

# IT 4823

## Information Security Administration

### Intrusion Detection



Notice: This session is  
being recorded.

Some lecture slides prepared by Dr Lawrie Brown for “*Computer Security: Principles and Practice*”, 1/e, by William Stallings and Lawrie Brown



Copyright © 2016 by Bob Brown



# Goals of Information Security

- **Detection**
- Prevention
- Response and Recovery

# Intrusions

- **Intrusion:** type of attack on information assets in which the instigator attempts to gain entry into or disrupt system
- **Incident response:** identification of, classification of, response to, and recovery from an incident
- **Intrusion prevention:** consists of activities that seek to deter an intrusion from occurring

Remember Prevention-Detection-Response?

# Intruders

- Significant issue: hostile/unwanted trespass
  - ~~from annoying to~~ serious
- User trespass
  - unauthorized logon, privilege abuse
- Software trespass
  - virus, worm, or Trojan horse
- Classes of intruders:
  - masquerader, misfeator, clandestine user

# Types of Intruders

## **masquerader**

- likely to be an outsider
- an unauthorized individual who penetrates a system to exploit a legitimate user account

## **mifeasor**

- generally an insider
- legitimate user who misuses privileges

## **clandestine user**

- can be either insider or outsider
- individual who seizes supervisory control to evade auditing and access controls or to suppress audit collection

# Examples of Intrusion

- Activities:
  - Remote root compromise
  - Web server defacement
  - Copying viewing sensitive data / databases
  - Distributing pirated software
- Mechanisms:
  - Exploiting software vulnerabilities
  - Guessing / cracking passwords
  - Running a packet sniffer
  - Impersonating a user to reset password
  - Using an unattended workstation

# Intrusion Detection

A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

# Corporate or Government Attacks

- Espionage (Government spying)
- Corporate spying
- Well-equipped with regard to resources
- Generally have a specific target (person or information) in mind.
- Consider “spear phishing” as an example.



# Criminal Enterprise

- Organized groups have become a threat
  - loosely affiliated gangs
  - typically young
  - often Eastern European or Russian (or from Miami!)
  - common target credit cards on e-commerce server
- Criminal hackers usually have specific targets
- Length of intrusion depends on nature of goal.
- IDS / IPS can help, but quick nature of attack is a problem
- Sensitive data needs strong protection

# Criminal Enterprise Behavior

1. Act quickly and precisely to make their activities harder to detect
2. Exploit perimeter via vulnerable ports
3. Use Trojan horses (hidden software) to leave back doors for re-entry
4. Use sniffers to capture passwords
5. May act quickly, or linger for months to collect, *e.g.* credit card data.
6. Make few or no mistakes.

# "Hackers"

- Motivated by thrill of access and status
  - hacking community a strong meritocracy
  - status is determined by level of competence
- Intruders without malicious intent are *not* tolerable
  - do consume resources and may slow performance
  - can't know in advance whether benign or malign
- IDS / IPS / VPNs can help counter
- Awareness led to establishment of CERTs
  - collect / disseminate vulnerability info / responses

# Hacker Behavior Example

1. Select target using IP lookup tools (or scan address spaces for open ports)
2. Map network for accessible services
3. Identify potentially vulnerable services
4. Brute force (guess) passwords
5. Install remote administration tool
6. Wait for admin to log on and capture password
7. Use password to access remainder of network

# Insider Attacks

- Among most difficult to detect and prevent
- Employees have access and systems knowledge
- May be motivated by revenge / entitlement
  - when employment terminated
  - taking customer data when move to competitor
- IDS / IPS may help but we also need:  
least privilege, monitor logs, strong authentication,  
termination process to block access, back up computer  
disks before reformatting/reissuing.

# Insider Behavior Example

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn't normally use for their daily jobs
3. Email former and prospective employers
4. Conduct furtive instant-messaging chats
5. Visit web sites that cater to disgruntled employees
6. Perform large downloads and file copying
7. Access the network during off hours.

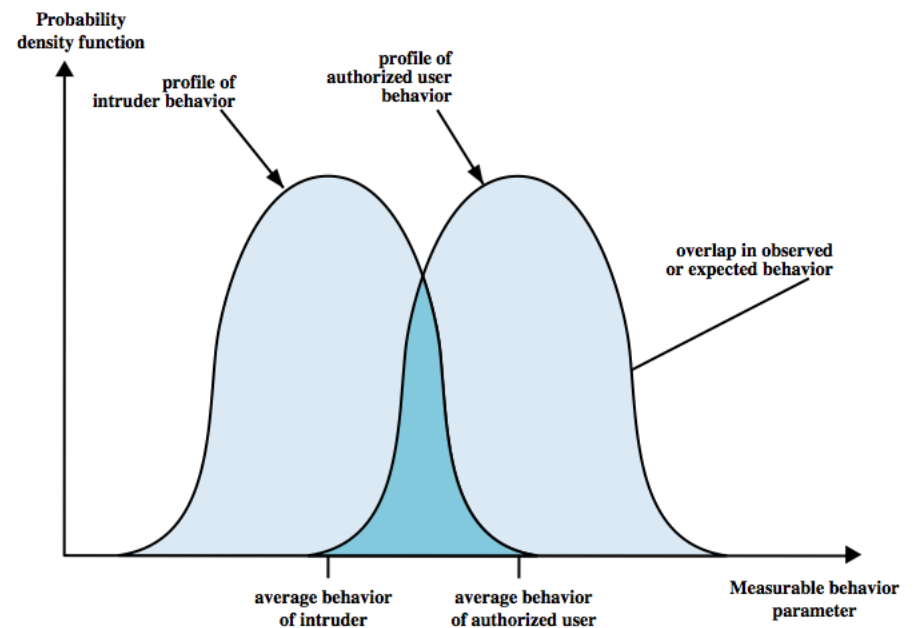
# Intrusion Techniques

- Objective: to gain access or increase privileges
- Initial attacks often exploit system or software vulnerabilities to execute code to get backdoor, *e.g.* buffer overflow...
- or to gain protected information, *e.g.* password guessing or acquisition

# IDS Principles

Assumption: intruder behavior differs from legitimate users

- expect overlap as shown
- observe deviations from past history
- Problems of:
  - False positives
  - False negatives
  - We must compromise





# Three Components of an IDS

- Sensors - collect data
- Analyzers - determine if intrusion has (potentially) occurred
- User interface - view output or control system behavior

# IDS Requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Be configurable according to security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

# Threat Monitoring

- Intrusion detections have their origins in systems to attempt to detect specific threats.
- Basic description: James Anderson, 1972
- First IDS: Denning and Neumann, 1984-86.
- Denning's intrusion detection model, 1987.
- Commercial IDSs, 1995.

# Detection and Reaction

- Intrusion detection: consists of procedures and systems created and operated to detect system intrusions
- Intrusion reaction: encompasses actions an organization undertakes when intrusion event is detected
- Intrusion correction activities: finalize restoration of operations to a normal state

# Intrusion Detection Systems (IDSs)

- An IDS detects a violation of its configuration constraints and activates an alarm.
- Many IDSs enable administrators to configure systems to notify them directly of trouble via e-mail or SMS.
- Systems can also be configured to notify an external security service organization of a “break-in.”

# Why Use an IDS?

- Prevent problem behaviors by increasing the perceived risk of discovery and punishment
- Detect attacks and other security violations
- Detect and deal with preambles to attacks
- Document existing threats to an organization
- Act as quality control for security design and administration, especially of large and complex enterprises
- Provide useful information about intrusions that take place

## Types of IDSs and Detection Methods

- IDSs operate as
  - network-based,
  - host-based, or
  - application-based systems
- All IDSs use one of two detection methods:
  - Signature-based
  - Statistical anomaly-based

# Host-Based IDS

- Host-based IDS (HIDS) resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDSs work on the principle of configuration or change management
- Advantage over NIDS: can usually be installed so that it can access information encrypted when traveling over network



## Advantages of HIDSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDS (application specificity)
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

## Disadvantages of HIDSs

- Pose more management issues
- Vulnerable both to direct attacks and attacks against host operating system
- Does not detect multi-host scanning, nor scanning of non-host network devices
- Susceptible to some denial-of-service attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

# Network-Based IDS (NIDS)

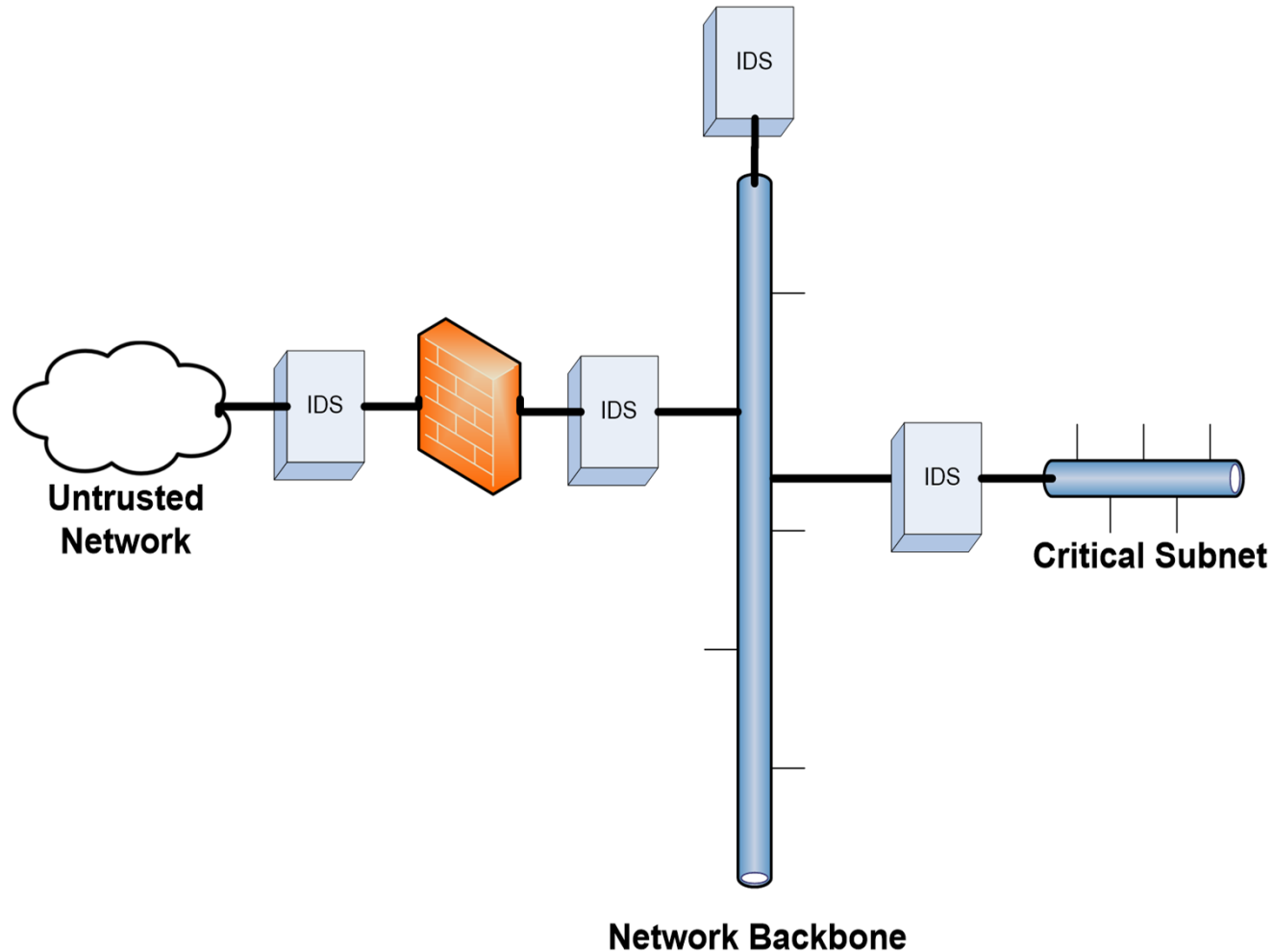
- Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
- When examining packets, a NIDS looks for attack patterns
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment

# Deploying Network-Based IDSs

NIST recommends four locations for NIDS sensors

- Location 1: behind each external firewall, in the network DMZ
- Location 2: outside an external firewall
- Location 3: On major network backbones
- Location 4: On critical subnets

# IDS Locations (NIST)



# NIDS Signature Matching

- To detect an attack, NIDSs look for attack patterns
- Done by using special implementation of TCP/IP stack:
  - In process of protocol stack verification, NIDSs look for invalid data packets
  - In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use

## Advantages of NIDSs

- Good network design and placement of NIDS can enable organization to monitor large network with a few devices
- NIDSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- NIDSs not usually susceptible to direct attack and may not be detectable by attackers

## Disadvantages of NIDSs

- Can become overwhelmed by network volume and fail to recognize attacks
- Require access to all traffic to be monitored (Not as easy as it sounds because of switching.)
- Cannot analyze encrypted packets
- Cannot reliably ascertain if attack was successful or not
- Some forms of attack are not easily discerned by NIDSs, specifically those involving fragmented packets



# Application-Based IDS

- Application-based IDS examines application for abnormal events
- AppIDS may be configured to intercept requests:
  - File System
  - Network
  - Configuration
  - Execution Space (memory allocation)

# Advantages and Disadvantages of Application IDSs

- Advantages
  - Aware of specific users; can observe interaction between application and user
  - Able to operate even when incoming data is encrypted
- Disadvantages
  - More susceptible to attack
  - Less capable of detecting software tampering
  - May be taken in by forms of spoofing

# Active Intrusion Prevention

- Some organizations implement active countermeasures to stop attacks
  - Logging off certain users
  - Stopping certain processes
  - Send a TCP “reset” message
- One tool (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

# Signature-Based IDS

- Examine data traffic in search of patterns that match known signatures
- Content-based
- Widely used because many attacks have clear and distinct signatures
- Problem with this approach is that as new attack strategies are identified, the IDS's database of signatures must be continually updated

# Statistical Anomaly-Based IDS

- The statistical anomaly-based IDS (stat IDS) or behavior-based IDS sample network activity to compare to traffic that is known to be normal
- When measured activity is outside baseline parameters or clipping level, IDS will trigger an alert (context-based)
- IDS can detect new types of attacks
- Requires much more overhead and processing capacity than signature-based
- May generate many false positives

# Log File Monitors

- Log file monitor (LFM) similar to NIDS
- Reviews log files generated by servers, network devices, and even other IDSs for patterns and signatures
- Patterns that signify attack may be much easier to identify when entire network and its systems are viewed holistically
- Requires allocation of considerable resources since it will involve the collection, movement, storage, and analysis of large quantities of log data

# Artificial Stupidity

The opposite of “artificial intelligence,” sort-of

Describe, and then filter out, those things that are not interesting.

What is left is either interesting, or should be added to the filters.

# IDS Response Behavior

- Once IDS detects an anomalous network situation, it has a number of options
- IDS responses can be classified as active or passive
  - Active response: definitive action initiated when certain types of alerts triggered, *e.g.* reconfigure firewall
  - Passive response options simply report
- Dangers of active response: can compromise system availability.



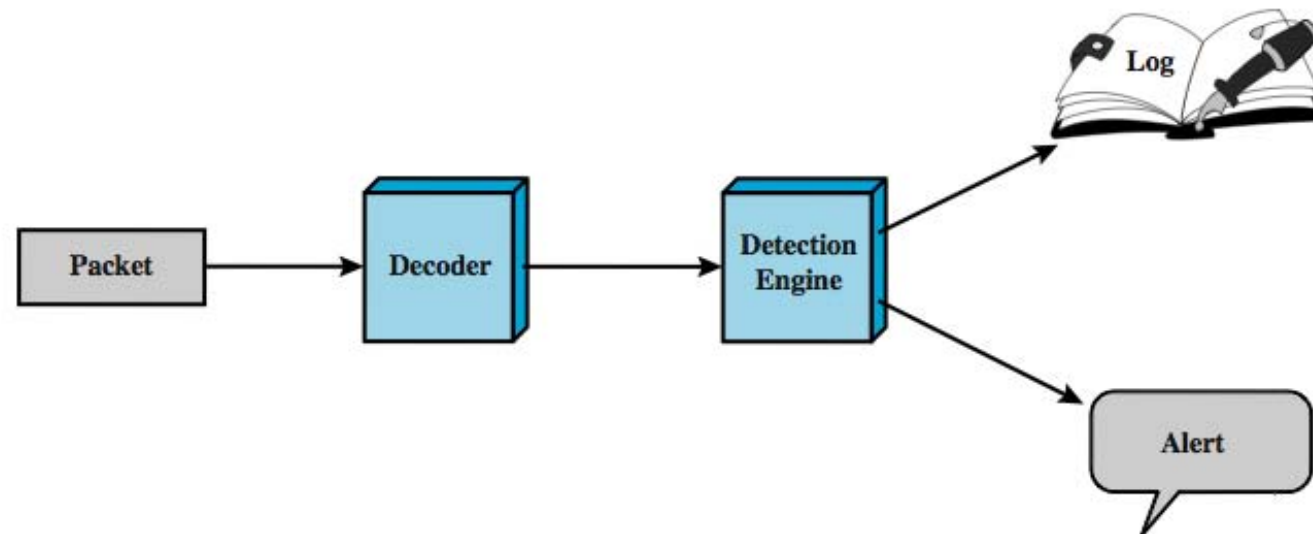
# Measuring the Effectiveness of IDSs

- IDSs are evaluated using two dominant metrics:
  - Administrators evaluate the number of attacks detected in a known collection of probes
  - Administrators examine the level of use at which IDSs fail
- Evaluation of IDS might read: “at 100 Mb/s, IDS was able to detect 97% of directed attacks.”
- Since developing this collection can be tedious, most IDS vendors provide testing mechanisms that verify systems are performing as expected

# Example: SNORT

## Lightweight IDS

- real-time packet capture and rule analysis
- passive or inline



# SNORT Rules

- use a simple, flexible rule definition language
- with fixed header and zero or more options
- header includes: action, protocol, source IP, source port, direction, dest IP, dest port
- many options
- example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \  
  (msg: "SCAN SYN FIN"; flags: SF, 12; \  
  reference: arachnids, 198; classtype: attempted-recon;)
```

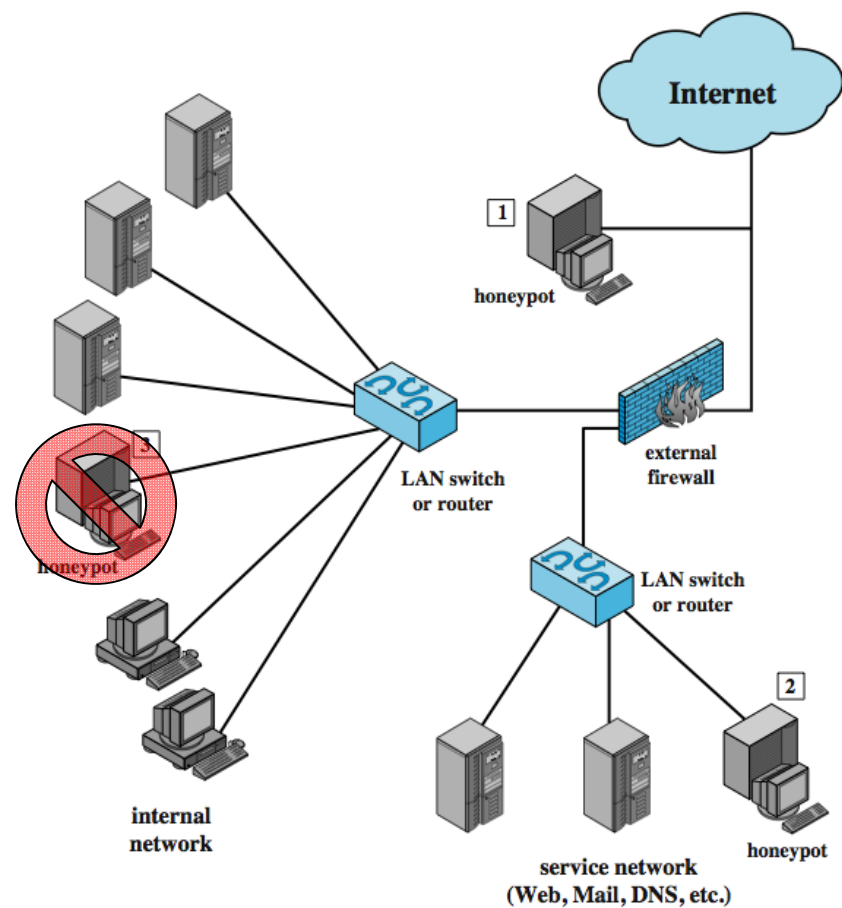
# Incident Response

- Assess the current situation
- Stop the attack; contain the damage.
- Collect evidence, if appropriate
- Correct the vulnerability that allowed the attack to succeed
- Restore normal operation
- Deal with publicity
- Deal with law enforcement, if appropriate

# Honeypots

- Are decoy systems
  - filled with fabricated info
  - instrumented with monitors / event loggers
  - divert and hold attacker to collect activity info
  - without exposing production systems
- Initially were single systems
- More recently are/emulate entire networks
- May or may not be effective, and could have legal implications.

# Honeypot Deployment



# Key Points

- Begin with policy
- Craft network architecture and security measures from it
- Assume failure will occur
  - Try to minimize it
  - Defend in depth
  - Have plan to handle failures

# Questions

