

ATME COLLEGE OF ENGINEERING

13th KM Stone, Bannur Road, Mysore - 560 028



A T M E

College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

- CYBER SECURITY



LECTURE NOTES

COURSE: Hackers Technique, Tools and Incident Handling

COURSE CODE: BCY515C

SEMESTER: V

COURSE COORDINATOR: Ms. Darshini Y

(ACADEMIC YEAR 2026)

INSTITUTIONAL MISSION AND VISION

Objectives

- To provide quality education and groom top-notch professionals, entrepreneurs and leaders for different fields of engineering, technology and management.
- To open a Training-R & D-Design-Consultancy cell in each department, gradually introduce doctoral and postdoctoral programs, encourage basic & applied research in areas of social relevance, and develop the institute as a center of excellence.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To cultivate strong community relationships and involve the students and the staff in local community service.
- To constantly enhance the value of the educational inputs with the participation of students, faculty, parents and industry.

Vision

Development of academically excellent, culturally vibrant, socially responsible and globally competent human resources.

Mission

- To keep pace with advancements in knowledge and make the students competitive and capable at the global level.
- To create an environment for the students to acquire the right physical, intellectual, emotional and moral foundations and shine as torch bearers of tomorrow's society.
- To strive to attain ever-higher benchmarks of educational excellence

MODULE 5

Chapter 1. Incident Response

AS A SECURITY PROFESSIONAL, you will be versed in a number of different technologies and techniques, each designed to prevent an attack and secure the organization. Each of the techniques you will learn is meant to prevent an attack or limit its scope, but the reality is that attacks can and will happen, and the techniques you have learned in this course cannot ever be guaranteed to stop an attack from penetrating your organization. As a security professional, this is a reality that you will have to accept.

Once you have accepted that an attack will inevitably penetrate your organization at some point, your job now becomes one of how to respond to these situations: This is the role of incident response. Incident response, as the name implies, is the process of how you and your organization will respond to a security incident when it occurs. Although security incidents are bound to happen, you shouldn't sit by and let them happen. You have to know how you will respond and the details to this response.

Incident response is not only the act of how you respond to a security incident but also the details involved in that response. If you respond incorrectly to an incident you could make a bad situation worse. For example, not knowing what to do, whom to call, or what the chain of command is in these situations would potentially do further damage.

Finally, something that will have substantial impact on incident response is its potential legal aspect. When a security incident happens, it may frequently fall under the banner of computer or related crimes, so it might require that additional care be taken when responding. When you decide that you wish to pursue criminal charges, you move from the realm of just responding to performing a formal investigation. The formal investigation will include special techniques for gathering and processing evidence for the purpose of potentially prosecuting the criminal later.

This chapter investigates and examines the various aspects of incident response and how you can plan and design a process for responding to that breach in your organization.

Chapter 14 Topics

This chapter covers the following topics and concepts:

- What a security incident is
- What the process of incident response is
- What incident response plans (IRPs) are
- What planning for disaster and recovery is
- What evidence handling and administration is
- What requirements of regulated industries are

Chapter 14 Goals

MODULE 5

When you complete this chapter, you will be able to:

- List the components of incident response
- List the goals of incident response

What Is a Security Incident?

A security **incident** in an organization is a serious event that can occur at any point from the desktop level to the servers and infrastructure that make the network work. A security incident can be anything including accidental actions that result in a problem up to and including the downright malicious. Regardless of why a security incident occurred, the organization must respond appropriately.

A security incident can cover a lot of different events, but to clarify what constitutes a security incident, the following guidelines tend to apply:

- The result is the theft or misuse of confidential information of any type, such as customer information, patient information, or financial information.
- It substantially affects the network infrastructure and services, such as performance or security.
- It inadvertently provides unauthorized access to any resource.
- It provides a platform for launching attacks against a third party.

Other events can and will be included on this list, depending on the organization and the environment in which it functions. For example, a company in the health care field would include additional events that pertain to patient information and unauthorized access to this information. A security incident can be simply thought of as an event or situation that adversely impacts the security stance of the organization.

FYI

The concept of investigating a crime versus investigating an incident can be confusing. In reality, there are a couple of points to consider when deciding the best course of action:

- Unless it is a serious crime with effects outside of your organization (for example, murder or theft of credit card information), you have no legal obligation to involve the police or press charges. Many businesses may opt not to report computer crimes because the fact that they were victimized may lead to bad publicity.
- In the event of an incident in which you do want to involve law enforcement, you will follow the rules of **evidence**. If you think things are moving toward this end, you should not try to handle things internally; instead, opt to let law enforcement professionals deal with the incident.

MODULE 5

The Incident Response Process

As a security professional, you are responsible for reducing the chance of a security breach or incident to the lowest possible level. However, no matter how hard you try, the reality is that you are only reducing the chance of a security incident, not eliminating it, which is nearly impossible. So as a well-prepared professional you must plan how you will react when a security incident occurs. This planning will reap benefits, as it will give you the edge when determining what to do after an incident and how to do it. Proper security incident response will determine whether an incident is dealt with swiftly and completely or if it gets worse and out of control.

One of the first things to keep in mind when thinking about incident response is the fact that you are very likely dealing with something that falls under the realm of crime, so it will require that special care. Responding to an incident of **computer crime** can be particularly challenging, as the evidence that needs to be collected is intangible.

FYI

Computer crime is already defined and covered in the United States (and other countries') legal codes) with varying degrees of scope and penalties. In the United States, computer crime is covered primarily under U.S. Code Title 18, 1030, titled "Fraud and related activity in connection with computers." This code is part of the Computer Fraud and Abuse Act of 1986 and has been amended three times since then: in 1994, 1996, and 2001.

When computer crime involves attacks or activities that cross state or even national borders, the rules can change substantially. The very definition of computer crime can vary widely depending on the jurisdiction involved. Therefore a computer crime involving more than one jurisdiction will require much more care.

Computer crime is defined as a criminal act in which a computer or similar device is involved as either the source or target of an attack. Computer crime can involve any act that affects national security or involves fraud, identity theft, or the distribution of malware. Computer crime does not discriminate against activities that are initiated via the Internet or launched from a private network.

Incident Response Policies, Procedures, and Guidelines

The next point that is important when considering incident response is to have a policy in place that defines the procedures and guidelines for responding to a security incident. The policy will define the course of action that a company or organization will take in the time following a security incident. The policy is quite commonly supplemented by procedures and guidelines that specify additional details, but the following are usually included:

- The individuals who will take responsibility for determining when and if a security incident has occurred

MODULE 5

- The individuals and/or departments that are to be part of the initial notification that a security incident has occurred
- The means through which they will be notified: e-mail, phone, or face to face
- The responsible person or parties that will take lead for responding to the incident
- Appropriate response guidelines for the given security incident

So, who will be involved in the incident response process? This depends on the organization, the assets involved, and the overall severity of the situation. Several departments within an organization can work together—human resources, public relations, information technology, corporate security, and others. The idea is to get the appropriate personnel and departments involved in order to properly deal with the situation at hand. These key people can also determine which information can be released and to whom. For example, employees may not be privy to all the details of security incident and may in fact be informed on only a need-to-know basis.

FYI

No less important in this process is the control of information or "need to know." The knowledge of an incident in the wrong hands can be catastrophic. Information of a security breach can rattle the confidence of the public, shareholders, employees, and customers, and as such should be tightly controlled wherever possible. The parties that are part of the first response effort will typically be the only ones with definite need to know, with others being added to the list later on.

Phases of an Incident and Response

There are several phases in the incident response process. Each incident will traverse these phases as the incident occurs, evolves, and moves to its final resolution. Every phase has distinct actions that take place within it, which you will learn more about as you move on, but let's take a high-level look at the incident response process itself. [Table 14-1](#) defines the phases of incident response and what happens at each step.

NOTE

Some organizations may add or remove steps in this process based on need or their unique situation, but generally will follow similar steps. The idea is to have a process clearly defined and to know responsibilities ahead of time so when a security incident happens, you know the process to deal with it.

Incident Response Team

As organizations grow in size and importance, it is likely that they will build or already have a group known as an incident response team. These teams will be composed of individuals that have the training and experience to properly collect and preserve evidence of a crime and the associated components of the response process. Incident response teams must have both the proper training and the requisite experience to respond to and investigate a security incident. As a security

MODULE 5

professional, it is very likely that you will take part in this team in some capacity as a key member or otherwise.

One of the components of incident response is the first responder or responders who will be the initial individuals to respond to an incident when one is reported. In the broadest sense, these can be the individuals appropriate for the security incident concerned, including the following:

- IT personnel
- Legal representation
- Leaders from affected departments
- Human resources
- Public relations
- Security officers
- Chief security officer

The goal of your security response team is to have in place key people who are well versed in and aware of how to deal with security incidents. These members will know what to do and have been drilled on how to do it in the event an incident occurs.

Table 14-1. Phases of incident response.

PHASE	DESCRIPTION
Incident identification	It is important for you to establish early on just what has actually occurred. Is the incident an actual security incident or is it something else? The incident response team will be responsible for making this determination as well as making the determination or discovery as to what was affected.
Triage	The next step after the determination that a security incident has occurred is to determine how seriously the incident has affected critical systems or data. Remember that not all systems or services will be affected the same way, and some will require more attention than others. Also remember that some systems are mission-critical and will require more attention as well. In a computer crime incident scenario, once the incident response team has evaluated the situation and determined the extent of the incidents, a triage approach will be implemented, and the situation will be responded to according to criticality. If multiple events have occurred, the most serious event will be addressed first, and remaining events will be investigated based on risk level.
Containment	It is necessary early on in the process of the incident response to contain and control the crime scene as much as possible. It is important that no

MODULE 5

PHASE	DESCRIPTION
	alterations of the crime scene or tampering of any sort occur to avoid damaging evidence. Disconnecting any devices, wires, peripherals, or even shutting down the system would constitute tampering. It is important to let trained professionals do their job at the crime scene.
Investigation	As the response team discovers the cause of the problem, the investigative process can start. The investigation is designed to methodically collect evidence without destroying or altering it in any way. This process can be performed by internal personnel or optionally by an external team where appropriate. The key detail in either case is that the team involved in the investigative process understand how to collect the evidence properly, as the end result of the process may be to take this collected information to court. So who may investigate a security incident? This may vary depending on the extent and type of security breach. In some cases, internal teams or consultants may be all that are needed to investigate and analyze a crime scene; however, in some cases that may not be enough. It is possible under certain conditions to get local law enforcement involved in the investigation of a crime. Of course this option will vary, depending on the skills of local law enforcement. In some cases police departments are very adept at dealing with computer crime, but this is not always the case. Investigations should never be taken lightly and once local law enforcement is involved, other issues arise. Police departments may not be able to respond in a timely fashion, as corporate security problems are not part of the police mission and therefore are low priority.
Analysis and tracking	Evidence that has been gathered is useless unless it is examined and dissected to determine what has occurred. At this point you will either be involving external professionals to examine the evidence or employing your own internal teams. These teams will be responsible for determining what evidence is relevant to the investigation and which is not.
Recovery and Repair	During the recovery and repair phase it is assumed that all relevant evidence has been collected and the scene has been cleaned. At this point the investigation of the security incident has been completed and the

MODULE 5

PHASE	DESCRIPTION
	affected systems can be restored and returned to service. This process will include restoring and rebuilding operating systems with their applications and data from backups or drive images. In the event that a system has experienced substantial damage in the course of an attack, it becomes necessary to repair the system. The recovery process is designed to deal with rebuilding a system after evidence has been collected, but it does not account for potential damages done that may need to be repaired. Additionally, the repair process may be needed as the collected evidence may have required the removal of components (that will need to be replaced) for preservation of evidence.
Debriefing and feedback	When it is all said and done, you will need to debrief and obtain feedback from all involved. The incident happened for a reason and presumably at this point you have determined what this reason is. The goal of this phase is to determine what you did right, what you did wrong, and how to improve. The lessons learned during this debriefing can then be used to determine the changes that will be made to improve the incident response process for the next time it is put into effect. Additionally, depending on the incident it may be necessary to start the process of informing clients and other agencies and regulatory bodies of the breach. This last point may in fact be the most important one because failure to inform the appropriate regulatory bodies can mean you or your company is guilty of a crime.

FYI

It is not unheard of for an organization to have no IRP or one that is grossly out of date. In some cases, organizations had a sound security response plan at one point, but it was never updated, resulting in a plan that cannot effectively deal with current situations. In other cases, this plan was overlooked, meaning that no one ever got around to or even thought of creating one in the first place.

Incident Response Plans (IRPs)

The composition of the response team is important, but so is the process team members must follow to respond to an incident. Once a security incident has been recognized and declared, it is vital that the team have a plan to follow. This **incident response plan (IRP)** will include all the steps and details required to investigate the crime as necessary.

MODULE 5**NOTE**

Remember that a security IRP will include all the steps needed to address a security incident and legally protect the company. A security incident that is investigated improperly can result in substantial legal problems for the company.

The Role of Business Continuity Plans (BCPs)

A plan that will become an important part of security in your organization is an item known as a business continuity plan (BCP). This policy defines how the organization will maintain what is accepted as normal day-to-day business in the event of a security incident or other events disruptive to the business. The importance of the BCP cannot be overstated as it is a necessary item in ensuring that the business continues to perform and can survive through a disaster. A BCP ensures protection for vital systems, services, and documents, informing key stakeholders and recovering assets as necessary. The BCP will include issues relating to infrastructure and maintaining the services needed to keep the business running using techniques such as fault tolerance and high availability. Furthermore, because the business requirements change periodically, the BCP will need to be reviewed on a regular basis to ensure it is still relevant.

FYI

A BCP does not dictate how the entire business will be brought back to an operational state; it addresses how to maintain some semblance of business operations. A BCP is designed to ensure that your company continues to deliver on its mission in the event of either a human or natural disaster. Cleaning up and restoring the business in the event of a disaster is the responsibility of a disaster recovery plan (DRP).

Next to a BCP, and closely intertwined with it, is the DRP. This document or plan states a policy that defines how personnel and assets will be safeguarded in the event of a disaster and how those assets will be restored and brought back to an operating state after the disaster passes. The DRP typically will include a list of responsible individuals that will be involved in the recovery process, hardware and software inventory, steps to respond and address the outage, and ways to rebuild affected systems.

Techniques That Support Business Continuity and Disaster Recovery

There are several techniques that can be used to keep the organization running and diminish the impact of a disaster when it occurs. Several of these techniques are discussed in this section.

Fault tolerance is a valuable tool in your arsenal, as it will give you the ability to weather potential failures while still providing some measure of service. While this level of service may not be optimal, it should be enough to maintain some level of business operations even if not at the normal level of performance. Fault tolerant mechanisms include service and infrastructure duplication designed to handle a component failure when it occurs.

MODULE 5

Common examples of fault tolerant devices include:

- **Redundant array of independent disks (RAID)**—Provides an array of disks that are configured so that if one disk fails, access to data or applications is not affected
- **Server clustering**—A technique used to group servers together in such a way that if one server fails, access to an application is not lost
- **Redundant power**—Can be provided by using systems such as backup generators and uninterrupted power supplies

Another tool in your toolbox is something known as high availability. This technique is simply a gauge of how well the system is providing its service, specifically how available the system actually is. Ideally a system should be available 100 percent of the time, but in practice this is not possible. High availability simply states, as a percentage, how available a system is, so the closer a system's availability is to 100 percent, the less time it has spent offline. High availability can be attained by having redundant and reliable backup systems.

FYI

Fault tolerance can be applied to just about any service and system available, with the limiting factors being cost and requirements. You will use fault tolerant mechanisms on those systems and services that are deemed of a higher importance and would adversely affect the business if they were taken offline. In cases where the cost of the fault tolerance systems is higher than the cost of actually losing the service, the use of such systems would be unnecessary.

An item that is generally not found too far from high availability and fault tolerance is something known as a service level agreement (SLA). This is a document that spells out the obligations of the service provider to the client. Specifically, an SLA is a legal contract that lays out what the service provider will provide, at what performance level, and steps that will be taken in the event of an outage. This document can be very detailed and include specific performance and availability levels that are expected and the associated penalties for not meeting these performance levels. Additionally, it will spell out the parties responsible and the extent of their responsibilities. In the event of a disaster, the individuals listed on the SLA will take care of the problems related to the disaster.

NOTE

SLAs are legal contracts and as such can have penalties for being broken. An SLA typically has provisions that penalize the service provider in the event that it does not meet its service obligations. Penalties can include financial penalties or even termination of service for repeated or flagrant violation.

Alternate sites are another technique that is used in the event of a system failure or disaster. The idea is to have another location from which to conduct business operations in the event of a disaster. Under ideal conditions, an alternate site is where all operations will be moved if the primary or normal site is no longer in a situation to provide said services.

MODULE 5

There are three types of alternate sites that can be utilized by an organization:

- **Cold site**—This type of site is the most basic type of alternate site and the most inexpensive to maintain. A cold site, by normal definition, does not include backed-up copies of data and configuration data from the primary location. This type of site also does not include any sort of hardware set up and in place. However, a cold site does include basic facilities and power. The cold site is the cheapest option, but it will mean greater outage times as this infrastructure will need to be built and restored prior to going back online.
- **Warm site**—A warm site is the middle-of-the-road option offering a balance between expense and outage time. A warm site typically has some, if not all, necessary hardware in place with other items such as power and Internet connectivity already established, though not to the degree that the primary site has in place. These types of sites also have some backups on hand, though they may be out of date by several days or even weeks.
- **Hot site**—A hot site represents the top of the line here. It means little to no downtime but also the greatest expense. These types of sites typically have a high degree of synchronization with the primary site up to the point of completely duplicating it. This type of setup requires a high degree of complexity in the form of complex network links and other systems and services designed to keep the sites in sync. This level of complexity adds to the expense of the site, but also has the advantage of substantially reduced (or eliminated) downtime.

NOTE

Alternate sites played a huge role for companies that were hit by Hurricane Katrina. Some companies that were hit by Katrina suffered huge losses because they did not have alternate sites as part of their disaster planning. Of course an event like Katrina is rare, but there still exists a potential for such an event; therefore, appropriate steps should be considered and evaluated.

Before an alternate site can work, however, you need to have a backup that must be kept secure because it contains information about your company, clients, and infrastructure. Backups should be stored safely and securely, with copies being kept both onsite and offsite to give optimal protection. Additionally, backups should always be stored on their own media and ideally stored in a locked location offsite. Other safeguards should be taken to protect the backups from environmental concerns such as fire, floods, and earthquakes.

Suitable backup storage locations will depend on the organization's own requirements and other situations. Recent backups can usually be stored onsite, with older archival copies stored someplace offsite. The offsite location is used in the event that the primary site suffers a major event that renders systems and data residing there either unusable or inaccessible.

Recovering Systems

Your BCP and DRP will spell out the process for recovering data, systems, and other sensitive information. Secure recovery requires a number of items to be in place, primary among which is

MODULE 5

the requirement to have an administrator designated to guide the recovery process. As with any backup and recovery process, steps should be taken to review the steps and relevance of the process, and update it where necessary.

Recovering From a Security Incident

When security incidents happen, and they will happen, you have to have a plan to restore business operations as quickly and effectively as possible. This requires that you and your team correctly assess the damage, complete the investigation, and then initiate the recovery process. During the time from the initial security incident onward, the organization presumably has been operating at some reduced capacity and you need to recover the systems and environment as quickly as possible to restore normal business operations. Other key details are the definite need to generate a report on what has happened and the ability to communicate with appropriate team members.

Loss Control and Damage Assessment

Early on, an assessment needs to be performed in order to determine the extent of damages and expected outage or downtime. During this phase, efforts are moving toward damage control.

Some steps you can expect to follow during the damage assessment are:

- The first responder may assess the area of damage to determine the next course of action.
- You should determine the amount of damage to facility, hardware, systems, and networks.
- If your company has suffered virtual—rather than physical—damage, you may need to examine log files, identify which accounts have been compromised, or identify which files have been modified during the attack.
- If your company has suffered physical—and not conceptual—damage, you may need to take a physical inventory to determine which devices have been stolen or damaged, which areas the intruder(s) had access to, and how many devices may have been damaged or stolen.
- One of the most important and overlooked components of damage assessment is to determine whether the attack is over; attempting to react to an attack that is still in progress could do more harm than good.

Inside the organization it is important to determine to whom to report security incidents; this is someone who has accountability and responsibility for safeguarding the organization's assets. These individuals can be different depending on the organization, but each of them will ultimately have accountability for security within the organization. The following is a list of potential reporting points in the organization:

- Chief information security officer (CISO)
- Information security officer (ISO)
- Chief security officer (CSO)
- Chief executive officer (CEO)
- Chief information officer (CIO)

MODULE 5

- Chief operating officer (COO)

NOTE

The ultimate goal of having an individual who is charged with the overall responsibility for security in the organization is to have leadership and legal accountability.

Business Impact Analysis

When working with incident recovery and analysis, an important part of the process is the business impact analysis (BIA). This term covers the process of analyzing existing risk and using various strategies to minimize said risk. The outcome of this process is a BIA report that covers all the potential risks uncovered and their potential impact on the organization. The BIA should go a long way toward illustrating the impact of any loss to the organization in which systems are integrated and rely on each other in increasing amounts.

In the context of the overall disaster recovery and planning, the BIA is used to illustrate the costs of a failure. For example, a BIA will demonstrate costs such as:

- Work backlogs
- Profit/loss
- Overtime
- System repair and replacement
- Legal fees
- Public relations
- Insurance costs

A BIA report emphasizes the importance of each of the various business components and proposes fund allocation strategies to protect them.

Planning for Disaster and Recovery

In order to properly plan for disaster recovery you will need to know where you stand (specifically where the company stands). You need to completely assess the state of preparedness of the organization and then you can understand what to do in order to be properly prepared.

In order to properly plan for disaster recovery, the following guidelines and best practices should be observed:

- Always consider and evaluate the proper redundancy measures for all critical resources. Look for adequate protection for systems such as servers, routers, and other devices in case they are needed for emergency usage.

MODULE 5

- Check with all critical service providers to ensure that adequate protection has been taken to guarantee that the services provided will be available.
- Check for the existence of or the ability to obtain spare hardware wherever necessary. Ensure that the devices not only are appropriate for use but also can be obtained in an emergency.
- Evaluate any existing SLAs that are currently in place so that you know what constitutes acceptable downtime.
- Establish mechanisms for communication that do not require company resources (as they may be unavailable). Such communication channels should also take into account that power may be unavailable.
- Ensure that the organization's designated alternate site can be accessed immediately.
- Identify and document any and all points of failure, as well as any up-to-date redundancy measures that have been put in place to safeguard these points.
- Ensure that the company's redundant storage is secure.

Testing and Evaluation

A plan can be well thought out and account for seemingly everything, but the reality is that unless it is periodically tested and retested, you can never tell just how effective or relevant it may be. Testing is the process through which a plan has its effectiveness measured and evaluated. When a plan is tested, care should be taken to ensure that the processes involved work as designed and intended.

Even if a plan is properly evaluated and tested, it must be reviewed regularly, as times change and the plan must adapt. Some of events that can affect or diminish the overall strength of a plan include:

- Situational and environmental changes that are introduced as an organization evolves to take on new roles and challenges
- Change of equipment due to upgrades and replacements
- Ignorance about or lack of interest in updating the plan
- New personnel who have no interest in or knowledge of the plan

These points plus others necessitate the regular testing and evaluation of a plan in order to prevent its obsolescence. When a plan is tested, special attention should be placed on the plan's strengths and weaknesses, including:

- Is the plan feasible and is it a viable recovery and repair process?
- Are backup facilities adequate for the environment?
- Are adequate human resources allocated to the process, and are these teams properly trained?
- Where are the perceived or real weaknesses in the current process?
- Are teams properly trained to deal with the recovery process?
- Can the process, as designed, carry out the tasks assigned to it?

MODULE 5

Because incident response and the plans that go with it sometimes require special skills, training may be required for all parties and teams involved. The range of special skills is large with extra training required for tasks that involve:

- System recovery and repair
- Fire suppression
- Evacuation of personnel
- Backup procedures
- Power restoration

For the test to verify the effectiveness of a plan, it is necessary to simulate as closely as possible the real conditions under which the plan will operate. In order to do this, consider the following factors:

- The actual size of the installation
- Data processing services and their sensitivity to failure
- Service level expected by users and the organization
- Acceptable downtime and recovery
- Type and number of locations involved
- Cost of and budget for performing the test

Preparation and Staging of Testing Procedures

Performing the right test on your plan will ensure accurate and appropriate results that are the most useful to you. Testing suites that can be performed on a plan include:

- Walkthrough
- Checklist
- Simulation
- Parallel
- Full interruption

Each test offers unique benefits that give it the ability to reveal different and sometimes more accurate results.

Structured Walkthrough

In this type of test, members of the disaster recovery team get together around a table and read through the plan together. The goal is to read through the steps and note how each department gets responsibilities handed off to it and how it interacts. This type of test will uncover potential gaps and bottlenecks in the response.

Checklist

MODULE 5

This type of test will assist in verifying that sufficient supplies are stored and available at the backup site, contact information is current, and the recovery plan is accessible and available to all who need it in an emergency. The recovery team should review and identify weak areas but also resources that are available.

Simulations

In this type of test, a disaster is simulated in such a way that normal business operations are not adversely affected. The test will seek to simulate a disaster as accurately as practical given the budget and situation. Features of this test include practicing backup and restore operations, incident response, communication and coordination of efforts, alternative site usage, and other similar details. Tasks or processes that cannot be economically or practically completed should be omitted where necessary, including travel requirements, taking down key systems, and involvement of certain teams.

Full Interruption

In this type of test, the complete disaster recovery plan is enacted under simulated conditions. This test will very closely simulate the event of a disaster, including the simulation of damage to systems such as communications and other services.

Due to the fact that this type of test interrupts services and the organization itself, extreme caution should be exercised to avoid a major impact on the organization. Ideally this type of test should be scheduled during slow periods, at the end of the month, after business hours, or at any point where critical business operations are such that they will not be affected.

Frequency of Tests

Testing must be run in order to ensure that the plan is still effective, but this testing is not a one-time thing and should be run on a regular basis to ensure that the plan remains effective. Tests should be considered and run as often as is practical—for example, quarterly, semiannually, or annually.

Analysis of Test Results

The purpose of all this testing is to provide data on how well a plan is working. Personnel should log events during the test that will help evaluate the results. The testing process should provide feedback to the disaster recovery team to ensure that the plan is adequate.

The recovery team, which normally consists of key management personnel, should assess test results and analyze recommendations from various team leaders regarding improvements or modifications for the plan. It is essential to quantitatively measure the test results, including:

- Elapsed time to perform various activities

MODULE 5

- Accuracy of each activity
- Amount of work completed

The results of the tests will most likely lead to changes in the plan. These changes should enhance the plan and provide a more workable recovery process. Testing the disaster recovery plan should be efficient and cost effective. It provides a means of continually increasing the level of performance and quality of the plan and the people who execute it. A carefully tested plan provides the organization with the confidence and experience necessary to respond to a real emergency. Disaster recovery plan testing should consider scheduled and unscheduled tests for both partial and total disasters.

Evidence Handling and Administration

Once the incident response process has been defined at a high level, it is time to turn your attention toward the collection of evidence from a crime scene. Although you may be involved in this process, it is possible that you will also involve special teams or external consultants.

NOTE

Involvement of those not trained to handle evidence properly can result in evidence that is not adequate to prosecute a crime or is indefensible in court. Typically those who collect evidence from crime scenes are specially trained to do so and have the required experience to do so to ensure that evidence is true and correct and is collected in a way that can be used in court.

Evidence Collection Techniques

Proper collection of evidence is essential and is something that is best left to professionals whenever the need arises. When a crime has been suspected, it may become necessary to expand the incident response to include trained professionals in the process. The process here is really one of **forensics**, or the methodical and defensible process of collecting information from a crime scene. This is a process best left to those professionals trained to do it because novices can inadvertently damage evidence in such a way that makes the investigation impossible or indefensible in court. Trained personnel will know how to avoid these blunders and properly collect everything relevant.

Evidence Types

Not all evidence is created equal and should not be treated as such because evidence is what ultimately proves your case. Collecting the wrong evidence or treating evidence incorrectly can have an untold impact on your case, which should not be underestimated.

[Table 14-2](#) lists some of the different types of evidence that can be collected and what makes each unique.

MODULE 5

Table 14-2. Types of evidence.

EVIDENCE	DESCRIPTION
Best	Best evidence is a category of evidence that is admissible by requirement in any court of law. In the case of documents, best evidence is the original document. The existence of best evidence eliminates your ability to use any copies of the same evidence in court.
Secondary	Evidence that fits the definition of secondary evidence is any evidence that is a copy of the original evidence. This could be items such as backups and drive images. This type of evidence may not always be admissible in a court of law and is not admissible if best evidence of the item exists.
Direct	Direct evidence is evidence that is received as the result of testimony or interview of an individual regarding something he or she directly experienced. This individual could have obtained the evidence as a result of observation. Evidence in this category can prove a case.
Conclusive	Evidence that fits within the category of conclusive evidence is evidence that is above dispute. Conclusive evidence is considered so strong that it directly overrides all other evidence types by its existence.
Opinion	Evidence that of this type is derived from an individual's background and experience. Opinion evidence is divided into the following types: • Expert—Any evidence that is based upon known facts, experience, and an expert's own knowledge • Non-expert—The opinion evidence of non-experts is limited to that based upon the witness's perception of a series of events where that perception is relevant to the case.
Corroborative	Evidence in this category is evidence that is obtained from multiple sources and is supportive in nature. This type of evidence cannot stand on its own and is used to bolster the strength of other evidence.

MODULE 5

EVIDENCE	DESCRIPTION
Circumstantial	Circumstantial evidence is any evidence that indirectly proves a fact through the use of deduction.

Chain of Custody

When collecting evidence for use in court, the **chain of custody** must be maintained at all times. The chain of custody is simple in theory as it documents the whereabouts of the evidence from the point of collection to the time it is presented in court and after, when it is returned to its owner or destroyed. The chain is essential as any breaks or question about the status of evidence at any point can result in a case being thrown out. A chain of custody will need to include every detail about the evidence such as how it was collected up to how it was processed.

A chain of custody can be thought of as enforcing or maintaining six key points at any point. These points will ensure that you focus on how information is handled at every step.

Chain of custody should always maintain these six points by asking the following questions:

- What evidence has been collected?
- How was the evidence obtained?
- When was the evidence collected?
- Who are the individuals who handled the evidence?
- What reason did each person have for handling the evidence?
- Where has the evidence traveled and where was this evidence ultimately stored?

Also remember to keep the chain of custody information up to date at all times. Every time any evidence is handled by an investigator, a record must be kept and updated to reflect this. This information should explain every detail such as what the evidence actually consists of, where it originated, and where it was delivered. It is important that no gaps exist at any point.

Additionally, for added legal protection, evidence can be validated through the use of hashing to prove that it has not been altered. Ideally the evidence you collected at the crime scene is the same evidence you present in court.

Remember, lack of a verifiable chain of custody is enough to lose a case.

Computer Removal

When any sort of computer crime is logged and reported it becomes necessary to examine the system and in some cases remove the computer from the crime scene. Of course, such a seizure of a computer means that the chain-of-custody requirements come into play and the system must be tagged and tracked up until it is presented in court.

MODULE 5

Also do not forget that computer evidence, like many different types of evidence, may require specific legal authorization to be taken. Requirements will vary depending on the company and situation in question, but it is another item to consider.

CHAIN OF CUSTODY KEY IN BONDS CASE

While not related to computer crime, this article demonstrates the concept of chain of custody and how it can call a case into question.

"Before the federal government attempts to convince a jury that Barry Bonds lied under oath when he denied he knowingly used steroids, prosecutors face another challenge: proving the drug tests which were positive for steroids belong to baseball's home run king and that the test results are reliable and relevant to the perjury trial set to begin March 2.

Bonds' defense team is expected to press the issue and ask Judge Susan Illston to throw out the evidence in pretrial motions due Thursday. Illston will have to weigh evidence the government seized in its 2003 raid of BALCO against the following facts:

- *No one saw Bonds urinate into a container when he provided samples that allegedly tested positive for steroids.*
- *Bonds never signed anything that authenticated the urine samples that tested positive for steroids were his."*

In this case, not having definite proof of where the evidence came from or a way to authenticate the evidence could have an impact on the case as the chain of custody is broken.

Source: Yahoo Sports

Rules of Evidence

No evidence, no matter the type, is necessarily admissible in court. Evidence cannot be presented in court unless certain rules are followed. These rules should be reviewed ahead of time. The rules of evidence presented here are general guidelines and are not consistent across jurisdictions.

The following list includes the five commonly accepted rules of evidence:

- **Reliable**—When presented is consistent and leads to a common conclusion
- **Preserved**—Chain of custody comes into play, and the records help identify and prove the preservation of the evidence in question.
- **Relevant**—Evidence that directly relates to the case being tried
- **Properly identified**—Evidence in which records can provide proper preservation and identification proof
- **Legally permissible**—Evidence that is deemed by the judge to fit the rules of evidence for the court and case at hand

MODULE 5

NOTE

Evidence laws and types will vary based on the jurisdiction and case involved. The rules presented here are appropriate for the United States, but you can expect variations of the rules when involving other countries in investigating and prosecuting potential computer crimes.

FYI

When generating a report, avoid the temptation to use flowery or overly technical language because the individuals who will eventually read the report may not be technically savvy. While technical information and jargon are helpful to some, you won't always know what the skill and knowledge level of the audience will be. Any language that is overly technical or filled with jargon can be included, but relegated to an appendix in the report.

Security Reporting Options and Guidelines

When considering the reporting of a security incident it is important to be aware of the structure and hierarchy of a company. The overall structure of reporting can have a huge impact on how things operate in the event of a security incident. Additionally, making individuals aware of this structure ahead of time is of the utmost importance so there is no confusion when the time comes to report an incident.

Reporting a Security Incident

Once an incident has been responded to, and a team has gotten involved to assess the damage and start the cleanup, the required parties will need to be informed. These parties will be responsible for getting the ball rolling whether it is legal action, investigative processes, or other requirements as necessary.

When considering how to report a security incident, the following guidelines are worth keeping in mind and can prove helpful at the time of crisis:

- Wherever feasible, refer to previously established guidelines as documented and described in the company IRP. The IRP should include guidelines on how to create a report and whom to report to. Furthermore, the IRP should define the formats and guidelines on how to put the report together in order to ensure that the information is actually usable by its intended audience.
- Consider the situations where it is necessary to report the incident to local law enforcement in addition to the company officials.
- Consider the situations and conditions about when and if the security incident must be reported to regulatory bodies as required by law.
- Security incidents reported outside the organization can and should be noted in the company incident report.

MODULE 5

During the preparation of a security incident report, include all the relevant information to detail and describe the incident. At a minimum, the following items should be included:

- Timeline of the events of the security incident that includes any and all actions taken during the process
- Risk assessment that includes extensive details of the state of the system before and after the security incident occurred
- Detailed list of any and all participants who took part in the discovery, assessment, and final resolution (if this has occurred) of the security incident. It is important to include all those who took part in this process regardless of how important or unimportant their roles may be perceived to be.
- Detailed listing of the motivations of the decisions that were made during the process. Document these actions in a format that states what each action was and what factors led to the decision to take the designated action.
- Recommendation as to what could be done to prevent a repeat of the incident and what could be done to reduce any damage that may result
- Two sections to ensure that it is usable by all parties. First, a long format report should be prepared that includes specific details and actions that occurred during the security incident. Second, the report should include an executive summary that provides a high-level, short-format description of what occurred.

Affected Party Legal Considerations

One of the biggest concerns you will have to face is inappropriate use of resources such as e-mail and Internet access. Employees have been known to use company resources for all sorts of activities, both work related and otherwise, some of which can result in problems for someone; the question is who. When an individual uses company resources for inappropriate reasons, the question becomes who is held liable: the company or the employee or both. It also brings up the question of what each party's rights are.

Protecting information is also important when considering the individuals involved. Not every issue will be one of employee versus company; other variations exist and their requirements will vary.

FYI

The scenario of liability has been played out numerous times in companies over the years, with organizations becoming the victim of legal actions because of the actions of an employee. For example, some companies have been the subject of legal action due to an employee using a company account to post hate speech or other comments. Other examples have seen companies become the subject of legal action due to an individual browsing pornographic content at work and offending a coworker who promptly files a harassment lawsuit.

Stating what is and is not appropriate use of resources can provide the company some measure of protection against these scenarios.

MODULE 5

Customers

- What data is considered private, what is considered public, and how does each need to be protected?
- What does a company need to do to protect customer information both professionally and legally?

Business Partners

- Who is responsible for the liability of data that is stored in one location and processed in another?
- Who is responsible for the necessary security and privacy of data transmitted to and from an organization and a business partner?

Requirements of Regulated Industries

Depending on the industry or business an organization works in, additional legal requirements may need to be considered when protecting information. A business that is part of the utility, financial, or health care industry should expect regulations to come into play that dictate data protection needs and other requirements. The security professional should exercise appropriate care when deploying a security solution in a regulated industry and, if necessary, seek legal support to ensure the proper regulations are being followed.

NOTE

You will need to become familiar with regulations such as the Healthcare Information Portability and Accounting Act (HIPAA) and Sarbanes-Oxley to make sure that you are meeting legal obligations. For example, HIPAA is a set of guidelines that will directly affect you if your company is in the health care industry.

Payment Card Industry Data Security Standard (PCI DSS)

For the payment card industry, a set of rules exists for incident response. Its Data Security Standard has certain specific requirements for its organizations' incident response plans.

Organizations must verify that their IRP describes the following:

- Roles, responsibilities, and communication strategies in the event of a compromise
- Coverage and responses capabilities for critical systems and their components
- Notification requirements for credit card associations and acquirers
- Business continuity planning
- Reference or inclusion of incident response procedures from card associations

MODULE 5

- Analysis of legal requirements for reporting compromises (for example, California Bill 1386)

There are several terms you should remember that will ensure that you are doing what is necessary to protect yourself. "Due care" is a policy that describes and dictates how assets need to be maintained and used during company operations. Under the banner of due care are guidelines on how to safely use equipment in line with approved company guidelines.

Next is the concept of due diligence, which is the process of investigating any and all security incidents and related issues pertaining to a particular situation. An organization needs to ensure that it is always exercising due diligence to make sure its policies are effective and stay effective. An organization also needs to exercise due diligence to make sure that no violations of laws or regulations are occurring.

Finally, due process references a key idea that when a policy or rule is broken, disciplinary measures are followed uniformly and employees are not considered guilty until they have been given proper process. Due process ensures that policies are applied uniformly to all employees regardless of who they are or other factors so as to respect their civil rights and to protect the company from potential lawsuits later.

CHAPTER SUMMARY

As a security professional you are expected to be versed in a variety of different technologies and techniques, each designed to prevent an attack and secure the organization. Each of the techniques you have learned is intended to prevent or limit the scope of an attack; however, you must accept the fact that attacks are going to happen, and some may be successful despite your best efforts. As a security professional, breaches of your security perimeter and defenses are a reality that you will have to accept.

After you have accepted that an attack will penetrate your defenses at some point, your job now becomes one of how to respond to these situations. Incident response is the process of how a security breach will be responded to. Even though security incidents are going to happen, it does not mean that you are powerless—you just have to know how you will respond and the details of that response.

Incident response is not only the act of how you respond to a security incident, but also the details involved in that response. How you respond to an incident is an important detail to have in mind because responding incorrectly to an incident could result in making a bad situation worse (for example, not knowing what to do, whom to call, or what the chain of command is in these situations).

Finally, something that will have substantial impact on incident response is the potential legal aspect. Exercising the concepts of due care, due diligence, and due process is absolutely essential. When a security incident happens, it typically falls under the banner of computer crimes and as

MODULE 5

such will require additional care to be taken when responding. The deployment of special teams trained in techniques such as forensics will be absolutely essential to get right. When you respond to a security incident that has gone to this level, you are now moving from the realm of just responding to performing a formal investigation. The formal investigation will include special techniques for gathering and processing evidence for the purpose of potentially prosecuting the crime later.

KEY CONCEPTS AND TERMS

- **Chain of custody**
- **Computer crime**
- **Evidence**
- **Forensics**
- **Incident**
- **Incident response plan (IRP)**

CHAPTER 14 ASSESSMENT

1. _____ used to define mechanisms to keep the business running consistently.
2. List at least three potential reporting points in an organization. These are people to whom a security incident should be reported.
3. _____ is a plan that defines the procedures for responding to a security incident.
 1. IRP
 2. DCP
 3. DRP
 4. None of the above
4. BCP is used to define the process and procedures used to clean up a disaster.
 1. True
 2. False
5. _____ must be gathered by trained professionals.
6. What type of evidence gives the most solid proof of a crime?
 1. Corroborative
 2. Circumstantial
 3. Best
 4. Opinion
7. _____ is used when best evidence cannot be acquired.
8. Another location from which to conduct business in the event of a disaster is called a(n) _____.

MODULE 5

Chapter 2. Defensive Technologies

ONE OF THE BIGGEST CHALLENGES you will have to face as a security professional is keeping the network you are responsible for secure. On the surface this may not sound like a big challenge, but consider the fact that more threats are emerging every day and are emerging at an increasingly rapid rate. More people will be interacting with and using your networks and accessing the resources found there. Also, your network and the infrastructure that it comprises have become more complex with increasing numbers of employees going mobile and using advanced connection techniques such as virtual private networks (VPNs).

All this complexity makes the usability and capability of the network much greater than it would be otherwise, but it also means that your job of securing and managing the network is a much more difficult task. Another point to consider is the fact that for all these systems to work together effectively, a certain level of trust must be built into the system, meaning that one system gives a certain level of credibility to another system. These points are things that you must consider in order to properly protect your network.

Securing your network and infrastructure requires a mix of capabilities and techniques, some of which have been introduced in this course. Let's take all the techniques, technologies, and strategies discussed during this course and break them into two categories: prevention and detection. In the past, quite a bit of effort was focused on the prevention of an attack, but what about those times when a new or unanticipated attack gets through your defenses? Sure, you can prevent an attack by using firewalls, policies, and other means, but there are other things that can help, too. That's where detection comes into play and where devices and technologies such as intrusion detection systems and honeypots can assist you.

Chapter 15 Topics

This chapter covers the following topics and concepts:

- What intrusion detection systems (IDS) are
- What the purpose of firewalls is
- What honeypots and honeynets are
- What the role of controls is

Chapter 15 Goals

When you complete this chapter, you will be able to:

- List the two forms of IDS
- Describe the goals of IDS
- List the detective methods of IDS
- List the types of firewalls
- Describe the purpose of firewalls
- Describe the purpose of honeypots

MODULE 5

- Describe the purpose of honeynets
- Describe the purpose of administrative controls

Intrusion Detection Systems (IDSs)

One of the tools that enables you to detect an attack is the intrusion detection system (IDS). These devices provide the ability to monitor a network, host, or application, and report back when suspicious activity is detected. The essence of intrusion detection is the process of detecting potential **misuse** or attacks and the ability to respond based on the alert that is provided. You can do a lot to secure your systems, but how do you know they are secure? The IDS provides the ability to monitor the systems under your care.

NOTE

Former President Ronald Reagan once made a comment about the former Soviet Union: "Trust, but verify." This is where the intrusion detection system comes into play. Your defenses should be working as designed to secure your network, but you should verify that they actually are doing so. Misplaced trust can be your worst enemy, and the IDS will serve as a way to prevent this.

An IDS is a hardware appliance or software-based device that gathers and analyzes information generated by a computer or network. This information is analyzed with the goal of detecting any activity that is unauthorized and suspicious, or looks for signs of privileges or access that are being misused. An IDS is essentially a packet sniffer on steroids. A packet sniffer by itself captures traffic, and it is up to you to analyze it and look for signs of problems, but in the case of an IDS, this capability is extended through the use of rules that allow the IDS to compare the intercepted traffic to known good or bad behavior.

Once an IDS determines that a suspected **intrusion** has taken place, it then issues an alarm in the form of an e-mail, page, message, or log file entry that the network administrator will evaluate. Remember that an IDS detects an attack. What it does not do is prevent an attack—if an IDS has detected an attack, it is already occurring.

Before going too far into the topic of IDS, it is necessary to define a few key terms. Each of the following is used to describe the environments and situations that an IDS is expected to operate in and what it is expected to detect:

- **Intrusion**—An unauthorized use or access of a system by an individual, party, or service. Simply put, this is any activity that should not be but is occurring on an information system.
- **Misuse**—The improper use of privileges or resources within an organization; not necessarily malicious in nature, but misuse all the same
- **Intrusion detection**—**Intrusion detection** is the technique of uncovering successful or attempted unauthorized access to an information system
- **Misuse detection**—**Misuse detection** is the ability to detect misuse of resources or privileges

MODULE 5

When an IDS is in operation, it has three mechanisms it can use to detect an intrusion, with each one offering a distinct advantage and disadvantage compared with the others:

- **Signature recognition**—Commonly known as misuse detection, it attempts to detect activities that may be indicative of misuse or intrusions.
 - **Signature analysis** refers to an IDS that is programmed to identify known attacks occurring in an information system or network.
 - For example, an IDS that watches Web servers might be programmed to look for the string "phf" as an indicator of a Common Gateway Interface (CGI) program attack. Looking for this particular string would allow the IDS to tip off the system owner that an attacker may be trying to pass illegal commands to the server in an attempt to gain information.
 - Most IDSs are based on signature analysis.
- **Anomaly detection**—**Anomaly detection** is a type of detection that uses a known model of activity in an environment and reports deviations from this model as potential intrusions. The model is generated by the system owner based on knowledge of what is acceptable and known behavior on the network. In modern systems, the IDS will be configured to observe traffic in a training mode in which it observes and learns what is normal and what is not on a given network.

Table 15-1. IDS response matrix.

	TRUE	FALSE
POSITIVE	An alert was generated in response to an actual intrusion attempt.	An alert was generated in response to a perceived but nonthreatening event.
NEGATIVE	An alert was not generated as no suspicious activity was detected nor did it occur.	An alert was not generated as no suspicious activity was detected, but such activity did occur.

When an IDS is configured to use one of these methods, it can respond with an alert using one of several criteria. When the IDS responds it can be in the positive or negative fashion, but it is not that simple because either response can be true or false. In [Table 15-1](#) the responses are provided and their respective characteristics generated.

It is important to get an understanding of the different types of IDS available. It is necessary for you as a security professional to know what an IDS can detect and where it may be useful as well as understanding where it is not. Make sure that you understand what activities each is sensitive to as this will determine the proper deployment for each and where you will get the best results:

MODULE 5

- **Network-based intrusion detection system (NIDS)**—An IDS that fits into this category is one that can detect suspicious activity on a network such as misuse or other activities such as SYN floods, MAC floods, or other similar types of behavior. **Network-based intrusion detection system (NIDS)** devices monitor the network through the use of a network card that is switched into promiscuous mode and connected to a spanning port on a switch so that all traffic passing through the switch is visible.

Indications of network intrusion:

- Repeated probes of the available services on your machines
- Connections from unusual locations
- Repeated logon attempts from remote hosts
- Arbitrary data in log files, indicating an attempt at creating either a denial of service (DoS) or a crashed service
- **Host-based intrusion detection system (HIDS)**—An IDS that fits into this category is one that can monitor activity on a specific host or computer. The ability of **host-based intrusion detection systems (HIDS)** extends to what is only on the specific host, not on the network. Included in the functionality of these types of IDS is the ability to monitor access, event logs, system usages, and file modifications.

These types of IDS can detect:

- Modifications to system software and configuration files
- Gaps in the system accounting, which indicate that no activity has occurred for a long period of time
- Unusually slow system performance
- System crashes or reboots
- Short or incomplete logs
- Logs containing strange timestamps
- Logs with incorrect permissions or ownership
- Missing logs
- Abnormal system performance
- Unfamiliar processes
- Unusual graphic displays or text messages
- **Log file monitoring**—Software in this category is specifically designed to analyze log files and look for specific events or activities. Software of this type can look for anything in log files from improper file access to failed logon attempts.

Log file activity that can be detected can include:

- Failed or successful logons
- File access
- Permission changes
- Privilege use
- System setting changes
- Account creation

MODULE 5

- **File integrity checking**—Software in this category represents one of the oldest and simplest types of IDS. Software in this category looks for changes in files that may indicate an attack or unauthorized behavior. These devices look for modifications in files using techniques such as hashing to uncover changes. One of the oldest IDS systems around, Tripwire, started by using this sort of technique.

Indications of file system intrusion:

- The presence of unfamiliar new files or programs
- Changes in file permissions
- Unexplained changes in file size
- Rogue files on the system that do not correspond to your master list of signed files
- Unfamiliar filenames in directories
- Missing files

The two main types of IDS discussed here are the HIDS and NIDS because they are the two most commonly encountered in the wild. [Table 15-2](#) compares the two to help you understand how they stack up against one another.

FYI

A system can be compromised by an attacker in a number of ways, including altering key files and/ or placing a rootkit. Once this process has been carried out, it can be very difficult to trust a system because you won't know what has been altered. However, it is possible to use file integrity checking to detect differences in files. File integrity checking can hash key files on a system and store the hashes for later comparison. On a regular basis, these hashes will be rechecked against the files. If they match, every file should be original; if the hashes are different, then a change has occurred. When these changes are detected, the system owner is notified and will take the appropriate action.

Table 15-2. NIDS and HIDS features.

FEATURE	NIDS	HIDS
Best suited for	Large environments where critical assets on the network need extra observation	Environments where critical system-level assets need monitoring
Management concerns	Not an issue in large environments; may incur too much overhead in smaller environments	Requires specific adjustments and considerations on a system level

MODULE 5

FEATURE	NIDS	HIDS
Advantage	Ideal for monitoring sensitive network segments	Ideal for monitoring specific systems

IDS Components

An IDS is not one thing—it is a collection of items that come together to make the overall solution. The IDS is formed by a series of components that make an effective solution designed to monitor the network or system for a range of intrusions. If you zoom out a bit, you can see that an IDS is not even centered or resident on a single system; it is distributed across a group of systems, each playing a vital role in monitoring the network.

In the solution that forms an IDS, there are a number of components, each with its own responsibilities. These components are responsible for monitoring for intrusion, but also are capable of performing other functions, such as the following:

- Pattern recognition and pattern matching to known attacks
- Analysis of traffic for abnormal communication
- Integrity checking of files
- Tracking of user and system activity
- Traffic monitoring
- Traffic analysis
- Event log monitoring and analysis

When you move from vendor to vendor, the features that are part of the IDS will vary in scope, capability, and implementation. Some IDSs offer only a subset of the features mentioned here, and others offer substantially more. All IDSs do tend to have the same components no matter which vendor is manufacturing the device.

NOTE

The command console can be as simple as opening a Web interface in a Web browser or as complex as a piece of software on the client. In some cases, the client is a custom-built system configured just for the purpose of monitoring and configuring the system. The capabilities of this console will vary dramatically depending on the vendor and the features present on the IDS.

Components of NIDS

The most visible component of an IDS is the command console, which represents the component where the system administrator manages and monitors the system. This is where the administrator carries out the day-to-day tasks of monitoring, tuning, and configuring the system in order to

MODULE 5

maintain optimal performance. The command console may be accessed from anywhere or have its access restricted to a specific system for security purposes.

Working in concert with and monitored by the command console is the network sensor. The network sensor is a discrete software application that runs on a designated device or system as needed. This sensor is essentially the same as a sniffer in that it runs in conjunction with a network card in promiscuous mode. The sensor has the ability to monitor traffic on a specific segment of the network due to the same restrictions that are placed on sniffers. This is why placement of a network sensor is so important: Placement of a sensor on the incorrect network segment could result in a critical segment not being monitored. [Figure 15-1](#) illustrates the components of a NIDS.

Another mechanism that works with an IDS is a hardware-based device known as a network tap. This device resides on the network and appears physically very similar to a hub or switch, but as part of an IDS it can be of value. A network tap has certain characteristics that make it unique; for example, it has no Internet Protocol (IP) address, it sniffs traffic, and it can be used by an IDS to collect traffic that is used to generate alerts. The main benefit of placing a network tap on the network in conjunction with an IDS such as a NIDS is that it will enhance the security and detection capabilities of the system.

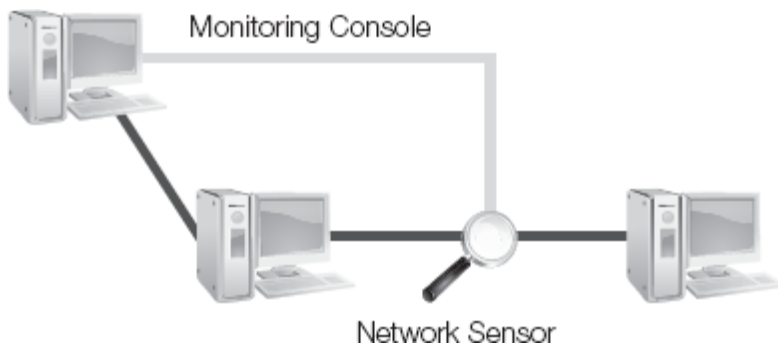


Figure 15-1. Components of a NIDS.

FYI

When networks had more hubs as part of their setup, placement of the sensor was less of an issue because traffic could be more easily observed anywhere on the network. With networks using more switches and other connectivity devices designed to manipulate and control collision domains, traffic takes much more consideration and planning to sniff. You can use switches that have an expansion port to mirror traffic to an additional port and monitor traffic on another collision domain.

An effective and robust alert generation and notification system is required to let the network owner know what is occurring when an attack happens. Alert notification and generation will occur when an event or some activity happens that needs the attention of the security or network administrator. The alerts that are generated can be delivered to the system owner using popup alerts, audio alerts, pagers, text messages and e-mail.

MODULE 5

How does an IDS function? The intrusion detection process is a combination of information gathered from several processes. The process is designed to respond to packets sniffed and analyzed. In this example, the information is sniffed from an Ethernet network with a system running the sensor operating in promiscuous mode, sniffing and analyzing packets off of a local segment.

NOTE

Alerts can be sent in any way that is appropriate and most likely to get the attention they deserve. When an alert comes in, a network administrator should review the message and the nature of the information and then take the appropriate response. Some modern IDS include all the methods of notification here as well as the ability to send text messages to specific personnel.

In the following steps, an IDS using a signature-based detection method is used to detect an intrusion and alert the system owner:

- A host creates a network packet.
 - At this point nothing is known other than the packet exists and was sent from a host in the network.
- The sensor sniffs the packet off the network segment.
 - This sensor is placed so it can read the packet.
- The IDS and the sensor match the packet with known signatures of misuse.
 - When a match is detected, an alert is generated and is sent to the command console.
- The command console receives and displays the alert, which notifies the security administrator or system owner of the intrusion.
- The system owner responds based on the information the IDS provides.
- The alert is logged for future analysis and reference.
 - This information can be logged in a local database or in a central location shared by several systems.

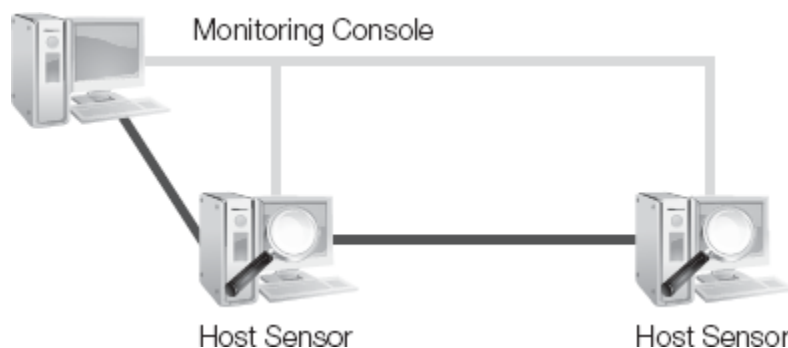


Figure 15-2. Components of a HIDS.

Components of HIDS

MODULE 5

A HIDS is designed to monitor the activity on a specific system. Many vendors offer this type of IDS so the features vary wildly, but the basic components are the same.

The first component of a HIDS is the command console, which acts much like its counterpart on the NIDS. This piece of software is the component that the network administrator will spend the most time with. Here the administrator will configure, monitor, and manage the system as needs change.

The second component in the HIDS is the monitoring agent software. This agent is responsible for monitoring the activities on a system. The agent will be deployed to the target system and monitor activities such as permission usage, changes to system settings, file modifications, and other suspicious activity on the system. [Figure 15-2](#) illustrates the components of a HIDS.

Setting Goals

When setting up an IDS, it is necessary to define the goals of the system prior to deploying it into production. As with any technology of this level of complexity, some planning is required to make things work properly and effectively. The first step in ensuring that an IDS is working as it should is to set goals. Two goals that are common are response capability and accountability.

When an IDS recognizes a threat or other suspicious activity it must respond in some fashion. The IDS receives the data, analyzes it, and then compares it to known rules or behaviors and when a match is found some response must occur. The question you must answer is what this action will be; in this case, an alert.

Responses can include any number of potential actions, depending on what your goal may happen to be. Some common responses include sending an alert to the administrator as a text message or e-mail, but this is not the only option. Additionally the IDS will log the event by placing an entry in a log file for later review and retrieval. In most cases, an organization would choose to place information in a log or event log because it provides additional benefits for the business—including the ability to analyze data historically and plan for expenditures. However, logs are not used only for planning budgets. They are also very useful in determining the effectiveness of security measures. Remember that an IDS detects attacks or suspicious activity after it has already occurred. If it has occurred, it means it has gotten around or passed through security measures unimpeded, in which case you need to know why and how it happened.

Accountability

Having the proper response in place is an important detail to address, and without a response plan in place the system loses its effectiveness. But this is not the only required element because you must establish accountability, too. As part of network security policy, you must define a process in which the source and cause of an attack are identified and investigated. This process is necessary due to the potential need to pursue legal action, not to mention the need for finding out the source and cause of the attack in order to adjust your defenses to prevent the problem from happening again.

MODULE 5

Limitations of an IDS

While an IDS is capable of performing a number of tasks in the realm of monitoring and alerting system administrators to what is happening on their network, it does have its limitations. You should always be aware of the strengths and weaknesses of the technologies you are working with, and IDSs are no exception. Knowing these limitations will also make sure that you use the technology correctly and it is addressing the issues it was designed to address.

It Is Not the Only Problem Solver

No matter what you are told by the vendor of a particular IDS, it is not a silver bullet that can solve all your problems. An IDS can only supplement existing security technologies; it cannot bring nirvana to the security of your network. You should expect an IDS to provide the necessary element of verification of how well your network security counter-measures are doing their respective jobs.

You should never expect an IDS to be able to detect and notify you about every event on your network that is suspicious; in fact, it will detect and report only what you tell it to. Also consider the fact that an IDS is programmed to detect specific types of attacks, and because attacks evolve rapidly, an IDS will not detect unfamiliar new attacks; it is not programmed or designed to do so. Remember, an IDS is a tool that is designed to assist you and is not a substitute for good security skills or due diligence. For example, as a system owner and security professional, you must regularly update the signature database of any IDS under your control that uses this mechanism. Another example is to understand your network and update your model or baseline on what is normal behavior and what is not, as this will change over time.

FYI

Try to focus on the type of IDS you are attempting to deploy and the features it offers you. Deploying an IDS in an environment or setting in which it is not designed to be deployed can be catastrophic. In a best-case scenario, you will get warnings about attacks that are bogus or irrelevant; in the worst case, you will not get any warning whatsoever. Take time to understand the features and capabilities you are being offered by a technology as well as the attacks and activities you are looking to monitor. An IDS is not a solution unto itself and will work in concert with other technologies and techniques.

Failed Hardware

If the hardware that is supporting the IDS fails and it has the sensor or the command console on it, your IDS may become ineffective or worthless. In fact, if a system that has a network sensor located on it fails, there is no way to gather the information to be analyzed. Also, an IDS cannot inform you of or prevent a hardware failure, so if this event occurs, you will be out of luck. Any serious failure in hardware, network communications, or other areas can wreak havoc with your monitoring capabilities. Planning ahead and implementing mechanisms such as redundant hardware and links is a way to overcome this limitation to prevent the IDS from going offline.

MODULE 5

Investigation of an Event

An IDS provides a way of detecting an attack, but not dealing with it. That is the responsibility of something known as an IPS, which will be discussed later. An IDS is extremely limited as to the actions it can take when an attack or some sort of activity occurs. An IDS observes, compares, and detects the intrusion and will report it; it then becomes your responsibility to follow up. All the system can do is warn you if something isn't right; it can't give you the reasons why.

As a security professional, you will have to make it a point to review the IDS logs for suspicious behavior and take the necessary action. You are responsible for the follow-up and action.

Analysis of Information Collected

Information from an IDS can be quite extensive and can be generated quite rapidly, and this data requires careful analysis in order to ensure that every potentially harmful activity is caught. You will have the task of developing and implementing a plan to analyze the sea of data that will be generated and ensuring that any questionable activity is caught.

Intrusion Prevention Systems (IPSs)

The next step beyond an IDS is an IPS. An IPS is a device that is used to protect systems from attack by using different methods of access control. This system is an IDS with additional abilities that make it possible to protect the network.

The devices that were originally developed as a way to extend the capabilities were already present in an IDS. When you look at IDS in all its forms you see that it is a passive monitoring device that offers limited response capabilities. An IPS provides the ability to analyze content, application access, and other details to make determinations on access. For example, an IPS can provide additional information that would yield insight into activities on overly active hosts, bad logon activities, access of inappropriate content, and many other network and application layer functions.

Responses that an IPS can use in response to an attack include:

- Regulating and stopping suspicious traffic
- Blocking access to systems
- Locking out misused user accounts

IPSs come in different forms, each offering a unique set of abilities:

- **Host-based**—IPSs in this category are those that are installed on a specific system or host and monitor the activities that occur there.
- **Network**—IPSs that fit into this category are designed to monitor the network and prevent intrusions on a specific host when activity is detected. In practice, these types of IPS are hardware appliances that are purposely built to carry out their function.

The Purpose of Firewalls

A challenge that you must address to protect your network and the assets therein to the highest possible degree is access control. The technologies and techniques in this area have varied and evolved dramatically over the years to include devices such as the IDS, authentication, and firewalls. Firewalls have undergone the greatest evolution, moving from a simple packet filtering device up to a device that can perform advanced analysis of traffic. Firewalls have become an increasingly important component of network security and as such you must have a firm command of the technology.

Firewalls separate networks and organizations into different zones of trust. If one network segment has a higher level of trust than another, a firewall can be placed between them as the demarcation point between these two areas. Such would be the case when separating the Internet from the internal network or two network segments inside an organization.

The firewall is located on the perimeter or boundary between the internal network and the outside world. The firewall forms a logical and physical barrier between the organization's network and everything outside. From this advantageous and important position, the firewall is able to deny or grant access based on a number of rules that are configured on the device. These rules dictate the types of traffic which are allowed to pass and the types which are not.

A firewall can also provide the ability to segment a network internally or within the organization itself. An organization may choose to control the flow of traffic between different parts of the organization for security reasons. For example, an organization may use a firewall to prevent the access to or viewing of resources and other assets on a particular network segment, such as those situations where financial, research, or company confidential information needs to be controlled.

An organization may choose to deploy a firewall in any situation where the flow of traffic needs to be controlled between areas. If there is a clear point where trust changes from higher to lower, or vice versa, a firewall may be employed.

In the early days of firewalls, the process of denying and granting access was very simple, but so were the threats (relative to today at least). Nowadays firewalls have had to evolve to deal with ever-increasing complexities that have appeared in growing numbers such as SYN floods, DoS attacks, and other behaviors. With the rapid increase and creativity of attacks, the firewalls of the past have had to evolve in order to properly counter the problems of today.

How Firewalls Work

Firewalls function by controlling the flow of traffic between different zones. Their methods can vary, but the goal is still to control the flow of traffic. [Figure 15-3](#) illustrates this process.

Firewall Methodologies

MODULE 5

Firewalls are typically described by their vendors as having all sorts of advanced and complex features in an effort to distinguish them from their competitors. Vendors have found creative ways to describe their products in an effort to sound compelling to potential customers.

NOTE

The first-generation firewall based on packet filtering was outlined in the late 1980s and resulted in the first operational firewalls. While by today's standards these firewalls are primitive at best, they represented a huge leap in security and provided the foundation for subsequent generations.

Firewalls can operate in one of three basic modes:

- Packet filtering
- Stateful inspection
- Application proxying

Packet filtering represents what could be thought of as the first generation of firewalls. Firewalls that used packet filtering could only do the most basic analysis of traffic, which meant that it was granting or denying access based on limited factors such as IP address, port, protocol, and little else. The network or security administrator would create what amounts to very primitive rules by today's standards that would permit or deny traffic.

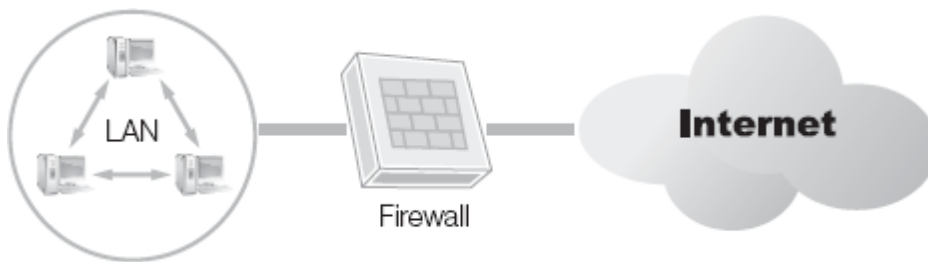


Figure 15-3. A firewall in action.

The downside of this type of device is that the filtering was performed by examining the header of a packet and not the contents of a packet. While this setup worked, it still left the door open for attacks to be performed. For example, a filter could be set up to deny File Transfer Protocol (FTP) access outright, but a rule could not be created to block specific commands within FTP. This resulted in an all-or-nothing scenario.

A firewall may also use a stateful packet inspection (SPI). In this setup, the attributes of each connection are noted and stored by the firewall, these attributes are commonly known as describing the state of the connection. These attributes typically contain details such as the IP addresses and ports involved in the connection and the sequence numbers of packets crossing the firewall. Of course, recording all these attributes helps the firewall get a better handle on what is occurring, but this comes at the cost of additional processing and extra load on the central processing unit (CPU) on the firewall device or system. The firewall is responsible for keeping track of a connection from

MODULE 5

the time it is created until it is finished, at which point the connection information is discarded by the firewall.

SPI offers the ability to track connections between points and this is where the power of this technique lies. In this technique, tracking the state of connection provides a means of ensuring that connections that are improperly initiated or have not been initiated correctly are ignored and not allowed to connect. A proxy firewall is a type of firewall that functions as a gateway for requests arriving from clients. Client requests are received at the firewall, at which point the address of the final server is determined by the proxy software. The application proxy performs translation of the address and additional access control checking and logging as necessary, and then connects to the server on behalf of the client.

Limitations of a Firewall

On the surface it sounds as if firewalls can do a lot just by controlling the flow of traffic; while this is true, they can't do everything. There are some things firewalls are not suited to performing and understanding, and understanding these limitations will go a long way toward letting you get the most from your firewall. Some companies in the past have made the ill-conceived decision to buy a firewall and set it up without asking what they are protecting from what and if the device will be able to do so. Unfortunately, a lot of companies have purchased firewalls, installed them, and later on wondered why security didn't improve.

The following areas represent the types of activity and events that a firewall will provide little or no value in stopping:

- **Viruses**—While some firewalls do include the ability to scan for and block viruses, this is not defined as an inherent ability of a firewall and should not be relied upon. Also consider the fact that as viruses evolve and take on new forms, firewalls will most likely lose their ability to detect them easily and need to be updated. This capability can retain its effectiveness, however, if the security administrator takes the time to regularly update the definition database on the firewall, either through subscriptions or manually. In most cases, antivirus software in the firewalls is not, and should not be, a replacement for system resident antivirus.
- **Misuse**—This is another hard issue for a firewall to address as employees already have a higher level of access to the system. Put this fact together with an employee's ability to disregard company rules against bringing in software from home or downloading from the Internet, and you have a recipe for disaster. Firewalls cannot perform well against intent.
- **Secondary connections**—In some situations, secondary access is present and presents a major problem. For example, if a firewall is put in place, but the employee can unplug the fax machine from the phone line, plug the fax into the computer, and plug the computer into the network with the modem running, the employee has now opened a hole in the firewall.
- **Social engineering**—Suppose a network administrator gets a call from someone who says he works for the Internet service provider that serves the administrator's network. The caller wants to know about the company's firewalls. If the administrator gives out the information

MODULE 5

without checking the caller's identity and confirming that he needs to know what he's asking about, the firewalls can lose their effectiveness.

- **Poor design**—If a firewall design has not been well thought-out or implemented, the net result is a firewall that is less like a wall and more like Swiss cheese. Always ensure that proper security policy and practices are followed.

Implementing a Firewall

There are many different options for installing firewalls, and understanding each way is key to getting the correct deployment for your organization. The following describes different options for firewall implementation:

- **Single packet filtering device**—In this setup, the network is protected by a single packet filtering device configured to permit or deny access. [Figure 15-4](#) illustrates this setup.

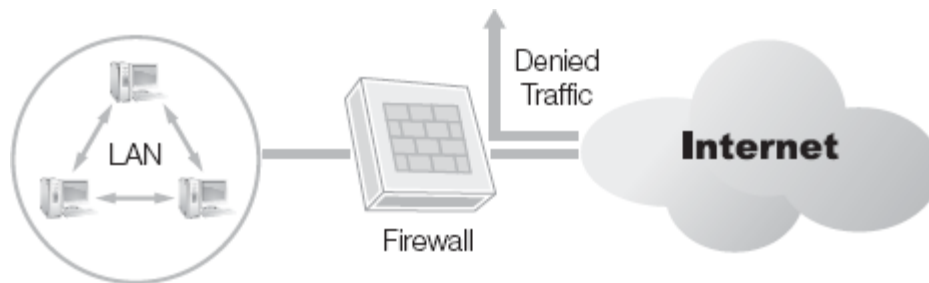


Figure 15-4. Single packet filtering device.

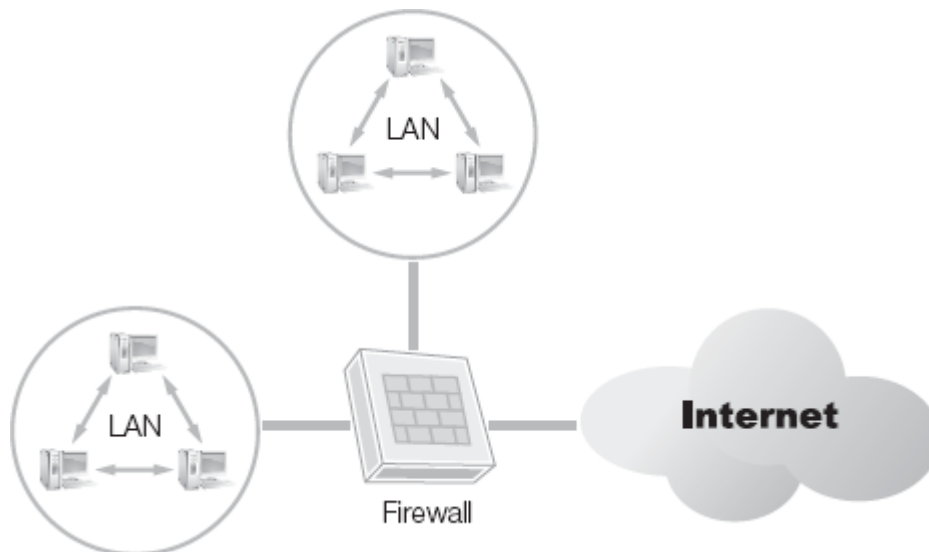


Figure 15-5. Multi-homed device.

MODULE 5

- **Multi-homed device**—This device has multiple network interfaces that use rules to determine how packets will be forwarded between interfaces. [Figure 15-5](#) illustrates a multi-homed device.
- **Screened host**—A screened host is a setup where the network is protected by a device that combines the features of proxy servers with packet filtering. [Figure 15-6](#) illustrates a screened host.
- **Demilitarized zone (DMZ)**—A region of the network or zone that is sandwiched between two firewalls. In this type of setup, the DMZ is set up to host publicly available services. [Figure 15-7](#) illustrates a DMZ.

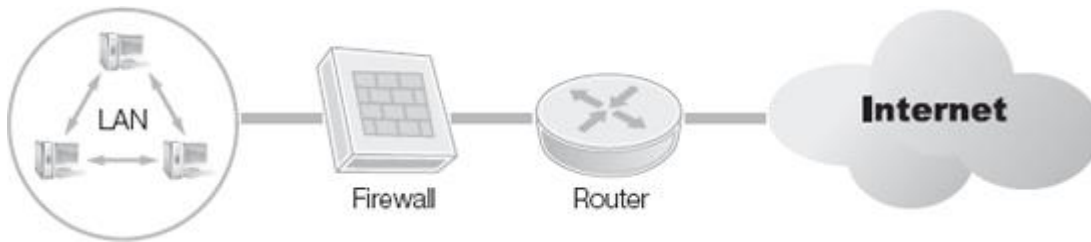


Figure 15-6. Screened host.

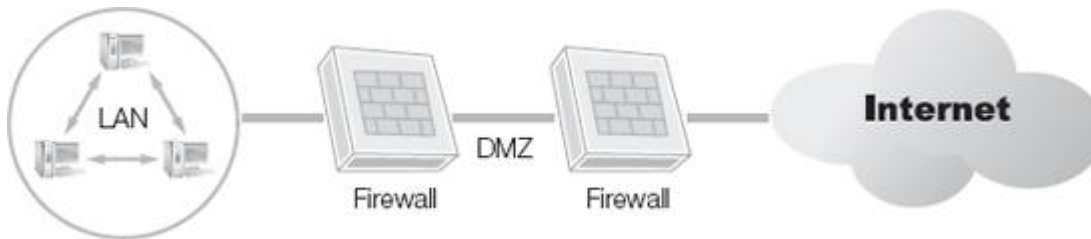


Figure 15-7. A DMZ.

In an organization it is possible that some services such as a Web server, DNS, or other resource may be required to be accessed by those outside the network. By its very nature this setup makes it so these systems are more vulnerable to attack as the outside world has access to them. In order to provide a means of protection, a DMZ is used to allow outside access while at the same time providing some protection. A DMZ can allow these hosts to be accessed by the outside world, although the outer firewall in the DMZ provides only limited connectivity to these resources. Additionally, even though those outside the firewall have access to the resources, they do not have any access to the internal network or this access is highly restricted being given only to specific hosts on the internal network.

To appreciate the utility of a firewall, consider the situation without this structure. If a single firewall were in place, the publicly accessible resources would be on the internal network, which would mean that anyone outside the network gaining access to the resources would in essence be on the internal network. Conversely, if the resources were moved outside the firewall, there would be little if any protection for them as access would be tough to control.

Authoring a Firewall Policy

MODULE 5

Before you charge out and put a firewall in place, you need a plan that defines how you will configure the firewall and what is expected. This is the role of policy. The policy you create will be the blueprint that dictates how the firewall is installed, configured, and managed. It will make sure that you are addressing the correct problems in the right way and that nothing unexpected is occurring.

For a firewall to be correctly designed and implemented, the firewall policy will be in place ahead of time. The firewall policy will represent a small subset of the overall organizational security policy. The firewall policy will fit into the overall company security policy in some fashion and uphold the organization's security goals, but enforce and support those goals with the firewall device.

The firewall policy you create will usually approach the problem of controlling traffic in and out of an organization in two ways. The first option when creating a policy and the firewall options that support it is to implicitly allow everything and explicitly deny only those things that you do not want. The other option is to implicitly deny everything and allow only those things you know you need. The two options represent drastically different methods of configuring the firewall. In the first option you are allowing everything unless you say otherwise, while the second will not allow anything unless you explicitly say otherwise. One is much more secure by default than the other.

Consider the option of implicit deny, which is the viewpoint that assumes all traffic is denied, except that which has been identified as explicitly being allowed. Usually this turns out to be much easier in the long run for the network/security administrator. For example, visualize creating a list of all the ports Trojans use plus all the ports your applications are authorized to use, and then creating rules to block each of them. Contrast that with creating a list of what the users are permitted to use and granting them access to those services and applications explicitly.

There are many different ways to approach the creation of firewall policy, but the ones that tend to be used the most are known as Network Connectivity Policy, the Contracted Worker Statement, and the Firewall Administrator Statement.

Network Connectivity Policy

This portion of the policy involves the types of devices and connections that are allowed and will be permitted to be connected to the company-owned network. You can expect to find information relating to the network operation system, types of devices, device configuration, and communication types.

This policy arguably has the biggest impact on the effectiveness of the firewall; this section is defining permitted network traffic and the shape it will take.

Included in this policy can be the following:

- Network scanning is prohibited except by approved personnel such as those in network management and administration.

MODULE 5

- Certain types of network communication are allowed, such as FTP and the Function Programming (FP) sites that are allowed to be accessed.
- Users may access the Web via port 80 as required.
- Users may access e-mail on port 25 as required.
- Users may not access Network News Transfer Protocol (NNTP) on any port.
- Users may not run any form of chat software to the Internet, including, but not limited to, AOL Instant Messenger, Yahoo Chat, Internet Relay Chat (IRC), ICQ, and Microsoft Network (MSN) Chat.
- Antivirus software must be installed and running on all computers.
- Antivirus updates are required on all computers.
- Antivirus updates are required on all servers.
- No new hardware may be installed in any computer by anyone other than the network administrators.
- No unauthorized links to the Internet from any computer are allowed under any circumstances.

This list is meant only to illustrate what you may find in these policies, but in practice you can expect to see a much longer and more complex list that will vary depending on the organization.

Contracted Worker Statement

This next policy is another that tends to be of use in larger organizations with large numbers of contracted or temporary workers. These types of workers may very well have enhanced connectivity requirements due to how they work. These individuals could, for example, require only occasional access to resources on the network.

Some examples of items in the contracted worker statement portion of the policy are:

- No contractors or temporary workers shall have access to unauthorized resources.
- No contractor or temporary worker shall be permitted to scan the network.
- No contractor or temporary worker may use FTP unless specifically granted permission in writing.

Firewall Administrator Statement

Some organizations may not have a policy for the firewall administrator, but it is not unheard of to have one. If yours is one that will require such a statement, the following are some examples that may be contained in a firewall policy:

- The firewall administrator should be thoroughly trained on the firewall in use.
- The firewall administrator must be aware of all the applications and services authorized to access the network.
- The firewall administrator will report to an entity such as the Chief Information Officer.
- There will be a procedure in place for reaching the firewall administrator in the event of a security incident.

MODULE 5

It is probably obvious that the firewall administrator is a clearly defined job role that will require the proper rules and regulations placed upon it. It is not uncommon for some organizations to have such a policy, but others will not. It can be a benefit in a large organization to know these items, and to have them written in the policy.

Firewall Policy

A firewall isn't just configured in the way the administrator wants; it requires a policy to be followed for consistent application. A firewall policy is designed to lay out the rules on what traffic is allowed and what is not. The policy will specifically define the IP addresses, address ranges, protocol types, applications, and other content that will be evaluated and granted or denied access to the network. The policy will give detailed information on this traffic and in turn will be used as the template or guideline on what to specifically configure on the firewall. The policy will also provide guidance on how changes to traffic and requirements are to be dealt with (how a change will be initiated to the firewall, who is responsible, and so on). This practice, known as implicit deny, decreases the risk of attack and reduces the volume of traffic carried on the organization's networks. Because of the dynamic nature of hosts, networks, protocols, and applications, implicit deny is a more secure approach than permitting all traffic that is not explicitly forbidden.

Honeypots/Honeynets

This section discusses the **honeypot**, a device that is unique among security devices. The honeypot is a computer that is configured to attract attackers to it, much like bears to honey. In practice these devices will be placed in a location so that if an attacker is able to get around the firewall and other security devices, this system will act as a decoy drawing attention away from more sensitive assets.

Goals of Honeypots

What is the goal of a honeypot? It can be twofold and will vary depending on who is deploying it. The honeypot can act as a decoy that looks attractive enough to an attacker that it draws attention away from another resource that is more sensitive, giving you more time to react to the threat. A honeypot can also be used as a research tool by a company to gain insight into the types and evolution of attacks and give them time to adjust their strategies to deal with the problem.

NOTE

An attacker that can detect a honeypot could cause serious problems for a security professional. An attacker that is able to uncover what is really going on may be upset or angered by the attempt and attack you more aggressively as a "reward."

The problem with honeypots? They need to look attractive, but not so attractive that an attacker will know that they are being observed and that they are attacking a noncritical resource. Ideally you want an attacker to view the resource as vulnerable and not so out of place that they can detect that it is a ruse. When you configure a honeypot, you are looking to leave out patches and do minor

MODULE 5

configuration options someone might overlook and that an attacker will expect to find with a little effort.

A honeypot is a single system put in place to attract an attack and buy you more reaction time in the event of an attack. Under the right conditions, the honeypot will assist you in detecting an attack earlier than you would normally and allow you to shut it down before it reaches production systems.

A honeypot also can be used to support an additional goal: logging. By using a honeypot correctly and observing the attacks that take place around it, you can build a picture from the logs that will assist you in determining the types of attacks that you will be facing. Once this information is gathered and a picture is built, you can start to build a better picture of the attacks and then plan and defend accordingly.

Building upon the core goal of a honeypot, which is to look like an attractive target, the next step is a **honeynet**, which builds on the lessons and goals of the honeypot and the goals from one vulnerable system to a group of vulnerable systems or a network.

Legal Issues

One of the issues that comes up when discussing honeypots and honeynets is the issue of legality. Basically the question is if you put a honeypot out where someone can attack it and does so, can you prosecute for a crime and would the honeypot be admissible as evidence? Some people feel that this is a cut-and-dried issue of entrapment, but others feel otherwise. Let's look at this a little more closely to understand the issue.

It has been argued that honeypots are entrapment because when you place one out in public you are enticing someone to attack it—at least that's the theory. In practice, attorneys have argued this point a handful of times without success due to certain points that have come up in other cases. Consider the police tactic of placing undercover female officers on a street corner playing the role of a prostitute. When officers stand there they simply wait and don't talk to anyone about engaging in any sort of activity, but when people approach the officer and ask about engaging in an illicit activity, they are arrested. A honeypot would be the same situation. No one forces attackers to go after honeypots; the attackers decide to do so on their own.

Role of Controls

Protecting the organization is a series of controls, a number of which you have experienced. These controls fit into one of three key areas, each designed to provide one piece of an overall comprehensive solution: administrative, physical, and technical.

Technical, administrative, and physical controls are mechanisms that will work together to provide what is commonly known as defense in depth. This is the key detail: controls working together to ensure that security is maintained. Defense in depth enhances security by layering security

MODULE 5

measures, as in the design of a castle. A castle has moats, walls, gates, archers, knights, and other defenses—which is what you are looking for with security controls. By combining layers, you gain the advantage of multiple mechanisms to protect your systems. Next you gain the advantage of having a hedge against failure, meaning that if one layer or mechanism fails, you have others to fall back on.

Administrative Controls

Administrative controls are those that fit in the area of policy and procedure. What you will find here are the rules that individuals and the company will follow to ensure a safe and consistently secure working environment. Listed in this section are some of the more common administrative controls that you would expect to see in practice:

- **Implicit deny**—Implicit deny is a rule or guideline that dictates that anything that is not directly addressed in policy is automatically in a default deny state. This means that if you miss a setting or configuration option, in software for example, you default to a state where no access is given. The opposite would be one where every action is given access unless explicitly taken away, much less secure.
- **Least privilege**—Least privilege is the rule or guideline that states that individuals will be given only the level of access that is appropriate for their specific job role or function. Anything that individuals do not need to perform their jobs is not given to them.
- **Separation of duties**—Separation of duties is a guideline that dictates that a user will never be in a situation where he or she can complete a critical or sensitive task alone. If one individual, for example, has the ability to evaluate, purchase, deploy, and perform other tasks that individual has too much power, which should instead be distributed among multiple people.
- **Job rotation**—This is the ability to rotate people periodically between job roles to avoid them staying too long in a sensitive job role. The idea is to help prevent abuse of power and to detect fraudulent behavior.
- **Mandatory vacation**—This technique is used to put employees on vacation for several days in order to give the company time to detect fraud or other types of behaviors. With an employee gone for several days (usually a period of a work week), the organization's auditors and security personnel can investigate for any possible discrepancies.
- **Privilege management**—The process of using authentication and authorization mechanisms to provide centralized or decentralized administration of user and group access control. Privilege management needs to include an auditing component to track privilege use and privilege escalation.

Technical Controls

Working in concert with administrative controls are technical controls that help enforce security in the organization. The technical controls you use will work with your other controls to create a robust security system. While there are a range of technical security controls, a handful stand out as more common than others.

MODULE 5

Preventive logical controls include:

- Access control software
- Malware solutions
- Passwords
- Security tokens
- Biometrics
- Access control software
- Antivirus software

Access control software is software designed to control access to and sharing of information and applications. Software in this category can enforce access using one of three methods: discretionary access control (DAC), role based access control (RBAC), and mandatory access control (MAC).

- **DAC**—An access method that depends on the owner or author of data to manage security. A prime example of DAC is the use of folder and file permissions. Under DAC the owner/creator of data can grant write, read, and execute permissions as necessary. The advantage of this security management model is that it facilitates a quick and easy way of changing security settings; however, it has the problems associated with being decentralized. The decentralization of security management means that there could be inconsistent application of settings.
- **RBAC**—An access control method based on the role that an individual holds within an organization. RBAC excels in environments in which a medium to large pool of users exists. In this access control model users are assigned to roles based on function and these are assigned permissions.
- **MAC**—A system that uses labels to determine the type and extent of access to a resource and the permission level granted to each user. This type of access control system requires more effort to manage than DAC or RBAC.

Malware has become a considerable threat to organizations. Anti-malware solutions are essential tools in protecting the security of an organization with many organizations moving towards robust centralized applications designed to safeguard against software.

Passwords are another technical control; in fact, they may be the most common type of technical control in use. Interestingly enough, it may be the least effective, as users have been known to post passwords on monitors, choose simple passwords, and do other things that make passwords insecure. The idea is to use strong passwords as a preventive technical control. Passwords should be supplemented with other controls and even additional authentication mechanisms such as tokens or biometrics.

Security tokens are devices used to authenticate a user to a system or application. These devices take the form of hardware devices such as cards, fobs, and other types of devices. These types of devices can take many forms, including smart cards, key fobs, or cards. Tokens are intended to provide an enhanced level of protection by making the user present two forms of authentication—typically the token and a password or personal identification number (PIN)—that identify him or

MODULE 5

her as the owner of a particular device. If so equipped, the device will display a number on an LCD display which uniquely identifies the user to the service, allowing the logon. The identification number for each user is changed frequently at a predefined interval, which typically is one minute to five minutes or longer.

These devices can be used by themselves, but they are frequently used in conjunction with other controls such as passwords.

Biometrics is another type of access control mechanism. It provides the ability to measure the physical characteristics of a human being. Characteristics measured here include fingerprints, handprints, facial recognition, and similar methods.

Data backup is another form of control that is commonly used to safeguard assets. Never overlook the fact that backing up critical systems is one of the most important tools that you have at your disposal. Such procedures provide a vital protection against hardware failure and other types of system failure.

Not all backups are created equal and the right backup makes all the difference:

- Full backups are the complete backups of all data on a volume; they typically take the longest to run.
- Incremental backups copy only those files and other data that have changed since the last full or incremental backup. The advantage is that the time required is much less, so it is done more quickly. The disadvantage is that these backups take more time than a full backup to rebuild a system.
- Differential backups provide the ability to both reduce backup time and speed up the restoration process. Differential backups copy from a volume that has changed since the last full backup.

Physical Controls

Physical security controls represent one of the most visible forms of security controls. Controls in this category include barriers, guards, cameras, locks, and other types of measures. Ultimately physical controls are designed to more directly protect the people, facilities, and equipment than the other types of controls do.

Some of the preventative security controls include the following:

- **Alternate power sources**—Items such as backup generators, uninterrupted power supplies, and other similar devices
- **Flood management**—Includes drains, ducting, and other mechanisms designed to quickly evacuate water from an area
- **Fences**—Structures that are designed to prevent access to sensitive facilities either as a simple deterrent or as an imposing physical barrier

MODULE 5

- **Human guards**—Placing the human element onsite around sensitive areas with the intention of providing an element of intelligence and the ability to react to unanticipated situations
- **Locks**—Devices placed in locations to prevent easy access to areas that are sensitive in nature
- **Fire suppression systems**—Covers devices such as sprinklers and fire extinguishers designed to suppress or lessen the threat of fires
- **Biometrics**—Often these devices are generally used in conjunction with locks to regulate physical access to a location.
- **Location**—Location provides some measure of protection by ensuring that facilities are not located where they may be prone to threats such as fire or flood. Also addresses issues of placing facilities or assets in locations where they may not easily be monitored.

Generally you can rely on your power company to provide your organization power that is clean, consistent, and adequate, but this isn't always the case. Anyone who has worked in an office building has noticed a light flicker, if not a complete blackout. Alternate power sources safeguard against these problems to different degrees.

Hurricane Katrina showed us how devastating a natural disaster can be, but the disaster wasn't just the hurricane; it was the flood that came with it. You can't necessarily stop a flood, but you can exercise flood management strategies to soften the impact. Choosing a facility in a location that is not prone to flooding is one option that you have available. Having adequate drainage and similar measures can also be of assistance. Finally, mounting items such as servers several inches off of the floor can be a help as well.

Fences are a physical control that represents a barrier that deters casual trespassers. While some organizations are willing to install tall fences with barbed wire and other features, it is not always the case. Typically the fence will be designed to meet the security profile of the organization, so if your company is a bakery instead of one that performs duties vital to national security, the fence design will be different as there are different items to protect.

Guards provide a security measure that can react to the unexpected as the human element is uniquely able to do. When it comes down to it, technology can do quite a bit, but it cannot replace the human element and brain. Additionally, once an intruder makes the decision to breach security, guards are a quick responding defense against them actually reaching critical assets.

The most common form of physical control is the ever-popular lock. Locks can take many forms including key locks, cipher locks, warded locks, and other types of locks—all designed to secure assets.

Fire suppression is a security measure that is physical and preventative. Fire suppression cannot stop a fire, but it can prevent substantial damage to equipment, facilities, and personnel.

CHAPTER SUMMARY

MODULE 5

One of the challenges you are going to face is that of verification. It is a challenge because the tools you will be using can do their job, but you need to be able to make sure they are always functioning as designed. The controls that you put in place today may not be equipped to deal with the problems that will arise tomorrow. Additionally your network and the infrastructure that it comprises will become more complex with larger numbers of employees going mobile and using advanced connection techniques such as VPNs.

All this complexity makes managing the security, while maintaining the usability and capability of the network, much more difficult than it would be otherwise. For all these systems to work together effectively, a certain level of trust must be built into the system, meaning that one system gives a certain level of credibility to another system. These points are things that you must consider in order to properly secure your network.

Securing your network and infrastructure requires a mix of capabilities and techniques, some of which have been introduced in this course. In the past, quite a bit of effort was focused on the prevention of an attack, but what about those times where a new or unanticipated attack gets through your defenses? Sure, you can prevent an attack by using firewalls, policies, and other technologies, but there are other things that can help. That's where detection comes into play and where devices and technologies such as the IDS and honeypots can assist you.

KEY CONCEPTS AND TERMS

- **Anomaly detection**
- **Honeynet**
- **Honeypot**
- **Host-based intrusion detection system (HIDS)**
- **Intrusion**
- **Intrusion detection**
- **Misuse**
- **Misuse detection**
- **Network-based intrusion detection system (NIDS)**
- **Signature Analysis**

CHAPTER 15 ASSESSMENT

1. HIDS can monitor network activity.
 1. True
 2. False
2. A(n) _____ monitors activity on one host, but cannot monitor an entire network.
 1. NIDS
 2. Firewall
 3. HIDS
 4. DMZ
3. A(n) _____ has the ability to monitor network activity.

MODULE 5

1. NIDS
2. HIDS
3. Firewall
4. Router
4. _____ can monitor changes to system files.
 1. Hashes
 2. HIDS
 3. NIDS
 4. Router
5. Signature-based IDSs look for known attack patterns and types.
 1. True
 2. False
6. Anomaly-based IDSs look for deviations from normal network activity.
 1. True
 2. False
7. An IPS is designed to look for and stop attacks.
 1. True
 2. False
8. What is used to monitor an NIDS?
 1. Console
 2. Sensor
 3. Network
 4. Router
9. What are deployed to detect activity on the network?
 1. Console
 2. Sensors
 3. Network
 4. Router
10. _____ can only monitor an individual network segment.
 1. HIDS
 2. NIDS
 3. NAT
 4. Sensors

table of contentssearch

Settings

14. Incident Response

15. Defensive Technologies

queue

Hacker Techniques, Tools, and Incident Handling

A. Answer Key

Table of contents collapsed