CPT Prep

Hardware keyloggers can be detected via software

A. True
B. False

Hardware keyloggers can be detected via software

False

A penetration tester will always discover vulnerabilities during a penetration test?

A. True
B. False

A penetration tester will always discover vulnerabilities during a penetration test?

False

The File Transfer Protocol (FTP) can run only on port 21

A. True
B. False

The File Transfer Protocol (FTP) can run only on port 21

False

Vulnerability assessment is the use of automated vulnerability scanning tools to identify gaps in the security posture.

A. True
B. False

Vulnerability assessment is the use of automated vulnerability scanning tools to identify gaps in the security posture.

True

Remote vulnerabilities can be exploited:

A. Without any legitimate access to the target system
B. Only with legitimate access to the target system

Remote vulnerabilities can be exploited:

A. Without any legitimate access to the target system

Keyloggers can be part of a Trojan:

A. True
B. False

Keyloggers can be part of a Trojan:

True

During a penetration test, you will find the following MD5 hash: 701bf1b91eb77ff6cde3f70b780ae32d. The plaintext for this message digest can be discovered by?

A. Brute force attack
B. Recovering the MD5 private key that created the hash

During a penetration test, you will find the following MD5 hash: 701bf1b91eb77ff6cde3f70b780ae32d. The plaintext for this message digest can be discovered by?

A. Brute force attack

Penetration testers should always have authorization from the proper authority when performing a penetration test.

A. True
B. False

Penetration testers should always have authorization from the proper authority when performing a penetration test.

A. True

A modern processor can distinguish instructions from data:

A. True
B. False

A modern processor can distinguish instructions from data:

B. False

A proof of concept is the same as an exploit:

A. True
B. False

A proof of concept is the same as an exploit:

A. True

The LAN Manager hashing algorithm uses the same DES key for every instance of it?

A. True
B. False

The LAN Manager hashing algorithm uses the same DES key for every instance of it?

B. True

The LAN Manager algorithm is weak because:

A. It stores passwords in unencrypted format
B. It converts all passwords to upper case
C. It is a secure replacement for NTLM, and NTLM has weaknesses inherent in it
D. It can only store passwords of 21 characters in length

The LAN Manager algorithm is weak because:

B. It converts all passwords to upper case

Trojans can be detected by which two means:

A. Examining contents of the registry, Antivirus
B. Antivirus, network IDS/IPS
C. Removing the registry, network IDS/IPS
D. Network port monitors, network IDS/IPS

Trojans can be detected by which two means:

B. Antivirus, network IDS/IPS

The purpose of passive intelligence gathering is to:

A. Use active port scanning intelligence gathering tools to determine information about your target organization
B. Find employees that work at the target organization
C. Determine email addresses of employees working at the target organization
D. Determine information about your target organization without alerting them

The purpose of passive intelligence gathering is to:

D. Determine information about your target organization without alerting them

Information Leakage vulnerabilities always:

A. Allow the attacker to gain control of the attacked system
B. Allow the attacker to deny service to legitimate users of the attacked system
C. Are the result of SQL injection vulnerabilities
D. Allow the attacker to gather sensitive or potentially damaging information

Information Leakage vulnerabilities always:

D. Allow the attacker to gather sensitive or potentially damaging information

Which of the following protocols can have their authentication information sniffed?

A. FTP, SSH, HTTP, POP
B. FTP, Telnet, HTTP, POP
C. FTP, Telnet, HTTP, SSL
D. FTP, Telnet, HTTPS, POP

Which of the following protocols can have their authentication information sniffed?

B. FTP, Telnet, HTTP, POP

The nmap tool is capable of performing the following scan types:

A. TCP Connect, TCP Syn/Stealth, UDP
B. TCP Reverse Connect, TCP Syn/Stealth, UDP
C. TCP Connect, TCP Smack, UDP
D. TCP Connect, TCP Syn/Stealth, IGRP

The nmap tool is capable of performing the following scan types:

A. TCP Connect, TCP Syn/Stealth, UDP

You attempt to do a banner grabbing attempt on a webserver. The banner is reported as: Apache/1.3.27. What do you know at this point?

A. It is not known at this point in time because banners can be forged
B. Apache/1.3.27, because banners cannot be forged
C. Apache/1.3.25, because Apache always reports a banner two revisions newer than what it actually is
D. IIS 5.0 with the Microsoft Banner Obscurity Service running

You attempt to do a banner grabbing attempt on a webserver. The banner is reported as: Apache/1.3.27. What do you know at this point?

A. It is not known at this point in time because banners can be forged

John the ripper is a fast password cracker because it has a very efficient type of algorithm. It implements which cracking mode by default?

A. Brute Force
B. Native mode
C. Hybrid
D. Dictionary

John the ripper is a fast password cracker because it has a very efficient type of algorithm. It implements which cracking mode by default?

C. Hybrid

On modern Linux systems, the user password hashes are stored in:

A. The /etc/passwd file
B. The /etc/hashes file
C. The /etc/shadow file
D. The /etc/password file

On modern Linux systems, the user password hashes are stored in:

C. The /etc/shadow file

Tracerouting with the TCP protocol is useful for penetration testers because:

A. It allows you to forge ICMP echo reply requests via TCP headers
B. It allows you to forge ICMP Response header requests via TCP headers
C. It allows you to use TCP protocol which is more likely to be allowed through firewalls and gateway
D. It allows you to use TCP protocol which is not stateful and therefore more stealthy than other protocol

Tracerouting with the TCP protocol is useful for penetration testers because:

C. It allows you to use TCP protocol which is more likely to be allowed through firewalls and gateway

Word gets out that you have recently achieved the CPT certification. You receive an email from a person named Abe, asking you to conduct a pen test. Abe says that he has authorization to the computer, because he owns it, even though his ex-wife is currently in possession of the computer he wants you to attack. How do you respond to the email?

A. Ask Abe for more details about his ex-wife, and begin the penetration test
B. Get in touch with Abe's ex-wife and determine if he really has authorization to order a penetration test
C. Ignore the email because there is no way to determine if Abe really has authorization to his ex-wife's computer
D. Send Abe a price quote of $25,000 for the penetration test, if he pays, begin the penetration test

Word gets out that you have recently achieved the CPT certification. You receive an email from a person named Abe, asking you to conduct a pen test. Abe says that he has authorization to the computer, because he owns it, even though his ex-wife is currently in possession of the computer he wants you to attack. How do you respond to the email?

C. Ignore the email because there is no way to determine if Abe really has authorization to his ex-wife's computer

WEP can be broken regardless of the key strength because:

A. It relies on the RC4 encryption algorithm which requires non-randomized Initialization Vectors (IVs). The IV in WEP is randomized.
B. It relies on the RC4 encryption algorithm which requires randomized Initialization Vectors (IVs). The IV in WEP is non-randomized.
C. It relies on the RSA encryption algorithm which requires randomized Initialization Vectors (IVs). The IV in WEP is randomized.
D. It relies on the RSA encryption algorithm which requires non-randomized Initialization Vectors (IVs). The IV in WEP is non-randomized.

WEP can be broken regardless of the key strength because:

B. It relies on the RC4 encryption algorithm which requires randomized Initialization Vectors (IVs). The IV in WEP is non-randomized.

When performing a penetration test, you are likely to use a buffer overflow attack. How does a buffer overflow work?

A. By rewriting kernel object memory structures to redirect user input to a in-process terminal memory
B. By obfuscating the ring-O device I/O memory address structure stack bit, only when set properly with
C. By overflowing Structured Exception Handlers only
D. By having overflowed data copy over data that is used to control the execution of the vulnerable program.

When performing a penetration test, you are likely to use a buffer overflow attack. How does a buffer overflow work?

D. By having overflowed data copy over data that is used to control the execution of the vulnerable program.

A penetration test seeks to determine risk to an organization by:

A. Identifying existing vulnerabilities in network and systems
B. Determining existing vulnerabilities in network and systems by heuristics analysis
C. Determining existing vulnerabilities in network and systems by completing a NIST scoring sheet.
D. Exploiting existing vulnerabilities in networks and systems

A penetration test seeks to determine risk to an organization by:

D. Exploiting existing vulnerabilities in networks and systems

What is the possible range of port numbers for TCP and UDP ports?

A. 1-65535
B. 2-1024
C. 0-1024
D. 0-65535

What is the possible range of port numbers for TCP and UDP ports?

A. 1-65535
D. 0-65535

Technically, RFC1700, Oct 94 states: 0-65535 TCP/UDP ports. That 0 TCP/UDP is reversed, but it does exist. Pick your poison, my first choice is D.

Bob your neighbor has been accused of port scanning a server on the internet owned by a very litigious corporation. Bob thinks it is possible that someone could have used his computer to perform the attack. You mention Idle Scanning to him, because Idle Scans ____

A. Idle scanning does not allow you to spoof the source of a port scan
B. By bouncing the request off of a quiet zombie host and monitoring IPID changes in the IP header
C. By bouncing the request off of a server running FTP and monitoring IPID changes in the IP header
D. By spoofing the destination IP address of the targeted system

Bob your neighbor has been accused of port scanning a server on the internet owned by a very litigious corporation. Bob thinks it is possible that someone could have used his computer to perform the attack. You mention Idle Scanning to him, because Idle Scans ____

B. By bouncing the request off of a quiet zombie host and monitoring IPID changes in the IP header

The netcraft determines the web server type and version by:

A. Sending an ICMP echo request ping
B. Sending a TCP version ping
C. Processing banner information received from the web server
D. Processing banner information sent to the web server

The netcraft determines the web server type and version by:

C. Processing banner information received from the web server

TCP Connection scanning does which of the following:

A. Forges source IP addresses
B. Forges destination IP addresses
C. Does not complete the 3 way handshake
D. Completes the 3 way handshake

TCP Connection scanning does which of the following:

C. Does not complete the 3 way handshake

D. Completes the 3 way handshake

Both conditions exist depending on the state of the port (open/closed). High probably they are looking for “D. Completes the 3 way handshake.”

In relation to penetration testing, the acronym DoS refers to what?

A. Degradation of Service
B. Desecration of Service
C. Denial of System
D. Denial of Service

In relation to penetration testing, the acronym DoS refers to what?

D. Denial of Service

After your CPT training, you discover a vulnerability in a piece of critical software. Your colleagues tell you that you should consider Responsible Disclosure. What is Responsible Disclosure?

A. Letting the software vendor know that the vulnerability has been discovered before discovered before releasing the vulnerability to the public
B. Informing the public as soon as possible and not informing vendors
C. The only ethical and moral way to release vulnerabilities
D. Never letting the public know about a vulnerability, because hackers are members of the public and could learn about the vulnerability

After your CPT training, you discover a vulnerability in a piece of critical software. Your colleagues tell you that you should consider Responsible Disclosure. What is Responsible Disclosure?

A. Letting the software vendor know that the vulnerability has been discovered before releasing the vulnerability to the public

As a candidate for the CPT certification, you are hired for a penetration test by Bob's Widget Factory. You notice the website is hosted at a 3rd party hosting company not controlled by the Bob's Widget Factory

A. Inform the hosting provider that you will be performing a penetration test, and begin the test
B. Do not inform Bob's Widget Factory as it is acceptable to run penetration tests against outsourced 3rd
C. Report these findings to Bob's Widget Factory and recommend they request authorization for the test from the 3rd Party
D. Report the owner of Bob's Widget Factory to the local authorities

As a candidate for the CPT certification, you are hired for a penetration test by Bob's Widget Factory. Bob's _____test, you notice the website is hosted at a 3rd party hosting company not controlled by the Bob's Widget Factory

C. Report these findings to Bob's Widget Factory and recommend they request authorization for the test from the 3rd Party

Which of the following are valid vulnerability types:

A. Protecting sensitive data, Loss of system control, Loss of system availability
B. Leaking sensitive data, Gain of system interdepenance, Loss of system availability
C. Leaking sensitive data, Loss of system control, Loss of system availability
D. Protecting sensitive data, Loss of system control, Increasing availability

Which of the following are valid vulnerability types:

C. Leaking sensitive data, Loss of system control, Loss of system availability

In order to sniff on a switch, you will need to have a tool that performs which type of attack:

A. ARP spoofing
B. Port stealing
C. RARP spoofing
D. ICMP spoofing

In order to sniff on a switch, you will need to have a tool that performs which type of attack:

A. ARP spoofing

The RFCs are:

A. A series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies
B. A series of standards developed by a consortium led by Microsoft, Sun, and IBM applicable to Internet technologies
C. A series of standards developed by Microsoft applicable to Internet technologies
D. A series of standards developed by the University of Wisconsin applicable to Internet technologies

The RFCs are:

A. A series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies

ICMP tunneling works as a covert channel because:

A. ICMP is not able to be parsed by most IDS/IPS solutions on the market
B. ICMP cannot be used as a cover channel because it cannot contain data as specified under the RFC
C. ICMP is not meant to be data transmission protocol and may not be monitored for traffic
D. ICMP is a layer specific protocol and is not monitored

ICMP tunneling works as a covert channel because:

C. ICMP is not meant to be data transmission protocol and may not be monitored for traffic

Netcat can be used to:

A. Launch a DoS attack via the –p setting
B. Connect to other programs, just like a Telnet client
C. Encrypt session traffic
D. Allow IRC clients to connect to it and work as a fully functional IRC server

Netcat can be used to:

B. Connect to other programs, just like a Telnet client

Your manager wants you to complete the CEPT exam after you have achieved the CPT exam. What is“shellcode”?

A. Very simple opcodes that are injected into another processes’ address space
B. The new shell scripting interface for Windows Vista
C. A scripting language that is used to write shell scripts for Unix
D. Code that is put in place to find the valid shell for an exploit

Your manager wants you to complete the CEPT exam after you have achieved the CPT exam. What is“shellcode”?

A. Very simple opcodes that are injected into another processes’ address space

The four types of Denial of Service vulnerabilities are:

A. Local, remote, Resource exhaustion attacks, System flaws that allow an arbitrary crash
B. Local, remote, Resource discovery attacks, System settings that are configured improperly
C. Local, remote, Resource discovery attacks, System flaws that allow loss of control
D. Local, internal, Resource exhaustion attacks, System flaws that allow an arbitrary crash

The four types of Denial of Service vulnerabilities are:

A. Local, remote, Resource exhaustion attacks, System flaws that allow an arbitrary crash

Local vulnerabilities can also be generally described as:

A. Privilege de-escalation vulnerabilities
B. Privilege escalation vulnerabilities
C. Remote Vulnerabilities
D. Drive by and click vulnerabilities

Local vulnerabilities can also be generally described as:

B. Privilege escalation vulnerabilities

On Windows, the LSA Secrets is a:

A. Possible location of the repair SAM file
B. Possible location of the live SAM file
C. The location of the Active Directory hash store
D. Registry locations that contains cached login passwords in clear text

On Windows, the LSA Secrets is a:

D. Registry locations that contains cached login passwords in clear text

Smashing the Stack for Fun and Profit was an important document that detailed how to perform:

A. A heap-based buffer overflow
B. A recompiled stack smashing routine for positive memory variance
C. An exploit for linux kernel memory structures
D. A stack-based buffer overflow and write shellcode

Smashing the Stack for Fun and Profit was an important document that detailed how to perform:

D. A stack-based buffer overflow and write shellcode

A secure replacement for netcat is:

A. Cryptcat
B. Cryptonetocato
C. Netcatcrypt
D. Catcrypt

A secure replacement for netcat is:

A. Cryptcat

During a penetration test, you find a server running a web server on Port 80. Port 80 is in an open state. You send a SYN ACK packet to port 80. What is the expected response?

A. A TCP RST packet
B. A TCP SYN packet
C. A TCP SYN ACK packet
D. A TCP ACK ACK packet

During a penetration test, you find a server running a web server on Port 80. Port 80 is in an open state. You send a SYN ACK packet to port 80. What is the expected response?

A. A TCP RST packet

UDP is not a connection oriented or stateful protocol because it does not contain:

A. A 3 Way Handshake to establish connections
B. Port numbers above 1024
C. A larger header than TCP
D. A memory resident buffer state table in the protocol

UDP is not a connection oriented or stateful protocol because it does not contain:

A. A 3 Way Handshake to establish connections

Your manager wants you to perform either a vulnerability assessment or a penetration test, but does not know to justify why. Vulnerability assessment is different from penetration testing because:

A. It tests conclusively for vulnerabilities and verifies their existence, whereas penetration testing does
B. Vulnerability assessment uses only manual techniques, while penetration testing uses only tools
C. Vulnerability assessment uses only tools, while penetration testing uses only manual techniques
D. It tests only for vulnerabilities that could exist, but does not conclusively verify their existence

Your manager wants you to perform either a vulnerability assessment or a penetration test, but does not know to justify why. Vulnerability assessment is different from penetration testing because:

D. It tests only for vulnerabilities that could exist, but does not conclusively verify their existence

You are instructed by your manager to perform a penetration test against a system protected by a firewall. You can use a tool to determine the ruleset on the firewall using ICMP responses. What could this penetration testing technique be using?

A. Firewall Scanning
B. Firewalking
C. Portscanning
D. Walking with the fire

You are instructed by your manager to perform a penetration test against a system protected by a firewall. You can use a tool to determine the ruleset on the firewall using ICMP responses. What could this penetration testing technique be using?

B. Firewalking

Your company is concerned about a news report of a zero day attack. What is this zero day attack?

A. A very quick attack that takes less than one day to complete
B. A private exploit for vulnerability that has not been disclosed to the software vendor or the general public
C. An attack that occurs every year on the first day of the new year
D. A bit of hacker fiction used to scare consumers into purchasing more security products for their computer

Your company is concerned about a news report of a zero day attack. What is this zero day attack?

B. A private exploit for vulnerability that has not been disclosed to the software vendor or the general public

If a port is closed, the response from a FIN scan will be:

A. A TCP/SYN packet
B. A TCP/RST packet
C. No response
D. A UPD resolve packet

If a port is closed, the response from a FIN scan will be:

B. A TCP/RST packet