Certified Professional Ethical Hacker

Exam Prep Guide

Edition: August 2014

Mile2™ IT Security Training

11928 Sheldon Road
Tampa, FL 33626
(813) 920-6799
(813) 354-2367 (fax)

www.mile2.com

Table of Contents

Introduction

The purpose of this book is to provide tindividuals with an introductory approach to penetration testing. This book will help individuals gain a valuable skill-set in penetration testing by understanding the importance of vulnerability assessments and ethical hacking. This book is solely prepared from the modules provided to students that take the Certified Professional Ethical Hacker Course.

The Certified Professional Ethical Hacker exam is taken on-line through Mile2's Assessment and Certification System, which is accessible with a Mile2 account. The C)PEH exam will take two hours and consist of 100 multiple choice questions.

Chapter 1: Security Fundamentals

Topics

- CIA Triad
- Security Definitions
- TCP/IP Basics
- Malware
- Network Devices and Sniffers
- Wireless Standards
- Database Basics

Background

The motivation for the Professional Ethical Hacker is the exponential rise in computer crime. Prevention is far more realistic than prosecution. Helping organizations secure themselves against security threats ultimately protects the lives and privacy of millions of people across the country. Following "9-11", anyone promoting information security is promoting national security against a growing army of cyber terrorist. Living in the "digital age" means that digital crime has a much larger fallout than localized street crimes. Apart from works of art, physical property that is stolen or vandalized can be quickly replaced by insurance funds. It is the loss of information, research data, design documents, social security numbers, account numbers, passwords, and medical records that poses the greatest threat to society today.

CIA Triad:

The classic CIA security triad presents three aspects of information to be guarded. Viewing ethical hacking and penetration testing from a high level, one might say that the ultimate goal of organizations requesting such services is to protect their information assets. Confidentiality is when only approved persons should have access to the data. Integrity is when only approved persons and processes should alter the data. Availability is when data must remain available when and where needed.

Confidentiality:

- Secrecy, sensitivity, privacy
- Prevents unauthorized disclosure of data
- Protects sensitive data and processes from things like:
  - Shoulder surfing
  - Social engineering

Integrity:

- Accuracy, completeness
- Prevents unauthorized modification
- Protects data and production environment from things like:
    - Modifying data or configurations
    - Changing security log information

Availability:

- Usability, timeliness
- Prevents disruption of services
- Protects production and productivity from things like:
    - Man-made, technical, or natural disaster
    - Failure of components or a device
    - Denial-ofservice attacks

A holistic approach must be taken to secure an organization and ensure the CIA of information assets. There is more to information security than firewalls and intrusion detection systems. You eventually find yourself as part of a well-defined or poorly defined security initiative of some organization. If necessary, you should encourage the organization to view security holistically rather than a one-time event, a box to be checked, or a technology-only concept.

Physical Security: Theft avoidance, locks, document shredding, limited access areas, guards, fire systems, HVAC, surveillance, and I.D. badges.

Operational Security: The largest aspect of securing an organization. Any and every behavior or process that affects the CIA of information, Access control, password selection, and backup plans.

Management Oversight of Security: only administration can give teeth to security policies. Only management can take a security policy off of paper and turn it into part of the organizational culture. This facet of security involves establishment of all policies that guide and promote security in the organization. Policies should deal with issues like disaster recovery, security, access, technology usage, accountability, chain of command, and contingency plan.

Security Definitions:

Vulnerability – Weakness in a mechanism that can threaten the confidentiality, integrity, or availability of an asset and lack of a countermeasure.

Threat – Someone uncovering a vulnerability and exploiting it.

Risk – Probability of a threat becoming real and the corresponding potential damages.

Exposure – When a threat agent exploits a vulnerability.

Countermeasures – A control put into place to mitigate potential losses.

The proper order in which to evaluate these concepts as they apply to your own network is threat, exposure, vulnerability, countermeasures, and finally risk. This is because there can be a threat (new SQL attack) but unless your company has the corresponding vulnerability (SQL server with the necessary configuration), then the company is not exposed and it is not a vulnerability. If the vulnerability does reside in the environment, then a countermeasure is applied to reduce the risk.

TCP/IP Basics

Basic network connectivity can be tested using the ping command. To determine the range of IP addresses mapped to a live host, Ping sends out ICMP Echo Request packets and if the address is live, an ICMP Echo Reply message will be received from an active machine. Alternatively, TCP or UDP packets can be sent if ICMP messages are blocked. TCP connections begin with your system sending a SYN packet to the server. The server responds with a SYN/ACK. Then your system responds with an ACK, and the connection is established.

TCP Flags:

- SYN – synchronize sequence number
- ACK – acknowledgement of sequence number
- FIN – final data bit is used during the 4-step teardown sequence
- RST – reset bit is used to close the connection without going through the 4-step teardown sequence
- PSH – push data bit is used to signify that the data in this packet should be put at the beginning of the queue of data to be processed
- URG – urgent data bit is used to signify that there is urgent control characters in this packet that needs to be processed immediately

Malware

There are several types of malicious code: viruses, worms, Trojan horses, and logic bombs. They usually are dormant until activated by an event the user or system initiates. They can be spread through using e-mail, sharing media (floppy disks), sharing documents and programs, or downloading things from the Internet, or they can be purposely inserted by an attacker. Adhering to the usual rule of not opening an e-mail attachment that comes from an unknown source is one of the best ways to combat malicious code. However, recent viruses and worms have infected personal e-mail address books, so this precaution is not a sure thing to protect systems from malicious code. If an address book is infected and used during an attack, the victim gets an e-mail message that seems to have come from a person he knows. Because he knows this person, he will proceed to open the email message and double-click the attachment. Bam! His address book is now infected, and his system just spread the virus to all his friends and acquaintances. Antivirus software should be installed to watch for known virus signatures, and host intrusion detection software can be used to watch for suspicious activity, file access, and changes to help detect evildoers and their malicious activity.

Malicious code can be detected through the following clues:

- File size increase
- Many unexpected disk accesses
- Change in update or modified timestamp
- Sudden decrease of hard drive space
- Unexpected and strange activity by applications

Types of Malware:

- Worms – Can reproduce on their own – different to virus and self-contained programs
- Logic Bomb – An event triggers the execution of specific code
- Trojan Horse – Program disguised as another program and useful program that contains hidden code exploiting the authorization process, enabling it to violate security

A virus is a small application, or string of code, that infects applications. Fred Cohen wrote the first virus in 1983 to demonstrate the concept because so many people did not believe it was possible. The main function of a virus is to reproduce, and it requires a host application to be able to do this. In other words, viruses cannot replicate on their own. A virus infects files by inserting or attaching a copy of itself to the file. The virus may also cause destruction by deleting system files, displaying graphics, reconfiguring systems, or overwhelming mail servers. Several viruses have been released that achieved self-perpetuation by mailing themselves to every entry in a victim's personal address book.

The virus masqueraded as coming from a trusted source. The ILOVEYOU, Melissa, and Naked Wife viruses used the programs Outlook and Outlook Express as their host applications and were replicated when the victim chose to open the message. Macros are programs written in Word Basic, Visual Basic, or VBScript and are usually used with Microsoft Office products. Macros automate tasks that users would otherwise have to carry out themselves. Users can define a series of activities and common tasks for the application to perform when a button is clicked, instead of doing each of those tasks individually.

Types of Viruses:

- Macro virus is easy to create because of the simplicity of the macro language
- Boot sector virus is malicious code inserted into the disk boot sector
- Compression virus initializes when it is decompressed
- Stealth virus hides its footprints and the changes it has made
- Polymorphic virus makes copies and then changes those copies in some way – uses a mutation engine
- Multipartite virus infects both boot sector and file system
- Self-garbling virus modifies own code to elude detection

More Malware: Spyware

Spyware is software or hardware installed on a computer, which gathers information about that user for later retrieval by whoever controls the spyware. This software is installed without the user's knowledge. Spyware can be broken down into two different categories, surveillance spyware and advertising spyware. Surveillance software includes key loggers, screen capture devices and Trojans. Large companies often use surveillance software to monitor employee computer usage.

A Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. The term comes from a Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Backdoors:

- Accessing a system by bypassing the access controls
- Allows attacker to enter the computer at any time
- Can be inserted by a Trojan horse
- Maintenance hook
    - Instructions in software that allow for easy access and maintenance
    - Allows entry to code at specific points without security checks

    - Usually accessed through a certain key sequence
    - Should be removed before deployment of software

Denial of Service:

A denial-of-service attack is tying up resources on a computer so it cannot respond to valid requests. It can be distributed and amplified by using other systems to commit the attack. The network stack is a portion of the operating system that enables devices to communicate over the network. This is where packets are built and sent over the wire and where packets are received and processed. Different operating systems and vendors interpret the Request for Comments (RFCs) for networking protocols differently, which end up in slightly different network stacks. These differences can contain their own flaws that can be taken advantage of to produce a denial-of-service attack. These attacks can be performed by sending malformed packets to a system, and because the system does not recognize the format, it does not know how to properly process it. This can cause the system to crash or stop processing other packets (denial of service).

A distributed denial-of-service attack is a logical extension of the denial-of-service that gets more computers involved in the act. The denial-of-service attacks overwhelm computers by one computer sending bad packets or continually requesting services until the system's resources are all tied up and cannot honor any further requests. The distributed denial-of-service uses hundreds or thousands of computers to request services from a server or server farm until the system or Web site is no longer functional.

Network Devices and Sniffers

A packet sniffer can intercept packets on a LAN. In its simplest form, as data streams flow over a network, the sniffer captures each packet and eventually decodes and analyzes its content. A packet sniffer is also called a network monitor, network analyzer, wireless sniffer, Ethernet sniffer, or protocol analyzer. Sniffers can be used for legitimate network management functions by system administrators to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer, an administrator can identify problem packets, pinpoint bottlenecks, and help maintain efficient network data transmission.

Passive sniffing is sniffing traffic through a hub without having to inject packets. Passive sniffing is basically connecting up to a network hub and starting a sniffer. Active sniffing is sniffing traffic on a local LAN, but in order to do that, packets must be injected that cause data to be rerouted to the sniffing machine. Active sniffing occurs on LANs that have switches connecting the computers.

Firewalls, IDS and IPS

A firewall is considered the first line of defense. The intent ofthe firewall is to provide access control by denying specific traffic. By denying the traffiic, it can in turn, deny some attacks. However, the firewall has to allow some traffic to the network or the individual user will not be able to access the Internet. An IDS is considered the second line of defense. The IDS will detect an attack on the system and will provide attack monitoring, however, it is unable to stop the attack. An IPS is considered the last line of defense. This system has the ability to shutdown in case of an attack.

Packet filtering firewalls are first generation firewalls that only look at the header information contained in a packet when making routing decisions. These types of devices have limited security capabilities because they cannot look deep into a packet to gain more information about it. Unlike stateful firewalls that keep track of the state of a connection, packet-filtering firewalls are one-dimensional. This type of functionality is built on the use of access control lists (ACL), which is built into most routers.

Proxy firewalls are placed between trusted and untrusted networks to provide an additional layer of security. In addition to simply acting as a buffer, proxy firewalls impersonate the destination computer by receiving the packet to ensure that it is safe before passing it on to the far-end device. The same is true on the return message. When the user from the trusted network replies to the untrusted user, the proxy firewall intercepts the message, scans it, repackages the packet with its own source address, and then forwards it on the destination. This is done so that the untrusted user cannot gain valuable addressing information from inside the network. Proxy firewalls ensure that there is never a direct connection between untrusted and trusted resources.

A circuit-level proxy is similar to a packet filter firewall as it makes routing decisions based solely on header information contained in the packet. However, it is different because it creates a virtual connection between the client and the server. The proxy protects internal resources by changing packet information so that external devices will not learn of the specific address of inside devices. Instead, the proxy inserts its source address into packet information and "acts" like the internal device.

Application-gateway firewalls receive connections from clients, dropping some and accepting others, but always creating a new connection with whatever restrictions exist whenever a connection is accepted. Although, in theory, this process should be transparent to users, in reality the transparency is less than ideal. A third type of firewall, the circuit-gateway firewall, has been designed to remedy this limitation by producing a more "seamless," transparent connection between clients and destinations using routines in special libraries. The connection is often described as a virtual circuit because the proxy creates an end-to-end connection between the client and the destination application. A circuit-gateway firewall is also advantageous in that rather than simply relaying packets by creating a second connection for each allowed incoming connection, it allows multiple clients to connect to multiple applications within an internal network.

Application-level proxies inspect the entire packet and make access decisions based on the content of the packet. They understand various services and protocols and the commands that are used by them. An application-level proxy can distinguish between an FTP GET command and an FTP PUT command, for example, and make access decisions based on this granular level of information; on the other hand, packet-filtering firewalls can allow or deny FTP requests only as a whole, not by the commands used within the FTP protocol. An application-level proxy works for one service or protocol. A computer can have many types of services and protocols (FTP, NTP, SMTP, Telnet, and so on)—thus, one application-level proxy per service is required. This does not mean that one proxy firewall per service is required, but rather that one portion of the firewall product is dedicated to understanding how a specific protocol works and how to properly filter it for suspicious data.

A circuit-level proxy creates a circuit between the client computer and the server and provides protection at the session layer. It does not understand or care about the higher level issues that an application-level proxy deals with. It knows the source and destination addresses and makes access decisions based on this type of header information. Providing application-level proxy services can be a tricky undertaking. The proxy must totally understand how specific protocols work and what commands within that protocol are legitimate. This is a lot to know and look at during the transmission of data. As an analogy, picture a screening station at an airport that is made up of many employees, all with the job of interviewing people before they are allowed into the airport and onto an airplane.

A stateful firewall – A third generation firewall that keeps track of each communication session by using a state table. State tables exist to record each and every step a device takes to establish communications. A stateful firewall only allows packets in that are responding to an internal device. A highly secure firewall solution, stateful inspection examines the bit patterns of packets and compares them with packets that have already been determined to be trusted. The biggest downside to stateful firewalls is that internal systems are exposed to the external (untrusted) network. This means that an internal device could give up its IP address to an external address. Note: Network Address Resolution (NAT) is a possible countermeasure.

Internal systems that want to communicate with an external system must establish a valid source port that the external entity can use when sending a response. Ports 0 – 1024 are reserved for "well-known" services, so the internal system chooses a port higher than 1024. Next, a dynamic packet filtering firewall comes into play. It creates an ACL with the chosen port so that the outside user's response will be allowed into the network. Dynamic packet filtering is the alternative to using "punch holes" in firewalls.

A kernel proxy firewall is considered a fifth-generation firewall. It differs from all the previously discussed firewall technologies because it creates dynamic, customized TCP/IP stacks when a packet needs to be evaluated. When a packet arrives at a kernel proxy firewall, a new virtual network stack is created, which is made up of only the protocol proxies that are necessary to examine this specific packet properly. If it is an FTP packet, only the FTP proxy is loaded in the stack. The packet is scrutinized at every layer of the stack, not just at the data payload. This means the data link header will be evaluated along with the network header, transport header, session layer information, and the application layer data. If anything is deemed unsafe at any one of these layers, the packet is discarded. Kernel proxy firewalls are faster than application layer proxy firewalls because all of the inspection and processing takes place in the kernel and does not need to be passed up to a higher software layer in the operating system. It is still a proxy-based system, so the connection between the internal and external entity is broken by the proxy acting as a middleman. It can perform NAT by changing the source address, as do the preceding proxy-based firewalls. Although various firewall products can provide a mix of these services and work at different layers of the OSI model, it is important that you understand the basic definitions and functionalities of these firewall types.

A screened host is a firewall that communicates directly with a perimeter router and the internal network. Traffic that is received from the Internet is first filtered via packet filtering on the outer router. The traffic that makes it past this phase is sent to the screened-host firewall, which applies more rules to the traffic and drops the denied packets. Then the traffic moves to the internal destination hosts. The screened host (the firewall) is the only device that receives traffic directly from the router. No traffic goes directly from the Internet, through the router, and to the internal network. The screened host is always part of this equation. If the firewall is an application-based system, protection is provided at the network layer by the router and at the application layer by the proxy. This arrangement offers a high degree of security because for an attacker to be successful, she would have to compromise two systems. What does the word-screening mean in this context? This just means that there is a layer that scans the traffic and gets rid of a lot of the "junk" before it is directed toward the firewall. A screened host is different from a screened subnet, which will be described soon.

Dual-homed refers to a device that has two interfaces: one facing the external network and the other facing the internal network. If firewall software is installed on a dual-homed device, and it usually is, the underlining operating system should have packet forwarding and routing turned off, for security reasons. If they are enabled, the computer will not apply the necessary ACLs, rules, or other restrictions required of a firewall. When a packet comes to the external NIC from the untrusted network on a dual-homed firewall, and the operating system has forwarding enabled, the operating system will forward the traffic instead of passing it up to the firewall software for inspection. Many network devices today are multi-homed, which just means that they have several NICs that are used to connect several different networks. Multi-homed devices are commonly used to house firewall software, since the job of a firewall is to control the traffic as it goes from one network to another. A common multi-homed firewall architecture allows a company to have several DMZs, as described earlier. One DMZ may hold devices that are shared between companies in an extranet, another DMZ may house the company's DNS and mail servers, and yet another DMZ may hold the company's web servers. Different DMZs are used for two reasons: to control the different traffic types (for example, make sure that HTTP traffic only goes toward the web servers and DNS requests go toward the DNS server) and to ensure that if one system on one DMZ is compromised, the other systems in the rest of the DMZs are not accessible to this attacker.

A screened-subnet architecture adds another layer of security to the screened-host architecture. It applies packet filtering to data entering the network and ports the traffic to the firewall. However, instead of the firewall then redirecting the traffic to the internal network, an interior router also filters the traffic. The use of these two physical firewalls creates a DMZ.

Wireless Standards

Some Wi-Fi network types are peer-to-peer/ad-hoc network. This allows for no central point of communications, no central management interface; all devices transmit to all devices and are easy to setup. Infrastructure mode has a central point of configuration/management, more secure (WEP/WPA/EAP) and devices still transmit in all directions.

Widely Deployed Standards:

- 802.11a – Data rates of 54 Mbps in the 5 GHz Unified National Information Infrastructure band.
- 802.11b – The most well-known and widely deployed standard that implements data rates of 11 Mbps in the 2.4 GHz Industrial, scientific, and medical band.
- 802.11g – Processor uses all the same technologies as 802.11a and is backwards compatible with 802.11b. Similar to 802.11b, 802.11g operates in the 2.4 GHz band at 54 Mbps speed.

MIMO stands for multiple-input | multiple-output; the use of multiple antennas to increase throughput and/or reduce bit error rates. MIMO can be split into three categories: Pre-coding – Used to increase the signal gain; Spatial Multiplexing – This technique is used for increasing channel capacity at higher Signal to Noise Ratio (SNR); Diversity Coding – Used to enhance signal diversity.

Database Basics

A database is a collection of information or data that is stored in a computer system usually organized by files, records, and fields. A database management system is a collection of programs designed to let you enter, organize and select data in the database. There are different types of databases: relational, network, flat, and hierarchal all refer to the way a database management system organizes information internally.

Overview of Database Servers:

- Tables – A collection of data or data structures linked through relations, tables are constructed of columns and rows
- Record Set – A record set is the requested data, a subset of the entire row
- Attributes – The data type a field can contain. Currency, Date, characters, etc
- Domain – A set of allowable values that an attribute can take i.e. currency field can allow $ and other currency characters.

- Data normalization – A process that database designers go through to eliminate redundant data, repeating groups and attributes.
- SQL – Data manipulation and relational database definition language, all SQL database systems use a core structure of SQL, vendors then have a subset proprietary to their own server, and common commands.

Questions and Answers

1. A ________ modifies its own code to elude detection.

   a. Compression virus
   b. Boot sector virus
   c. Stealth virus
   d. Self-garbing virus

Answer: D

Module 01: A self-garbing virus modifies own code to elude detection.

2. ________: A process that database designers go through to eliminate redundant data, repeating groups and attributes.

   a. Data normalization
   b. SQL

Answer: A

Module 01: Data normalization is a process that database designers go through to eliminate redundant data, repeating groups and attributes.

3. ________: Data manipulation and relational database definition language.

a. Data normalization
b. SQL

Answer: B

Module 01: SQL is data manipulation and relational database definition language.

4. ________ stands for push data bit used to signify that data in this packet should be put at the beginning of the queue of data to be processed.

a. ACK
b. FIN
c. URG
d. PSH

Answer: D

Module 01: PSH stands for push data bit used to signify that data in this packet should be put at the beginning of the queue of data to be processed.

5. A ________ can reproduce on their own which is different from viruses and self-contained programs.

a. Worms
b. Logic Bomb
c. Trojan Horse

Answer: A

Module 01: A worm can reproduce on their own which is different from viruses and self-contained programs.

Chapter 2: Access Controls

Topics

- Access Controls Defined
- Categories of Access Controls
- Physical Access Controls and Devices
- Logical Access Controls

Background

A cornerstone in the foundation of information security is to control how resources are accessed so that they can be protected from unauthorized modification or disclosure. The controls that enforce access control can be technical, physical, or administrative in nature.

Access controls are security features that control how users and systems communicate and interact with other systems and resources. They protect the systems and resources from unauthorized access and can be a component that participates in determining the level of authorization after an authentication procedure has successfully completed. Although we usually think of a user as the entity that requires access to a network resource or information, there are many other types of entities that require access to other network entities and resources that are subject to access control. It is important to understand the definition of a subject and an object (see other slides) when working in the context of access control.

Access control is a broad term that covers several different types of mechanisms that enforce access control features on computer systems, networks, and information. Access control is extremely important because it is one of the first lines of defense used to fight against unauthorized access to systems and network resources.

When a user is prompted for a username and password to be able to use a computer, this is access control. Once the user logs in and later attempts to access a file, that file may have a list of users and groups that have the right to access it. If the user is not on this list, the user is denied. This is another form of access control. The users' permissions and rights may be based on their identity, clearance, and/or group membership.

Access Controls Defined

Access would be considered physically reaching a restricted area of a facility. More specifically, access is the term used for when data begins to flow from an object to a subject.

A ***subject*** is a working unit that asks for access to an object or the data within an object. A subject can be a human, a program, or a process that accesses an object to complete a task. For example, when a program opens a file, the program is the subject and the file is the object.

An ***object*** is a passive unit that holds information. A room, computer, database, file, computer program, directory, or field contained in a table within a database can all be considered as an object. When you look up information in a database, you are the active subject and the database is the passive object.

Security elements that control how users and systems communicate and interact with other systems and resources would be considered ***access controls***. After a successful authentication procedure, access controls keep unauthorized access to systems and resources and help determine the level of authorization.

Access control is not limited to only a user requiring access to a network or information. There are many other things that can require access to other network entities and resources that can be subject to access control as well.

Access privileges are permissions defining the extent of access a subject has to an object and defining circumstances in which these permissions can be used. Access rules are statements specifying subject's access rights, enforcement of security policies and business objectives, collectively referred to as user profiles, and enforced through software. Access path is a path that a request travels through, it can be through different layers of software and mechanisms that can be bypassed in layers should also be seen as part of the path.

Categories of Access Controls

Physical:

- Doors and Locks
- Removal of floppy and CD-R●M drives
- Security guards controlling access to facility and equipment
- Computer chassis locks

Technical (logical):

- Encryption
- Passwords and tokens
- Biometrics
- Operating system and application controls
- Identification and authorization technologies

Administrative:

- Policies and procedures
- Security awareness training
- Quality assurance

Physical Controls:

The tightest firewalls and the longest passwords are of no use against an intruder who is able to access a server physically rather than hacking into the network. Physical controls are a major part of access controls and go into creating a more holistic approach to security, introduced earlier.

An intrinsic, and ancient aspect of access control are physical barriers; ideally several barriers. Each barrier, separating a "subject" from a physical "object" (i.e. a server room), should have some form of security restricting access past the barrier to only approved "subjects."

Often facilities can be partitioned into various zones. Zones help security personnel bring more granular access control to specific areas of a facility. Zones also help alert administrators to specific security breaches so that time is not wasted on an entire facility in the event of a breach.

Logical Controls:

Technical controls, also called logical controls, are the software tools used to restrict subjects' access to objects. They are core components of operating systems, add-on security packages, applications, network hardware devices, protocols, and access control matrixes. These controls work at different layers within a network or system and need to maintain a synergistic relationship to ensure that there is no unauthorized access to resources and that the resources' availability, integrity, and confidentiality are guaranteed. Technical controls protect the integrity and availability of resources by limiting the number of subjects that can access them and protect the confidentiality by preventing disclosure to unauthorized subjects. The following sections explain how some technical controls work and where they are implemented within an environment.

Administrative Controls:

- Policies, procedures, standards, and guidelines
- Employee management
- Testing and drills
- Risk management and analysis
- Information classification
- Awareness training

Security Roles:

Data owner – A person who is ultimately responsible for the protection and use of data or specific piece of information. This involves classifying the data to determine who and what can access it, and involves delegating who is in charge of maintaining the mechanisms that protect it. The foundation of a data owner's responsibility is the basis of the due care/due diligence concept. Because of this responsibility, the role should fall on the shoulders of a senior manager/executive.

Data Custodian – The person responsible for maintaining and protecting the data. Typically, this function is fulfilled by an IT professional or group as it falls within their normal job description and skill set. Tasks of a data custodian include: performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the company's security policy, standards, and guidelines that pertain to information security and data protection. Data custodians work to ensure data confidentiality, integrity, and availability.

Each level of employee within a company has a specific responsibility that is tied to the security program. These responsibilities are detailed below:

Senior manager – Ultimately responsible for ensuring a thorough security program, which includes the protection of its assets.

Security professional – Carries out senior manager's directives and is functionally responsible for the security program.

User – Performs day-to-day tasks that support the overall security program.

Access Criteria:

There are three steps to granting access; they are authorization, authentication and identification. When granting access to a location or computer system, you will want to ensure they have a security clearance that meets the guidelines for access. Does the individual have a need-to-know for the specific information being shared? Make sure that you provide the individual with the least amount of rights possible to ensure they are only accessing the data they are allowed to view. In the end, you will want to default to no access if the individual cannot prove the type of access needed to conduct the mission.

Physical Access Control Mechanisms

The following list is mechanisms with examples for physical access controls:

- Biometrics – Retina scan, Fingerprint, Voice Print
- Token Devices – Synchronous and Asynchronous Devices
- Memory Cards – ATM cards, Proximity card
- Smart Cards – Credit Cards, Identification Card
- Cryptographic Keys – Private Key

Biometric System Types:

- Fingerprint – Ridge endings and Bifurcations – Minutiae
- Finger Scan – Same as Fingerprint but extracting a smaller amount of Data
- Palm Scan – All prints from Fingers and Creases, Ridges and Grooves from the Palm
- Hand Geometry – Shape of (length and width) Hand and Fingers
- Retina Scan – Blood vessel pattern of Retina on back of eyeball
- Iris Scan – Colored portion of eye that surrounds the pupil
- Signature Dynamics – Captures Electrical signals of signature process
- Keyboard Dynamics - Captures Electrical signals of typing process
- Voice Print – Distinguishes differences in sounds, frequencies and patterns
- Facial Scan – Bone structure, nose ridges, forehead size and eye width
- Hand Topology – Side-view of hand, reviewing size and width

Synchronous Token:

A synchronous token device synchronizes with the authentication service by using time or a counter as the core piece of the authentication process. If the synchronization is time based, the token device and the authentication service must hold the same time within their internal clocks. The time value on the token device and a secret key are used to create the one-time password, which is displayed to the user. The user enters this value and a user ID into the computer, which then passes them to the server running the authentication service. The authentication service decrypts this value and compares it to the value that it expected. If the two match, the user is authenticated and allowed to use the computer and resources. If the token device and authentication service use counter-synchronization, the user will need to initiate the logon sequence on the computer and push a button on the token device. This causes the token device and the authentication service to advance to the next authentication value. This value and a base secret are hashed and displayed to the user. The user enters this resulting value along with a user ID to be authenticated. In either time- or counter-based synchronization, the token device and authentication service must share the same secret base key used for encryption and decryption.

Asynchronous Token:

A token device that is using an asynchronous token-generating method uses a challenge/response scheme to authenticate the user. In this situation, the authentication server sends the user a challenge, a random value also called a nonce. The user enters this random value into the token device, which encrypts it and returns a value that the user uses as a one-time password. The user sends this value, along with a username, to the authentication server. If the authentication server can decrypt the value and it is the same challenge value that was sent earlier, the user is authenticated. Both token systems can fall prey to masquerading if a user shares his identification information (ID or username) and the token device is shared or stolen. The token device can also have battery failure or other malfunctions that would stand in the way of a successful authentication. However, this type of system is not vulnerable to electronic eavesdropping, sniffing, or password guessing. If the user has to enter a password or PIN into the token device before it provides a one-time password, then strong authentication is in effect because it is using two factors —something the user knows (PIN) and something the user has (the token device).

Memory Cards:

The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information. A memory card can hold a user's authentication information, so that the user only needs to type in a user ID or PIN and present the memory card, and if the data that the user entered matches the data on the memory card, the user is successfully authenticated. If the user presents a PIN value, then this is an example of two-factor authentication— something the user knows, and something the user has. A memory card can also hold identification data that is pulled from the memory card by a reader. It travels with the PIN to a back-end authentication server. An example of a memory card is a swipe card that must be used for an individual to be able to enter a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building. Another example is an ATM card.

If Buffy wants to withdraw $40 from her checking account, she needs to enter the correct PIN and slide the ATM card (or memory card) through the reader. Memory cards can be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed per computer, and card generation adds additional cost and effort to the whole authentication process. Using a memory card provides a more secure authentication method than using a password because the attacker would need to obtain the card and know the correct PIN. Administrators and management need to weigh the costs and benefits of a memory token-based card implementation to determine if it is the right authentication mechanism for their environment.

Smart Card:

- Microprocessor and integrated circuits
    - Holds and processes data
- Tamperproof device
    - After a threshold of failed login attempts, it can render itself unusable
- PIN or password "unlocks" smart card functionality
- Smart card could be used for:
    - Holding biometric data in template

    - Responding to challenge
    - Holding private key
    - Holding user work history, medical information, and money
- Added cost compared to other authentication technologies
    - Reader purchase
    - Card generation and maintenance

Cryptographic Keys:

Another way to prove one's identity is to use a private key or generate a digital signature. A private key or digital signature could be used in place of using a password. Passwords are the weakest form of authentication and can be easily sniffed as they travel over a network. Private keys and digital signatures are forms of authentication used in environments that require higher security protection than what is provided by passwords. A private key is a secret value that should be in the possession of one person, and one person only. It should never be disclosed to an outside party.

A digital signature is a technology that uses a private key to encrypt a hash value (message digest). The act of encrypting this hash value with a private key is called digitally signing a message. A digital signature attached to a message proves that the message originated from a specific source, and that the message itself was not changed while in transit. A public key can be made available to anyone without compromising the associated private key; this is why it is called a public key. We explore private keys, public keys, digital signatures, and public key infrastructure, but for now, understand that a private key and digital signatures are other mechanisms that can be used to authenticate an individual.

Logical Access Controls

The following list is mechanisms with examples for logical access controls:

- Application Level – Shopping cart, CMS driven site, and the level at which the user interfaces
- Middleware Level – Database and it works between the Operating System and Application level
- Operating System Level – Linux and Windows
- Hardware Level – Devices

Some features that can be used at the operating system level to deny access are creating groups for each work role or project, assigning specific roles to individual users, and using access control list to block access to certain files and folders.

Accounts and Groups (Linux Only):

- Accounts are created and managed using the password file located in /etc/passwd
- Each line contains the information for one account
- You can add a user by simply typing **adduser** and follow the prompts
- You can change a password by typing **passwd [username]**
- It is world readable so to encrypt our passwords we use the shadow format, it places an x where the password would be in the passwd file and places the password in the shadow file

Linux and UNIX Permissions:

Every file has permissions. Every file has an owner and an owner group. The root user and the owner can access the file. There are three different areas: owner, group owner and everyone else. There are three different levels of permission: read, write and execute. This allows for nine standard forms of permissions. You can look at the permissions of all the files in a given directory by running the Linux/UNIX **ls -l** command.

There are 10 characters when it comes to discussing file permissions. If the first character is a d, then it is a directory, otherwise it is a file. The next nine characters are the file permissions. The first group of three covers the owner and in most cases the owner can perform all levels of access. The second group covers the owner group. The third group covers the all others or everyone account. If there is a "-", then access is not allowed for that particular permission.

Set UID Programs:

If the SetUID program is configured to always execute with the permissions of its owner, this allows for a user to have access to change his password without root level access. You can find all programs whose SetUID is set to run as root by typing the following command: **find / -uid 0 -perm -4000 -print**.

Trust Relationships:

A trust relationship is created when one user trusts another user on the system. This trust can be implemented using the system wide /etc/host.equiv file or individual users' .rhosts files. When using rhosts, you also need to use the UNIX tools called r-commands.

- rlogin – A remote interactive command shell
- rsh – A remote shell to execute one command
- rcp – A remote copy command

The /etc/hosts.equiv file contains a list of machine names or IP addresses that the system will trust. The user can create the .rhosts file in your home directory setting up trust with other machines.

Questions and Answers

1. ________ are shopping carts, CMS driven sites, and the level at which the user interfaces.

   a. Application Levels
   b. Middleware Levels
   c. Operating System Levels
   d. Hardware Levels

Answer: A

Module 02: Application Levels are shopping carts, CMS driven sites, and the level at which the user interfaces.

2. ________ are database and work between the Operating system and Application level.

   a. Application Levels
   b. Middleware Levels
   c. Operating System Levels
   d. Hardware Levels

Answer: B

Module 02: Middleware levels are database and it works between the Operating system and Application level.

3. ________ are Linux and Windows.

  a. Application Levels
  b. Middleware Levels
  c. Operating System Levels
  d. Hardware Levels

Answer: C

Module 02: Operating System levels are Linux and Windows.

4. True or False. Users peform day-to-day tasks that support the overall security program.

a. True
b. False

Answer: A

Module 02: Users preform day-to-day tasks that support the overall security program.

5. ________ are retina scan, fingerprint and voice print.

a. Biometrics
b. Token Devices
c. Memory Cards
d. Smart Cards

Answer: A

Module 02: Biometrics are retina scan, fingerprint and voice print.

Chapter 3: Protocols

Topics

- OSI Model
- TCP/IP Suite
- UDP versus TCP
- ARP
- ICMP
- DNS
- SSH
- SNMP
- SMTP

Background

Protocols make it possible for a computer to communicate over the network. A *protocol* is the special set of rules that end points in a telecommunication connection use when they communicate. Network development proved to be difficult as companies had created their own proprietary protocols, which meant the computers did not interact with each other. In the 1980s, the International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) model to eliminate the problem of communications. As a penetration tester it is important to understand all of the technologies in computer communications. Additionally, you should know the basis of secure network architecture and design is a thorough knowledge of the OSI and Transmission Control Protocol/Internet Protocol (TCP/IP) models as well as IP networking in general.

OSI Model

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

Application Layer:

The application layer, layer 7, works closest to the user and provides file transmissions, message exchanges, terminal sessions, and much more. This layer does not include the actual applications but includes the protocols that support the applications. When an application needs to send data over the network, it passes instructions and the data to the protocols that support it at the application layer. This layer processes and properly formats the data and passes it down to the next layer within the OSI model. This happens until the data that the application layer constructed contains the essential information from each layer necessary to transmit data over the network.

The data is then put on the network cable and is transmitted until it arrives at the destination computer. Some examples of the protocols working at this layer are the Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), Line Printer Daemon (LPD), File Transfer Protocol (FTP), Telnet, and Trivial File Transfer Protocol (TFTP). If a user makes a request to send an e-mail message through her e-mail client Outlook, the e-mail client sends this information to SMTP. SMTP adds its information to the user's information and passes it down to the presentation layer.

Presentation Layer:

The presentation layer, layer 6, receives information from the application layer protocols and puts it in a format that all computers following the OSI model can understand. This layer provides a common means of representing data in a structure that can be properly processed by the end system. This means that when a user constructs a Word document and sends it out to several people, it does not matter whether the receiving computer has different word processing programs; each of these computers will be able to receive this file and understand and present it to its user as a document. It is the data representation processing that is done at the presentation layer that enables this to take place.

For example, when a Windows XP computer receives a file from another computer system, information within the file's header explains what type of file it is. The Windows XP operating system has a list of file types it understands and a table Applications send requests to an API, which is the interface to the supporting protocol, describing what program should be used to open and manipulate each of these file types. For example, the sender could create a Word file in Word 2000, while the receiver uses Open Office. The receiver can open this file because the presentation layer on the sender's system converted the file to American Standard Code for Information Interchange (ASCII), and the receiver's computer knows that it opens these types of files with its word processor, Open Office.

The presentation layer is not concerned with the meaning of data, but with the syntax and format of that data. It works as a translator, translating the format an application is using to a standard format used for passing messages over a network. If a user uses a Corel application to save a graphic, for example, the graphic could be a Tagged Image File Format (TIFF), Graphic Interchange Format (GIF), or Joint Photographic Experts Group (JPEG) format.

Session Layer:

When two applications need to communicate, or transfer information, a connection session may need to be set up between them. The session layer, layer 5, is responsible for establishing a connection between the two applications, maintaining it during the transfer of data, and controlling the release of this connection. A good analogy for the functionality within this layer is a telephone conversation. When the presentation layer receives data from the application layer and puts it into a standard format. The telephone network circuitry and protocols set up the connection over the telephone lines and maintains that communication path, and when Kandy hangs up, it releases all the resources it was using to keep that connection open.

Similar to how telephone circuitry works, the session layer works in three phases: connection establishment, data transfer, and connection release. It provides session restart and recovery, if necessary, and provides the overall maintenance of the session. When the conversation is over, this path is broken down and all parameters are set back to their original settings. This process is known as dialog management. Some protocols that work at this layer are Network File System (NFS), Structured Query Language (SQL), NetBI●S, and remote procedure call (RPC). The session layer protocol can enable communication between two applications to happen in three different modes.

Transport Layer:

When two computers are going to communicate through a connection-oriented protocol, they will first agree on how much information each computer will send at a time, how to verify the integrity of the data once it is received, and how to determine whether a packet was lost along the way. The two computers agree on these parameters through a handshaking process at the transport layer, layer 4.

The agreement on these issues before transferring data helps provide more reliable data transfer, error detection, correction, recovery, and flow control, and it optimizes the network services needed to perform these tasks. The transport layer provides end-to-end data transport services and establishes the logical connection between two communicating computers.

Network Layer:

The main responsibilities of the network layer, layer 3, are to insert information into the packet's header so that it can be properly addressed and routed, and then to actually route the packets to their proper destination. In a network, many routes can lead to one destination. The protocols at the network layer must determine the best path for the packet to take. Routing protocols build and maintain their routing tables at this layer. These tables are maps of the network, and when a packet needs to be sent from computer A to computer M, the protocols check the routing table, add the necessary information to the packet's header, and send it on its way.

The protocols that work at this layer do not ensure the delivery of the packets. They depend on the protocols at the transport layer to catch any problems and resend packets, if necessary. IP is a common protocol working at the network layer, although other routing and routed protocols work there, as well. Some of the other protocols are the Internet Control Message Protocol (ICMP), Routing Information

Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Internet Group Management Protocol (IGMP).

Data Link Layer:

As we continue down the protocol stack, we are getting closer to the actual network wire over which all this data will travel. The outer format of the data packet changes slightly at each layer, and it comes to a point where it needs to be translated into local area network (LAN) or wide area network (WAN) technology binary format for proper line transmission. This happens at the data link layer.

Physical Layer:

The physical layer, layer 1, converts bits into voltage for transmission. Signals and voltage schemes have different meanings for different LAN and WAN technologies. If a user sends data through his dial-up software and out his modem onto a telephone line, the data format, electrical signals, and control functionality are much different than if that user sends data through the NIC and onto a unshielded twisted pair (UTP) wire for LAN communication.

The mechanisms that control this data going onto the telephone line, or the UTP wire, work at the physical layer. This layer controls synchronization, data rates, line noise, and medium access. Specifications for the physical layer include the timing of voltage changes, voltage levels, and the physical connectors for electrical, optical, and mechanical transmission.

Protocols at each OSI Model Layer

- Application – DNS; FTP; TFTP; BOOTP; SNMP; RLOGIN; SMTP; TELNET; HTTP
- Presentation – ASCII; TIFF; GIF; JPEG; MPEG; MIDI; MIME
- Session – NetBIOS; NFS; SQL; RPC
- Transport – TCP; UDP; SPX; SSL
- Network – IP; ICMP; RIP; IGMP; IPX
- Data Link – SLIP; PPP; ARP; RARP; L2F; L2TP
- Physical – High-speed Serial Interface (HSSI); X.21; EIA/TIA-232 and EIA/TIA-449

TCP/IP Suite

Transmission Control Protocol/Internet Protocol (TCP/IP) – A suite of protocols that dictates the way data travels from one device to another. The two main components of the suite are TCP and IP.

A connectionless protocol, IP works within the network layer and has the primary purposes of inter-network addressing and data routing. IP receives data from the transport layer and addresses the packet with the source and destination information.

The TCP/IP protocols work together to process data and pass it from one layer to another. The whole process involves breaking data into forms that each layer can read and understand so that it can be successfully delivered to its destination computer.

TCP/IP Layers:

- Application Layer – The top layer that includes the applications services that run on the network
- Transport Layer – The layer that handles the end-to-end data delivery; also referred to as the host-t o-host layer
- Internet Layer – Layer that provides logical addressing and data routing
- Network Layer – Bottom layer that maps loosely to the data link and physical layers of the OSI model

Port and Protocol Relationships:

In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are pre- assigned to them by the IANA, and these are known as well-known ports (specified in RFC 1700}. Port numbers range from 0 to 65536, but only ports numbers 0 to 1023 are reserved for privileged services and designated as well-known ports. This list of well-known port numbers specifies the port used by the server process as its contact port.

TCP and UDP services generally have a client-server relationship. For example, a TELNET server process initially sits idle at a system, waiting for an incoming connection. A user then interacts with a TELNET client process, which initiates a connection with the TELNET server. The client writes to the server, the server reads from the client and sends back its response. The client reads the response and reports back to the user. Thus, the connection is bidirectional and can be used for reading and writing.

The port is a software construct that is used by the client or server for sending or receiving messages; a port is identified by a 16-bit number. Server processes are usually associated with a fixed port, e.g., 25 for SMTP or 6000 for X Windows; the port number is 'well-known' because it, along with the destination IP address, needs to be used when initiating a connection to a particular host and service. Client processes, on the other hand, request a port number from the operating system when they begin execution; the port number is random although in some cases it is the next available port number.

UDP versus TCP

Transport layer protocols within TCP/IP:

- Transmission Control Protocol (TCP) – Reliable, connection-oriented data transfer
- User Datagram Protocol (UDP) – Unreliable, connectionless data transfer

TCP provides end-to-end communications between host systems by completing something called the "TCP three-way handshake". This is the process of synchronizing with the far-end and waiting for an acknowledgement before beginning the data transfer. This connection-oriented handshake ensures reliability. Once the data transfer begins, TCP periodically checks in on the process to make sure it is being delivered properly. This procedure is called windowing.

The other way to transfer data is UDP. This protocol does not establish any connection with the far-end and does no monitoring to see if the message was actually delivered. UDP is used in instances where the receipt of the data is not critical and when low overhead is required. Because there is no synchronization or acknowledgement, UDP requires very little overhead to operate.

ARP

In order for one system to communicate with another, it needs to know its physical and logical address. When the sending device does not know the physical address, it uses the address resolution protocol (ARP). The sending device sends an ARP request broadcast to the entire network, which asks the device with xxx-IP address to respond with its MAC or physical address. Each device on the network receives the request. When the intended device receives it, it responds to the requestor with its MAC address. The sending device now has both the logical address (IP) and physical address (MAC) and is able to establish communication.

ICMP

ICMP (Internet Control Message Protocol) is at the same relative layer as IP; its purpose is to transmit information needed to control IP traffic. It is used mainly to provide information about routes to destination addresses. ICMP redirects messages and informs hosts about more accurate routes to other systems, whereas ICMP unreachable messages indicate problems with a route. Additionally, ICMP can cause TCP connections to terminate "gracefully" if the route becomes unavailable. Ping is a commonly-used ICMP-based service.

Internet Control Message Protocol (ICMP) – An IP management and control protocol that delivers messages between hosts regarding the health of the network. ICMP messages include the availability of hosts, as well as routing information and updates. Some ICMP utilities are: PING (Packet Inter-Network Groper) and Traceroute.

DNS

Imagine how hard it would be to use the Internet ifwe had to remember actual specific IP addresses. The Domain Name Service (DNS) is a method of resolving hostnames to IP addresses so that names can be used instead of IP addresses when referencing unique hosts on the Internet. Not too many years ago, when the Internet was made up of about 100 computers (versus over 1 million now), a list used to be kept that mapped every user's hostname to their IP address. This list was kept on an FTP server so that everyone could access it.

It did not take long for the task of maintaining this list to become overwhelming, and the computing community looked to automate it. A hierarchical system for domain names was developed, and in 1992 the National Science Foundation (NSF) awarded Network Solutions, Inc. (NSI) the contract to manage and maintain domain names and the registration process of those names. NSI handled the name registration and a hostname resolution directory of DNS servers. It also maintained the authoritative databases of the Internet, which are the root DNS servers. An authoritative root DNS server contained 13 files, one for each of the top-level domain servers. Until 1999, the Internet Assigned Numbers Authority (IANA) maintained and coordinated the allocation of IP addresses.

Large Internet service providers (ISPs) would apply to the registries for blocks of these IP addresses and allocate the blocks to smaller ISPs or individual users. However, after 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) took over the responsibilities of IP address block allocation, DNS management, and root server system management. NSI still maintains the authoritative root databases. Wonderful. We have had a history lesson but how does DNS work and what is its place in a network? When a user types in a uniform resource locator (URL) in his web browser, the URL is made up of words or letters that are in a sequence that makes sense to that user, such as www.logicalsecurity.com.

SSH

Secure Shell (SSH) functions as a type of tunneling mechanism that provides terminal-like access to remote computers. SSH is a program and a protocol that can be used to log into another computer over a network. For example, the program can let Paul, who is on computer A, access computer B's files, run applications on computer B, and retrieve files from computer B without ever physically touching that computer. SSH provides authentication and secure transmission over vulnerable channels like the Internet.

SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh, which provide the same type of functionality that SSH provides but in a much less secure manner. SSH is a program and a set of protocols that work together to provide a secure tunnel between two computers. The two computers go through a handshaking process and exchange via a Diffie-Hellman session key that will be used during the session to encrypt and protect the data that is exchanged. Once the handshake takes place and a secure channel is established, the two computers have a pathway to exchange data with the assurance that the information will be encrypted and its integrity will be protected.

An SSH client program is typically used for establishing connections to an SSH daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, Linux, FreeBSD, Solaris and OpenVMS. Proprietary, freeware and open source versions of various levels of complexity and completeness exist.

SNMP

The two main components within SNMP are managers and agents. The manager is a server that polls different devices to check their status, receives traps from agents, and provides a centralized place to hold all network-wide information. The server component is usually referred to as the Network Management Station (NMS) or just the manager.

The agent is a piece of software that runs on a network device, which can be integrated, into the operating system or a daemon that runs independent of the operating system. The agent has a list of objects that it is to keep track of for the device that it is installed upon. This list of objects is held in a database like structure called the Management Information Base (MIB).

SMTP

Simple Mail Transfer Protocol (SMTP) – A simple protocol that manages the exchange of e-mail messages between two mail servers. Defined by the IETF, SMTP ensures that messages can be transferred within a network or through different networks that pass through one or several gateways.

SMTP is a simple protocol that controls the exchange of e-mail messages between two mail servers. The protocol is used in the Internet and is defined by the IETF. Using SMTP, a process can transfer mail to another process on the same network or to some other network via a relay or gateway process accessible to both networks. A mail message may pass through a number of intermediate relay or gateway hosts on its path from sender to ultimate recipient.

The model consists of user agents, which are applications that provide e-mail services (create and view messages). The MTA (message transfer agent) is the component that uses the SMTP protocol to forward messages to other MTAs. A user creates a message and chooses Send. The message is queued locally with other Outbox messages for delivery at a designated time. The local MTA forwards the messages to the relay MTA, which may be a corporate e-mail server located at the LAN/Internet connection, or a mail server at an ISP that home users connect with across their dial-up connection.

SMTP uses a client/server relationship. The client is the system with mail to send. It establishes a two-way transmission channel to an SMTP server over a TCP connection.

Questions and Answers

1. IP, ICMP, RIP, IGMP, and IPX are protocols found at which layer of the OSI Model?

   a. Session Layer
   b. Transport Layer
   c. Network Layer
   d. Data Link Layer

Answer: C

Module 03: IP, ICMP, RIP, IGMP, and IPX are protocols found at the Network Layer.

2. SLIP, PPP, ARP, RARP, L2F, and L2TP are protocols found at which layer of the OSI Model?

   a. Session Layer
   b. Transport Layer
   c. Network Layer
   d. Data Link Layer

Answer: D

Module 03: SLIP, PPP, ARP, RARP, L2F, and L2TP are protocols found at the Data Link Layer.

3. High-speed Serial Interface (HSSI), H.21, EIA/TIA-232, and EIA/TIA-449 are protocols found at which layer of the OSI Model?

a. Session Layer
b. Transport Layer
c. Physical Layer
d. Data Link Layer

Answer: C

Module 03: High-speed Serial Interface (HSSI), H.21, EIA/TIA-232, and EIA/TIA-449 are protocols found at the Physical Layer.

4. ASCII, TIFF, GIF, JPEG, MPEG, MIDI, MIME are protocols found at which layer of the OSI Model?

a. Application Layer
b. Presentation Layer
c. Session Layer
d. Transport Layer

Answer: B

Module 03: ASCII, TIFF, GIF, JPEG, MPEG, MIDI, and MIME are protocols found at the Presentation Layer.

5. NetBIOS, NFS, SQL, and RPC are protocols found at which layer of the OSI Model?

a. Presentation Layer
b. Session Layer
c. Transport Layer
d. Network Layer

Answer: B

Module 03: NetBIOS, NFS, SQL, and RPC are protocols found at the Session Layer.

Chapter 4: Cryptography

Topics

- Encryption Overview
- Symmetric Encryption
- Asymmetric Encryption
- Hashing
- Hybrid Encryption
- Advanced Encryption Methods
- Attack Vectors

Background

Encryption has been used throughout history. The Egyptians used Hieroglyphics, Caesar used substitution cipher, Spartans used skytale, and Thomas Jefferson used a Cipher wheel. Skytale was a thin sheet of papyrus wrapped around a stick. As systems have become more complex and the data to protect more valuable, cryptography methods have also evolved. There are many different algorithms and applications that are used to keep information safe in today's corporate networked environment.

Encryption Overview

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge a key. Encryption also implicitly refers to the reverse process, decryption, to make the encrypted information readable again. Encryption, by itself, can protect the confidentiality of messages but other techniques are still needed to protect the integrity and authenticity of a message. Message Authentication Code (MAC) and Digital Signatures are examples of Integrity and Non-Repudiation mechanisms.

Cryptographic Definitions:

- Cryptography – Science of hiding the meaning of communication
- Cipher – Something that transforms characters or bits into an unreadable format
- Cryptographic Algorithm – Procedures that turn readable data into an unreadable format
- Cryptanalysis – Science of studying and breaking encryption mechanisms
- Cryptology – Study of cryptography and cryptanalysis
- Key Clustering– When two keys generate the same cipher text from the same plain text

A mathematical procedure for performing encryption on data is an encryption algorithm. Through the use of an algorithm, information into meaningless cipher text and requires the use of a key to transform the data back into its original form. There are two main methods of implementing encryption, Block and Stream ciphers. Block cipher is a type of symmetric key cipher, which operates on blocks or groups of bits of a fixed or unvarying length. Stream cipher is a symmetric cipher in which the input digits are encrypted successfully or one at a time, and the transformation of successive digits varies during the encryption.

Symmetric Encryption

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption. The encryption key is trivially related to the decryption key, in that they may be identical. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. Symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms.

The disadvantage of symmetric-key algorithms is the requirement of a shared secret key, with one copy at each end. Since the keys are subject to potential discovery by a cryptographic adversary, they need to be changed often and kept secure during distribution and in service.

Weaknesses:

- Key distribution – It requires a secure method to get the key to the destination
- Scalability – Each pair of users need a unique pair of keys, so the number of keys can grow and become unmanageable
- Limited security – It can provide confidentiality, but not true authenticity or non-repudiation

Asymmetric Encryption

In symmetric key cryptography, a single secret key is used between entities, whereas in public key systems, each entity has different keys, or asymmetric keys. The two different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required in order to decrypt the message. In a public key system, the pair of keys is made up of one public key and one private key. The public key can be known to everyone, and the private key must be known and used only by the owner. Many times, public keys are listed in directories and databases of e-mail addresses so that they are available to anyone who wants to use these keys to encrypt or decrypt data when communicating with a particular person.

Key Exchange

Diffie-Hellman key exchange (D-H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. El Gamal is an asymmetric system that is based on D-H. Asymmetric encryption is not very efficient.

Up to this point, we have figured out that symmetric algorithms are fast but have some drawbacks (lack of scalability, difficult key management, and provide only confidentiality). Asymmetric algorithms do not have these drawbacks but are very slow. We just can't seem to win. So, we turn to a hybrid system that uses symmetric and asymmetric encryption methods together.

Hashing

A hash is a process to create a unique string of characters from any data source – password or executable. The output is of a fixed length defined by the algorithm. The output changes completely if the source changes. It is used mainly for data integrity and secure password authentication. The hash cannot be reversed to the plain text – one way.

A good hashing algorithm should not produce the same hash value for two different messages. If the algorithm does produce the same value for two distinctly different messages, this is called a collision. An attacker can attempt to force a collision, which is referred to as a birthday attack. This attack is based on the mathematical birthday paradox that exists in standard statistics.

A hash collision is when two distinct data sources are input into a hashing function, which then produce identical outputs. A good hashing algorithm should minimize this potential as much as possible, to within low probability values. Cracking the hash refers to deliberately changing the data source so that it matches a previously created hash. This negates the integrity of the source data.

Hybrid Encryption

Symmetric encryption is fast, it has many algorithms available but has the problem of key management. Asymmetric encryption is inefficient for large amounts of data but handles the key exchange in a secure manner. They neither allow for authentication nor ensure non-repudiation. Hybrid encryption systems bring the best of both together without the downfalls. Hybrid encryption is very common in secure networks and even for the regular home user.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), its successor, are cryptographic protocols, which provide secure communications on the Internet for such things as e-mail, Internet faxing, and other data transfers. SSL runs on layers beneath application protocols such as HTTP/S, FTP, SMTP, and NNTP and above the TCP or UDP transport protocol.

Advanced Encryption Methods

The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. It can be more flexible and less expensive than end-to end and link encryption methods.

IPSec has strong encryption and authentication methods, and although it can be used to enable tunneled communication between two computers, it is usually used to establish virtual private networks (VPNs) among networks across the Internet. IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to use; rather, it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology.

IPSec uses two basic security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity. IPSec can work in one of two modes: transport mode, in which the payload of the message is protected, and tunnel mode, in which the payload and the routing and header information are protected.

Public Key Infrastructure is a user invisible system to allow for the easy usage of encryption systems and the heightened security they offer. The main components include:

- Certificate Authority
- Registration Authority
- Digital certificates
- Certificate revocation lists
- Public key-enabled applications and services

Quantum Cryptography:

Quantum cryptography, or quantum key distribution, uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. A central problem in cryptography is the key distribution problem. Public key cryptography relies on the computational difficulty of certain hard mathematical problems, whereas quantum cryptography relies on the laws of quantum mechanics.

Attack Vectors

The Diffie-Hellman algorithm is vulnerable to a man-in-the-middle attack, because no authentication occurs before public keys are exchanged. In our example, when Tanya sends her public key to Erika, how does Erika really know that it is Tanya's public key? What if Lance spoofed his identity, told Erika he was Tanya, and sent over his key? Erika would accept this key, thinking that it came from Tanya. Let's walk through the steps of how this type of attack would take place:

1. Tanya sends her public key to Erika, but Lance grabs the key during transmission so that it never makes it to Erika.

2. Lance spoofs Tanya's identity and sends over his public key to Erika. Erika now thinks that she has Tanya's public key.

3. Erika sends her public key to Tanya, but Lance grabs the key during transmission so that it never makes it to Tanya.

4. Lance spoofs Erika's identity and sends over his public key to Tanya. Tanya now thinks that she has Erika's public key.

5. Tanya combines her private key and Lance's public key and creates symmetric key S1.

6. Lance combines his private key and Tanya's public key and creates symmetric key S1.

7. Erika combines her private key and Lance's public key and creates symmetric key S2.

Questions and Answers

1. ________ is when two keys generate the same cipher text from the same plain text.

   a. Cryptanalysis
   b. Cryptology
   c. Key Clustering
   d. Cipher

Answer: C

Module 04: Key clustering is when two keys generate the same cipher text from the same plain text.

2. True or False. A hash is a process to create a unique string of characters from any data source – password or executable.

   a. True
   b. False

Answer: A

Module 04: A hash is a process to create a unique string of characters from any data source – password or executable.

3. True or False. A hash collision is when two distinct data sources are input into a hashing

function, which then produce identical outputs.

a. True
b. False

Answer: A

Module 04: A hash collision is when two distinct data sources are input into a hashing function, which then produce identical outputs.

4. ________ is the science of studying and breaking encryption mechanisms.

a. Cryptography
b. Cipher
c. Cryptographic Algorithm
d. Cryptanalysis

Answer: D

Module 04: Cryptanalysis is the science of studying and breaking encryption mechanisms.

5. ________ is the study of cryptography and cryptanalysis.

a. Cryptanalysis
b. Cryptology
c. Key Clustering
d. Cipher

Answer: B

Module 04: Cryptology is the study of cryptography and cryptanalysis.

Chapter 5: Why Vulnerability Assessment?

Topics

- What is a Vulnerability Assessment?
- Compliance and Project Scoping
- Assessing Current Network Concerns
- Network Vulnerability Assessment Methodology
- Policy Review (Top-Down) Methodology
- Technical (Bottom-Up) Methodology

What is a Vulnerability Assessment?

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. This basic process involves a diligent analysis of the target system for any weaknesses, technical flaws or vulnerabilities. A vulnerability from the perspective of disaster management means assessing the threats from potential hazards to the population and to infrastructure. It may be conducted in the political, social, economic or environmental fields.

Compliance and Project Scoping

Developing the scope of a project is the early work where we decide what boundaries we will set to limit the work of this project. Those boundaries are defined by:

- What physical limits will exist?
- What parts of the organization will be included?
- How much of the network will be reviewed?
- How many people will be consulted?
- How many people will be working on the project?

Most failed projects come to grief because the scope of the project was poorly defined to begin with, or because the scope was not managed well and was allowed to "creep" until it was out of control. If we are going to manage the project well, then setting the scope for the project is key to its success.

Setting the scope for a network vulnerability assessment project means that we will start with a Project Overview Statement and then develop the Project Scope Document. The Project Scope Document consists of elements of the Project Overview Statement, a task list, and the documents that set limits on the task list. The task list and the documents that set limits on the tasks will form the basis of our project plan for the network vulnerability assessment.

Assessing Current Network Concerns

All network services, ones in the DMZ included, have similar circumstances: they rely on the layer 2 and 3 protocols below them to work; they run on a host operating system and they must accept a certain amount of connections to do their job. Although, there are many different countermeasures that could be applied to these services; the fact is that many services in the DMZ are not configured with the highest degree of security available and others still have flaws in the codes that make running the service, at all, a risk.

Vulnerabilities in the Service

Only recently have developers been held accountable for the security of their code as well as its functionality. In the past, when a program was developed, the only test was whether it worked. These days, security has to be defined at the Functional Requirements phase of the Software Development Lifecycle to ensure that it can be validated throughout the development process. So what do you do if you are not a developer? Constant vigilance is your only choice. Being aware of versions of ALL of your network services and checking the appropriate sites for known attacks and patches to fix known vulnerabilities is the best way to mitigate risk. Running older versions is also not recommended; vendors usually implement the newest security features in their current products, not retrofitted into their legacy ones.

Vulnerabilities in the Host OS

No matter which Host OS you run on a server, there's a risk of other services, inherent to the OS itself that could be vulnerable to attack. If you are setting up a DNS server for your DMZ, there is no reason to have Microsoft File and Print Services running on the box. Certainly, there are times that you need a server to host more than one service (DNS and Mail for instance) but that should be carefully tested, documented, and deployed.

Vulnerabilities in the Protocols Used

No matter how secure the Application layer services are, they depend on lower layer protocols to get the job done. This is why ARP cache poisoning is such a devastating attack when it can be employed, because typical Layer 7 services pay no heed to what MAC address was the source or if it's changed during the session. With that being said, there are similar weaknesses in other protocols like IP, TCP, and Session layer protocols that can be exploited in a similar way.

Vulnerabilities in the Client

Let's not forget the client! If we can trick the client into thinking we are the server, we've won, or intercepting the request or the reply...or impersonating the client to the server. Especially in DMZ resources, the client may be unknown to the server so authentication mechanisms typically employed on the LAN are not available. There are new RFCs and techniques under review but they aren't widely used at this time.

Vulnerabilities in the Intermediate Systems

Let's face it; clients don't connect directly to servers unless they are plugged into the same switch or hub. So we really do have to trust all of the proxies, firewalls, routers, and gateways that we go through on our journey from client to server and back again. A compromise of a router in-between a client and server could compromise all sessions and be undetectable.

Network Vulnerability Assessment Methodology

Some key terms in the network vulnerability assessments include:

- **Risk**: the probability that a threat will exploit a vulnerability to adversely affect an information asset
- **Threat:** an event, the occurrence of which could have an undesired impart
- **Threat impact**: a measure of the magnitude of loss or harm on the value of an asset
- **Threat probability**: the chance that an event will occur or that specific loss value may be attained should the event occur
- **Safeguard**: a risk-reducing measure that acts to detect, prevent, minimize loss associated with the occurrence of a specified threat or category of threats
- **Vulnerability**: the absence or weaknesses of a risk-reducing safeguard

Phase I: Data Collection

During this phase, you will need to review the applicable state and federal laws affecting this particular client, review available documentation (note all areas of concern), and draw up a list of known bugs and security vulnerabilities to test for in the client environment.

Phase II: Interviews, Information Reviews and Hands-On Investigation

Here is a list of steps that should be performed during this phase:

1. The network vulnerability assessment team defines roles or functions about which it wants to gather information
2. The team lead and POC develop an interview schedule
3. The client POC arranges interviews with appropriate client staff members and provides office space for the network vulnerability assessment team
4. Appropriate members of the network vulnerability assessment team interview identified appropriate staff members and other identified personnel
5. The network vulnerability assessment team (usually) requests additional documents (that were not provided in Phase I)
6. The network vulnerability assessment team requests additional interviews, as needed
7. The team lead requests facility and network clearance and passwords for team members from the client POC, as required

8. The network vulnerability assessment team tours computing facilities and conducts tests of operating systems, hardware, network devices, and software
9. The network vulnerability team tours facilities and performs physical plant inspection

Phase III: Analysis

The process of analysis actually begins with the acquisition of the first document only ends in the generation of the Draft Report during Phase IV. Analysis spans most of the network vulnerabilities assessment process and generates the majority of content in the report. This phase entails:

- Risk Analysis
- Security Policy
- Threat Analysis

To be successful, the network vulnerability assessment team will have to identify what network security concerns have the highest priority. This will allow the team to focus on these threats and risks that can cause the enterprise the most damage. Understanding that security concerns include personnel and physical, as well as technical issues, will ensure the most comprehensive assessment prospect.

Use all of the resources available to plot what threats will be addressed. Do your research to gather significant issues and then prioritize these risks based on the probability of occurrence and impact to the enterprise or network. Concentrate on those issues that will bring the biggest impact to your organization. Use your team to identify additional items and measure their specific impact.

Developing a checklist will assist the network vulnerability assessment team in ensuring that basic security controls are examined. Do not just use the checklist. Listen and ask questions and be ready to include additional information in the examination process.

Policy Review (Top-Down) Methodology

As with any assessment process, it is important to ensure that policies establish the direction management wants to go with regard to security. The top-down portion of the network vulnerability assessment (NVA) looks at the policies requested in the Pre-NVA checklist.

Definitions:

- Policy – A high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area. A policy should be brief (which is highly recommended) and set at a high level.
- General Program Policy – Sets the strategic directions of the enterprise for global behavior and assign resources for its implementation. This includes such topics as information management, conflict of interest, employee standards of conduct, and general security measures.
- Topic-Specific Policy – Addresses specific issues of concern to the organization. Topic-specific policies might include e-mail usage, physical security, application development, system maintenance, and network security.
- System or Application-Specific Policy – Focus on decisions taken by management to protect a particular application or system, it might include controls established for the financial management system, accounts payable,

business expense forms, employee appraisal, and order inventory.

A security policy is the articulation of an organization's residual risk position. It describes the security controls that govern an organization's information systems and stakeholders. Properly followed, these controls define a specific set of conditions to help protect a company's assets and its ability to conduct business.

All good security policies must be written, in one or more interrelated documents.

Maintenance of the 'least privilege' principle through describing stakeholder behavior – excessive (wasteful) and inappropriate (risky) access is forbidden. Mitigation of organizational liability towards internal and external stakeholders. Preservation and protection of valuable, confidential, or proprietary information from unauthorized access or disclosure.

Policy Review (Top-Down) Methodology

The goal of this six-step process is to maximize the time spent during the technical phases of a network vulnerability assessment (NVA):

- Step 1 – Site survey
- Step 2 – Develop a test plan
- Step 3 – Build the toolkit
- Step 4 – Conduct the assessment
- Step 5 – Analysis
- Step 6 – Documentation

Questions and Answers

1. ________ is the probability that a threat will exploit a vulnerability to adversely affect an information asset.

   a. Risk
   b. Threat
   c. Treat Impact
   d. Threat probability

Answer: A

Module 05: Risk is the probability that a threat will exploit a vulnerability to adversely affect an information asset.

2. ________ is an event, the occurrence of which could have an undesired impart.

   a. Risk
   b. Threat
   c. Treat Impact
   d. Threat probability

Answer: B

Module 05: Threat is an event, the occurrence of which could have an undesired impart.

3. ________ is a measure of the magnitude of loss or harm on the value of an asset.

a. Risk
b. Threat
c. Treat Impact
d. Threat probability

Answer: C

Module 05: Threat impact is a measure of the magnitude of loss or harm on the value of an asset.

4. ________ is the chance that an event will occur or that specific loss value may be attained should the event occur.

a. Risk
b. Threat
c. Treat Impact
d. Threat probability

Answer: D

Module 05: Threat probability is the chance that an event will occur or that specific loss value may be attained should the event occur.

5. ________ is a risk-reducing measure that acts to detect, prevent, and minimize loss associated with the occurrence of a specified threat or category of threats.

a. Risk
b. Safeguard
c. Treat Impact
d. Threat probability

Answer: B

Module 05: Safeguard is a risk-reducing measure that acts to detect, prevent, and minimize loss associated with the occurrence of a specified threat or category of threats.

Chapter 6: Reconnaissance, Enumeration, Scanning

Topics

- What Information is gathered by the Hacker?
- Passive vs. Active Reconnaissance
- Footprinting Defined
- Methods of obtaining Information
- Domain Name Registration
- Scanning Live Systems
- Enumeration

What Information does the Hacker gather?

When the hacker is gathering information, they are trying to gain the following information about the system:

- Whose system is it? Find the owner
- What type of systems are used (job advertisements, way back machine)
- How big is the company? Have they merged recently with another company?
- How do their sites communicate with each other?

- What type of telephone/PABX/communication systems are used?
- Is the IT support local or off site?
- What is accessible from the Internet? What services, routers, DMZ's?

Passive vs. Active Reconnaissance

Passive reconnaissance is the process of collecting information about an intended target without direct contact with the target. Active Reconnaissance is the process of collecting information about an intended target by making contact with the target through Social Engineering or Electronic probing of the target system. The primary goal and outcome of reconnaissance is footprinting.

Footprinting Defined

The process of gathering data regarding a specific network environment, usually for the purpose of exploiting system vulnerabilities. Footprinting begins by determining the location and objective of an intrusion. Finally, creating a network diagram and/or a company blueprint for later attack analysis.

Methods of obtaining Information

Social engineering is the practice of persuading people to believe you are someone you are not, to obtain confidential information by manipulation of legitimate users. Social engineers may use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. A hacker can obtain information about a target from the Internet, newspapers, employees, employee family members, consultants, vendors, customers, and security experts.

Social Engineering Techniques:

- Authority – Attackers pose as victim's boss, boss's secretary, other company personnel
- Strong Emotion – Get victim into heightened emotional state so they don't pay as much attention to the details/facts.
- Overloading – Provide more information than target can handle so wrong statements go unnoticed also known as 'Double Talk'.
- Reciprocation – "If a stranger does you a favor, then asks you for a favor, don't reciprocate without thinking carefully

about what he's asking for." *Kevin Mitnick, The Art of Deception*

- Deceptive Relationships – Depending on the target, an attacker may build and maintain a relationship for years for the sole purpose of exploiting it.
- Integrity and Consistency – People will even carry out commitments they believe were made by their fellow employees.
- Social Proof – People usually rely on what other people are doing or saying to a certain degree.

Domain Name Registration

DNS databases contain information about FQDNs and IP addresses. They also contain information such as which servers are the Mail servers and which are Active Directory servers. Nslookup is used to query domain name servers. The output information can be used to diagnose DNS issues. However, hackers can use Nslookup's output to determine what servers to target. Both UNIX and Windows come with an Nslookup client, and it is built into many tools. Traceroute is used to determine the path taken from the attackers to a target network by exploiting the Time to Live to get to the target machine.

Scanning Live Systems

Scanning is a method for discovering exploitable communication channels. Port scanning is how attackers identify open and available TCP/IP ports, services applications on a system. Applications and services on a system are associated with well-known port numbers. For example port 80 is HTTP, port 23 is Telnet, and port 25 is SMTP.

You should understand the three-way handshake. As long as the three-way has not been completed, the law has not been broken. A port scan is like checking to see if the door is unlocked but not entering to see whether someone's at home. No crime has been committed yet so in most cases the police can't do anything at this point. If a computer system is attacked many times by a port scan, one can argue that the port scan was, in fact, a denial-of-service attack, which is usually an offense.

Basic network connectivity can be tested using the ping command to determine the range of IP addresses mapped to a live host. Ping sends out ICMP Echo Request packets, and if the address is live, an ICMP Echo Reply message will be received from an active machine. Alternately, TCP or UDP packets can be sent if ICMP messages are blocked.

In a TCP Connect port scan, the attacker sends SYN packets to sequential port numbers on a target to see which port numbers reply. A connection is tried to port 1, then port 2, then port 3… An open port will reply with a SYN/ACK, a closed port will reply with RST/ACK, or no reply if filtered.

A half-open TCP SYN port scan is the same as the vanilla TCP open scan, however the attacker does not complete the three-way handshake. An open port will still reply with a SYN/ACK, a closed port will reply with a RST/ACK. Advantage over TCP Connect scan: may not be detected by simple IDS and no law has been broken at this time.

A TCP Connect or half-open scan should receive either a SYN/ACK or a RST/ACK packet. However, a third possibility exists: No response. This is often due to a firewalled port being filtered, or possibly the packets being lost due to network congestion.

Enumeration

Enumeration is the process of obtaining network resources, usernames and passwords, services and machine names. Information that can be gained by enumeration: Banners from FTP servers, web servers, email servers; FQDNs and IP addresses; IP configuration of routers and servers; Information from Active Directory; Usernames and share names.

Any DNS server that is accessible from the Internet can be queried and tell a hacker about server names and IP addresses. If the DNS server contains records for not only the DMZ servers, but also internal servers, this is a security hole. If the hacker is able to determine internal machine names, the hacker can then find out the machine's IP addresses.

Windows 2000/2003 Active Directory is accessed using Lightweight Directory Access Protocol (LDAP). LDAP uses the X.500 naming scheme for objects in the directory. This naming scheme uses Distinguished Names to identify objects in the directory.

Windows NT and higher support "Null Sessions", which are an anonymous connection allowed to retrieve certain information such as usernames, groups, shares, and services.

Questions and Answers

1. True or False. Passive reconnaissance is the process of collecting information about an intended target by making contact with the target through Social Engineering or Electronic probing of the target system.

   a. True
   b. False

Answer: B

Module 06: Passive reconnaissance is the process of collecting information about an intended target without direct contact with the target.

2. True or False. Active reconnaissance is the process of collecting information about an intended target without direct contact with the target.

   a. True
   b. False

Answer: A

Module 06: Active reconnaissance is the process of collecting information about an intended target by making contact with the target through Social Engineering or Electronic probing of the target system.

3. True or False. Authority is where attackers pose as victim's boss, boss's secretary, or other company personnel.

a. True
b. False

Answer: A

Module 06: Authority is where attackers pose as victim's boss, boss's secretary, or other company personnel.

4. True or False. Strong emotion gets victims into heightened emotional state so they don't pay as much attention to the details/facts.

a. True
b. False

Answer: A

Module 06: Strong emotion gets victims into heightened emotional state so they don't pay as much attention to the details/facts.

5. True or False. Overloading provides more information than target can handle so wrong statements go unnoticed also known as 'Double Talk'.

a. True
b. False

Answer: A

Module 06: Overloading provides more information than target can handle so wrong statements go unnoticed also known as 'Double Talk'.

Chapter 7: Gaining Access

Topics

- Physical Access Attacks
- Lock Picking In Depth
- The Metasploit Project
- Saint Exploit – Cost Effective Choice
- CORE Impact

Background

An exploit is a common term in the computer security community that refers to a malicious computer attack that takes advantage of a vulnerability, bug, glitch, or security hole that can lead to privilege escalation or denial of service on a computer system. Exploits can be classified by the type of vulnerability they attack on the system.

Many exploits are designed to provide root level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root. Blackhat hackers do not publish their exploits but keep them private to themselves or other malicious hackers. Such exploits are referred to as 'zero day exploits' and to obtain access to such exploits is the primary desire of unskilled malicious attackers, so called script kiddies.

Physical Access Attacks

Physical security is key to protecting a company's network. Physical security measures that prevent or deter attackers from accessing a facility resource or information stored on physical media can be as simple as a locked door or as elaborate as multiple layers of armed guard posts.

A hacker can use a form of social engineering to enter a business premises. Say they pose as a fire inspector to gain access to the ceilings where cable run. Hackers may also use dumpster diving to retrieve sensitive computer information.

Lock Picking In Depth

Lock picking is an art that requires many hours of practice. Some 'sport' lock pickers refer to the 'Zen of lock picking' - becoming one with the lock. With practice, you can open most locks in just a few seconds. To learn how to pick locks, you must understand how the internal mechanics work. One of the best methods is to acquire several locks and take them apart. Study the different types of locks to better prepare you to pick them in the field.

In order to understand the 'feel' of lock picking you need to know how the movement of a 'binding' pin is affected by the torque applied by your wrench and the pressure applied by your pick. The 'binding' torque is caused by the friction of the pin against the cylinder, hull and spring. When the pressure of the pick exceeds the friction, the pin will raise into the hull.

Definitions

- Binding Pin – Insert the torque wrench and apply a turning pressure to the cylinder. The first pin will 'bind' against the hull. Attempt to raise the binding pin until the cylinder rotates slightly
- Binding – When the binding pin is at the sheer line, the cylinder will rotate slightly. The next pin will now bind. Repeat the process until all pins are at the sheer line. Be careful not to push the pin too far into the hull. This will bind the key pin and prevent the cylinder from rotating. To resolve this, torque must be released to drop the pin
- Binding Order – The order in which the pins bind is different for each lock type.

It depends on the manufacturing process and the lateral position of the pins

- Raking – At home, you can take your time picking a lock, but in the field, speed is always essential. A lock picking technique called raking can quickly open most locks. Basically, you use the pick to rake back and forth over the pins while you adjust the amount of torque on the plug
- Shimming Door Locks – By inserting a thin, strong, 'credit card' shaped object between the door and the frame, you can force the locking wedge into the lock. There are tools available which are shaped to bend around corners to move the wedge

The Metasploit Project

The Metasploit framework is an advanced, FREE open-source project used for developing, testing, and using exploit code. The Framework3 was written in the Ruby programming language and includes various components written in C and assembler. It runs on Linux and Windows and can be used in conjunction with a postgres database. This project can be roughly compared to commercial offerings such as Immunity's

CANVAS and Core Security Technology's (Core-Impact).

Saint Exploit – Cost Effective Choice

Exploits vulnerabilities found by the SAINT vulnerability scanner. It allows the user to verify the existence of vulnerabilities by exploiting them and gathering evidence of penetration includes IPv4 and IPv6 exploits. It features exploit tunneling that allows you to run penetration tests from an exploited target. It features a seamless integration with SAINT's GUI. It boasts an extensive, multi-platform exploit library and includes remote, local, and client exploits. It provides automatic penetration testing, runs individual exploits on demand, and includes web site emulators and an e-mail forgery tool with built-in design templates.

CORE Impact

The product features the CORE IMPACT Rapid Penetration Test, an industry first step-by-step automation of the penetration testing process.

The steps in this process include:

- Information Gathering
- Attack and Penetration
- Local Information Gathering

- Privilege Escalation
- Privilege Escalation
- Clean Up
- Report Generation

Questions and Answers

1. ________ inserts the torque wrench and apply a turning pressure to the cylinder. The first pin will 'bind' against the hull. Attempt to raise the binding pin until the cylinder rotates slightly.

a. Binding Pin
b. Binding
c. Binding Order
d. Raking

Answer: A

Module 07: Binding Pin inserts the torque wrench and apply a turning pressure to the cylinder. The first pin will 'bind' against the hull. Attempt to raise the binding pin until the cylinder rotates slightly.

2. ________ is when the binding pin is at the sheer line, the cylinder will rotate slightly. The next pin will now bind. Repeat the process until all pins are at the sheer line. Be careful not to push the pin too far into the hull. This will bind the key pin and prevent the cylinder from rotating. To resolve this, torque must be released to drop the pin.

a. Binding Pin

b. Binding
c. Binding Order
d. Raking

Answer: B

Module 07: Binding is when the binding pin is at the sheer line, the cylinder will rotate slightly. The next pin will now bind. Repeat the process until all pins are at the sheer line. Be careful not to push the pin too far into the hull. This will bind the key pin and prevent the cylinder from rotating. To resolve this, torque must be released to drop the pin.

3. ________ is the order in which the pins bind is different for each lock type. It depends on the manufacturing process and the lateral position of the pins.

a. Binding Pin
b. Binding
c. Binding Order
d. Raking

Answer: C

Module 07: Binding order is the order in which the pins bind is different for each lock type. It depends on the manufacturing process and the lateral position of the pins.

4. ________ is at home you can take your time picking a lock, but in the field, speed is always essential. A lock picking technique called raking can quickly open most locks. Basically, you use the pick to rake back and forth over the pins while you adjust the amount of torque on the plug.

a. Binding Pin
b. Binding
c. Binding Order
d. Raking

Answer: C

Module 07: Raking is at home you can take your time picking a lock, but in the field, speed is always essential. A lock picking technique called raking can quickly open most locks. Basically, you use the pick to rake back and forth over the pins while you adjust the amount of torque on the plug

5. ________ is done by inserting a thin, strong, 'credit card' shaped object between the door and the frame, you can force the locking wedge into the lock.

a. Binding Pin
b. Binding
c. Shimming Door Locks
d. Raking

Answer: C

Module 07: Shimming Door Locks is by inserting a thin, strong, 'credit card' shaped object between the door and the frame, you can force the locking wedge into the lock.

Chapter 8: Maintaining Access

Topics

- Backdoor Overview
- Linux Backdoor
- Windows Backdoor Countermeasures
- NetCat
- Meterpreter

Backdoor Overview

Accessing a system using a bypass method to access controls allows the attacker to enter the computer at any time. One way that you can install a backdoor is to use a Trojan horse or a maintenance hook. The software provides instructions that allow for easy access and maintenance. It allows entry to code at specific points without security checks. It is accessed through a certain key sequence and should be removed before deployment of software.

The primary purpose of a rootkit is to allow an attacker unregulated and undetected access to compromised systems repeatedly. Rootkits are used by a hacker for various reasons:

- Hide backdoor processes
- Elevate process privileges

- Hide files
- Hide registry entries
- Disable auditing and edit event logs
- Redirect executable files
- Hide device drivers
- Hide user accounts

Linux Backdoor

They usually have four groups of tools: Trojan programs such as altered versions of login, netstat and ps; Backdoors such as inetd insertions; Interface sniffers and system log cleaners. Most user-mode rootkits replace critical operating system files with new versions that perform some of the items above.

Windows Backdoor Countermeasures

To detect the installation of a rootkit, you can use anti-rootkit tools like Ice Sword. Some anti-spyware products may detect rootkits as well. On a known clean system, use a hashing and file monitoring solution to alert if critical system files changed. You need to document services and install procedures to ensure that you can tell a difference if something stops working on the system. If a system is suspect, boot into safe mode. This may make rootkit files visible, if the rootkit uses drivers. Once a rootkit has been detected, erase and reinstall the operating system without Internet connectivity, patch with all service packs and hot fixes. Backups should be scanned, as they may contain malicious hidden content.

NetCat

It creates outbound or inbound connections, TCP or UDP, to or from any port. It has the ability to use any local source port. It can use any locally configured network source address. It has a built-in port scanning capability with a randomizer and a built-in loose source routing capability.

Meterpreter

The purpose of meterpreter scripts are to give end-users an easy interface to write quick scripts that can be run against remote targets after successful exploitation with Metasploit.

Chapter 9: Covering Tracks

Topics

- Covering Tracks Overview
- Disable Auditing and Clearing the Event Log
- Hiding Files with NTFS Alternate Data Streams
- NTFS Countermeasures
- Hiding Files with Steganography
- Steganography Tools
- Shredding Local Evidence
- Anonymizing Tools
- TORs

Covering Tracks Overview

Once a hacker compromises a system, they will disable auditing. clear the event log, hide data in NTFS alternate data streams, hide data in images, shred files that may give clues to the hacker's actions, and install a rootkit to hide processes and files and give them a backdoor for future use.

Disable Auditing and Clearing the Event Log

The hacker will attempt to disable auditing once they have accessed the system. Windows Resource Kit's auditpol.exe tool can disable auditing. It requires Administrator or System rights to execute. The hacker would turn on auditing when they log off the system. It is best to run this tool locally on the victim's computer.

The hacker will clear event logs in order to hide his previous actions. The problem is that when a log is cleared using Event Viewer, it will remove all entries, but create one record stating that the event log has been cleared by 'Hacker'. Another alternative is to use the program elsave.exe to clear the Windows event log. This program does not leave one record behind.

Hiding Files with NTFS Alternate Data Streams

NTFS alternate data streams is the ability to append data to existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer. The command: type c:\winnit\system32 calc.exe >

file.txt:program.exe will append the Windows calculator program onto the file file.txt, to run the program, type the following: start ./file:program.exe. Alternate Data Streams are not detectable using built-in Windows tools, the only indicator is a reduction in free disk space.

NTFS Countermeasures

Scan your systems for Alternate Data Streams on a regular basis. Use ADS detection tools like: If you detect files that have ADS attached, copy those files to FAT and then back to NTFS to lose hidden content.

Some tools to use are:

- LADS
- Streams
- INS
- CruicalADS

Hiding Files with Steganography

Steganography takes one piece of information and hides it within another. Computer files (images, sounds, recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas replacing them with information. The files can then be sent or transported without anyone knowing what really lies inside of them.

Steganography Tools

There are various freeware, shareware, and commercial programs for hiding text in .bmp, .jpg, .wav or mp3 files. The data that is inserted into the image is encrypted, such that it is less detectable. Often, adding the data does not increase the file size. There are tools available that detect if an image has had data added to it.

Shredding Local Evidence

Total Privacy allows you to get total confidence and peace of mind for secure computer use by completely and permanently removing all traces and history of your recent activity. Total Privacy helps improve and optimize your computer's performance. By deleting all those unnecessary temporary files, install/uninstall records and by cleaning your Internet browser cache. A Linux Live CD is designed to audit information technology security, an attacker can protect themselves from locally cached evidence. The CD is a ROM format, therefore any evidence stored in RAM is wiped out when the machine is rebooted.

Anonymizing Tools

Below are some tools that can be used for anonymous means:

- SecurSURF creates an encrypted virtual tunnel between your computer and one of our high bandwidth security proxy servers. This tunnel shields you from the most sophisticated methods of online spying and snooping.
- RoboForm – User ID/password management application
- Thunderbird – Portable E-mail access
- Hushmail – Web based email solution

TORs

TOR is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It enables software developers to create new communication tools with built-in privacy features. A branch of the U.S. Navy uses TOR for open source intelligence gathering, and one of its teams used TOR while deployed in the Middle East recently. Law enforcement uses TOR for visiting or watching web sites without leaving government IP addresses in their web logs and for security during sting operations.

Questions and Answers

1. ________ creates an encrypted virtual tunnel between your computer and one of our high bandwidth security proxy servers. This tunnel shields you from the most sophisticated methods of online spying and snooping.

a. SecurSURF
b. RoboForm
c. Thunderbird
d. Hushmail

Answer: A

Module 09: SecurSURF creates an encrypted virtual tunnel between your computer and one of our high bandwidth security proxy servers. This tunnel shields you from the most sophisticated methods of online spying and snooping.

2. ________ is User ID/password management application.

a. SecurSURF
b. RoboForm
c. Thunderbird
d. Hushmail

Answer: B

Module 09: RoboForm is User ID/password management application.

3. ________ is portable E-mail access.

a. SecurSURF
b. RoboForm
c. Thunderbird
d. Hushmail

Answer: C

Module 09: Thunderbird is portable E-mail access.

4. ________ is a Web based email solution.

a. SecurSURF
b. RoboForm
c. Thunderbird
d. Hushmail

Answer: D

Module 09: Hushmail is a Web based email solution.

5. True or False. TOR is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet.

a. True
b. False

Answer: A

Module 09: TOR is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet.

Chapter 10: Buffer Overflows

Topics

- Buffer Overflows Defined
- Secure Code Review Process
- General Prevention Techniques

Buffer Overflows Defined

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. In this case, a buffer is a sequential section of memory allocated to contain anything from a character string to an array of integers. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.

Many people know that buffer overflows take place when too much data is accepted as an input value, which in turn writes over specific memory segments. A buffer can be overflowed with too much data, but for it to be of any use to an attacker the code that is inserted into the buffer must be of a necessary length followed up by commands the attacker wants to be executed. So a buffer overflow can take place where arbitrary data is shoved into various memory segments, or a carefully crafted set of data can be pushed in that will accomplish a specific task like giving an attacker an open command shell with administrative privilege.

When a programmer writes a piece of software that will accept data, a variable has to be constructed to hold it. The variable, and the data within it, needs to have a place to reside in memory. The programmer must allocate this memory space, which is referred to as a buffer. A buffer is a contiguous segment of memory that holds several instances of the same type of data. You can think of a buffer as a small bucket to hold water (variable that holds data). We have several of these small buckets stacked on top of one another (memory stack) and if too much water is poured into the top bucket, it spills over into the buckets below it (buffer overflow).

When a Web browser requests a Web page from a server it sends over an HTTP Request command. The Web server sends back an HTTP Reply along with the Web page. So the information coming from the Web server is basically parameters and data that need to be placed onto a memory stack for a procedure to process to properly show the user the Web page in the browser.

The previously listed versions of Internet Explorer do not carry out proper bounds checking, which could allow for an excessively long value to be accepted as an HTTP Reply from the Web server. These accepted values then writes over buffers on the stack, along with the return pointer.

This can take place if a user connects to a malicious site that sends this type of formatted data and can also take place via Outlook and Outlook Express. When an e-mail message has a malicious link within it, the attack will initiate when the user clicks on it. If the e-mail client is configured to open the first message when the client initializes, then this attack can take place with no further user activity. This means that this type of attack can take place without the need of a user opening any type of attachment or clicking on a link. The attack happens through basic HTML tags, thus easily accomplished. The Internet Explorer, Outlook and Outlook Express use the URLMON.DLL to allow a user to view a Web site. Any other applications that are written to use this file could also experience this type of vulnerability.

Reconfiguring the browser's security settings will not affect this type of attack because there are no scripts or Active X controls needed. The HTTP reply message contains field information to tell the browser how to present the HTML code along with the necessary HTML code of the Web page. Within the HTTP reply the two fields "Content-encoding" and "Content-type" are of a specific length, which the security settings do not interact with or validate.

Secure Code Review Process

A secure code review is the process in which code is reviewed for flaws that could compromise the confidentiality, integrity or availability of a system. The objective is to catch as many problems as possible, educate others on how to write secure code and how to conduct secure code reviews, and strengthen your knowledge of the application.

We have to know the vulnerabilities in order to find a security vulnerability. There are numerous ways to accomplish this: Attend training; read, read, read; there is a wealth of knowledge published on known vulnerabilities and ways to protect your system. The last part is to practice (it is important to learn by doing), pair experienced reviewers with junior reviewers to spread the knowledge.

To protect the business you want to know what assets are being accessed by the code and the level of protection that is required. You will need to understand what is being protected to know if your code is protecting it. Review uses cases: Do different types of users take different paths or do a walk through at the code level using the use cases to structure your review.

The perception of time constraints is usually why code reviews are not done. Remember, fixing security issues after deployment can be costly and more time consuming. The deployment process will have to be repeated for issues found in production. You have to determine how long you can allow insecure code to be exposed to the public. It is important to have a target when doing the review. Here are some basics:

- What components have the largest attack surfaces?
    - What components are touched by the most users/processes?
    - Web facing services?
- What components protect the most important data?

    - Database access code
    - Encryption components
    - Session management code
    - What is most important to your company?
- Will time allow it?
    - Will time allow reviews after major components are complete?
    - Will time only allow a review after the code is complete?
        - Remember it's always better to find bugs as early in the process as possible
        - If you wait until the code is complete and issues are founds, more code may have to be changed
- Put some process in place
    - Any review that finds issues is better than no review at all

When conducting a source code review, you will want to include the following individuals:

- Developers who are familiar with the architecture
- Developers with knowledge of security

When you are review the code, you want to look for the following information:

- Configuration
    - Many configuration files have default settings that have known security flaws
    - Is there any sensitive information in the configuration files?
        - Database usernames/passwords
        - Test IDs?
    - Protect files according to what resources they control
- Authentication
    - Is strong authentication being used?
        - Brute force attacks and Dictionary-based attacks
        - Attacks that attempt to guess login credentials by escalating known credentials or using common words

- Logging
    - Are all login attempts being logged?
        - Remember Intrusion Detection
    - Is logging centralized
        - Using a centralized approach encourages consistency and code reuse
    - What is being logged?
        - Is the application logging sensitive information?
        - Does the log file allow scripting tags to be written?
- Error and Exception Handling
    - How are errors and exceptions handled?
        - Does the application return any sensitive information to the user?
    - Ensure that all sensitive operations are wrapped appropriately
        - Database methods
        - Encryption processes
- Data Validation
    - Weak validation is usually the reason most attacks are successful

- Is the application validating the data for the following:
  - Type
  - Format
  - Length
  - Range
  - Valid business values
- Data should be validated before constructing SQL statements
- Validate that output does not contain scripting characters

Here are ways to fix the issues:

- Fixing the issues
  - Document and Rank issues
    - Budget, time and how much risk the issues pose to determine fixes
  - Are issues related to lack of training?
    - Are securing best practices being used?
    - Are policies being adhered to?
      - Do policies address common issues?

Automated Tools

- Can be used to find common issues
    - They normally don't find complex issues
        - Flaws in encryption algorithms
        - Flawed business logic
    - Consider using both an automated approach and manual
        - Catch low hanging fruit with automated tools
        - Catch more complex issues with manual review
    - Tools

General Prevention Techniques

We have to change the culture and integrate secure software development into the process. Encode the secure development into your policies, measure your effectiveness, establish an accountability model for security, and appoint a security liaison.

- Educate both the developer and the end user
- Utilize Threat Modeling
- Create or use Code Checklists

- Perform Security Testing
- Patch the Operating System and Application as patches are released

Questions and Answers

1. True or False. A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.

  a. True
  b. False

Answer: A

Module 10: A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer.

2. True or False. When a programmer writes a piece of software that will accept data, a variable has to be constructed to hold it.

  a. True
  b. False

Answer: A

Module 10: When a programmer writes a piece of software that will accept data, a variable has to be constructed to hold it.

3. True or False. The programmer does not have to allocate this memory space, which is referred to as a buffer.

a. True
b. False

Answer: B

Module 10: The programmer must allocate this memory space, which is referred to as a buffer.

4. True or False. A buffer is a contiguous segment of memory that holds several instances of the same type of data.

a. True
b. False

Answer: A

Module 10: A buffer is a contiguous segment of memory that holds several instances of the same type of data.

5. True or False. When a Web browser requests a Web page from a server it sends over an HTTP Request command.

a. True
b. False

Answer: A

Module 10: When a Web browser requests a Web page from a server it sends over an HTTP Request command.