# Unit V

Advanced Computer Forensics: Advanced Encryption, Advanced hacking, Source addresses, the problem of present, the outlook for future, Summary, Conclusions, Recommendations, Computer Forensics needs and challenges

## Advanced Computer Forensics:

The rise of the so-called information economy, borne along by proliferating computers, sprawling telecommunications, and the Internet, has radically transformed how people do business, govern, entertain themselves, and converse with friends and family. Private documents that in the past would have been committed to paper and hand-delivered or stowed under lock and key are now routinely created, sent, and stored electronically.

The very things that allow such speed and ease of communication have also made it far more difficult to ensure one's privacy. In an electronic age, an interloper can intercept and alter messages far more easily now than when face-toface exchanges were the norm.

## Advanced Encryption

On German television several years ago, a stunned audience looked on as an unsuspecting Web surfer had his computer scanned while he was visiting a site. The site operators determined that a particular online banking program was installed on his computer, and they remotely modified a file in it so that the next time the user connected to his bank online, he also directed his bank to send a payment to the owners of that Web site.

The vulnerability of computer data affects everyone. Whenever a computer is connected to a network, be that a corporate intranet or the Internet, unless proper precautions are taken, the data residing in the machine can be accessed and otherwise modified by another knowledgeable user. Even computer data that the user may believe to be deleted or overwritten can be retrieved. Courts now routinely subpoena individuals' and companies' magnetic media as evidence; forensic experts can reconstruct data files that have been erased. The best way to protect electronic data is to encrypt it.

The purpose of encryption is to render a document unreadable by all except those authorized to read it. The content of the original document, referred to by cryptographers as "plaintext," is scrambled using an algorithm and a variable, or key. The key is a randomly selected string of numbers; generally speaking, the longer the string, the stronger the security.

### Symmetric Encryption

Vernam's one-time pad is an example of symmetric encryption, in which the same key is used to both encode and decode a message. Many of the encryption schemes available today are also symmetric, most notably the Data Encryption Standard (DES).

### A MENU OF SYMMETRIC ENCRYPTION ALGORITHMS

In symmetric encryption, the same key is used to encrypt and decrypt a message.

Here are the most popular.

THE DATA ENCRYPTION STANDARD (DES) was developed in the 1970s and is still used worldwide, although it has been replaced by the Advanced Encryption Standard (AES).

### TRIPLE DES

Encrypting the already DES-encrypted output with a different output with a different key provides no measurable security, but adding a third round of DES encryption yields a highly secure, albeit slower, algorithm. Most purportedly triple-DES implementations, however, use only two keys: key 1 for the first round of encryption, key 2 for the second round, and key 1 again for the third round.

### THE INTERNATIONAL DATA ENCRYPTION ALGORITHM

The international data encryption algorithm (IDEA) uses a 128-bit key developed by ETH Zurich, in Switzerland. Its U.S. and European patents are held by Ascom Systec Ltd. of Bern, Switzerland, but noncommercial use is free. IDEA is viewed as a good algorithm for all except the best-funded attacks. It is used in Pretty Good Privacy (PGP) and Speak Freely (a program that allows an encrypted digitized voice to be sent over the Internet).

### BLOWFISH

Blowfish is a 64-bit block code with key lengths of 32 to 448 bits. Developed in 1993 by Bruce Schneier of Counterpane Internet Security Inc., San Jose, California, it is used in over 100 products and is viewed as one of the best available algorithms.

### TWOFISH

Twofish, also developed by Schneier, is reputedly very strong, and, as one of five candidates for AES, is now being extensively reviewed by cryptanalysts.

### RC4

RC4 is a stream cipher of unknown security, designed by Ronald Rivest for RSA Security Inc., Bedford, Massachusetts. It adds the output of a pseudorandom number generator bit by bit to the sequential bits of the digitized plaintext.

## Public Key Encryption

An ingenious scheme that avoids many of the problems of symmetric encryption was proposed in 1976 by Stanford professor Martin Hellman and his graduate student Whitfield Diffie.

The method works like this: Bob and Alice have a copy of openly available software that implements the public-key algorithm. Each directs his or her copy of the software to create a key, or rather, a pair of keys. A file encrypted with one key of a pair can only be decrypted with the other key of that same pair.

If Bob wants to encrypt a message that only Alice can read, he uses Alice’s public key (which is available to anyone); that message can only be decoded by Alice’s private key (Figure 20.1) [2]. The reciprocal process (sending an encrypted message from Alice to Bob) is clear. In effect, Bob and Alice can now

exchange encrypted files in the absence of a secure means to exchange keys, a major advantage over symmetric encryption.

Sender authentication verifies that the sender is who he or she appears to be. Suppose Bob sends a message to the world after encrypting it with his private key. The world uses Bob's public key to decrypt that message, thereby validating that it could only have come from Bob.

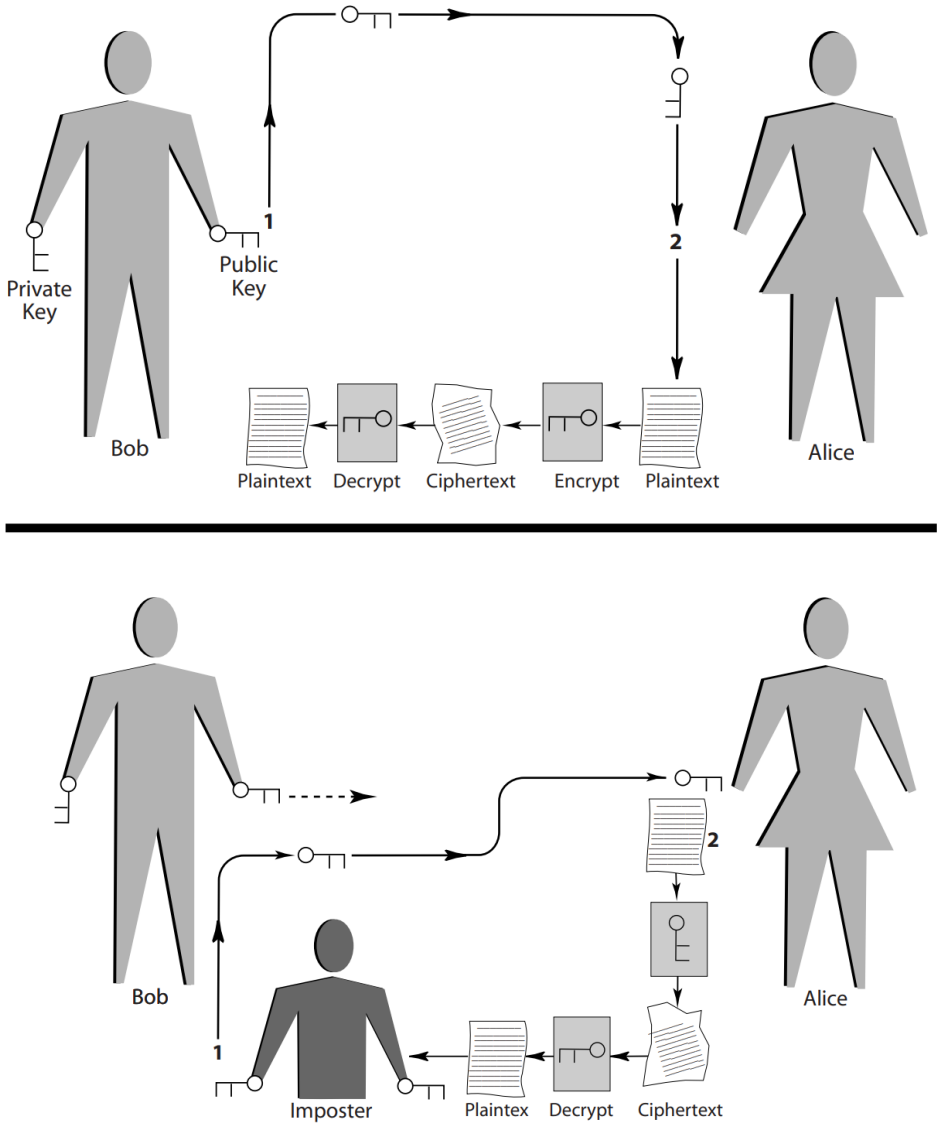


**FIGURE 20.1** In public-key encryption [top], Alice encrypts a message using Bob's public key, and Bob decrypts it using his private key. This scheme allows encrypted files to be sent in the absence of a secure means to exchange keys, a major improvement over symmetric encryption. It's still possible, though, for Alice to receive a public key (or a conventional symmetric key) that ostensibly came from Bob, but that, in fact, belongs to a third party claiming to be Bob—the so-called man-in-the-middle attack (bottom).

Public-key encryption has been a part of every Web browser for the past few years. It is used, for example, when sending credit-card information to an online vendor or when sending email using the standard S/MIME protocol and a security certificate, which can either be obtained from online commercial vendors or created locally using special software.

One drawback of public key encryption is that it is more computationally intensive than symmetric encryption. To cut back on the computing, almost all implementations call on the symmetric approach to encrypt the plaintext and then use public key encryption to encode the local key. The differently encrypted plaintext and key are then both sent to the recipient.

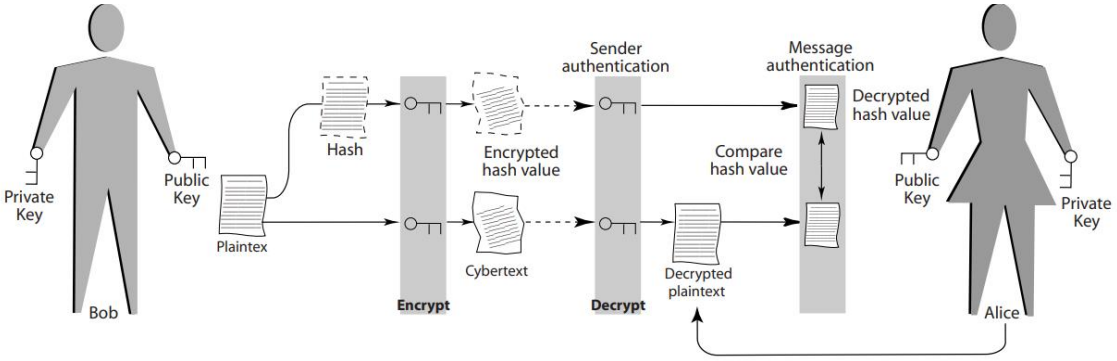


**FIGURE 20.2** Public key encryption allows Alice to verify that a message from Bob actually came from him and that it is unaltered from the original. Here's how: Bob encrypts the hash value with his private key, encrypts the plaintext with Alice's (green) public key, and sends both to her. Alice then decodes the received ciphertext using her own (orange) private key, decodes the hash value using Bob's public key, thereby confirming the sender's authenticity, and compares the decrypted hash value with one that she calculates locally on the just decrypted plaintext, thereby confirming the message's integrity.

## Advanced hacking

Today, as enterprise-wide networks reach the plant floor and zip data to the far side of the world in a twinkling, and, as the number of computers, personal digital assistants, telephones, and pagers communicating with the network increases, there is a corresponding increase in the opportunities for a critical blunder that would allow an attacker to enter your system. The consequences could be ruinous.

### HACK YOURSELF BEFORE SOMEBODY ELSE DOES

How do you test your system to make sure it's as safe as possible? Can you recommend software, hardware, or services that can identify security issues before they become problems? What kind of procedures do you have in place to make sure that the latest patches are applied to Web servers?

The best way to retain your network security is to do frequent security audits, including trying to gain access using easily available hacking tools. In addition, you should ensure that you only run the services you need and only open the ports needed by your network. Your gateway to the Internet should be a system without any important company data or a hardware solution backed up by a firewall. You should

also set up Windows Update notification for the server and have a backup server ready when you need to run the update.

## Tools of the Trade:

The Internet is filled with Web sites that offer tips and tools for the neophyte hacker. Kids, criminals, and terrorists are some of the people who avail themselves of this information—so more and more intruders are knocking at port doors. The barrier to entering the hacker world has become very low. If you have a political motivation against wheat farmers and you want to deface their Web page, you could just go online and learn how to do it.

### Future threat: advanced malicious code in software:

Malicious code embedded in software is not new; users have always run the risk of downloading a virus or a trojan horse with shareware and games from the Net. The occasional intruder has even been found in shrink-wrapped products, but the hack into Microsoft's source code recently, raises worries that popular software may be the next target.

## Good and Bad Hackers:

Not all hackers have malicious intentions. Some hackers work for companies to secure their systems and some contribute to security by notifying software vendors when they spot vulnerability. Breaking things is easy. Building a solution is difficult, but arguably more fulfilling, but for every hacker who swaps his black hat for a white one, dozens of others continue to keep governments and companies on their toes.

## Idle Hands:

People see movies like WarGames and think hackers are going to start World War III. The truth is that computer hackers for the most part are smart, bored kids. Hackers usually start in their teens and stop by the time they're 30, but anyone can be a hacker—from the 16-year-old who defaces Web sites to the 36-year-old who sabotages a former employer's server. People in the underground indicate that not all hackers are true hackers.

## By Any Other Name

It used to be that hacking had nothing to do with breaking the law or damaging systems. The first hackers, who emerged at MIT in the 1960s, were driven by a desire to master the intricacies of computing systems and to push technology beyond its known capabilities. The hacker's ethic, an unwritten dictum governing the hacker world, indicates that a hacker should do no harm. A hacker should pass through a network without a trace. Somehow that message has gotten lost in the noise of Web defacements and data thefts.

## Signs of the Times

Hacking has definitely changed in the past 43 years. Talk to any hacker over 25, and he's likely to lament the passing of the good old days, when coding was an art form and learning how systems worked was an exercise in persistence. They say new hackers today are often younger and less skilled than their predecessors and more likely to focus on showy exploits than the noble pursuit of knowledge.

### Bigger Threats

Script kiddies may get attention, but experts agree that the most dangerous hackers are the ones who don't make any noise: criminal hackers and cyber terrorists.

Why Hackers Hack Aside from criminal and political motives, the reasons that hackers hack range from malice and revenge to simple boredom. Despite the image of hackers as dysfunctional loners, many are drawn to hacking by the sense of community it gives. Of course, a big part of hacking's attraction is the sense of power that comes from uncovering information you shouldn't possess. A hacker called Dead Addict once described the high that comes from discovering valuable information, followed by the low that comes from realizing you can't do anything with it.

### White Hats

There are a lot of the reasons why hackers' ability to hack into computers fade with age. Life fills their time and their ethics begin to change. The majority eventually find their interest waning. You only have three directions to go with hacking: you can keep doing the same old tricks, you can become a real criminal cracker, or you can use those skills wisely to build new software and create a more secure Internet.

## Advanced Tracker Hackers

As the number of computer crimes spirals, the computer forensics experts skills are getting ever more precious. These are the data detectives who search for digital clues remaining on computers after malicious (or black-hat) hackers have done their dirty deeds.

### Anonymity in Retrieving System Logs

The 9-11 terrorist attacks have had numerous effects on national security. One of these is legislation that increases the ability of federal agencies to intercept Internet traffic. Another side effect was the loss of the well-known Web anonymity service hosted by ZeroKnowledge, which turned out not to be related to any of the national security activities during 9-11. Web anonymizers allow people to visit Web sites without disclosing their identities to the owner of the Web site, or even a local administrator who can log the URLs that a user visits.

### Source Addresses

A source address is an IP address embedded in the header of an IP packet. When the packet is received, the source address becomes the destination address in the reply packet. If you spoof your source address, reply packets wind up going to the address that you've spoofed, and you don't see the results.

### Routing to the Rescue

Surprisingly, the U.S. Navy has researched network anonymity. This research formed the basis for the Freedom Network and may show up in other systems for anonymity as well. Suppose that you proxy your Web requests through a third party who promises to keep its logs a secret. You connect to this server via secure sockets layer (SSL) so that anyone sniffing the connection can only see that you're visiting an

anonymizer, and not your final destination site, which is encrypted. Sounds like a reasonable solution, but it hasn't worked in the past.

If the proxy doesn't even know your real source address. There have been several approaches to this problem, and one of the most recent is Onion Routing.

In Onion Routing, instead of having a single proxy for relaying, there's a network of proxies. Each of these proxies runs the same software, which not only relays your packets but also encrypts them. The first Onion Router chooses a route for your connection, and then encrypts your data several times, each time using the public key for one of the routers in its network of routers.

This is where the "onion" comes in. Each layer of encryption resembles the skin of an onion: the Onion Router you've connected to first encrypts your data using the key of the last router in its list of routers—this makes up the innermost layer of Advanced Computer Forensics 651 the onion. Once this layer of encryption is removed, the packet is sent to its real destination. Then, the first Onion Router adds another layer of encryption. This layer includes the address of the last router in the list, and gets encrypted with the second to last router's key.

Onion Routing is even more effective if you run one of the routers. Your Onion Router must also be a full participant in the network, so that other Onion Routers can use it. Otherwise, packets coming from your Onion Router will only contain packets from your network, and can reveal your approximate source, even with the content still encrypted.

Onion Routing is only one approach to the problem of network anonymity.

## Who Needs It?

The Onion Routing project closed down in January 2000, after processing over 30 million requests. Its home page contains an interesting disclaimer, essentially saying that anyone using the Navy's network should expect their traffic to be monitored a very chilling statement when one considers the alleged intent of Onion Routing.

Denial of Service Pity the poor intrusion detection system (IDS)—it has the reputation of an irritating snitch and the track record to prove it. Perhaps no other security device has done its job so well and then been reviled so roundly for doing it. Designed to sniff out and warn system administrators when hackers are trying to exploit network vulnerabilities or launch denial-of-service (DoS) attacks, the original IDSs did their job all too well. That was both bad and good news.

## A Second Look

It's thus time for network professionals who gave up on the IDS a few years ago to go looking again. Indeed, market research numbers indicate that more and more of them plan to deploy IDSs in the coming years.

## Moving to Anomoly Tracking

The traditional network-based IDS discover malicious traffic by detecting the presence of known patterns, a process usually called “signature matching.” These systems work much like an anti-virus software package (detecting a known “bad” pattern generates an alarm) and effectively discover known patterns.

## Faster Systems

Most IDSs on the market now can keep up with a 400 Mbit/sec Ethernet. Beyond that, they begin to drop packets and become less efficient. When vendors push their IDS offerings beyond 400 Mbits/sec, they’re only looking at a subset of packets.

## Moving to Appliances

Another trend among IDS products is the network-based IDS appliance. Unlike first-generation IDS products, which required installing and configuring the vendor’s intrusion-monitoring software on a PC, these appliances merge hardware and software into a preconfigured unit.

## Outsourcing Intrusion Detection

Advances in IDS technology notwithstanding, organizations worried about unauthorized intrusions and DoS attacks should also consider outsourcing their intrusion detection needs. Outsourcing intrusion detection to an MSSP, which monitors customers’ IDSs via the Internet, can make sense for several reasons. Not the least of these is cost.

## Signs of Attempted and Successful Break-Ins

Hackers are succeeding more and more in gaining root-privilege control of government computer systems containing sensitive information. Computers at many agencies are riddled with security weaknesses. When an attacker gets root privileges to a server, he or she essentially has the power to do anything that a systems administrator could do, from copying files to installing software or sniffer programs that can monitor the activities of end users.

## Forensics

Threats to an enterprise’s information infrastructure can come in a number of unsuspecting forms. Beyond fending off network intrusions and DoS attacks, companies must stave off threats of industrial espionage.

## Divining Good Forensics

Obtaining a good digital fingerprint of a perpetrator requires that steps be taken to preserve the electronic crime scene. The examination will usually begin with a look at the disk drive. Minimal handling preserves its integrity, so any disk investigation should begin by making a copy of the original, using the least intrusive manner available.

## Leave It to the Pros

Although today’s sophisticated data-recovery tools have become fairly efficient, the process of recovery remains a tedious, labor-intensive task.

## How a Hacker Works?

Obviously, knowing how the hacker's mind works is only half of the battle. You must also know your network inside and out, identify its vulnerable points, and take the necessary steps to protect it.

### Diagram Your Network

You should begin by diagramming the topology of your network. You can do this with a sophisticated tool such as Visio, or you can use a less complex tool such as Word.

### Always-On Means Always-Vulnerable

Currently, the greatest security vulnerability is always-on Internet access using static IP addresses. With always-on access and a static IP, you are a like a big bull's-eye sitting on the Internet waiting to get hit.

A number of common ports are scanned and attacked: FTP (21) Telnet (23) SMTP (25) DNS (53) HTTP (80) POP3 (110) NNTP (119) IMAP (143) SNMP (161)

### Ways to Protect the Network

There are a number of ways to compensate for these vulnerabilities. First, you can implement firewall filtering. One of the best protections against port attacks is to implement a firewall with dynamic packet filtering, also called "stateful inspection firewalls."

### Seeing What the Hacker Sees

In addition to protecting against the well-known vulnerabilities, you need to see what the hacker sees when he looks at your network. The best way to do this is to use nmap, a program that gives you a look at your network from a hacker-like perspective.

### Software Vulnerabilities

Hackers also often exploit software security problems. They take advantage of these behind-the-scenes parts of the software to gain access to your system. Thus, you should take stock of all the software running on your Internet-exposed systems.

### Security Expert Web Sites

In addition to staying on top of your vendors' security updates and patches, you should also stay current on the security risks and problems that are identified by security experts in the industry.

## The problem of present

An IT worker faced federal criminal charges recently in U.S. District Court in Miami for allegedly downloading a virus into his employer's computer system, crashing the network for nearly two full days.

The U.S. Secret Service, which splits its focus between protecting heads of state and conducting criminal investigations, is handling twice as many cases that involve insider attacks than occurred in 2004. The FBI is currently investigating seven such cases in New England alone.

### Grocer Victimized

In the Miami case previously mentioned, Herbert Pierre-Louis, a hardware engineer who worked in the IT department at Purity Wholesale Grocers, is being charged with computer sabotage for the June 18, 1998, incident at the $2.6 billion national grocery outlet based in Boca Raton, Florida. The Assistant U.S. Attorney indicated the damage was well over the $6,000 waterline that is one of the key factors making this a federal crime.

### Similar Cases Prosecuted

Now that same statute is being used in three other cases. One of those cases charges a network consultant with sabotaging the computer network at one of his clients, Steinberg Diagnostic Medical Imaging in Las Vegas. The consultant is charged with three counts of network intrusion for changing passwords in the network, which locked administrators out of their own system.

## Outlook for the Future

Atlanta-based Internet Security Systems Inc. (ISS) has long been concerned about drive-by hackers. That's right—drive-by hackers. ISS claims perpetrators can equip their laptops with wireless technology, sit inconspicuously on a park bench or in a car, and casually monitor traffic, access applications, and hijack data flowing over someone else's wireless network, unbeknownst to the victim. To combat this threat, which sounds like it could be a plot line from an upcoming James Bond film; ISS recently drew the curtain on wireless local area network (WLAN) security software and consulting practices.

### Summary

Hackers and crackers are everywhere, but you may think your company's system is too minor for them to. Not true. Hackers don't always target specific machines—they scan hundreds with special programs to find any that might be vulnerable to attack. The intruder could be a teen hoping to use your system to launch an attack on a Web site, or a bitter ex-employee looking for payback. The Internet today is like a walk through a vineyard, with the attackers stopping here and there to pick a grape at their leisure. The feast is seemingly never-ending. Even a secure company network can be riddled with holes such as badly configured routers that expose data in transit to snoops. Think your firewall will protect you? Not always. Attacks at Microsoft and EBay prove otherwise.

### Conclusions

- Hackers often break into computers through well-documented holes (they read security alerts, too) when users don't install patches.
- Hackers often enter networks through old computers that are no longer in use.
- This can happen when administrators forget to disconnect an ex-employee's system from the modem or network.
- An older system is less likely to have the latest security patches installed.
- A shared terminal that's not attached to any one employee is often overlooked when security updates are done.
- Any workstation that's left on and connected to both a modem and the network gives hackers one way to dial into the machine, bypass the firewall, and gain access to the network.

- You encrypt important data on your server, but you neglect to encrypt remote backups.
- Hackers can target data on a less-protected off-site machine that stores backups.
- Security is an ongoing task. It's not something you install and forget about; it's something you live with.
- Intrusion detection systems (IDSs) come in several forms, with the most commonly deployed called "host" and "network" systems. Some experts include the "desktop" IDS in this market, whereas others would also list so-called honeypots and honeynets.
- A host-based IDS is a piece of software that runs on a network-based computer—a Web or application server, for instance. It tracks and analyzes entries in the host system's application and operating system event logs.
- Host-based systems are particularly valuable in monitoring insider threats because they can show when unauthorized personnel attempt to access prohibited data or resources.
- A network-based IDS, which can be software running on a stand-alone PC or on a dedicated appliance, tracks and analyzes the packets that make up network data traffic.
- Network-based IDSs are generally "promiscuous" in that they look at every packet on a network or network segment.
- Network-node IDS systems detect packets headed to a single network node.
- A desktop IDS offers file-level protection. Rather than monitoring network traffic, it examines activity on individual systems, looking for potential attacks on files or registry entries on Windows PCs.
- The desktop IDS is also very useful in trojan horse detection.
- A honeypot is a system designed to be attacked, with the intent of deception or alerting of intrusion activity.
- Honeypots emulate known vulnerabilities, other systems, or are modified production systems that create "caged" environments.
- A honeynet is a network of production systems, residing behind a firewall, which is designed to be compromised. Once breached, the resulting information gathered during the attack is analyzed to learn about the tools, tactics, and motives of the possible intrusion.