Intrusion Detection Systems and Incident Handling 320/520

Fundamental Network Knowledge, and Introduction to TCPdump

Network and Communication Fundamentals

- Why is the fundamental networking and communication knowledge required?
- IDS can handle most attacks BUT some require advanced traffic analysis and network protocol knowledge

Network and Communication Fundamentals

- Network layers:
  - Application Layer - enables the data transfer an application server and a client
    - DNS
    - FTP
    - SNMP
    - SMTP
  - Transport Layer - packages the data that needs to be transmitted between hosts - data packaged as packets
    - TCP
    - UDP

Network and Communication Fundamentals

- Network layers:
  - Internet Protocol Layer - handles the addressing and routing of the data received from the transport layer
    - Packet header
      - Source & Destination IP address
      - IP protocol number
    - Packet payload

Network and Communication Fundamentals

- Network layers:
  - Hardware Layer - handles the communications to the physical medium on which it resides
- The four layers work in tandem to exchange data between hosts
- Network based IDS/IPS system work mostly on the application layer
- Some also analyze the traffic at the transport layer

Network and Communication Fundamentals

- TCP/IP Suite of Protocols Fundamentals
  - TCP
    - Provides reliable connection between two systems
    - Ensures that both system are ready to communicate and that the information moved is transferred without anything lost
    - Ensures that all packets are sequenced and acknowledged (using windowing)
    - Common applications using TCP - FTP, SSH, SMTP

Network and Communication Fundamentals

- TCP
  - TCP header information provides key information about a session
  - TCP control bits
    - can be set independently
    - Total of 8: URG, ACK, PSH, RST, SYN, FIN, CWR and ECE
  - TCP connections involve a three-way handshake

Network and Communication Fundamentals

- TCP - Problems
  - TCP connections are susceptible to SYN flood attacks
  - TCP is susceptible to non-random-sequence numbers
  - Random source and destination ports also can cause problems in detecting intrusions

Network and Communication Fundamentals

- UDP
  - Provides an unreliable but much faster approach to deliver packets
  - Does not involve a state of connection (unlike the TCP protocol which relies on state tracking)
  - Used for application for which speed is preferred to completeness of information (such as audio or video data)
  - Common Applications using UDP - TFTP, Broadcasts, NFS

Network and Communication Fundamentals

- UDP - Problems
  - UDP is less secure than TCP
  - UDP is susceptible to spoofing
  - UDP can enable flooding attacks
  - UDP is a common target for open ports scan

Network and Communication Fundamentals

- IP
  - Handles the datagram services between hosts
  - Addresses consist of four numbers separated by full stops - the addresses are used to determine where the packets are delivered
  - Supports packet fragmentation

Network and Communication Fundamentals

- IP - Problems
  - Susceptible to packet modification
  - Common attack method uses packet fragmentation
  - The IP identification can be used maliciously to gather information about the system (stealth scan)

Network and Communication Fundamentals

- ICMP - protocol for relaying messages
  - Functionality
    - Flow control
    - Unreachable destination alert
    - Redirecting route
    - Remote host check

Network and Communication Fundamentals

- ICMP - Problems
  - Protocol regularly used for attacks
  - ICMP is susceptible to traffic redirection
  - ICMP susceptible to message abuse (ping)

Network and Communication Fundamentals

- Data Transmission Key Concepts
  - Data Flow
    - Source and destination do not “talk” to each other directly
    - Messages contain information for each of the layers
  - Data Encapsulation
    - Data added by each layer
    - Address information added to the frame
  - Addresses
    - Physical addresses - used by the Ethernet card to interface with the network
    - Logical addresses - translated using the ARP
    - IP address typically dynamic - allocated using DNS

Network and Communication Fundamentals

- Service Ports
  - Used to provide basic functionality
  - Services are not port specific!
  - Port allocation is “standardized”
  - Requires careful checking for hacker activity
- Client ports
  - Selected for a connection
  - Can be reused once the connection has been terminated

Network and Communication Fundamentals

- TCPdump Tool
  - Gathers data from the network
  - Can be critical for understanding how an attack is carried out
  - Output from TCPdump can be challenging to interpret - there are other tools that can used to analyse the data (such as Wireshark)

Network and Communication Fundamentals

- TCPdump Tool
  - Filters can be used to specify to be collected
    - TCPdump provides a filter syntax
    - Filter rules can collated into an input file passed onto TPCdump
  - Can generate very detailed but also very large output files
    - The amount of data can be specified at command line
  - Standard mode - shows the most relevant fields in the packet
  - All fields can be shown in hexadecimal format

Network and Communication Fundamentals

- TCPdump Tool
  - IP Header information can be extracted from the output and thus enables the extraction of the embedded protocol
  - Information that can be extracted
    - IP Datagram length
    - TCP Header length
- TCPdump Output
  - 09:32:43:910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
  - What does it represent?

Intrusion Detection Systems and Incident Handling 320/520

Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Concepts, Approaches, Functionality, Limitations, General System Threats

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS aim - to automatically detect and identify possible security incidents
- IDS vs IPS - IPS may have the capacity to stop incidents
- IDS/IPS
  - Recognize violations of existing security rules
  - Recognize reconnaissance activity

Intrusion Detection Systems and Intrusion Prevention Systems

- What does and IDS/IPS do when an incident is detected?
  - Typical functions:
    - IDS/IPS collect/log data about the incident
    - Trigger alerts to the key personnel involved in the system security
    - Compile reports that summarize the events of interest

Intrusion Prevention Systems

- When an incident is detected
  - May stop the attack
    - Block access
    - Terminate connection
  - Reconfigure the security setup
    - Network devices
    - Firewall settings
  - Modifies the attack data
    - Email attachments deleted

Intrusion Detection Systems and Intrusion Prevention Systems

- How do they work?
  - Data collected from various sources
    - Hardware - network devices
    - Software - system logs
  - Analysis of data to identify attacks and intrusions (worst case scenario)
  - Formulate response
    - Passive
    - Active

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS vs Firewalls
  - Firewalls
    - Can detect intrusions
    - Generate alerts in case of attacks
  - Key difference: packet analysis - not done by firewalls
  - Firewalls work in tandem with IDS/IPS - reduce the amount of traffic to be analyzed

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS approaches to detection
  - Signature based approach
    - Simple comparison with known attack patterns
    - Does not require advanced network communication knowledge
    - Good: works well with known threats
    - Bad: cannot handled previously unseen threats
      - Not flexible and cannot track state of communications
      - Lack of adaptation means that an attacker can split the payload into several parts that have no resemblance with a known threat

Intrusion Detection Systems and Intrusion Prevention Systems

- Anomaly based approach
  - Uses existing definitions (profiles) of “normal” system behaviour to identify “abnormalities”
  - Mostly based on statistical analysis of the system activity
    - Users
    - Traffic
    - File access and CPU resources
  - Good: can recognize previously “unseen” abnormal activity
    - It is adaptive
    - Can be applied to different levels
  - Bad: requires effective system profiles which are difficult to generate
    - Profile tuning is difficult at best
    - Can generate false alarms

Intrusion Detection Systems and Intrusion Prevention Systems

- Stateful protocol analysis approach
  - Uses existing definitions of “normal” protocol activity to identify “abnormal” activity
  - The definitions of the “normal” activity is not host specific (unlike the anomaly based approach)
  - Requires tracking and understanding of states in protocols
  - Good: definitions are available
  - Bad: definitions not guaranteed to handle all threats (new threats need patching)

Intrusion Detection Systems and Intrusion Prevention Systems

- Basic functionality of an IDS/IPS system
  - Continuous monitoring of the system
  - Enables the alert and response to be automatic
  - Detailed analysis of large amounts of data at various levels

Intrusion Detection Systems and Intrusion Prevention Systems

- Basic functionality of an IDS/IPS system
  - Limit or prevent damage to the system
  - Can be combined with other network defenses to increase the effectiveness of the overall system

Intrusion Detection Systems and Intrusion Prevention Systems

- Limitations of an IDS/IPS system
  - ***WILL NOT PREVENT ATTACKS OR GUARANTEE THAT ALL ATTACKS WILL BE DETECTED***
  - Cannot be a substitute for skilled security personnel
  - Require tuning and updating
  - Will generate many false alarms which need to carefully analyzed and categorized

Intrusion Detection Systems and Intrusion Prevention Systems

- Limitations of an IDS/IPS system
  - Cannot handle all types of session slicing
  - Proxy attacks can be used to bypass an IDS
  - Data intensive attacks may overload the system and thus reduce the effectiveness of the IDS/IPS

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS additional usage:
  - Can be used to evaluate the network perimeter devices
  - Enforce security policy
  - Source of forensic evidence

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS additional usage:
  - Alert to internal attacks
  - Alert to buffer overflow attacks
  - Detect Backdoors and Trojans

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS additional usage:
  - Protect application integrity
  - Protect database access
  - Protect against Domain Name Server exploits
  - Protect against Email based exploits

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS additional usage:
  - Delay system intrusion or misdirect hacker attacks

Intrusion Detection Systems and Intrusion Prevention Systems

- What are the main threats to a system?
  - External
    - Generated by personnel outside the network with no initial authorized access to the system
  - Internal
    - Generated by personnel from inside the network with some form of authorized access to the system

Intrusion Detection Systems and Intrusion Prevention Systems

- What are the main threats to a system?
  - Unstructured
    - Based on well known system security holes
    - Less likely to result in major incidents
  - Structured
    - Typically involve more elaborate attacks requiring a good understanding of a system's security holes

Intrusion Detection Systems and Intrusion Prevention Systems

- Network attacks categories:
  - Information gathering attacks
  - Access attacks
    - Data retrieval
    - System access
    - Privilege escalation
  - Denial of Service attacks

Intrusion Detection Systems and Incident Handling 320/520

Intrusion Detection/Prevention Systems (IDS/IPS)

Categories, Organization, IDS/IPS Customization and Management

Intrusion Detection Systems and Intrusion Prevention Systems

- Intrusion Detection/Prevention System Categories:
  - Network Based
  - Wireless
  - Network Behaviour Analysis
  - Host Based

Intrusion Detection Systems and Intrusion Prevention Systems

- Network Based IDS (NIDS)
  - Focuses on monitoring and analyzing network activity
  - Can handle different types of incidents
  - Typically involves multiple systems
- Wireless
  - Monitors and analyzes the wireless network protocols
  - Cannot handle attacks at the application or higher layer network protocols

Intrusion Detection Systems and Intrusion Prevention Systems

- Network Behaviour Analysis (NBA)
  - Focused on detecting anomalies in the traffic flows and policy violations
- Host Based
  - Focused on a single system (host)
  - Can check for suspicious activity at different levels (user profile, system profile)

Intrusion Detection Systems and Intrusion Prevention Systems

- Typical IDS/IPS components:
  - Agents
    - monitor and analyze system activity (typically one host)
  - Agent Management Server
    - collect and combine data from multiple agents
      - correlated data can help identify incidents that individual agents cannot detect
      - used for multiple system monitoring and may be multi-layered

Intrusion Detection Systems and Intrusion Prevention Systems

- Typical IDS/IPS components:
  - Database Server
    - stores useful incident information by agent for analysis
  - Console
    - used to interface with the IDS
      - may allow only monitoring and analysis of traffic and incidents
      - may also enable device and ruleset configuration
- The components are connected via either the existing network or a separate network (to provide better security).

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS customization - key tools/parameters
  - Abnormal/Normal behaviour limit
  - Black/White lists
  - Alert Grading
  - Code IDE

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS management
  - IDS/IPS design key aspects
    - Agent placement
    - Server, Database and Console analysis (are they needed, were should they be placed?)
    - System connectivity and interface with other components

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS management
  - IDS design key aspects
    - Security analysis of existing communication network
    - Reliability of overall design
  - IDS/IPS component security
    - Use different user privileges
    - Set limits on traffic and deploy access rules
    - Use encryption to secure communication

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS management
  - IDS/IPS component deployment
    - May require a testing stage
    - Appliance based components - require basic configuration
    - Software based components - involves a more elaborate hardening process

Intrusion Detection Systems and Intrusion Prevention Systems

- IDS/IPS management
  - IDS/IPS maintenance requires:
    - To monitor the IDS components to determine and address possible security problems
    - Consistent checking of the IDS performance
    - Regular system vulnerability evaluations
    - Prompt updates of the IDS's appliance and software components

Intrusion Detection Systems and Incident Handling 320/520

Introduction to Packet Analysis and Wireshark

Introduction to Packet Analysis

- Packet analysis - process of collecting and analyzing traffic data
  - Aim: gain an understanding of what is happening in the network
  - Involves a packet sniffer such as TCPdump and Wireshark
    - Three stages:
      - Gather raw data
      - Convert data into usable format
      - Analyse packet information

Introduction to Packet Analysis and Wireshark

- Packet Analysis Setup
  - Access to raw data can be a challenge
    - Most current switches and routers do not allow port mapping
    - Network equipment handles data in different ways - sniffer deployment requires network physical organization analysis
  - Requires network cards with promiscuous mode capability
    - Promiscuous mode enables the capture of all traffic
    - If not in promiscuous mode, the traffic not addressed to it is dropped

Introduction to Packet Analysis and Wireshark

- Packet Analysis Setup
  - Hub Case
    - Seldom encountered
    - Enables quick access to the data (via any free port on the hub) - the traffic from all systems connected to the hub can captured
    - Data collected has to be filtered
  - Switch Case
    - Prevalent setup
    - Data capture can be done via port mirroring, hubbing out or ARP caching

Introduction to Packet Analysis and Wireshark

- Port mirroring - requires:
  - Privileges to access the interface of the switch that supports port mirroring
  - A port available for the packet sniffer
  - Careful estimate of traffic flow - excess traffic will result in dropped packets
- Hub out - requires:
  - Switch and hub setup
  - A port available for the packet sniffer

Introduction to Packet Analysis and Wireshark

- ARP Cache Poisoning - requires:
  - The use of ARP messages with fake MAC addresses

Introduction to Packet Analysis and Wireshark

- Handling Wireless Setups
  - More difficult than the Ethernet setups
  - Wireless networks can have multiple channels with different frequencies
  - One channel can be monitored at any one time
  - To capture traffic, the target channel information is needed
  - Channel switching is needed when specific channel information is not available

Introduction to Packet Analysis and Wireshark

- Handling Wireless Setups
  - Range of communication needs to be carefully considered - distance can lead to lost packets
  - Interference - can lead to corrupted or lost packets
  - Wireless cards have different modes - monitor mode allows packet sniffing

Introduction to WireShark

- Tool that enables packet analysis on both Windows and UNIX platforms
- Easier to use than TCPdump
- Uses a window based interface
- Provides support for most protocols
- Can be used capture live network data or use captured traffic files for analysis
- Data can be captured form different sources (for example Ethernet, wireless)
- Supports filters (similar to the TCPdump tool)

Introduction to WireShark

- Wireshark supports command line arguments
  - for packet capture and input/output options
  - specify filter options
- Wireshark Capture Filters
  - use TCPdump filters
  - one can target specific protocols and packet data
- Wireshark Display Filters
  - uses a different syntax
  - procesing is slower than capture filters

Introduction to Wireshark

- Name Resolution Capabilities
  - Three types: transport name resolution, network name resolution, MAC name resolution
  - Key for more effective packet capture by reducing the amount of data to be analyzed
- Name Resolution has some drawbacks
  - Incurs a processing penalty
  - Name resolution sometimes fails

Introduction to Wireshark

- Protocol Analysis Capabilities
  - Protocol can be divided into sections
  - User can select the tools to be used in the protocol data translation
- TCP Stream Following
  - Allows a detailed understanding of the traffic
  - Rather than having to check the low level information, the stream follow tool allows a higher level reconstruction of the traffic information

Using Wireshark

- To detect network scans
  - Can be the result of
    - normal activity
    - information gathering
    - worm activity
  - TCP ACK Scan
    - used to find open ports
    - analysis of logs provide evidence of connect attempts
    - easier to detect as the connection is completed and thus recorded

Using Wireshark

- TCP SYN Scan
  - connection not completed
  - less likely to recorded
- Null Scan
  - Sends packets with invalid flag settings
  - Open packets drop the packets and do not respond whereas closed ports provide a reply
  - Only applicable to some Oses
- To analyze trojan traffic
  - requires prior trace

Intrusion Detection Systems and Incident Handling 320/520

Network Based Intrusion Detection/Prevention Systems and Network Behaviour Analysis Systems

Network Based Intrusion Detection/Prevention Systems

- Network Based Intrusion Detection (NBID)
  - Basic setup components:
    - Sensors: hardware & software
    - Management server/s - desirable feature
    - Console
    - Database server/s - optional feature
  - Monitoring may be done on several network components and involve a large number of sensors
  - Communication security is critical (separate network for management server is preferable)
  - Sensor placement and mode depends on the overall strategy

Network Based Intrusion Detection/Prevention Systems

- Sensor mode:
  - Inline
    - Checks all traffic that passes through it
    - May block traffic is it is determined to be part of an attack
  - Passive
    - All traffic going through the sensors can be processed
    - It uses a copy of the actual traffic
    - Approaches to capture traffic:
      - Spanning port
      - Network tap
      - Load Balancer

Network Based Intrusion Detection/Prevention Systems

- Some NBIDs can collect data and store on:
  - Host information
  - Host operating system
  - Host application software
  - Network organization

Network Based Intrusion Detection/Prevention Systems

- NBIDs also collect detailed information about events of interest:
  - Event class and rating
  - IP information
  - Port information
  - Protocol information
  - User information and privileges
  - Data exchanged statistics
  - Packet Information

Network Based Intrusion Detection/Prevention Systems

NBIDs Detection and Analysis Capabilities:

- Application Layer
  - Attacks (such as password guessing)
  - Reconnaissance
  - Specific protocol analysis (such as DNS or DHCP)
- Transport Layer
  - Attacks (fragmentation)
  - Reconnaissance (port scanning)
- Network Layer
  - Attacks
  - Reconnaissance

Network Based Intrusion Detection/Prevention Systems

- NBIDs Detection and Analysis Capabilities:
  - Application services
  - Security Policy Violations
- Some NBID sensors can estimate the likelihood of a successful attack

Network Based Intrusion Detection/Prevention Systems

- NBID typical limitations:
  - Traffic load
    - Number of connections & duration of connections
    - Protocols used for the communications
  - Secure communications that use encryption
  - Targeted “blinding” attacks can mask actual attacks

Network Based Intrusion Detection/Prevention Systems

- NBID Prevention Capabilities
  - Passive Approach
    - Applicable only to some scenarios involving the TCP protocol
    - Limited effectiveness
    - Involves session terminating commands
  - Inline Approach
    - Applicable to a wider range of scenarios
    - Approaches used:
      - Packet rejection
      - Bandwidth control
      - Content control

Network Based Intrusion Detection/Prevention Systems

- Combined Approach
  - Involves either devices reconfiguration or carrying out a predefined set of actions

Network Behaviour Analysis Systems

- Network Based Analysis Systems (NBAS)
  - Basic setup components (similar to NBID):
    - Sensors: hardware & software
    - Management server/s - desirable feature
    - Console
  - Monitoring may be done on one or several network components - generally the information gathered is about the flow from routers/switches
    - IP addresses
    - Port information
    - Session time information

Network Behaviour Analysis Systems

- Similar to the NBID, communication security is important (separate network for management server is preferable)

- NBAS collect data that characterizes the “normal” activity in the network
  - Service information and associated ports
  - Host contact information

Network Behaviour Analysis Systems

- In addition NBAS log information detailed information on incidents
  - Incident type and severity
  - IP addresses
  - Packet headers
  - Communication Statistics

Network Behaviour Analysis Systems

- NBAS can detect
  - Denial of Service attacks
    - Uses bandwidth “norms”
    - May use information on known Denial of Service approaches
  - Scanning
    - Checks flow patterns for different communications layers
  - Worms
    - Checks port usage
    - Host list

Network Behaviour Analysis Systems

- NBAS can detect
  - Anomalous services
    - Based on normal activity definition
    - Involves an application level protocol analysis
  - Unauthorized activity
    - Can be done at
      - User level
      - Service level
- NBAS - good at detection intrusions that generate large amounts of traffic or “abnormal” flow activity

Network Behaviour Analysis Systems

- NBAS detection effectiveness
  - Work well once the attacks that vary from established “normal” network flow activity
  - Detection is delayed until the variation is picked by the analysis
  - Slow attacks may occur for substantial amount of time
  - Balance between number of actual vs false alerts requires long term monitoring and adjustments

Network Behaviour Analysis Systems

- NBAS have some important drawbacks
  - Cannot stop attacks when they start
  - Require a significant amount of resources for flow analysis
  - Require information from network sensors to be available immediately to improve the effectiveness of the detection approach

Network Behaviour Analysis Systems

- NBAS prevention approaches
  - Similar to the NDIS approaches
  - Can be inline, passive or both
  - Can reconfigure sensory and routing equipment
  - May require a predefined security set of rules

Intrusion Detection Systems and Incident Handling 320/520

Host Based Intrusion Detection/Prevention Systems and Network Layer Attacks

Host Based IDS/IPS

- Host based IDS/IPS
  - Focused on a single system rather than a group of connected systems
  - Broader range of target information
  - Components:
    - Agent
    - Management server (often used when compiling data from more than one host)
    - Database server
    - Console

Host Based IDS/IPS

- Agent aim: to protect either a server, client system or service
- Unlike the NBIDS or NBAS, the communication is done via standard network
- If prevention capability is to be provided, this is done typically via a shim
  - Shims can be used to provide access to a wide range of resources
  - Allows for a more effective response and analysis

Host Based IDS/IPS

- Host IDS/IPS collect data on events of interest similar to the NBIDS
  - Incident class and severity
  - Port information
  - User information
  - Application information

Host Based IDS/IPS

- Host Based IDS/IPS Incident Detection
  - Depends on the detection approach used
  - Code based approaches
    - Buffer overflow detection
    - Code behaviour
    - System call analysis
    - Authorized/Unauthorized application list check

Host Based IDS/IPS

- Host Based IDS/IPS Incident Detection
  - Network Based approaches
    - Traffic Analysis
    - Traffic Filtering
  - File System Based approaches
    - File integrity checking
    - File access checking
    - File privileges checking

Host Based IDS/IPS

- Host Based IDS/IPS Incident Detection
  - System and application log analysis based
  - Network setup analysis based

Host Based IDS/IPS

- Host Based IDS/IPS have a number drawbacks
  - Monitoring processes require substantial system resources and often result in a slowdown of the traffic or overall system response
  - Using several approaches to detect possibly malicious behaviour often can lead to false alarms when the overall context is not considered
  - Difficulty to operate with existing security software

Host Based IDS/IPS

- A Host Based IDS can handle a wide range of malicious activities and this is dependent on the detection approach employed
  - Code based - malicious code not allowed to be executed
  - Network analysis based - suspicious traffic can be dropped, file transfers can be stopped

Host Based IDS/IPS

- Filesystem analysis based - access to system critical files can be refused
- Process analysis based - key processes for security purposes (such as running an virus checker in the background) can be restarted if necessary

Network Layer Attacks

- Attacks can target specific communication layers but the overall goal (regardless of the layer used for the attack) is to gain access to restricted resources and/or cause damage to the system
- Network Layer attacks
  - Header abuses
  - Stack exploits
  - Bandwidth saturation

Network Layer Attacks

- Common Information Gathering and Attack Approaches
  - NMAP ICMP Ping - gather information about a system/network
  - IP Spoofing - used to conceal the actual origin of the attack by providing a false address

Network Layer Attacks

- Common Information Gathering and Attack Approaches
  - IP Fragmentation - used to disguise an attack by dividing the malicious activity over multiple fragments which the IDS has to reconstruct in order to determine that attack is underway.

Network Layer Attacks

- Common Information Gathering and Attack Approaches
  - Low TTL values - used to gather information about a network's setup
  - Smurf attack - outdated approach that exploits the ICMP echo request to flood the target with ICMP echo response packets
  - DDoS - attack with the aim of overwhelming the target with packets thus causing problems for the actual communications

Network Layer Attacks

- Common Information Gathering and Attack Approaches
  - Linux Kernel IGMP attack - exploits the IGMP code

Network Layer Attacks

- How handle network layer attacks:
  - Use filtering
  - Routing protocol reconfiguration
  - Traffic analysis

Intrusion Detection Systems and Incident Handling 320/520

Wireless Intrusion Detection/Prevention Systems and Transport and Application Layer Attacks

Wireless Intrusion Detection/Prevention Systems

- Wireless general setup
  - Station - wireless capable devices such as laptops or mobile phones
  - Access point - connects wireless capable devices to distribution system (wired infrastructure)
  - Wireless switch - help managing the connectivity between stations and access points
  - Two types of networks:
    - Ad Hoc
    - Infrastructure

Wireless Intrusion Detection/Prevention Systems

- Wireless IDS/IPS components - similar to wired networked IDS/IPS
  - Sensors have added complexity due to the need to monitor wireless traffic
  - Wireless sensors sample rather than examine all packets - this is due to the fact that wireless communications can be done via multiple channels
  - Sensors regularly switch channels to monitor all communications
  - Wireless sensors come in different variants
    - Dedicated
    - Bundled with the access point
    - Bundled with the wireless switch

Wireless Intrusion Detection/Prevention Systems

- Wireless IDS/IPS sensor location
  - Critical problem because of the extra challenges involved in monitoring wireless traffic
  - Key factors:
    - Physical location security
    - Capture range
    - Wired network access
    - Cost
    - Access point and wireless switch location

Wireless Intrusion Detection/Prevention Systems

- Wireless IDS/IPS collect and store data on wireless device and network organization
- Data related to events of interest is collected
  - Incident gravity
  - Session information
  - Channel information
  - Sensor information

Wireless Intrusion Detection/Prevention Systems

- Wireless IDS/IPS Incident Detection
  - Rogue wireless devices
  - Wireless devices with security gaps
  - Failed access attempts
  - Anomalous communication patterns
  - Information gathering tools (war driving tools)
  - DOS attacks
  - Man-in-the-middle attacks

Wireless Intrusion Detection/Prevention Systems

- Wireless IDS/IPS have some drawbacks:
  - Susceptible to evasion approaches - fragmentation or “fast” attacks are more likely to be successful
  - Cannot detect passive surveillance
  - Can be compromised by insecure wireless protocols
  - Data collected for forensic purposes is only a sample thus understanding an attack approach is considerably more difficult
  - Physical attacks are easier to carry out as the sensors are often located in easily accessible areas

Wireless Intrusion Detection/Prevention Systems

- Wireless IDS/IPS can handle incidents in two ways:
  - Session termination
  - Malicious traffic rejection

Transport Layer Attacks

- Transport Layer Attacks types:
  - Connection resource exhaustion
  - Header abuses
  - Transport stack exploits

Transport Layer Attacks

- Most malicious activity is more focused on information gathering than out and out attacks
  - Port Scans - attempt to determine services available from a target system
    - TCP Scans
      - Ack Scan
      - Syn Scan
      - Idle Scan
      - Null Scan
    - UDP Scans

Transport Layer Attacks

- Port Sweeps - attempt to determine if a service is available on multiple target systems
  - Could be an indicator of an already compromised system
- TCP Prediction Attacks - attack involves the injection of malicious data
- SYN Flood Attack - attack overwhelms target system with modified packets

Application Layer Attack

- Application layer attacks differ in the sense that they do not generally rely on lower layer exploits
- Three types of application layer attacks:
  - Programming bug exploits
  - Trust exploits
  - Resource Exhaustion

Application Layer Attacks

- Buffer Overflow Attacks - relies on programming errors in an application's source code which renders it unable to handle all the data copied into it
  - It enables the hacker to control the execution of the application once the attack has been successful
- SQL Injection Attacks - exploits query for databases
  - Enables the extraction or modification of the database information
  - Can be used to obtain administrator privileges (by resetting the system's password)

Application Layer Attacks

- Phishing attacks - attack tricks legitimate user into disclosing account details
- Backdoor attacks - attack enables the hacker to control a remote target system
  - Only the hacker has access to extra functionality which can lead to very serious consequences (system is used to attack and control other machines)
- Handling application layer attacks is challenging because it encryption and encoding schemes used.

Intrusion Detection Systems and Incident Handling 320/520

SNORT Intrusion Detection System

SNORT Introduction

- Many possible solutions: OSSEC, NAGIOS, NESSUS, SNORT
- SNORT - commonly used free IDS; can fulfill several functions (packet sniffing, system alert and logging)
- SNORT hardware requirements:
  - Aim: to limit packet loss
  - Reasonably fast CPU
  - Large hard drive
  - Network sensors
- Once hardware setup determined, a detailed testing is required of both hardware and software.

SNORT

- SNORT - can be used on multiple platforms
  - UNIX, Windows, Mac OSX, Solaris, NetBSD
  - OS choice depends on the admin skill (UNIX based implementations tend to have a steeper learning curve) and overall version speed
  - Many add-ons available: OinkMaster, SnortReport
- How does it work?
  - Packet Decoders
  - Preprocessors

SNORT

- Detection Engine
  - Rule Matching
  - Thresholding
- Alert and Logging

SNORT

- Rule system is stateless
  - Problem – what if the pattern encompasses situations in which stateful packet inspection is required?
- SNORT's answer? Preprocessors

SNORT

- Snort Preprocessors - add significant analysis strength to Snort
  - Stream4
  - Frag2
  - HTTP_Inspect decode
  - RPC decode
- User can build their own preprocessors
  - Templates are available
  - Need to be linked to Snort

SNORT

- Snort Output Plug-Ins
  - Several plug-ins are provided for multiple reporting formats
  - Data can be stored into databases as well as sent to UNIX sockets
  - User can write their own plug-in
  - Alternative is to write plug-in wrappers

SNORT Rules

- SNORT is highly customizable - the users can define their own sets of rules
  - To handle new traffic patterns
  - Handle newly discovered malicious behaviour
- What is SNORT rule?
  - Set of instructions tailored for specific patterns which trigger predefined actions
  - Components:
    - Header
    - Instruction set
  - Rule usage:
    - Examine and analysis of traffic patterns
    - Fine tune alerts

SNORT Rules

- If a pattern condition cannot be defined, no rule can derived for that pattern!
- Snort rules use variables
  - Syntax is simple

    ```
    var <desired_variable_name> <variable_value>
    ```

  - Variables can be dynamic
- Snort rule headers contain signature information
  - Four categories: action, protocol, source and destination

SNORT Rules

- Examples:
  - var <variable_name> <value>
  - portvar <variable_name><ports>
  - ipvar <variable_name><ip's> - to be used for IPV6 cases
  - var INTERNAL_NET 192.168.1.0/24
  - alert udp any any -> $INTERNAL_NET 53 (msg:"DNS connection";)
  - Variable can be overridden from command line –use the –S switch

SNORT Rules

- Rule – check done in two steps: header + options
- Defines everything that is involved
- Header:
  - Specifies action, protocol, IPs, ports and direction

SNORT Rules

- Example

alert tcp 192.168.1.0/24 any -> 10.1.1.0/24 any (msg:”Internal recon attempt via SA probe”; flags: SA;)

- Header? Required
- Options? Not required

SNORT Rules

- Options:
  - General (commonly used)
    - Msg, sid, classtype, priority
  - Non-payload
    - TTL, fragoffset, sameip, fragbits, tos, flags, flow (established or stateless, to_server or to_client), stateless, seq
  - Payload
    - Content – offset, depth, distance, within, fast_pattern
  - Post-detection – logto, tag

SNORT

- Snort rule enables several types of actions
  - Alert
  - Log
  - Ignore
  - Alert and then apply dynamic rule
- In addition Snort also enable custom rule actions
- What is good rule?
  - No simple answer…
    - It should specific
    - It should precise
    - It should be clear

SNORT

- Performance is key!
  - How?
    - Check number of dropped packets
    - Use 3rd party tools
  - What are the common sense things to do?
    - Rules-set check
    - Logs!

SNORT

- Snort enables configuration tailoring via:
  - Config file
    - Uses a simple format that needs to be strictly followed
  - Command line
- Snort enables correlation of data for intrusion detection and traffic analysis

SNORT

- Snort provides multiple tools for tackling intrusion detection:
  - Swatch
  - SnortSnarf
  - ACID
  - SGUIL

SNORT

- Snort can be combined with Barnyard
- Barnyard - assists Snort with generating alert output
  - Uses Snort output and converts using one of the existing output plug-ins.
  - Allows Snort to do its analysis at a faster rate
  - Can be run in batch mode or continuous processing modes

SNORT

- Snort allows active response rather than just intrusion detection - tools available:
  - Snortsam
  - Fwsnort
  - Snort_inline

Intrusion Detection Systems and Incident Handling 320/520

Incident Handling

Preparation, Response Kit and Documentation

Incident Handling

- Computer Security Incident - what is it?
  - Unauthorized or unlawful action involving a computer system
- What is the aim of incident handling?
  - Coordinated, concise and effective response
- Requires a clear setup and procedure
  - Preparation work is KEY to successful incident handling
  - Unlikely to find multiple identical incidents - many variations possible
  - Response needs to allow for varying incidents and conditions
  - Reports produced need to be clear and specify all pertinent facts

Incident Handling

- Preparation work:
  - Organization level
    - System security
    - User training
    - Data Backup
  - Response team level
    - Build incident response kit
    - Team member training
- Incident response depends on severity of event
  - Requires information gathering (type of event, likely impact)
- Data collection is a key aspect of incident handling

Incident Handling

- Individual system preparation
  - Record file checksum information of key files
    - Use tools such as MD5
  - Enable system and application logging
  - Revise the security defense arrangement of the system
  - Back-up data (to determine if anything is missing)

Incident Handling

- Network preparation
  - Deploy IDS
  - Use encryption on traffic
  - Implement authentication system
  - Develop network topology to enables more effective monitoring

Incident Handling

- Response
  - Legal
  - Administrative
- Event investigation
  - Who?
  - Why?
  - When?
  - How?
  - Where?

Incident Handling

- Data collection and logging
  - Process must ensure data integrity
  - Two types of data
    - Host based data
      - Live data
      - Forensic duplication
    - Network based data
      - Logs
      - Traces

Incident Handling

- Incident Handling Reporting
  - Documentation needs to be done in a timely manner - delays should be avoided
  - Documentation should be clear and easy to understand by all parties involved in the investigation
  - Documentation should be standardized and templates should be derived to enhance and speed up the process of documentation

Incident Handling

- Incident Response Kit
  - Hardware
    - Requires higher end hardware
    - Should enable connectivity with varying systems
    - Disk space is critical especially for larger scale data collection
    - Mobility is key
  - Software
    - Different OS versions
    - Boot disks
    - Software that enables viewing of all types of files
    - Block level copy tools

Incident Handling

- Incident Response
  - Compile information about the incident
    - system details
    - contained or not?
    - any measures applied?
  - Collect evidence
    - Host based
    - Network based
    - Other

Incident Handling

- Incident Response
  - Interview relevant personnel
    - System administrators
    - Managers
    - End users
  - Consider factors that determine the response
    - Has something similar been handled before?
    - Cost?
    - Origin of incident?
    - Legal issues?