Network Security Notes Exam 1

Wednesday, October 8, 2025 3:27 PM

Module 1 Networking basics

networking: transporting + exchanging data btw nodes over a shared medium in an information system
- nodes - physical networked devices which checks for identification (IP address) to grant access. Connect over a link (cables, fiberoptic, bluetooth)
  - examples: modems, PCs, printers

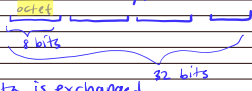
email, video, msgs, file sharing

Types of Area Networks: personal, local, wide, wireless, campus, metropolitan, storage, system, passive optical local, enterprise private, virtual private, home

IP addresses: IPv4 IPV6 3 unique identifiers

either static or dynamic
- static: never change
- dynamic: changes

8 bits = 1 byte — in octet, number is expressed in binary



TCP/IP: specifies how data is exchanged

4) (Application) — HTTP/s, TLS, DNS allows user to interact w/ the application (SNMP = simple network Management Protocol: manages devices on the internet, Telnet = connection btw local + remote computer)
3) (Transport) — TCP/UDP reliability, flow control + correction of data (TCP = connection-oriented (email, file sharing) UDP = connectionless (videos))
2) (Internet) — IPv4, IPv6 deals w/ IP packets + addresses - uses Routers: forwards data packets btw networks) uses an internal routing table
1) (Network) — Ethernet, WLAN defines how data should be sent physically (MAC = Media Access Control = hardware IP; NIC = network interface controller = holds MAC address)

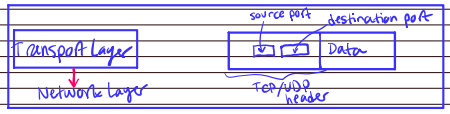
TCP - defines how apps communicate across network (down data)
IP = directs each packet to the correct destination

packets:

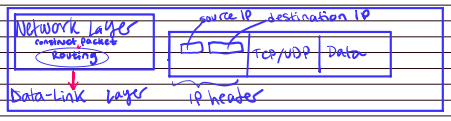
How a packet is constructed:

Application:

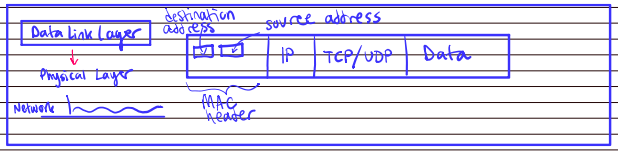
Transport:



Internet:



Link Layer:



PACKET SPOOFING

- The attacker creates packets, changing the source IP address to impersonate a different computer system, disguise the sender's identity or both.

1. **man-in-the-middle** (MiTM) attack is when the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

PACKET SPOOFING — DDOS

2. An attacker using IP spoofing pings the server repeatedly, using the target's IP address as the source. The server thinks the target is making legitimate requests and overwhelms the target with responses, causing it to malfunction.

How IP spoofing works in denial-of-service attacks

How To detect Packet Spoofing: Packet filtering systems = these are located in routers + firewalls
→ detect inconsistencies btw IP address contained on the ACL (Access Control List)

2 types of Packet filtering

1. **Ingress filtering** examines incoming packets to see if the source IP header matches a permitted source address. It rejects any that don't match or that display other suspicious behavior.
2. **Egress filtering** examines outgoing IT scans for source IP addresses that don't match those on the company's network. This approach prevents insiders from launching an IP spoofing attack.

How to protect against Packet Spoofing:
- ~ use strong authentication
- ~ make ACL of IP's
- ~ use packet filtering
- ~ Internet encryption protocols - hides IP addresses
- ~ make software + monitor networks

Packet Sniffing: observes msgs being sent + received by applications + protocols (never sends packets to itself) looks at TCP, UDP, ICMP, etc.

GUI: Wireshark: captures packets from a network connection, filtering packets, and see the very middle of a network packet

command line: TCPdump

Scapy: implement your own sniffing tools

Module 2 Cyber Kill Chain = 7 steps

enhances visibility into an attack. enriches an analyst's understanding of an adversary's tactics

1) Reconnaissance: harvesting email addresses, conference info, etc
2) Weaponization: explore + backdoor become a single deliverable payload
3) Delivery: delivering weaponized bundle to the victim (via email, web, USB, etc.)
4) Exploitation: exploiting a vulnerability to execute code on victim's system
5) Installation: installing malware / spyware / ransomware onto asset
6) Command & Control: command channel for remote manipulation of victim
7) Actions on Objectives: w/ "Hands on keyboard" access, intruders accomplish original goal.

- Reconnaissance = Planning Phase for attackers

Passive Reconnaissance: rely on public knowledge, w/o direct engagement (DNS records on DNS servers, etc.) OSINT

Active Reconnaissance: direct engagement w/ target (ex. connecting to HTTP, FTP, SMTP server, social engineering); illegal

Target Retailer Example: stole financial + personal info and put it on a server in Eastern Europe

Reconnaissance: stole credentials from Fazio Mechanical Services through phishing
- attacker did simple google search to access Target's 3rd party vendors fix: limit public information

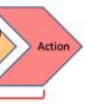
Weaponization: attacker created an attack vector: (remote access malware, ransomware, virus, worm) to exploit vulnerability
- set up backdoors so they can continue to access system fix: couldve used a real-time monitoring + anti-malware

- Delivery: intruder launches attack; send victim stuff to your software, not the free version for individual use
  attack. Attacker sent infected emails to Fazio fix: train staff to report + delete spam email
- exploitation: malicious code is injected + executed on victim's system; lateral attacker movement to identify weak points
  - RAM scraping malware started recording millions of card swipes
    stored it. fix: block effect of malware on servers by deleting it or not making it automatic
- installation: malware is installed on victim's system; this is a turning point. attacker got access to Fazio's systems - used default acct. name
  Fix: remove default accounts
- Command & Control: uses malware to get remote control of Target's internal network for 1 month + and compromised servers w/ exfiltration malware
  attackers were able communicate w/ outside internet + target's cardholder network
  fix: analyze location of credentialled users in network

Packet Spoofing :

- **Ingress filtering** examines **incoming** packets to see if the source IP header matches a permitted source address. It rejects any that don't match or that display other suspicious behavior.
- **Egress filtering** examines **outgoing** IP scans for source IP addresses that don't match those on the company's network. This approach prevents insiders from launching an IP spoofing attack.

unities



vided by its
the attackers'
s to steal as
records.

stored it. fix: block effect of malware on servers by deleting it or not making it automatic

-Installation: malware is installed on victim's system; this is a turning point. attacker get access to Fazio's systems - used default acct. name. Fix: remove default accounts

-Command & Control: uses malware to get remote control of Target's internal network for 1 month + and compromised servers w/ exfiltration malware

attackers were able communicate w/ outside internet + target's cardholder network

fix: analyze location of credentialled users in network

use strong firewalls btw Target's internal system + outside internet

also blacklisted common command & control connections.

-actions on objectives: sensitive data was transmitted to the outside Russian server - plain-text via FTP over 2 wks.

fix: whitelist could've dismissed connections btw USA + Russian servers, while allowing approved FTP logins

-Target's FireEye software found the malware + destination of servers

fix: act on info found in FireEye

Weaknesses in the Cyber Kill Chain: • limited attack detection profile

• no insider threat detection - doesn't cover SQL injection, cross-site scripting, + zero-day vulnerabilities

• lack of flexibility - attackers will not follow all 7 steps, or in order.

deepfake phishing, AI-driven attacks, ransomware campaigns

Module 3 - Reconnaissance: info-gathering

Passive Recon & Tools:

Reconnaissance: info-gathering stage of ethical hacking

whois: public database that houses the info

when a domain name is registered.

whois server listens on TCP port 43 for incoming requests

Syntax: whois domainName ← used for finding

gives a bunch of info about someone/something :. get some information about them + attack

new attack surfaces

Syntax: nslookup domainName

nslookup OPTIONS DOMAIN_NAME SERVER

OPTIONS = contains query type is shown in the table in the next slide

you can use A for IPv4

AAAA for IPv6

DOMAIN_NAME = name of website you're looking at

SERVER: DNS server you want to query

dig: domain information groper

Syntax: dig domainName

dig SERVER DOMAIN_NAME TYPE

you can add extra parameters to specify which DNS server you want to query as well as the type

DNS Dumpster can find subdomains and if they exist — nslookup + dig cannot.

DNS Dumpster is a free domain research tool which helps discover hosts related to a domain

ex. tryhackme.com

wiki.tryhackme.com

webmail.tryhackme.com

cannot see these without DNS dumpster

Shodan.io is a search engine

Active Reconnaissance & Tools: ctrl + Shift + I → devTools: lets you see what received + exchanged w/ the remote server

web browser tools: FoxyProxy: quickly change proxy server

User Agent Switcher + Manager: pretend to be accessing the webpage from a different OS or browser

Wappalyzer: see technology used

Ping = primary TCP/IP command used to troubleshoot connectivity reachability + name resolution

packet sent → packet received

Syntax: ping MACHINE_IP

ping hostname

to specify # of packets: syntax: ping -c 10 MACHINE_IP ← sends only 10 packets

(if Linux, and not specify #, ctrl+C to stop)

if no ping back, pc is booting or OS crashed, is unplugged, or faulty network device across the path

-firewall blocks (MS Windows firewall blocks pings by default)

Traceroute = traces route taken by the packets from your system to another host.

purpose: as a packet hops (traverses) between routers, to get those IP addresses

reveals # of routers btw 2 systems

Syntax: traceroute MACHINE_IP Linux + Mac ? each line in output represents 1 router/hop

tracert MACHINE_IP Windows

if I'm in instagram.com and I did "traceroute instagram.com" I would get exactly 1 hop. 1 hop if @ yself

Telnet: before SSH, Teletype Network. All data sent as cleartext — hence a securit vulnerability

purpose: connects to a service that runs TCP and access its banner

Syntax: telnet MACHINE_IP PORT

telnet 50.74.239.202 80 } hydra web server, on Port 80 (HTTP)

Need to ask for a page: GET / HTTP/1.1 } gives home page

NetCat = supports BOTH UDP + TCP - functions as a client

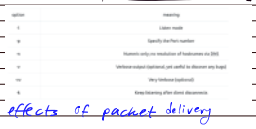
that connects to a listening port

- acts like a server that listens on a chosen port

Syntax: nc MACHINE_IP port

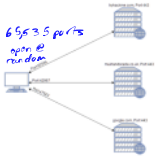
GET /page.html HTTP/1.1 } gives us a specific page

Syntax: to have netcat act like a server: nc -lvnp PORT_NUMBER



Module 4 NMap = Given an IP, which services are running on it, ports constrict to receive a connection

port scanning



NMap will connect to each port of target in turn.

- network scanner used to find hosts and services by seeing the effects of packet delivery

Nmap commands:

nmap -p 80 X.X.X.X most common port scan

nmap --top-ports 20 50.74.239.202

amt of most common ports — host

nmap -iL filename.txt scan hosts from a file

nmap -oN fileScanResults.txt ipAddress save scan results on an IP to a file

nmap -A -T4 ipAddress

-A: OS detect; -T4: timing template (Paranoid, Stealth, etc.)

nmap -sV ipAddress detect service/daemon versions

nmap -sU ipAddress } UDP scanning

nmap -sT ipAddress } TCP scanning

Nmap Scripting Engine (NSE):

is a scripting engine which allows users to use a pre-defined set of scripts, or write your own, using Lua scripting language

nmap -Pn --script vuln ipAddress ← run a full vulnerability test against the target

nmap -sV --script=http-malware-host ipAddress ← a script to detect malware

Module 5 Firewalls

hardware, software, software-as-a-service (SAAS)

public/private cloud

Firewalls filter traffic flowing through its ports

How a Firewall Works

nmap -Pn --script vuln ipAddress ← run a full vulnerability test against the target
nmap -sV --script=http-malware-host ipAddress ← script to detect malware

Module 5 Firewalls

hardware, software, software-as-a-service (SAAS)
public/private cloud

Firewalls filter traffic flowing through its ports
network-based: in a hardware appliance or built into a router installed btw LAN & internet
eg SoHo (Small office Home Office) → can't help if bad traffic coming from inside

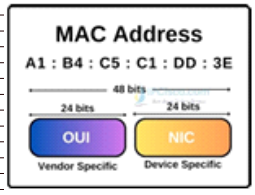
host-based: software firewall installed on a "host" that provides firewall services to just that machine

Whitelisting: instead of blocking specific addresses/devices, allows only SPECIFIC addresses/devices to access data/networks

Benefits	disadvantages
+ very secure approach to data security	- difficult to implement - need a lot of info updates
only allow good ppl in	- not flexible
+ good for lists of bad ppl	- IP address spoofing to lose as someone good

Greylisting = temporarily blocking items from system until analyzing further
→ used in email securing to combat spam ⇒ reject all emails, then looking through and removing the good ones out of the spam filter

Media Access Control (MAC) Filtering
every device that connects to your device has a MAC address ~ you can limit access through the physical hardware address
↳ allow/disallow access for particular MAC addresses on your network



ACL = access control list
→ determines who is allowed/denied in firewall

Syntax:
access-list 10 deny 10.11.12.0 0.0.0.255 ← doesn't allow any flow, just block
(access-list: create an ACL; 10: its number; deny: actual rule; 10.11.12.0 0.0.0.255: we want firewall to apply)

access-list 10 permit any ← gets flow going

TYPES OF FIREWALLS 18

STATELESS FIREWALL

- ACLs are considered **stateless firewalls**. Stateless firewalls only focus on **individual packets** using preset rules to filter traffic.
- Although rules within ACLs look a little different depending on what hardware you're using, they generally include the following elements:
  - **Permission** - PERMIT/ALLOW or DENY traffic.
  - **Protocol** - TCP, UDP, etc.
  - **Source** - the source IP address (where packet is from)
  - **Destination** - the destination IP address (where packet is going)
  - **Port or Protocol** - Typically, you'll often see a well-known port such as port **443** for **HTTPS** in a rule. However, some devices support codes such as HTTPS for HTTPS traffic.

TYPES OF FIREWALLS

STATEFUL FIREWALL

- A **stateful firewall** inspects traffic and makes decisions based on the **traffic context or state**.
- It keeps track of established sessions, inspects traffic based on its state within a session, and it blocks traffic that isn't part of an established session.
- **Example**: A TCP session starts with a three-way handshake. If a stateful firewall detects TCP traffic without a corresponding three-way handshake, it recognizes this as suspicious traffic and can block it.

- A **web application firewall** (WAF) is a firewall specifically designed to protect a web application.
- A web server hosts the web application, and the WAF is placed ***between*** the web server and web server clients.
- The WAF can be a stand-alone appliance or software added to another device.
- Note that you wouldn't use a WAF in place of a network-based firewall. Instead, it provides **an added layer of protection** for the web application in addition to a network-based firewall.

NEXT GENERATION FIREWALL

- A **next-generation firewall** (NGFW) is an advanced firewall that adds capabilities that aren't available in first-generation or second-generation firewalls.
- The first generation of firewalls were **packet-filtering** firewalls, using stateless firewall rules, and could only allow or block traffic after evaluating individual packets.
- The second generation of firewalls added in **stateful firewall** rules. This allows firewalls to evaluate traffic based on its session state.

- An NGFW performs **deep-packet inspection**, adding application-level inspection as a core feature.
- The NGFW is aware of common application protocols used on the Internet, such as FTP and HTTP.
- By using deep-packet inspection, the NGFW can identify application commands and detect potentially malicious traffic. This allows it to apply **content filtering** and **URL filtering**.

Capability	Traditional firewall	Next generation firewall	Advantages of next generation firewall
Inspection	Stateless	Stateful	Blocks traffic that deviates from expected norm compared to established connections
Visibility	Rudimentary, only lower TCP/IP layers	Deep, includes all TCP/IP layers	Enables more granular and robust analysis of traffic
Services	Basic	Comprehensive	Includes UTM services such as antivirus, content filtering, IDS/IPS, and logging in addition to packet filtering
Protection	Limited	Enhanced	Identifies, prevents, and reports a broader variety of attacks

- The default firewall configuration tool for Ubuntu is **Uncomplicated Firewall (UFW)**. Developed to ease `iptables` firewall configuration, `ufw` provides a user friendly way to create an IPv4 or IPv6 host-based firewall.