Security+ 2008

To order additional copies contact:

LearnKey
35 North Main
St. George, UT 84770
1.435.674.9733
www.learnkey.com

Belongs to: _____

School: _____

Instructor: _____

Security+ 2008

First Edition

LearnKey

LearnKey, Inc. provides self-paced training courses and online learning solutions to education, government, business and individuals world-wide. With dynamic video based courseware, and effective learning management systems, LearnKey solutions provide expert instruction for popular computer software, technical certifications and application development. LearnKey delivers content on the Web, by enterprise network, and on interactive CD-ROM. For a complete list of courses visit:

http://www.learnkey.com

LearnKey

Security+ 2008
Student Manual

Table of Contents

LearnKey (435) 674-9733 www.learnkey.com

Security Plus

Introduction

Using this Workbook

In the *Introduction* section, you will find an outline for each session of training and sample lesson plans. These are included to give you an overview of the training content and to help you structure your lessons. The content, delivered by industry professionals, is the most up-to-date, comprehensive content available.

The exercises included in this workbook are meant to serve as supplementary material for the OnlineExpert courses. The following types of exercises are included for each session of training:

Fill-in-the-Blanks: The student completes a comprehensive fill-in-the-blank exercise while watching each session of the training. Each exercise follows the instructor's lecture and can be used as a review for the Quiz, the Pre-Tests, and the Post-Tests.

Glossary Crossword and Word Search Puzzles: These puzzles, taken directly from the courses' glossary, are intended to help your students become more familiar with the terms found in each session.

Short Answer: The short answer questions facilitate recall of the basic training concepts to further aid in retention of the course topics and information in preparation for the training's Pre-Assessments and Post-Tests.

Matching: The matching exercise provides additional learning reinforcement of terms and concepts found throughout the training in the courses' glossary.

Research Topic: The research topic gives your students the opportunity to research an applicable real-world situation whose answer will require using their understanding of the training as well as outside resources to generate a response.

Projects: The individual and group projects require your students to apply the knowledge gained during the training to complete the assigned task. By using both individual and group projects students receive the added benefit of applying the knowledge they have gained in a situation that mimics life in the workforce.

Quiz: The quizzes will help you gauge your students' progress. They also provide your students additional preparation for the training Pre-Tests and Post-Tests.

LearnKey

These workbook exercises, used in conjunction with the LearnKey training, give your students the best learning experience possible.

Objective Mapping: The objective mapping provides a quick reference as to where in the training a specific certification exam objective is covered.

Running & Training Time Table: The running and training time tables will help you to better plan your lessons based on the time you have available. The running time is the actual time required to simply watch the training. The training time is an estimated average time that it will take to watch and discuss the concepts presented as well as do any applicable exercises.

Skills Assessment: The skills assessment will help you and your students to gauge their understanding of course topics prior to beginning any coursework. Understanding where your students as a group feel less confident will aid you in planning and getting the most from the training.

LearnKey

Security+ 2008 Course Map

Session 1

Security Requirements	Requirements Methods of Classification Due Care Due Diligence Due Process User Education HR Security	Objectives Covered: 6.4 (Classification of Information, Acceptable Use Policies, Security Related HR Policy, Due Care, Due Process, and Due Diligence, User Education and Awareness Training)
Security Threats	Understanding Threats Viruses and Worms Trojans, Spyware, and Malware Rootkits Logic Bombs and Spam Spam Filtering Botnets	Objectives Covered: 1.1 (Virus, Worm, Trojan, Spyware, Spam, Adware, Rootkits, Logic Bomb, Botnets)
Privilege Escalation	Initial Entry Escalation Methods After Escalation Performing a Logic Bomb	Objectives Covered: 1.1 (Privilege Escalation); 2.5 (Privilege Escalation)
Hardware Security Risks	BIOS USB Devices Storage Cell Phones	Objectives Covered: 1.2 (All of them: BIOS, USB devices, Cell phones, Removable storage, Network attached storage)
Network Vulnerabilities	Vulnerable Devices Weak Passwords Backdoors Denial of Service Vampire Taps	Objectives Covered: 2.5 (Weak passwords, back doors, default accounts, DoS); 2.6 (Vampire taps)
Infrastructure Risks	Old Protocols TCP/IP Issues Null Sessions Spoofing Man-in-the-Middle DDoS DNS Vulnerabilities ARP Poisoning	Objectives Covered: 2.1 (All of them: Antiquated protocols, TCP/IP hijacking, Null sessions, Spoofing, Man-in-the-middle, Replay, DoS, DDoS, Domain name kiting, DNS poisoning, ARP poisoning)

LearnKey

Session 2

Wireless Vulnerabilities	Wi-Fi 802.11 Implementations Data Emanation War Driving Default Behaviors Rogue APs Hijacking	Objectives Covered: 2.7 (Data emanation, War driving, SSID broadcast, rogue access points, weak encryption
Wireless Encryption	Encryption Cracking WEP Authentication Understanding WEP WEP Key Problems Weak Initialization Vectors	Objectives Covered: 2.7 (Data emanation, War driving, SSID broadcast, rogue access points, weak encryption)
Personal Device Security	Portable Devices Blue Jacking Bluesnarfing Black Jacking Laptops	Objectives Covered: 2.7 (Blue jacking, bluesnarfing)
Authentication Fundamentals	Identification Authentication One Factor Multiple Factors Single Sign On	Objectives Covered: 3.6 (One, two and three-factor authentication, Single sign-on); 3.7 (Mutual); 3.8 (difference between identification and authentication (identity proofing)
Authentication Hardware	Thumb Scanners FAR and FRR Smart Cards RFID	Objectives Covered: 3.7 (Biometric reader) – also cover smart cards, keys, RFID-based authentication and other hardware devices that may be referenced on the exam
Authentication Protocols	Understanding Protocols PAP and CHAP LAN Manager NTLM NTLMv2	Objectives Covered: 3.7 (RADIUS, RAS, LDAP, VPN, Kerberos, CHAP, PAP, 802.1X, TACACS)
Advanced Authentication Protocols	Kerberos Kerberos Tickets Kerberos Access LDAP 802.1X/RADIUS TACACS RAS	Objectives Covered: 3.7 (RADIUS, RAS, LDAP, VPN, Kerberos, CHAP, PAP, 802.1X, TACACS)
User, Groups and Roles	Active Directory Users Groups Group Strategy Guidelines Roles	Objectives Covered: 3.3 (Complete coverage of this non-specific objective)
Authorization Models	Group Policy Editor Password Policies Lockout Policies Creating Accounts Account Parameters	Objectives Covered: 3.5 (All objectives: ACL, Group policies, Password policies, Domain password policies, User names and passwords, Time of day restrictions, Account expiration, Logical tokens)

LearnKey

Session 3

ACLs	Managing Folder Access Network Resource Permissions	Objectives Covered: 3.4 (Complete coverage of this non-specific objective)
Access Control Methods	MAC DAC RBAC Least Privilege Implicit Deny Duty Separation	Objectives Covered: 3.2 (MAC, DAC, Role & Rule based access control); 3.1 (Implicit deny, Least privilege, Separation of duties, Job rotation)
Remote Access Security	Overview RA Encryption RA Authentication Enabling RAS RAS Authentication Options	Objectives Covered: 3.7 (Remote access policies, Remote authentication)
Physical Security	Understanding Physical Security Affecting Factors Access Control Facility Access Checklist Internal Access Checklist Network Access Checklist	Objectives Covered: 3.9 (All objectives covered: Physical access logs/lists, Hardware locks, Physical access control – ID badges, Door access systems, Man-trap, Physical tokens, Video surveillance – camera types and positioning)
OS Hardening	Patches Service Packs Linux Hardening Windows Hardening Creating Security Templates Security Analysis	Objectives Covered: 1.3 (Patches, Patch management, Service packs, hotfixes Objectives Covered: 1.3 (Group policies, Security templates, Configuration baselines)
Application Security	Buffer Overflows Dependencies Stack-Based Overflows Heap-Based Overflows After the Attack Countermeasures Instant Messaging P2P Networks	Objectives Covered: 1.4 (Buffer overflows, Instant messaging, P2P)
Web Application Security	Web Servers Communications Common Attacks Web Applications ActiveX and Java XSS Browsers and Cookies Input Validation	Objectives Covered: 1.4 (ActiveX, Java, Scripting, Browser, Cookies, Input validation, Cross-site scripting (XSS))
Email Security	Email Protocols Email Threats Email Authentication Confidentiality SMTP Relay Spam Solutions	Objectives Covered: 1.4 (SMTP open relays)

LearnKey

Session 4

Client Security Solution	avast Software Spam Filtering Pop-Up Blocking Personal Firewalls HIDS	Objectives Covered: 1.5 (All objectives covered: HIDS, Personal software firewalls, Antivirus, Anti-spam, Popup blockers)
Virtualization and Security	Virtualization Defined Benefits Scenarios Virtual PC Hyper-V VMWare Planning Security Issues	Objectives Covered: 1.6 (Complete coverage of this non-specific objective)
Network Firewalls	Understanding Firewalls Firewall Types Firewall Installation Well Known Ports Port Blocking	Objectives Covered: 2.3 (Firewalls); 2.4 (Firewalls)
Network Security Design	Subnetting Virtual LANs Connecting Networks DMZ NAT	Objectives Covered: 2.2 (DMZ, VLAN, NAT, Network interconnections, NAC, Subnetting)
Telephony Security	Traditional PBX VoIP SIP Security H.323 Security	Objectives Covered: 2.2 (Telephony) [Both traditional and VoIP]
Intrusion Detection and Prevention	Intrusion Monitoring IDS Solutions Detection Methods IPS Solutions IPS Detection States Intrusion Indications IDS Implementations Intrusion Responses Honeypots	Objectives Covered: 2.3 (NIDS, NIPS, Honeypot); 2.4 (NIDS); 4.5 (Behavior-based, Signature-based, Anomaly-based)
Controlling Internet Access	Proxy Servers Internet Filters Creating a Firewall Rule	Objectives Covered: 2.3 (Proxy servers, Internet content filters); 2.4 (Proxy servers, Internet content filters)
Protocol Analyzers	Installing Wireshark Capturing Email Logon Creating HTTP Filter Viewing Passwords	Objectives Covered: 2.3 (Protocol analyzers); 2.4 (Protocol analyzers); 4.2 (Protocol analyzers); 4.4 (Protocol analyzers);

LearnKey

Session 5

Wireless Network Security	War Driving SSID Issues Rogue APs Weak Encryption Configuring WPA	Objectives Covered: 2.7 (War driving, SSID broadcast, Rogue access points, Weak encryption) The difference between this section and Section A of Session 2 is that this session covered protection mechanisms and the previous section covered attack methods.
Monitoring Systems	Performance Tools Task Manager Performance Snap-In Baselines Creating a Baseline Creating a Second Baseline Comparing Baselines with Excel	Objectives Covered: 4.4 (Performance monitor, Systems monitor, Performance baseline)
Scanning the Network	Port Scanning Angry IP Scanner Scanning Devices Service Enumeration Configuring Nmap GUI Nmap Scanning	Objectives Covered: 4.2 (Port scanners, Network mappers)
Vulnerability Scanning	Sectools.org OVAL National Vulnerability Database Password Crackers Pen Testing	Objectives Covered: 4.2 (Vulnerability scanners, OVAL (Open Vulnerability and Assessment Language), Password crackers); 4.3 (Complete coverage of this non-specific objective)
Logging and Auditing	Importance of Logs DNS Logs System Logs Performance Logs Access Logs Firewall Logs Antivirus Logs Auditing	Objectives Covered: 4.6 (Security application, DNS, System, Performance, Access, Firewall, Antivirus); 4.7 (User access and rights review, Storage and retention policies, Group policies)
Cryptography 101	Encryption Simple Encryption CIA Non-Repudiation Whole Disk Key Management Steganography Encryption Testing TPM	Objectives Covered: 5.1 (All objectives)
Encryption Algorithms	Encryption Types Key Factors DES 3DES RSA ECC PGP AES RC4 Secure Transfer One-Time Pad	Objectives Covered: 5.3 (All objective)

LearnKey

Session 6

Encryption Protocols and Hashing	Hashing Hashing Protocols Digital Signatures SSL/TLS TLS Goals SSL Operations PPTP L2TP IPSec HTTP Solutions SSH	Objectives Covered: 5.4 (All objectives); 5.2 (All objectives)
Public Key Cryptography	Certificates PK Cryptography PKI Components PKI Processes	Objectives Covered: 5.5 (All objectives); 5.6 (All objectives)
Risk Assessments	Failure Points RAID Spare Parts Redundant Servers Redundant ISP Power Supply Spare Sites	Objectives Covered: 6.1 (All objectives)
Incident Response	Incidents Defined IR Process First Responders Computer Forensics Chain of Custody Reporting Damage Control	Objectives Covered: 6.3 (All objective)
Disaster Recovery	Planning Backup Practices Backup Methods Backup Types Media Rotation Restoration DR Exercises	Objectives Covered: 6.2 (All objectives covered); 6.5 (All objectives)
Social Engineering	Definition Example Attacks Dumpster Diving Passive Attacks Inside and Outside Attacks Reverse Phishing Attacks	Objectives Covered: 6.6 (All objectives)
Security Policies	Importance General Policies Functional Policies Sans.org	Objectives Covered: 6.4 (Secure disposal of computers, Password complexity, Change management, Mandatory vacations, Personally Identifiable Information (PII), SLA)

LearnKey

Session Objectives

Course Objectives: Session 1

1. Understand security vulnerabilities and threats
2. Ensure security requirements are defined
3. Be able to explain the process of privilege escalation

Course Objectives: Session 2

1. Explain wireless vulnerabilities and learn to protect against common wireless attacks
2. Describe authentication concepts, hardware and software
3. Differentiate between authentication and authorization

Course Objectives: Session 3

1. Plan for different access control methods based on specific scenarios
2. Describe and implement physical security controls
3. Ensure that operating systems and applications are configured securely

Course Objectives: Session 4

1. Design for perimeter and end point security
2. Understand the vulnerabilities and security solutions for telephony
3. Explain the different intrusion detection and prevention systems

Course Objectives: Session 5

1. Implement effective monitoring systems and applications
2. Perform network scanning to discover vulnerabilities and improperly configured devices
3. Describe the fundamentals of encryption and cryptography

Course Objectives: Session 6

1. Explain the differences among the many encryption protocols
2. Perform risk assessments and plan for disasters
3. Understand security policies and explain how they protect against intrusions such as social engineering, wireless attacks and other network-based attacks

LearnKey

Security+ 2008 Outlines

Session 1

Introduction
- Prerequisites
- Knowledge Domains
- Security Importance
- Applications

Security Requirements
- Requirements
- Classification
- Due Care
- Due Diligence
- Due Process
- User Education
- HR Security

Security Threats
- Understanding Threats
- Viruses and Worms
- Trojans, Spyware, and Malware
- Rootkits
- Spam Filtering
- Botnets

Privilege Escalation
- Initial Entry
- Escalation Methods
- After Escalation
- Performing a Logic Bomb

Hardware Security Risks
- BIOS
- USB Devices
- Removable Storage
- Cell Phones

Network Vulnerabilities
- Vulnerable Devices
- Weak Passwords
- Backdoors
- Denial of Service
- Vampire Taps

Infrastructure Risks
- Old Protocols
- TCP/IP Issues
- Null Sessions
- Spoofing
- Man-in-the-Middle
- Replay Attacks
- DDoS
- DNS Vulnerabilities
- ARP Poisoning

LearnKey (435) 674-9733
www.learnkey.com

LearnKey

Session 2

Wireless Vulnerabilities
- Wireless LANs
- Wi-Fi
- Data Emanation
- War Driving
- Default Behaviors
- Rogue APs
- Hijacking

Wireless Encryption
- Encryption Cracking
- WEP
- Authentication
- Understanding WEP
- WEP Key Problems
- Weak Initialization Vectors

Personal Device Security
- Portable Devices
- Bluejacking
- Bluesnarfing
- Blackjacking
- Laptops

Authentication Fundamentals
- Identification
- Authentication
- One Factor
- Multiple Factors
- Single Sign-On

Authentication Hardware
- Thumb Scanners
- FAR and FRR
- Smart Cards
- RFID

Authentication Protocols
- Understanding Protocols
- PAP and CHAP
- LAN Manager
- NTLM
- NTLMv2

Advanced Authentication Protocols
- Kerberos
- Kerberos Tickets
- Kerberos Access
- LDAP
- 802.1X/RADIUS
- TACACS
- RAS

Users, Groups, and Roles
- Active Directory
- Users
- Groups
- Group Strategy
- Guidelines
- Roles

Authorization Models
- Group Policy Editor
- Password Policies
- Lockout Policies
- Creating Accounts
- Account Parameters

LearnKey

Session 3

CLs
- Managing Folder Access
- Network Resource Permissions

Access Control Methods
- MAC
- DAC
- RBAC
- Least Privilege
- Implicit Deny
- Duty Separation

Remote Access Security
- Remote Access
- RA Encryption
- RA Authentication
- Enabling RAS
- RAS Authentication Options

Physical Security
- Understanding Physical Security
- Affecting Factors
- Access Control
- Facility Access Checklist
- Internal Access Checklist
- Network Access Checklist

OS Hardening
- Patches
- Service Packs
- Patch Management
- Linux Hardening
- Windows Hardening
- Creating Security Templates
- Security Analysis

Application Security
- Buffer Overflows
- Dependencies
- Stack-Based Overflows
- Heap-Based Overflows
- After the Attack
- Countermeasures
- Instant Messaging
- P2P Networks

Web Application Security
- Web Servers
- Communications
- Common Attacks
- Web Applications
- ActiveX and Java
- XSS
- Browser Options
- Cookies
- Input Validation

E-mail Security
- E-mail Protocols
- E-mail Threats
- E-mail Authentication
- Confidentiality
- SMTP Relay
- Spam Solutions

LearnKey

Session 4

Client Security Solutions
- avast Software
- Spam Filtering
- Pop-Up Blocking
- Personal Firewalls
- HIDS

Virtualization and Security
- Virtualization Defined
- Benefits
- Scenarios
- Virtual PC
- Hyper-V
- VMware
- Planning
- Security Issues

Network Firewalls
- Understanding Firewalls
- Firewall Types
- Firewall Installation
- Well Known Ports
- Port Blocking

Network Security Design
- Subnetting
- Virtual LANs
- Connecting Networks
- DMZ
- NAT
- NAC

Telephony Security
- Traditional PBX
- VoIP
- SIP Security
- H.323 Security

Intrusion Detection and Prevention
- Intrusion Monitoring
- IDS Solutions
- Detection Methods
- IPS Solutions
- IPS Detection States
- Intrusion Indications
- IDS Implementations
- Intrusion Responses
- Honeypots

Controlling Internet Access
- Proxy Servers
- Internet Filters
- Creating a Firewall Rule

Protocol Analyzers
- Installing Wireshark
- Capturing E-mail Logon
- Creating HTTP Filter
- Viewing Passwords

LearnKey

Session 5

Wireless Network Security
- War Driving
- SSID Issues
- Rogue APs
- Weak Encryption
- Configuring WPA

Monitoring Systems
- Performance Tools
- Task Manager
- Performance Snap-In
- Baselines
- Creating a Baseline
- Creating a Second Baseline
- Comparing Baselines with Excel

Scanning the Network
- Port Scanning
- Angry IP Scanner
- Scanning Devices
- Service Enumeration
- Configuring Zenmap GUI
- Nmap Scanning

Vulnerability Scanning
- Sectools.org
- OVAL
- National Vulnerability Database
- Password Cracker
- Pen Testing

Logging and Auditing
- Importance of Logs
- DNS Logs
- System Logs
- Performance Logs
- Access Logs
- Firewall Logs
- Antivirus Logs
- Auditing

Cryptography 101
- Encryption
- Simple Encryption
- CIA
- Non-Repudiation
- Whole Disk
- Key Management
- Steganography
- Encryption Testing
- TPM

Encryption Algorithms
- Encryption Types
- Key Factors
- DES
- 3DES
- RSA
- ECC
- PGP
- AES
- RC4
- Secure Transfer
- One-Time Pad

LearnKey

Session 6

Encryption Protocols and Hashing
- Hashing
- Hashing Protocols
- Digital Signatures
- SSL/TLS
- TLS Goals
- SSL Operations
- PPTP
- L2TP
- IPSec
- HTTP Solutions
- SSH

Public Key Cryptography
- Certificates
- PK Cryptography
- PKI Components
- PKI Processes

Risk Assessments
- Risk Management
- Asset Identification
- Threat Identification
- Risk Assessment
- Risk Tracking

Redundancy Planning
- Failure Points
- RAID
- Spare Parts
- Redundant Servers
- Redundant ISP
- Power Supply
- Spare Sites

Incident Response
- Incident Defined
- IR Process
- First Responders
- Computer Forensics
- Chain of Custody
- Reporting
- Damage Control

Disaster Recovery
- Planning
- Backup Practices
- Backup Methods
- Backup Types
- Media Rotation
- Restoration
- DR Exercises

Social Engineering
- Definition
- Example Attacks
- Dumpster Diving
- Passive Attacks
- Inside/Outside Attacks
- Reverse
- Phishing Attacks

Security Policies
- Importance
- General Policies
- Functional Policies
- sans.org

LearnKey

Skills Assessment

Instructions: Rate your skills with the following tasks on a level from 1-5.

Skills	Poor 1	2	3	4	Excellent 5
Create User in a Batch File					
Replay Attack Steps					
Hijacking Steps					
Group Policy					
New User Creation					
Changing Security Templates					
Analyzing Security					
Firewall					
Adding Ports					
Adding and Blocking Ports					
Blocking a Service					
Wireshark Capture					
Set Baseline					
Log Files					
Configuring Angry IP Scanner					
Enabling Security Logging					
Response Steps					

Security Plus

Session 1

Session 1 Time Tables

Session 1	
Introduction	00:16:11
Security Requirements	00:19:24
Security Threats	00:19:25
Privilege Escalation	00:14:43
Hardware Security Risks	00:12:32
Network Vulnerabilities	00:10:50
Infrastructure Risks	00:22:23
Training Time	01:55:28

Session 1	
Introduction	
Security Requirements	00:29:0
Security Threats	
Privilege Escalation	00::22:0
Hardware Security Risk	00:18:48
Network Vulnerabilities	00:16:15
Infrastructure Risks	00:33:35
Training Time	02:53:20

Fill-in-the-Blanks

Instructions: While watching Session 1, fill in the missing words according to the information presented by the instructor.

Introduction

1. _____ is the kind of information that would be available at your Web site.
2. _____ is the information you keep inside your company; this data is generally the most valuable.

Security Requirements

1. Anytime we implement a security technology we _____ something.
2. Value does not just come from the cost of losing the data; it also comes from the loss if _____ gain that data.
3. The _____ is broken into two parts: information that is accessible to everyone within our organization and very sensitive information, to which only a select few people are allowed access.
4. One important thing with data is that you have the ability to _____ the data has been handled effectively.
5. Due diligence indicates the appropriate effort into _____ and _____ the due care procedures.
6. The requirement of a risk assessment is simple; you have to prove if you are a _____ and that you have measures in place to look for risks in your organization.
7. Due process helps to protect _____ and _____ within a regulatory domain.
8. Look at _____ first and then implement the appropriate security measures.

Security Threats

1. _____ help take care of the most common threats.
2. Viruses and worms can cost a tremendous amount of money in today's organization, but the cost of not protecting them is _____.
3. Trojans may come in under the guise of _____ or _____.
4. Once the rootkit is installed, the attacker has either an _____ into the environment or the rootkit will send information to the hacker from within the network.
5. Many of the e-mail servers have spam filters; for those that don't, there are _____ spam filter add-ons that can be purchased.
6. Attackers will try to find computers that are vulnerable; they will take them over and use portions of the _____ on those machines to do their cracking, their password attacks, or their distributed denial of service attacks.

Privilege Escalation

1. If capabilities of every user are limited, the likelihood of privilege escalation is _____.
2. The attacker will only be able to do what the _____ with which the attacker has gained access can do.
3. While social engineering may be used to escalate privileges, _____ may also be used.
4. A new exploit is _____ likely to be protected against in the targeted organization.
5. A logic bomb is an attack that is launched from _____, when the attacker has physical access to the machine.

Hardware Security

1. One of the primary areas of concern as a security administrator is the _____ in the organization.
2. Microsoft has implemented the ability to disable adding _____ through group policies.
3. If the USB ports are still available, a user could plug in a USB drive that has _____ on it and then install the _____, posing a potential threat.

Network Vulnerabilities

1. Some of the most important devices to secure in an environment are the very devices used to _____.
2. One of the key methods of protection for infrastructure equipment is using _____, because most devices use _____ for authentication, and do not
support any other kind of authentication.
3. Many of the default passwords can be located with a quick _____.
4. To hurt the entire network, take the _____ or _____ in such a way that it is no longer valuable to the users.
5. _____ is just as easy when it comes to a denial of service implementation as any of the old flooding attacks.
6. If the network is using older media types, something called _____ or _____, then a vampire tap could be utilized.

Infrastructure Risks

1. The network infrastructure is a very important part of a network; it includes the _____, the _____, and _____ that make up the core capability for users to communicate.
2. The infrastructure can be attacked _____ or via the _____.
3. The concept of the Null Session Attack has been around since the _____.
4. The first step in attacking anything is _____.
5. In a Man-in-the-Middle attack, the attacker sits between the _____ and the _____**,** potentially taking over the session.
6. Replay attacks are broken into three phases: _____, _____, and _____.
7. If you have redundant Internet connections, simply _____ the connection through which the distributed denial of service attack is coming.
8. The only way to ensure a distributed denial of service attack has been stopped is to subscribe to an _____.
9. When registering a domain name on the Internet, you are given a _____.
10. The attacker will use the ARP poisoning method to get devices to communicate with the _____, instead of a router on the machine's network.

Glossary Crossword

Instructions: Use the terms and clues below to complete the crossword puzzle.

Acceptable Use
Back Door
BIOS
Botnets
Cybercrime
DoS
Due Care
Due Process
Social Engineering
Spoofing
Spyware
Trojan Horse
Vampire Tap
Virus
Worm

Across

3. Software that is used to configure and provide an interface between software and hardware on a computer, also refers to the firmware code that runs when a computer is powered on in order to boot the machine.

6. An attack method in which an attacker restricts access to a network, Web site, or other computer system or component. This may be achieved by flooding, exploiting application code errors, or hardware destruction.

8. A set of rules or guidelines that define allowable actions in relation to computers and associated components such as software, services, networks, and others.

9. The act of using a different identity to mask activities.

12. A malicious or destructive application, program, or code that presents itself as a helpful application.

13. Any illegal activity that is initiated or achieved using computers and associated components.

Down

1. An attack method used to gain information that relies on human tendencies, such as perception and trust.

2. A set of guidelines that protects information such as patient records, customer information, and legal documentation of any kind.

3. A group of computers or networks that are in control of an attacker.

4. An application or software that gathers information about a user or an organization without their knowledge or informed consent.

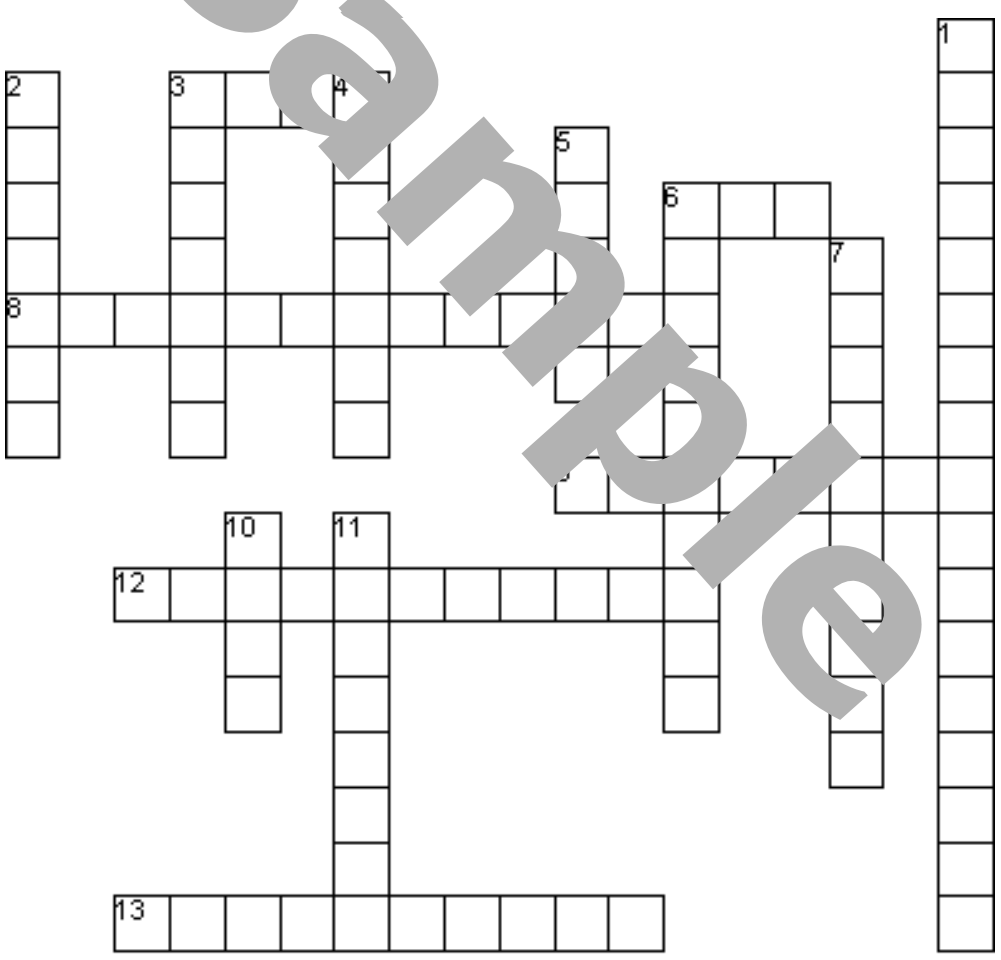
5. Any program with a malicious or destructive purpose.

6. A law principle that guarantees fair and equal legal rights for individuals and organizations.

7. A device that is used to obtain access to the electromagnetic waves within a coaxial cable by penetrating the cable with a pointed needle.

10. A malicious or destructive program that is self-promulgating.

11. An opening left in a program that can allow access to a system, or an application installed on a

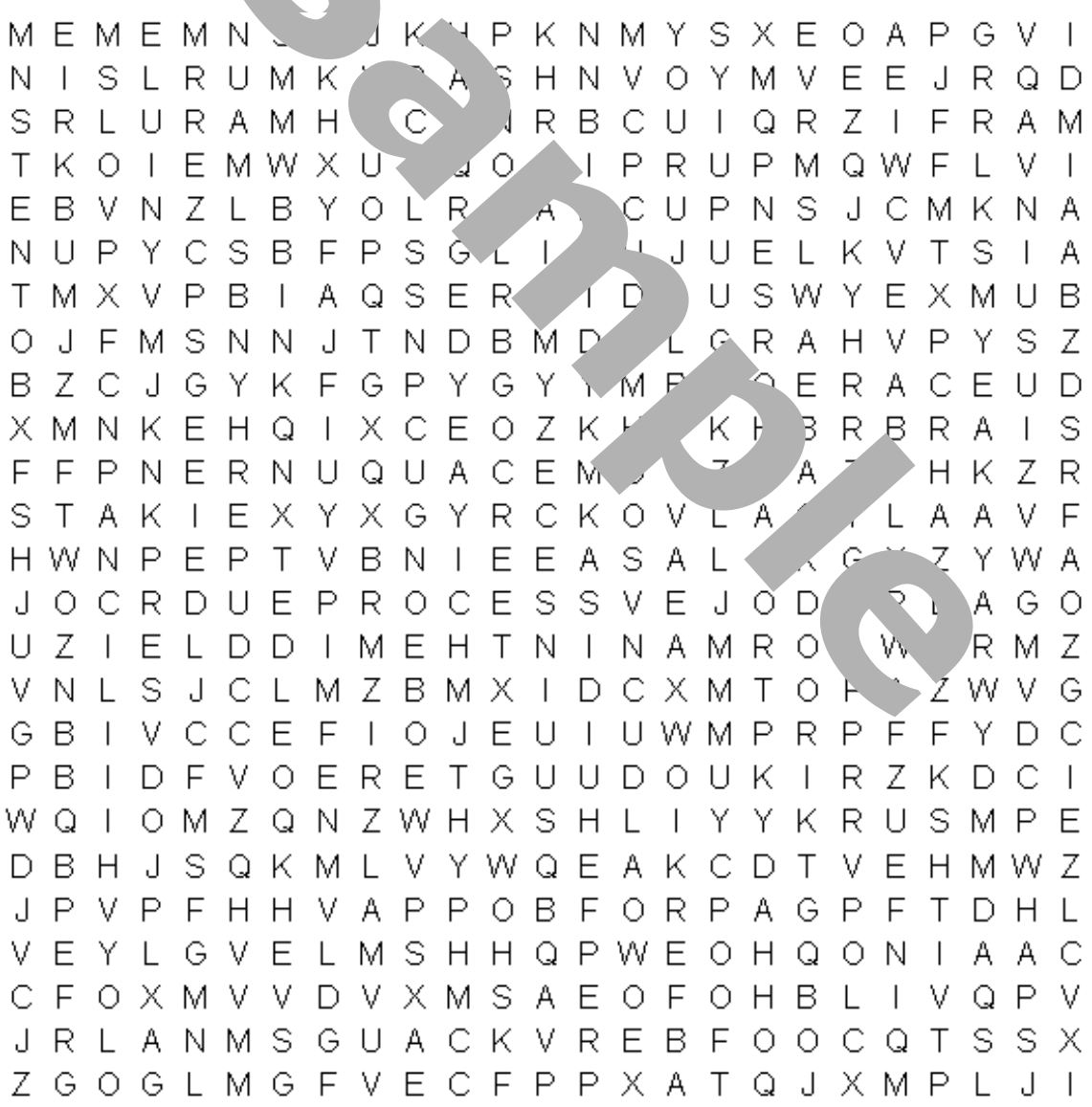


Glos- sary Word Search

Instructions: Use the clues below to complete the word

ceptable Use
Back Door
BIOS
Botnets
Cybercrime
DoS
Due Care
Due Process
Social Engineering
Spoofing

Ac-



LearnKey

Short Answer

Instructions: Use the information learned while watching Session 1 to answer the questions.

1. Describe data classification and how it affects your security measures.

2. Explain what three factors are key when doing a risk assessment of security threats.

3. Compare virus, worm, Trojan, and spyware.

4. Describe some methods by which an attacker might try to escalate privileges on a system?

5. Why would an attacker wish to escalate user privileges?

6. What are the risks of an unsecured USB port?

7. Explain some vulnerabilities to which network devices might be susceptible?

8. Give some examples of infrastructure risks and mention how they work.

LearnKey

Glossary Matching

Instructions: Match the glossary term described in Session 1 to its definition.

a.	BIOS	f.	vampire tap	k.	botnets
b.	due process	g.	Trojan Horse	l.	social engineering
c.	Man-in-the-Middle	h.	cyber crime	m.	spyware
d.	backdoor	i.	virus	n.	acceptable use
e.	worm	j.	due care	o.	spoofing

1. ___ An opening left in a program that can allow access to a system or an application installed on a machine that can provide access to crackers.

2. ___ Any illegal activity that is initiated or achieved using computers and associated components.

3. ___ A set of guidelines that protects information such as patient records, customer information, and legal documentation of any kind.

4. ___ A law principle that guarantees fair and equal legal rights for individuals and organizations.

5. ___ A set of rules or guidelines that define allowable actions in relation to computers an associated components such as software, services, networks, and others.

6. ___ Any program with a malicious or destructive purpose.

7. ___ A malicious or destructive program that is self-promulgating.

8. ___ A malicious or destructive application, program, or code that presents itself as a helpful application.

9. ___ An application or software that gathers information about a user or an organization without their knowledge or informed consent.

10. ___ A group of computers or networks that are in control of an attacker.

11. ___ An attack method used to gain information that relies on human tendencies, such as perception and trust.

12. ___ Software that is used to configure and provide an interface between software and hardware on a computer.

13. ___ An attack method in which an attacker restricts access to a network, Web site, or other computer system or component.

14. ___ A device that is used to obtain access to the electromagnetic waves within a coaxial cable by penetrating the cable with a pointed needle.

15. ___ The act of using a different identity to mask activity.

16. ___ An attack method where the attacker places a machine or application between two valid devices for the purpose of listening to or manipulating communications.

Research Topic

Instructions: Research the topic below using the Internet and then write a few paragraphs reporting your findings. Be sure to research thoroughly and site your resources. This page may be used to take notes.

You can find many "Threat Lists" on the Internet, some more useful than others. They are a good start at knowing what to guard against on your network.

A. Find three security "Threat Lists" on the Internet and document how useful you find each list. How does each site rate the threats? How are threats summarized? Can you drill down into particular threats to get greater detail? How detailed do they get?

B. Choose one threat that appears on all three lists and describe it. How does it work? Who is most vulnerable? Identify what steps IT support personnel would take to combat this threat.

Write a truthful but simplified executive summary that a CIO (chief information officer) could use to explain the problem to end-users and customers.

Individual Project

Instructions: Assign each student the following project. Each student should prepare a short 5-10 minute class presentation of the information researched.

Research how to perform a man-in-the-middle attack on a network and then determine what measures could help protect against the method you found.

Group Projects

Instructions: Divide into groups and assign each group one of the following subjects to research. Each group should prepare a short 5-10 minute class presentation of the information researched.

1. Select a software package or operating system to research and find one vulnerability in that software. Vulnerability meaning a software bug that could be exploited by a person with malintent. How does the exploit work? What kind of programming mistake did the software developer make? Cite your sources.

2. Research botnets. What are the various uses for a botnet? How are they controlled? What steps can be taken to help eliminate the threat of botnets?

Session 1 Quiz

Instructions: Circle the letter of the option that BEST answers the question.

1. Which types of technical information security experiences are recommended before taking the Security+ certification? Choose all that apply.
   A. Permissions
   B. Defining groups
   C. Configuring firewalls
   D. Defining user accounts

2. Which concepts are associated with the organizational security knowledge domain? Choose all that apply.
   A. Encryption algorithms
   B. Disaster recovery plans
   C. Securing routers and switches
   D. Standard operating procedures and policies

3. Which concept deals with the value of perception?
   A. Brand equity
   B. Hardware quality
   C. Password strength
   D. Tampering with screen resolution

4. What is the first step to securing a system?
   A. Downloading updates
   B. Analyzing requirements
   C. Clearing machines of all pre-existing data

5. The majority of information fits into which information class?
   A. Public
   B. Internal
   C. Restricted

6. Which term is used to describe individuals taking care to avoid negligence when carrying out information protection duties?
   A. Due care
   B. Due process
   C. Due diligence
   D. Due acknowledgements

7. Fair treatment, equality, and the opportunity to explain scenarios fit under which category?
   A. Due care
   B. Due process
   C. Due diligence
   D. Due acknowledgements

9. Which term is used to describe the measurement of predictability?
   A. Severity
   B. Likelihood
   C. Detectability

10. How are Trojan horses generally received?
    A. Hackers injecting code into Web sites
    B. Through password bypassing software
    C. Presented as, or bundled with, a helpful application

11. Which feature of Kerio MailServer displays checked messages, tagged messages, and rejected messages?
    A. Results
    B. Statistics
    C. Scheduling
    D. Traffic charts

12. Which are steps in privilege escalation? Choose all that apply.
    A. Initial entry
    B. Finding holes
    C. Testing privileges
    D. Escalating privileges

13. An attacker can place a logic bomb in place of a commonly used executable.
    A. True
    B. False

14. Which term is used to describe software that configures the hardware in a computer?
    A. BIOS
    B. DOSS
    C. InWare
    D. SoftBoot

15. Which are features associated with BIOS? Choose all that apply.
    A. Boot passwords
    B. Change BIOS settings
    C. BIOS access passwords
    D. Enable or disable network boot options through BIOS settings

16. Stealing a thumb drive is an example of which type of threat?
    A. Data theft
    B. Software injection
    C. Social engineering

17. Which attack methods may be used with Network-Attached Storage? Choose all that apply.
    A. Denial of service
    B. Malware injection
    C. Rootkit installation
    D. Configuration attacks

18. Which device is used to rebuild communications as frequency shifts occur?
    A. Analog regenerator
    B. Digital trunking scanner
    C. Network sniffer application
    D. Connectivity modification emission

19. Which describe the functions of a backdoor? Choose all that apply.
    A. An application that provides access to crackers
    B. A network-based database that provides hash decryption
    C. An opening left in a program that allows additional access
    D. An operating system configuration that allows multiple user logon

20. Which device attempts to make a connection by surrounding and penetrating a cable in order to access electromagnetic wave transmission?
    A. Eclipse box
    B. Vampire tap
    C. Werewolf clamp
    D. Twilight trapper

21. What aspect of an Intrusion Detection System (IDS) is the simplest yet least flexible method of protection against network-born malware?
    A. Pattern matching
    B. Stateful inspection
    C. Protocol decode analysis
    D. Heuristic analysis

22. A security vulnerability of Terminal Access Controller Access Control System (TACACS+) is that accounting information is sent in _____.
    A. RC4 encryption
    B. Cleartext transmission
    C. MD5 digests
    D. TACACS format

23. Which are reasons why you should be concerned with e-mail spam? Choose all that apply.
    A. It violates US federal law
    B. It threatens physical server room security
    C. It blocks Internet access
    D. It consumes computer and network resources

24. File Transfer Protocol (FTP) uses TCP ports ____ and ____.
    A. 21, 22
    B. 19, 20
    C. 25, 110
    D. 20, 21

25. Which type of attack is triggered by an event or process?
    A. A virus
    B. A worm
    C. A Trojan horse
    D. A logic bomb

26. Which of the three major security topology types creates a basic firewall gateway that can use specialized hardware (e.g., Cisco PIX), a router running ACLs, or a computer running UNIX or Windows?
    A. Bastion host
    B. Screened host gateway
    C. Screened subnet gateway
    D. Circuit-level gateway

27. What is the primary characteristic of a polymorphic virus?
    A. The ability to hide from detection software
    B. The ability to lie dormant until triggered
    C. The ability to cause damage to word processors
    D. The ability to change its internal code

28. What is the primary concern regarding backdoor access?
    A. Backdoors are never used
    B. Backdoors destroy legitimate code
    C. Backdoors are always malicious
    D. Backdoors are undocumented

29. TCP/IP replay attacks are possible due to which weaknesses or vulnerabilities?
    A. Weak entropy pools
    B. Weak TCP sequence numbers
    C. Weak authentication schemes
    D. Weak user-awareness

30. Which attack involves appearing as an authorized source to gain access into a network?
    A. Masquerading
    B. Brute force
    C. Man-in-the-Middle
    D. IP spoofing

Backdoors

Security Plus

- Backdoors are defined in two ways
  - An opening left in a program allowing additional access to the software or system
  - An application that can be [illegible] on a machine to provide access [illegible]
    - Back Orifice
    - NetBus

Notes:

Viruses and Worms

Security Plus

- A virus is any malicious program
  - Traditional viruses include boot sector, program, and macro viruses
  - Usually depend on human actions to promulgate
- A worm is like a virus without the need for human interaction
  - Self-promulgating
  - Many are self-adjusting

Notes:

Denial of Service

Security Plus

- A DoS attack comes in two forms
  - Single DoS
    - A single machine is used to launch an attack
  - DDoS (distributed denial of service)
    - Dozens, hundreds, or thousands of machines are used to launch an attack

Notes: