# Network Security

## Network Vulnerabilities

### What makes network vulnerable?

* Unkow attacks
  + Attacks may be launched from thousands of miles away.
  + Hack a machine from another hacked machine., Many points of attack: from any machine to any machine, Sharing, System/Network complexity, Unknown perimeter (host on multiple networks,Unknown paths (packets may travel over many different paths to a destination)

### Hazy network perimeter

* HAPPENED when it’s difficult to def the boundaries of a network due to factors such as cloud-based services and mobile access. PROBLEM: can create vulnerabilities and make it harder to control and monitor activity. SOLVE: use tools and strategies suck as network segmentation, access controls, and monitoring to improve network security.

## Network Attacks

### Threat Precursors

* Are techniques or activities that can be used by potential attackers to gather information about a network, system, or organization.
* COMMON THREAT: Port scan, war dialers, social engineering, dumpster diving, network mapping, vulnerability scanners, vendor documentation.

### Eavesdropping, Wiretapping

* **Eavesdropping**: the unauthorized interception of information by a third party.
* **Wiretapping**: the interception of telephone communications by a third party.
* TECHNIQUE can be done by using:Packet sniffers: wireshark, ettercap, tcpdump| Cable-based: wiretaps, inductance(tap wire, read signals without physical contact)| Insecure wireless networks: also possibility of theft of service

### Packet Sniffing

* Packet sniffing is the process of capturing and analyzing network traffic. DONE using a packet sniffer tool. Promiscuous mode can be used to read all packet on the network.
* *Ethernal Frame Structure* used to transmit data over Ethernet networks
  + STRUCTURE: preamble, destination MAC address, source MAC address, type, data, and CRC.
  + When a packet is sent over a subnet: all within collision domain read until dst address is found. If the des adress matches the device’s address, the packet copied to main memory and the CPU interrupts the OS to process the packet.
  + In *promiscuous mode*, read all packets on the network
  + In *wireless networks*, the Etherneet frame structure is modified to include a wireless header and fields to support wireless communication.

### Snoofing

* Snoofing is the act of capturing and analyzing network traffic.
* involves falsifying or manipulating the data in a packet to gain unauthorized access to a network or information.
* Masquerading involves an attacker pretending to be a different user or device in order to gain unauthorized access to a network or information. CAN BE USED TO DO session hijacking, man in the middle attack, and replay attack.

#### At Network Layer:

* involves Internet Protocol adress with a false address, which can be used to attacks such as phishing and network scanning.
* ICMP redirect attack redirect message inform a host of a better route to a destination. CAN BE USED TO redirect traffic to a malicious host. CAN BE PREVENTED by disabling ICMP redirect messages.

#### At Transport Layer:

* involves TCP/IP address with a false address, which can be used to attacks such as phishing and network scanning.
* ACTION: TCP establishes a connection via 3-way handshake
  + X -> S: SYN(ISNx), SRC = T
  + S -> T: SYN(ISNs), ACK(ISNx)
  + X -> S: ACK(ISNs), SRC = T
  + X -> S: ACK(ISNs), SRC=T,nasty-data
* *Non-blind spoofing*: attack impersonates the client to send ISNx. If attacker X is in the same subnet as the victim, he can simply sniff ISNs. With the correct ISNs, X can impersonate the trusted client T
* *Blind spoofing*: if attack in a different network, he cannot sniff the sequence number and acknowledgement number. He need to predict ISNs of the server(Known as *Sequence Number Prediction*)

### After Spoofing

* Man in the middle attack: beffore session starts.
* Session hijacking: after session starts. CAUSE: corrupt an established connection and re-establish it using the corrupted sequence number.
* Denial of service: can be direct DoS attacks(ICMP destination unreachable attacks). Spoofing help to hide the attacker’s identity.

### DoS (attack from a single source) and DDoS (attack from multiple sources)

* An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
* Attack on avalability of some resources
  + Network bandwidth: flood the network with bogus traffic
  + System resources: overload or crash network devices
  + Application Resources: crash or overload application
* DoS: ping of death, ARP spoofing, SYN spoofing, Flooding
* *Ping of Death* send oversize ICMP datagrams to the victim. The victim’s system will crash, freeze, or reboot.

### Source Address Spoofing (a type of DoS attack)

* technique used by attackers to falsify the source IP address of their network traffic, make it appear like it is coming from a trusted source.
* PURPOSE: use to deceivee and mislead the victim and evade detection or gain access to a network.
* SOLUTION: study backscatter traffic to detect DoS attacks.In honeynet, advertise routes to unused IP addresses to monitor attack traffic.

### TCP SYN spoofing (a type of DoS attack)

* An attack that spoofs the source IP aadress of a TCP SYN packet to prevent the establishment of a TCP connection and consume server resources.
* PREVENT: SYN cookies, firewall.

### SYN spoofing (a type of DoS attack)

* A defense technique can be used to prevent SYN flooding attacks by immediately tearing down half-open connections.

### Flooding (a type of DoS attack)

* A type of DoS attack that sends a large number of connection or information requests to a target.
* Any type of network packet can be used to flood DoS attacks.
* PING flood: send a large number of ICMP echo requests to a victim.
* **UDP flood** uses large number of UDP packets directed to some port number on the target system: server needs to respond
* **TCP SYN flood** uses large number of TCP SYN packets to a victim: server needs to respond with SYN-ACK
* *Countermeasure*: detect spoofing, packet filtering

### Reflection (a type of DoS attack)

* GOAL: overwhelm the target’network resources with a large volume of traffic, make it unavailable to legitimate users.
* attacker sends request packets with a *spoofed source address*1 of the victim, to a known service at the *intermediary*2 to generate *response packets*3 to the victim.
  + 1: response packets go to the target, 2: if requests in a smaller size result in responses in a large size, it’s an amplification attack., 3: intermediary is of high capacity
* *Countermeasure*: detect spoofing, blocking spoofed packets, packet filtering

### Amplification (a type of DoS attack)

* A type of network-based attack that uses a large number of requests to overwhelm the target’s network resources.

#### **Smurf attack**

* Attacker spoofs the IP source address as the victim’s IP. Sends a PING request to a broadcast address.Every host on the intermediary network replies(Flooding victim and intermediary network).

#### DNS Amplification attack

* GOAL: overwhelm the target’s network resources with a large volume of traffic, make it unavailable to legitimate users.
* STEP: Selects a large number of legitimate DNS servers as intermediary. Create a series of DNS requests containing the spoofed source address of the victim. Sends the requests to the selected DNS servers.
* A 60 byte request results in a 512 byte response. Amplification by converting a small request to a much large response.

#### Amplification attack

* A variation of reflector attacks aims to flood the targeet with responses from a large number of intermediary servers.
* Can be cause by: Increase the number of responses to a single request - Smurf
  + Increase the size of response packet - DNS Amplification
  + Directly increasing the number of request - DDoS

### DDoS

* Overwhelm target or it surrounding with flood od traffic.
* Attack vulnerable system from exploit system vul or trick into downloading trojan horse or other malicious code. Create zombie network. Use zombie network to launch DDoS attack.

#### DDoS Defenses

* Cannot be prevented entirely
* Defenses:
  + Attack Prevention - before the attack : Block spoofed source addresses on routers, block IP directed broadcasts, block suspicious services and combinations, use reverse filters.
  + Attack Detection and filtering - during the attack: Capture and analyze packet to identify attacks
  + Attack Source Traceback and Indentification - during and after the attack
  + Attack Reaction - after the attack : Implement contingency plan, implement good incident response plan.

# Network Security Controls

#### **Segmentation**

* is the process of dividing a network into smaller pieces. It is a security best practice that limits the damage of a breach.
* Demilitarized Zone(DMZ) is a network segment that located between an organization internal network and the public internet. PURPOSE: provide an additional layer of security for the internal network.

#### **Redundancy**

* is an important component of a comprehensive disaster recovery plaan that helps to ensure fast recovery and minimal data loss and can offer benefits like scalability, flexibility, and cost saving
* Critical for disaster recovery, can be implemented with:
  + Failover mode: Automatically switch to a backup system when the primary system fails.
  + Cloud-based redundancy: Replicating critical components or systems across multiple data centers in different locations.
* Eliminate single point of failure(a component that can cause a failure of the entire system) and increase availability.

### Encryption

* The most important and effective control against many network threats.

#### Link Encryption

* Encrypts the data as it is transmitted over a physical link between network deevices such as routers and switches.
* Messaages are decrypted at routers. Transparent to the user. Protect data transmitted over untrusted physical links.
* STEP: include selecting the encryption algorithm aand protocol, configuring the network devices, and testing the implementation.
* Need to decryption in transit.

#### **End-to-End Encryption**

* Encrypts the data at the application/presentation layer of the network stack.
* UNLIKE link encryption, end to end encryption does not involve decryption in transit.
* The data remains encrypted from the source to the destination.
* STEP: include selecting the encryption algorithm and protocol, intergraating the encrryption functionality into the application, and testing the implementation.
* GOOD: protect data confidentiality against flawed or untrusted lower layers

### Protocols

#### SSL/TLS (Secure Sockets Layer/Transport Layer Security)

* SSL designed to couter attack the concern over credit card transaction over the internet.
* Used mainly to secure Web traffic, but it can also be used to secure other types of traffic.
* Negotiation: choice of cipher suites, key exchange algorithm, protocol version
* SSL authentication: Anonymouse, RSA authentication, Diffie-Hellman parameters
* Key exchange: Diffie-Hellman key exchange, RSA-based key exchange
* Secure communication:
  + Encryption: RC4, DES, 3DES, AES,. (TLS 1.2 still support DES because of compatibility reasons))
  + Authentication: HMAC, using MD5, SHA1, SHA2

##### Steps

* Protocol Sequence: Negotiate parameters, authentication, key exchange, session.
* The client sends a ClientHello message to the server indicating the SSL/TLS version and the cryptographic algorithms it supports.
* The server responds with a ServerHello message, indicating the SSL/TLS version and the cryptographic algorithm it will use.
* The server sends its digital certificate to the client, which contains the public key used to encrypt the session key.
* The client generates a session key, encrypts it with the server’s public key, and sends it to the server.
* The server decrypts the session key using its private key, and the client and server exchange messages using the session key to encrypt and decrypt the data.
* When the session is complete, the client and server exchange closure messages to terminate the connection.

##### TLS 1.3 One round trip negotiation

* Why so many round in handshake?
  + Because the new handshake process is designed to provide increased security and privacy for user.
* STEP: ClientHello, ServerHello, Certificate, ServerKeyExchange, CertificateRequest, ServerHelloDone, Certificate, ClientKeyExchange, CertificateVerify, ChangeCipherSpec, Finished, ChangeCipherSpec, Finished
* TCP+TLS 1.2 : at least two round trips
* TCP+TLS 1.3 : 1 or 0 round trips
* TLS 1.3 stop supporting these ciphers: RC4, DES, 3DES, AES-CBC, MD5, SHA1, RSA key exchange.

### IPsec (part of IPv6, backported to IPv4)

* IPsec is a suite of protocols that provides security services at the IP layer.
* constructs a secure channel upon the IP layer
* Host-level security, transparent to applications, available to most OS(Windows, Linux, MacOS, iOS, Android)

#### IPsec Protocol Suite

* IPsec is specified in a number of RCFs
* Policy management
* Packet processing
* Key management

#### Two modes: Transport mode and Tunnel mode

* Transport mode: encrypts only the data portion of each packet, leaving the header unencrypted.
  + End systems are the initiatior and recipient of the protected traffic
  + Simply encrypt the payload but NOT the header
* Tunnel mode: encrypts the entire IP packet, including the header.
  + Gateways act on behalf of the hosts to protect the traffic
  + Encrypt the entire packet, the payload and the headers

#### IPsec Protocols

* Authentication Header (AH): provides authentication and integrity but not confidentiality.
  + Simple design: add header with authentication data
  + Security parameterrs
  + Authentication data
* ESP - Encapsulated Security Payload: provides authentication, integrity, and confidentiality.
  + Encapsulate datagram rather than add a header
  + Encrypt & authenticate the payload

#### IPsec Header

In AH transport mode, the IP header, authentication header, and IP payload (e.g. TCP, UDP, ICMP messages) are signed by the authentication header to ensure message integrity. In the IPsec header, the authentication header is added to the IP header.

In ESP transport mode, the IP header, ESP header, IP payload, and ESP trailer are encrypted with the ESP header, providing confidentiality and integrity protection. The ESP header and trailer are added to the IP header in the IPsec header.

In AH tunnel mode, a new IP header is added to the existing IP header, and the authentication header is signed to ensure integrity. In the IPsec header, both the IP header and the authentication header are included.

In ESP tunnel mode, a new IP header is added to the existing IP header, and the ESP header, IP payload, and ESP trailer are encrypted and signed for confidentiality and integrity protection. The ESP header and trailer are included in the IPsec header.

# Firewalls

* is a deevice that filters traffic between a protected indise network and less trusted outside network.

## Firewall Tasks

* Basic Task: allow or block traffic (based on sourceip and/or destination ip, and/or destination port)
* Why block traffic based on src port? Because some ports are used for specific services, and some ports are used for malicious activities.
* Task: Filtering traffic, block malicious trafic, allow authorized traffic, logging traffic, provide VPN access, Performing network address translation(NAT), enforcing network policies.

## Firewall Policy

* A firewall policy is a set of rules that determine whether to allow or block traffic. By mapping attributes to IP addresses, ports, and protocols, a firewall policy defines the traffic that is allowed to pass through the firewall.

### Default Policy

* Default policy(whitelisting): allow or block all traffic that is not explicitly allowed or blocked by the firewall policy.
* Default deny: specifies connectivity that is explicility allow, more secure but may break functionality, most organization default deny.
* Default accept(blacklisting): specifies connectivity that is explicitly blocked, less secure but more functionality, most home users default accept. ### Rule Order
* The order of the rules in a firewall policy is important because the firewall processes the rules in order, starting with the first rule in the list.
* firewall policies are non-monotonic (means a mix of allow and deny)
* Policy is evaluated until the packet matches a rule (first match, not best match)
* Can optimize firewall performance (e.g., frequent deny first)
* Can be useful to express complex requirements (e.g., isolate 10.0.2.0/24)

## Firewall Limitation

* cannot prrotect against malicious insiders, connection that don’t go through it, completely new threats, cannot protect fully against viruses, Most network traffic now transmitted over HTTP, which is difficult to filter, Does not help once the attacker is inside the network.

## Practicaal Issues

* Network layer firewalls are dominant: DMZ allow multi-tiered firewalling, tools are wide available, easy to configure, high performance.
* Issues: network perimeter is disappearing, hard to debug, maintain consistency, and manage.

## Firewall Types

### Stateless Packet Filtering

* Stateless packet filtering is the simplest type of firewall. It examines each packet individually and does not recognize any relationship between packets.
* Each packet is considered independent, but a single packet may not contain enough information to determine whether it should be allowed or blocked.

### Why stateful packet filtering?

* Problem with UDP: cannot distinguish between a new connection and a reply to an existing connection. TAKEAWAY: put DNS into DMZ
* Problem with ICMP: can be used in reflection attacks. TAKEAWAY: simple packet filter cannot match things up.
* Problem with RPC: bind to random port number, no way to know which to permit and block. TAKEAWAY: simple packet filter cannot protect RPC.
* Problems with FTP, SIP: use secondary channel for data transfer, TAKEAWAY: state should be maintained for FTP and SIP.

### Stateful Packet Filtering

* Stateful packet filtering is a firewall architecture that keeps track of the state of network connections traveling across it.
* Record per connection state in a dynamic state table to maintain state information
* CAN: handle UDP query/response, associate ICMP packets with connections, solve some of the in-bound/out-bound filtering issues (e.g., FTP but not RPC), but it still needs to block against address-spoofing

### Stateless vs Stateful

* **Stateless**:
  + PRO: much faster processing of packets
  + CONS: more complex rule specification, less secure, diffucult to handle multi-protocol such as FTP
* **Stateful**:
  + PRO: easier to specify rules, more secure, easier to handle multi-protocol, can handle FTP
  + CONS: slower processing of packets

### Network Address Translation (NAT)

* Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
* Translates private IP address to public IP address → Share a public IP among many internal hos
  + For outbound packets, it creates a state table entry and translates the address.
  + For inbound packets, it looks up the state table entry and translates the address
* Similar to stateful packet filter, but offers more flexibility
* WEAKNESS: NAT breaks end-to-end connectivity, NAT breaks IPsec, NAT breaks some applications (e.g., FTP, SIP, H.323, etc.)

### UPnP

* PURPOSE: allow devices to discover each other and establish network services for data sharing, communications, and entertainment.
* PRO: easy to use, no need to configure firewall
* CONS: no authentication, malware, flash, XSS can be used to exploit UPnP

### Circuit-Level Gateway(Proxy)

* A circuit-level gateway is a type of firewall that works at the session layer of the OSI model and can monitor Transmission Control Protocol (TCP) handshaking between packets to determine whether a requested session is legitimate.
* PRO: hides internal network, can be used to implement policy, can be used to log traffic
* CONS: slower than packet filter, cannot protect against malicious insiders, cannot protect against viruses, cannot protect against connection that don’t go through it, cannot protect against completely new threats.

### Application-level FW(Proxy)

* An application-level gateway is a type of firewall that filters traffic based on the application specific commands or data contained in the packet.
* Similar to circuit-level gateway, but works at application layer
* CAN: filter based on application data, log application data, hide internal network
* CONS: same as circuit-level gateway

## Implementing Firewall

* STEP: identify network assets, define security policies, choose a firewall, configure firewall rule, test firewall configuration, monitor and maintain firewall

# Intrusion Detection System (IDS)

## Intrusion Detection

* Most controls are preventive, but they are not effective against insider and impersonation attacks.
* Intrusion detection is a detective control
* **IDS** is a device(hard or software) that monitors a system or a network for malicious activity

## What to detect?

### Trojan Horse

* malicious program with open know effect and a hidden malicious effect. Hidden effect: steal info, control the computer, install malicious software, monitor and control hardware.

### Virus

* malicious program that can replicate itself and spread to other computers, perform some malicious activity, and hide itself.
* TYPE: boot sector, executable file infector, multipartite, polymorphic viruses, macro viruses, script viruses, etc.
* How it work: infect a file, spread to other files, execute malicious code, hide itself, and replicate itself.

### Worm

* a program that propagates from one computer to other using network, email, or other means. GOAL: exploit software vulnerabilities in client or server programs and actively seeks vulnerable machines to infect.
* Worm propagation: can use network connections to spead from system to system, can spead through share media

#### Intruder behavior and legitimate user behavior

* Intruder behavior: port scanning, password guessing, buffer overflow, etc.
* Key different: Intention, access pattern, authentication attempts, network traffic, system and application usage, anomalies in behavior, obfuscation and evasion techniques.

## Type of IDs

* Main diff is where the detector is deployed
* **Logging**: analyzes log files generateed by end system
* **Hybrid IDS**: a central analyzer combines data from multiple sensors

### Host-based IDS

* **Host-based IDS**: installed on each end system, collect and analyzes data for that host
* STRERNGTHS: Less inconsistencies or ambiguties, work for encrypted message, protect against non-network threats, Limitation: Expensive

### Network-based IDS

* **Network-based IDS**: monitor traffic at selected point on a network and examines packets header and payload for suspicious activity. (often placed on a router or a firewall)
* Sensor: timestamp, connection ID, source IP, destination IP, source port, destination port, protocol, packet size, etc. Helps to identify the source of the attack.
* OPERATION: maintain state for each connection, analyze packet header and payload, compare with known attack signatures, generate alerts, log suspicious activity, etc.
* STRENGTHS: **cheap** (a single NIDS can protect many host and look for global patterns), **simple**(easy to install and manage, smaller trusted computing base), **Eaasy to deploy**(OS independent, not affect end system , not consume any resources on end system), **Easy to scale up**
* LIMITATION: Inconsistent or ambiguous interpretation obetween the detector and the end host. Cannot detect attacks that do not go through the detector, attacks that do not generate network traffic, attacks that are encrypted, attacks that are not known, attacks that are not malicious.

### NIDs vs HIDs

* Deployment: NIDs(one detector protects many host, need special hardware), HIDs(one detector per host, need special software)
* Dependency: NIDs(OS independent), HIDs(OS specific)
* Context: NIDs(See only packets, unencrypted streams; has to reverse engineer behavior of applications; limited to network atta), HIDs(View the full picture on a single host; can detect non- network attac)
* Visibility: NIDs(Monitor broader events to uncover global patterns; can detect even failed attacks if it is deployed outside firewall), HIDs(Monitor only local event)
* Overhead: NIDs(Efficient, no or little latency), HIDs(Overhead on end system, Consumes host CPU/memor)
* Subversion: NIDs(nvisible in the network, harder for an attacker to subv), HIDs(Can be disabled by attacke)

## Type of Detection Method

* How the detector scans data to find attacks? signature-based, anomaly-based.

### Signature-based IDs

* know as misuse detection, scans for pre defined patterns of known attacks. Keep a list of patten that are not allowed and generate alerts.
* Require rule set be up to date, can detect only the know attack with good precision, easy to share the signature,

#### Rule

* def a pattern/signature that is associated with the attack.

#### Limitation:

* Wont catch new attack without a known signature, may not catch know attack if the variant doesnt match the signature, signature set are large,

### Anomaly-based IDS

* know as behavior detection, scans for abnormal behavior. Learn the normal behavior of the system and generate alerts when it detects abnormal behavior.
* Ideas: attacks look unusual/ Strategy: look for behavior that out of the ordinary.
* Profile: login sesion activity, comannd program execution, file and device accesses,
* How to buiid profile: Build manually(hard- specification bade detection), generated by stastical methods
* PRO: detect attack that haven’t been seen before

#### Risk

* attacker may train the IDS to accept his activity as normal behavior

#### Limitation

* Can Fail to detect known attacks, detect new attack if they don’t look unusual to the model, false positive rate might be high

### Misuse vs Anomaly

* Misuse: detect known attack, easy to share signature, easy to evade, high false positive rate
* Anomaly: detect new attack, hard to share, hard to evade, low false positive rate
* Root pwd modified while admin is on vacation: misuse
* Four consecutive failed login attempts: anomaly
* Failed connection attempt on 50 sequential ports: anomaly
* User who usually logs in from US logs in from China: anomaly
* UDP packet to port 1434: misuse
* Debug in the body of a SMTP message: mostly not an attack

## Detection Errors

* **False positive**: detector alerts when there is no attack(harmless behavior is flagged as malicious)
* **False negative**: detector fails to alert when there is an attack(an attack is not detected)
* All IDS suffer from both type of error

## Detection Accuracy

* often assessed in term of the rate at which these error occur
* **False positive rate**: P the detector alerts when there is no attack
  + FPR = FP/(FP+TN) = # of normal being mark as intrusion/# of normal
* **False negative rate**: P the detector fails to alert when there is an attack
  + FNR = FN/(FN+TP) = # of intrusion being mark as normal/# of intrusion
* **True negative rate**: P the detector correctly identifies normal behavior
  + TNR = TN/(TN+FP) = # of normal being mark as normal/# of normal
* **True positive rate**: P the detector correctly identifies malicious behavior
  + TPR = TP/(TP+FN) = # of intrusion being mark as intrusion/# of intrusion
* **Precision**: P the detector correctly identifies malicious behavior
  + Precision = TP/(TP+FP) = # of intrusion being mark as intrusion/# of intrusion
* **Recall**: P the detector correctly identifies malicious behavior
  + Recall = TP/(TP+FN) = # of intrusion being mark as intrusion/# of intrusion

### Detection Goal

* Ideal detector has 0% FPR and 0% FNR: almost impossible
* Good detector is achieving effective balance between FPR and FNR

## Base Rate Fallacy

* Occurs when we assess P(Y|X) without considering the prior probability of Y and the total P of Y
* consider a detector that is 99% sensitive: It means its false positive rate is 1% And its false negative rate is 1
* We use two random variables to denote the events:
  + 𝐴 denotes an Alarm is generated (marking a packet as attack)
  + 𝐼 denotes the event is indeed an Intrusion
* What we know:
  + 0.01% attack base rate → Pr 𝐼 = 0.0001
  + 1% FPR → TNR = 99%, which means: Pr(A|~I)= 0.01, Pr(𝐴|𝐼)= 0.99
  + 1% FNR → TPR = 99%, which means: Pr(~𝐴|𝐼) = 0.01, Pr(𝐴|𝐼) = 0.99
* To compute the precision of the detector Use Bayes’ rule of conditional probability, we get:
  + Pr(A) = Pr(A|I)Pr(I) + Pr(A|I)Pr(I) = 0.99 × 0.0001 + 0.01 × 0.9999 = 0.01
  + Pr(I|A) = Pr(A|I)Pr(I)/Pr(A) = 0.99 × 0.0001/0.01 = 0.0099
* When detector is less sensitive, its precision is also low.
* When the attack is not rare, a detector with a good recall can achieve good precision.
* When the attack is rare, the same detector has poor precision.
* When the attack is rare, further improving detector sensitivity does not help much

### 1. Assume an attacker controls a large botnet. He wants to attack a victim web server.

1. He wants to use the TCP SYN flooding attack. Please describe how this attack works.
   * TCP SYN flooding uses large number of TCP data packets that do not belong to known connections.

* The attacker sends a large number of TCP SYN packets to the victim web server, with the aim of consuming its network bandwidth and resources.
  + The web server will respond to each SYN packet by sending a SYN-ACK packet back to the source IP address.
  + This will cause the target system to continuously wait for the response to the SYN packets, that will never arrive.
  + The web server will be overwhelming the system with trafic and will not be able to respond to legitimate requests.
  + The attacker can also use spoofed IP adresses in order to make the attack more difficult to trace.
  + The attacker can take down the web server when the number of SYN packets is large enough.

1. Suppose the victim web server uses SYN cookies to protect itself. Will the attack still succeed? Why or why not?
   * The answer is yes, the attack can still succeed.
   * SYN cookies will make the web server less vulnerable to SYN flood attacks. Make it harder for the attacker to take down the web server. But it is possible for the attacker to overwhelm the server’s network bandwidth or other resources, which can result in a denial of service.
   * So if the attacker has enough resources that can overwhelm the server’s network bandwidth, the attack can still succeed.
2. The attacker then wants to use the TCP flooding attack. Will this attack work? Why or why not?
   * The answer is yes, the attack will work.
   * While SYN cookies can prevent the server from becoming overwhelmed by half-open connections, they do not necessarily protect the server from the volume of traffic generated by a TCP flooding attack.

### 2. What is amplification DDoS attack? Choose one UDP-based amplification attack as an example to explain how it is amplified.

* Amplification DDoS attack is a type of DDoS attack that relies on amplification factor to increase the amount of traffic sent to the victim.
* DNS amplification attack: is a UDP-based amplification attack
  + Selects a large number of legitimate DNS serves as intermediary amplifiers.
  + Creates a series of DNS requests to containing the spoofed source address of the victim.
  + Send the requests to the selected DNS servers.
  + This will cause amplification by increasing the size of the response packets.

### 3. Link-to-link encryption and end-to-end encryption can be used to protect data transmitted over networks. Which means is used by VPN?

* VPN uses end-to-end encryption to protect data transmitted over networks. Since link-to-link encryption only protects data transmitted over a single link.
* VPNs use link encryption between the end-user and VPN server.

| Rule | Direction | SRC Address | Dest Addr | Protocol | Dest Port | Action |
| --- | --- | --- | --- | --- | --- | --- |
| A | in | External | Internal | TCP | 25 | Permit |
| B | out | Internal | External | TCP | >1023 | Permit |
| C | out | Internal | External | TCP | 25 | Permit |
| D | in | Internal | Internal | TCP | >1023 | Permit |
| E | Either | Any | Any | Any | Any | Deny |

If an attacker (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of the local hosts (172.16.3.4), will the attack succeed? Sucess

* Packet 1: A TCP packet from 10.1.2.3 to 172.16.3.4 and port 8080 allowed by D;
* Packet 2: A TCP packet from 172.16.3.4 to 10.1.2.3 and port 5150 allowed by B.

### 7. Describe the differences between NIDS and HIDS. Can they be combined?

* NIDS is a network-based intrusion detection system that monitors and analyzes network traffic for suspicious activity.
* HIDS is a host-based intrusion detection system that monitors and analyzes the internals of a computing system as well as the network packets on its network interfaces.
* Yes they can be combined. Since NIDS and HIDS have different roles in monitoring and analyzing network and host activity, and can be combined to provide a more comprehensive approach to intrusion detection and prevention.
* IDS1 is less specific, so it will have a higher chance of generating false positive alerts.IDS2 is more specific, so it will have a higher chance of generating false negative alerts.This mean IDS1 will generating more alerts, some of which will be false alarms, while IDS2 will generate fewer alerts, but they are more likely to be true alerts. However, IDS2 is more likely to miss potential attacks than IDS1.