Information Systems Security

Presented By
Dr. Mohamed Marie

2 Chapter

Attacks and Monitoring

This chapter presents the following:

- **Monitoring**
- **Intrusion Detection**
- **Penetration Testing**
- **Access Control Attacks**

Introduction

Generally, **access control** ***is any hardware, software, or organizational administrative policy or procedure that grants or restricts access, monitors and records attempts to access, identifies users attempting to access, and determines whether access is authorized***.

This domain is discussed in this chapter and in the previous chapter (Chapter 1, "Accountability and Access Control"). Be sure to read and study the materials from both chapters to ensure complete coverage of the essential material for the CISSP certification exam.

Monitoring

Monitoring ***is the programmatic means by which subjects are held accountable for their actions while authenticated on a system***.

It is also the process by which unauthorized or abnormal activities are detected on a system.

Monitoring ***is necessary to detect malicious actions by subjects, as well as to detect attempted intrusions and system failures.***

It can help reconstruct events, provide evidence for prosecution, and ***produce problem reports and analysis***.

Monitoring

Using log files ***to detect problems is another matter. In most cases, when sufficient logging and auditing is enabled to monitor a system, so much data is collected that the important details get lost in the sheer volume of resulting data.*** You can use numerous tools to search through log files for specific events or ID codes. The art of **data reduction** is crucial when working with large volumes of monitoring data obtained from log files. ***The tools used to extract the relevant, significant, or important details from large collections of data are known as data mining tools.*** For true automation and even real-time analysis of events, a specific type of data mining tool is required, namely, an **intrusion detection system (IDS).** See the next section for information about IDSs.

Monitoring

Accountability *is maintained by recording the activities of subjects and objects as well as core system functions that maintain the operating environment and the security mechanisms.*

The **audit trails** *created by recording system events to logs can be used to evaluate a system's health and performance.*
System crashes *may indicate faulty programs, corrupt drivers, or intrusion attempts.*

The event logs *leading up to a crash can often be used to discover the reason a system failed.*
Log files *provide an audit trail for recreating a step-by-step history of an event, intrusion, or system failure.*

Monitoring

Monitoring ***is a necessary function of the auditing process through which subjects are held accountable for their actions and activities with regard to other subjects, objects, or functions on any given system.***

Additionally, ***you can build up several supportive layers of defense around monitoring, auditing, and accounting practices that include the real-time detection and deterrence of network-borne attack patterns that originate both inside and outside the perimeter of your business environment.***

Intrusion Detection

An intrusion detection system ***is a product that automates the inspection of audit logs and real- time system events. IDSs are primarily used to detect intrusion attempts, but they can also be employed to detect system failures or to rate overall performance.***

IDSs watch for violations of confidentiality, integrity, and availability. The goal of an IDS is to provide perpetrator accountability for intrusion activities and provide a means for a timely and accurate response to intrusions.

Attacks ***recognized by an IDS can come from external connections (such as the Internet or partner networks), viruses, malicious code, trusted internal subjects attempting to perform unauthorized activities, and unauthorized access attempts from trusted locations.***

An IDS is considered a form of a technical detective security control.

Intrusion Detection

An IDS ***can actively watch for suspicious activity, peruse audit logs, and send alerts to administrators when specific events are discovered.***
It can also lock down important system files or capabilities, track slow and fast intrusion attempts, highlight vulnerabilities, identify the intrusion's origination point, and track down the logical or physical location of the perpetrators. In addition, an **IDS** ***can terminate or interrupt attacks and intrusion attempts, and it can reconfigure routers and firewalls to prevent repeats of discovered attacks.***

IDS alerts ***can be sent or communicated with an onscreen notification (the most common) by playing a sound, sending an email notification, alerting a pager, or recording information in a log file.***

Intrusion Detection

A response by an IDS can be active, passive, or hybrid:
Active response ***Directly affects the malicious activity of network traffic or the host application***
Passive response ***Does not affect the malicious activity but records information about the issue and notifies the administrator***
Hybrid response ***Stops unwanted activity, records information about the event, and possibly even notifies the administrator***

Generally, an **IDS is used** ***to detect unauthorized or malicious activity originating from inside or outside your trusted network***. The capability of an IDS to stop current attacks or prevent future attacks is limited. Typically, **the responses that an IDS** ***can take against an attack include blocking ports, blocking source addresses, and disabling all communications over a specific cable segment.*** Whenever an IDS discovers abnormal traffic (such as spoofed traffic) or violations of its security policy, filters, or rules, it records a log detail of the issue and then drops, discards, or deletes the relevant packets.

Intrusion Detection

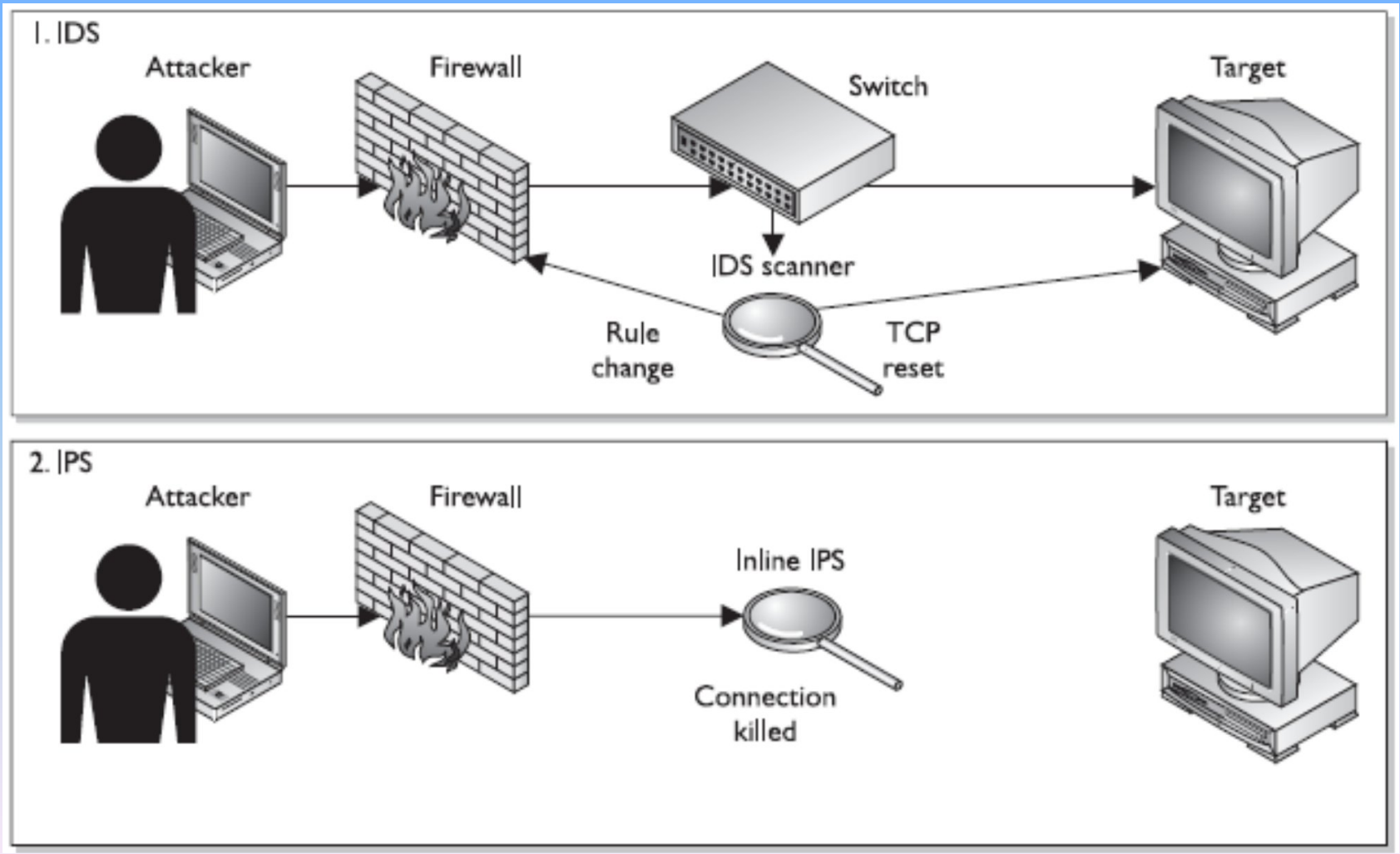
An IDS should be considered one of the many components that a well-formed security endeavor employs to protect a network. **An IDS** ***is a complementary security tool to a firewall.***

Other security controls, such as physical restrictions and logical access controls, are necessary components as well (please refer to Chapter 1 for a discussion of these controls).

Intrusion prevention ***requires adequate maintenance of overall system security, such as applying patches and setting security controls. It also involves responding to intrusions discovered via an IDS by erecting barriers to prevent future occurrences of the same attack***. This could be as simple as updating software or reconfiguring access controls, or it could be as drastic as reconfiguring a firewall, removing or replacing an application or service, or redesigning an entire network.

Intrusion Detection

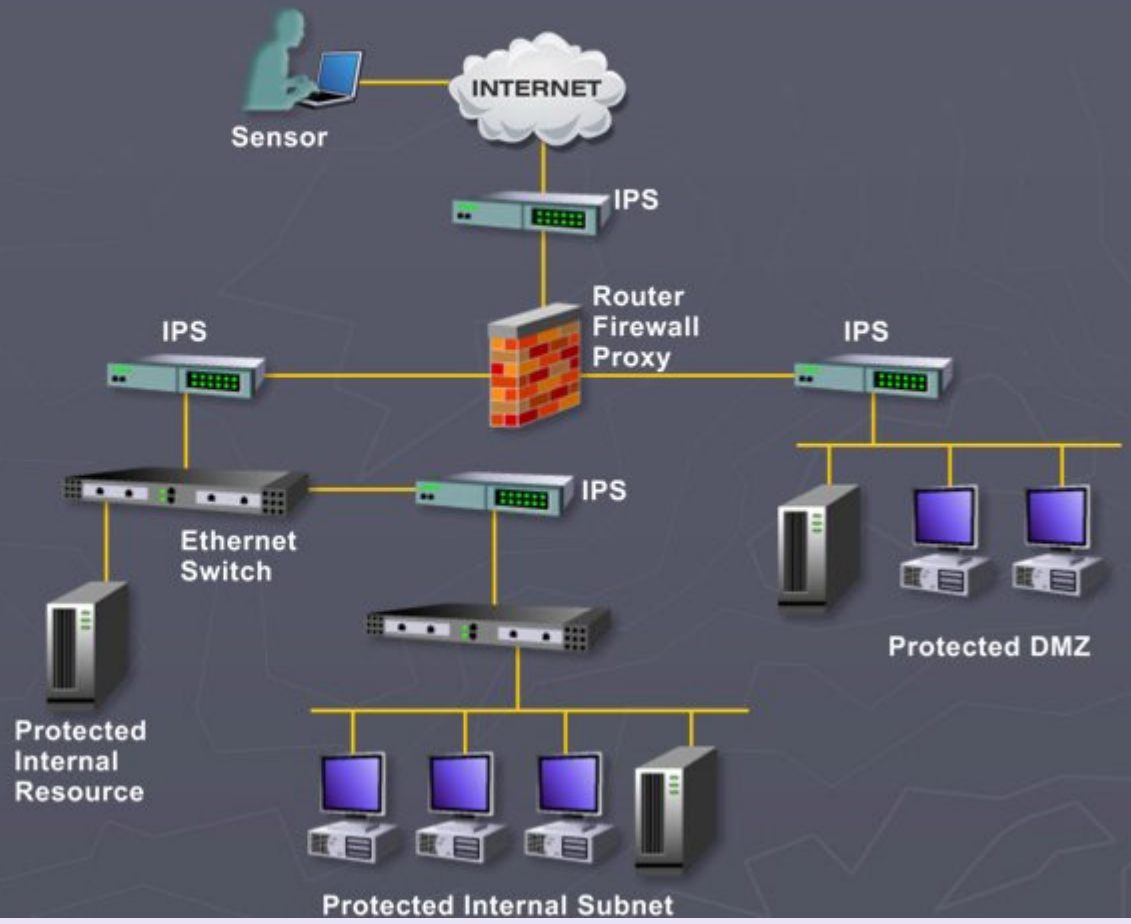
IDS vs. IPS architecture



Intrusion Detection

Intrusion Prevention System

- IPS is a preventive and proactive technology, whereas an IDS is a detective and after-the-fact technology
- Access control decisions based on application content, rather than IP address or ports as traditional firewalls had done



Intrusion Detection

When an intrusion is detected, ***your first response should be to contain the intrusion***.

Intrusion containment ***prevents additional damage to other systems but may allow the continued infestation of already compromised systems***. Later, once compromised systems are rebuilt from scratch, be sure to double-check compliance with your security policy—including checking ACLs, service configurations, and user account settings—before connecting the reestablished system to your network.

IDS type and classification ***defines the scope of responsibility and functional role for each system.***

Host-Based and Network-Based IDSs

IDS types ***are most commonly classified by their information source. There are two primary types of IDSs***: **host based** and **network based**. A ***host-based* IDS** ***watches for questionable activity on a single computer system.*** A ***network-based IDS watches for questionable activity being performed over the network medium.***

Host-Based IDS

Because the attention of a host-based IDS is focused on a single computer (whereas a network- based IDS must monitor the activity on an entire network), ***it can examine events in much greater detail than a network-based IDS can***.

A host-based IDS ***is able to pinpoint the files and processes compromised or employed by a malicious user to perform unauthorized activity***.

Host-Based and Network-Based IDSs

Host-Based IDS

Host-based IDSs ***can detect anomalies undetected by network-based IDSs***; however, a host- based IDS cannot detect network-only attacks or attacks on other systems.

Because a host-based IDS ***is installed on the computer being monitored, attackers can discover the IDS software and disable it or manipulate it to hide their tracks. A host-based IDS has some difficulty with detecting and tracking down denial-of-service (DoS) attacks, especially those of a bandwidth consumption nature.***

A host-based IDS also consumes resources from the computer being monitored, thereby reducing the performance of that system.

A host-based IDS is ***limited by the auditing capabilities*** of the host operating system and applications.

Host-Based and Network-Based IDSs

Host-based IDSs are considered ***more costly to manage*** than network-based IDSs.

Host- based IDSs require that an installation on each server be monitored and require administrative attention at each point of installation, while network-based IDSs usually require only a single installation point. ***Host-based IDSs have other disadvantages as well; for example, they cause a significant host system performance degradation, and they are easier for an intruder to discover and disable***.

Host-Based and Network-Based IDSs

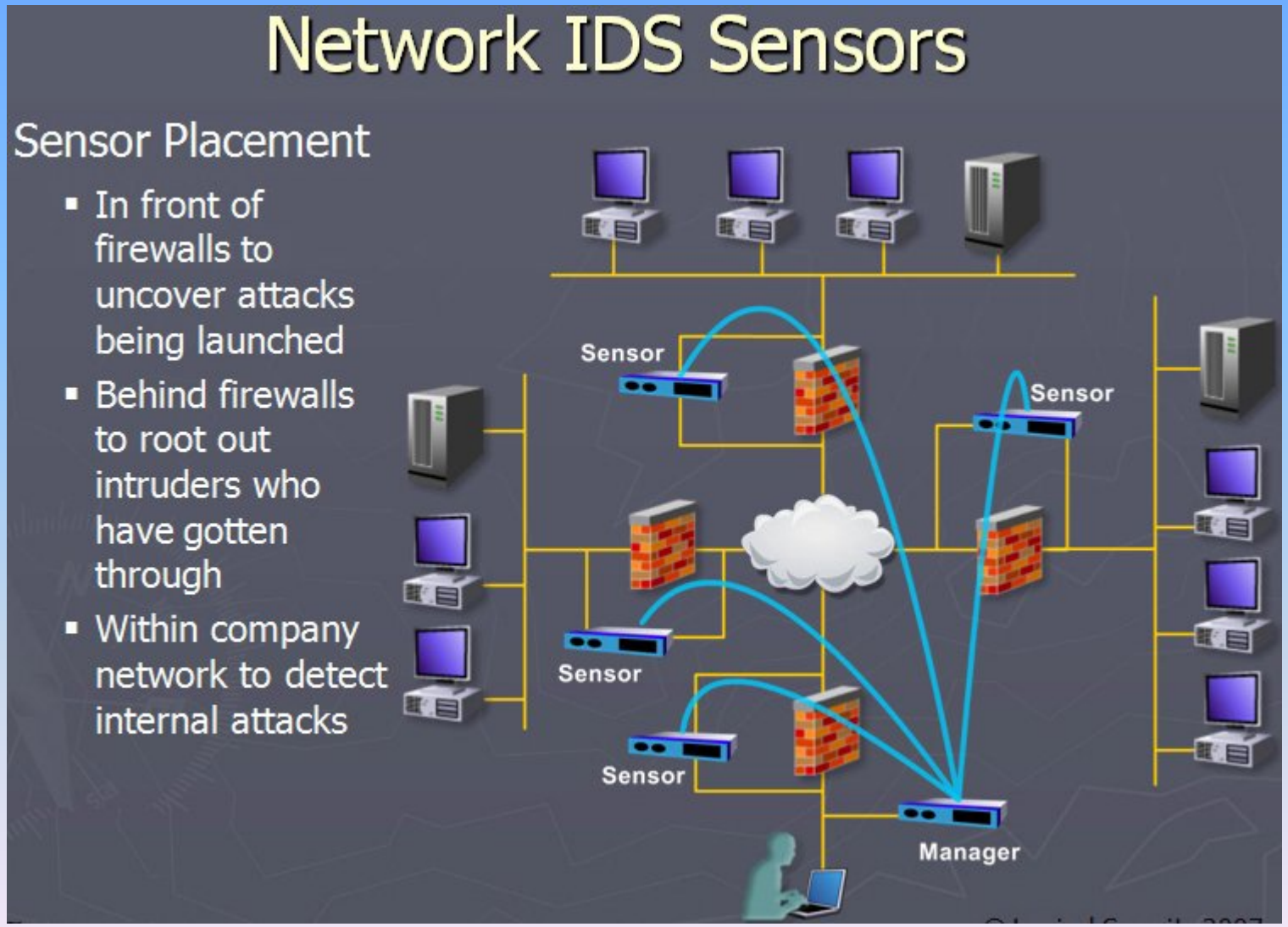
Network-Based IDS

Network-based IDSs ***detect attacks or event anomalies through the capture and evaluation of network packets.*** A single network-based IDS is capable of monitoring a large network if installed on a backbone of that network, where a majority of the network traffic occurs. ***Some versions of network-based IDSs use remote agents to collect data from various subnets and report to a central management console***.

Network-based IDSs are installed onto **single-purpose computers**. This allows them to be hardened against attack, reduces the number of vulnerabilities to the IDS, and allows the IDS to operate in stealth mode. In **stealth mode**, ***the IDS is invisible to the network, and intruders would have to know of its exact location and system identification to discover it.***

A **network-based IDS** ***has little negative affect on overall network performance, and because it is deployed on a single-purpose system, it doesn't adversely affect the performance of any other computer***.

Host-Based and Network-Based IDSs



Host-Based and Network-Based IDSs

Network-Based IDS

Network-based IDSs ***are used to monitor the content of traffic if it is encrypted during transmission over the network medium. They are usually able to detect the initiation of an attack or the ongoing attempts to perpetrate an attack (including DoS), but they are unable to provide information about whether an attack was successful or about which specific systems, user accounts, files, or applications were affected.***

Often, a network-based IDS can provide some ***limited functionality*** ***for discovering the source of an attack by performing Reverse Address Resolution Protocol (RARP) or Domain Name System (DNS) lookups***.

Host-Based and Network-Based IDSs

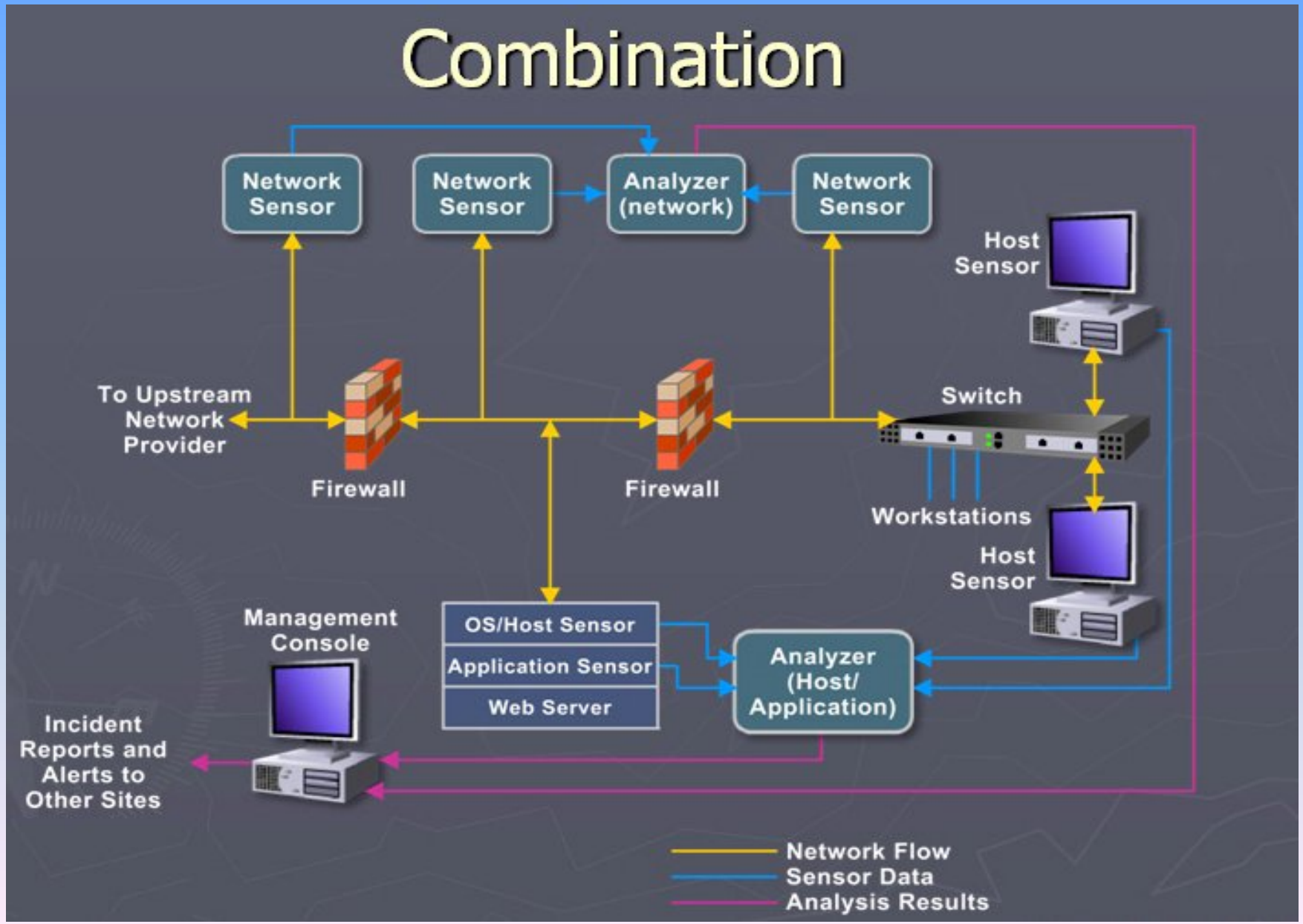
Network-Based IDS

An IDS should not be viewed as a single universal security solution. It is only part of a multifaceted security solution for an environment. Although an IDS can offer numerous benefits, there are several drawbacks to consider.

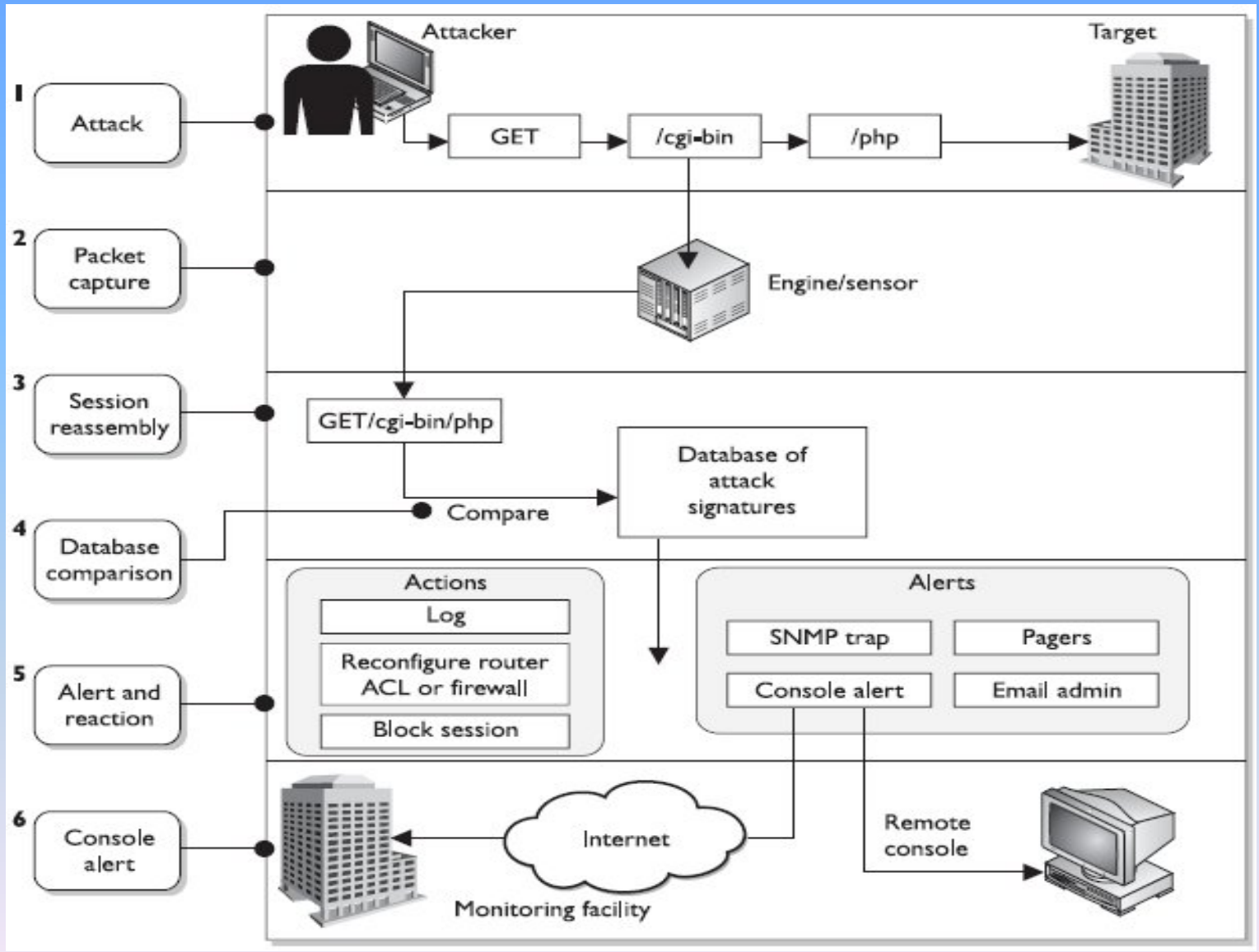
A **host-based IDS** ***may not be able to examine every detail if the host system is overworked and insufficient execution time is granted to the IDS processes.***

A **network-based IDS** ***can suffer the same problem if the network traffic load is high and it is unable to process packets efficiently and swiftly***. A network-based IDS is also ***unable to examine the contents of encrypted traffic***.

Host-Based and Network-Based IDSs



Host-Based and Network-Based IDSs



Network-Based IDSs Architecture

Knowledge-Based and Behavior-Based Detection

An IDS can detect malicious events by two common means. One way is to use **knowledge-based detection** (also called ***signature-based detection*** or ***pattern-matching detection***). Basically, the IDS ***uses a signature database and attempts to match all monitored events to its contents***. If events match, then the IDS assumes that an attack is taking place (or has taken place). The IDS vendor develops the suspect chart by examining and inspecting numerous intrusions on various systems. What results is a **description**, or **signature**, of common attack methods or behaviors. An IDS using knowledge-based detection functions in much the **same way as many antivirus applications**.

The primary **drawback** to a knowledge-based IDS is that it is ***effective only against known attack methods***. New attacks or slightly modified versions of known attacks often go unrecognized by the IDS. This means that the knowledge-based IDS ***lacks a learning model***; that is, it is ***unable to recognize new attack patterns as they occur***. Thus, this type of IDS is only as useful as its signature file is correct and up-to-date. ***Keeping the signature file current*** is an important aspect in maintaining the best performance from a knowledge-based IDS.

Knowledge-Based and Behavior-Based Detection

The second detection type is **behavior-based detection** (also called ***statistical intrusion detection, anomaly detection***, and ***heuristics-based detection***). Basically, behavior-based detection ***finds out about the normal activities and events*** on your system through **watching and learning**. Once it has accumulated enough data about normal activity, it can detect abnormal and possible malicious activities and events.

A behavior-based IDS can be labeled an expert system or a pseudo-artificial intelligence system because it ***can learn and make assumptions about events***. In other words, the **IDS** ***can act like a human expert by evaluating current events against known events***.

The ***more information provided to a behavior-based IDS about normal activities and events, the more*** **accurate** ***its anomaly detection becomes***.

Knowledge-Based and Behavior-Based Detection

The primary **drawback** of a behavior-based IDS is that it produces **many false alarms**. The normal pattern of user and system activity can vary widely, and thus establishing a definition of normal or acceptable activity can be difficult. ***The more a security detection system creates false alarms, the less likely security administrators will heed its warnings***. ***Over time, the IDS can become more efficient and accurate, but the learning process takes considerable time***.

Using ***known behaviors***, ***activity statistics***, and ***heuristic evaluation of current vs. previous events***, a behavior-based IDS can **detect unforeseen, new, and unknown vulnerabilities, attacks, and intrusion methods**.

Although knowledge-based and behavior-based detection methods do have their differences, **both employ an alarm-signal system**. When an intrusion is recognized or detected, an alarm is triggered. The alarm system can notify administrators via email or popup messages or by executing scripts to send pager messages. In addition to administrator notification, the alarm system ***can record alert messages in log and audit files*** as well as generate ***violation reports*** detailing the detected intrusions and discoveries of vulnerabilities.

Knowledge-Based and Behavior-Based Detection

Signature-based

• Pattern matching, similar to antivirus software
• Signatures must be continuously updated
• Cannot identify new attacks

Two types:
• **Pattern matching** Compares packets to signatures
• **Stateful matching** Compares patterns to several activities at once

Anomaly-based

• Behavioral-based system that learns the "normal" activities of an environment
• Can detect new attacks
• Also called behavior- or heuristic-based

Three types:
• **Statistical anomaly–based** Creates a profile of "normal" and compares activities to this profile
• **Protocol anomaly–based** Identifies protocols used outside of their common bounds
• **Traffic anomaly–based** Identifies unusual activity in network traffic

IDS-Related Tools

Intrusion detection systems are often deployed in concert with several other components. These IDS-related tools expand the usefulness and capabilities of IDSs and make them more efficient and less prone to false positives.

These tools include

- **honey pots**,
- **padded cells**,
- **vulnerability scanners**

Described in the following sections.

IDS-Related Tools

Understanding Honey Pots

Honey pots ***are individual computers or entire networks created to serve as a snare for intruders. They look and act like legitimate networks, but they are 100 percent fake.***

When honey pot access is detected, it is most likely an unauthorized intruder. Honey pots are deployed to keep an intruder logged on and performing their malicious activities long enough for the automated IDS to detect the intrusion and gather as much information about the intruder as possible. ***The longer the honey pot retains the attention of the intruder, the more time an administrator has to investigate the attack and potentially identify the person perpetrating the intrusion.***

HoneynetWeb.mov

IDS-Related Tools

Understanding Padded Cells

A **padded cell** ***system is similar to a honey pot, but it performs intrusion isolation using a different approach. When an intruder is detected by an IDS, the intruder is automatically transferred to a padded cell.*** The padded cell has the look and layout of the actual network, but within the padded cell the intruder can neither perform malicious activities nor access any confidential data.

A padded cell ***is a simulated environment that offers fake data to retain an intruder's interest.*** The transfer of the intruder into a padded cell is ***performed without informing the intruder*** that the change has occurred. Like a honey pot, the padded cell system is heavily monitored and used by administrators to gather evidence for tracing and possible prosecution.

IDS-Related Tools

Understanding Vulnerability Scanners

Another type of IDS-related tool is a **vulnerability scanner**. **Vulnerability scanners** ***are used to test a system for known security vulnerabilities and weaknesses. They are used to generate reports that indicate the areas or aspects of the system that need to be managed to improve security.*** The reports may recommend applying patches or making specific configuration or security setting changes to improve or impose security.

A vulnerability scanner ***is only as useful as its database of security issues. Thus, the database must be updated from the vendor often to provide a useful audit of your system***. The use of vulnerability scanners in cooperation with IDSs may help reduce false positives by the IDS and keep the total number of overall intrusions or security violations to a minimum. When discovered vulnerabilities are patched quickly and often, the system provides a more secure environment.

IDS-Related Tools

Intrusion Prevention System

An extension to the concept of the IDS is the **intrusion prevention system (IPS),** ***which seeks to actively block unauthorized connection attempts or illicit traffic patterns as they occur.*** IPS designs fall under the same type (host- and network-based) and classification (behavior- or signature-based) as IDS counterparts, and they are often deployed together for complete network coverage. Additionally, many IPS platforms are capable of dissecting higher-level application protocols in search of malicious payloads.

Penetration Testing

In security terms, a ***penetration*** occurs when an attack is successful and an intruder is able to breach the perimeter of your environment. The breach can be as small as reading a few bits of data from your network or as big as logging in as a user with unrestricted privileges. ***One of the primary goals of security is to prevent penetrations.***

One common method to test the strength of your security measures is to perform penetration testing, a vigorous attempt to break into your protected network using any means necessary. ***It is common for organizations to hire external consultants to perform the penetration testing so the testers are not privy to confidential elements of the security's configuration, network design, and other internal secrets.***

Penetration Testing

Penetration testing seeks to find any and all detectable weaknesses in your existing security perimeter. The operative term is *detectable*; there are undetected and presently unknowable threats lurking in the large-scale infrastructure of network software and hardware design that no amount of penetration testing can directly discover and reveal. ***Once a weakness is discovered, countermeasures can be selected and deployed to improve the security of the environment***. One significant difference between penetration testing and actual attacking is that once a vulnerability is discovered, the intrusion attempt ceases before the vulnerability is actually exploited and causes system damage. There are open source and commercial tools (such as Metasploit and Core IMPACT) that take penetration testing one step further and attempt to exploit known vulnerabilities in systems and networks, which can be used by good guys and bad guys alike.

Penetration Testing

Penetration testing can be performed using automated attack tools or suites or performed manually with common network utilities and scripting. Automated attack tools range from professional vulnerability scanners to wild, underground attack tools discovered on the Internet. Tools are also often used for penetration testing performed manually, but much more onus is placed on knowing how to perpetrate an attack.

Penetration testing should be performed only with the consent and knowledge of management. Performing unapproved security testing could result in productivity loss, trigger emergency response teams, or even cost you your job and potentially earn you some jail time.

Methods of Attack

These are the common or well-known classes of attacks or attack methodologies:

- **Brute-force and dictionary attacks**
- **Denial-of-service attacks**
- **Spoofing**
- **Man-in-the-middle attacks**
- **Spamming**
- **Sniffers**

All of these methods will eventually be attempted on your network. Assessing the severity of each on a case-by-case basis is less relevant than assessing each element as part of a much larger combination of risk potential and threat value.

Simple one-stage attacks (brute-force/dictionary lookups, spoofing, and denial-of-service attacks) are the most common occurrences, because they're the easiest to mount against a target and require only basic Internet accessibility. Eavesdropping, sniffing, and man-in-themiddle attacks are more complex and involve an intrusion component to propel an attacker inside the network perimeter.

Methods of Attack

Brute-Force and Dictionary Attacks

We'll discuss brute-force and dictionary attacks together because they are waged against the same entity: **passwords**. Either type of attack can be waged against a password database file or against an active logon prompt.

A brute-force attack ***is an attempt to discover passwords for user accounts by systematically attempting every possible combination of letters, numbers, and symbols.*** With the speed of modern computers and the ability to employ distributed computing, brute-force attacks are becoming successful even against strong passwords. With enough time, all passwords can be discovered using a brute-force attack method. ***Most passwords of 14 characters or less can be discovered within 7 days on a fast system using a brute-force attack program.***

Methods of Attack

Brute-Force and Dictionary Attacks

The longer the password (or the greater the number of keys in an algorithm's key space), the more costly and time-consuming a brute-force attack becomes. When the number of **possibilities** is increased, the cost of performing an exhaustive attack increases as well. In other words, the longer the password, the more secure against brute-force attacks it is.

A dictionary attack ***is an attempt to discover passwords by attempting to use every possible password from a predefined list of common or expected passwords***. This type of attack is named such because the possible password list is so long, it is as if you were using the entire dictionary one word at a time to discover passwords.

Methods of Attack

Brute-Force and Dictionary Attacks

Passwords ***are stored in an account's database file on secured systems. However, instead of being stored as plain text, passwords are hashed, and only their hash values are actually stored***. This provides a **reasonable level of protection**. However, using reverse hash matching, a password attacker tool looks for possible passwords (through either brute-force or dictionary methods) that have the same hash value as a value stored in the account's database file. When a hash value match is discovered, then the tool is said to have *cracked* the password.

Combinations of these two password attack methodologies can be used as well. For example, a brute-force attack could use a dictionary list as the source of its guesswork

Methods of Attack

Brute-Force and Dictionary Attacks

Protecting passwords from brute-force and dictionary attacks requires numerous security precautions and rigid adherence to a strong security policy:

- **Controlling physical access to systems** (password file)
- **Controlling electronic access to password files** Tightly control and monitor electronic access to password files.
- **Creating a strong password policy**
- **Deploying two-factor authentication**
- **Using account lockout controls** Use account lockout controls to prevent brute-force and dictionary attacks against logon prompts.
- **Encrypting password files**

Methods of Attack

Denial-of-Service Attacks

Denial-of-service (DoS) ***attacks are attacks that prevent the system from processing or responding to legitimate traffic or requests for resources and objects. The most common form of denialof-service attacks is transmitting so many data packets to a server that it cannot process them all.*** Other forms of denial-of-service attacks focus on the exploitation of a known fault or vulnerability in an operating system, service, or application. ***Exploiting the fault often results in system crash or 100 percent CPU utilization.***

No matter what the actual attack consists of, any attack that renders the victim unable to perform normal activities can be considered a denial-of-service attack.

Denial-of-service attacks can result in ***system crashes***, ***system reboots***, ***data corruption***, ***blockage of services***, and more.

Unfortunately, denial-of-service attacks based on *flooding* (that is, sending sufficient traffic to a victim to cause a DoS) are a way of life on the Internet.

Methods of Attack

Denial-of-Service Attacks

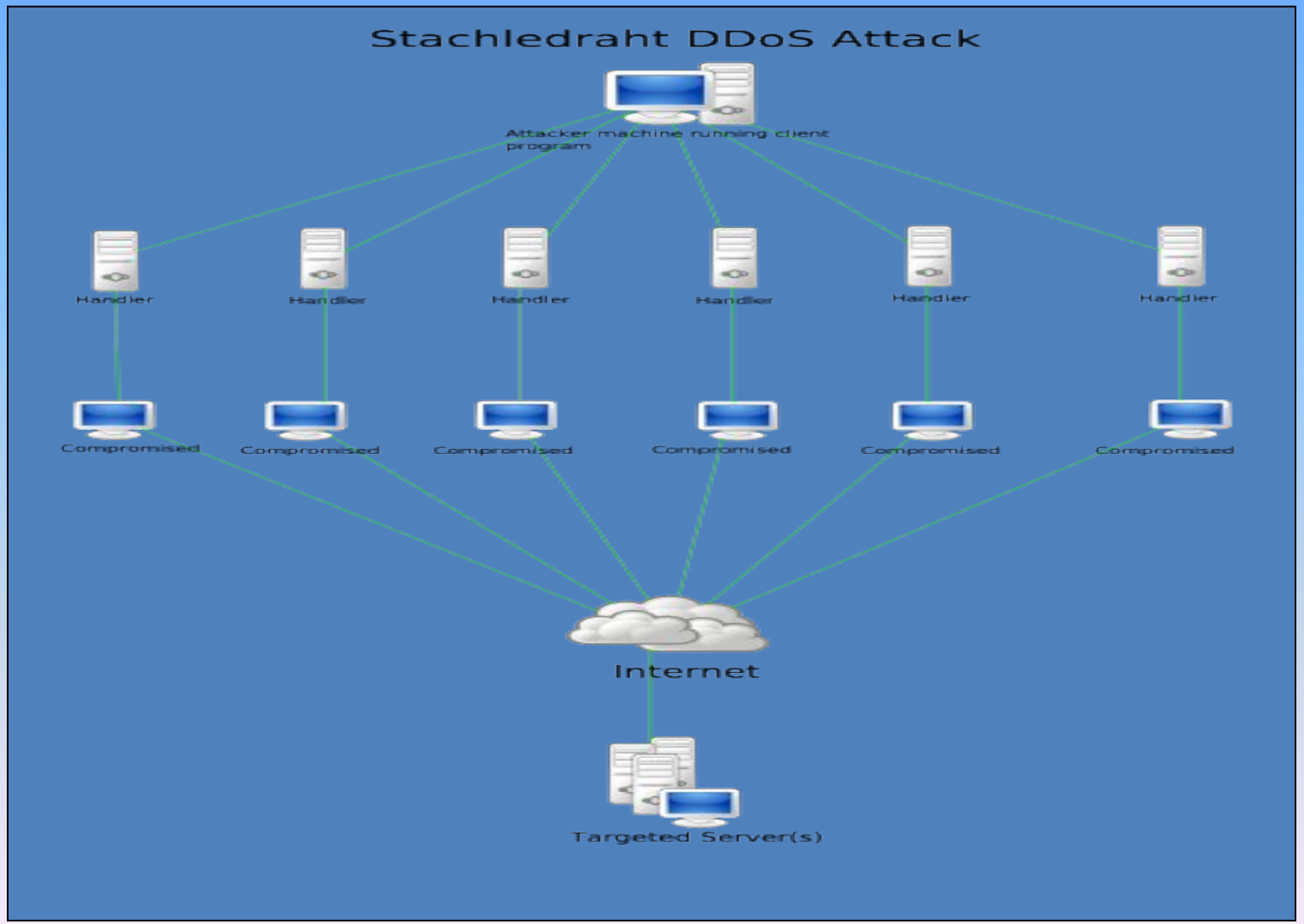
There are several types of DoS flood attacks. The first, or original, type of attack employed a **single attacking system** **flooding a single victim with a steady stream of packets**. Those packets could be valid requests that were never completed or malformed or fragmented packets that consume the attention of the victimized system. ***This simple form of DoS is easy to terminate just by blocking packets from the source IP address.***

Another form of attack is called the **distributed denial of service (DDoS).** A distributed denial of service occurs when the ***attacker compromises several systems and uses them as launching platforms against one or more victims.*** The compromised systems used in the attack are often called ***slaves*** or ***zombies***.

A DDoS attack results in the ***victims being flooded with data from numerous sources***.

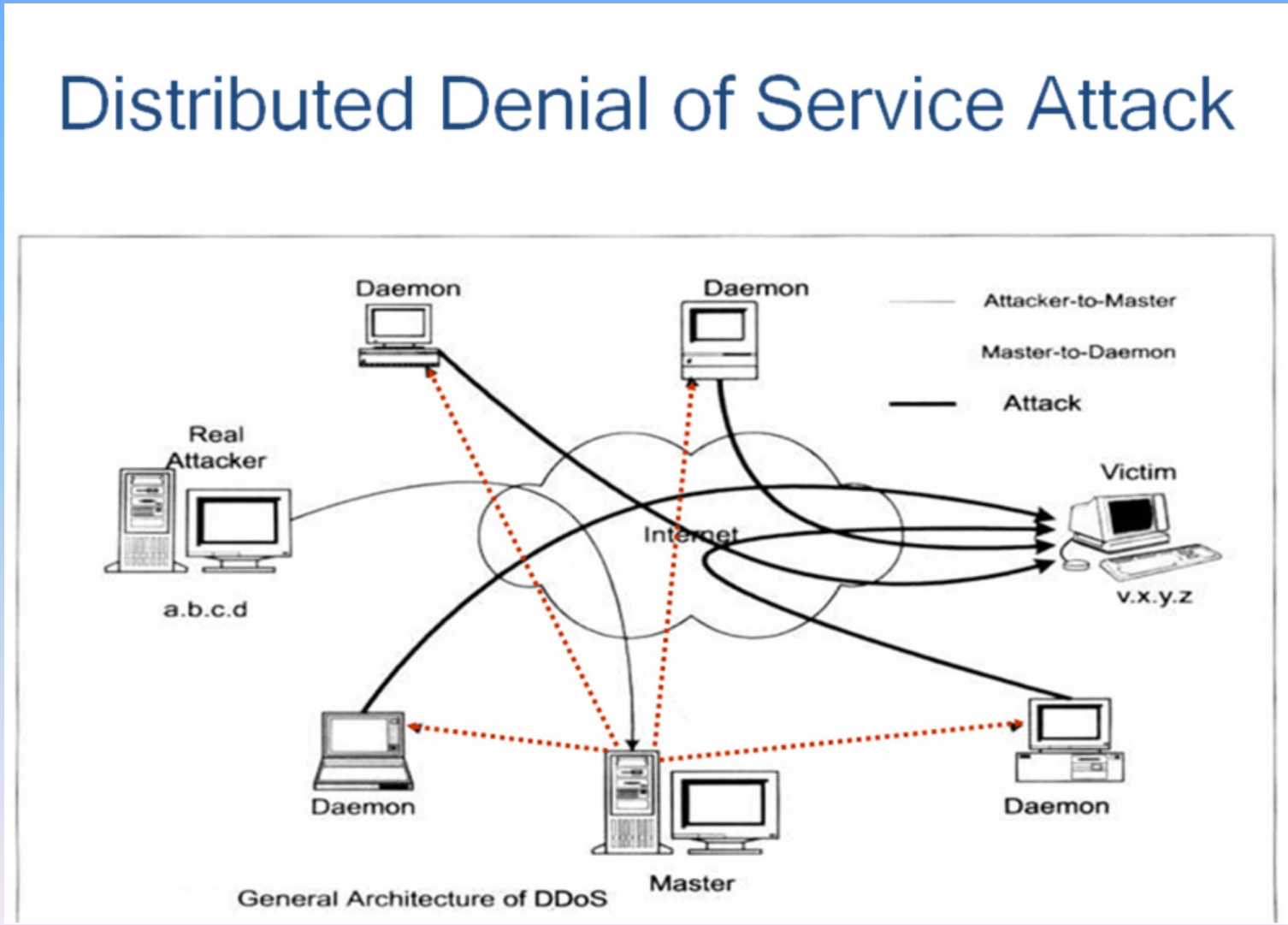
Methods of Attack

Denial-of-Service Attacks



Methods of Attack

Denial-of-Service Attacks



Methods of Attack

Denial-of-Service Attacks

A more recent form of DoS, called a **distributed reflective denial of service (DRDoS),** has been discovered. DRDoS attacks take advantage of the ***normal operation mechanisms of key Internet services, such as DNS and router update protocols***. **DRDoS attacks function** ***by sending numerous update, session, or control packets to various Internet service servers or routers with a spoofed source address of the intended victim.*** Usually these servers or routers are part of the high-speed, high-volume Internet backbone trunks. ***What results is a flood of update packets, session acknowledgment responses, or error messages sent to the victim***. A DRDoS attack can result in so much traffic that upstream systems are adversely affected by the sheer volume of data focused on the victim. This type of attack is called a *reflective attack* because the high-speed backbone systems reflect the attack to the victim. Unfortunately, these types of attacks **cannot be prevented** because they exploit **normal functions** of the systems. ***Blocking packets from these key Internet systems will effectively cut the victim off from a significant section of the Internet***.

Methods of Attack

Denial-of-Service Attacks

Not all instances of DoS are the result of a malicious attack. Errors in coding operating systems, services, and applications have resulted in DoS conditions. For example, a process failing to release control of the CPU or a ***service consuming system resources*** out of proportion to the service requests it is handling can cause DoS conditions. Most vendors quickly release patches to correct these self-inflicted DoS conditions, so it is important to stay informed.

Many forms of DoS attacks have been committed over the Internet. Specific, historically significant examples of denial-of-service attacks are discussed in greater detail throughout the remainder of this section.

HoneynetWeb.mov
how dos work.swf
Radware_Defense_Pro.swf
Riorey8.swf
Flash file

Methods of Attack

SYN Flood Attack

SYN flood ***attacks are waged by breaking the standard three-way handshake used by TCP/IP to initiate communication sessions***.

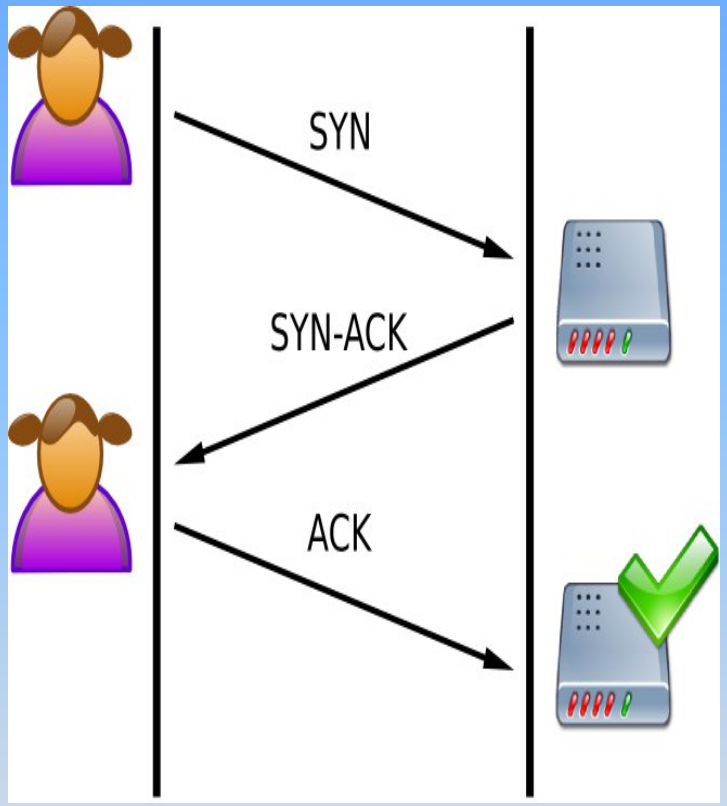
- A client sends a SYN packet to a server,
- The server responds with a SYN/ACK packet to the client,
- And the client then responds with an ACK packet back to the server.

This three-way handshake establishes a communication session that is used for data transfer until the session is terminated.

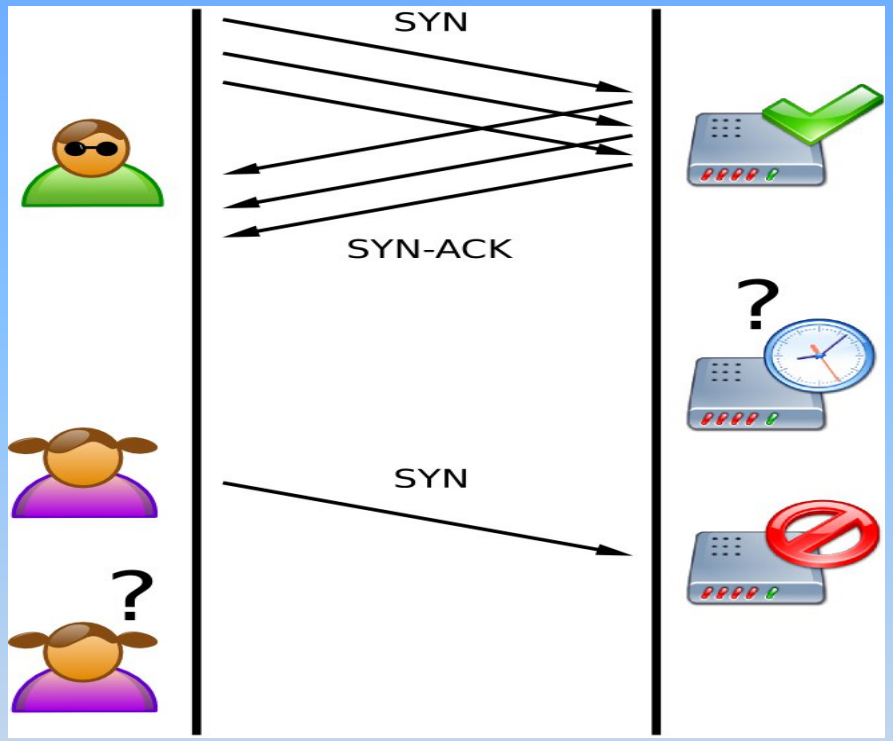
A SYN flood ***occurs when numerous SYN packets are sent to a server but the sender never replies to the server's SYN/ACK packets with the final ACK.***

Methods of Attack

SYN Flood Attack



A normal connection between a user (Alice) and a server. The three-way handshake is correctly performed.



SYN Flood. The attacker (Mallory) sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

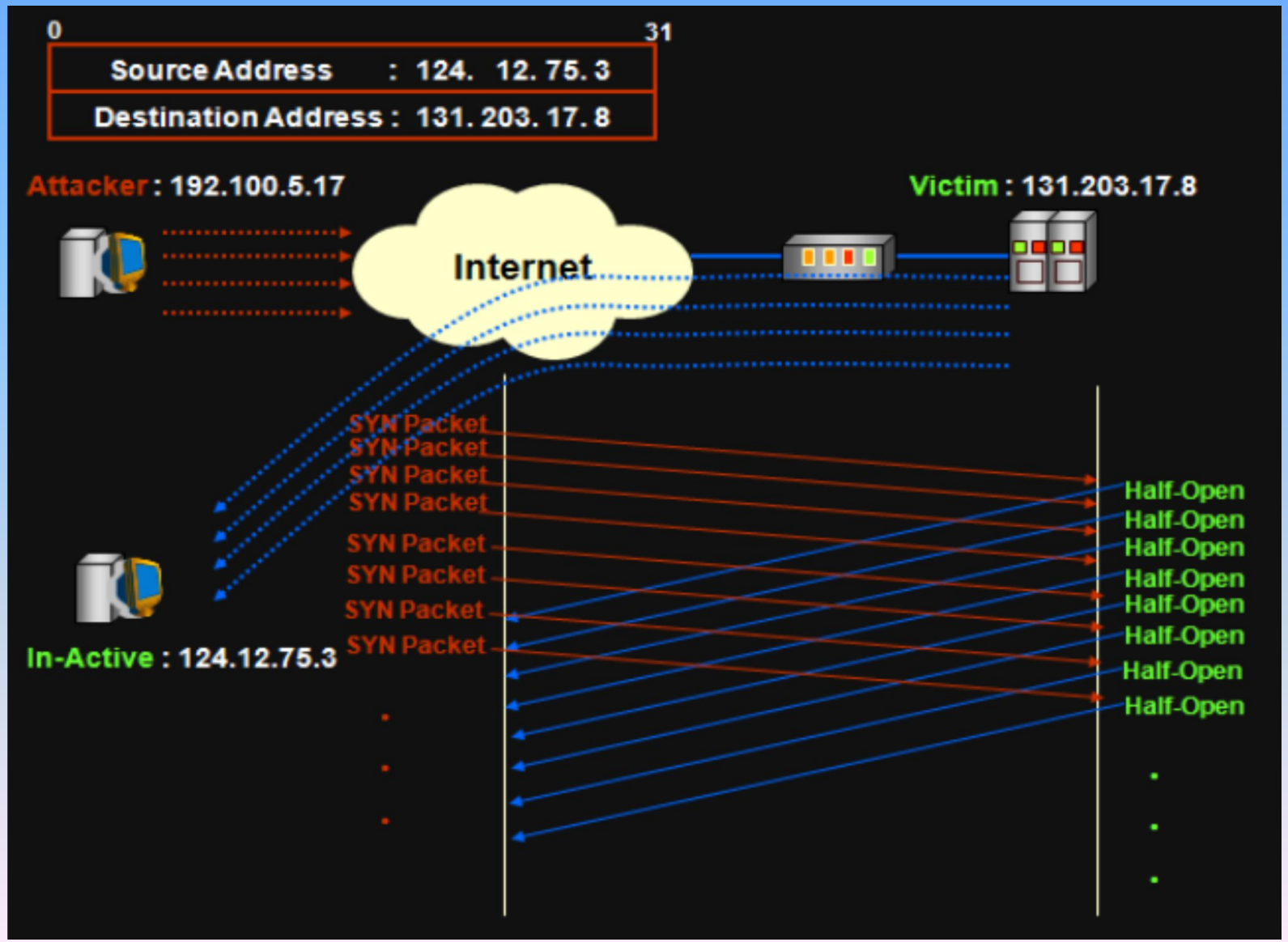
Methods of Attack

SYN Flood Attack

In addition, the transmitted SYN packets usually have a **spoofed source** address, so the SYN/ACK response is sent somewhere other than to the actual originator of the packets. ***The server waits for the client's ACK packet, often for several seconds, holding open a session and consuming system resources.*** If a significant number of sessions are held open (for example, through the receipt of a flood of SYN packets), this results in a DoS. The server can be easily overtaxed by keeping sessions that are never finalized open, thus causing a failure. That failure can be as simple as being unable to respond to legitimate requests for communications or as serious as a frozen or crashed system.

Methods of Attack

SYN Flood Attack



Methods of Attack

SYN Flood Attack

One countermeasure to SYN flood attacks is increasing the number of connections a server can support. However, this usually requires additional hardware resources (memory, CPU speed, and so on) and may not be possible for all operating systems or network services.

A more useful countermeasure is to ***reduce the timeout period for waiting for the final ACK packet***. ***However, this can also result in failed sessions from clients connected over slower links*** or can be hindered by intermittent Internet traffic. ***Network-based IDSs may offer some protection against sustained SYN flood attacks by noticing that numerous SYN packets originate from one or only a few locations***, resulting in incomplete sessions. An IDS could warn of the attack or dynamically block flooding attempts.

Methods of Attack

Smurf Attack

A smurf attack ***occurs when an amplifying server or network is used to flood a victim with useless data.***

One common attack is to send a message to the broadcast server of a subnet or network so that every node on the network produces one or more response packets. The attacker sends information request packets with the victim's spoofed source address to the amplification system. Thus, all the response packets are sent to the victim. ***The scenario of such an attack is as follows:***

•the attacking machine sends a ping request (ping is a tool that exploits the ICMP protocol, making it possible to test connections on a network by sending a packet and waiting for the response) to one or more broadcast servers while falsifying the source IP address (the address the server is supposed to respond to in theory) and providing the IP address of a target machine.

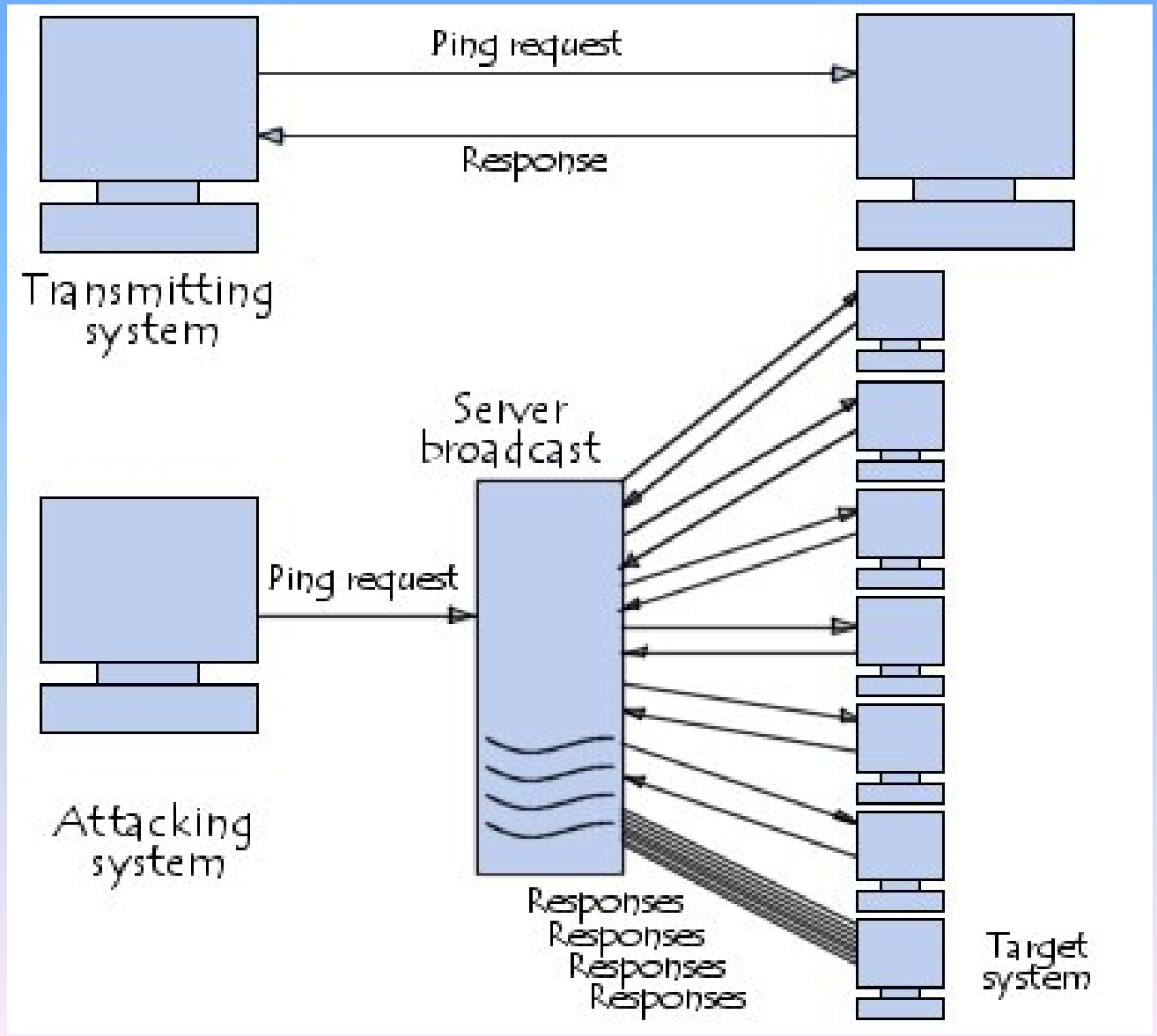
•the broadcast server passes on the request to the entire network;

•all of the network's machines send a response to the broadcast server,

•the broadcast server redirects the responses to the target machine.

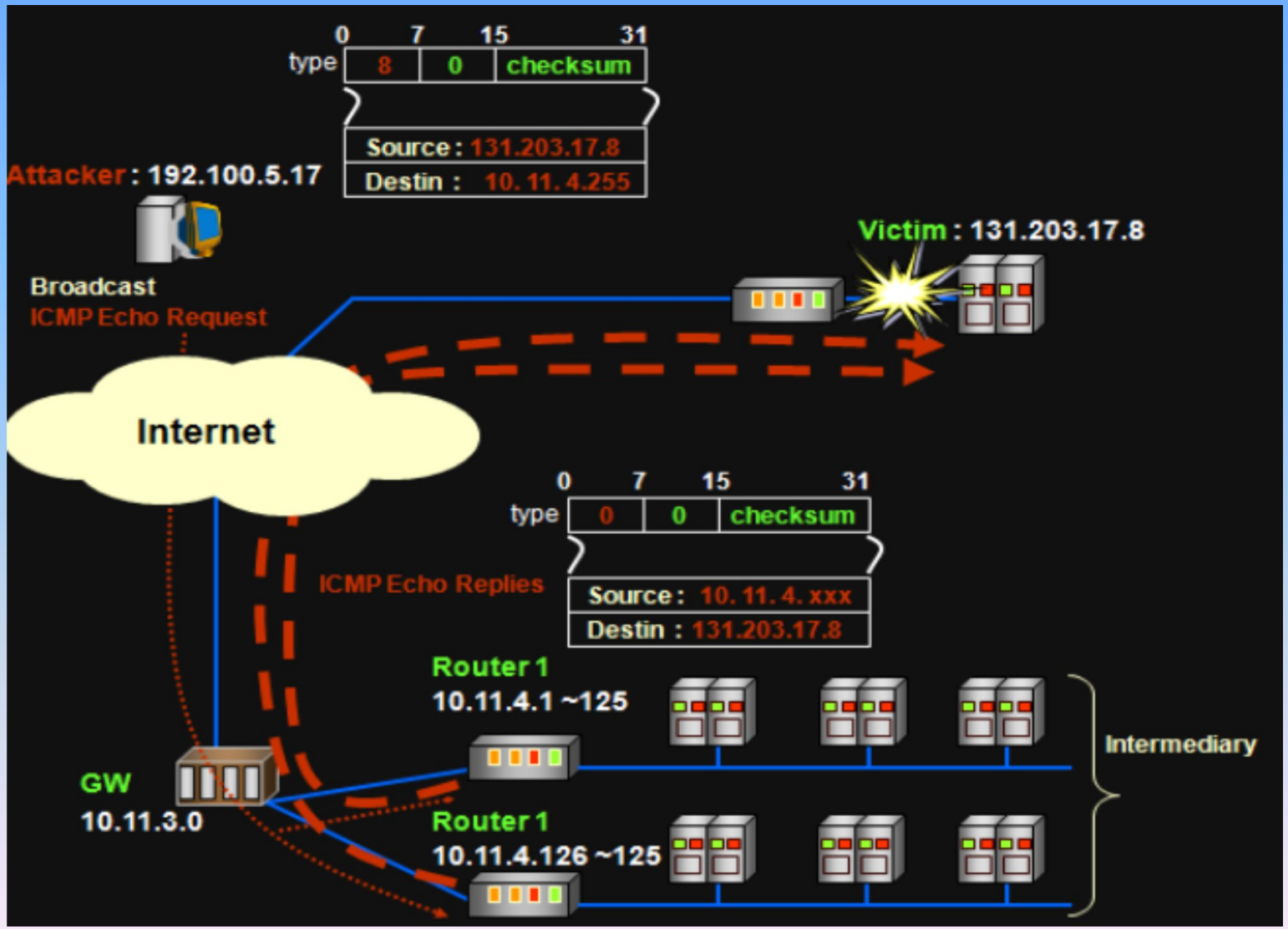
Methods of Attack

Smurf Attack



Methods of Attack

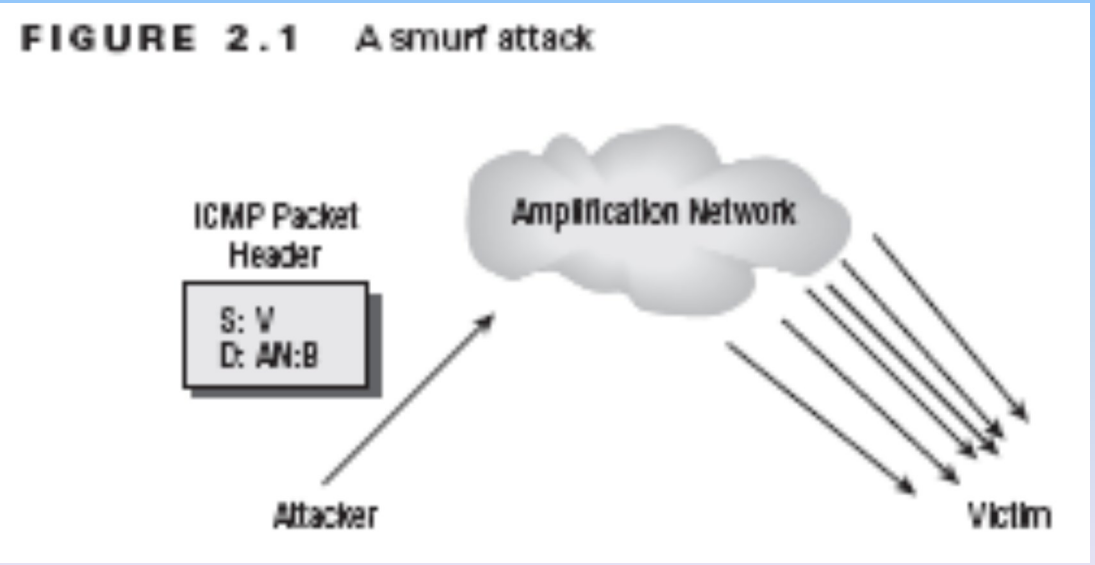
Smurf Attack



Methods of Attack

Smurf Attack

Countermeasures for smurf attacks include disabling directed broadcasts on all network border routers and configuring all systems to drop ICMP ECHO packets. ***An IDS may be able to detect this type of attack, but there are no means to prevent the attack other than blocking the addresses of the amplification network. This tactic is problematic because the amplification network is usually also a victim.***



Methods of Attack

Ping-of-Death, WinNuke, Stream, Teardrop, and Land Attacks

The attacks named in this section head date back as far as the 1990s, but each uses interesting and devastating (at the time of their creation) techniques to subvert how incoming IP data is handled on the unwitting recipient's end. In the interim, specific defenses have been erected so that these attacks have very little chance of succeeding today.

A **ping-of-death** attack employs an oversized ping packet. Using special tools, ***an attacker can send numerous oversized ping packets to a victim***. In many cases, ***when the victimized system attempts to process the packets, an error occurs, causing the system to freeze, crash, or reboot***. The ping of death is more of a ***buffer-overflow attack, but because it often results in a downed server, it is considered a DoS attack***. Countermeasures to the ping-of-death attack include keeping up-to-date with OS and software patches, properly coding in-house applications to prevent buffer overflows, avoiding running code with system- or root-level privileges, and blocking ping packets at border routers/firewalls.

Methods of Attack

Ping-of-Death, WinNuke, Stream, Teardrop, and Land Attacks

A **WinNuke** ***attack is a specialized assault against Windows 95 systems***. ***Out-of-band TCP data is sent to a victim's system, which causes the OS to freeze***. Countermeasures for this attack consist of updating Windows 95 with the appropriate patch or changing to a different OS.

A **stream** ***attack occurs when a large number of packets are sent to numerous ports on the victim system using random source and sequence numbers.*** The processing performed by the victim system attempting to make sense of the data will result in a DoS. Countermeasures include patching the system and using an IDS for dynamic blocking.

A **teardrop** ***attack occurs when an attacker exploits a bug in operating systems. The bug exists in the routines used to reassemble (that is, resequence) fragmented packets***. An attacker sends numerous specially formatted fragmented packets to the victim, which causes the system to ***freeze or crash***. Countermeasures for this attack include patching the OS and deploying an IDS for detection and dynamic blocking.

Methods of Attack

Ping-of-Death, WinNuke, Stream, Teardrop, and Land Attacks

A **land** ***attack occurs when the attacker sends numerous SYN packets to a victim and the SYN packets have been spoofed to use the same source and destination IP address and port number as the victim.*** This causes the system to think it sent a TCP/IP session opening packet to itself, which causes a system failure and usually results in a system freeze, crash, or reboot. Countermeasures for this attack include patching the OS and deploying an IDS for detection and dynamic blocking.

Methods of Attack

Beware the Botnets!

All the older attack methods described in the preceding section are well documented today, which grants them zero stealth and minimal effectiveness when used against modern computing networks and operating systems. A more troubling trend has, however, emerged in recent years, including the rise of **botnets**. ***These are coordinated networks of compromised machines used in a cohesive or scheduled manner to attack, compromise, and disrupt other end users or entire networks.*** They are also widely employed to distribute spam on behalf of third parties who seek to find paying customers through unwanted email or to disseminate phishing lures to part unwary or naive recipients from their hard-earned cash.

botnets_MR_en.swf

Methods of Attack

Beware the Botnets!

For every botnet, there is usually one or more controlling computers, often called *botnet controllers*, which provide cutouts between the actual botnet operator (usually called a *bot herder*) and the compromised machines. ***This enables bot herders to control larger number of computers (many botnets number in excess of 100,000 compromised PCs, and some instances of botnets in excess of a million machines have been reported in 2007 and 2008) and to protect themselves from discovery even if their botnets are detected and disabled***.

With hundreds of thousands to millions of potential attacking machines in their corrals, the ability of botnets to mount huge and devastating ***DoS attacks is painfully obvious***. As we write this chapter, they've been used recently to slow down or deny access to global portals including **Google, Yahoo, and Microsoft.**

Methods of Attack

Spoofing Attacks

Spoofing ***is the art of pretending to be something other than what you are. Spoofing attacks consist of replacing the valid source and/or destination IP address and node numbers with false ones.*** Spoofing is involved in most attacks because it grants attackers the ability to hide their identity through misdirection.

Spoofing is employed when an intruder uses a stolen username and password to gain entry, when an attacker changes the source address of a malicious packet, or when an attacker assumes the identity of a client to fool a server into transmitting controlled data.

Methods of Attack

Spoofing Attacks

Two specific types of spoofing attacks are ***impersonation*** and ***masquerading***. Ultimately, these attacks are the same: someone is able to gain access to a secured system by pretending to be someone else. These attacks often result in an unauthorized person gaining access to a system through a valid user account that has been compromised. **Impersonation** ***is considered a more active attack because it requires the capture of authentication traffic and the replay of that traffic in such a way as to gain access to the system.*** **Masquerading** ***is considered a more passive attack because the attacker uses previously stolen account credentials to log on to a secured system.***

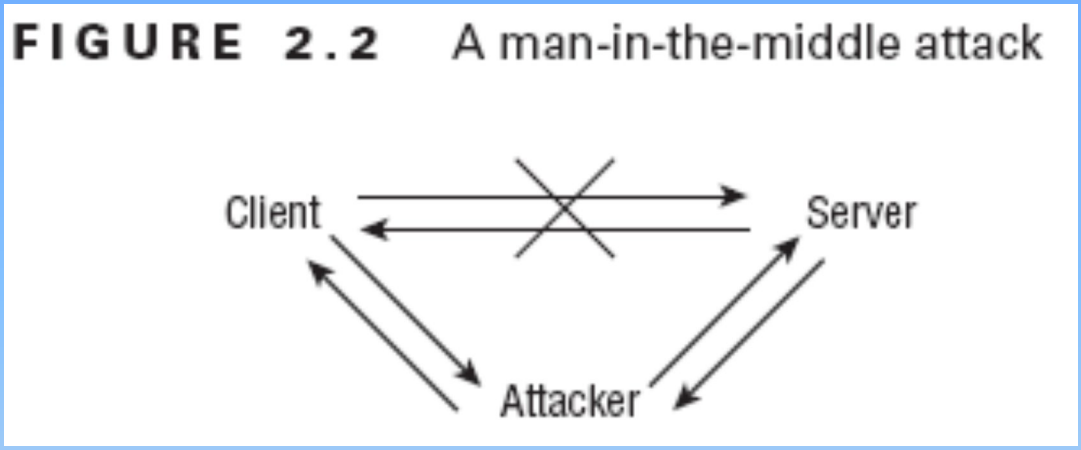
Methods of Attack

Man-in-the-Middle Attacks

A man-in-the-middle ***attack occurs when a malicious user is able to gain a position between the two endpoints of an ongoing communication.*** There are two types of man-inthe-middle attacks. One involves **copying** or sniffing ***the traffic between two parties***; this is basically a sniffer attack (see the next section). ***The other involves attackers positioning themselves in the line of communication where they act as a store-and-forward or proxy mechanism*** (see Figure 2.2). The attacker functions as the receiver for data transmitted by the client and the transmitter for data sent to the server. The ***attacker is invisible to both ends*** of the communication link and is able to alter the content or flow of traffic. Through this type of attack, the attacker can ***collect logon credentials or sensitive data as well as change the content of the messages exchanged between the two endpoints .***

Methods of Attack

Man-in-the-Middle Attacks



To perform this type of attack, the attacker must often alter routing information and DNS values, steal IP addresses, or defraud ARP lookups to impersonate the server from the perspective of the client and to impersonate the client from the perspective of the server.

An offshoot of a man-in-the-middle attack is known as a **hijack attack**. In this type of attack, ***a malicious user is positioned between a client and server and then interrupts the session and takes it over***. Often, the malicious user impersonates the client to extract data from the server. The server is unaware that any change in the communication partner has occurred. The client is aware that communications with the server have ceased, but no indication as to why the communications were terminated is available.

Methods of Attack

Man-in-the-Middle Attacks

Another type of attack, a *replay attack* (also known as a **playback attack**), is similar to hijacking. ***A malicious user records the traffic between a client and server; then the packets sent from the client to the server are played back or retransmitted to the server with slight variations of the time stamp and source IP address (that is, spoofing).*** In some cases, this allows the malicious user to restart an old communication link with a server. Once the communication session is reopened, the malicious user can attempt to obtain data or additional access. The captured traffic is often authentication traffic (which typically includes logon credentials, such as username and password), but it could also be service access traffic or message control traffic. Replay attacks can be prevented by employing complex sequencing rules and time stamps to prevent retransmitted packets from being accepted as valid.

Methods of Attack

Man-in-the-Middle Attacks

Countermeasures to these types of attacks require ***improvement in the session establishment, identification, and authentication processes***. Some man-in-the-middle attacks are thwarted through patching the OS and software. An IDS cannot usually detect a man-in-the-middle or hijack attack, but it can often detect the abnormal activities occurring via “secured” communication links. Operating systems and many IDSs can often detect and block replay attacks.

Methods of Attack

Sniffer Attacks

A sniffer attack (also known as a ***snooping*** attack) ***is any activity that results in a malicious user obtaining information about a network or the traffic over that network.*** A sniffer is often a packet- capturing program that duplicates the contents of packets traveling over the network medium into a file. ***Sniffer attacks often focus on the initial connections between clients and servers to obtain logon credentials (for example, usernames and passwords), secret keys, and so on.*** When performed properly, sniffing attacks are invisible to all other entities on the network and often precede spoofing or hijack attacks. A replay attack (discussed in the preceding section) is a type of sniffer attack.

Countermeasures to prevent or stop sniffing attacks require ***improving the physical access control, actively monitoring for sniffing signatures*** (such as looking for packet delay, additional routing hops, or lost packets, which can be performed by some IDSs), ***and using encrypted traffic over internal and external network connections***.

Methods of Attack

Spamming Attacks

Spam ***is the term describing unwanted email, newsgroup, or discussion forum messages***. Spam can be as innocuous as an advertisement from a well-meaning vendor or as malignant as floods of unrequested messages with viruses or Trojan horses attached. ***Spam is usually not a security threat but rather a type of denial-of-service attack***. As the level of spam increases, locating or accessing legitimate messages can be difficult. In addition to the nuisance value, spam consumes a significant portion of Internet resources (in the form of bandwidth and CPU processing), resulting in overall slower Internet performance and lower bandwidth availability for everyone.

Spamming attacks ***are directed floods of unwanted messages to a victim's email inbox or other messaging system. Such attacks cause DoS issues by filling up storage space and preventing legitimate messages from being delivered***. In extreme cases, spamming attacks can cause system freezes or crashes and interrupt the activity of other users on the same subnet or ISP.

Spam attack **countermeasures** include using ***email filters, email proxies, and IDSs to detect, track, and terminate spam flood attempts***.

Methods of Attack

Crackers, Hackers, and Attackers

Crackers ***are malicious users intent on waging an attack against a person or system***. Crackers may be motivated by greed, power, or recognition. ***Their actions can result in stolen property (data, ideas, and so on), disabled systems, compromised security, negative public opinion, loss of market share, reduced profitability, and lost productivity***.

A term commonly confused with *crackers* is *hackers*, who are technology enthusiasts with no malicious intent. Many authors and the media often use the term *hacker* when they are actually discussing issues relating to crackers. To avoid confusion, we use the term ***attacker for malicious intruders*** throughout this book.

Thwarting an attacker's attempts to breach your security or perpetrate DoS attacks requires vigilant effort to keep systems patched and properly configured. **IDSs and honey pot systems** often offer means to detect and gather evidence to prosecute attackers once they have breached your controlled perimeter.

Access Control Compensations

Access control is used to regulate or specify which objects a subject can access and what type of access is allowed or denied. ***Numerous attacks, discussed in the previous sections, are designed to bypass or subvert access control.*** In addition to the specific **countermeasures** for each of these attacks, ***you can use certain measures to help compensate for access control violations***. A ***compensation measure is not a direct prevention of a problem but rather a means by which you can design resiliency into your environment to provide support for a quick recovery or response***.

Backups ***are the best means to compensate against access control violations***. With reliable backups and a mechanism to restore data, any corruption or file-based asset loss can be repaired, corrected, or restored promptly. RAID technology can provide fault tolerance to allow for quick recovery in the event of a device failure or severe access violation.

Access Control Compensations

In general, avoiding single points of failure and deploying fault-tolerant systems can help ensure that the loss of use or control over a single system, device, or asset does not directly lead to the compromise or failure of your entire network environment. **Fault tolerance countermeasures** ***are designed to combat threats to design reliability***. Having backup communication routes, mirrored servers, clustered systems, failover systems, and so on, can provide instant automatic or quick manual recovery in the event of an access control violation.

Your business continuity plan should include procedures for dealing with access control violations that threaten the stability of your mission-critical processes. Likewise, you should include in your insurance coverage categories of assets for which you may require compensation in the event of severe access control violations.

Exam Essentials

mxl_eds_layersdemo2.swf
01CIEGE.swf
02CIEGE.swf
03CIEGE.swf
04CIEGE.swf
05CIEGE.swf
06CIEGE.swf
D F L - M 5 1 0 . s w f
iwss.swf
layered_defense_loader.swfmxl_eds_layersdemo2.swf
01CIEGE.swf
02CIEGE.swf
03CIEGE.swf
04CIEGE.swf
05CIEGE.swf
06CIEGE.swf
DFL-M510.swf
iwss.swf

06CIEGE.swf
D F L - M 5 1 0 . s w f