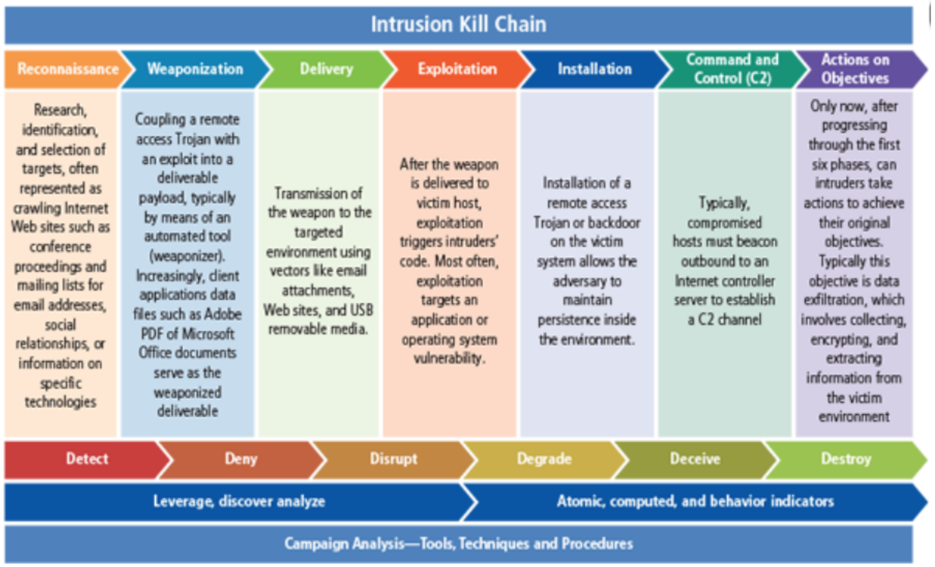
7 - Intrusion Detection and Prevention Systems

- Intrusion: occurs when an attacker attempts to gain entry into an organization's information systems or disrupt their normal operations.
- **IDPS Terminology**
    - Alarm clustering and compaction
    - Alarm filtering
    - Alert or alarm
    - Confidence value
    - Evasion
    - False attack stimulus
    - False negative
    - False positive
    - Noise
    - Site policy
    - Site policy awareness
    - True attack stimulus
    - Tuning
- **Why Use an IDPS?**
    - To identify and report an intrusion
    - Data Collection
    - Attack Deterrence

The Cyberattack and Kill Chain



Intrusion Kill Chain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control (C2)	Actions on Objectives
Research, identification, and selection of targets, often represented as crawling Internet Web sites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies	Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF of Microsoft Office documents serve as the weaponized deliverable	Transmission of the weapon to the targeted environment using vectors like email attachments, Web sites, and USB removable media.	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.	Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel	Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration, which involves collecting, encrypting, and extracting information from the victim environment

Detect
Deny
Disrupt
Degrade
Deceive
Destroy
Leverage, discover analyze
Atomic, computed, and behavior indicators
Campaign Analysis—Tools, Techniques and Procedures

Source: https://countuponsecurity.com/tag/kill-chain/.

- **Types of IDPS**
    - **Network Based**
        - Good design can enable organization to monitor a large network with only a few devices
        - Needs to monitor all network traffic
            - Can become overwhelmed by large amounts of traffic
        - Cannot analyze encrypted packets
        - Cannot tell if an attack was successful
        - Compares measured activity to known signatures in knowledge base
        - Uses special implementation of TCP/IP stack
            - NIDPS looks for invalid packets during the protocol stack verification
            - Higher-order protocols are examined for unexpected packet behavior or improper use during application protocol verification
        - Not usually susceptible to attack
    - **Wireless NIDPS**
        - Monitors and analyzes wireless network traffic.
        - Cannot monitor TCP UDP traffic
        - Has following issues

        - Physical security
        - Sensor range
        - Access point and wireless switch locations
        - Wired network connections
        - Cost
        - AP and wireless switch locations
    - Events that can be detected:
        - Unauthorized WLANS and WLAN devices
        - Poorly secured WLAN devices
        - Unusual usage patterns
        - The use of wireless network scanners
        - DoS attacks and conditions
        - Impersonation and main-in-the-middle attacks.
- **Network Behavior Analysis-System**
    - Identify problems related to the flow of network traffic.
        - Source and Dest IP address
        - Source and Destination TCP or UDP ports or ICMP types and codes
        - Number of packets and bytes transmitted in the session.
        - Starting and ending timestamps for the session.
    - Can commonly detect
        - DoS attacks
        - Scanning
        - Worms
        - Unexpected application services
        - Policy Violations
    - Prevention Capabilities
        - Passive only
            - Ending the current TCP session.
        - Inline only
            - Performing inline firewalling.
        - Both passive and inline
            - Reconfiguring other network security devices
            - Running a third-party program or script.
- **Host Based**
    - HIDPS resides on a particular computer or server.
        - Monitors activity only on that system
    - Can access encrypted information traveling over the network
    - Functions on host system, where encrypted traffic will have been decrypted and is available for processing.

- Monitors system config databases and config files.
  - Triggers an alert when file attributes change, new files created or existing files are deleted
- Can monitor system logs for specific events.
  - Creates its own log file for even if attackers modify system logs
- Not affected by use of switched network protocols
- Disadvantages:
  - More management issues
  - Vulnerable both to direct attacks and attacks against the host operating system
  - Does not detect multihost scanning, nor scanning of non-host network devices
  - Susceptible to some DoS attacks
  - Can use large amounts of disk space
  - Can inflict performance overhead on its host systems.

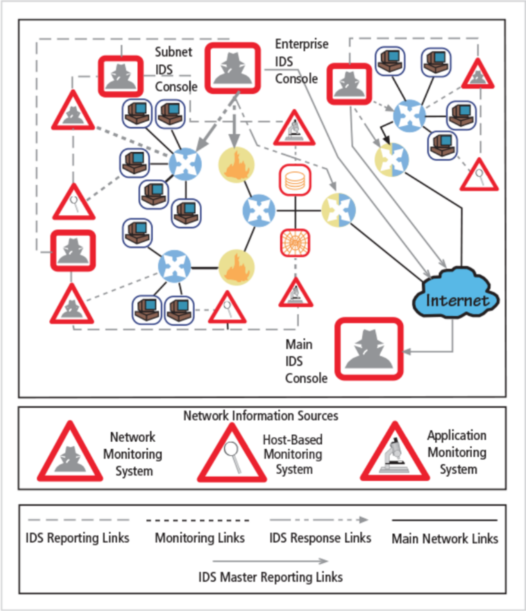
- **IDPS Detection Methods**
  - **Signature Based Detection (knowledge based detection)**
    - Examines network traffic in search of patterns that match known signatures or pre-configured attack patterns
    - Widely used as many attacks have known signatures.
    - Attacks evolve over time and the attack patterns must be added to the IDPS's database of signatures.
  - **Anomaly Based Detection**
    - Collects statistical summaries by observing traffic that is known to be normal.
    - IDPS can detect new types of attacks.
    - Requires much more overhead and processing capacity than signature-based detection
    - May generate false positives.
  - **Stateful Protocol Analysis**
    - The system compares known normal or benign protocol profiles against observed traffic.
    - Can examine authentication sessions for suspicious activity or for attacks that incorporate unusual commands
    - Stores and uses relevant data detected in a session to identify intrusions involving multiple requests/responses
      - Allows IDPS to better detect specialized, multisession attacks (also called deep-packet inspection
    - Requires heavy processing
  - **Log File Monitors**
    - Reviews log files looking for patterns and signatures that may indicate an attack or intrusion is in the process or has already occurred.
    - Similar to NIDPS
    - Patterns that signify an attack may be much easier to identify when the entire network and its systems are viewed as a whole.
    - Requires considerable resources since it involves the collection, movement, storage, and analysis of large quantities of log data.
- **IDPS Response Behavior**
  - May be classified as active or passive
    - Active

- Collecting additional information about the intrusion, modifying the network environment and taking action against the intrusion
- Passive
    - Setting off alarms or notifications and collecting passive data through SNMP traps.
- Response Options
    - Audible/visual alarm
    - SNMP traps and plugins.
    - Email message
    - Phone, pager, or SMS message
    - Log entry
    - Evidentiary packet dump
        - Encrypted data evidence to be used later in court…
    - Take action against the intruder.
    - Launch program
    - Reconfigure firewall

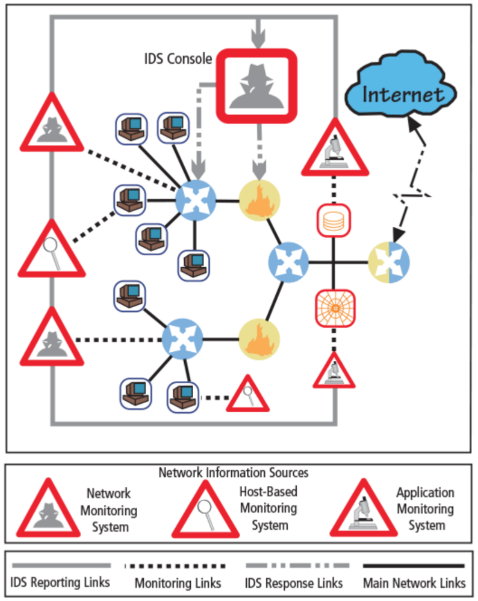
- **Selecting IDPS Approaches and Products**
- **Strengths and Limitations of IDPSs**
    - Strengths
        - Monitoring and analysis of system events and user behaviors
        - Testing the security states of system configurations
        - Baselining the security state of a system, then tracking any changes to that baseline.
        - Recognizing patterns of system events that correspond to known attacks
        - Recognizing patterns of activity that statistically vary from normal activity
        - Manage operating system audit and logging mechanisms and the data they generate
        - Alerting appropriate staff by appropriate means when attacks are detected
        - Measuring enforcement of security policies encoded in the analysis engine
        - Providing default information security policies
        - Allowing people who are not security experts to perform important security monitoring functions
    - Limitations
        - Can't compensate for weak or missing security mechanisms
        - Not instantaneous detecting, reporting and responding when there is a heavy network or processing load
        - New attacks happen all the time
        - Sophisticated users can circumvent.
        - Needs human intervention for automatic investigation
        - Cannot resist all attacks that are intended to defeat or circumvent them
        - Cannot compensate for problems with the fidelity of information sources
        - Trouble dealing effectively with switched networks
- **Deployment and Implementation of an IDPS**

- Control Strategies
    - Centralized Control Strategy
        - All IDPS control functions are implemented and managed in a central location
    - Fully Distributed Control Strategy
        - All control functions are applied at the physical location of each IDPS component
    - Partially Distributed Control Strategy
        - Combines the two, while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks

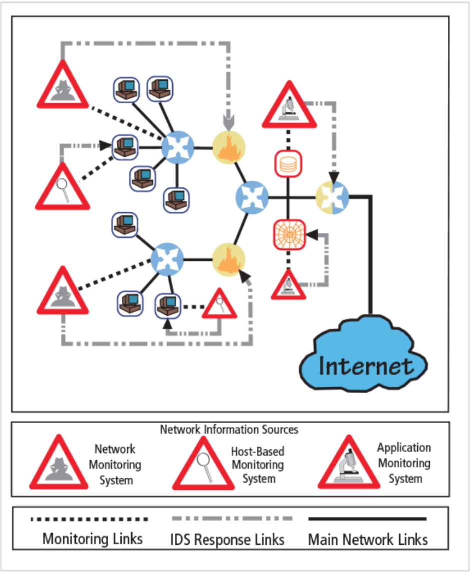
Partially Distributed IDPS Control*


Subnet IDS Console
Enterprise IDS Console
Internet
Main IDS Console
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
IDS Reporting Links
Monitoring Links
IDS Response Links
Main Network Links
IDS Master Reporting Links

Centralized IDPS Control*

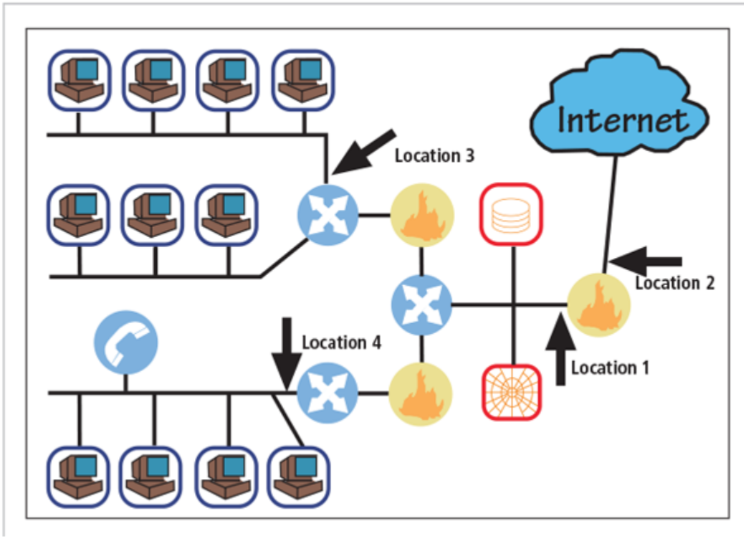

IDS Console
Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
IDS Reporting Links
Monitoring Links
IDS Response Links
Main Network Links

Fully Distributed IDPS Control*


Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
Monitoring Links
IDS Response Links
Main Network Links

- **Deployment**
    - NIDPS
        - Behind each external firewall, in the network DMZ
        - Outside an external firewall
        - On major network backbones
        - On critical subnets
    - HIDPS
        - Start with most critical systems first
    - Both are used in tandem to cover the individual systems that connect to an organization's network and the networks themselves.

Network IDPS Sensor Locations*



- **Measuring the Effectiveness of IDPSs**

    - Thresholds
    - Blacklists and Whitelists
    - Alert Settings
    - Code viewing and editing

Honeypots, Honeynets and Padded Cell Systems

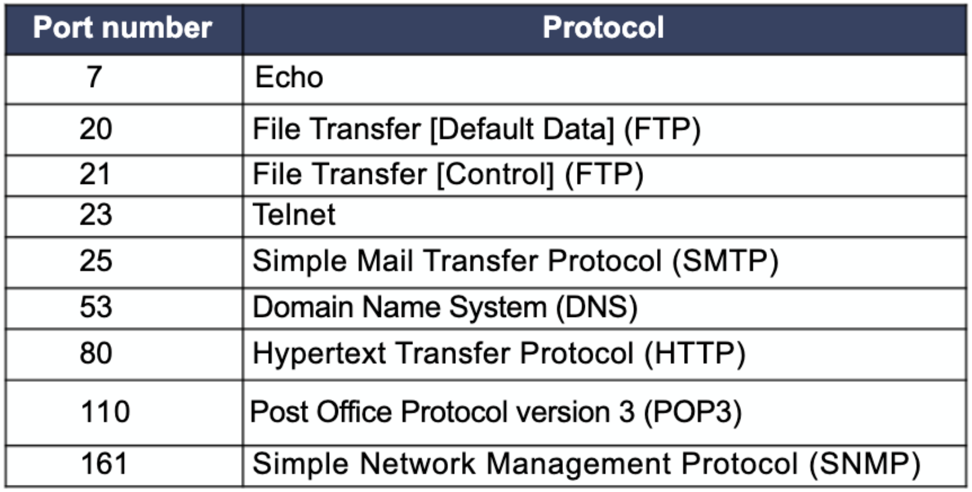
- **Honeypots**
    - Decoy systems designed to lure potential attackers away from critical systems.
- Honeynets
    - A network of honeypots
- **Padded Cell system**
    - A hardened honeypot that operates with a traditional IDPS.
    - When attacker detected the system seamlessly transfers them to a special simulated environment where they can cause no harm
- **Trap-and-Trace Systems**
    - Used in conjunction with honey pots and used to trace attacker back to its source
    - Cant be used unless you a service provider attempting to prevent misuse and:
        - It is used for systems maintenance and testing
        - It is used to track connections or
        - You have permission from the user of the service.
        - Enticement is legal, entrapment is not
        - Must obtain a court order under section 3123 of Title 18, US Code Chapter 206 or under Foreign Intelligence Surveillance Act of 1978

- **Active Intrusion Prevention**
    - LaBrea takes up unused IP address space to pretend to be a computer and allow attackers to complete a connection request, but then holds connection open

Scanning and Analysis Tools

- **Footprinting:**
    - Process of collecting publicly available information about a potential target
- **Fingerprinting**
    - Systematic survey of target organizations Internet addresses collected during the footprinting phase to identify network services offered by hosts in that range
    - Reveals useful information about internal structure and nature of the target system or network to be attacked
- **Port Scanners**
    - Tools that can perform generic scans or those for specific types of computers, protocols, or resources.

- **Firewall Analysis Tools**
    - Nmap -I (nmap idle)
    - Firewalk
        - Uses incrementing TTL packets to determine the path into a network as well as the default firewall policy.
    - HPING
        - Modified Ping client.
- **Operating System Detection Tools**
    - XProbe
        - Sends many different ICMP queries to the target host.
        - XProbe matches the responses from the targets TCP/IP stack with its own internal database of responses
- **Vulnerability Scanners**
    - Active vulnerability scanners
        - Examine networks for highly detailed information.
        - Initiates traffic on the network to determine security holes.
        - Nessus
        - Core Impact
        - GFI LanGuard
        - MBSA
        - Nexpose
        - Nipper
        - OpenVAS
        - QualysGuard
        - Retina
        - Secunia PSI
        - SAINT
        - Metasploit
    - Passive vulnerability scanners
        - Listens on the network and identifies vulnerable versions of both server and client software.
        - Tenable Network Security: Passive Vulnerability Scanner (PVS)
        - Casaba: Watcher Web Security Scanner



Port number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

- **Packet Sniffers**
    - Network Protocol Analyzer.
    - Can be used to eavesdrop on network traffic.
    - Sniffer
        - Commercially available
    - Snort
        - Open Source
    - Wireshark

- To use a packet sniffer legally you have to
    - Be on a network that the organization owns
    - Be under direct authorization of the networks owners, and
    - Have knowledge and consent of the contents creators
- Ettercap
    - ARP spoofing and session hijacking

- **Wireless Security Tools**
    - Should include
        - Ability to sniff wireless traffic
        - Scan wireless hosts
        - Asses the level of privacy or confidentiality afforded on the wireless network
        - Tools identified by Sectools.org
            - Aircrack
                - Wireless network protocol cracking tool
            - Kismet
                - Wireless network protocol sniffer, network detector, and IDPS
                - Works by passively sniffing the networks
            - NetStumbler
                - Freeware Windows file parser
            - inSSIDer
                - Enhanced scanner for Windows, OSX, and Android
            - KisMac
                - GUI passive wireless stumbler for OSX (variation of Kismet)
            - AirSnare
                - Monitors the airwaves for any new devices or access points.

Ch. 7 Review Questions

1. What common security system is an IDPS most like? In what ways are these systems similar?
    a. Burglar alarm and they are similar in the way that they alert/warn when an intrusion event has happened.
2. How does a false positive alarm differ from a false negative alarm? From a security perspective, which is less desirable?
    a. A false negative is when an intrusive event was failed to be detected whereas a false positive attack in an event where an attack was detected but no attack actually occurred. The false negative is the least desired as the whole point of IDPS is to detect intrusions.
3. How does a network-based IDPS differ from a host-based IDPS?
    a. NDIPS works on the network level and monitors traffic across the network. HIDPS is installed on host machines and analyzes traffic on that system. HIDPS can analyze encrypted traffic (NIDPS cant) as well as monitor/analyze log files.
4. How does a signature-based IDPS differ from a behavior-based IDPS?
    a. Signature-based IDPS detects attacks that have well-known signatures or behaviors. Common attacks have similar attacks and can be detected.
    b. Behavior-based compares current data and traffic patterns to a normal baseline.
5. What is a monitoring (or SPAN) port? What is it used for?
    a. A SPAN port is a specially configured connection on a network that views all traffic moving through a device/switch and replicates it to be analyzed by an IDPS or other analysis software.
6. List and describe the three control strategies proposed for IDPSs.
    a. Centralized - All IDPS control functions are implemented and managed in a central location
    b. Fully Distributed - All control functions are applied at the physical location of each IDPS component
    c. Partially Distributed - Combines the two, while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks.
7. What is a honeypot? How is it different from a honeynet?

    a. A decoy system designed to lure potential attackers away from critical systems and encourage attacks against themselves. A honey-net is a network of honeypots on a subnet.

8. How does a padded cell system differ from a honeypot?
    a. A padded cell is a hardened honeypot that operates with a traditional IDPS. Once an intrusion is detected they are seamlessly transferred to a special simulated environment.
9. What is network footprinting?
    a. Footprinting is the collecting of publicly available information about a potential target, i.e. internet addresses owned by target.
10. What is network fingerprinting?
    a. Systematic survey of target org's internet addresses collected during footprinting phase to ID the network services offered by the hosts in that range. Reveals useful information about internal structure and nature of the target system or network to be attacked.
11. How are network footprinting and network fingerprinting related?
    a. Network fingerprinting uses network footprinting to dig deeper into internal structures of the target.
12. Why do many organizations ban port scanning activities on their internal networks?
    a. Port scanning is used by attackers to detect open ports that may be used for exploitation and gain access/control of the network
13. Why would ISPs ban outbound port scanning by their customers?
    a. To prevent attacks like DoS and DDoS and potential lawsuit.s
14. What is an open port? Why is it important to limit the number of open ports to those that are absolutely essential?
    a. An open port is an open communication to the system/computer/network. Attackers can use open ports to send commands to a computer and potentially gain access to a server
15. What is a system's attack surface? Why should it be minimized when possible?
    a. Features/functions of a system that are exposed to attackers/unauthorized users. A large attack surface means there are more avenues for the attacker to gain access/control of your network.
16. What is a vulnerability scanner? How is it used to improve security?

   a. A software program that scans a range of network addresses and port numbers for open services. They can help you identify weaknesses in your organization and fix them.

17. What is the difference between active and passive vulnerability scanners?
    a. An active vuln scanner initiates traffic on the network for highly detailed information to determine security holes. A passive vuln scanner listens on the network and identifies vulnerable versions of both server and client software.
18. What is Metasploit Framework? Why is it considered riskier to use than other vulnerability scanning tools?
    a. Metasploit is a software tool that is a collection of exploits in one interface which allows pen-testers to have an automated/smoother workflow.
19. What kind of data and information can be found using a packet sniffer?
    a. Packet sniffers collect packets going across a network and analyzes them.
20. What capabilities should a wireless security toolkit include?
    a. Packet sniffer, ability to analyze network, scan wireless hosts and assess the level of privacy or confidentiality afforded on the wireless network.