DO NOT REMOVE EXISTING POINTS. INSTEAD, ADD ANY MISSING OR RELATED FACTS TO THE RESPECTIVE POINT/HEADING.

Editing is completed. Enjoy.

Possible Structure of 4 questions of the paper - Just an opinion ;)

1. Basics (Models, Protocols, Basics of Security & Networking, Social Engineering, Malware,Cyber Attacks and etc)

2. DoS attacks related shit (Firewall,Packet capturing, Attacks and Defenses, Session Hijacking, Honeypots)

3. IDS related shit (IDS, Snort)

4. Forensics (Computer and Network Forensics)

Check the last section for some simple sample questions to revise and remember key points.

Table of Contents

Questions 33

AAA

- Authentication – Allow people who are allowed
- Authorization – Allow people to access allowed resources/ do tasks
- Accounting – Logging activities of the people

Authentication

- Allow only the people who are allowed to access the system
- 3 factors
    - Something you know - Passwords
        - Popular, simple, well known by many
        - Techniques -
            - Encryption and Protocols
            - Kerberos
            - Radius Server with AAA (Authentication, Authorization, Accounting)
        - Weakness –
            - Social Engineering
            - Interception – Packet Sniffing
            - Replay
            - Impersonation – Spoofed web sites
            - Brute Force – Cloud eg ec2
            - Password Leakage
            - Keylogging
            - Rainbow tables

    - Something you are – Biometrics
        - Fingerprints, Retinas scan, Voice Recognition, Face Scan
    - Something you have – Tokens
        - Cards (magnetic or wireless)

- MAC (Mandatory Access Control) and DAC (Discretionary Access Control)
    1. MAC provides access based on levels while DAC provides access based on identity
    2. DAC is more labor intensive than MAC
    3. DAC is more flexible than MAC
    4. MAC access can only be changed by admins while DAC access can be provided by other users

Threats

- Vulnerability – A weakness that could be triggered accidentally or exploited intentionally to cause security breach (Raj's inability to not to talk to girls)
- Threat – The source that triggers the vulnerability (Penny and other hot girls)
- Risk – If vulnerability is triggered, what is the impact (Not being able to say things to women and causing to lose being dated or even lose jobs and etc)
- Control – A system or procedure to mitigate the risk (Raj drinking alcohol to talk to girls)

Sources of Threats

- Natural Disasters
- External Threats
    - Crackers
    - Script Kiddies
    - Thieves
    - Terrorists
    - War

- Malicious Insider Threat
- Structured & Targeted – Criminal Groups
- Environment – Failure in the environment
- Legal and Commercial Threats

Social Engineering

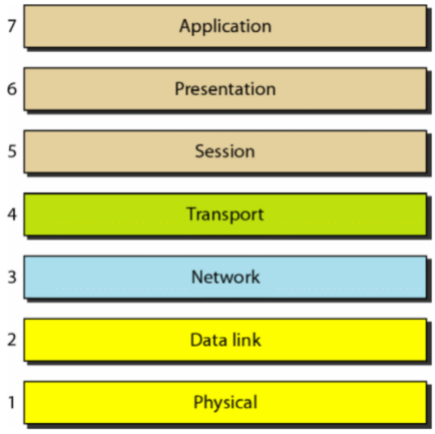
- Impersonation
- Dumpster Diving – The attacker needs some information
- Shoulder Surfing
- Tailgating (piggybacking) - Entering a secure area without authorization by following close behind the person that has been allowed to open the door or checkpoint
- Phishing - A combination of social engineering and spoofing (disguising one computer resource as another/ Spoof website). It is an attempt to get sensitive information for malicious reasons by disguising as a trustworthy entity. These are not targeted. More like you use the hook to catch whatever the fish that gets caught)
- Vishing / SMiShing - A phishing attack conducted through a voice channel (telephone or VoIP for instance)
- Spear Phishing / Whaling –
    - Email might show that the attacker knows
        - The recipient's full name
        - Job title
        - Telephone number or other details that help to convince the target that the communication is genuine.
    - A spear phishing attack directed specifically against upper levels of management in the organization (CEOs and other "Big beasts") is sometimes called whaling.
    - This is a targeted attack unlike phishing.
- Pharming –
    - Redirecting users from a legitimate website to a malicious one

Malware

- A catch-all term to describe –
    - Malicious software threats and
    - Social engineering tools designed to vandalize or compromise computer systems
- Computer Virus
    - Boot sector viruses – They attack boot sector info, partition tables and foke systems
    - Program viruses - Attached to other programs and gets executed when application is executed
    - Script viruses - Web related. They attack the interpreter
    - Macro viruses - Microsoft office related attacks
    - Multipartite viruses - Use boot sector & executable file infection methods
- Worms – Memory Resident ,replicates over network resources, self contained, can install backdoors
- Cell Phone Viruses
- Logic Bombs - Waits for a pre configured time or an event (Like a time bomb)
- Fork Bomb – Spawns a large number of processes. Could lead to resource starvation.
- Trojan – A program that pretends to be something else, functions as backdoor apps
- Spyware - A program that monitors user activity and sends information to someone else
- Adware – Software or browser plugins that display ads
- Rootkits – They modify the system files in a way its presence is undetectable (Kernel level)
- Backdoors - This is something which allows entry to a system, completely disregarding any security on the front door.
- Virus Alert Hoaxes
- Spam
- Spim and Spit – Same as Spam distributed through IM and VoIP.

Network

- Network – A set of technologies that connects computers
- Internet – A network of computer networks
- Protocol - A set of rules and formats that govern the communication between communicating peers
- Layer - Modularization of a complex system based on high level responsibilities.
- OSI – Open System Interconnection Model

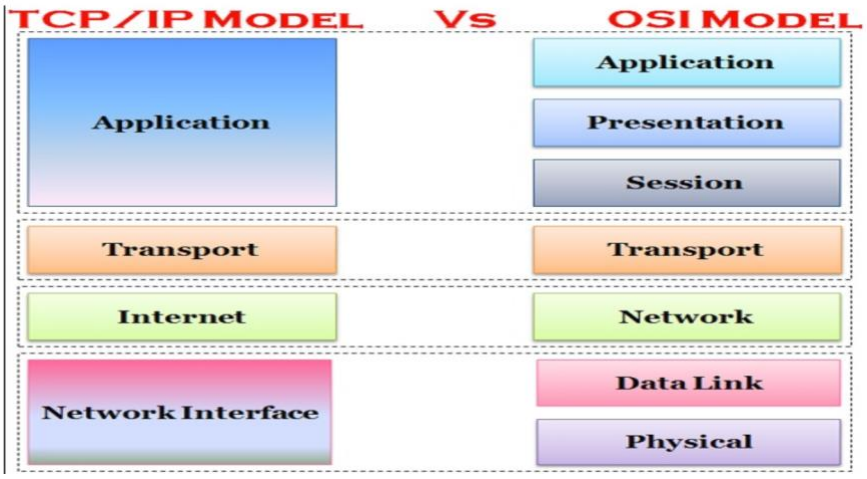


  - **P**lease **D**o **N**ot **T**ell **S**ecret **P**asswords **A**nymore
  - Responsibilities
    - Physical Layer – Movements of individual bits from one node to next
    - Data Link – Moving frames from one node to another
    - Network – Delivery of individual packets from the source host to the destination host
    - Transport – Delivery of a message from one process to another
    - Session – Dialog control and synchronization
    - Presentation – Presents data
    - Application – Providing services to the user

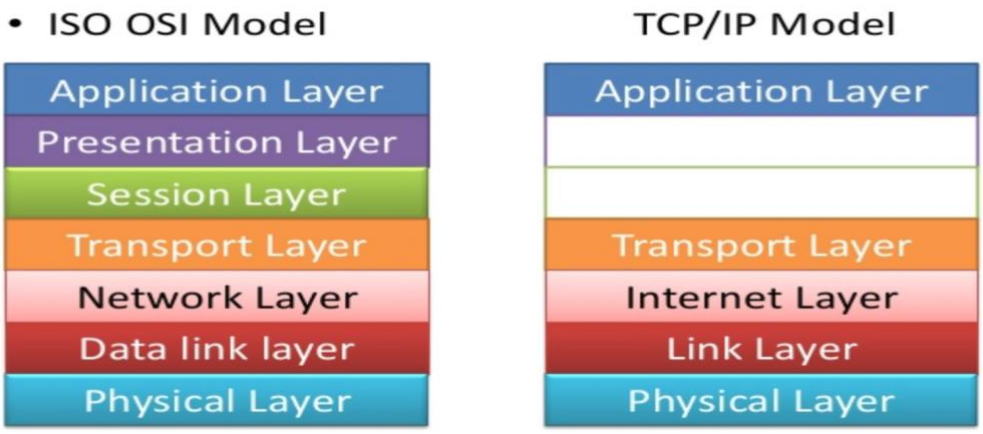
OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent. Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY		Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed). Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports). Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control. Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address). Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end). Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

- TCP/IP Model
  - This is for the internet. Not for a network.
  - Networks are also identified using logical addresses just like individual ones.
  - Application – App-App / Web browser – Web browser communication
  - Transport – Port - Port / Process – Process communication
  - Internet – Host – Host communication
  - Physical - I/O from/to the physical link



4 LAYER



5 LAYER

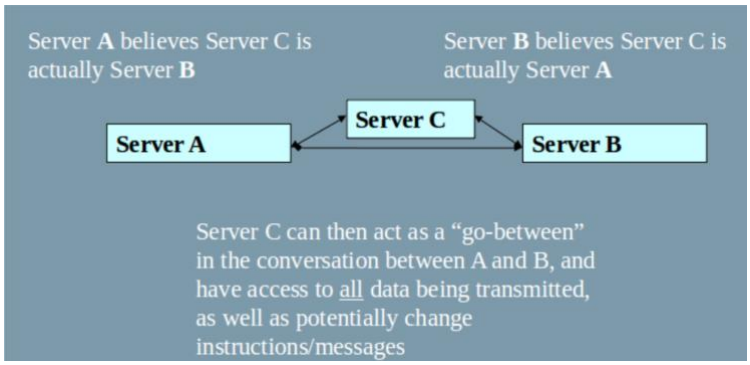
- Fiver or four layers depending on which continent the book is written in.
- On the internet every network packet has the following 5 layer structure
    - Application: HTTP
    - Transport – UDP (Won't make sure every bit is transferred) & TCP (makes sure)
    - Network – IP
    - Link – Ethernet or WIFI
    - Physical – Ethernet Cable

Security & CIA

- Goals
    - Confidentiality
    - Integrity
    - Availability
- Protect the **Confidentiality** of data
- Preserve the **Integrity** of data
- Promote the **Availability** of data for authorized user
- Confidentiality -
    - Keep data and communication secret
    - It is the ability to hide information from those people unauthorised to view it

- Integrity -
    - Must make sure the message received should be the original message
- Availability -
    - Keeps data and resources available for authorized use, especially during tragic situations
    - It can be disrupted in 3 ways
        - Denial of Service (DoS) – Due to international attacks of undiscovered flaws in implementation
        - Loss of Information – It can happen due to natural disasters
        - Equipment Failures
- Security – Is ensuring that only authorized people can perform authorized actions, without interference from others and without risk of data interception
- Everyone is Responsible, should be considered from the beginning rather than an add-on
- Types of Intruders
    - Amateurs - Not sophisticated. Use resources for their own purposes.
    - Crackers - Access resources without permission. ආතල් එකට කරන උන්. They do it for fun but sometimes for other reasons as well.
    - Career criminal - Planned attacks, financial gain
    - Military - To disable enemies, gain strategic advantage
- Types of attacks
    - Interception - Unauthorized party gets access to an asset (Harms the Confidentiality)
    - Interruption - Asset becomes unusable (lost or destroyed) (Harms the Availability)
    - Modification - Existing asset is changed (Harms the Integrity)
    - Fabrication - Fake asset is planted in the system (Harms the Integrity)
- Passive attacks / Indirect Breaches – An unauthorized party such as a hacker / intruder monitors networks and look for vulnerabilities in a network.
    - Packet sniffing – Anyone listening to the traffic can hear all the noise by setting their NIC into promiscuous mode (monitor mode)
- Active Attacks / Direct Breaches – A hacker attempt to exploit the network in order to make changes to the targets data.

- Password cracking
- Trojan Horse
- Spoofing / Man-in-the-middle (MITM) attacks
  - IP spoofing – Pretending to have the IP address of another machine
  - MITM – Intercepting messages passed from server-server and altering the message in the process



- Back door - This is something which allows entry to a system, completely disregarding any security on the front door.

Defenses

- Packet Sniffing –
  - Use switches or bridges to cut down amount of traffic for a single host
  - Use encryption
  - Use anti-sniff tools to detect machines that are set in promiscuous mode
- Port Scanning –
  - Shut off unused ports
  - Install a Port Sentry - A software that intercepts port connections
- Password Cracking – Change password regularly
- Trojan Horse –
  - Keep a DB of signatures of important apps and regularly check the apps to match the signatures
  - Linux has Tripwire which does this automatically
- IP Spoofing – Ensure to speak with the right host from the start
- MITM – Establish encrypted sessions

Cyber Attack - Stages

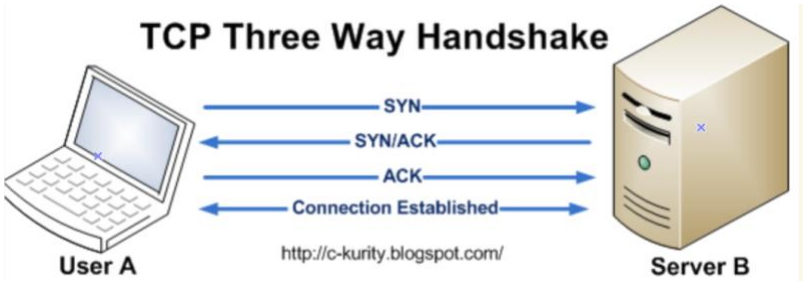
- Reconnaissance (Investigation) – Attackers get information from a variety of factors to understand their victim.
- Scanning – Once the target is identified, next is to identify a weak point that allows the them to gain access.
- Incursion – Attacker breaks into the network, installing malware to systems often without the victim's awareness.
- Capture – With access to the network, attacker stay low to avoid detections. They create a battle plan inside the organization.
- Escalate – They gain access and then escalate. They get privilege access to move freely. Once that happens, the network is owned by the attacker.

Social Engineering

- Sources of Information Gathering
    - From websites
    - Whois
    - Public servers (such as using NMAP)
    - Social Media
    - Public Reports
    - Power of Observation
    - Using Profiling Software (CUPP – Common User Password Profiler, WYD – Who's Your Daddy, Maltego)
- Elicitation – "The subtle extraction of information during an apparently normal and innocent conversation" – By NSA
- Pretexting – The background story, dress, grooming, personality and attitude that make up the character you will be for social engineering audit.

TCP – Transmission Control Protocol

- Provides reliable, ordered and error-checked delivery of a stream of octets (bytes)
- Connection Establishment
    - Uses a 3-way handshake.
    - Passive Open – Before a client attempts to connect with a server, server must first bind to and listen at a port to open it up for connections.
    - Active Open – Once the passive open is established, a client may initiate an active open.
    - 4 possible flags
        - SYN (Synchronization)
        - ACK (Acknowledgement)
        - FIN (Finished)
        - RST (Reset)
    - 3-way handshake
        - **SYN** (Synchronization) – The active open is performed by the client sending a SYN packet to the server.
        - **SYN-ACK** (Synchronize - Acknowledgment) – The server replied with a SYN-ACK (combination of SYN and ACK).
        - **ACK** (Acknowledgment) – Finally the client sends an ACK back to the server.



Attacks

- DoS (Denial of Service) Attacks
    - SYN Flood – Flood server without acknowledging back server's SYN response by initiating multiple new TCP connections from spoofed IP addresses – Cashier at a supermarket being overloaded by multiple customers
    - ICMP (Internet Control Message Protocol) Flood / Ping Flood – Large number of echo requests with spoofed source IP address – Cashier at a supermarket being overloaded by one customer with a large number of items.
    - UDP (User Datagram Protocol) attack – Sends a large number of UDP packets to random ports on a remote host. - Random customers overloading with items to multiple cashiers
- Land Attack – Use the IP address of the victim as source and destination IP address causing it to lock up. Basically, the attacker changes the source host to as the destination host causing victim server to send requests to the server itself.

- Teardrop Attack – Based on fragmentation and reassembly of IP attacks. It crashes the target network device.
- Ping of Death – Based on IP packet size greater than 65535

Firewall

- Firewall - A device that that provides secure connectivity between networks (internal/external)

- It may be a hardware, software or a combination that is used to prevent unauthorized programs or users from accessing the target network/computer

Software vs. Hardware Firewalls

Software Firewall	*Hardware Firewall*
-Protect a single computer -Usually less expensive, easier to configure	-Protect an entire network. -Usually more expensive, harder to configure
Norton Internet Security	Cisco PIX
Mcafee Internet Security	NetScreen
Outpost	WatchGuard
Ms. ISA Server	Check Point

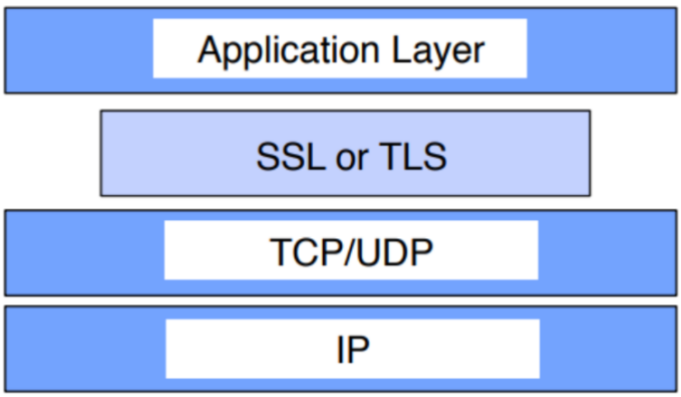
- Firewall Techniques
    - Packet Filter
        - It looks at all packets entering and leaving the network and accepts/rejects it based on user defined rules.
        - It is vulnerable to IP spoofing
    - Application gateway (proxy server)
        - User uses TCP/IP applications such as FTP and Telnet servers.
        - Very effective but can impose a performance decrement.
- Firewall Implementation - IPTables is a package & kernel module for Linux for filtering, network address translation and packet mangling

Packet Capture & Analysis

- **Wireshark** – Used to capture packets and analyze.
- TCP/IP
    - Application Layer- HTTP
        - 4 phases
            - Open Connection

- Request
- Response
- Close

- Basic Authentication
  - Has no cookies
  - Browser cache the credentials for a period of time
  - No standard way to logout
  - No way to customize login experience
  - Insecure since full credentials pass over the wire
- Form Based Authentication
  - Commonly used
  - Login experience can be customized
  - Must be paired with SSL/TLS to secure transactions
  - Uses static HTTP headers with no handshake
  - Server side – WWW-authenticate HTTP header
  - Client side – Authorization header
- SSL/TLS & HTTPS
  - SSL – Secure Sockets Layer protocol
  - TLS – Transport Layer Security protocol



  - All encrypted except for header
  - SSL/TLS is used to add security capabilities to standard HTTP

- HTTP begins with **http://** and used **port 80** by default
- HTTPS begins with **https://** and used **port 443** by default

- Transport Layer
  - **UDP (User Datagram Protocol)**
    - Lightweight and connectionless
    - Small packet size (60% less than TCP) and in header size UDP (8 bytes) & TCP (20 bytes)
    - No connection to create or maintain
    - More control over when data is sent
    - Does not compensate for loss of data
    - Does not deliver or guarantee packet delivery in order
    - Does not check if network is busy
  - **TCP (Transmission Control Protocol)**
    - Reliable and connection based
    - Should negotiate a connection before packets can be sent (3-way handshake)
    - Delivery ACK packets segments are numbered
    - Check **TCP – Transmission Control Protocol** section for 3-way handshake.

Denial of Service (DoS) Attacks

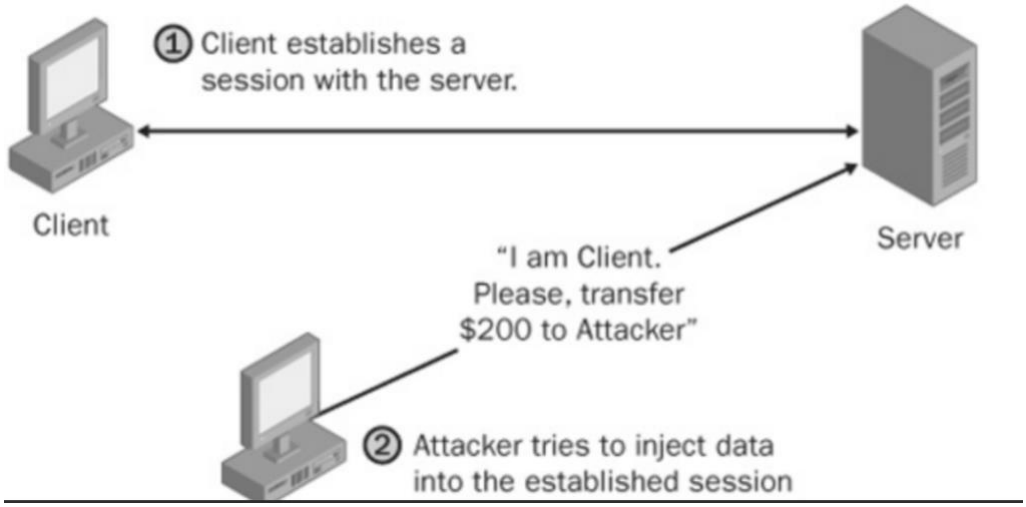
- It is an attempt by an attacker to deny his victim's access to a resource.
- 4 categories
  - Flooding or other network disruption attacks - Attacks the network linkage between systems
  - Resource Starvation Attacks – CPU Starvation, Memory Starvation, Consumption of Disk Storage
  - Disruption of Service – Application level or Host level
  - Physical Attacks
- A DoS attack is all about making a service unavailable to a user.

- Distributed Denial of Service (DDoS) – Same as DoS but amplifies it by using multiple hosts.
- DoS attack uses a more powerful host whereas a DDoS attack would use multiple mid-level hosts to generate enough traffic
- DDoS is harder to detect because it is coming from several IP addresses.
- Protect from SYN Flood –
    - Filtering
    - TCP half open "Time to live"
    - Firewalls and proxies
- Protect from UDP Flood –
    - Limit the rate of ICMP responses
    - Filter out or block malicious UDP packets using Firewalls

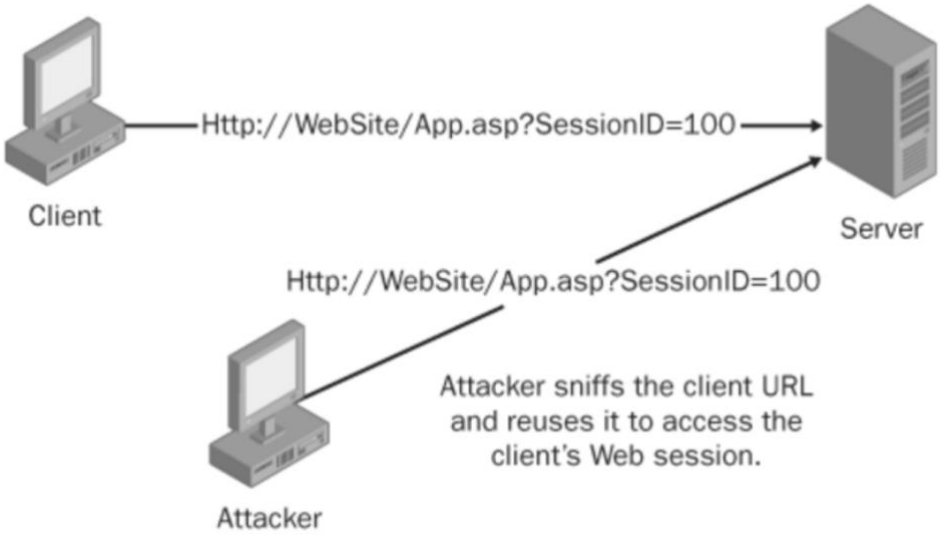
Session Hijacking

- An attacker takes control of or modifies any communication between two hosts.
- Most communications are protected from the beginning at the session setup such as providing credentials but do not **during** the session. Session Hijacking takes advantages of this fact.
- 3 categories
    - MITM
    - Blind Hijacks
    - Session Theft
- MITM –
    - An attacker intercepts all communications between two hosts
    - Protocols that rely on the exchange of public keys to protect communication are often target of MITM.
- Blind Hijack Attack –
    - An attacker can inject data such as malicious commands into those communications

- It is called blind hijacking because the attacker can only inject data into communication stream
- It is time based. Should happen effectively.

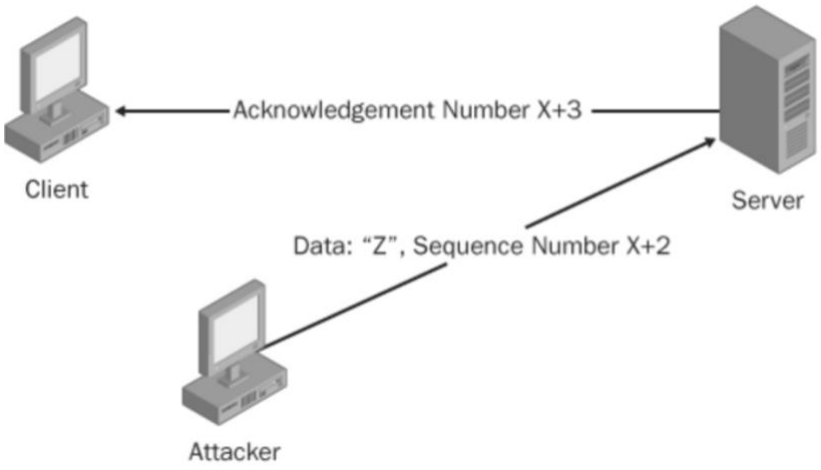


- Session Theft Attacks –
  - The attacker neither intercepts nor injects data into existing communications between two hosts
  - Instead the attacker creates new sessions or utilizes old sessions.
  - It's like getting a used ID and checking whatever happened in the past.



- Above hijacking methods are mostly network level attacks
- Following are transport level hijacking
- Hijacking a TCP session

- The attacker comes at the ACK stage
- The attacker sends an ACK to the server with the proper ACK number as the victim's one should be
- The attacker needs to spoof victim's IP
- Determine the correct sequence number the server is expecting
- Injecting data into the session before the client sends its packet



- Protect from Hijacking in a network level
  - Implement SSL/ TLS, SSH or IPSec (Internet Protocol Security)
  - Encrypt the packet so that the number won't get detected

Honeypots

- An isolated system that can be used as a decoy to attract attackers
- You can learn the patterns of the attackers and protect their actual hosts
- Distracts attackers from valid network resources
- Like the movie White Chicks

Actual Hosts Honeypots

- Collection of honeypots is a Honeynet.
- Shutdown the Honeypot machine if the attacker gets to know about it. Pull the plug
- Advantages
    - Discourage Attacks
    - Divert Attackers efforts
    - Educate - Can be used to study and collect attack profile data.
- It has its own firewall, router and etc., to look legitimate.
- The honeypot manufacturer is not responsible for the honeypots being compromised. The data owner is responsible if they don't pull the plug before the honeypot gets detected and gets compromised.
- **Tripwire** monitors file changes on a machine and can be used to warn if a honeypot machine is compromised.

IDS – Intrusion Detection Systems

- An application that detects attacks against a single computer or a network.
- Issues alerts in real time, logs the attacks and can be used on a single machine (HIDS), or as a part of a network (NIDS).
- Signature Detection –
    - Matches network traffic against a known list of bad signatures.
    - Examines packet header. Not the content.
- NIDS (Network Intrusion Detection System) –
    - NIC runs in promiscuous Mode
    - Snort is an NIDS
- HIDS (Host Intrusion Detection System) –
    - Operates only on the host
    - NIC not in promiscuous mode
    - Can check integrity of files on the system
    - Snort can be run on a single host
- IDS principles

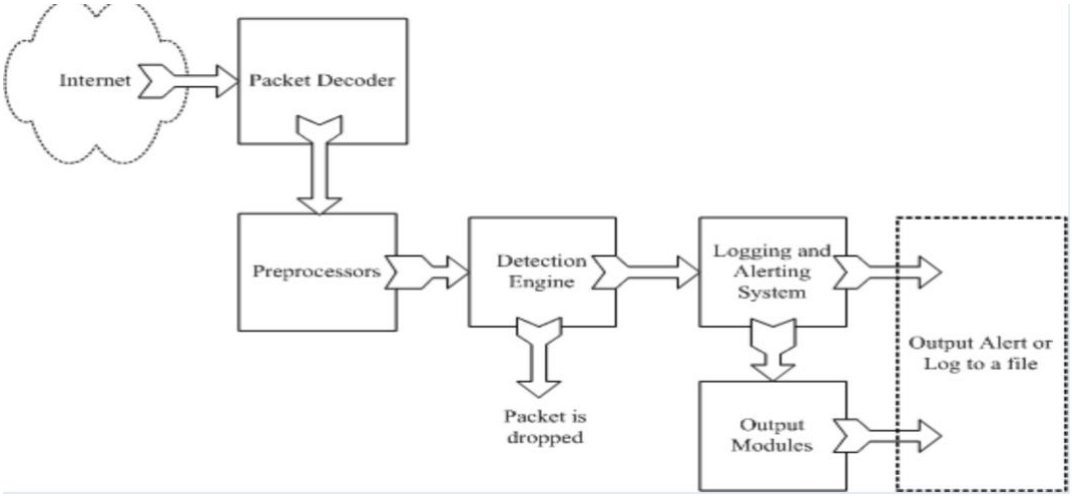
- Assume intruder behavior differs from legitimate users
- Overlap in behaviors causes problems

Detection Result	Reality	Outcome
True	True	True Positive
True	False	False Positive
False	True	False Negative
False	False	True Negative

- The result of IDS – Positive or Negative
- The first word of the outcome verifies the second word.
- If the IDS say there is an intrusion, the result is **Positive**. But in the real scenario if there is no intrusion it will say the IDS's result is **false**. Hence, **False Positive**.
- The goal of an IDS isn't to increase the success rate of catching attacks but to minimize the number of regular requests that are flagged as attacks (False Positive).

Snort

- It's an open network intrusion detection system
- It's a packet sniffer monitoring network traffic
- Unlike **Wireshark**, this provides a defense mechanism rather than just sniffing.
- Snort works in the network level while **Tripwire** check on the file access
- Examines each packet to detect malicious payload or anomalies
- Detects attack methods through protocol analysis and content search and match
- It runs in promiscuous mode
- Lightweight, uses small amount of memory and processor time and easily configured



- The decoder takes packets from the different network interfaces & prepares for **Preprocessing** or **Detection Engine.**
- Snort Preprocessor –
    - These are components or plugins
    - That can be used with snort to arrange or modify data packets before detection engine takes over
    - Some preprocessors also perform detection by finding anomalies in packet headers & generating alerts.
- Snort Detection Engine –
    - Detect if any intrusion activity exists in a packet
    - Rules are read into internal data structures of chains where they are matched against all packets.
    - Rules are applied to different parts of a packet
        - IP header
        - Transport Layer level header (TCP, UDP, ICMP)
        - Application Layer level header (DNS, FTP, SMTP)
        - Packet Payload – Look for a string inside the data that is present inside the packet
- Snort Rule Format –

Rule Action – Protocol – Source IP – Source Port – Direction Operator – Destination IP – Options

- **Rule action** is what do you need to do when you detect a **protocol** coming from the **source IP** address from this **port** to the **destination IP** address and **port**. Additional customizations can be added (**Options**). The rule can be

adapted to support packets coming from source to destination or both ways (Directional Operator)

- Snort Basic Output
    - It logs its outputs in various formats. It can be based on
        - Speed
        - Ease Post – Processing
        - Machine Read
        - Human Readability
        - Tcpdump binary – Is the ultimate in speed & flexible post-processing.
- You can run Snort
    - Daemon mode (background process)
    - Packet sniffing mode (command line)
- Rule Categories
    - Low-level protocols (ICMP, TCP)
    - High-level protocols (HTTP, FTP)
    - Web server specific (Web-attack, Web-Client)
    - Exploit specific (Back Door)
    - Service impacting (DoS, DDoS)
    - Policy Specific (Infor, Misc, Porn)
    - Scanning & probing activities (Scan, Bad-Traffic)
    - Viruses, worms & other malware (Virus)

ARP (Address Resolution Protocol) Poisoning

- The attacker sends a DoS attack and overloads the Switch or Router that is used by the network.
- When overloaded it reverts to acting like a Hub.
- Then set one of the machines used in the DoS attack to promiscuous mode and send a message to the hub informing it is the network gateway.

- Afterwards, when legitimate users log back to the switch, there traffic is sent through machine that was set as the gateway.
- A successful ARP poisoning attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack.

Computer Forensics

- Digital Forensics –
    - It is generally held to be about retrieving and using digital evidence.
    - This might be data recovered from a computer hard drive or any device that stores data
    - It is used to find
        - Evidence for a crime scene
        - To check how a system was hacked
        - To identify inappropriate user access to a system
- Data can be
    - Hidden from normal users
    - Deleted but recoverable
    - If it is overwritten, it is physically deleted and is lost FOREVER!
- 4 main steps to proceed with forensics
    - Shutting down
        - Check for running processes
        - Take a screenshot of it
        - Check if live connections to the PC is running
        - Take a copy of system memory content and do a Magnet RAM memory capture
    - Transport
        - Victims PCs are stored in a secure location.
        - During transport, be aware that the PC is evidence.
    - Preparation

        - Remove drives from machine
        - Prepare a form to write details on the drives
    - Documentation
        - Take pictures from all angles of the PC
        - Record BIOS (Basic Input/output System & UEFI (Unified Extensible Firmware Interface) information
        - Record the time and date of the system
        - Note down the time zone
- Mathematical Authentication
    - Always create a **hash** of the original copy
    - Document what hashing algorithm is in used (Such as SHA2).
- Digital evidence is fragile
- It can also degrade over time
- Fundamental rules as investigators
    - Rule 1 - Never mishandle the evidence
        - Should be handled with extreme care
        - Purpose is to minimize disruptive contact with evidence
        - If needed, should be done in a least disruptive manner & documented
    - Rule 2 - Never work on the original evidence
        - Working on the original evidence digitally, leads to being it compromised
        - Process
            - Create a copy
            - Ensure its authenticity vs the original
            - Do the investigations in a read only manner.
    - Rule 3 - Document everything
        - CoC – Chain of Custody - It refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.
- Evidence gathering measures

    - Avoid changing the evidence
    - Determine when evidence is created
    - Search everything on the device
    - Determine information about encrypted files and what's inside
    - Present the evidence well
- Logical Analysis
    - It involves using the native OS to pursue the data
    - It is looking for the things that are visible
- Physical Analysis
    - It is looking for the things that may have been overlooked or invisible to the user
    - Swap File
        - It is a place where an investigator should physically analyze
        - It is the most important type of ambient data
        - It is like a scratch pad to write data to when additional RAM is needed
    - Unallocated Space
        - Free space in the hard drive that is not allocated for storage

Network Forensics

- Network Forensics – It is categorized as a single branch of digital forensics which includes the areas of monitoring and analyzing computer network traffic and allows individuals to gather information, compile evidence, and/or detect intrusions.
- Network Forensics methods

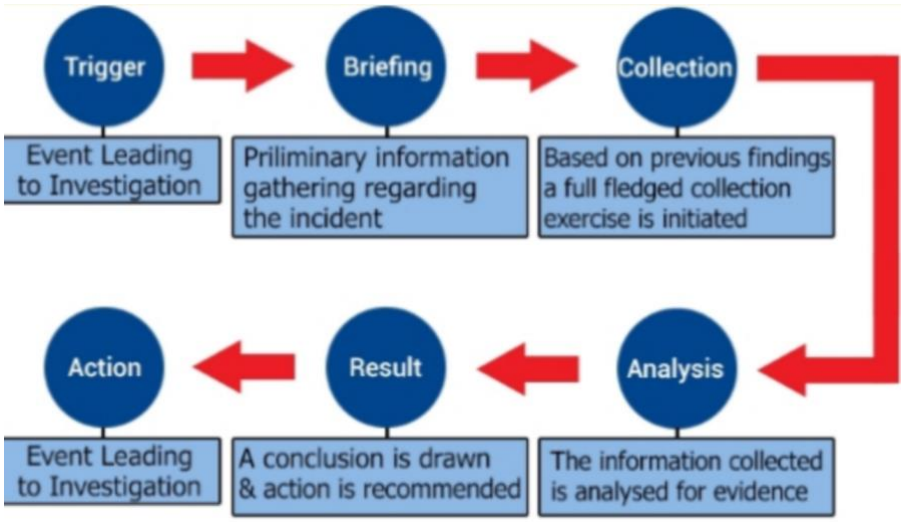
Catch-it-as-you-can	Stop, look and listen
• All packets are captured • Large storage needed • Analysis in batch mode	• Requires faster processor for incoming traffic • Each analyzed in memory

• Usually @ packet level • For later analysis	• Certain ones are stored • Usually @ packet level

- 007 in networking

  - Everything begins with a trigger
  - Trigger is an event or incident that alerts the organization about unauthorized activities
  - It could be reactive or proactive
  - Types of critical questions are as following - **5WH**

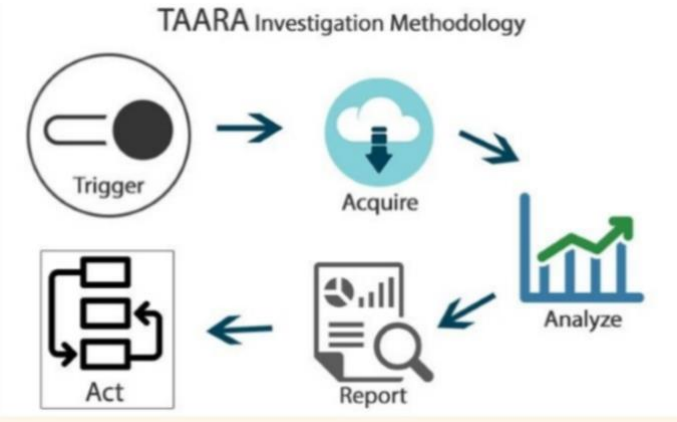
- Actions and recommendation process
  - Trigger - > Briefing -> Collection -> Analysis -> Result -> Action



- Characteristics to be an effective Network Forensics Bond
  - Preparation
  - Information gathering / evidence gathering
  - Understanding of human nature
  - Instant action
  - Use of technology
  - Deductive reasoning

My name is Bond. Network Forensics Bond

- TAARA methodology
  - Trigger -> Acquire -> Analyze -> Report -> Act



  - Trigger – Incident that leads to the investigation
  - Acquire – Predefined incident response plan and it involves identifying, acquiring & collecting information & evidence of the incident

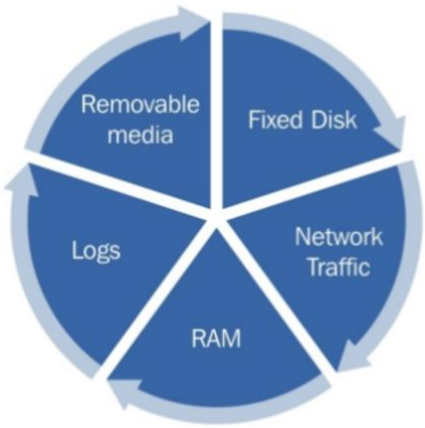
- Analysis – All the evidence that is collated, correlated, and analyzed. The sequence of events is identified
- Report – Based on the preceding analysis, a report is produced before stakeholders in order to determine the next course of action
- Action – The action recommended in the report is implemented

- Sources of Network-Based Evidence
  - Wire (Copper as twisted pair or coaxial cable)
    - Forensic value – Investigators can tap into physical cabling to copy and preserve network traffic as it is transmitted across the line
    - Two types of taps
      - Vampire taps – Puncture the insulation & connect to wire
      - Infrastructure taps – Replicate signals to a passive station without degrading the original signal
  - Air (Wireless / Radio Frequency)
    - Forensic Value – Wireless access points broadcast all signals so that any station within range can receive them
  - Router –
    - Forensic Value –
      - Routers having routing tables. It maps ports on the router to the networks that they connect.
      - It allows the investigator to trace the path that network traffic takes to traverse multiple networks
  - Authentication servers –
    - Forensic Value – It typically logs successful and/or failed login attempts and other events. Investigators can analyze logs to identify
      - Brute-force password guessing attacks
      - Account logins at suspicious hours and unusual locations
      - Unexpected privileged logins, which may indicate questionable activities
  - Central Log Servers –
    - Forensic Value –

- These servers are designed to help professionals identify and response to network security incidents.
- Even if an individual server is compromised, logs originating from it may remain intact on the log server

- Firewall –
  - Forensic Value –
    - Firewalls can be configured to produce alerts and log allowed or denied traffic, system configurations changes, errors, and a variety of other events.
    - These logs can help operators manage the network and also serve as evidence for forensic analysts.

- Identifying sources of evidence
  - 2 types
    - Evidence obtainable from within the network
    - Evidence from outside the network
  - Within network
    - From network & device logs
      - Firewalls, IDS, Anti-Virus servers, OS event logs, application logs
    - Network traffic
      - The packets transmitted are captured and reconstructed for analysis
    - Memory of individual PCs
      - Volatile memory (RAM)
    - Hard drives
      - Traces of internet activity, email, efforts to cover tracks & obfuscate evidence



EVIDENCE WITHIN NETWORK

- Outside Network
  - ISP logs (Internet Service Provider)
    - Login/Logoff, user names, resources accessed, online content & activity, IP addresses, date & time usage, duration of usage
  - Mobile devices

- Challenges in network evidence
  - Acquisition –
    - Can be difficult to locate specific evidence
    - Pinpointing the correct location of evidence can be tricky
    - Difficulty gaining access to it for political or technical reasons
  - Content –
    - Network devices often have very limited storage
  - Storage –
    - Storage network devices commonly don't employ secondary or persistent storage
    - Data can be volatile and might not survive a reset of the device
  - Privacy –
    - There may be legal issues and constraints
  - Seizure
    - Seizing a network device can be much more disruptive than doing it to an HDD

Questions

- Just some questions on the notes under 4 categories to help with remembering. Answer the questions. No essay questions.

Basics

1. Name 2 Transport Layer protocols and its qualities
2. What are the 7 layers of the OSI model and its responsibilities?
3. What is the difference between the 5 layer and the 4 layer structure of TCP/IP model?
4. Name the 5 layers of the network packet on the internet
5. What is Phishing and state the differences of Phishing and Vishing/SMiShing, Spear Phishing, Whaling.
6. State the 5 stages of a Cyber Attack
7. State differences in TCP and UDP?
8. What sort of defences should you follow for Packet Sniffing, Port Scanning, Password Cracking, Trojan Horse, IP spoofing and MITM
9. State 4 Active attacks
10. State the 4 types of attacks & 4 types of intruders
11. What is Security?
12. State the CIA triad and what it means
13. State 6 type of malware and what it does
14. What is a macro virus?
15. What is the difference between MAC & DAC.
16. State the 3 factors of Authentication

DoS related

1. State 3 types of DoS attacks and how it works
2. How does Land Attack work?
3. State 2 firewall techniques and how it works
4. State 3 sessions Hijacks and what happens in it
5. On what fact does the attacks use as an advantage of in Session Hijacking?

6. What are honeypots and honeynets?
7. State advantages of honeypotting
8. State the differences in HTTP basic and form based authentications
9. What is SSL/TLS and how does that involve in HTTP?
10. What is a DoS attack what is its purpose?
11. What are the 4 categories of a DoS attack?
12. What is the difference between DoS and DDoS?
13. What sort of protection should you follow for SYN and UDP floods?
14. Describe how the 3-way handshake happens in a TCP connection

IDS

1. What is an IDS?
2. What is SIgnature Detection?
3. What is the difference between NIDS & HIDS?
4. What is the goal of an IDS?
5. What is SNORT?
6. State the process of how a packet goes through a SNORT system
7. State the different parts if a packet SNORT rules can be applied
8. What is the SNORT rule format?
9. What sort of stage you can run SNORT?
10. State 7 rule categories in SNORT
11. What is ARP poisoning?

Forensics

1. What is Digital Forensics?
2. What is it used to find?
3. What are the 4 steps to proceed with forensics and how it works?
4. State the 3 fundamental rules of an investigator
5. What is Network Forensics?
6. State the 2 methods in network forensics and the difference
7. Characteristics of an Network Forensics Bond
8. What is TAARA?
9. State the sources of network based evidence
10. State 5 types of evidences within a network
11. State the challenges in network evidence

Extra

1. What is the difference between Wireshark, SNORT and Tripwire?