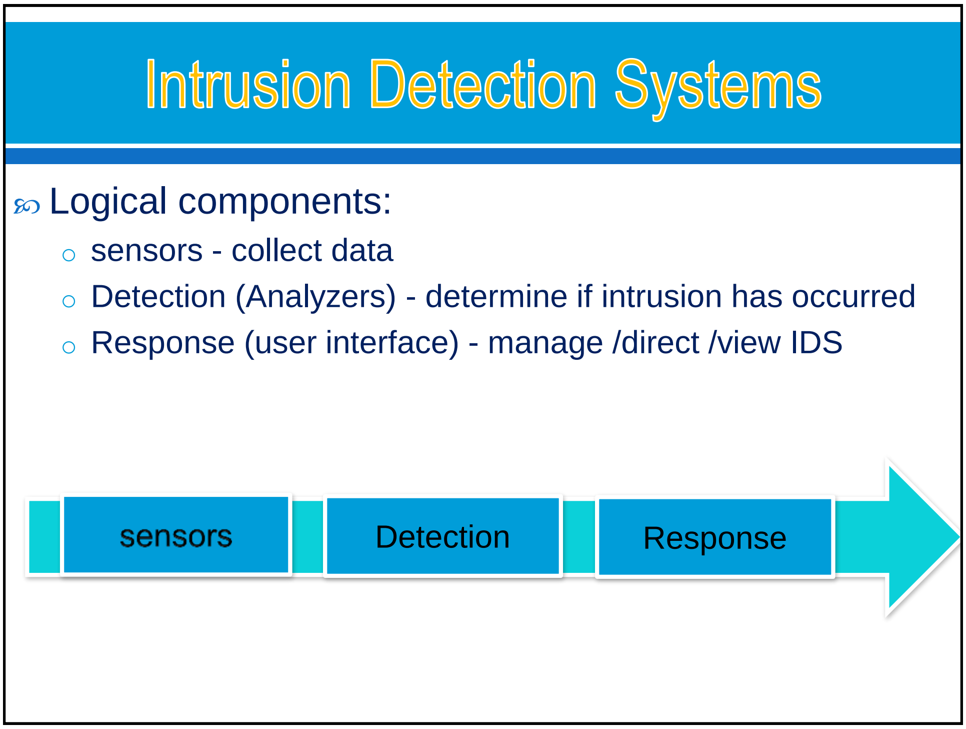
IDS/IPS

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Intrusion Detection Systems

- IDS:
  - is a system of devices or applications
  - has capability of detecting illegitimate intrusions on networks





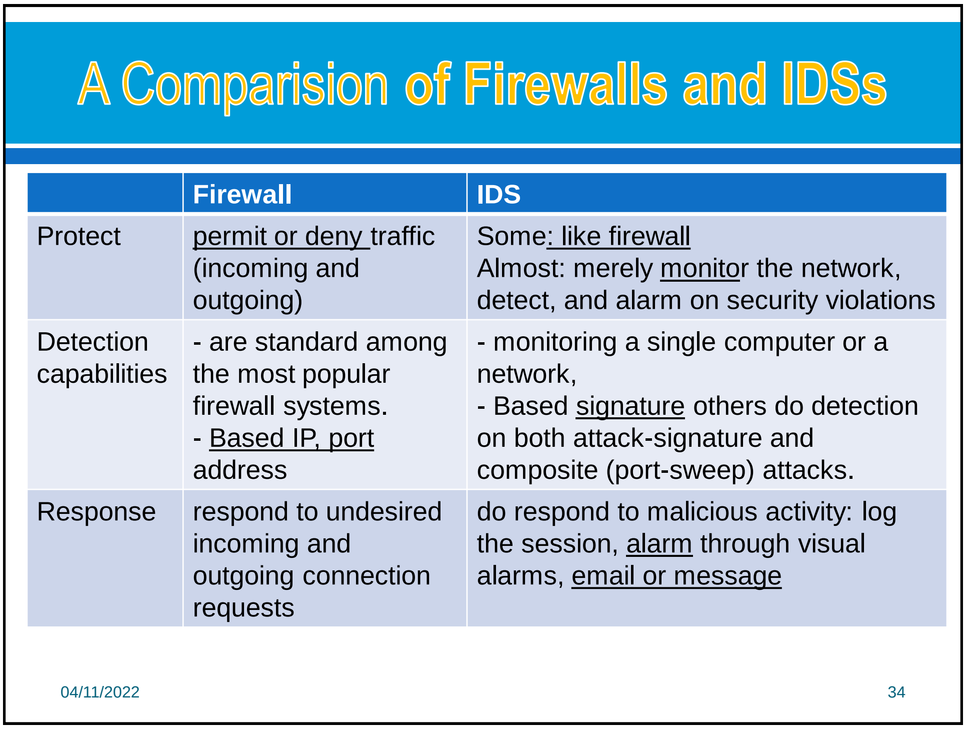
Intrusion Detection Systems

- Logical components:
  - sensors - collect data
  - Detection (Analyzers) - determine if intrusion has occurred
  - Response (user interface) - manage /direct /view IDS

sensors

Detection

Response

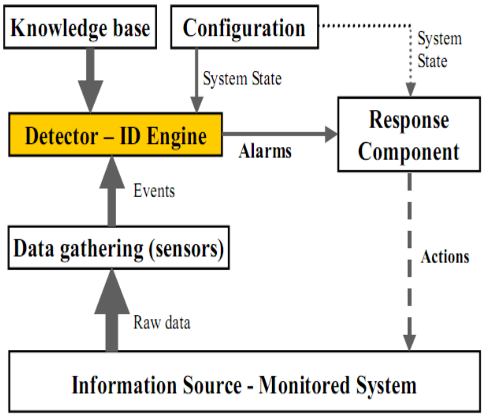


A Comparision of Firewalls and IDSs

	Firewall	IDS
Protect	permit or deny traffic (incoming and outgoing)	Some: like firewall Almost: merely monitor the network, detect, and alarm on security violations
Detection capabilities	- are standard among the most popular firewall systems. - Based IP, port address	- monitoring a single computer or a network, - Based signature others do detection on both attack-signature and composite (port-sweep) attacks.
Response	respond to undesired incoming and outgoing connection requests	do respond to malicious activity: log the session, alarm through visual alarms, email or message

IDS - Architecture

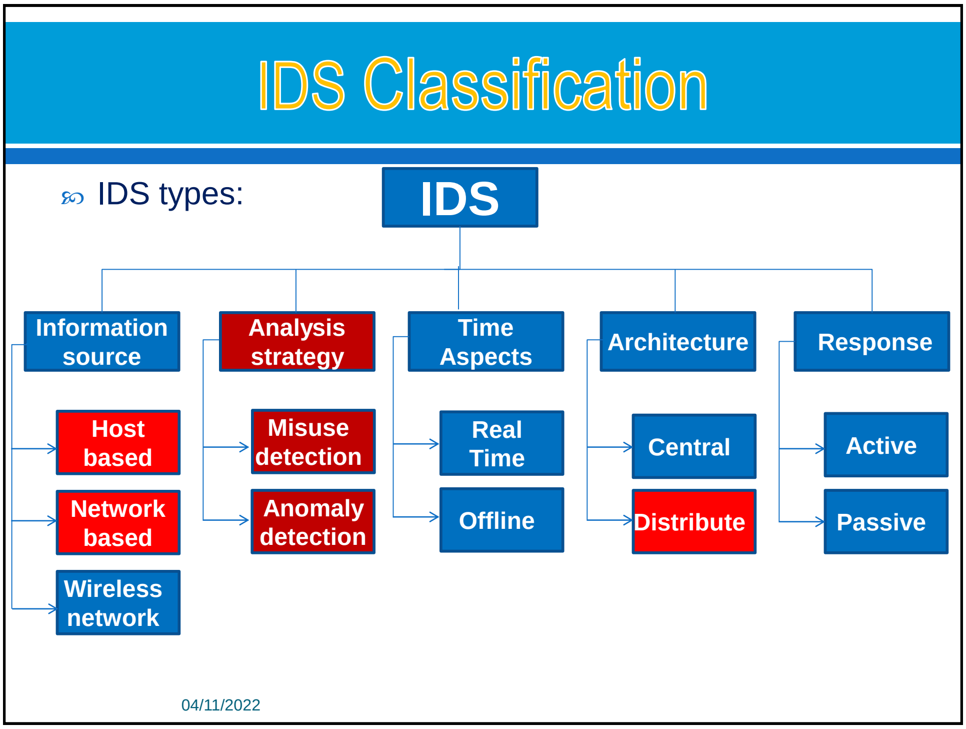
- **Data gathering device** (sensor):
  thu thập dữ liệu từ hệ thống giám sát
- **Detector** :
  phân tích dữ liệu để xác định các hành vi xâm nhập
- **Knowledge base** (database):
  - Các dấu hiệu tấn công đã được biết trước (signature-based)
  - Các profile về các hành vi hợp pháp trong hệ thống (alnomaly-based).
- **Configuration device**:
  cung cấp các thông tin về cấu hình hiện tại của IDS
- **Response component**:
  bắt đầu các hành động khi một hành vi xâm nhập được phát hiện.



04/11/2022 35

IDS Requirements

- run continually
- be fault tolerant
- resist subversion
- impose a minimal overhead on system
- configured according to system security policies
- adapt to changes in systems and users
- scale to monitor large numbers of systems
- provide graceful degradation of service
- allow dynamic reconfiguration



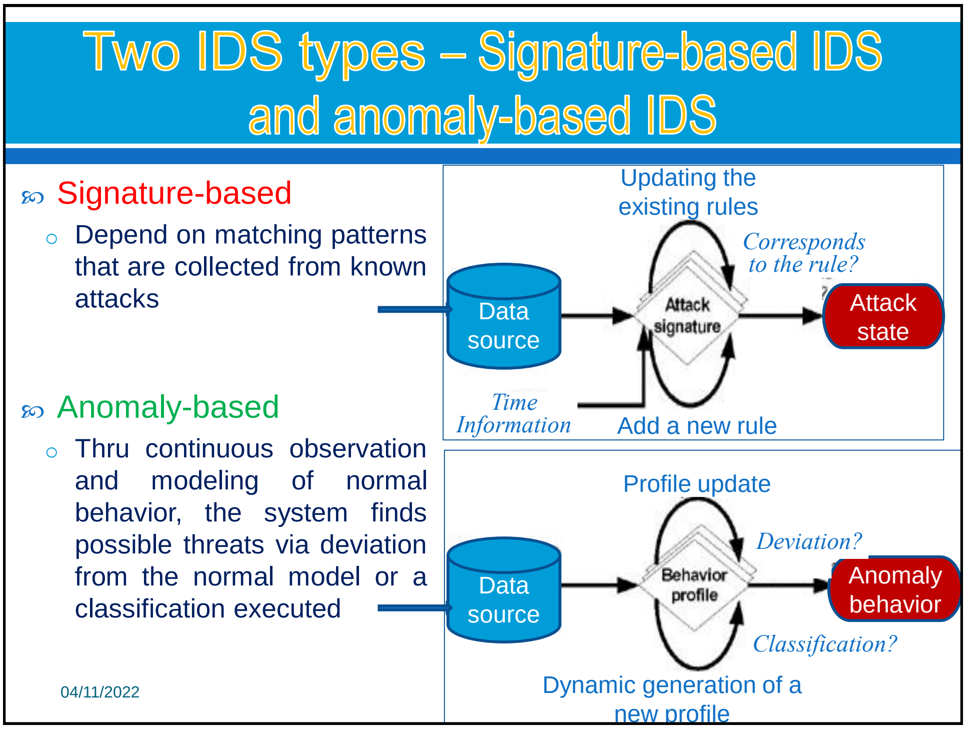
IDS Classification

- IDS types:

IDS

- Information source
  - Host based
  - Network based
  - Wireless network
- Analysis strategy
  - Misuse detection
  - Anomaly detection
- Time Aspects
  - Real Time
  - Offline
- Architecture
  - Central
  - Distribute
- Response
  - Active
  - Passive

04/11/2022



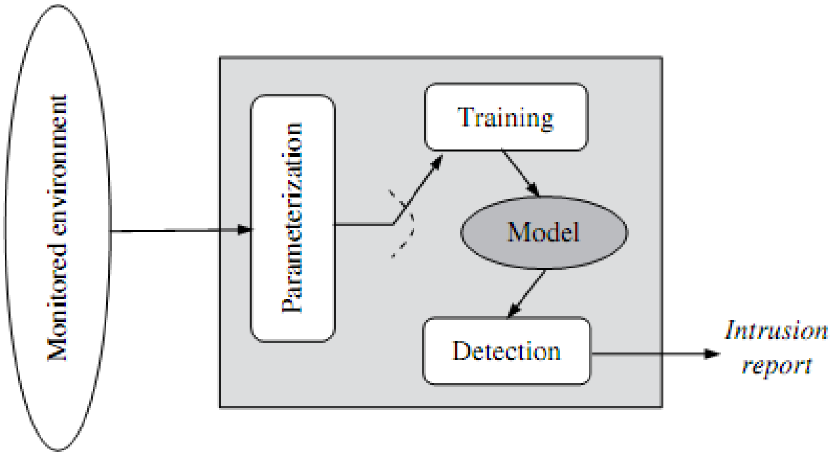
Two IDS types – Signature-based IDS and anomaly-based IDS

- Signature-based
  - Depend on matching patterns that are collected from known attacks

- Anomaly-based
  - Thru continuous observation and modeling of normal behavior, the system finds possible threats via deviation from the normal model or a classification executed

04/11/2022

Anomaly Detection



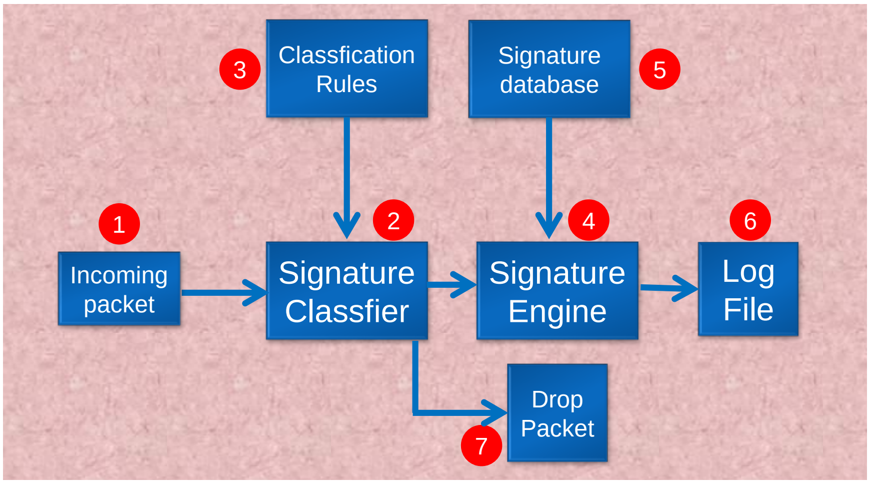
Anomaly Detection

- threshold detection
  - checks excessive event occurrences over time
  - alone a crude and ineffective intruder detector
  - must determine both thresholds and time intervals
- profile based
  - characterize past behavior of users / groups
  - then detect significant deviations
  - based on analysis of audit records
    - gather metrics: counter, guage, interval timer, resource utilization
    - analyze: mean and standard deviation, multivariate, markov process, time series

Anomaly Detection

- Advantage:
  - detect insider attacks based on collected normal activities in the system;
  - ability to detect previously unknown attacks; and
  - it is very difficult for an attacker to know which certainty activity can be executed without generate an alarm.
- Limits:
  - the system must go through a training period in which appropriate user profiles are created by defining normal traffic profiles, that is a difficult task and consumes a lot time.
  - Because it is looking for anomalous events rather than attacks, so they will generate false alarms when there is an anomalous behavior but not an attack

Signature-based: basic Architecture

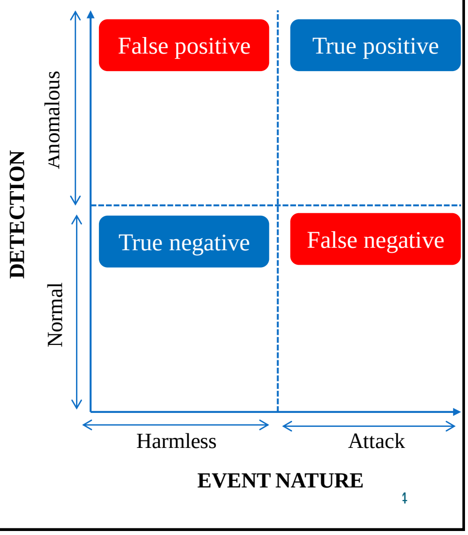


Signature Detection

- observe events on system and applying a set of rules to decide if intruder
- approaches:
  - rule-based anomaly detection
    - analyze historical audit records for expected behavior, then match with current behavior
  - rule-based penetration identification
    - rules identify known penetrations / weaknesses
    - often by analyzing attack scripts from Internet
    - supplemented with rules from security experts

Two IDS types – Pos & cons

- Signature-based
  - (+) Detect known attacks
  - (-) **False negative alarm**
  - (-) Can penetrate to know signatures, then another method is used to attack
- Anomaly-based
  - (+) Detect unknown attacks
  - (-) **False positive alarm**
  - (+) Can't penetrate to know certainty activity can be executed without generate an alarm.



DETECTION	Harmless	Attack
Anomalous	False positive	True positive
Normal	True negative	False negative

EVENT NATURE

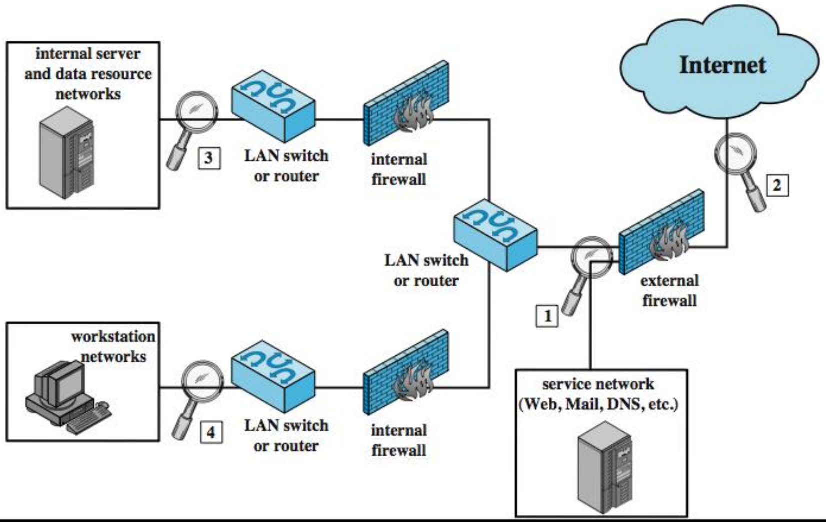
Host-Based IDS

- specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions
- two approaches, often used in combination:
  - anomaly detection - defines normal/expected behavior
    - threshold detection
    - profile based
  - signature detection - defines proper behavior

Network-Based IDS

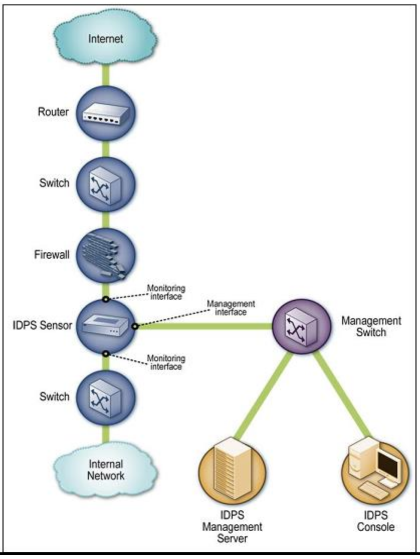
- network-based IDS (NIDS)
  - monitor traffic at selected points on a network
  - in (near) real time to detect intrusion patterns
  - may examine network, transport and/or application level protocol activity directed toward systems
- comprises a number of sensors
  - inline (possibly as part of other net device)
  - passive (monitors copy of traffic)

NIDS Sensor Deployment



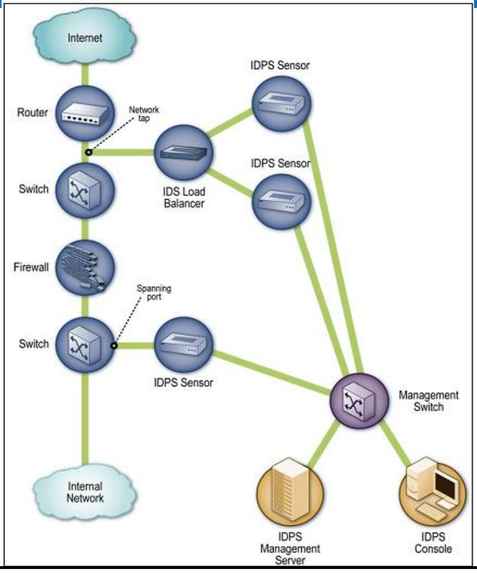
Network-Based IDS

- Sensor Inline



Network-Based IDS

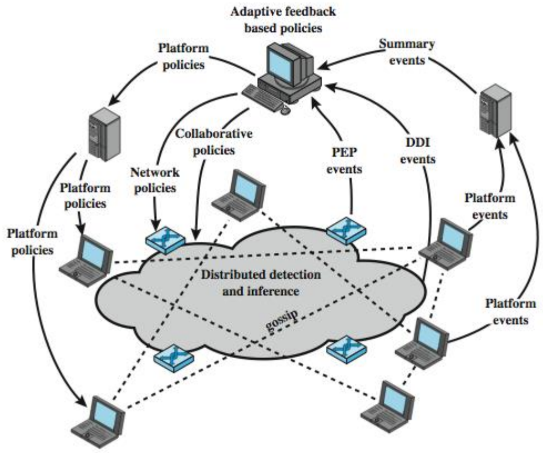
- Sensor **Passive**



Intrusion Detection Techniques in NIDS

- signature detection
  - at application, transport, network layers; unexpected application services, policy violations
- anomaly detection
  - of denial of service attacks, scanning, worms
- when potential violation detected sensor sends an alert and logs information
  - used by analysis module to refine intrusion detection parameters and algorithms
  - by security admin to improve protection

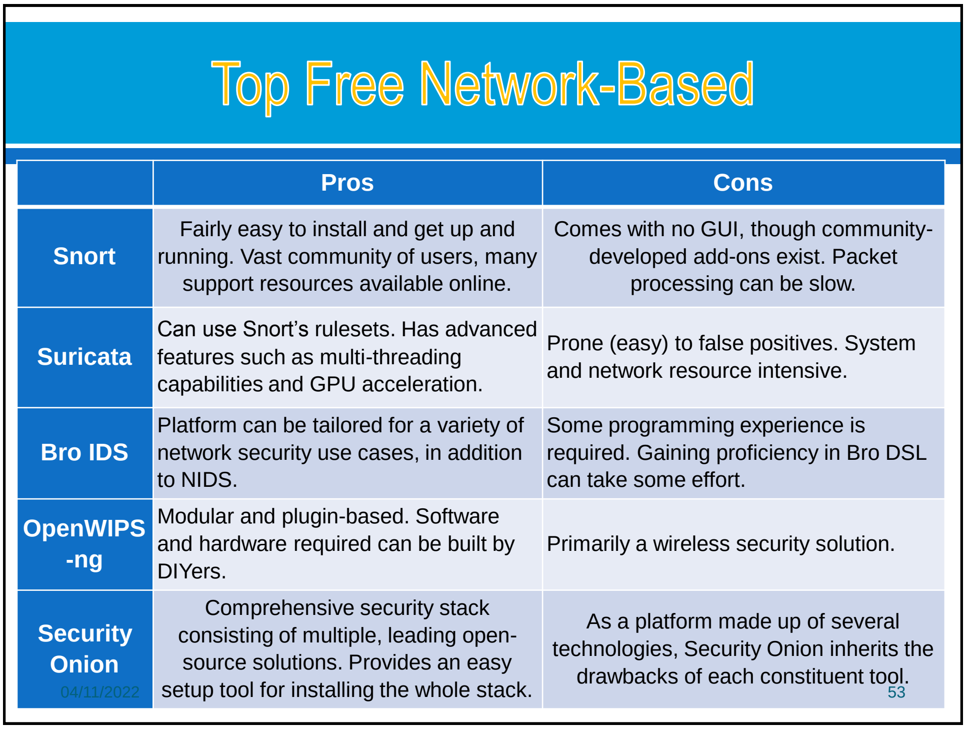
Distributed Adaptive Intrusion Detection



PEP = policy enforcement point
DDI = distributed detection and inference

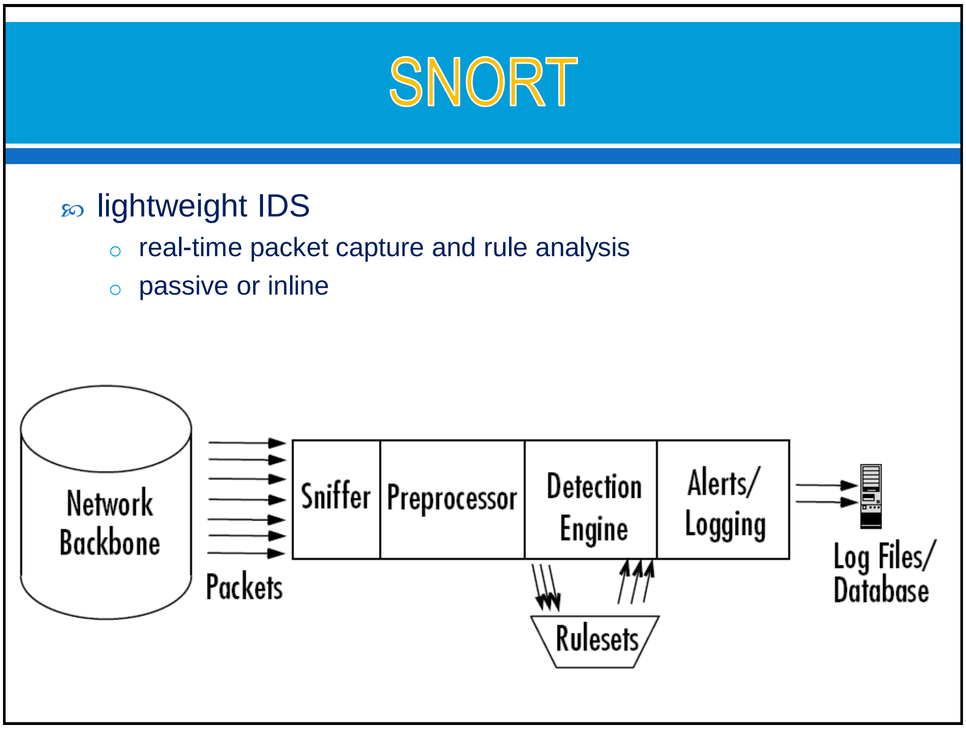
IDS Devices

- Cisco
- Fortinet



Top Free Network-Based

	Pros	Cons
Snort	Fairly easy to install and get up and running. Vast community of users, many support resources available online.	Comes with no GUI, though community-developed add-ons exist. Packet processing can be slow.
Suricata	Can use Snort's rulesets. Has advanced features such as multi-threading capabilities and GPU acceleration.	Prone (easy) to false positives. System and network resource intensive.
Bro IDS	Platform can be tailored for a variety of network security use cases, in addition to NIDS.	Some programming experience is required. Gaining proficiency in Bro DSL can take some effort.
OpenWIPS-ng	Modular and plugin-based. Software and hardware required can be built by DIYers.	Primarily a wireless security solution.
Security Onion	Comprehensive security stack consisting of multiple, leading open-source solutions. Provides an easy setup tool for installing the whole stack.	As a platform made up of several technologies, Security Onion inherits the drawbacks of each constituent tool.

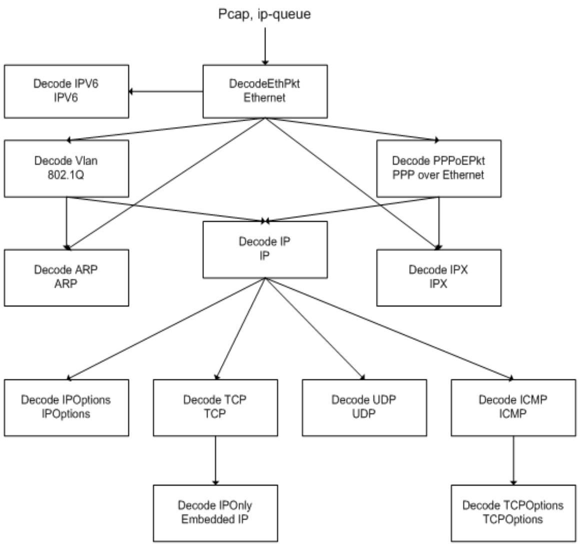


SNORT

- lightweight IDS
  - real-time packet capture and rule analysis
  - passive or inline

SNORT

- **Packet Decoder**



SNORT Rules

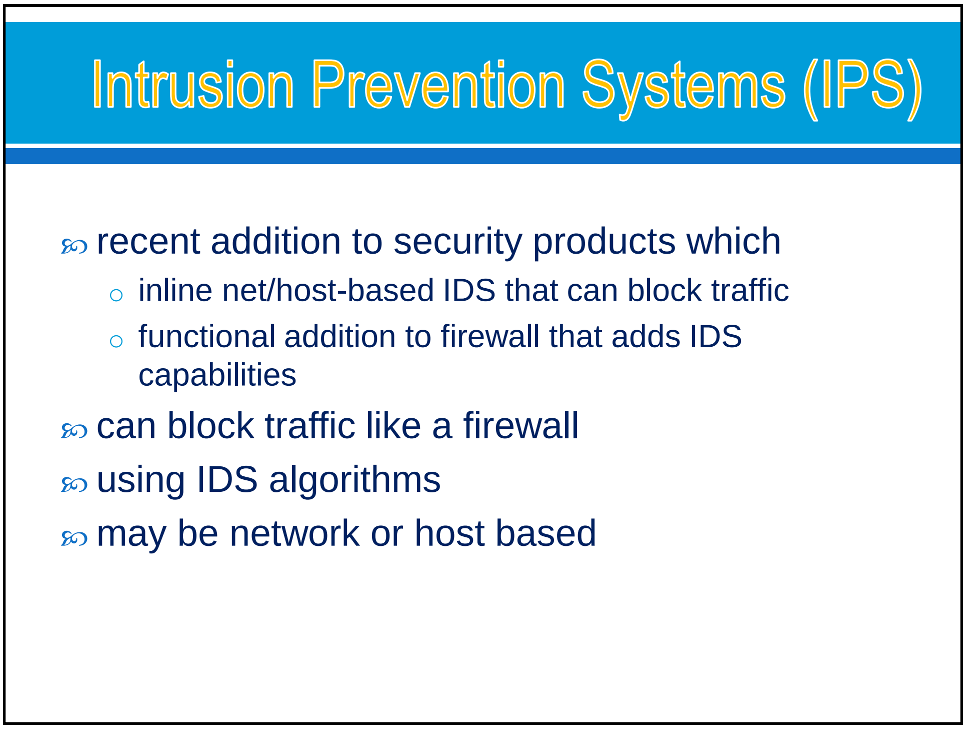
- use a simple, flexible rule definition language
- with fixed header and zero or more options

Header	Option

action	protocol	source IP	direction	source port	dest IP	dest port

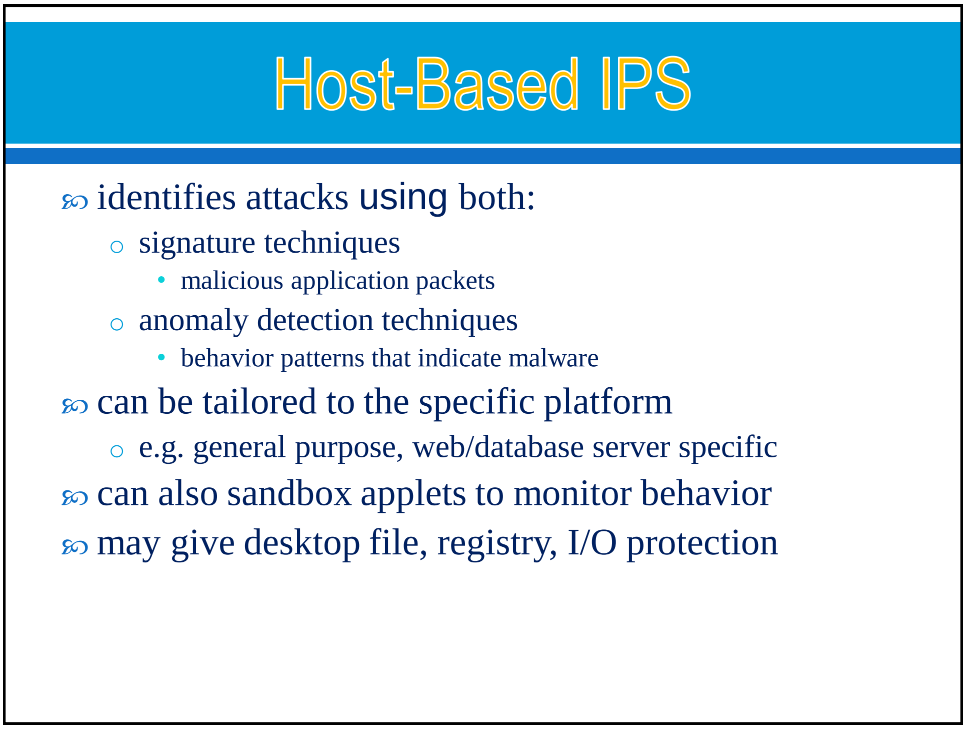
- example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)
```



Intrusion Prevention Systems (IPS)

- recent addition to security products which
  - inline net/host-based IDS that can block traffic
  - functional addition to firewall that adds IDS capabilities
- can block traffic like a firewall
- using IDS algorithms
- may be network or host based



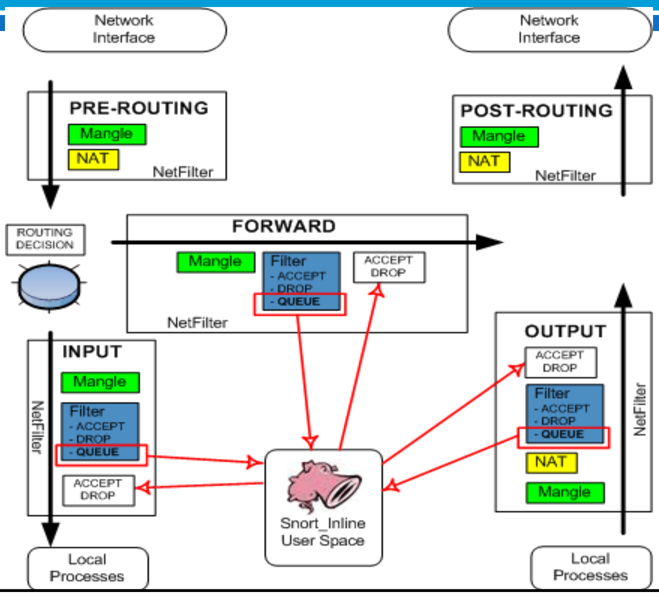
Host-Based IPS

- identifies attacks using both:
  - signature techniques
    - malicious application packets
  - anomaly detection techniques
    - behavior patterns that indicate malware
- can be tailored to the specific platform
  - e.g. general purpose, web/database server specific
- can also sandbox applets to monitor behavior
- may give desktop file, registry, I/O protection

Network-Based IPS

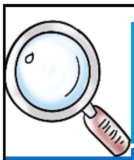
- inline NIDS that can discard packets or terminate TCP connections
- uses signature and anomaly detection
- may provide flow data protection
  - monitoring full application flow content
- can identify malicious packets using:
  - pattern matching, stateful matching, protocol anomaly, traffic anomaly, statistical anomaly
- cf. SNORT inline can drop/modify packets

Snort-Inline IPS



Snort-Inline modes

- Drop Mode
  A packet is dropped if it matches an attack signature.
  Three options are available in this mode:
  - Drop: Drops a packet, sends a reset back to the host, logs the event.
  - Sdrop: Drops a packet without sending a reset back to he host.
  - Ignore: Drops a packet, sends a reset back to the host, does not log the event
- Replace Mode
  A packet is modified if it matches an attack signature.

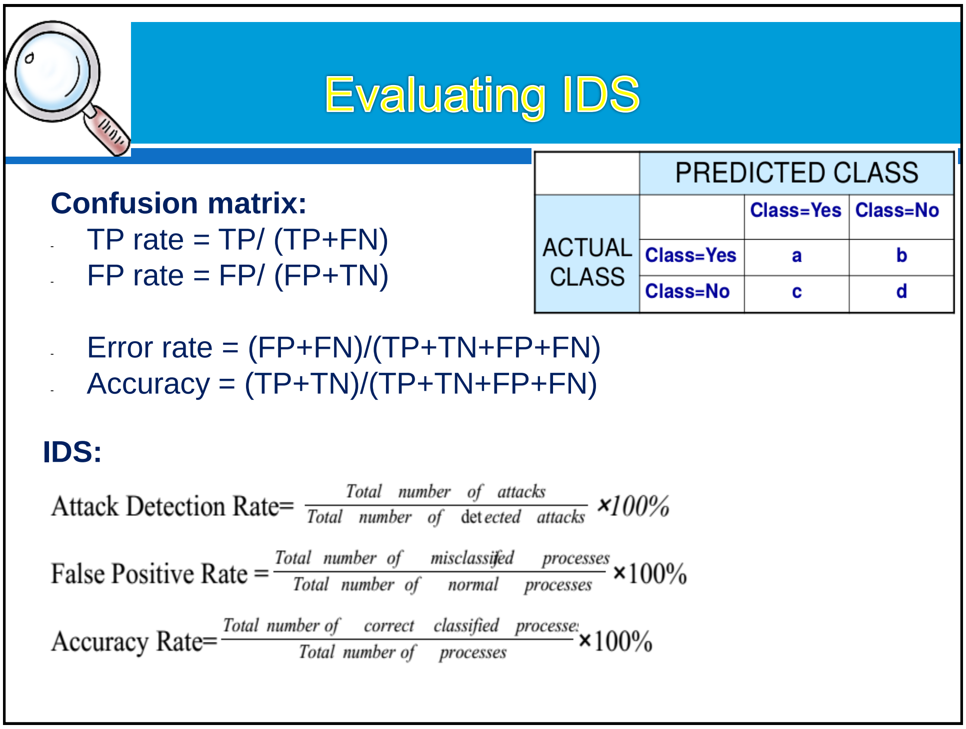


Evaluating IDS

Confusion matrix:

	PREDICTED CLASS		
ACTUAL CLASS		**Class=Yes**	**Class=No**
	Class=Yes	**a**	**b**
	Class=No	**c**	**d**

Parameter	Definition
True Positive Rate (TP)	Attack occur and alarm raised
False Positive Rate (FP)	No attack but alarm raised
True Negative Rate (TN)	No attack and no alarm
False Negative Rate (FN)	Attack occur but no alarm



Evaluating IDS

Confusion matrix:

- TP rate = TP/ (TP+FN)
- FP rate = FP/ (FP+TN)

	PREDICTED CLASS		
		Class=Yes	Class=No
ACTUAL CLASS	Class=Yes	a	b
	Class=No	c	d

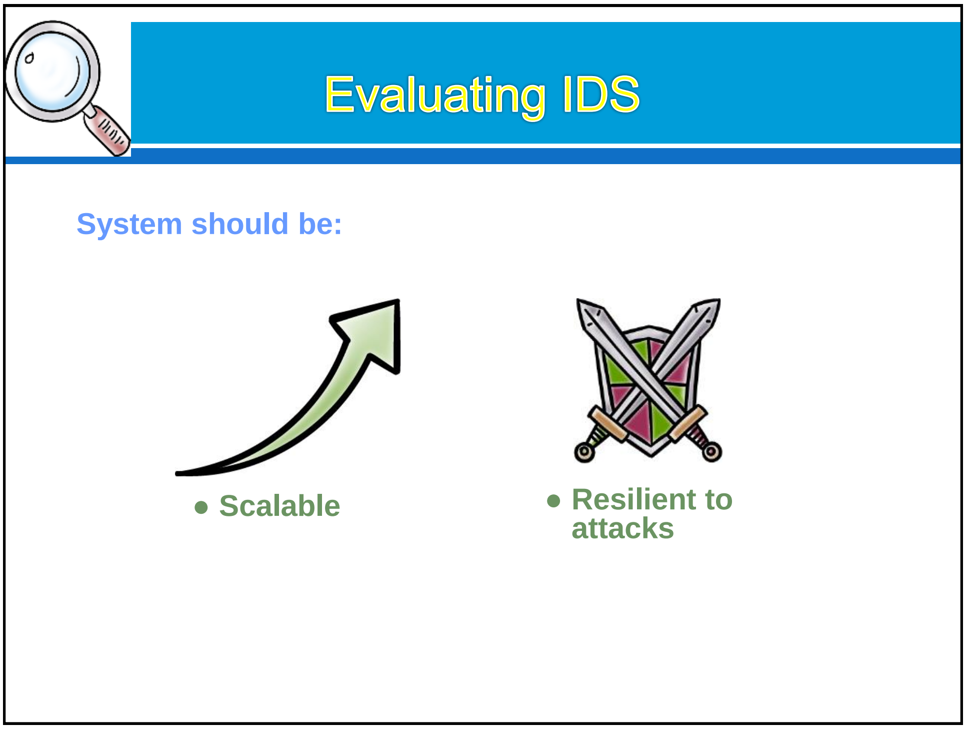
- Error rate = (FP+FN)/(TP+TN+FP+FN)
- Accuracy = (TP+TN)/(TP+TN+FP+FN)

IDS:

$$\text{Attack Detection Rate} = \frac{\textit{Total number of attacks}}{\textit{Total number of detected attacks}} \times 100\%$$

$$\text{False Positive Rate} = \frac{\textit{Total number of misclassified processes}}{\textit{Total number of normal processes}} \times 100\%$$

$$\text{Accuracy Rate} = \frac{\textit{Total number of correct classified processes}}{\textit{Total number of processes}} \times 100\%$$



Evaluating IDS

System should be:

- Scalable
- Resilient to attacks

Summary

- IDS
- Comparison
- Architecture
- Requirement
- Classification
- Signature-based and anomaly-based IDS
- Host-based and network-based IDS
- IPS

Practice

- Set up an IDS with one of the following:
  - **Snort**
  - **Suricata**
  - **Bro IDS**
  - **OpenWIPS-ng**
  - **Security Onion**
- Simulate attacks and use IDS above to detect
  - **DDOS: hping3, slowloris.pl**
  - **Brute Force:** xHydra (Kali Linux)