End of chapter questions

Chapter 7: Review Questions

7.1 Define a denial-of-service (DoS) attack.

- is an attack on availability
- can target end hosts, critical servers, or network based infrastructure

Restricts availability by overwhelming with traffic (network based), consuming resources, or poisoning some application.
Some examples include a SYN flood (resource based), reflection attack (network based), or SIP flood (application based).

7.2 State the difference between a SYN flooding attack and a SYN spoofing attack.

Key difference: With a SYN flood, the total volume of packets is the aim of the attack rather than the system code. This is the difference between a SYN spoofing attack and a SYN flooding attack.
(text isn't super clear on this)

SYN flooding sends SYN requests to a host but does not complete the three-way handshake. The victim's resources (threads) are consumed while it waits for the handshake to be completed.
SYN spoofing works the same way, but spoofs the source IP. As a result, the 2nd part of the three-way handshake is sent to some IP that the attacker has chosen. This masks the attacker's identity.

SYN Spoofing: attacker generates SYN connection request packets with forged source addresses. The TCP connections table becomes full, and future requests - including legitimate requests - are rejected

SYN Flood:

- keep known TCP connections table filled taking advantage of 3 way handshake
- target receives stream of spoofed TCP SYNs and starts "half-open" connections
- attacker never completes the connection
- **takes very little resources for attacker, where target has to spawn new thread for each attack**

7.3 What is the goal of an HTTP flood attack?

- goal is to consume considerable resources ie overwhelm targeted web server(s)

A network based attack that overwhelms the victim with session-based HTTP requests. It's hard to differentiate between legitimate and malicious traffic.
A spidering attack is a variant where a page is opened, and then each link on that page is recursively requested.
This also consumes lots of the attackers resources, so bots are often used.

7.4 What is a poison packet attack? Give two examples of such an attack.

- an attack that sends packets which trigger a bug in the system's network handling software, causing it to crash
- targeted system can no longer communicate over network until software is reloaded ie reboot
- two examples: ping of *DEATH*, teardrop, both directed at older Windows systems

An Application based attack that causes an App to fail.
An example is the fragmented packet attack, where the offset/fragment is used to make data overlap, crashing the program.

7.5 Why do many DoS attacks use packets with spoofed source addresses?

- source address spoofing makes the attacking systems hard to identify
- Prevents a reflective flood on attacker themselves
- packets are not reflected back to the true source

A smurf attack sends requests w/ victim's IP as the source, reflecting responses to the victim.
If the attacker's identity is hidden, he is less likely to be blocked.
Using normal looking source IP's causes traffic to blend in, and look not-malicious.

7.6 What is "backscatter traffic?" Which types of DoS attacks can it provide information on? Which types of attacks does it not provide any information on?

- Backscatter traffic: responses generated from spoofed DoS attack, ie response packets sent from victim
- **direct flooding** and **SYN flooding** results in response packets being scattered across the internet which is detectable
- **reflection attack** has no backscatter

7.7 What is the difference between a DDoS attack and a classic DoS attack? Why are DDoS attacks considered more potent than classic DoS attacks?

- DoS (**denial of service**): one computer and one internet connection is used to flood server with packets
- DDoS (**distributed denial of service**): similar to DoS but outcome is much different. Utilises many computers and many internet connections. Computers behind attack are typically distributed around world, ie botnet.
- key difference: scale of attack. Target server will be overloaded by hundreds / thousands of requests with DDoS

DDoS uses intermediaries, while DoS is just one attacker. The traffic is multiplied, making a network based attack more potent. The attacker is hidden, making it hard to find the original source. And because of the many intermediaries, it's hard to differentiate between normal and malicious traffic.

7.8 What architecture does a DDoS attack typically use?

- botnet consisting of zombies, either volunteer computers or infected computers
- Large DDoS networks have handler zombies and agent zombies

7.9 Define an HTTP flood.

- refers to attack that bombards Web servers with HTTP requests (a type of DoS attack)
- attackers sends large volume of seemingly legitimate session-based HTTP requests to victims' servers
- **countermeasures**:
    - use challenge request, ie captcha
    - use ML based detection engine

7.10 Define a Slowloris attack.

- attacker sends multiple partial HTTP requests to victims
- victim server will wait for attacker to complete HTTP request header, up to timeout period
- attacker will periodically send additional HTTP requests

Attacker keeps the session alive by sending a few more headers just before the session expires. This is a resource-based attack.

7.11 From an attacker's perspective, what are the drawbacks of a classic ping flood attack?
- attacker must have at least as large as bandwidth capacity as target
- attacker can be easily identified
- attack impacts attacker's resources
- target may limit the number of ping requests from one source

7.12 What defenses are possible against nonspoofed flooding attacks? Can such attacks be entirely prevented?
- If the attacker is stupid and using their own IP address as source, it can easily be traced back to attacker's location and dealt with by ISP
- attacks using particular packet types can be throttled by imposing limits on the rate these packets will be accepted
- high-end routers have the ability to limit packet rates

Limit the number of requests allowed from one source. Unusually large amounts of traffic can be identified and the source can be blocked. SYN cookies can free up threads.

7.13 What is the purpose of SYN cookies?
- to defend against SYN spoofing attack

Allows the victim to drop unfinished connections once it's queue fills up. Instead of keeping the thread open, it dumps the queue, and re-constructs it using the cookie if it does receive an ACK.

7.14 What defences are possible against a DNS amplification attack? Where must these be implemented? Which are unique to this form of attack?
- some defences include:
    - prevent address spoofing (would need network operators' cooperation)
    - IP address based authorization
    - use signed queries to authenticate the clients
    - do not offer recursive service to external networks
- must be implemented **?**
- unique in the sense that it's reflection based which exploits the disparity in bandwidth consumption between the attacker and targeted web source.

A DNS amplification attack sends (large) DNS responses to the victim. Countermeasures include IP address authorization, signed queries, local caching, and the prevention of spoofing.
Defences must be placed at the network level, not the host level.

7.15 What defenses are possible to prevent an organization's systems being used as intermediaries in a broadcast amplification attack?
- block the use of IP directed broadcasts

Also, a firewall can be put in place to block traffic from any source, using any protocol, except for a few known exceptions.

7.16 To what do the terms *slashdotted* and *flash crowd* refer to? What is the relation between these instances of legitimate network overload and the consequences of a DoS attack?
- these terms refer to events such as the olympics or breaking news which cause sites to experience very high traffic

- the relation between these instances and consequences of DoS attacks is the high traffic (i think), also may set off alerts on firewall and/or IDS/IDPS systems

7.17 What steps should be taken when a DoS attack is detected?

- identify type of attack
- use suitable filters to block the flow of attack packets
- ask ISP to trace flow of packets to identify source
- learn from attack for future attacks

7.18 What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others?

- do a network trace using Wireshark
- ask ISP to trace the flow of packets back in an attempt to identify their source
- nonspoofed packets are much easier to trace back than spoofed packets

Chapter 8: Review Questions

8.1 List and briefly define the skill level of intruders.

- skill levels:

- **apprentice:** minimal technical skill, use existing attack toolkits. Largest demographic of hackers.
- **journeyman:** sufficient skill to modify and extend attack toolkits to use newly discovered vulnerabilities
- **master:** mad skillz, capable of discovering brand new categories of vulnerabilities, or ability to write new powerful tool kitz

- classes of intruders:

- cyber criminals: individuals or members of organized crime group with a **goal of financial reward**
- activists: individuals or groups **motivated by social or political causes**
- state-sponsored organizations: groups **sponsored by govt to conduct espionage or sabotage**
- others: motivated by reputation

8.2 List five examples of intrusion.

- defacing a web server
- guessing and cracking passwords
- using an unattended logged in workstation without permission
- running a packet sniffer on a workstation to capture usernames and passwords
- copying a database containing credit card numbers

8.3 How are intruders classified according to skill level?

- apprentice: minimal technical skill, use existing attack toolkits. Largest demographic of hackers.
- journeyman: sufficient skill to modify and extend attack toolkits to use newly discovered vulnerabilities
- master: mad skillz, capable of discovering brand new categories of vulnerabilities, or ability to write new powerful tool kitz

8.4 What is meant by security intrusion?

- unauthorized act of bypassing the security mechanisms of a system

8.5 List and briefly describe the classifications of intrusion detection systems based on the source and the type of data analyzed.

- host-based detection (**HIDS**)
  - type of data analyzed:
    - system call traces
    - log file records
    - file integrity checksums
    - registry access
- network-based detection (**NIDS**):
  - sensors:
    - inline: all track passes through this sensor
    - passive: monitors a copy of all traffic
  - two categories:
    - signature / heuristic detection based
    - anomaly detection based
  - techniques used
    - pattern matching
    - stateful matching
    - protocol anomaly

    - traffic anomaly
    - statistical anomaly

- distributed / hybrid intrusion detection:

`Sensors on a distributed IDS collect data from the Application, Transport, and Network layer. This includes HTTP patterns for overflows and password guesses, TCP data for fragmentation, and IP data for spoofed addresses.`

8.6 What are three benefits that can be provided by an IDS?

- if an intrusion is detected quickly enough, intruder can be identified and ejected from the system before damage is done
- effective IDS can act as a deterrent
- intrusion detection enables the collection of information about intrusions, helping to strengthen intrusion prevention measures

8.7 What is the difference between a false positive and a false negative in the context of an IDS?

- false positive (FP): ie false alarms. authorized users / processes identified as intruders
- false negative (FN): intruders not being identified as intruders

8.8 Explain the base-rate fallacy.

-occurs when trying to detect something that happens rarely (intrusions). since the base-rate is low, we tend to either overestimate (leading to FP) or underestimate (leading to FN) the actual chances of a supposed intrusion being real. too many FP's? might ignore warnings. too many FN's? false sense of security.

8.9 List some desirable characteristics of an IDS.

-run continually with (minimal supervision)
-be fault tolerant
-resist subversion (detected if it has been modified)
-minimal overhead
-allow for (dynamic) configuration
-be scalable
-adapt to changes in system and user behaviour
-provide graceful degradation of service (a break in part of the IDS shouldn't break other working parts)

8.10 What is the difference between anomaly detection and signature or heuristic intrusion detection?

-Signature: focuses on analyzing past attacks to detect incoming attacks ("once bitten, twice shy")
-Anomaly: focuses on modeling 'normal' behaviour of users/systems, and uses deviations from that behaviour as sources of possible attacks ("this does not feel right")

8.11 List and briefly define the three broad categories of classification approaches used by anomaly detection systems.

-Statistical: Analyze observed behaviour using univariate/multivariate/time-series models of observed metrics
-Knowledge based: Classify observed data using predefined rules.
-Machine learning: Use data-mining techniques/labeled training data to build models.
- Threshold-metrics

8.12 List the advantages of using machine-learning approaches for anomaly detection.

-Flexibility (variety of ML algorithms available, each with pros and cons)
-Adaptability (given labelled data, can work in many environments)
-Ability to capture interdependencies between observed metrics (might be able to identify previously unknown relations between variables)

8.13 What is the difference between signature detection and rule-based heuristic identification?

Signature based: Relies on a large collection of known patterns signatures (must have many signatures to reduce false alarms).
Rule based: Relies on a set of rules to detect penetrations. These rules can be derived from analyzing attack tools/scripts on the Internet or gathered through domain expertise (e.g. interview sys admins).

8.14 What is the major advantage of HIDS over NIDSs and firewalls?

HIDS can detect both external and internal intrusions.

8.15 Which of anomaly HIDS or signature and heuristic HIDS are currently more commonly deployed? Why?

Signature/heuristic HIDS are more 'wisely used' as they're not as dependent on the underlying filesystem - Anomaly HIDS have issues with a lack of a system call interface in Windows. Likewise, they can't detect changes made to currently running processes as they can only examine files, not processes (this is me bsing)
- Anomaly HIDS use more resources

8.16 What advantages do a Distributed HIDS provide over a single system HIDS?

- more effective defense can be achieved by coordination / cooperation among IDSs across a network
`More data -> more detection`

8.17 Describe the types of sensors that can be used in a NIDS.

- Inline: all traffic must pass through sensor. Generally inserted / combined with either firewall or network switch
- Passive: monitors a copy of all traffic; actual traffic does not pass through sensor
`Sensors can pick up App layer info (DHCP, DNS< HTTP, SMTP), Transport layer info (TCP< UDP), and Network layer info (IP addr, illegal headers).`

8.18 What are the advantages of locating the NIDS sensor inside the external firewall?

- Documents number of attacks originating on the internet that target the network
- Documents types of attacks originating on the Internet that target the network
- Can identify flaws in external firewall's rules(?)
`Can detect traffic that originated from internal machines. If the sensor is outside the external firewall, internal traffic never passes through it.`

8.19 Are either anomaly detection or signature and heuristic detection techniques or both used in NIDS?

- Both

8.20 What are some motivations for using a distributed or hybrid IDS?

- Combining multiple different IDS technologies can theoretically produce a much stronger IDS
- Possesses the benefits of multiples approaches while overcoming many of the drawbacks
- A single host may not be able to detect an attempted intrusion but another may catch it
- If enough "gossip" is generated, then the hybrid IDS may be able to determine that the low-level noise is actually a true positive

8.21 What is SNORT? What are the logical components of a SNORT installation?

- Open source, highly configurable, portable IDS. Can be host based or network based
- Characteristics:

    - easily deployed on most nodes
    - efficient operations that uses small amount of memory / processor time
    - easily configured
- Logical components
    - packet decoder
    - detection engine
    - logger
    - Alerter

SNORT rules include:
Action: what to do if an intrusion is detected
Protocol: analyze packet if it matches the protocol. For example, some protocols might be considered safe, and not worth the electrons that analysis would require.
src/dst ip and port: allow or deny traffic based on where it's coming from, where it's going, and what port.

8.22 List four logical components of Snort architecture.

- **Packet decoder**: identifies packet protocol headers at the data link, transport, and application layers
- **Detection engine**: tasked with intrusion detection
- **Logger**: stores the packet info
- **Alerter**: alert can be sent for every detected packet

Chapter 9: Review Questions

9.1 List the different types of firewalls.

- Packet filtering firewall
- Stateful inspection firewall
- Application proxy firewall
- Circuit-level proxy firewall

Host/Personal based firewalls: software to secure an individual host. Restricts the flow of packets like a packet filtering firewall, but it's placed on the host server.

9.2 List four characteristics used by firewalls to control access and enforce a security policy.

- Filtering characteristics include:

- IP addresses and protocols
- applications
- user identity
- network activity

Transport layer address (MAC address)
Interface

9.3 Which type of attacks is possible on a packet filtering firewall?

- susceptible to certain TCP / IP protocol attacks

A packet-filtering firewall resides on the Transport and Network layer, so it doesn't inspect Application Layer data, so it is susceptible to Application attacks like a teardrop attack.

9.4 How does a traditional packet filter make filtering decision?

- heuristic based, ie user creates and maintains the rule set

An example of a filter rule might be: deny all incoming packets to port 22 except from source x.

9.5 What is the difference between a packet filtering firewall and a stateful inspection firewall?

- **packet filter** makes filtering decisions on an individual packet basis
    - does not take into consideration any higher layer context
- **stateful packet inspection** firewall tightens up the rules for TCP traffic: it creates a directory of outbound TCP connections
    - there is an entry for each currently established connection
    - this firewall reviews the same packet info as a packet filtering firewall, but also records information about TCP connections

Packet filters only inspect headers, and does not look at Application layer data. So a packet filter can sometimes be bypassed by simply sending a packet with the "reply" flag ticked.
Stateful inspection firewalls analyze down to the Application Layer. Also, it monitors and tracks ingoing and outgoing traffic. This allows it to apply rules based on communication patterns instead of simply individual packets.

9.6 What is the difference between a gateway and a firewall?

- all the network layer information - including application layer - can be used
- gateway looks at applications, and can provide deep packet inspection
- can be used to monitor and filter the data, as well as blocking it

A gateway is hardware that acts as a connector between two different networks. An example would be a router which connects a local network to the internet. A firewall is both hardware and software that inspects data flowing through it and makes decisions including whether or not the packet should be allowed to pass.

9.7 Describe a situation where circuit-level gateways can be used.

- used for outbound traffic, whereas incoming traffic may have an application gateway for deeper inspection (at the cost of higher overhead)

-relays transport layer segments from one end to another without examining the contents

When a user is requesting a web-page, the request first passes through the circuit-level gateway on the transport layer. The gateway forwards the request, acting as a proxy, and thus hiding the internal user information (IP, MAC, etc). When the gateway receives a response, it sends it to the requester.

9.8 How do FTP and Telnet work through a firewall?

- use a proxy server
- permit incoming connections at a restricted port range

9.9 What are the common characteristics of a bastion host?

Bastion host = typically used to host IPSec or gateways. They are exposed to the outside world and must take extra security cautions, such as:

-Only uses essential services (as deemed by the network admin)

-Might have extra layers of authentication before access to proxy services is allowed

-Only supports a subset of the standard application set.

-Only allows access to specific hosts systems

-Each proxy is independent of each other on the bastion host.

The Bastion host is the only host on a network which is exposed to the outside world, and is thus the only host vulnerable to attacks. It filters out malicious traffic, and forwards safe traffic to the network it stands in front of. It is placed outside the firewall, or if there are two firewalls, it's placed in the DMZ.

9.10 Why is it useful to have host-based firewalls?

-Can be tailored to the host

-Independent of network topology (can deal with internal and external attacks)

-Extra layer of defence

9.11 What is a DMZ network and what types of systems would you expect to find on such networks?

DMZ = demilitarized zone. It is a network config where device sit between an external firewall and an internal firewall. Such networks exist when we need to access some portion of them externally, but still need some protections on it's internal components (e.g. a website can have its web server in the DMZ, and its database inside the internal firewall).

9.12 What are the differences between an IDS, an IPS, and a firewall?

IDS - attempts to detect malicious activity

IPS (aka IDPS - intrusion detection and prevention system) - extends IDS to include the ability to prevent or block detected malicious activity. Typically more sophisticated than firewalls as they can also inspect non-packet based effects (system resources, directory traversal)
Firewall - Analyzes packets and enforces policy based on ruleset. Typically limited to packet/header information (source, destination, port, etc.)

9.13 List the types of malicious behaviors addressed by a Host-based Intrusion Prevention System (HIPS)?

- **Modification of system resources**
    - rootkits, trojan horses, and backdoors operate by changing system resources such as libraries / directories / registry settings / user accounts
- **privilege-escalation exploits:**
    - attempts to give ordinary users root access
- **buffer-overflow exploits**
- **access to email contact list**
- **directory traversal**

9.14 What are the different places an IPS can be based?

- single bastion inline
- single bastion T
- double bastion inline
- double bastion T
- distributed

9.15 List at least three malicious behaviors addressed by HIPS.

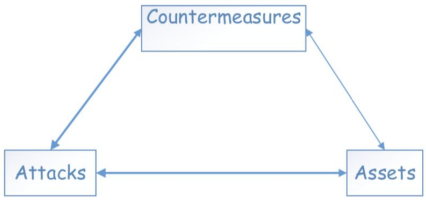
- Modification of system resources
- privilege-escalation exploits
- buffer-overflow exploits
- access to email contact list
- directory traversal

9.16 List a few methods used by a NIPS device to identify malicious packets.

-Pattern matching (compared packets to packets from known attacks)
-Stateful matching (look at traffic stream vs individual packets)
-Protocol anomaly (look for deviations from RFCs)
-Traffic anomaly (look for floods and new services on the network)
-Statistical anomaly (have baselines for certain activity, alert when deviations are observed)

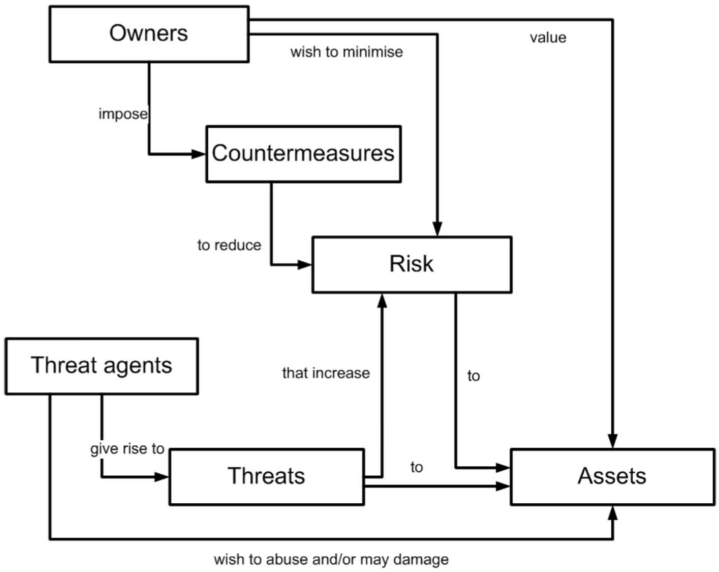
Lecture Notes
Lecture 1

Typical evaluation process of threats :



Vulnerability: a flaw or weakness that can be exploited
Threat: a possible danger of a vulnerability exploit
Risk: an expectation of loss as a result of a vulnerability
Attack: actual instantiations of threats
Adversary: a threat to a system

Security concepts and relationships:



Three categories of assets:

1) Low: limited
2) Moderate: serious
3) High: severe or catastrophic

CIA Triad of Security

1) Confidentiality
    a) data confidentiality
    b) privacy

2) Integrity
    a) data integrity
    b) system integrity
3) Availability
    a) disruption of access to information

Breaches of each:
Confidentiality: unauthorized disclosure of information
Integrity: unauthorized modification of destruction of information
Availability: disruption of access to or use of information

Essential network and computer security requirements:

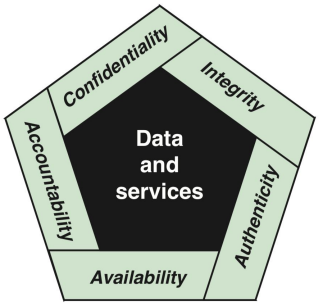


Figure 1.1 Essential Network and Computer Security Requirements

General Model
Attacks, categorized as:

- active: easier to detect / harder to protect
- passive: hard to detect / easier to protect

or

- inside
- outside

Countermeasures:
Identify:

- organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

Protect:

- appropriate safeguards to ensure delivery of critical services

Detect:

- identify occurrence of cybersecurity event

Respond:

- take action regarding a detected cybersecurity incident

Recover:

- maintain plans for resilience and restore any capabilities that were impaired due to incident

Countermeasures may result in:

- new vulnerabilities
- residual vulnerabilities
- goal to minimize risk given constraints

Threats and Assets

	Availability	**Confidentiality**	**Integrity**
Hardware	Stolen/disabled equipments	An unencrypted drive/DVD	
Software	Deleted programs	Unauthorized copy	Malware
Data	Deleted files	Unauthorized read, Inference	Modification of existing files
Comm. Lines	Messages deleted	Message read, traffic analysis	Messages deleted, modified, duplicated or fabricated

Security Functional Requirements

Security Design Principles

Security Strategies

- Policies
- Implementations
- Assurance

Lecture 2

Models
DARPA model

- TCP (transmission control protocol)
- IP (Internet protocol)
- Used **packet switching** instead of circuit switching
- packet consists of
    - packet header
    - data

OSI Model

- encapsulation: each stack layer adds it own header, and possibly a footer to data unit received before passing it on to the next layer.
- Layers
    - Application
    - Presentation
    - Session
    - Transport
    - Network
    - Data link
    - Physical
- Multilayer protocols:
    - http over wired ethernet: [Ethernet [IP [TCP [HTTP]]]
- add SSL:
    - [Ethernet [IP [TCP [SSL [HTTP]]]]
    - [Ethernet [IPSec [IP [TCP [SSL [HTTP]]]]

TCP

- Ports:
    - An integer range of: 0 - 65535
        - Privileged services: 0 - 1023
        - Registered software ports: 1024 - 49151
        - 49152 - 65535
    - Both ends agree to use
    - process called “listening on” or “binding on”
- Addressing:
    - Every network interface card (NIC) has a unique 48 or 64 bit factory burned number
    - Every software process that communicates must have a network address
    - Network device / node can use multiple types of addresses
        - MAC address
        - IP address

        - Machine name
        - Organizational / domain name

Transport Layer Protocols

- TCP / UDP
- TCP: connection oriented reliable protocol (3-way handshakes)
- supports full duplex communications
- has large overhead

TCP Headers

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																	Urgent pointer (if URG set)														
20	160	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.)																															
...	...	...																															

- Unskilled Attackers Pester Real Security Folk!
    - URG
    - ACK
    - PSH
    - RST
    - SYN
    - FIN

UDP

- Size up to 65535 bytes long
- No pre established session
- Smaller overhead

UDP Headers

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

IP Protocols

- exchange data between peers not on same network
- protocols focus on:
    - discovering paths from source to destination (routing)
    - Node / path node availability
    - Dynamic address configuration

    - packet addressing
    - resolution between network layer addresses and lower level addresses

- examples of network layer protocols:
    - Internet control message protocol (ICMP)
    - Address resolution protocol (ARP)
    - Reverse address resolution protocol (RARP)
    - Routing information protocol (RIP)
    - Open shortest path first (PSPF)
    - Border gateway protocol (BGP)
    - Internet group management protocol (IGMP)
    - Internet protocol (IP)
        - provides route addressing for data packets
        - connectionless, unreliable datagram service
        - does not guarantee packets will be delivered
    - Internet protocol security (IPSec)
    - Internetwork Packet exchange (IPX)
    - Network address translation (NAT)
    - Simple key management for internet protocols (SKIP)

IP Addressing

- internet addressing
- size: 32 bit unsigned binary value
- used by IP protocol to uniquely identify a host
- each IP packet contains source IP and destination IP address
- destination must be translated or mapped to a physical device

Routing

- IP routing: process of sending packets from a host on one network to another host on a different remote network
    - a device that can simultaneously function as both a normal host and a router
    - routing tables determine the next hop address to which the packet should be forwarded

Headers

- 20 bytes for IPv4 (max size cannot exceed 60 bytes)
- 40 bytes for IPv6
- TTL: time to live, time datagram is allowed to travel
    - each router subtracts 1 from the TTL value

IP Packet Headers

- protocol numbers:
    - 1: Internet control message protocol (ICMP)
    - 2: internet group management protocol (IGMP)
    - 4: IP (IP encapsulation)
    - 6: Transmission Control Protocol (TCP)

    - 17: User datagram protocol (UDP)

Vulnerabilities

- TCP / IP have numerous security vulnerabilities including
    - sniffing
    - spoofing
    - man in the middle
    - syn flood
    - fragment attack

ICMP - internet control message protocol

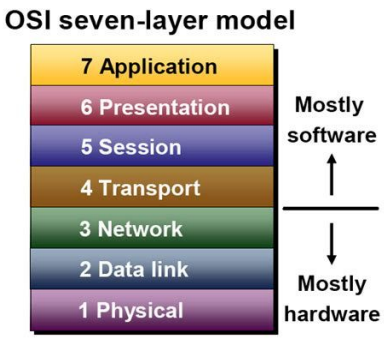
- 8 byte header
    - first 4 bytes are fixed
    - last 4 bytes depend on type / code of that ICMP packet
- variable sized data section
- Types:
    - ping
    - traceroute
        - sends packets with TTL starting at 1. keeps track of responses
        - mac os uses UDP ; windows uses ICMP

ARP (address resolution protocol)

- used in interoperability of logical and physical addressing schemes
- uses lookup table

Devices

- Layer 1: Hubs
    - repeats data it receives on one port to all other systems on its other port
- Layer 2: Bridge
    - connects two physical segments of a network. maps mac addresses to network segments, ie sends messages to all devices on the segment
- Layer 3: Switch
    - mixture of hub and bridge. keeps track os mac addresses attached to each of its ports



Lecture 3 - Firewalls and Intrusion Prevention Systems
Reject and notify vs Discard and not notify:

Design Goals

- single choke point: can allow for offering other service: IPSec, Auditing, NAT, etc
- authorized traffic only

Types:

1) Packet Filtering: apply a set of rules to each individual incoming / outgoing packet

- **Two default policies:**
    a) Permissive: let every packet through
    b) Restrictive: no to all

- **Packet filtering characteristics:**
    a) src and dest IP addresses
    b) source and destination transport layer addresses
    c) IP protocol field
    d) interface

- Considered OSI layer 3 solution (TCP / IP internet layer solution)
- Packet Filtering Advantages vs Disadvantages:
    a) Advantages:
        i) simple
        ii) transparent to users
        iii) speed
    b) Disadvantages
        i) complex to maintain
        ii) does not examine application layer data
        iii) does not support user authentication
        iv) limited logging
        v) susceptible to certain TCP / IP protocol attacks
- **Attacks**
    a) Stateful inspection
        i) TCP ACK scan attack
            (1) find an open port on a network protected by a packet filter
            (2) send a packet with the ACK bit set, without prior 2 steps of TCP 3 way handshake
            (3) no response / unreachable -> filtered
            (4) RST -> not filtered, open port
        ii) Firewall attack
            (1) attacker must know:
                (a) IP address of firewall

(b) IP address of one system on inside of network

(2) to check port, attacker sends packet to known IP address on inside firewall. TTL field set to x + 1

(a) no response: if firewall does not let traffic through on port p

(b) open port: time exceeded message

- **Limitations and weaknesses** of packet filtering:
  a) Lack of consideration for any higher-layer context
  b) stateless: rules applied to individual packets
  c) filter has to allow for incoming traffic on high number of ports

- **Stateful Filter**
  a) Use state table (stateful inspection firewall)
    i) state information is only kept while session is alive
  b) Non-stateful protocols
    i) UDP / DNS / ICMP can use a timer, but costly
  c) Advantages:
    i) do not have to open a large range of ports to allow inbound communication
    ii) Can prevent DoS attacks better than packet filtering approach
  d) Disadvantages
    i) complex
    ii) does not examine application layer
    iii) no user authentication
    iv) not all protocols have stateful information
    v) more overhead
    vi) more stringent control over security than packet filtering

- **Application Level Gateway**
  a) Proxy that intercepts traffic to / from application (server) and inspect it first
  b) Advantages:
    i) all network layer info can be used - can be used to monitor and filter the data, as well as blocking it
    ii) User authentication can be enforced
    iii) Can provide detailed logs
  c) Disadvantages:
    i) may need separate proxy for each application to be protected
    ii) not all applications used supported
    iii) process traffic in software
    iv) performance overheads
    v) issues with encrypted software

- **Circuit Level Gateway (proxy)**

a) stand alone system, or specialized function as part of application level gateway
b) two transport layer connections, one on each side of communication
c) relays transport layer segments from one end to another without examining contents
d) SOCKS: socket secure
e) layer 5 (Transport layer) ; TCP port 1080 ; protocol manages both TCP and UDP
f) Offers user authentication

- Bastian Host - specialized computer deliberately exposed on a public network
    a) runs secure version of OS
    b) only install essential services
    c) require additional user authentication
    d) only allow access to specific host systems

- **Host-Based / Personal Firewall**
    a) can be tailored to the host (typically software module)
    b) independent of network topology (both internal and external based attacks must go through it)
    c) typically used with stand alone firewalls as an additional layer of defence

Locations and Configurations

DMZ

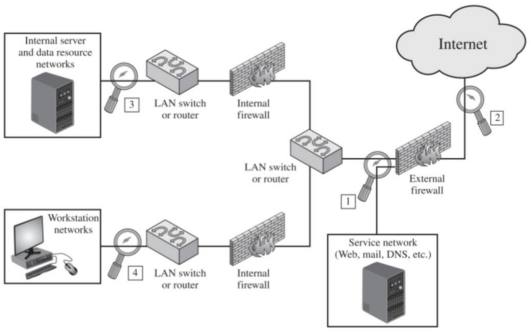
- segment of network for public services
    - includes mail, web, and DNS
- deploy multiple firewalls with different stringent filtering capabilities to protect DMZ and the rest of the network

VPN

- Provides outside access over public / insecure channels
- security protocol at IP level: IPsec

Distributed FWs (slide 14)

- **Host-based, or Host-resident FW's**
- **Screening Routers:** with stateless or full packet filtering
- **Single bastion inline:** with stateful filters and / or application proxies
- **Single bastion T:** same as single bastian inline, but has a third DMZ network interface
- **Double bastion inline:** DMZ sandwiched between two bastion firewalls
- **Double bastion T:**



- **Distributed:** vulnerable?

IPS: Intrusion Prevention Systems

- Host-Based IPS (HIPS): can provide end-point protection using
  - signature-based detection techniques
  - anomaly-based detection techniques
  - sandbox approach
  - **Techniques to identify malicious packets:**
    - System calls
    - File system access
    - System registry settings
    - Hos input / output

- **Network-Based IPS** (NIPS):
  - signature-based detection techniques
  - anomaly-based detection techniques
  - **Techniques to identify malicious packets:**
    - pattern matching
    - stateful matching
    - protocol anomaly
    - traffic anomaly
    - statistical anomaly
- Hybrid IPS

Lecture 4

Availability: focuses on preserving authorized access

- more nuanced

Confidentiality and integrity: focus on preventing unauthorized access / modification

- tends to be binary

Categories of typical attacks include:

- **Network-based:** vast majority of traffic directed at the target server is malicious, generated directly or indirectly by the attacker. Overwhelms and denies legit traffic access to server.

- **Resource-based:** aims to overload or crash its network handling software (SYN spoofing attack)
- **Application-specific:** targets application resources (slowloris)

- **Design requirements of attack**
    - attacks as effective as possible and hard to detect
    - use as little resources as possible
    - attacker not impacted by attack

Network Based:

- **Flooding-** direct as much traffic as possible toward the target
    - **ICMP** - ping flood using ICMP echo request packets
        - send an abnormally large number of pings at target in order to overwhelm services
        - attacker must have at least as large bandwidth capacity as target'
        - impacts attackers resources
        - attacker can be easily identified
        - target may limit the number of ping requests from one source
        - use spoofed addresses to increase effectiveness
        - **reflector attack**
            - may use normal systems as intermediaries
        - **amplifier attack**
            - variant of reflector that employees large number of intermediaries
        - smurf attack
            - variant of ping flood attack
            - sends broadcast ECHO request to network with victim's return network
            - victim is saturated with echo replies (icmp)
        - Fraggle
            - very similar to smurf attack
            - uses spoofed UDP instead of ICMP
        - **DNS Amplification Attack**
            - 60 byte UDP DNS request up to 512 - 4000 byte response
            - creates a series of DNS requests containing the spoofed source address of the target system, and sends to DNS servers
            - may use recursive DNS name servers
            - **Countermeasures:**
                - IP address based authorization
                - incoming interface based selection ?
                - use local caching nameserver
                - use signed queries to authenticate clients
                - do not offer recursive service to external networks
                - prevent address spoofing

    - **UDP** - UDP echo attack, sending UDP packets to the diagnostic echo service
        - ■
    - TCP - use TCP packets with as large payload as possible

Resource Based Attacks

SYN Flood

- takes advantage of 3 way handshake
- starts with target receiving stream of spoofed TCP SYNs
- target starts half-open connections, as per requests
- attacker never completes the connection
- uses comparatively low traffic , as compared to flooding attacks

SYN Cookies

- cookies can replace the random server sequence number returned to the client
    - typically is a function of source addr, source port, dest addr, coarse time, and server secret
    - cookies are unforgeable and tamper-proof
    - server will establish connection only if cookie received is identical to recomputed cookie
- Disadvantages:
    - requires some computational resource
    - method blocks certain TCP extensions
    - not enabled by default

Teardrop Attack

- crash from offsets in packets overlapping

SIP Flood

- Force execution of application related, resource consuming operations

HTTP Flood

- attack sends seemingly legit HTTP GET or POST requests
    - web server responds
- Countermeasures:
    - use challenge request such as captcha to identify requests from a bot

Slowloris

- attacker opens multiple connections and send multiple partial HTTP requests to the victim
- victim server will wait for the attacker to complete HTTP request header
- **Countermeasure:**
    - provisioning more resources to the http server

    - using proxies

Countermeasures:

- resource consumption policies
- provision adequate resource backups
- turn off directed broadcasts
- deploy source address anti-spoof filters

Lecture 5

- **Intrusion detection:** process of monitoring events occurring on network and analysing them for signs of possible incidents which are violations of policies
    - Design considerations:
        - what to monitor
        - where to do the monitoring
        - how to analyze collected data

Components

- **Sensors:** responsible for collecting data
- **Analyzers:** analyze sensor's data to determine if an intrusion has occurred
- **User interface:** provide input / output to IDS

Design Goals

- Detect a wide variety of intrusions
- Detect intrusions in a timely fashion
- Present analysis in easy to understand format
- Be accurate

- False positives: authorized user identified as intruder
- False negatives: intruder not identified as intruder

Base Rate Fallacy

- TP is low (compared to the actual number of intrusions) - a false sense of security
- FP is high (compared ot actual number of intrusions) - warnings may be ignored

Requirements

- Run continually
- Impose minimal overhead
- Allow for dynamic configuration
- Be scalable
- Provide graceful degradation of service

Common Detection Methodologies

- **Signature Based Detection:** study and analyze past attacks, and use that knowledge / patterns to detect incoming attacks
    - Advantages:
        - simple - only need to compare against known attacks / patterns
        - low cost - in terms of time and resource use
    - Disadvantages:
        - Requires a large signature set to reduce false positives
        - cannot detect new zero-day attacks / variants of known attacks / or those using evasion techniques
        - typically lack ability to remember previous events when processing the current event
- **Anomaly Detection:** study and analyze the 'normal' behaviour of users and systems, and use deviation from that behaviour as indication of attack
    - Advantages:
        - many attributes can be used to model 'normal' behaviour
        - can be very effective at detecting previously unknown attacks
    - Disadvantages:
        - need dynamic profiles
        - malicious activity may become part of profile
        - may produce FP's
        - complex computing activities may become part of profile
        - depending on the type used, may initially require large computational time and resources

    - **Types of Anomaly Detection**
        - **Threshold Metrics:** expects occurrence of particular event to be in a given range
        - **Statistical:** analyze behaviour using univariate, multivariate, or time-series models of observed behaviour
        - **Knowledge based:** based on set of rules that model legitimate behaviour
        - **Machine learning:** automatically determine suitable classification model from training data using data mining techniques
            - **Advantages:**
                - flexible
                - adaptable
                - captures interdependencies between observed metrics
            - **Disadvantages:**
                - need rich training set
                - high resource
                - dependent on assumption about accepted behaviour
    - Placement
        - **HIDS** (host based detection system) - what should they log?
            - system call traces

            - audit records
            - file integrity checksums
            - registry access
        - **Distributed HIDS**
            - in centralized architecture, may create a bottleneck, and possible major point of attack

- NIDS (network based intrusion detection)
    - Sensors are available in two formats:
        - **Appliances**
            - specialized hardware and sensor software. Typically have a security hardened OS, with no direct network access
        - **Software Only**
            - can be installed on any, or customized OS
    - Sensor types:
        - **Inline sensor:** network must pass through sensor
        - **Passive sensor:** monitors copy of network traffic
    - **NIDS Data Sources** - collect information from different layers of network stack
        - **Application layer:** DHCP, DNS, HTTP, FTP, IMAP, SMTP, POP
        - **Transport layer:** TCP, UDP, TCP specific attacks such as SYN floods
        - **Network layer info:** IPv4 / IPv6 / ICMP / IGMP
- Hybrid IDS

Exchange Formats:

- Intrusion detection message exchange requirements
- The intrusion detection message exchange format
- The intrusion detection exchange protocol

Honeypots

- Decoy systems designed to:
    - divert an attacker from accessing critical systems
    - collect information about the attackers activity
    - encourage attacked to stay on system long enough for administrators to respond
- **Two kinds:**
    - low interaction honeypot: not a full replica
    - high interaction honeypot: full fledged, real system replica

Lab Notes

Lab 3

netstat -na

- check status of queue, ie half opened connections associated with a listening port
- state of these connections is **SYN-RECV**
- if three way handshake is finished, state is **ESTABLISHED**