

# Intrusion Detection Systems and Network Security



## Chapter 13

### Background

- A layered network security approach starts with a well-secured system:
  - Up-to-date application and operating system patches.
  - Well-chosen passwords.
  - The minimum number of services running.
  - Restricted access to available services.
  
- Layers of protective measures, such as antivirus products, firewalls, sniffers, and intrusion detection systems, can be added.



## Background

- Intrusion detection systems (IDS)
  - One of the more complicated and interesting types of network/data security devices
  - An IDS is to the network as burglar alarms are to the physical world - it watches and alerts you when something bad happens.
  
- We will examine:
  - The various types of intrusion detection systems.
    - How they work.
    - The benefits and weaknesses of specific types.
    - The future of these systems.
  
- Some more topics:
  - Honeypots
  - Incident response

3



## Intrusion Detection Terms and Concepts

- Intrusion
  - Any use or attempted use of a system that exceeds authentication limits
  
- Intrusion detection system (IDS)
  - Software/hardware that monitors activity on the system or network
  - Delivers an alert if it notices suspicious activity

4



## Intruders

- Intruders – Both external or internal
  - External intruders are hackers or crackers
  - Internal intruders are more common and very dangerous
  
- An organizational security policy should state what steps will be taken to handle intrusions

5



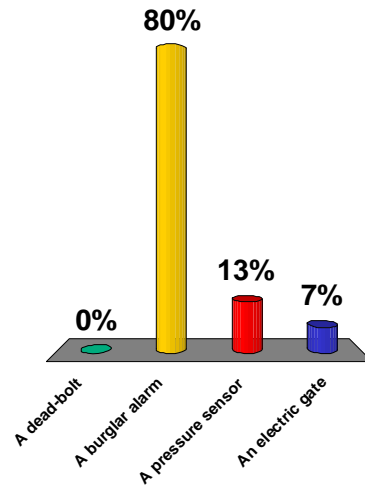
## Dealing with Intruders

- Block and ignore
  - Simplest tactic for handling intrusions
  - Block the intruder and address the vulnerability
  - Don't take any further action
- Block and investigate
  - Block the intruder and address the vulnerability
  - Collect evidence and try to determine the intruder's identity
  - Although this may result in finding and stopping the intruder, it can be costly and time-consuming
- Honeypot (bait the intruder)
  - Allow the intruder to access a part of your network
  - Try to catch the intruder while he/she explores
  - This is a potentially dangerous approach
    - The intruder does have at least partial access
    - Crackers may become interested in your site

6

## An IDS is most like

- A. A dead-bolt
- 😊 B. A burglar alarm
- C. A pressure sensor
- D. An electric gate



7

## IDS

- Purpose:
  - Identify suspicious or malicious activity.
  - Note activity that deviates from normal behavior.
  - Catalog and classify the activity.
  - Respond to the activity.
- Principles:
  - Must run unattended for extended periods of time
  - Must stay active and secure
  - Must be able to recognize unusual activity
  - Must operate without unduly affecting the system's activity
  - Must be configurable

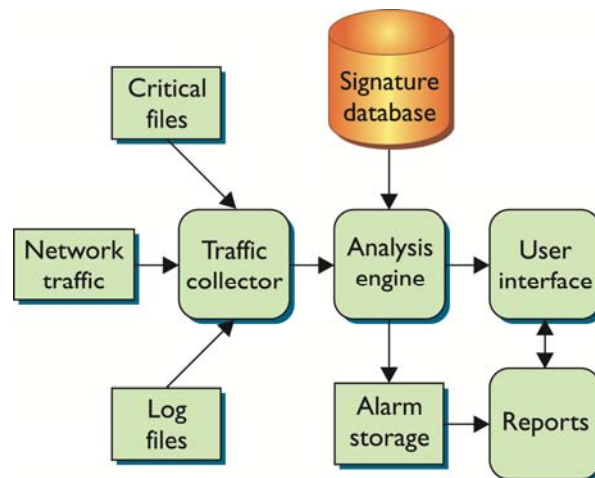
8

## IDS Components

- **Traffic collector**
  - Collects activities/events for the IDS to examine.
    - On a host-based IDS, this could be log files, audit logs, or traffic coming to or leaving a specific system.
    - On a network-based IDS, this is typically a mechanism for copying traffic off the network link—basically functioning as a sniffer.
- **Analysis engine:**
  - Examines the collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database.
- **Signature database:**
  - Is a collection of patterns and definitions of known suspicious or malicious activity
- **User interface and reporting:**
  - Is the component that interfaces with the human element, providing alerts when appropriate and giving the user a means to interact with and operate the IDS.

9

## IDS Components



10



## Tuning an IDS

---

- Most IDSs can be “tuned” to fit a particular environment.
  - Signatures may be turned off – the IDS will not to look for certain types of traffic.
  - Alarm levels can be adjusted depending upon certain types of traffic.
  - Some IDS also allow users to “exclude” certain patterns of activity from specific hosts.

11



## Types of IDS

---

- Host-based IDS (HIDS)
- Network-based IDS (NIDS)
- Distinguished by detection method:
  - Signature-based IDS - Relies heavily on a predefined set of attack and traffic patterns called signatures.
  - Anomaly-based (heuristic) IDS - Monitors activity and attempts to classify it as either “normal” or “anomalous.”



## IDS Categories

- **Host-Based IDS**
  - Concerned only with activity on an individual system
  - Usually has no visibility into the activity on the network or systems around it.
- **Network-Based IDS**
  - Has visibility only into the traffic crossing the network link it is monitoring
  - Typically has no idea of what is happening on individual systems.
- **Distinguished by detection method:**
  - **Signature-based IDS** - Relies heavily on a predefined set of attack and traffic patterns called signatures.
  - **Anomaly-based (heuristic) IDS** - Monitors activity and attempts to classify it as either “normal” or “anomalous.”

13



## Host-Based IDS

- Operates in:
  - Real time, looking for activity as it occurs.
  - Batch mode, looking for activity on a periodic basis.
- May be self-contained, but many of the newer commercial products have been designed to report to and be managed by a central system.
- Host-based systems
  - Use local system resources to operate.
  - Examines log files, audit trails, and network traffic coming in to or leaving a specific host.

14



## Host based IDS Focus

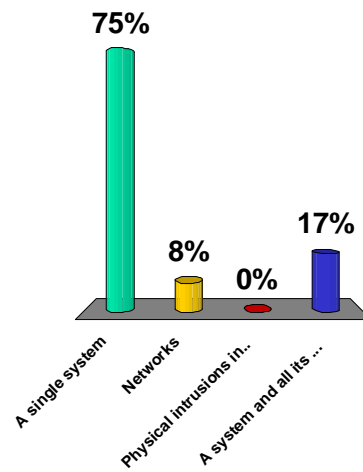
- Focus on the log files or audit trails from the local operating system.
  - The IDS looks for hostile actions or misuse activities, such as:
    - Logins at odd hours
    - Login authentication failures
    - Adding new user accounts
    - Modification or access of critical system files
    - Modification or removal of binary files (executables)
    - Starting or stopping processes
    - Privilege escalation
    - Using certain programs

15



## Host-based IDSs monitor ...

- 😊 A. A single system
- B. Networks
- C. Physical intrusions into facilities
- D. A system and all its surrounding systems

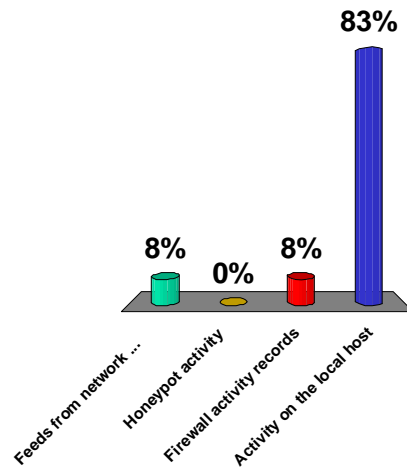


16



## What does a host-based IDS examine

- A. Feeds from network capture devices such as sniffers
- B. Honeypot activity
- C. Firewall activity records
- 😊 D. Activity on the local host



17

## IDS Logical Layout

- Most of the Host-based intrusion detection systems operate in a similar fashion.
- The **traffic collector** pulls in information for the other components, such as the analysis engine.
  - It pulls already generated data from the local system – error messages, log files, and system files.
  - It is responsible for reading files, selecting items of interest, and forwarding them to the analysis engine.
  - On some host-based systems, it also examines specific attributes of critical files such as file size, date modified, or checksum.

18



## IDS Analysis Engine

- Analysis engine:
  - A sophisticated decision and pattern-matching mechanism.
  - Looks at data given to it by the traffic collector and matches it to known patterns of activity stored in the signature database.
  - If the activity matches a known pattern, the analysis engine reacts with an alert or alarm.
  - Capable of remembering how the current activity compares to historic or future traffic, so that it may match more complicated, multi-step malicious activity patterns.
  - Needs to be capable of examining traffic patterns as quickly as possible.
    - The longer it takes to match a malicious pattern, the less time the IDS or human operator has to react to malicious traffic.

19



## IDS Signature Database

- The signature database is a collection of predefined activity patterns that have already been identified and categorized as activity patterns typical of suspicious or malicious activity.
  - When the analysis engine has a traffic pattern to examine, it compares it to the signatures in the database.

20



## User Interface

- It is the visible component of the IDS—the part that humans interact with.
  - Independent of the type and complexity, the interface allows users to interact with the system by:
    - Changing parameters
    - Receiving alarms
    - Tuning signatures and response patterns

21



## Host-Based IDS

- Advantages:
  - Operating system-specific.
    - More detailed signatures.
  - Reduced false positive rates.
  - Examination of data after decryption.
  - Application specific.
  - Alarm may impact determination of a specific system.
- Disadvantages:
  - Need for an IDS process or application on every host to be watched.
  - An IDS has a high cost of ownership.
  - An IDS uses local system resources.
  - An IDS has a focused view and cannot relate to activity around it.
  - A locally logged IDS may be compromised or disabled.

22



## Sub-classification -Active vs. Passive Host IDS

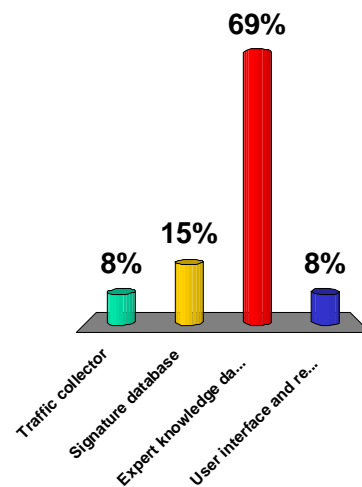
- Sub-classification
  - how they examine the activity around them and whether or not they interact with that activity.
- Passive system
  - Watches the activity, analyzes it, and generates alarms.
  - Does not interact with the activity itself in any way.
  - Does not modify the defensive posture of the system to react to the traffic.
- An Active IDS
  - Contains the same components and capabilities as the passive IDS.
  - Also reacts to the activity it is analyzing.

23



## Which of the following is NOT a component of an IDS

- Traffic collector
- Signature database
- ☺ ■ Expert knowledge database
- User interface and reporting



24



## Network-Based IDS

---

- Network-based IDS
  - Focuses on network traffic.
    - Bits and bytes traveling through cables interconnecting the systems.
  - Examines network traffic as it passes by.
  - Must be able to analyze traffic by protocol, type, amount, source, destination, content, and traffic already seen.
  - The analysis must happen quickly.
    - The IDS must be able to handle traffic at whatever speed the network operates to be effective.

25



## Network-Based IDS

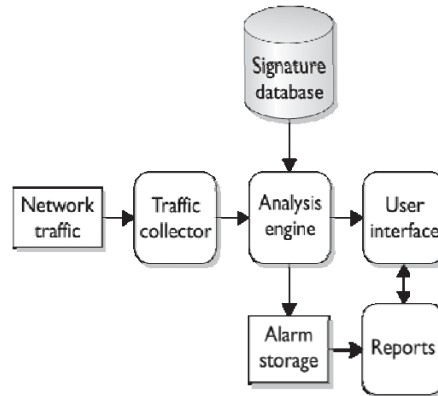
---

- What does it look for?
  - Like host-based systems, a network-based IDS looks for activities that represent hostile actions or misuse.
    - Denial-of-Service attacks
    - Port scans or sweeps
    - Malicious content in the data payload of a packet or packets
    - Vulnerability scanning
    - Trojans, viruses, or worms
    - Tunneling
    - Brute-force attacks

26

## Network IDS Components

- The components of a network-based intrusion detection system are similar to those of a host-based system.
  - Traffic collector
  - Analysis engine
  - Signature database
  - User interface



27

## Network IDS Traffic Collector

- The traffic collector in a network-based IDS pulls traffic from the network.
  - It behaves the same way as a network traffic sniffer.
    - It pulls every packet from the connected network.
- The traffic collector attaches itself logically to a network interface card (NIC) and instructs the NIC to accept every packet it can.
  - A NIC that accepts and processes every packet regardless of the packet's origin and destination is said to be in “promiscuous” mode.

28



## Network IDS Analysis Engine

- It has the same function as its host-based counterpart, with substantial differences.
  - The network analysis engine must be capable of collecting packets and examining them individually.
    - If necessary, it reassembles them into an entire traffic session.

29



## Analysis Engine Pattern Matching

- Patterns and signature matching is more complicated than host-based signatures.
  - The analysis engine must remember what traffic preceded the traffic currently being analyzed to determine whether or not that traffic fits a larger pattern of malicious activity.
- The network-based analysis engine must be able to keep up with the flow of traffic on the network, rebuilding network sessions and matching patterns in real time.

30



## Network IDS Signature Database

- The network-based IDS signature database is usually larger than host-based IDS.
  - To examine network patterns, the IDS must recognize traffic targeted at different applications and operating systems as well as traffic from a wide variety of threats such as worms, assessment tools, and attack tools.
  - Some of the signatures are large.
    - The IDS must examine network traffic occurring in a specific order over a period of time in order to match a particular malicious pattern.

31



## Advantages and Disadvantages

- Advantages and Disadvantages of NIDS
  - NIDS advantages
    - It takes fewer systems to provide IDS coverage.
    - Deployment, maintenance, and upgrade costs are usually lower.
    - A network-based IDS has visibility into all network traffic and can correlate attacks among multiple systems.
  - NIDS disadvantages
    - It is ineffective when traffic is encrypted.
    - It cannot see traffic that does not cross it.
    - It must be able to handle high volumes of traffic.
    - It does not know about activity on the hosts themselves.

32





## Sub-classification : Active vs. Passive NIDS

- Network-based IDS can be distinguished by how they examine the traffic and whether or not they interact with that traffic.
  - Passive IDS
    - Watches the traffic, analyzes it, and generates alarms.
    - But does not interact with the traffic itself in any way or modify the defensive posture of the system to react to the traffic.
  - Active IDS
    - Contains all the same components and capabilities of the passive IDS with one critical addition.
    - Reactive response to an attack such as a **TCP reset**.

33



## Defense via TCP Reset

- A common defense for an active IDS is to send a TCP reset message.
  - Within the TCP protocol, the reset message (RST) essentially tells both sides of the connection to drop the session and stop communicating immediately.
- One serious drawback of a reset message is that it affects only the current session and there is nothing to prevent the attacker from coming back and trying again.
  - Although temporary, sending a reset message is usually the only defensive measure implemented on IDS deployments.
    - The fear of blocking legitimate traffic and disrupting business processes, even for a few moments, outweighs the perceived benefit of discouraging potential intruders.

34



## Using Rules and Setting Thresholds for Detection

- A rule tells the IDS which packets to examine and what action to take
  - Similar to a firewall rule
  - Alert tcp any any -> 192.168.1.0/24 111  
(content:"|00 01 86 a5|";msg:"mountd access");
    - Alert specifies the action to take
    - Tcp specifies the protocol
    - Any any 192.... specifies the source and destination within the given subnet
    - 111 specifies the port
    - Content specifies the value of a payload
    - Msg specifies the message to send

35



## Using Rules and Setting Thresholds (continued)

- A threshold is a value that represents the boundary of normal activity
- For example, if the login failure threshold is three, the IDS takes some action after the third failed attempt
  - Action might be to lock the account and notify an administrator
- Other thresholds include file I/O, network activity, administrator logins and actions

36



## Exploring a Typical IDS

- Snort is an example of an IDS
  - A highly configurable packet sniffer, Snort analyzes network traffic in real time
  - Freely available
  - Originally written for UNIX, but now available for Windows also
  - Sniffs a packet from the network
    - Preprocessor looks at the packet header and decides whether to analyze it further
    - If so, the detection engine compares pattern from rules to the packet payload
    - If the payload matches, the appropriate action is taken
  - Can be used in a plain packet sniffer mode or in full IDS mode
  - Has numerous options that are used to configure its activity

37



## Operation of a NIDS

- **Port Scan:**
  - A reconnaissance activity performed by a hacker to find out about the systems they wish to attack.
  - Using various tools, attacker attempt to connect to various services (Web, FTP, SMTP, etc.) to see if these exist on the intended target.
  - In normal network, a single user might connect to the FTP service provided on a single system.
  - During a port scan, attacker may attempt to connect to the FTP service on every system.
  - As the attacker's traffic pass by the IDS, this pattern of attempting to different services on different systems is noticed.
  - When IDS compares the activity to its signature database, it will match this traffic against the port scanning signature & generate an alarm.

38

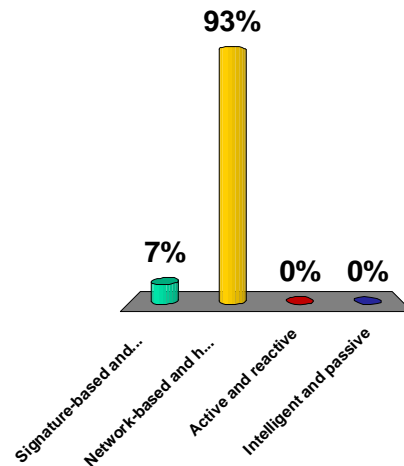
## Operation of a NIDS

- **Ping of death.**
  - Certain operating systems could be crashed by sending a very large ICMP echo request packet to the system.
  - The vulnerable operating system is not able to handle the requests and locks up.
  - This simple traffic pattern is easily identified by NIDS that looks for ICMP packets over a certain size.

39

## What are the two main types of intrusion detection systems

- A. Signature-based and event-based
- B. Network-based and host-based
- C. Active and reactive
- D. Intelligent and passive



40



## IDS and Signatures

- Signature set
  - A critical element of any good intrusion detection system
  - Used when analyzing traffic or events.
  - It is a set of patterns that determines if activity is potentially hostile.
  - This may be simple or complicated, depending on the activity highlighted.
  - IDS must have a decent signature base with examples of known, undesirable activity
- **If an IDS matches the current events against a signature, it may be successful**
  - It has correctly matched the current event with a known signature and reacted accordingly (usually with an alarm or alert of some type).
- **Response**
  - No way for an IDS to know the true intent behind an activity and determine whether or not it is benign or hostile.
  - Therefore, the IDS can react only as it has been programmed

41



## Signature Characteristics

- Signatures can be divided into two main groups:
  - **Content-based signatures**
    - Simplest since they look at the content of network packets or log entries.
    - Easy to build.
    - Look for something simple such as a certain string of characters or a certain flag set in a TCP packet.
  - **Context-based signatures**
    - More complicated since they match large patterns of activity and examine how certain types of activities fit into the other activities going on around them.
    - Address the question “how does this event compare to other events that have already happened or might happen in the near future?”
    - More difficult to analyze and take more resources to match.
    - IDS must “remember” past events to match certain context signatures.

42

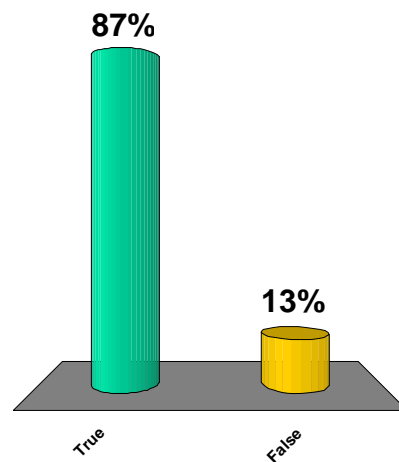
## False Positives and Negatives

- IDS Limitation - Its signature set.
  - Can match only the activity for which it has stored patterns.
- False positive:
  - An IDS matches a pattern and generates an alarm for benign traffic, meaning the traffic was not hostile and not a threat, but was classified
  - In other words, the IDS matched a pattern and raised an alarm when actually not needed.
- False negative:
  - Hostile activity that does not match an IDS signature and, therefore, goes undetected
  - The IDS is not generating any alarms, even though it should be, giving a false sense of security.

43

A false positive is when a IDS generates an alarm when no attack has occurred.

1. True
2. False



44



## IDS Models

- IDS Model
  - A method for examining behavior so that the IDS can determine if that behavior is “not normal” or in violation of established policies.
  
- Additional way to classify IDS: Based on the detection model they use:
  - **Anomaly detection model**
    - Detection based off variances from “normal” behavior
  - **Misuse detection model**
    - Looks for suspicious activity or activity that violates a policy
    - Less complex than anomaly detection
    - More efficient than anomaly detection

45



## Anomaly Detection Model

- The intrusion detection system must know what “normal” behavior on the host or network being protected really is.
  - **Once the “normal” behavior baseline is established, the IDS can then identify deviations from the norm, which are further scrutinized to determine if that activity is malicious.**
  
- Profile Building
  - Building the profile of normal activity is usually done by the IDS.
  - Done with some input from security administrators, and can take days or months.

46



## Why Anomaly Detection

- **Anomaly detection was developed to make the system capable of dealing with variations in traffic and better able to determine which activity patterns were malicious.**
  - IDS must be flexible and capable enough to account for things such as new systems, new users, and movement of information resources
  - A perfect anomaly-based system ignores patterns from legitimate hosts and users but still identify those patterns as suspicious should they come from a potential attacker.
  - Most anomaly-based systems suffer from high false positives, especially during the “break-in” period while it is learning the network.
  - An anomaly-based system is not restricted to a specific signature set and is far more likely to identify a new exploit or attack tool that would go unnoticed by a traditional IDS.

47



## Misuse Detection Model

- Misuse detection model
  - The IDS looks for suspicious activity or activity that violates specific policies and then reacts as it has been programmed.
  - More efficient model.
    - It takes fewer resources to operate
    - does not need to learn what “normal” behavior is
    - generates an alarm whenever a pattern is successfully matched.
  - Greatest weakness
    - Reliance on a predefined signature base
    - any activity, malicious or otherwise, that the misuse-based IDS does not have a signature for will go undetected.

48



## Preventative IDS

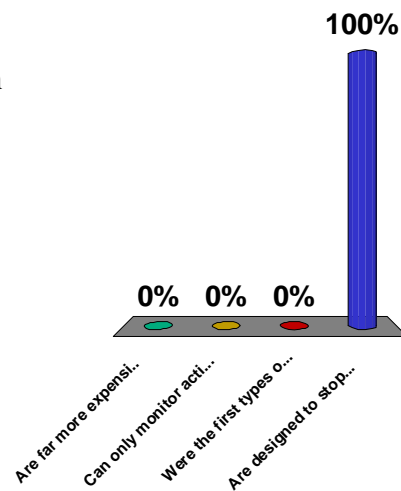
### ■ Preventative IDS

- Designed to both identify malicious activity and prevent it from having any impact on the network and information systems.
- The simple concept
  - Identify bad traffic and make sure it does not do any harm.
  - A preventative IDS may see an attacker attempting to execute a buffer overflow on a local system and will intercept the attacker's system call to prevent it from executing.
- Typically, a hybrid system, having both network-based and host-based portions.
  - The host-based portion serves as a security wrapper for the protected system, catching known, malicious patterns and stopping the attack before it is allowed to execute and affect the local system.
  - The network-based portion operates in a similar manner catching the malicious activity and preventing it from reaching the intended target.

49

## Preventative intrusion detection systems

- A. Are far more expensive and effective than other types
- B. Can only monitor activity on the host itself
- C. Were the first types of IDSs
- D. Are designed to stop malicious activity from occurring

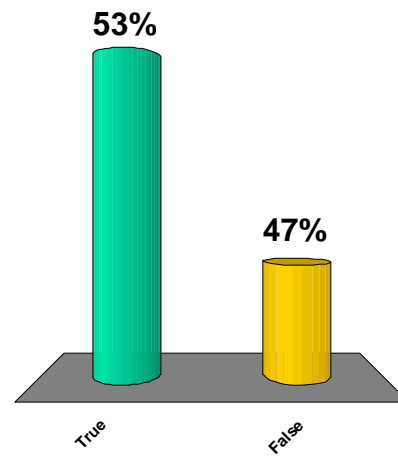


50



A signature database is a collection of patterns used to determine whether or not the activity is hostile

1. True
2. False

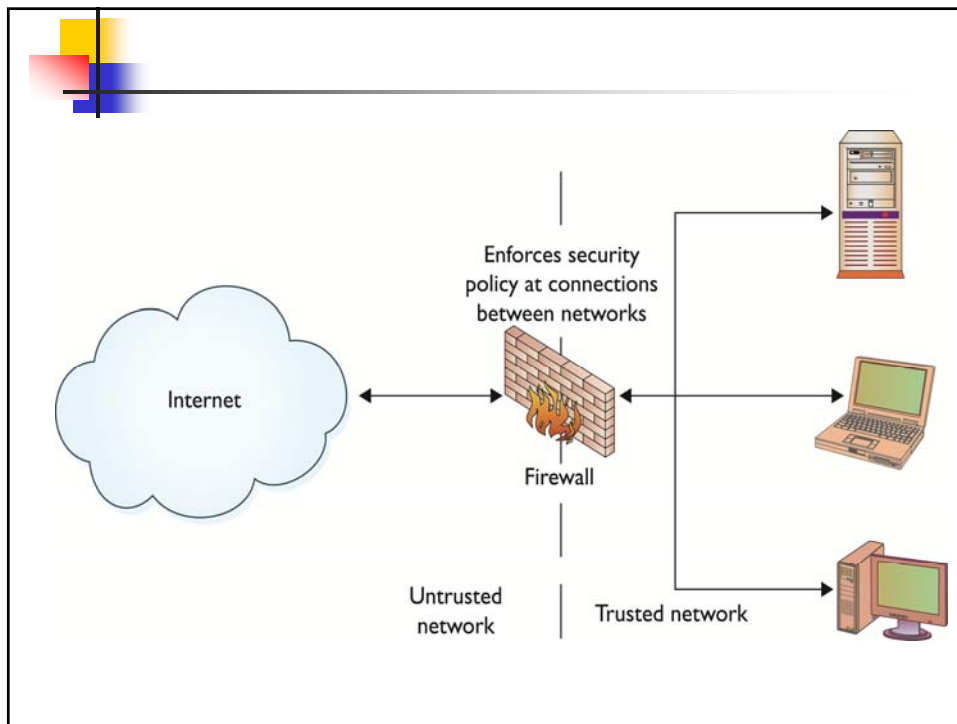


51



## Firewalls

- A network device—hardware, software, or a combination thereof
- Determines what traffic should be allowed or denied to pass in or out of a network



## How Firewalls Work

### ■ Firewall Mechanisms

- Network Address Translation (NAT)
  - One of the most basic security functions provided by a firewall is NAT.
  - NAT translates private (nonroutable) IP addresses into public (routable) IP addresses.
  - This service allows you to mask significant amounts of information from outside of the network.
  - This allows an outside entity to communicate with an entity inside the firewall without truly knowing its address
- Basic packet filtering
- Stateful packet filtering
- Application layer proxy
- Access control lists (ACLs)



## How Firewalls Work

---

- Firewall Mechanisms
  - Basic packet filtering
    - looks at each packet entering or leaving the network and then either accepts the packet or rejects the packet based on user-defined rules.
    - Each packet is examined separately.
  - Stateful packet filtering
    - Also looks at each packet, but it can examine the packet in its relation to other packets.
    - Stateful firewalls keep track of network connections and can apply slightly different rule sets based on whether the packet is part of an established session or not.



## How Firewalls Work

---

- Firewall Mechanisms
  - Application layer proxy
    - examine the content of the traffic as well as the ports and IP addresses.
    - For example, an application layer has the ability to look inside a user's web traffic, detect a malicious website attempting to download malware to the user's system, and block the malware.
  - Access control lists (ACLs)

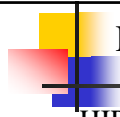


## Intrusion Prevention Systems

- Modern HIDS is often referred to as host-based intrusion prevention systems (HIPS).
- In addition to IDS functions, it has the capability of stopping or preventing malicious attack.
- Must sit inline on the network.
- Still can't inspect encrypted traffic, although some vendors included the ability to inspect SSL sessions.
- Often rated by the amount of traffic that can be processed without dropping packets.

•**An IDS is like a burglar alarm—it** watches and alerts you when something bad happens.

•**An IPS is like an armed security guard—it** watches, stops the bad activity, and then lets you know what happened.



## Host-based intrusion prevention systems components

- HIPS use the following components to prevent attacks:
  - Integrated system firewall
    - The firewall component checks all network traffic passing into and out of the host.
    - Users can set rules for what types of traffic they want to allow into or out of their system.
  - Behavioral- and signature-based IDS
    - This hybrid approach uses signatures to match well-known attacks and generic patterns for catching “zero-day” or unknown attacks for which no signatures exist.
  - Application control
    - allows administrators to control how applications are used on the system and whether or not new applications can be installed.
    - Helps to control a system's baseline and prevent malware from being installed.



## Host-based intrusion prevention systems (HIPS)

---

- Enterprise management
  - installed with an “agent” that allows them to be managed by and report back to a central server.
  - This type of integrated remote management capability is essential in any large-scale deployment of host-based IDS/IPS
  
- Malware detection and prevention
  - include scanning and prevention capabilities that address spyware, malware, rootkits, and other malicious software.



## Integrated security products

---

- Advantages:
  - Provide a great deal of security-related features in a single package.
  - Often cheaper and more convenient than purchasing a separate antivirus product, a firewall, and an IDS.
  
- Disadvantage
  - if one portion of the integrated product fails, the entire protective suite may fail.
  - Symantec’s Endpoint Protection and McAfee’s Internet Security are examples of integrated, host-based protection products.



## Proxy Servers

---

- Takes client requests and forwards to the destination server on behalf of the client
- Security application for filtering undesirable traffic and blocking potentially hostile web sites



## Types of Proxy Servers

---

- Anonymizing proxy
  - This is used to hide information about the requesting system when a webpage request is made.
  - often used by individuals who are concerned about the amount of personal information being transferred across the Internet and the use of tracking cookies and other mechanisms to track browsing activity.
- Caching proxy
  - Keeps local copies of popular client requests to reduce bandwidth usage and increase performance.
  - If the content is old or the caching proxy does not have a copy of the requested content, the request is forwarded to the destination server.



## Types of Proxy Servers *(continued)*

- Content-filtering proxy
  - Filters client requests based on acceptable use policy.
  - typically support user-level authentication, so access can be controlled and monitored and activity through the proxy can be logged and analyzed
  - Very popular in schools, corporate environments, and government networks.
  
- Open proxy
  - Open for use to any internet user, can also function in some case to anonymize requests.
  - This type of proxy has been the subject of some controversy, with advocates for Internet privacy and freedom on one side of the argument, and law enforcement, corporations, and government entities on the other side.



## Types of Proxy Servers *(continued)*

- Reverse proxy
  - Sits in front of web servers and intercepts all incoming web requests to perform tasks such as filtering, shaping or balancing incoming requests or serving up static content.
  
- Web proxy
  - solely designed to handle web traffic and is sometimes called a *web cache*. Most web proxies are essentially specialized caching proxies.
  - does not require client systems to be configured to intercept client requests.





## Proxy Servers

- Deploying a proxy solution within a network environment is usually done either by
  - **Alt 1:** setting up the proxy and requiring all client systems to configure their browsers to use the proxy
  - **Alt 2:** deploying an intercepting proxy that actively intercepts all requests without requiring client-side configuration.
- Security perspective
  - proxies are most useful in their ability to control and filter outbound requests.
  - By limiting the types of content and web sites employees can access from corporate systems, many administrators hope to avoid loss of corporate data, hijacked systems, and infections from malicious web sites.
  - Administrators also use proxies to enforce corporate acceptable use policies and track use of corporate resources.



## Internet Content Filters

- Used to:
  - Filter undesirable content
  - Filter malicious code such as browser hijacking attempts
- Challenges:
  - Blacklists of websites difficult to maintain
  - Keyword filtering may generate false positives
  - Determined users will attempt to bypass the system



## Protocol Analyzers

---

- Software or an integrated software/hardware system that can capture and decode network traffic
  
- Used by network administrators for:
  - Analyzing network problems
  - Detecting misconfigured applications or misbehaving applications
  - Gathering and reporting network usage and traffic statistics
  - Debugging client/server communications
  
- Requires NIC capable of promiscuous mode
  - Tells the NIC to process every packet that it sees regardless of the intended destination

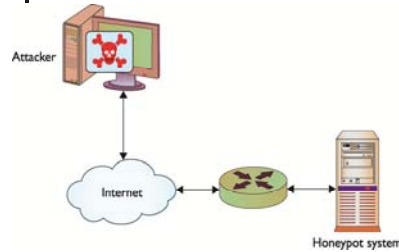


## Protocol Analyzers

---

- Relevant security applications:
  - Detect undesirable traffic
  - Capture traffic for incident response
  - Looking for evidence of malicious activity
  - Looking for unusual traffic
  - Testing encryption between systems or applications

## Honeytrap and Digital Sandbox



- One of the most effective techniques for collecting information about malicious activity is to observe activity first-hand.
  - Watching attackers as they probe, navigate, and exploit their way through a network.

## Honeytrap and Digital Sandbox

### ■ Honeytrap

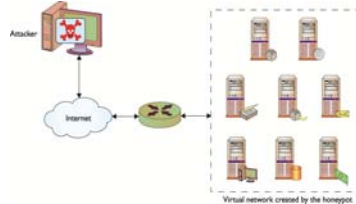
- An artificial environment where attackers can be contained and observed without putting real systems at risk
- system or group of systems designed to attract an attacker's attention.
- Gives the appearance of a real network, application servers, users systems, and network traffic.
- In most cases, it is made up of one or a few systems running specialized software to simulate the user and network traffic common to most targeted networks.
- Appear to be running versions of applications that are known to be vulnerable to specific exploits.
- Allows the attackers methods to be observed without putting real systems at risk
- Activity recorded for later analysis
- Afford information and additional security but require significant cost and effort to maintain

A honeynet is a group of honeypots

70

## Honeypots

- When attackers connect to the honeypot, they are presented with an entire “virtual” network of servers and PCs running a variety of applications.
- Anytime an attacker has been lured into probing or attacking the virtual network, the honeypot records the activity for later analysis:
  - what attackers do,
  - which systems and applications they concentrate on,
  - what tools are run,
  - how long they stay, etc.



71

## PC-based Malware Protection

- Malware protection for PCs now a necessity due to the proliferation of “always-on” broadband connections.
- Unprotected and unpatched systems are compromised within two hours of coming online, on average.



## Antivirus Products

- Used to identify, neutralize, or remove malicious programs, macros, and files.
- Scanning approaches:
  - **Signature-based scanning**
    - scan programs, files, macros, e-mails, and other data for known worms, viruses, and malware.
    - The antivirus product contains a virus dictionary with thousands of known virus signatures that must be frequently updated, as new viruses are discovered daily
    - Will catch known viruses but is limited by the virus dictionary—what it does not know about it cannot catch.
  - Heuristic scanning
    - Looks for commands or instructions that are not normally found in application programs, such as attempts to access a reserved memory register.
    - Most antivirus products use either a weight-based or rule-based system in their heuristic scanning
    - If the set threshold is passed based on a single behavior or combination of behaviors, the antivirus product will treat the process, application, macro, and so on, performing those behaviors as a threat to the system



## Antivirus Products

- Modern antivirus products have:
  - **Automated updates**
  - **Automated scanning**
  - **Media scanning**
  - **Manual Scanning**
  - **E-mail scanning**
  - **Resolution**



## Personal Software Firewalls

- Host-based protective mechanism that controls traffic going into and out of a single system.
- Various free and commercial firewall software is available.



## Pop-up Blockers and Windows Defender

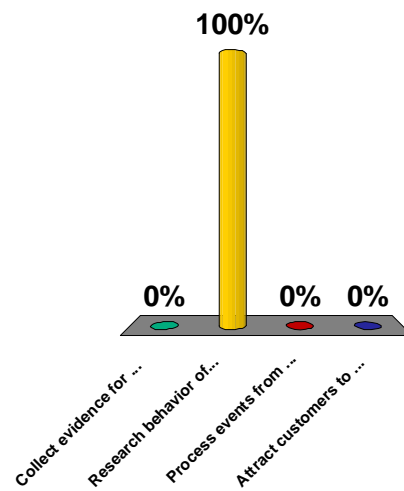
- Pop-up Blockers
  - Attempts to prevent web pages from opening a new tab or window
- Windows Defender
  - Designed to remove spyware and unwanted programs from your PC
  - Includes spyware detection and removal, scheduled scanning, automatic updates, real-time protection, software explorer, and configurable responses

## Antispam

- Designed to reduce the amount of electronic junk mail or “spam”
- Filtering methods include:
  - Blacklisting
  - Header filtering
  - Content filtering
  - Language filtering
  - User-defined filtering
  - Trapping
  - Egress Filtering
  - Enforcing the specifications of the protocol

## Honeypots are primarily used to


- A. Collect evidence for law enforcement
- B. Research behavior of attackers using virtual targets
- C. Process events from firewalls and routers
- D. Attract customers to e-commerce sites



78



## The main purpose of a honeypot is

- A. To identify hackers so they can be tracked down by the FBI.
- B. To slow hackers down by providing an additional layer of security that hackers must pass before accessing the actual network.
- C. To distract hackers away from attacking an organization's live network.
-  D. To help security professionals better understand and protect against threats to the system.

