What Is IDS - Intrusion Detection System

IDS - sec mechanisms that detect + respond to unauth/malicious activities in comp network/system

Main purpose - monitor network traffic + analyse for suspicious behaviour → alert sysadmins when potential breach/intrusion detected

Work via comparing NW activities against signatures + employing behavioural analysis + anomaly detection techniques. Signature - pattern/identifier indicative of known attack/malicious activity

IDS Purpose in NW Sec

Monitor network traffic + systems for unauth/malicious/suspicious activity

Detect potential breaches + attacks on network - maintain CIA of data + resources

Complements other sec measures e.g. firewalls, antivirus SW

Help orgs proactively ID + respond to incidents + maintain secure network environment

IDS Role/Function in NW Sec

Threat Detection - Examine NW traffic + sys logs - ID patterns/signatures indicative of known threats (malware / virus/attacks) | Detect unusual behaviour that may suggest unknown (zero-day) threats.

Anomaly Detection - Look for abnormal activity that deviates from normal behaviour patterns. Helps ID new threats that don't have predefined signatures | **Incident Response -** Intrusion/suspicious activity detected - IDS generates alert to admins/ SOC (Security operations Center) | Alerts help staff respond quickly + mitigate potential incidents | **Real-Time Monitoring -** Continuously monitors NW - provides realtime visibility into activity + potential threats. Enables swift response → minimise attack damage | **Network Traffic Analysis -** Examines NW packets + data flows - provides insight into NW behaviour + traffic patterns. Helps admins optimise NW performances + ID bottlenecks | **Compliance + Auditing -** IDS assists orgs meeting security regulations + compliance standards via providing detailed logs + reports of NW activities | **Protection of Critical Assets**. Helps safeguard critical assets from unauth access/malicious activity. Crit assets - DBs, servers, sensitive info | **Reduced False Positives -** Sophisticated algorithms + machine learning → reduced false pos. Staff focus on genuine threats | **Intrusion Prevention System Integration** - Some advanced IDS' can integrate w Intrusion Prevention Systems (IPS) - allows proactive measures to block/mitigate threats automatically

Different IDS Types

Network Based IDS - Monitors NW traffic - analyses packets for suspicious patterns/anomalies | Operates at NW perimeter - effective for large scale monitoring | Can detect various attack types - port scans, DoS, malware propagation | **Host Based IDS -** Resides on individual hosts/servers - monitors system log files + activities | More detailed view of host-specific events + effective at detecting insider threats + local attacks | Gives realtime alerts for unauth access attempts, file modification, unusual user behaviour | *HIDS shows attack results, NIDS shows delivery mechanism of attack* | **Signature Based IDS -** Uses signatures of known attacks | When ID's a match → trigger alert / take action to mitigate threat | Effective against known threats | Not effective for new/evolving threats | **Anomaly Based IDS -** Establishes baseline of normal behaviour for NW/host | Detects deviations from baseline - may potentially indicate intrusion | Can ID new threats - more adaptable | **Hybrid IDS -** Combines signature + anomaly | Improved accuracy + less false positives | Comprehensive protection against wide range of threats

IDS Components:

Sensor + Agent - Role - act as data collector + monitor NW traffic | Placement - at critical points in NW | Function - capture + analyse | incoming/outgoing packets for potential threats | **Sensor** - monitor wired/wireless NW's | **Agent** - monitor endpoints/hosts

Analyser - Role - process data collected by sensors - ID patterns + anomalies | Techniques - signature + anomaly based analysis

Signature based - compare incoming data against known signatures

Anomaly based - detect deviations from normal NW behaviour

Management Server - Collects data from sensors/agents + correlates and analyses data | **Database Server -** Role - store historical data recorded by sensors/agents + attack signatures + baseline NW behaviour | Importance - enables comparison of current NW activity vs past events | **IDS Console -** Does administrative/management tasks + event monitoring, alerting, controlling sensors | **Alerting Mechanism -** Role - notify sysadmins about potential breaches | Triggers - activated when analyser detects suspicious/malicious activity | Notification types - email, SMS, system alerts, SNMP traps

IDS Deployment Strategies

Inline Deployment - IDS placed directly in NW traffic path - blocks suspicious activity in realtime | +Immediate response | -Can cause latency + single point of failure | **Passive Deployment -** IDs analyses a copy of NW traffic | -No realtime response ability | +No performance impact

Hybrid Deployment - Combines inline + passive to get benefits of both Analyses copy of NW traffic + blocks malicious traffic | +Enhanced accuracy + minimises latency

IDS Deployment Options

Host Based IDS (HIDS) - Focus - monitors activity on single host + detects anomalies | Use cases - detecting local attacks + suspicious activity on servers, workstations etc. | +Provides in-depth visibility into host-level events | -Potential performance overhead

Network Based IDS (NIDS) - Focus - analyse NW traffic to ID potential threats e.g. suspicious patterns/behaviours | Use cases - detecting malicious traffic before it reaches target host | +Gives broader view of NW activity | -May miss host-level events | **Hybrid H+NIDS –** has both host + network based capabilities | +Comprehensive coverage - NW + host level

Distributed IDS (DIDS) - Multiple IDS sensors connected across various locations | +Scalability | +Broad NW monitoring capability | **Signature-based IDS –** predefined signatures to ID atks | +quick + efficient for known threats | -struggles with new/evolving atks | **Anomaly-based IDS –** establishes baseline for norm behaviour -> flags deviations as potential threats | +effective for new atks | -likely false pos | -needs constant finetuning | **Behaviour Based IDS -** Focus on detecting malicious patterns rather than specific signatures | +Enhanced detection of attacks | -Can be resource intensive

Deployment Considerations

False Positives + Negatives - Challenge - find balance to reduce false alerts without missing genuine threats | Mitigation - fine-tuning signatures + anomaly detection thresholds | **Resource Utilisation -** Concern - IDS can consume lots of processing power + bandwidth | Solution - optimise IDS setting to minimise performance impact

IDS Architectures

Centralised Architecture - All sensor data sent → central IDS for analysis + decision making | +Simple management + correlation | -Bottlenecks + single point of failure | **Distributed Architecture -** Multiple sensors at strategic points in NW | +Fast response time + fault tolerance | -Needs careful coordination + management | **Cloud Based Architecture -** Sensors + data analysis hosted in cloud | +Scalable, flexible, reduced infrastructure needs | -Data privacy + network dependence

IDS Benefits

Threat detection - can ID various attack types e.g. malware, unauth access, unusual behaviour - aids early detection| **Realtime monitoring** – continuous monitoring -> gives realtime alerts when suspicious activity detected | **Enhanced security** - extra layer of security | **Proactive response** - early detection → fast response → reduced potential damage | **Compliance + auditing** - aids org meeting regulatory requirements via detailed logs + incident reports | **Network visibility –** gives insight into NW traffic patterns + malicious activities | helps ID vulnerabilities + weak points

IDS Limitations

False positives - may lead to alert fatigue + distract staff from real threats **Advanced evasion techniques** - some attacks can bypass IDS - reducing system effectiveness | **Limited to known signatures** - traditional IDS relies on signature based detection → not effective against new attacks | **Resource intensive** - IDS needs processing power + storage to analyse NW traffic / system behaviour - can impact system performance | **Inability to prevent attacks** - IDS only a detection tool, can raise alert for sec team but not actually stop attacks in realtime | **Encrypted traffic challenge** - encrypted traffic may limit IDS detection ability

Network Security Concepts

Network security - all measures taken to protect a network from unauthorised access, data theft and cyber-attacks | **Important for:** safeguarding sensitive info - ensuring business continuity + maintaining user trust

Key components - firewalls, encryption, access controls, IDS + IPS (prevention system), authentication protocols

Common NW Security Threats

Malware - viruses, worms, trojans, ransomware | **Phishing attacks** - deceptive emails/messages to trick users into revealing sensitive info **DDoS** - service denial via overwhelming network resources | **Man in the Middle** - interception + modification of communication between 2 parties **Insider threats** - unauthorised actions by staff with access to NW **Password attacks** - brute force, password guessing, credential theft

NW Security Protocols

SSL/TLS - secure socket layer + transport layer security - for secure data transmission | **IPsec** - internet protocol security - for securing IP communication via encryption + authentication | **VPN** - virtual private network - create secure connections over public internet | **SSH** - secure shell - for encrypted remote access + secure file transfers | **DNSSEC** - domain name system security extension - for securing DNS queries

NW Security Measures

Firewalls - monitor + control incoming/outgoing NW traffic based on predefined rules | **IDS** - detect + alert on suspicious activity/attacks | **IPS** - takes action to block/prevent detected threats | **Network segmentation** - divide NW into small segments to contain breaches | **Access Control Lists (ACL)** - restrict access to NW resources based on user privileges | **Encryption** - protect data by converting it to secure format that requires key to decipher

NW Security Best Practices

Regular updates - all NW devices + SW up to date w latest security patches **Strong passwords** - enforce use of complex pw's + implement multi-factor authentication | **Employee training** - educate users about security threats + practices to prevent social engineering attacks | **Data backup** - regular backups of critical data to prevent loss in case of incident | **Least privilege** - users given min level of access required to perform duties | **Incident response plan** - comprehensive plan to respond to sec incident promptly

NW Security Auditing

Regular assessments - periodic audits to ID vulnerabilities | **Vulnerability scanning** - automated tools to discover + assess weaknesses in NW **Penetration testing** - simulated attacks to evaluate NW;s resistance to real-world threats | **Log monitoring** - analyse NW logs to detect anomalies + potential breaches

Emerging NW Security Technologies

AI - using AI for threat detection + response

Software-Defined Networks (SDN) - centralised NW control for enhanced sec management

Blockchain - immutable distributed ledger to protect sensitive data

IoT security - ensuring security of IoT devices + NWs

What is Computer Network

Computer Network - collection of interconnected computing devices that are capable of sharing data, resources and info with each other. Multiple computers/servers/printers can communicate + collaborate - enables users to access shared resources, exchange data and perform various tasks. Network can vary in size/complexity - small LANs → large-scale WANs | Network can be wired via physical cables (ethernet / fiber optic) or wireless (Wifi / cellular)

Computer Network Components

Nodes - any devices connected to network computers/phones/servers/printers/routers **Links** - connections that facilitate data transmission between nodes. Can be wired /wireless | **Protocols** - rules + conditions that govern data transmission + communication within NW E.g. TCP/IP, UDP, HTTP | **Network Devices** - devices that help manage + control data flow within NW e.g. routers, switches, hubs, firewalls

What is NW Trace Analysis

NW Trace Analysis - process of examining + interpreting captured NW traffic data (NW traces) or packet captures to gain insight into communication patterns/NW behaviour + detect anomalies/potential security issues

NW Trace - detailed record of data packets travelling over NW @ specific time - captured via special tools/SW | Communication between devices in NW - handled by different protocols - that have their own uses + behaviours | **Challenge** - thousands of protocols

Trace Analysis Steps

Data capture - capture NW traffic via tools like packet sniffers/monitoring devices | Tools intercept + record packets flowing in NW + capture source/dest IP, protocols, packet size, timestamps | **Data analysis** - analyse data to gain insight into NW behaviour - ID patterns /anomalies/trends/potential sec issues | **Security monitoring** - by inspecting NW traffic - can detect + investigate potential sec breaches, malware infection, unauthorised access, any suspicious activities that may indicate cyber attack | **Troubleshooting** - by analysing traces, NW admins can ID performance bottlenecks, misconfigurations and other problems affecting NW's overall health | **Traffic profiling** - trace analysis allows creation of traffic profiles that help understand normal NW behaviour → can be used to detect deviations from normal patterns, potential indicative of sec threats/operational problems **Forensics** - trace analysis provides detailed record of NW activities that can be used as evidence in legal proceeding or incident response | **Performance optimisation** - by studying traces, admins can optimise NW performance by ID'ing heavy bandwidth users, inefficient protocols or excessive NW congestion

NW Trace Analysis Importance

Early threat detection - helps ID potential cyber threats + sec breaches before they escalate | **Network troubleshooting** - essential for diagnosing + resolving NW performance + connectivity issues | **Incident response** - important for investigation sec incidents + responding promptly to mitigate risks | **Forensics investigations** - crucial in gathering evidence for post-incident analysis + legal proceedings

Role of NW Trace Analysis in Cybersecurity

Threat Detection - ID malicious activities + abnormal behaviours on NW | Detecting unusual traffic patterns, port scans + reconnaissance attempts | **Intrusion detection -** Monitor for unauthorised access + potential data breaches | Analysing intrusion attempts, login anomalies + suspicious user activities | **Malware analysis -** ID + respond to malware infections | Analysing NW communication between infected hosts + command-and-control servers | **Incident response -** Investigate security incidents + data breaches | Tracing source + impact of sec incidents for effective response | **Traffic profiling -** Understand normal NW behaviour + baseline traffic patterns | Establishing benchmark for ID'ing deviations + anomalies | **Forensics -** Gather evidence for post-incident analysis + legal proceedings | Capturing + preserving traces for forensic examination

NW Trace Analysis Advantages

Real-time monitoring - useful in detecting + responding to ongoing threats **Historical analysis** - helps in reviewing past network activity to uncover hidden patterns **Proactive security** - help ID vulnerabilities before they are exploited **Data-driven decision making** - help making informed security decisions based on NW insights

NW Trace Analysis Application Areas

Incident response – used in investigating + responding to cybersec incidents | e.g. analyse NW logs to ID source of data breach/malware inf. | **Forensic investigation –** used to gather evidence + reconstruct events | e.g. capture packets to trace intruder activity | **NW performance optimisation –** help diagnose/troubleshoot performance issues | e.g. analyse packet delays + congestion -> make changes | **Intrusion detection/prevention –** used to detect+prevent unauth access attempts | e.g. monitor for suspicious log-ins / brute force atks | **Malware analysis –** used to ID + understand malware behaviour in NW | e.g. analyse comm patterns to detect C2 servers | **ID insider threats –** helps recognise malicious activities from internal users | e.g. monitor for unauth data exfil by staff | **NW baseline establishment –** used to get baseline of normal behaviour -> help anomaly detection | e.g. profile NW traffic during regular operations

NW Communication Concepts

NW comms – exchange of data/info between devs over NW | **Client-server model** - client sends requests → server responds w data/services | **Data transmission -** Happens via data packets | **Packet** - unit of data sent over NW | Data encapsulation used for wrapping data w headers + trailers for transmission | **Protocols** - rules governing data transmission + communication | **Ports** - numeric identifiers for specific communication endpoints **IP Addresses** - unique identifiers for devices on NW (either IPv4 or IPv6) | **Domain Name System (DNS)** - used to translate human-readable domain names → IP addresses

Packet Capture

Packet capture - process of intercepting + capturing data packets that traverse computer NW | Packets usually contain various types of info e.g. web page content, emails, file transfers, video streams etc | Used for NW analysis + troubleshooting + sec purposes | NW Admins + sec professionals use capture tools to - examine NW traffic + ID anomalies + diagnose NW issues + investigate sec incidents

Packet Capture Tools

Wireshark - one of most widely used open-source - supports various platforms + provides extensive protocol decoding capabilities | **tcpdump** - command line tool for unix systems - allows user to capture + display packets in realtime or save to file for later use | **NetworkMiner** - analyses captured packets + extracts files + metadata from them - useful for forensic investigations | **Smartsniff** - NW monitoring tool for windows - captures TCP/IP packets + allows users to view captured data in different formats | **Microsoft message analyser** - capture + analysis tool specifically designed for windows

Packet Capture Importance

NW visibility - help gain insight into data transmitted across NW
Troubleshooting - help ID + diagnose NW performance + connectivity issues
Sec analysis - help detect + investigate potential sec threats + attacks
Protocol analysis - help understand how different protocols operate in NW

Wireshark Features

Live packet capture - realtime capture + display of traffic | **Rich protocol supports** - decode hundreds of protocols for indepth analysis | **Filter + search** - packets based on criteria | **Packet analysis** - inspect packet content + headers + payload | **Statistics + graphs** - of NW data | **Exporting data** - save captured data in various formats for further examination

Wireshark Use Cases

Troubleshooting network issues - diagnose connectivity, performance or sec problems | **Analysing sec incidents** - investigate suspected attacks/malicious behaviour | **Validating protocol compliance** - ensure devices adhere to standards **Protocol analysis + optimisation** - understand protocol behaviour + optimise NW performance

Filtering + Collecting NW Traces

Process of selectively capturing specific packets based on criteria - reduce volume of total captured data + focus on relevant info

Types of packet filters - Capture filters - applied before packets are stored - reduced overhead | **Display filters** - applied during analysis to filter packets for display | **Example Filtering Criteria -** Source/destination IP addresses. Protocols + ports. Packet type e.g. TCP/UDP/ICMP | **Why is filtering important - Efficient storage** - reduce size of capture files. **Focused analysis** - reduce irrelevant traffic. **Minimise noise** - avoid unnecessary distractions | **Collecting network traces - Capture locations** - choose appropriate NW segments for monitoring. **Capture tools** - use tools like wireshark etc. **Storage** - ensure sufficient storage space for capture files

Packet Capture Best Practices

Capture duration - capture packets for an appropriate time period
Capture window - match capture window with occurrence of event
Documentation - record filtering criteria + capture setup to use for later reference

NW Protocols

TCP - Reliable + connection oriented. Ensures data delivery via establishing connection before transmission. Error checking + flow control + data sequencing
UDP - Unreliable + connectionless. Suitable for realtime apps w low overhead. No connection + best-effort delivery
ICMP - Network layer protocol for error reporting + diagnostics. Used by devices to communicate NW-related issues. Commonly used for ping + traceroute
HTTP - Application layer protocol for web communication. Used by browsers + servers to exchange data. Request-response model for fetching web pages/resources
SMTP - Application layer protocol for email. Used for sending + relaying emails between mail servers. Store + forward mechanism for email delivery
DNS - Resolves domain names → IP @. Used to translate user friendly names to machine-readable IP's. Distributed + hierarchical structure for name resolution
FTP - Application layer protocol for file transfer. Used for up/downloading files between client/server. Separate control + data channels for communication

Packet Headers

Header – control info attached to payload that ensures proper routing + delivery + processing | **Header Parts** – **Src + Dst IP** - ID devices on both ends | **Why useful** - ID comm patterns between hosts + detect unauth access / connections + map NW topology + data flow | **Src + Dst Port** – ID app / service running on host | **Why useful** – show what apps running + ID unusual services/backdoors + detect port scans + enforce sec policies | **Protocol** – shows which protocol being used | **Why useful** – understand nature of comms + ID protocol-specific atks + performance analysis based on protocol characteristics + filter for specific NW activity | **Sequence + ACK #** - track order of packets + confirm receipt of data | **Why useful** – detect lost/out-of-order packets + ID retransmissions from congestion/atk + reconstruct TCP sessions in right order + detect TCP-based atks (SYN flood / session hijacking)

Packet Structure + Header Analysis

Packet - Unit of data transmitted over NW. Every packet has - header (metadata) + payload (actual data) | **Header Fields -** Provide necessary info for packet handling + routing. Common fields - source/dest IP, protocol type, TTL, checksum etc. | **Ethernet Frame - Header fields** - source/dest MAC + ethertype (type of payload). Used for ID'ing devices based on MAC + ethertype | **IP Packet - Header fields** - source/dest IP, TTL, protocol, header checksum etc.. Used for route determination based on IP @ | **TCP Segment - Header fields** - source/dest port, sequence #, ACK #, flags (SYN/ACK etc.). Used for TCP connection establishment + flow control + error recovery | **UDP Datagram - Header fields** - source/dest port, length, checksum etc.. | Used for connectionless data transmission - suitable for realtime apps | **ICMP Packet - Header fields** - type, code, checksum, data. Used for error reporting + diagnostic messages for NW troubleshooting

Protocol Key Fields + Their Significance

TCP - Source port - sender's application/service. **Dest port** – receivers application/service | **Sequence #** - Ensures ordered data delivery | **ACK #** - confirms received data | **Flags** – SYN, ACK, FIN – manage TCP connection state | **SYN** – used to establish 3way handshake | **ACK** – used to acknowledge successful receipt of packet | **FIN** – no more data from sender
UDP - Source/dest ports – same as in TCP. **Length** – total length of UDP data gram **Checksum** – error checking for data integrity
Internet Protocol - Source IP @ - identify sender's device | **Dest IP @** - identify receiver's device | **Time-to-live TTL** – limits packets lifetime | **Protocol** – specifies next layer protocol (TCP/UDP/ICMP etc) | **Identification, flags, fragment offset** – manage IP fragmentation
ICMP - Type – identify type of ICMP msg (echo request, time exceeded) | **Code** – additional context for ICMP msg | **Checksum** – ensures data integrity for ICMP msg
HTTP - Request method – specify HTTP operation (GET, POST etc) | **Status code** – server's response (200 OK, 404 not found) | **Host** – identify target host in requests

Identifying Normal vs Suspicious Traffic Patterns

Normal NW Traffic Patterns - Patterns shown by regular, legit activities. Predictable + repetitive + consistent behaviour | Examples - web browsing, email traffic, SW updates | **Indicators of Normal Traffic - Consistent communication** - regular data exchange between trusted hosts | **Known protocols** - traffic associated w standards + expected protocols | **Regular intervals** - transfers occur at typical intervals || **Identifying Suspicious Traffic Patterns - a**nomalous / irregular NW behaviours - may indicate sec threat. Unusual frequency / patterns / destinations | **Indicators of Suspicious Traffic - Uncommon protocols** - traffic uses uncommon/non-standard protocols. **Abnormal port usage** - traffic on unusual ports. **Unexpected data volume** - large transfers at unusual times | **Network Anomalies - Sudden spikes** - unusual surges in traffic volume **Unusual connections** - communication w unauthorised/unexpected hosts **Unexplained outbound traffic** - data exfiltration attempts | **Monitoring + Baseline** - Establishing NW baseline - understand normal traffic patterns | Continuous monitoring - detecting deviations from baseline

Analysing DoS Attack

Characteristics – high traffic volume | exhausting resources (CPU, bandwidth, memory) | multiple source IPs (botnet) | **DoS Types –** SYN flood, exploits TCP 3way HS to exhaust server resources | UDP flood, overwhelm target w UDP pkts | HTTP flood, flood web server w http requests to exhaust resources | **Mitigation strategies –** traffic filtering (block malicious traffic at NW perimeter) | rate limiting (limit max # requests from IP) | web app firewalls (protects from app layer atks) | load balancers (distribute traffic on multiple servers) | anomaly detection (ID strange traffic for early warning) | black hole routing (redirect atk traffic to null route -> dropped) | **Incident response –** rapid detection (monitor for signs realtime | mitigation + containment (immediate action to block / divert) | forensics + reporting (document atk for analysis + legal purposes)

C2 Traffic Analysis (Malware Infection)

C2 traffic – comms between malware infected host <-> C2 server | enables atkrs to control + exfiltrate data from infected system | **Characteristics –** unusual protocols (malware uses non-standard prtcls to evade detection) | encrypted comms (used to hide malicious nature) | abnormal timing (abnormal, irregular intervals between comms) | **Analysis –** capture traffic -> ID protocols used -> examine encrypted payload for malware clues | **DNS tunnelling –** atkr encapsulates data in DNS requests | How detect – monitor DNS traffic for unusually large/frequent requests | **IP analysis –** IP (ID known C2 servers / unusual dsts) | geolocation (trace location of C2 servers) | **HTTP analysis –** headers (extract user-agent, referrer, cookies) | decryption (decrypt SSL/TTLS for deeper inspection) | **Botnet tracking –** sinkholing (redirect C2 traffic -> controlled server for analysis) | track C2 domains (monitor domain registrations + changes)
Incident response – containment (isolate infected sys from NW) | malware removal (from infected sys) | remediation (apply sec patches + updates to prevent reinfection)

Identifying Anomalies + Patterns in NW Traffic

Primary goal - detect anomalies + sec threats + performance issues
Identifying Anomalies - Look for: **Unusual spikes** - sudden + significant increases in traffic volume | **Unexpected protocols** - traffic using non-stand/suspicious protocols | **Outliers** - any devices/users deviating significantly from the norm
Recognising Patterns - Look for: **Regular traffic cycles** - any identifiable patterns in traffic flow @ specific times | **Seasonal variations** - traffic changes based on holidays/business cycles | **User behaviour** - ID patterns in user access + data transfer
Flow Analysis - Look for: **Flow records** - capture metadata about network communications. **Flow data visualisation** - use tools to visualise flow data
Time of Day Analysis - Peak hours - ID times of high NW activity | **Off-hours activity** - analyse NW behaviour during low-activity periods
Long-Term Trends - Capacity planning - predict future resource requirements based on traffic trends | **Network upgrades** - ID need for NW infrastructure enhancements
Realtime Alerts - Automated Alerting - configure system to notify when anomalies occur | **IDS** - use IDS to detect suspicious activities in realtime

Statistical Analysis Techniques

Using statistical methods to analyse NW data for insights
Common Statistical Techniques - Mean, median, mode - measured of central tendency to understand the average behaviour | **Standard deviation** - measure of data dispersion around the mean | **Percentiles** - divide data into hundredths to analyse distribution | **Correlation analysis** - examining relationships between different variables | **Regression analysis** - predicting trends + outcomes based on historical data
Average Bandwidth Calculation - Mean bandwidth - calculating avg bandwidth usage over a specific period | **Key metric for capacity planning** - helps allocate resources effectively
Time Series Analysis - Analyse data over time to ID recurring patterns/trends
Seasonal decomposition - separating data into seasonal, trend and residual components | **Moving averages** - smoothing out fluctuation to reveal underlying trends
Peak Hours Analysis - Determining peak usage - identifying hours w highest NW traffic | **Resource allocation** - optimise NW infrastructure for peak demands
Probability Distribution - Normal distribution - bell-shape curve - useful for many natural phenomena | **Poisson distribution** - models rare events occurring at random intervals | **Exponential distribution** - describes time between events in a Poisson process
Hypothesis Testing - Form + test hypotheses about NW behaviour
Machine Learning in NW Analysis - Anomaly detection - use ML algorithms to detect abnormal behaviour | **Classification** - categorise traffic into different classes | **Predictive analysis** - forecast future NW trends
Data Visualisation - Present complex statistical results visually for better understanding | Charts, graphs, heatmaps - visually represent statistical insights

Identifying Bandwidth Issues + Bottleneck

Causes of Bandwidth Issues - Insufficient bandwidth - inadequate capacity to handle current traffic demands | **Network congestion** - traffic overload leading to data packet delays + losses | **Misconfigured Devices** - improperly configured network devices affecting throughput | **Background Applications** - non-essential apps consuming bandwidth
Identifying Bandwidth Bottlenecks - Network monitoring tools - like SNMP, NetFlow, or packet capture for analysis | **Traffic analysis** - ID heavy bandwidth consumers + their data patterns | **Realtime observation** - detect sudden drops/fluctuations in NW performance | **Periodic performance reports** - review historical data for trends + bottlenecks

Bandwidth Issues Solutions

Upgrading bandwidth - increase network capacity to handle higher traffic loads | **Quality of service** - prioritise critical traffic over less important data **Traffic shaping** - control data flow to prevent congestion | **Caching + content** delivery networks - reduce data retrieval times | **Bandwidth optimisation** - compressing data + using efficient protocols | **Application control** - manage background app bandwidth usage | **Load balancer** - distribute NW traffic across multiple servers to avoid overload | **Global server load balancing** - distribute traffic across multiple data centres

Extracting Files from Packets

Objective - ID transferred files + detect malware + investigate data exfiltration
Common File Transfer Protocols - File Transfer Protocol FTP - classic file exchange between client-server | **Trivial File Transfer Protocol TFTP** - lightweight protocol for firmware upgrades | **Hypertext Transfer Protocol HTTP** - for file downloads via web browser
Identifying File Transfer - Packet inspection - analyse packet payloads for file signature e.g. file headers | **File extension analysis** - recognise files based on extensions e.g. .doc .pdf etc.. | **Traffic filtering** - capture packets specifically related to file transfer
Wireshark for Data Extraction - Exporting objects - extract files from captured traffic via export objects feature | **Follow TCP stream** - reassemble TCP data to obtain transferred files
Artifact Analysis - Malware detection - scan extracted files for potential malware | **Metadata extraction** - gather file metadata e.g. timestamp, authors **Data reconstruction** - reassemble split files for complete analysis

Challenges + Limitations for File Extraction

Challenges - Encrypted traffic - inability to extract data from encrypted packets | **Fragmented data** - must reassemble parts for fragmented files **False positives** - careful analysis required to differentiate files from non-files
Legal + Ethical Considerations - Privacy concerns - handling sensitive/personal info responsibly | **Chain of custody** - maintain integrity for legal investigations

Recovering Transferred Data

Data Fragmentation - Breaking data down into smaller fragments for transmission | **Fragmentation Goal** - have efficient data transfer over NW w varying MTU's (Max Transmission Unit)
Fragmentation Process - Original data divided into smaller segments by sender | Each fragment includes header info required for reassembly
Fragmented Data Challenges - Out-of-order arrival - fragments may not arrive in order | **Packet loss** - fragments may be lost during transmission | **Duplicate fragments –** multiple copies of same fragment
Reassembly Techniques - IP fragmentation reassembly - reconstructing IP datagrams from fragments | **TCP stream reassembly** - reassembling TCP data segments for complete content | **Sequence numbers** - using seq # to order fragments correctly
Time + Buffer Constraints - Timeouts - max wait time for missing fragments **Buffer size** - allocate sufficient buffer space for reassembly
Wireshark Reassembly - Follow TCP stream - feature for TCP stream reassembly | **IP fragmentation** - view + reassemble IP fragments
Data Recovery in Forensics - Network forensics - reconstruct data for investigations | **Evidence recovery** - analyse fragmented data for legal proceedings

Analysing Encrypted Traffic
Challenges - Data privacy - protecting sensitive user info during analysis | **Lack of visibility** - inability to inspect payload contents due to encryption | **Decryption overhead** - resource-intensive process for decrypting large volumes
Methods - SSL/TLS Decryption - decrypt secure sockets layer/transport layer security traffic via private keys | **Forward proxies** - inspect traffic before it reaches the destination | **MITM** - intercept encrypted traffic for analysis
Certificates + Trust Considerations - Certificate management - handle SSL/TLS certificates securely | **Certificate trust** - ensure trust in decryption process
Deep Packet Inspection - Pattern recognition - ID patterns within encrypted data **Behaviour analysis** - analyse traffic behaviour for anomalies
NW Traffic Analysis - Metadata analysis - examine metadata for insights | **Flow analysis** - analyse flow patterns to detect suspicious activities
Ethical + Legal Implications - Privacy compliance - adhere to data privacy laws + regulations | **User consent** - obtain appropriate consent for traffic analysis
Integrating Trace Analysis with IDS
Combining trace analysis with IDs for comprehensive security
Goal - enhance threat detection + investigation + incident response
IDS Role - Monitor NW traffic for malicious activities Detect + alert on potential sec breaches
Integration Benefits - Comprehensive visibility - NTA + IDS = broader view of NW activities | **Enhanced threat detection** - NTA data increases IDS alert accuracy |**Incident response** - streamlined response by correlating IDS alerts w trace analysis
Data Correlation + Enrichment - Combining data sources - can merge IDS alerts w packet capture data for easy correlation | **Contextual info** - extra data = better understanding of attack's scope
Advanced Threat Hunting - Behavioural analysis - can ID subtle attack patterns via trace data | **Zero-day detection** - can unveil previously unknown attack signatures
Post-Incident Analysis - Forensic investigation - can reconstruct attack scenarios via NW traces | **ID root causes** - can use trace data to understand attack source
Challenges + Considerations - Storage + scalability - result of handling large volumes of packet capture data | **Data privacy** - challenge to ensure compliance with privacy regulations | **Resource requirements** - high demands for adequate resources for realtime analysis
Best Practices - Automated processing - streamline data analysis with automation, if possible | **Threat intelligence integration** - augment IDS alerts with external threat data
Incident Response + Forensics
Incident response - process of coordinated actions taken in response to cybersecurity incident | **Goal** - minimise damage + restore operations + investigate incident
Role of NTA in IR - Realtime detection - NTA helps ID ongoing incident via traces | **Attack triage** - NTA helps prioritise incidents based | **Immediate containment** - NTA helps isolate compromised systems for damage control
Investigating Incident Scope - Trace reconstruction - NTA helps piece together sequence of events via packet capture | **Traffic analysis** - NTA helps ID attack vectors + patterns for attribution | **Timeline creation** - NTA helps build chronological overview of incident
Analysing Attack Artifacts - Malware analysis - NTA helps examine malware behaviour via captured data | **Payload inspection** - NTA helps analyse malicious payloads transmitted in packets | **Command + Control** (C2) **traffic** - NTA helps trace communication between attackers and C2 servers
Network Forensics for Legal Proceedings - Chain of custody - helps maintain integrity of packet captures as evidence | **Forensic reporting** - helps in presenting findings in court-admissible manner
Benefits of Network Trace Analysis - Root Cause Identification - Understanding the initial attack vector and entry point | **Attribution and Threat Intelligence** - Uncovering the identity of the attackers | **Proactive Incident Handling** - Rapid response through real-time analysis |
Challenges in Network Forensics - Data Volume - Handling and processing large amounts of packet capture data | **Data Retention** - Ensuring sufficient storage for extended investigation periods
Incident Response Lifecycle - Preparation - Establishing incident response plans, including trace analysis procedures | **Detection and Analysis** - Identifying incidents through trace data and conducting analysis | **Containment**, **Eradication**, and **Recovery** - Mitigating the incident's impact and recovering operations | **Post-Incident Review** -w Conducting a post-mortem analysis to improve incident response

Post-Intrusion Analysis
Goal - assess scope + impact of breach for recovery + mitigation
Network Trace Analysis in Post-Intrusion - Data Reconstruction - Piecing together the attack timeline using packet captures| **Traffic Patterns** - Analyze communication between attackers and targets| **Egress Points** - Identify data exfiltration pathways|**Identifying Compromised Systems - Host Analysis** - Inspect packet captures for signs of intrusion on individual hosts| **User Behaviour** - Recognize unusual activities indicative of compromised accounts|
Data Exfiltration Detection - Payload Inspection - Examine packets for sensitive data transmission| **Anomalous Traffic** - Identify large or suspicious data transfers| **Network Mapping and Lateral Movement - Identifying Attack Paths** - Tracing attackers' movements across the network| **Propagation Analysis** - Analyzing malware spread between systems|**Correlating with Other Logs - Event Logs** - Aligning network trace data with system and application logs| **SIEM Integration** - Correlating network events with security information and event management|**Forensic Artifacts - Registry Entries** - Analyzing registry changes due to malware| **File Artifacts** - Investigating files created, modified/deleted during breach|**Impact Assessment and Reporting - Business Impact** - Assessing the financial and operational consequences| **Incident Report** - Documenting findings for management and stakeholders|
NW Trace Analysis Best Practices
Data Privacy + Legal Considerations - Handling Sensitive Info
Goal - ensure compliance w data protection regulation
Anonymization and Pseudonymization - Anonymization - Remove identifying information from network traces| **Pseudonymization** - Replace identifying data with pseudonyms for privacy|**Personally Identifiable Information (PII) - PII Identification** - Recognize & safeguarding personal data| **PII Masking** - Conceal sensitive data in captured packets|**Encryption+Secure Storage - Encryption** - Secure data during storage & transmission| **Secure Storage** - Safeguard packet capture files from unauthorized access|**Consent+Ethical Considerations - Informed Consent** - Obtain permission b4 capturing and analyzing data| **Ethical Analysis** - Ensure ethical use of network trace information|**Legal Frameworks and Regulations -** General Data Protection Regulation (GDPR) - Compliance with EU privacy laws| California Consumer Privacy Act (CCPA) - Protecting consumer data in California, USA| Other Regional Laws - Comply with data protection laws in relevant jurisdictions|**Data Retention Policies - Retention Periods** - Define how long captured data should be stored| **Data Destruction** - Properly disposing of data after the retention period|**Incident Response and Legal Proceedings - Chain of Custody** - Maintain integrity of network trace data for legal purposes| **Expert Testimony** - Present trace analysis findings in court proceedings|
Awareness and Training - Personnel Education - Train staff on data privacy and handling procedures| This helps to keep abreast of changes in data protection regulations|
Documenting + Reporting Findings
Goal - communicate results effectively to stakeholders + management | Involves presenting NTA findings in structured manner
Components of Comprehensive Report - Executive Summary - Succinct overview of the analysis and key findings | **Introduction -** Background information about the incident or analysis | **Methodology -** Explanation of the approach and tools used for trace analysis | **Data Presentation -** Visual Aids - Incorporating charts, graphs, and diagrams for clarity | Packet Examples – incl | selected packet snippets to illustrate findings | **Analysis and Findings -** Incident Details - Overview of the analyzed incident or issue | Observations - Detailed examination of network traces and their implications | Root Cause Analysis - Identifying the primary cause of the network problem or security incident | **Recommendations** - Mitigation Strategies - Proposed solutions to address identified issues | Preventive Measures - Recommendations to prevent similar incidents in the future | **Impact Assessment** - Quantifying Impact - Evaluate the severity of the incident's consequences | Business Continuity - Analyze the impact on operations and services | **Legal and Ethical Considerations -** Data Privacy - Ensure compliance with privacy regulations in the report | Restricted Information - Omit sensitive data from public reports |
Clarity and Readability - Concise Language - Use clear and straightforward language in the report | Logical Flow - Organize the report in a logical and coherent manner | **Review and Validation -** Peer Review - Have the report reviewed by other analysts for accuracy | Data Verification - Ensure the accuracy of information presented | **Audience Considerations -** Technical vs | Non-Technical - Adapt the report to the audience's level of expertise | Management and Stakeholders - Focus on the key insights relevant to them

Continuous Learning + Professional Development
Goal – stay current w evolving cybersecurity trends + threats | commitment to ongoing education = skull enhancement
Cybersecurity Landscape Dynamics - Emerging Threats - Understand new attack vectors and techniques |Helps you to keep up with evolving NW technologies
Formal Education Programs - Pursue academic programs in to help you enhance your cybersecurity knowledge | Certifications - Obtain industry-recognized certifications to enhance your skills and knowledge | Learn about new tools and technologies | **Industry Conferences and Workshops -** Cybersecurity Events - Attend conferences and workshops | Collaborate with peers and experts, this exposes you to new opportunities | **Professional Security Organizations -** membership Benefits - Join cybersecurity associations (e |g |, AISA) | You will gain access to exclusive resources for members | **Cybersecurity Blogs and News -** Threat Intelligence Sources - Subscribe to reputable cybersecurity blogs | Stay informed about recent breaches and incidents | **Capture the Flag (CTF) Challenges -** Ethical Hacking Challenges - Participate in CTF competitions | Helps you to improve your hands-on cybersecurity abilities | **Ethical Hacking Labs -** Practice Environments - Utilize safe environments for ethical hacking | Helps you to test new tools and techniques | **Professional Growth Planning -** Career Goals - Set objectives for career advancement in cybersecurity | If possible, plan a roadmap for skill development
Introduction to Firewalls
Firewalls - security devices/SW designed to monitor + control incoming/outgoing NW traffic | Can also be part of a co4mputer system/NW designed to stop unauthorised traffic flowing from 1 NW to another | Act as a barrier between a trusted internal NW and untrusted external NWs (internet) | They differentiate NWs within a trusted NW | **UFW** – uncomplicated firewall – use friendly interface for managing the iptables firewall on linux ubuntu | **Main functionalities -** Filtering data; Redirecting traffic; Protecting against network attacks
Firewall Importance
First Line of Defense - Initial defense against unauthorized access and potential threats | **Traffic Control -** Regulate network traffic - preventing malicious data from entering the network + sensitive data from leaving | **Intrusion Prevention -** Help prevent unauthorized users/attackers from gaining unauthorized access **Data Protection -** Safeguard sensitive data - such as personal information and proprietary data - from being compromised
Firewalls Roles in NW Defense
Traffic Filtering - Examine data packets + make decisions based on predetermined rules | **Access Control** - Determine which users/systems/app are allowed to communicate w each other | **Threat Mitigation -** Can block/allow traffic based on threat intelligence + behaviour analysis | **Policy Enforcement -** Enforce sec policies - ensuring compliance w company guidelines + industry regulations
Firewall Benefits
Enhanced Security - Reduced attack surface + potential entry points for attackers **Network Segmentation -** Enables separation of NWs - improved security + resource optimisation | **Early Threat Detection -** Can detect + block suspicious activity before it reaches critical systems | **Risk Management -** Minimising access → better risk management + data protection
Firewall Requirements
All traffic between trust zones should pass through firewall | Only authorised traffic (defined by policy) should be allowed to pass through | Firewall itself must be immune to penetration - implies using hardened system with secure OS | Consists of HW/SW or both | Monitors + filters traffic attempting to enter/leave protected private NW | Tool that separates protected NW or part of NW - from unprotected NW | **Most FW perform 2 functions** - Packet filtering based on accept/deny policy | App proxy gateways that provide services to inside users whilst protecting hosts from unwanted outside users
Firewall Filter Characteristics
IP address + protocol values - Used by packet filter + stateful inspection firewalls; Used to limit access to specific services | **Application protocol -** Used by an app-level gateway that relays + monitors exchange of info for specific app protocols **User identity -** For inside users who ID themselves using some form of secure auth tech | **Network activity -** Controls access based on considerations such as time of request/rate of requests/ other activity patterns
Policy (ACLs)
Includes <action> and 1+ of the following **– src @/ @ block | dst @ / @ block | protocol | src/dst ports**

Action	Source address	Source port(s)	Destination address	Destination port
allow	192.0.2.1	1024-65535	192.0.2.101	80/tcp
allow	192.0.2.101	80	192.0.2.1	1024-65535/tcp
deny	any	any	any	any

Firewall Rule Configuration
Rule Components - Source - traffic origin - IP @, NW, user | **Destination** - traffic target - IP @, NW, service | **Port** - port # or range for services | **Protocol** - communication protocol | **Action** - what to do with matched traffic - allow/deny/log
Rule Evaluation Order - Rules are evaluated in sequential order | First matching rule is applied - subsequent rules ignored | Place more specific rules before general ones
Default Deny - Deny all traffic by default - only permit specified | Ensures tight security but may lead to unexpected service disruptions **Default Allow -** Allow all traffic by default - only deny specific | Easier for usability but increased attack surface
Firewall Rule Best Practices
Specificity – craft rules only to match necessary traffic | minimise wildcard usage (inc. accuracy) | **Least privilege –** only grant min access | restrict resource access based on roles + needs | **Review + update –** regularly review + adjust rules based on changing needs
Effective Rules for Enhanced Security:
Rule optimisation is a balance between security and functionality
Regularly audit + fine-tune rules to reflect current needs
Collaborate w network admins for comprehensive rules
Sensible Firewall Rule Components
Default deny | driven by org policy | linked to natural-language policy | defined in simple terms | use reusable objects | has descriptive comments
Why Default Deny
Easier to ID allowed actions than not allowed | easier FW auditing
Firewall Policy / Controls
User control - controls access to the data based on role of the user who is attempting to access it; Applied to users inside the firewall perimeter | **Service control -** controls access by the type of service offered by the host | Applied on the basis of network add., protocol of connection + port # | **Direction control** - determines direction in which request may be initiated and are allowed to flow through the firewall Tells whether traffic is inbound or outbound
Firewall Actions
Accepted - allowed to enter connected NW/host via firewall
Denied/Dropped - not permitted, silent discard
Rejected - similar to deny but tells src about decision via ICMP packet
Filtering types - Ingress - inspects incoming traffic to safeguard internal NW + prevent attacks from outside | **Egress** - inspects outgoing traffic + prevents users inside NW reaching outside NW e.g. blocking social media sites on school NW
Firewalls Types:
Packet Filter Firewall (stateless) - decisions based on each packet header info - doesnt look at payload | Doesn't care if packet is part of existing stream | Doesn't maintain packet states - stateless firewall
Stateful Firewall - tracks traffic state by monitoring all interactions until connection closed, decision based on state info | Keeps connection state table to understand packet content | Allows more refined filtering vs stateless | Can automatically add implied rules to allow traffic related to traffic permitted by explicit rules
Application / Proxy Firewall - Controls input/output and access to/from an app/service | Acts as intermediary by impersonating intended recipient | Client's connection terminates at proxy - separate connection initiated from proxy → destination | Data on connection - analysed up to app layer top determine if pkt allowed/rejected
Host vs NW Firewalls
Network Firewalls - Devices placed in path in NW to control packet flow passing through them | Provide protection for more than 1 device + are independent from device they protect
Host Firewalls - SW on host that provide traffic control for host | Firewall capabilities usually part of host OS
Next-Gen Firewall - Application aware proxies can have complete awareness of traffic details they control
They are largely incapable of handling traffic they are not designed for - can cause significant performance/complexity issues | Next-gen firewalls can unpack + inspect payload data → inform traffic control decisions at line speed | Aware of app-layer data like a proxy but doesnt impact data transfer rate | **Benefits –** single choke point | location for monitoring sec events | protect internal + external sys | filter comms based on content | do NAT | aid IDS/forensics via logging