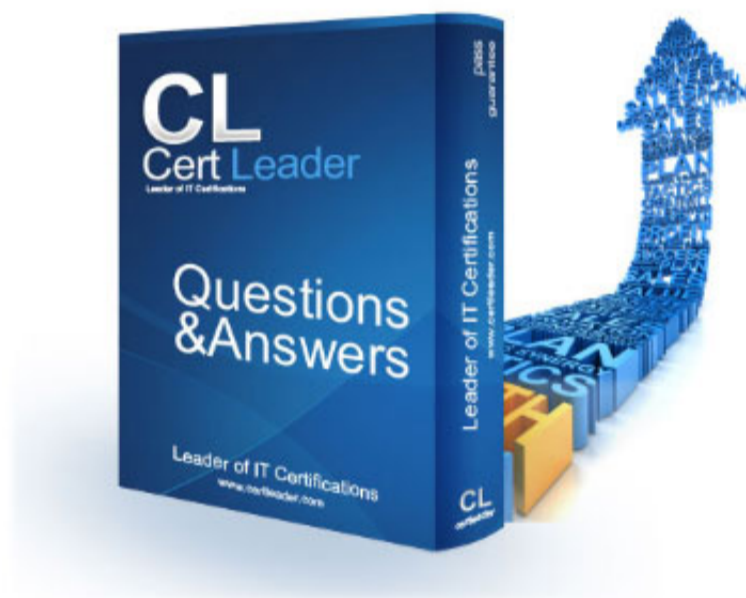


312-50v10 Dumps

Certified Ethical Hacker v10

<https://www.certleader.com/312-50v10-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

- A. Regularly test security systems and processes.
- B. Encrypt transmission of cardholder data across open, public networks.
- C. Assign a unique ID to each person with computer access.
- D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

- A. Event logs on the PC
- B. Internet Firewall/Proxy log
- C. IDS log
- D. Event logs on domain controller

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

Which of the below hashing functions are not recommended for use?

- A. SHA-1.ECC
- B. MD5, SHA-1
- C. SHA-2. SHA-3
- D. MD5. SHA-5

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company. What is the main security risk associated with this scenario?

- A. External script contents could be maliciously modified without the security team knowledge
- B. External scripts have direct access to the company servers and can steal the data from there
- C. There is no risk at all as the marketing services are trustworthy
- D. External scripts increase the outbound company data traffic which leads greater financial losses

Answer: A

NEW QUESTION 5

- (Exam Topic 1)

Code injection is a form of attack in which a malicious user:

- A. Inserts text into a data field that gets interpreted as code
- B. Gets the server to execute arbitrary code using a buffer overflow
- C. Inserts additional code into the JavaScript running in the browser
- D. Gains access to the codebase on the server and inserts new code

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

- A. SSH communications are encrypted it's impossible to know who is the client or the server
- B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
- C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
- D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

Darius is analysing IDS logs. During the investigation, he noticed that there was nothing suspicious found and an alert was triggered on normal web application traffic. He can mark this alert as:

- A. False-Negative
- B. False-Positive
- C. True-Positive
- D. False-Signature

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- A. My Doom
- B. Astacheldraht
- C. R-U-Dead-Yet?(RUDY)
- D. LOIC

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

- A. Traffic is Blocked on UDP Port 53
- B. Traffic is Blocked on UDP Port 80
- C. Traffic is Blocked on UDP Port 54
- D. Traffic is Blocked on UDP Port 80

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

- A. Double quotation
- B. Backslash
- C. Semicolon
- D. Single quotation

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Human intelligence
- C. Social intelligence
- D. Real intelligence

Answer: A

NEW QUESTION 14

- (Exam Topic 1)

Which of the following provides a security professional with most information about the system's security posture?

- A. Wardriving, warchalking, social engineering
- B. Social engineering, company site browsing, tailgating
- C. Phishing, spamming, sending trojans
- D. Port scanning, banner grabbing, service identification

Answer: D

NEW QUESTION 17

- (Exam Topic 1)

Which of the following program infects the system boot sector and the executable files at the same time?

- A. Stealth virus
- B. Polymorphic virus
- C. Macro virus
- D. Multipartite Virus

Answer: D

NEW QUESTION 19

- (Exam Topic 1)

Which of the following is the best countermeasure to encrypting ransomwares?

- A. Use multiple antivirus softwares
- B. Keep some generation of off-line backup
- C. Analyze the ransomware to get decryption key of encrypted data
- D. Pay a ransom

Answer: B

NEW QUESTION 23

- (Exam Topic 1)

Which of the following steps for risk assessment methodology refers to vulnerability identification?

- A. Determines if any flaws exist in systems, policies, or procedures
- B. Assigns values to risk probabilities; Impact values.
- C. Determines risk probability that vulnerability will be exploited (Hig
- D. Medium, Low)
- E. Identifies sources of harm to an IT syste
- F. (Natural, Huma
- G. Environmental)

Answer: C

NEW QUESTION 28

- (Exam Topic 1)

Nedved is an IT Security Manager of a bank in his country. One day, he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

What is the first thing that Nedved needs to do before contacting the incident response team?

- A. Leave it as it is and contact the incident response team right away
- B. Block the connection to the suspicious IP Address from the firewall
- C. Disconnect the email server from the network
- D. Migrate the connection to the backup email server

Answer: C

NEW QUESTION 32

- (Exam Topic 1)

Trinity needs to scan all hosts on a /16 network for TCP port 445 only. What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.

- A. nmap -sn -sF 10.1.0.0/16 445
- B. nmap -p 445 -n -T4 --open 10.1.0.0/16
- C. nmap -s 445 -sU -T5 10.1.0.0/16
- D. nmap -p 445 --max -Pn 10.1.0.0/16

Answer: B

NEW QUESTION 36

- (Exam Topic 1)

What is the least important information when you analyze a public IP address in a security alert?

- A. ARP
- B. Whois
- C. DNS
- D. Geolocation

Answer: A

NEW QUESTION 37

- (Exam Topic 1)

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. Suicide Hacker
- B. Black Hat
- C. White Hat
- D. Gray Hat

Answer: D

NEW QUESTION 41

- (Exam Topic 1)

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

- A. SQL injection attack
- B. Cross-Site Scripting (XSS)
- C. LDAP Injection attack
- D. Cross-Site Request Forgery (CSRF)

Answer: B

NEW QUESTION 44

- (Exam Topic 1)

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

- A. nslookup -fullrecursive update.antivirus.com
- B. dnsnoping -rt update.antivirus.com
- C. nslookup -norecursive update.antivirus.com
- D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 49

- (Exam Topic 1)

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

What kind of Web application vulnerability likely exists in their software?

- A. Host-Based Intrusion Detection System
- B. Security through obscurity
- C. Defense in depth
- D. Network-Based Intrusion Detection System

Answer: C

NEW QUESTION 52

- (Exam Topic 1)

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.

Which of the following types of firewalls can protect against SQL injection attacks?

- A. Data-driven firewall
- B. Stateful firewall
- C. Packet firewall
- D. Web application firewall

Answer: D

NEW QUESTION 54

- (Exam Topic 1)

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

- A. Hash value
- B. Private key
- C. Digital signature
- D. Digital certificate

Answer: D

NEW QUESTION 56

- (Exam Topic 1)

Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

- A. None of these scenarios compromise the privacy of Alice's data
- B. Agent Andrew subpoenas Alice, forcing her to reveal her private key
- C. However, the cloud server successfully resists Andrew's attempt to access the stored data
- D. Hacker Harry breaks into the cloud server and steals the encrypted data
- E. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

Answer: D

NEW QUESTION 59

- (Exam Topic 1)

Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

- A. Bootrom Exploit
- B. iBoot Exploit
- C. Sandbox Exploit
- D. Userland Exploit

Answer: D

NEW QUESTION 60

- (Exam Topic 1)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

- A. Nmap
- B. Cain & Abel
- C. Nessus
- D. Snort

Answer: D

NEW QUESTION 63

- (Exam Topic 1)

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

Answer: B

NEW QUESTION 67

- (Exam Topic 1)

A virus that attempts to install itself inside the file it is infecting is called?

- A. Tunneling virus
- B. Cavity virus
- C. Polymorphic virus
- D. Stealth virus

Answer: B

NEW QUESTION 69

- (Exam Topic 1)

In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

- A. Keyed Hashing
- B. Key Stretching
- C. Salting
- D. Double Hashing

Answer: C

NEW QUESTION 70

- (Exam Topic 1)

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.

He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Answer: C

NEW QUESTION 72

- (Exam Topic 1)

If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

- A. -sP
- B. -P
- C. -r
- D. -F

Answer: B

NEW QUESTION 74

- (Exam Topic 1)

In the field of cryptanalysis, what is meant by a “rubber-hose” attack?

- A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
- B. Extraction of cryptographic secrets through coercion or torture.
- C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
- D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

NEW QUESTION 76

- (Exam Topic 1)

A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what driver and library are required to allow the NIC to work in promiscuous mode?

- A. Libpcap
- B. Awinpcap
- C. Winprom
- D. Winpcap

Answer: D

NEW QUESTION 78

- (Exam Topic 1)

These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

- A. Black-Hat Hackers
- B. Script Kiddies
- C. White-Hat Hackers
- D. Gray-Hat Hacker

Answer: C

NEW QUESTION 82

- (Exam Topic 1)

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

- A. Produces less false positives
- B. Can identify unknown attacks
- C. Requires vendor updates for a new threat
- D. Cannot deal with encrypted network traffic

Answer: B

NEW QUESTION 83

- (Exam Topic 1)

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

- A. tcp.port != 21
- B. tcp.port = 23
- C. tcp.port ==21
- D. tcp.port ==21 || tcp.port ==22

Answer: D

NEW QUESTION 87

- (Exam Topic 1)

Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

- A. Hire a security consultant to provide direction.
- B. Do not back up either the credit card numbers or their hashes.
- C. Back up the hashes of the credit card numbers not the actual credit card numbers.
- D. Encrypt backup tapes that are sent off-site.

Answer: A

NEW QUESTION 91

- (Exam Topic 1)

Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious Java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical Java script. What is the name of this technique to hide the code and extend analysis time?

- A. Encryption

- B. Code encoding
- C. Obfuscation
- D. Steganography

Answer: A

NEW QUESTION 94

- (Exam Topic 1)

During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

- A. Private keys
- B. User passwords
- C. Public keys
- D. Public and private keys

Answer: C

NEW QUESTION 98

- (Exam Topic 1)

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

- A. Bluesmacking
- B. Bluesniffing
- C. Bluesnarfing
- D. Bluejacking

Answer: D

NEW QUESTION 99

- (Exam Topic 1)

You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.

Which of the below scanning technique will you use?

- A. ACK flag scanning
- B. TCP Scanning
- C. IP Fragment Scanning
- D. Inverse TCP flag scanning

Answer: C

NEW QUESTION 103

- (Exam Topic 1)

A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks. What process would help him?

- A. Banner Grabbing
- B. IDLE/IPID Scanning
- C. SSDP Scanning
- D. UDP Scanning

Answer: A

NEW QUESTION 106

- (Exam Topic 1)

In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

- A. Chosen-plaintext attack
- B. Ciphertext-only attack
- C. Adaptive chosen-plaintext attack
- D. Known-plaintext attack

Answer: A

NEW QUESTION 111

- (Exam Topic 2)

The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

- A. non-repudiation.
- B. operability.
- C. security.
- D. usability.

Answer: A

NEW QUESTION 116

- (Exam Topic 2)

On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

- A. `nessus +`
- B. `nessus *s`
- C. `nessus &`
- D. `nessus -d`

Answer: C

NEW QUESTION 120

- (Exam Topic 2)

An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

- A. By using SQL injection
- B. By changing hidden form values
- C. By using cross site scripting
- D. By utilizing a buffer overflow attack

Answer: B

NEW QUESTION 124

- (Exam Topic 2)

Which of the following is a preventive control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

Answer: A

NEW QUESTION 127

- (Exam Topic 2)

After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

- A. SHA1
- B. Diffie-Helman
- C. RSA
- D. AES

Answer: A

NEW QUESTION 131

- (Exam Topic 2)

Which of the following examples best represents a logical or technical control?

- A. Security tokens
- B. Heating and air conditioning
- C. Smoke and fire alarms
- D. Corporate security policy

Answer: A

NEW QUESTION 134

- (Exam Topic 2)

What are the three types of authentication?

- A. Something you: know, remember, prove
- B. Something you: have, know, are
- C. Something you: show, prove, are
- D. Something you: show, have, prove

Answer: B

NEW QUESTION 139

- (Exam Topic 2)

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

- A. Metasploit scripting engine
- B. Nessus scripting engine
- C. NMAP scripting engine
- D. SAINT scripting engine

Answer: C

NEW QUESTION 142

- (Exam Topic 2)

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy
- C. Remote-access policy
- D. Permissive policy

Answer: C

NEW QUESTION 144

- (Exam Topic 2)

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

- A. Vulnerability scanning
- B. Social engineering
- C. Application security testing
- D. Network sniffing

Answer: B

NEW QUESTION 148

- (Exam Topic 2)

An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

- A. Classified
- B. Overt
- C. Encrypted
- D. Covert

Answer: D

NEW QUESTION 153

- (Exam Topic 2)

A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

- A. if (billingAddress = 50) {update field} else exit
- B. if (billingAddress != 50) {update field} else exit
- C. if (billingAddress >= 50) {update field} else exit
- D. if (billingAddress <= 50) {update field} else exit

Answer: D

NEW QUESTION 158

- (Exam Topic 2)

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

- A. UDP 123
- B. UDP 541
- C. UDP 514
- D. UDP 415

Answer: C

NEW QUESTION 161

- (Exam Topic 2)

At a Windows Server command prompt, which command could be used to list the running services?

- A. Sc query type= running
- B. Sc query \\servername
- C. Sc query
- D. Sc config

Answer: C

NEW QUESTION 165

- (Exam Topic 2)

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

- A. Scripting languages are hard to learn.
- B. Scripting languages are not object-oriented.
- C. Scripting languages cannot be used to create graphical user interfaces.
- D. Scripting languages are slower because they require an interpreter to run the code.

Answer: D

NEW QUESTION 167

- (Exam Topic 2)

While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

- A. Packet filtering firewall
- B. Application-level firewall
- C. Circuit-level gateway firewall
- D. Stateful multilayer inspection firewall

Answer: C

NEW QUESTION 169

- (Exam Topic 2)

A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

- A. The consultant will ask for money on the bid because of great work.
- B. The consultant may expose vulnerabilities of other companies.
- C. The company accepting bids will want the same type of format of testing.
- D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NEW QUESTION 170

- (Exam Topic 2)

Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

- A. Results matching all words in the query
- B. Results matching "accounting" in domain target.com but not on the site Marketing.target.com
- C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
- D. Results for matches on target.com and Marketing.target.com that include the word "accounting"

Answer: B

NEW QUESTION 175

- (Exam Topic 2)

Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

- A. Port scanning
- B. Banner grabbing
- C. Injecting arbitrary data
- D. Analyzing service response

Answer: D

NEW QUESTION 180

- (Exam Topic 2)

While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

- A. 10.10.10.10
- B. 127.0.0.1
- C. 192.168.1.1
- D. 192.168.168.168

Answer: B

NEW QUESTION 184

- (Exam Topic 2)

Which of the following is used to indicate a single-line comment in structured query language (SQL)?

- A. --
- B. ||
- C. %%
- D. "

Answer: A

NEW QUESTION 185

- (Exam Topic 2)

In the software security development life cycle process, threat modeling occurs in which phase?

- A. Design
- B. Requirements
- C. Verification
- D. Implementation

Answer: A

NEW QUESTION 186

- (Exam Topic 2)

A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

- A. -sO
- B. -sP
- C. -sS
- D. -sU

Answer: A

NEW QUESTION 189

- (Exam Topic 2)

A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.

How can NMAP be used to scan these adjacent Class C networks?

- A. NMAP -P 192.168.1-5.
- B. NMAP -P 192.168.0.0/16
- C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
- D. NMAP -P 192.168.1/17

Answer: A

NEW QUESTION 192

- (Exam Topic 2)

A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

- A. Perform a dictionary attack.
- B. Perform a brute force attack.
- C. Perform an attack with a rainbow table.
- D. Perform a hybrid attack.

Answer: C

NEW QUESTION 193

- (Exam Topic 2)

What is the best defense against privilege escalation vulnerability?

- A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
- B. Run administrator and applications on least privileges and use a content registry for tracking.
- C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
- D. Review user roles and administrator privileges for maximum utilization of automation services.

Answer: C

NEW QUESTION 194

- (Exam Topic 2)

Which type of antenna is used in wireless communication?

- A. Omnidirectional
- B. Parabolic
- C. Uni-directional
- D. Bi-directional

Answer: A

NEW QUESTION 198

- (Exam Topic 2)

Fingerprinting VPN firewalls is possible with which of the following tools?

- A. Angry IP
- B. Nikto
- C. Ike-scan
- D. Arp-scan

Answer:

C

NEW QUESTION 199

- (Exam Topic 2)

Which tool can be used to silently copy files from USB devices?

- A. USB Grabber
- B. USB Dumper
- C. USB Sniffer
- D. USB Snoopy

Answer: B

NEW QUESTION 201

- (Exam Topic 2)

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

- A. 768 bit key
- B. 1025 bit key
- C. 1536 bit key
- D. 2048 bit key

Answer: C

NEW QUESTION 206

- (Exam Topic 2)

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

- A. Input validation flaw
- B. HTTP header injection vulnerability
- C. 0-day vulnerability
- D. Time-to-check to time-to-use flaw

Answer: C

NEW QUESTION 211

- (Exam Topic 2)

Which type of scan measures a person's external features through a digital video camera?

- A. Iris scan
- B. Retinal scan
- C. Facial recognition scan
- D. Signature kinetics scan

Answer: C

NEW QUESTION 213

- (Exam Topic 2)

An NMAP scan of a server shows port 25 is open. What risk could this pose?

- A. Open printer sharing
- B. Web portal data leak
- C. Clear text authentication
- D. Active mail relay

Answer: D

NEW QUESTION 217

- (Exam Topic 2)

To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

- A. Recipient's private key
- B. Recipient's public key
- C. Master encryption key
- D. Sender's public key

Answer: B

NEW QUESTION 218

- (Exam Topic 2)

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

- A. They are written in Java.
- B. They send alerts to security monitors.
- C. They use the same packet analysis engine.

D. They use the same packet capture utility.

Answer: D

NEW QUESTION 219

- (Exam Topic 2)

A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

- A. Spoofing an IP address
- B. Tunneling scan over SSH
- C. Tunneling over high port numbers
- D. Scanning using fragmented IP packets

Answer: B

NEW QUESTION 224

- (Exam Topic 2)

How does an operating system protect the passwords used for account logins?

- A. The operating system performs a one-way hash of the passwords.
- B. The operating system stores the passwords in a secret file that users cannot find.
- C. The operating system encrypts the passwords, and decrypts them when needed.
- D. The operating system stores all passwords in a protected segment of non-volatile memory.

Answer: A

NEW QUESTION 227

- (Exam Topic 2)

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- A. Usernames
- B. File permissions
- C. Firewall rulesets
- D. Passwords

Answer: D

NEW QUESTION 230

- (Exam Topic 2)

Which command line switch would be used in NMAP to perform operating system detection?

- A. -OS
- B. -sO
- C. -sP
- D. -O

Answer: D

NEW QUESTION 232

- (Exam Topic 2)

Which of the following cryptography attack methods is usually performed without the use of a computer?

- A. Ciphertext-only attack
- B. Chosen key attack
- C. Rubber hose attack
- D. Rainbow table attack

Answer: C

NEW QUESTION 237

- (Exam Topic 2)

A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

- A. True negatives
- B. False negatives
- C. True positives
- D. False positives

Answer: D

NEW QUESTION 238

- (Exam Topic 2)

Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

- A. Cross-site scripting
- B. SQL injection
- C. Missing patches
- D. CRLF injection

Answer: C

NEW QUESTION 239

- (Exam Topic 2)

During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

- A. Using the Metasploit psexec module setting the SA / Admin credential
- B. Invoking the stored procedure xp_shell to spawn a Windows command shell
- C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
- D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Answer: D

NEW QUESTION 243

- (Exam Topic 2)

Passive reconnaissance involves collecting information through which of the following?

- A. Social engineering
- B. Network traffic sniffing
- C. Man in the middle attacks
- D. Publicly accessible sources

Answer: D

NEW QUESTION 245

- (Exam Topic 2)

Which of the following is a detective control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

Answer: C

NEW QUESTION 250

- (Exam Topic 2)

Which of the following is a component of a risk assessment?

- A. Physical security
- B. Administrative safeguards
- C. DMZ
- D. Logical interface

Answer: B

NEW QUESTION 254

- (Exam Topic 2)

Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

- A. Cain
- B. John the Ripper
- C. Nikto
- D. Hping

Answer: A

NEW QUESTION 259

- (Exam Topic 2)

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

- A. False positive
- B. False negative
- C. True positive
- D. True negative

Answer: A

NEW QUESTION 264

- (Exam Topic 2)

Which of the following is considered an acceptable option when managing a risk?

- A. Reject the risk.
- B. Deny the risk.
- C. Mitigate the risk.
- D. Initiate the risk.

Answer: C

NEW QUESTION 266

- (Exam Topic 2)

ICMP ping and ping sweeps are used to check for active systems and to check

- A. if ICMP ping traverses a firewall.
- B. the route that the ICMP ping took.
- C. the location of the switchport in relation to the ICMP ping.
- D. the number of hops an ICMP ping takes to reach a destination.

Answer: A

NEW QUESTION 269

- (Exam Topic 2)

What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

- A. tcp.src == 25 and ip.host == 192.168.0.125
- B. host 192.168.0.125:25
- C. port 25 and host 192.168.0.125
- D. tcp.port == 25 and ip.host == 192.168.0.125

Answer: D

NEW QUESTION 270

- (Exam Topic 2)

Which of the following items of a computer system will an anti-virus program scan for viruses?

- A. Boot Sector
- B. Deleted Files
- C. Windows Process List
- D. Password Protected Files

Answer: A

NEW QUESTION 273

- (Exam Topic 2)

Which of the following is a client-server tool utilized to evade firewall inspection?

- A. tcp-over-dns
- B. kismet
- C. nikto
- D. hping

Answer: A

NEW QUESTION 278

- (Exam Topic 2)

What information should an IT system analysis provide to the risk assessor?

- A. Management buy-in
- B. Threat statement
- C. Security architecture
- D. Impact analysis

Answer: C

NEW QUESTION 279

- (Exam Topic 2)

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

- A. Paros Proxy

- B. BBProxy
- C. BBCrack
- D. Blooover

Answer: B

Explanation:

Blackberry users warned of hacking tool threat.

Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.

References:

<http://www.computerweekly.com/news/2240062112/Technology-news-in-brief>

NEW QUESTION 283

- (Exam Topic 2)

Least privilege is a security concept that requires that a user is

- A. limited to those functions required to do the job.
- B. given root or administrative privileges.
- C. trusted to keep all data and access to that data under their sole control.
- D. given privileges equal to everyone else in the department.

Answer: A

NEW QUESTION 287

- (Exam Topic 2)

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

- A. Fast processor to help with network traffic analysis
- B. They must be dual-homed
- C. Similar RAM requirements
- D. Fast network interface cards

Answer: B

Explanation:

Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.

References: <https://en.wikipedia.org/wiki/Dual-homed>

NEW QUESTION 292

- (Exam Topic 2)

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- A. WHOIS
- B. IANA
- C. CAPTCHA
- D. IETF

Answer: A

NEW QUESTION 296

- (Exam Topic 2)

While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

- A. Validate web content input for query strings.
- B. Validate web content input with scanning tools.
- C. Validate web content input for type, length, and range.
- D. Validate web content input for extraneous queries.

Answer: C

NEW QUESTION 298

- (Exam Topic 2)

A security policy will be more accepted by employees if it is consistent and has the support of

- A. coworkers.
- B. executive management.
- C. the security officer.
- D. a supervisor.

Answer: B

NEW QUESTION 303

- (Exam Topic 2)

A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

- A. Issue the pivot exploit and set the meterpreter.
- B. Reconfigure the network settings in the meterpreter.
- C. Set the payload to propagate through the meterpreter.
- D. Create a route statement in the meterpreter.

Answer: D

NEW QUESTION 306

- (Exam Topic 2)

What statement is true regarding LM hashes?

- A. LM hashes consist in 48 hexadecimal characters.
- B. LM hashes are based on AES128 cryptographic standard.
- C. Uppercase characters in the password are converted to lowercase.
- D. LM hashes are not generated when the password length exceeds 15 characters.

Answer: D

NEW QUESTION 311

- (Exam Topic 3)

Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

- A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
- B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
- C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
- D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NEW QUESTION 314

- (Exam Topic 3)

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

- A. Key registry
- B. Recovery agent
- C. Directory
- D. Key escrow

Answer: D

NEW QUESTION 318

- (Exam Topic 3)

Which of the following guidelines or standards is associated with the credit card industry?

- A. Control Objectives for Information and Related Technology (COBIT)
- B. Sarbanes-Oxley Act (SOX)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. Payment Card Industry Data Security Standards (PCI DSS)

Answer: D

NEW QUESTION 320

- (Exam Topic 3)

Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

- A. Ping of death
- B. SYN flooding
- C. TCP hijacking
- D. Smurf attack

Answer: A

NEW QUESTION 323

- (Exam Topic 3)

To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

- A. Harvesting
- B. Windowing
- C. Hardening
- D. Stealthing

Answer: C

NEW QUESTION 325

- (Exam Topic 3)

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

- A. Sender's public key
- B. Receiver's private key
- C. Receiver's public key
- D. Sender's private key

Answer: D

NEW QUESTION 328

- (Exam Topic 3)

Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

- A. MD5
- B. SHA-1
- C. RC4
- D. MD4

Answer: B

NEW QUESTION 330

- (Exam Topic 3)

SOAP services use which technology to format information?

- A. SATA
- B. PCI
- C. XML
- D. ISDN

Answer: C

NEW QUESTION 333

- (Exam Topic 3)

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

- A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
- B. The root CA stores the user's hash value for safekeeping.
- C. The CA is the trusted root that issues certificates.
- D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Answer: C

NEW QUESTION 337

- (Exam Topic 3)

Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

- A. RSA 1024 bit strength
- B. AES 1024 bit strength
- C. RSA 512 bit strength
- D. AES 512 bit strength

Answer: A

NEW QUESTION 341

- (Exam Topic 3)

An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

- A. Timing attack
- B. Replay attack
- C. Memory trade-off attack
- D. Chosen plain-text attack

Answer: D

NEW QUESTION 346

- (Exam Topic 3)

Which initial procedure should an ethical hacker perform after being brought into an organization?

- A. Begin security testing.
- B. Turn over deliverables.
- C. Sign a formal contract with non-disclosure.
- D. Assess what the organization is trying to protect.

Answer: C

NEW QUESTION 347

- (Exam Topic 3)

While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:

```
<script>alert(" Testing Testing Testing ")</script>
```

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

- A. Buffer overflow
- B. Cross-site request forgery
- C. Distributed denial of service
- D. Cross-site scripting

Answer: D

NEW QUESTION 349

- (Exam Topic 3)

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

- A. Regulatory compliance
- B. Peer review
- C. Change management
- D. Penetration testing

Answer: C

NEW QUESTION 353

- (Exam Topic 3)

Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

- A. Timing options to slow the speed that the port scan is conducted
- B. Fingerprinting to identify which operating systems are running on the network
- C. ICMP ping sweep to determine which hosts on the network are not available
- D. Traceroute to control the path of the packets sent during the scan

Answer: A

NEW QUESTION 355

- (Exam Topic 3)

Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

- A. Poly key exchange
- B. Cross certification
- C. Poly key reference
- D. Cross-site exchange

Answer: B

NEW QUESTION 360

- (Exam Topic 3)

An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

- A. Unplug the network connection on the company's web server.
- B. Determine the origin of the attack and launch a counterattack.
- C. Record as much information as possible from the attack.
- D. Perform a system restart on the company's web server.

Answer: C

NEW QUESTION 362

- (Exam Topic 3)

Which statement best describes a server type under an N-tier architecture?

- A. A group of servers at a specific layer
- B. A single server with a specific role
- C. A group of servers with a unique role
- D. A single server at a specific layer

Answer: C

NEW QUESTION 366

- (Exam Topic 3)

Which type of security document is written with specific step-by-step details?

- A. Process
- B. Procedure
- C. Policy
- D. Paradigm

Answer: B

NEW QUESTION 369

- (Exam Topic 3)

A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

- A. Implementing server-side PKI certificates for all connections
- B. Mandating only client-side PKI certificates for all connections
- C. Requiring client and server PKI certificates for all connections
- D. Requiring strong authentication for all DNS queries

Answer: C

NEW QUESTION 371

- (Exam Topic 4)

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

- A. Height and Weight
- B. Voice
- C. Fingerprints
- D. Iris patterns

Answer: A

Explanation:

There are two main types of biometric identifiers:

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.

References:

<http://searchsecurity.techtarget.com/definition/biometrics>

NEW QUESTION 372

- (Exam Topic 4)

Perspective clients want to see sample reports from previous penetration tests. What should you do next?

- A. Decline but, provide references.
- B. Share full reports, not redacted.
- C. Share full reports with redactions.
- D. Share reports, after NDA is signed.

Answer: A

Explanation:

Penetration tests data should not be disclosed to third parties.

NEW QUESTION 373

- (Exam Topic 4)

You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.

Which port would you see listening on these Windows machines in the network?

- A. 445
- B. 3389
- C. 161
- D. 1433

Answer: A

Explanation:

The following ports are associated with file sharing and server message block (SMB) communications: References: <https://support.microsoft.com/en-us/kb/298804>

NEW QUESTION 374

- (Exam Topic 4)

What is a "Collision attack" in cryptography?

- A. Collision attacks try to find two inputs producing the same hash.
- B. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
- C. Collision attacks try to get the public key.
- D. Collision attacks try to break the hash into three parts to get the plaintext value.

Answer: A

Explanation:

A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result. References: <https://learncryptography.com/hash-functions/hash-collision-attack>

NEW QUESTION 376

- (Exam Topic 4)

It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).

Which of the following vulnerabilities is being described?

- A. Shellshock
- B. Rootshock
- C. Rootshell
- D. Shellbash

Answer: A

Explanation:

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. References: [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

NEW QUESTION 378

- (Exam Topic 4)

How does the Address Resolution Protocol (ARP) work?

- A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
- B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
- C. It sends a reply packet for a specific IP, asking for the MAC address.
- D. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

Answer: A

Explanation:

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

References:

<http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP>

NEW QUESTION 383

- (Exam Topic 4)

What is the benefit of performing an unannounced Penetration Testing?

- A. The tester will have an actual security posture visibility of the target network.
- B. Network security would be in a "best state" posture.
- C. It is best to catch critical infrastructure unpatched.
- D. The tester could not provide an honest analysis.

Answer: A

Explanation:

Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.

A possible solution to this danger is to conduct intermittent “unannounced” penetration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with “announced” penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.

References:

<http://www.siteproneews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/>

NEW QUESTION 386

- (Exam Topic 4)

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.

What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.dstport==514 && ip.dst==192.168.0.150
- B. tcp.srcport==514 && ip.src==192.168.0.99
- C. tcp.dstport==514 && ip.dst==192.168.0.0/16
- D. tcp.srcport==514 && ip.src==192.168.150

Answer: A

Explanation:

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.

References: <https://wiki.wireshark.org/DisplayFilters>

NEW QUESTION 390

- (Exam Topic 4)

Which of the following is an extremely common IDS evasion technique in the web world?

- A. unicode characters
- B. spyware
- C. port knocking
- D. subnetting

Answer: A

Explanation:

Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life.

One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.

References:

<http://books.gigatux.nl/mirror/apacheseconomy/0596007248/apachesc-chp-10-sect-8.html>

NEW QUESTION 393

- (Exam Topic 4)

During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.

What type of firewall is inspecting outbound traffic?

- A. Application
- B. Circuit
- C. Stateful
- D. Packet Filtering

Answer: A

Explanation:

An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

References:

<http://searchsoftwarequality.techtarget.com/definition/application-firewall>

NEW QUESTION 394

- (Exam Topic 4)

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

- A. Botnet Trojan
- B. Turtle Trojans
- C. Banking Trojans
- D. Ransomware Trojans

Answer: A

Explanation:

In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

NEW QUESTION 397

- (Exam Topic 4)

Which of the following describes the characteristics of a Boot Sector Virus?

- A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
- B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
- C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
- D. Overwrites the original MBR and only executes the new virus code

Answer: A

Explanation:

A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.

References: <https://www.techopedia.com/definition/26655/boot-sector-virus>

NEW QUESTION 401

- (Exam Topic 4)

When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.

What should you do?

- A. Forward the message to your company's security response team and permanently delete the message from your computer.
- B. Reply to the sender and ask them for more information about the message contents.
- C. Delete the email and pretend nothing happened
- D. Forward the message to your supervisor and ask for her opinion on how to handle the situation

Answer: A

Explanation:

By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.

References:

https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NEW QUESTION 406

- (Exam Topic 4)

It is a short-range wireless communication technology intended to replace the cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.

Which of the following terms best matches the definition?

- A. Bluetooth
- B. Radio-Frequency Identification
- C. WLAN
- D. InfraRed

Answer: A

Explanation:

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

References:

<http://www.bbc.co.uk/webwise/guides/about-bluetooth>

NEW QUESTION 411

- (Exam Topic 4)

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.

What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- A. Terms of Engagement
- B. Project Scope
- C. Non-Disclosure Agreement
- D. Service Level Agreement

Answer: A

NEW QUESTION 412

- (Exam Topic 4)

A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

- A. Delegate
- B. Avoid
- C. Mitigate
- D. Accept

Answer: A

Explanation:

There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References:

<http://www.dbpmanagement.com/15/5-ways-to-manage-risk>

NEW QUESTION 414

- (Exam Topic 4)

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.

What nmap script will help you with this task?

- A. http-methods
- B. http_enum
- C. http-headers
- D. http-git

Answer: A

Explanation:

You can check HTTP method vulnerability using NMAP. Example: `#nmap -script=http-methods.nse 192.168.0.25` References:

<http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/>

NEW QUESTION 419

- (Exam Topic 4)

This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.

What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

- A. footprinting
- B. network mapping
- C. gaining access
- D. escalating privileges

Answer: A

Explanation:

Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.

References:

<http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html>

NEW QUESTION 423

- (Exam Topic 4)

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

- A. c:\compmgmt.msc
- B. c:\services.msc
- C. c:\ncpa.cp
- D. c:\gpedit

Answer: A

Explanation:

To start the Computer Management Console from command line just type compmgmt.msc

/computer:computername in your run box or at the command line and it should automatically open the Computer Management console.

References:

<http://www.waynezim.com/tag/compmgmtmsc/>

NEW QUESTION 424

- (Exam Topic 4)

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which Algorithm is this referring to?

- A. Wired Equivalent Privacy (WEP)
- B. Wi-Fi Protected Access (WPA)
- C. Wi-Fi Protected Access 2 (WPA2)
- D. Temporal Key Integrity Protocol (TKIP)

Answer: A

Explanation:

WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

References: <https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html>

NEW QUESTION 429

- (Exam Topic 4)

Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.

What is this style of attack called?

- A. zero-day
- B. zero-hour
- C. zero-sum
- D. no-day

Answer: A

Explanation:

Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.

References: <https://en.wikipedia.org/wiki/Stuxnet>

NEW QUESTION 433

- (Exam Topic 4)

Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any

information besides the company name.

What should be the first step in security testing the client?

- A. Reconnaissance
- B. Enumeration
- C. Scanning
- D. Escalation

Answer: A

Explanation:

Phases of hacking

Phase 1—Reconnaissance Phase 2—Scanning

Phase 3—Gaining Access Phase 4—Maintaining Access Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance

References:

<http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html>

NEW QUESTION 434

- (Exam Topic 4)

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?

alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!");

- A. An Intrusion Detection System
- B. A firewall IPTable
- C. A Router IPTable
- D. FTP Server rule

Answer: A

Explanation:

Snort is an open source network intrusion detection system (NIDS) for networks . Snort rule example:

This example is a rule with a generator id of 1000001.

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

References:

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html>

NEW QUESTION 436

- (Exam Topic 4)

It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.

Which of the following terms best matches the definition?

- A. Ransomware
- B. Adware
- C. Spyware
- D. Riskware

Answer: A

Explanation:

Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.

References: <https://en.wikipedia.org/wiki/Ransomware>

NEW QUESTION 438

- (Exam Topic 4)

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.

What testing method did you use?

- A. Social engineering
- B. Tailgating
- C. Piggybacking
- D. Eavesdropping

Answer: A

Explanation:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION 440

- (Exam Topic 4)

It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?

- A. HIPAA
- B. ISO/IEC 27002
- C. COBIT
- D. FISMA

Answer: A

Explanation:

The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.))[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".

References: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

NEW QUESTION 442

- (Exam Topic 4)

The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.

What tool can you use to view the network traffic being sent and received by the wireless router?

- A. Wireshark
- B. Nessus
- C. Netcat
- D. Netstat

Answer: A

Explanation:

Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NEW QUESTION 443

- (Exam Topic 4)

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

- A. Immediately stop work and contact the proper legal authorities.
- B. Copy the data to removable media and keep it in case you need it.
- C. Confront the client in a respectful manner and ask her about the data.
- D. Ignore the data and continue the assessment until completed as agreed.

Answer: A

NEW QUESTION 447

- (Exam Topic 4)

You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.

What should you do?

- A. Report immediately to the administrator
- B. Do not report it and continue the penetration test.
- C. Transfer money from the administrator's account to another account.
- D. Do not transfer the money but steal the bitcoins.

Answer: A

NEW QUESTION 450

- (Exam Topic 5)

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP

Answer: A

Explanation:

MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is

used to determine access to the network. MAC Filtering is often used on wireless networks.
References: https://en.wikipedia.org/wiki/MAC_filtering

NEW QUESTION 452

- (Exam Topic 5)

The "black box testing" methodology enforces which kind of restriction?

- A. Only the external operation of a system is accessible to the tester.
- B. Only the internal operation of a system is known to the tester.
- C. The internal operation of a system is only partly accessible to the tester.
- D. The internal operation of a system is completely known to the tester.

Answer: A

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.
References: https://en.wikipedia.org/wiki/Black-box_testing

NEW QUESTION 457

- (Exam Topic 5)

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What Web browser-based security vulnerability was exploited to compromise the user?

- A. Cross-Site Request Forgery
- B. Cross-Site Scripting
- C. Clickjacking
- D. Web form input validation

Answer: A

Explanation:

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics

If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

NEW QUESTION 462

- (Exam Topic 5)

Which of the following tools can be used for passive OS fingerprinting?

- A. tcpdump
- B. nmap
- C. ping
- D. tracer

Answer: A

Explanation:

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

References:

<http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html>

NEW QUESTION 466

- (Exam Topic 5)

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

- A. Security through obscurity
- B. Host-Based Intrusion Detection System
- C. Defense in depth
- D. Network-Based Intrusion Detection System

Answer: C

NEW QUESTION 469

- (Exam Topic 5)

The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?

- A. Hack attack
- B. Sniffing
- C. Dumpster diving

D. Spying

Answer: C

NEW QUESTION 472

- (Exam Topic 5)

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application. What kind of Web application vulnerability likely exists in their software?

- A. Cross-site scripting vulnerability
- B. Cross-site Request Forgery vulnerability
- C. SQL injection vulnerability
- D. Web site defacement vulnerability

Answer: A

Explanation:

Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, **very large**), output encoding (such as **very large**) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "**very large**"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION 474

- (Exam Topic 5)

Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

- A. a port scanner
- B. a vulnerability scanner
- C. a virus scanner
- D. a malware scanner

Answer: B

NEW QUESTION 478

- (Exam Topic 5)

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Public Key
- B. Secret Key
- C. Hash Algorithm
- D. Digest

Answer: A

Explanation:

Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG.

References: https://en.wikipedia.org/wiki/Public-key_cryptography

NEW QUESTION 480

- (Exam Topic 5)

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

Answer: A

Explanation:

Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

References:

<http://ieeexplore.ieee.org/xpl/login.jsp?tp=>

[&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D561](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D561)

NEW QUESTION 484

- (Exam Topic 5)

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

- A. \$146
- B. \$1320
- C. \$440
- D. \$100

Answer: A

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

Suppose than an asset is valued at \$100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * \$100,000, or \$25,000.

In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

NEW QUESTION 488

- (Exam Topic 5)

What is the difference between the AES and RSA algorithms?

- A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.
- B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
- C. Both are symmetric algorithms, but AES uses 256-bit keys.
- D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.

Answer: B

NEW QUESTION 493

- (Exam Topic 5)

You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless.

When you verify the configuration of this Windows system you find two static routes.

route add 10.0.0.0 mask 255.0.0.0 10.0.0.1

route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

- A. Both static routes indicate that the traffic is external with different gateway.
- B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
- C. Both static routes indicate that the traffic is internal with different gateway.
- D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Answer: D

NEW QUESTION 497

- (Exam Topic 5)

Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

- A. Internal Whitebox
- B. External, Whitebox
- C. Internal, Blackbox
- D. External, Blackbox

Answer: C

NEW QUESTION 502

- (Exam Topic 5)

Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

- A. A race condition is being exploited, and the operating system is containing the malicious process.
- B. A page fault is occurring, which forces the operating system to write data from the hard drive.
- C. Malware is executing in either ROM or a cache memory area.
- D. Malicious code is attempting to execute instruction in a non-executable memory region.

Answer: D

NEW QUESTION 503

- (Exam Topic 5)

Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

- A. All of the employees would stop normal work activities
- B. IT department would be telling employees who the boss is
- C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
- D. The network could still experience traffic slow down.

Answer: C

NEW QUESTION 508

- (Exam Topic 5)

A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

- A. Network elements must be hardened with user ids and strong password
- B. Regular security tests and audits should be performed.
- C. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- D. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- E. The operator knows that attacks and down time are inevitable and should have a backup site.

Answer: A

NEW QUESTION 513

- (Exam Topic 5)

You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

- A. Network-based IDS
- B. Firewall
- C. Proxy
- D. Host-based IDS

Answer: A

Explanation:

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: <https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids>

NEW QUESTION 515

- (Exam Topic 5)

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Preparation phase
- B. Containment phase
- C. Identification phase
- D. Recovery phase

Answer: A

Explanation:

There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:

References: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

NEW QUESTION 520

- (Exam Topic 5)

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.

Why he cannot see the servers?

- A. The network must be down and the nmap command and IP address are ok.
- B. He needs to add the command ""ip address"" just before the IP address.
- C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
- D. He needs to change the address to 192.168.1.0 with the same mask.

Answer: C

NEW QUESTION 524

- (Exam Topic 5)

Which of the following statements regarding ethical hacking is incorrect?

- A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
- B. Testing should be remotely performed offsite.
- C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
- D. Ethical hacking should not involve writing to or modifying the target systems.

Answer: A

Explanation:

Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

References:

<http://searchsecurity.techtarget.com/definition/ethical-hacker>

NEW QUESTION 527

- (Exam Topic 5)

An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

- A. The sequence does not matter
- B. Both steps have to be performed against all hosts.
- C. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
- D. First the ping sweep to identify live hosts and then the port scan on the live host
- E. This way he saves time.
- F. The port scan alone is adequate
- G. This way he saves time.

Answer: C

NEW QUESTION 532

- (Exam Topic 5)

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

- A. Application Layer
- B. Data tier
- C. Presentation tier
- D. Logic tier

Answer: D

NEW QUESTION 534

- (Exam Topic 5)

Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

- A. A new username and password
- B. A fingerprint scanner and his username and password.
- C. Disable his username and use just a fingerprint scanner.
- D. His username and a stronger password.

Answer: B

NEW QUESTION 538

- (Exam Topic 5)

Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

- A. Network-based intrusion detection system (NIDS)
- B. Host-based intrusion detection system (HIDS)
- C. Firewalls
- D. Honey pots

Answer: A

NEW QUESTION 540

- (Exam Topic 5)

Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

- A. Fuzzy-testing the code
- B. Third party running the code
- C. Sandboxing the code
- D. String validating the code

Answer: A

NEW QUESTION 541

- (Exam Topic 5)

Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

- A. Blind SQLi
- B. DMS-specific SQLi
- C. Classic SQLi
- D. Compound SQLi

Answer: A

NEW QUESTION 545

- (Exam Topic 5)

A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below: According to the section from the report, which of the following choice is true?

- A. MAC Spoof attacks cannot be performed.
- B. Possibility of SQL Injection attack is eliminated.
- C. A stateful firewall can be used between intranet (LAN) and DMZ.
- D. There is access control policy between VLANs.

Answer: C

NEW QUESTION 549

- (Exam Topic 5)

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

- A. Wireshark
- B. Maltego
- C. Metasploit
- D. Nessus

Answer: C

NEW QUESTION 553

- (Exam Topic 5)

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

- A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
- B. Attempts by attackers to access the user and password information stored in the company's SQL database.
- C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
- D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Answer: A

Explanation:

Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.

Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.

References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

NEW QUESTION 557

- (Exam Topic 5)

Which of these options is the most secure procedure for storing backup tapes?

- A. In a climate controlled facility offsite
- B. On a different floor in the same building
- C. Inside the data center for faster retrieval in a fireproof safe
- D. In a cool dry environment

Answer: A

Explanation:

An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.

References:

<http://www.entrustm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery-strategy>

NEW QUESTION 562

- (Exam Topic 5)

What is correct about digital signatures?

- A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
- B. Digital signatures may be used in different documents of the same type.
- C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
- D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Answer: A

NEW QUESTION 567

- (Exam Topic 5)

What is the role of test automation in security testing?

- A. It can accelerate benchmark tests and repeat them with a consistent test setu
- B. But it cannot replace manual testing completely.
- C. It is an option but it tends to be very expensive.
- D. It should be used exclusivel
- E. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- F. Test automation is not usable in security due to the complexity of the tests.

Answer: A

NEW QUESTION 571

- (Exam Topic 5)

Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Social Engineering
- B. Sniffing
- C. Eavesdropping
- D. Scanning

Answer: A

Explanation:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

References: [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

NEW QUESTION 572

- (Exam Topic 5)

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- A. msfpayload
- B. msfcli
- C. msfencode
- D. msfd

Answer: C

NEW QUESTION 575

- (Exam Topic 5)

The "white box testing" methodology enforces what kind of restriction?

- A. The internal operation of a system is completely known to the tester.
- B. Only the external operation of a system is accessible to the tester.
- C. Only the internal operation of a system is known to the tester.
- D. The internal operation of a system is only partly accessible to the tester.

Answer: A

Explanation:

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

References: https://en.wikipedia.org/wiki/White-box_testing

NEW QUESTION 580

- (Exam Topic 5)

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

- A. Nikto
- B. Snort
- C. John the Ripper
- D. Dsniff

Answer: A

Explanation:

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

NEW QUESTION 585

- (Exam Topic 5)

An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is most likely able to handle this requirement?

- A. RADIUS
- B. DIAMETER
- C. Kerberos
- D. TACACS+

Answer: A

Explanation:

Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.

References: <https://en.wikipedia.org/wiki/RADIUS>

NEW QUESTION 589

- (Exam Topic 5)

A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

- A. Ignore it.
- B. Try to sell the information to a well-paying party on the dark web.
- C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
- D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

Answer: C

NEW QUESTION 590

- (Exam Topic 5)

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

- A. Identify and evaluate existing practices
- B. Create a procedures document
- C. Conduct compliance testing
- D. Terminate the audit

Answer: A

Explanation:

The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION 591

- (Exam Topic 5)

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.

What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

- A. Protocol analyzer
- B. Intrusion Prevention System (IPS)
- C. Network sniffer
- D. Vulnerability scanner

Answer: A

Explanation:

A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

References: https://en.wikipedia.org/wiki/Packet_analyzer

NEW QUESTION 595

- (Exam Topic 6)

Why would an attacker want to perform a scan on port 137?

- A. To discover proxy servers on a network
- B. To disrupt the NetBIOS SMB service on the target host
- C. To check for file and print sharing on Windows systems
- D. To discover information about a target host using NBTSTAT

Answer: D

NEW QUESTION 600

- (Exam Topic 6)

While performing online banking using a Web browser, Kyle receives an email that contains an image of a well-crafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?

- A. Clickjacking
- B. Web Form Input Validation
- C. Cross-Site Request Forgery
- D. Cross-Site Scripting

Answer: C

NEW QUESTION 601

- (Exam Topic 6)

While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

- A. Immediately stop work and contact the proper legal authorities
- B. Ignore the data and continue the assessment until completed as agreed
- C. Confront the client in a respectful manner and ask her about the data
- D. Copy the data to removable media and keep it in case you need it

Answer: A

NEW QUESTION 604

- (Exam Topic 6)

Matthew received an email with an attachment named "YouWon\$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

- A. Key-logger
- B. Trojan
- C. Worm
- D. Macro Virus

Answer: B

NEW QUESTION 605

- (Exam Topic 6)

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Turnstile
- B. Bollards
- C. Mantrap
- D. Receptionist

Answer: B

NEW QUESTION 608

- (Exam Topic 6)

Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

- A. It is a network fault and the originating machine is in a network loop
- B. It is a worm that is malfunctioning or hardcoded to scan on port 500
- C. The attacker is trying to detect machines on the network which have SSL enabled
- D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Answer: D

NEW QUESTION 612

- (Exam Topic 6)

Which of the following is NOT an ideal choice for biometric controls?

- A. Iris patterns
- B. Fingerprints
- C. Height and weight
- D. Voice

Answer: C

NEW QUESTION 616

- (Exam Topic 6)

A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

- A. Turtle Trojans
- B. Ransomware Trojans
- C. Botnet Trojan
- D. Banking Trojans

Answer: C

NEW QUESTION 619

- (Exam Topic 6)

It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

- A. Containment
- B. Eradication
- C. Recovery
- D. Discovery

Answer: A

NEW QUESTION 624

- (Exam Topic 6)

What is the term coined for logging, recording and resolving events in a company?

- A. Internal Procedure
- B. Security Policy
- C. Incident Management Process
- D. Metrics

Answer: C

NEW QUESTION 629

- (Exam Topic 6)

In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

- A. Port Scanning
- B. Hacking Active Directory
- C. Privilege Escalation
- D. Shoulder-Surfing

Answer: C

NEW QUESTION 630

- (Exam Topic 6)

You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

- A. Disable Key Services
- B. Create User Account
- C. Download and Install Netcat
- D. Disable IPTables

Answer: B

NEW QUESTION 635

- (Exam Topic 6)

Which of the following BEST describes the mechanism of a Boot Sector Virus?

- A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
- B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
- C. Overwrites the original MBR and only executes the new virus code
- D. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

Answer: A

NEW QUESTION 637

- (Exam Topic 6)

.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

- A. Collision Attack
- B. Evil Twin Attack
- C. Sinkhole Attack
- D. Signal Jamming Attack

Answer: B

NEW QUESTION 639

- (Exam Topic 6)

The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is \$500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

- A. \$62.5
- B. \$250
- C. \$125
- D. \$65.2

Answer: A

NEW QUESTION 642

- (Exam Topic 6)

Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?

- A. Gaining access
- B. Escalating privileges
- C. Network mapping
- D. Footprinting

Answer: D

NEW QUESTION 643

- (Exam Topic 6)

In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.

Example:

allintitle: root passwd

- A. Maintaining Access
- B. Gaining Access
- C. Reconnaissance
- D. Scanning and Enumeration

Answer: C

NEW QUESTION 648

- (Exam Topic 6)

The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

- A. Accept
- B. Mitigate
- C. Delegate
- D. Avoid

Answer: C

NEW QUESTION 649

- (Exam Topic 6)

Which of the following will perform an Xmas scan using NMAP?

- A. nmap -sA 192.168.1.254
- B. nmap -sP 192.168.1.254
- C. nmap -sX 192.168.1.254
- D. nmap -sV 192.168.1.254

Answer: C

NEW QUESTION 654

- (Exam Topic 6)

You want to analyze packets on your wireless network. Which program would you use?

- A. Wireshark with Aircap
- B. Aircap with Aircap
- C. Wireshark with Winpcap
- D. Ethereal with Winpcap

Answer: A

NEW QUESTION 658

- (Exam Topic 6)

A software tester is randomly generating invalid inputs in an attempt to crash the program. Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?

- A. Mutating
- B. Randomizing
- C. Fuzzing
- D. Bounding

Answer: C

NEW QUESTION 663

- (Exam Topic 6)

Which of the following is a restriction being enforced in “white box testing?”

- A. Only the internal operation of a system is known to the tester
- B. The internal operation of a system is completely known to the tester
- C. The internal operation of a system is only partly accessible to the tester
- D. Only the external operation of a system is accessible to the tester

Answer: B

NEW QUESTION 666

- (Exam Topic 6)

Destination unreachable administratively prohibited messages can inform the hacker to what?

- A. That a circuit level proxy has been installed and is filtering traffic
- B. That his/her scans are being blocked by a honeypot or jail
- C. That the packets are being malformed by the scanning software
- D. That a router or other packet-filtering device is blocking traffic
- E. That the network is functioning normally

Answer: D

NEW QUESTION 667

- (Exam Topic 6)

In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

- A. Network layer headers and the session layer port numbers
- B. Presentation layer headers and the session layer port numbers
- C. Application layer port numbers and the transport layer headers
- D. Transport layer port numbers and application layer headers

Answer: D

NEW QUESTION 670

- (Exam Topic 6)

A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

- A. Scanning
- B. Reconnaissance
- C. Escalation
- D. Enumeration

Answer: B

NEW QUESTION 672

- (Exam Topic 6)

You are about to be hired by a well-known Bank to perform penetration tests. Which of the following documents describes the specifics of the testing, the associated violations, and essentially protects both the bank's interest and your liabilities as a tester?

- A. Service Level Agreement
- B. Non-Disclosure Agreement
- C. Terms of Engagement
- D. Project Scope

Answer: C

NEW QUESTION 674

- (Exam Topic 6)

Which of the following Nmap commands would be used to perform a stack fingerprinting?

- A. Nmap -O -p80 <host(s.>
- B. Nmap -hU -Q<host(s.>
- C. Nmap -sT -p <host(s.>
- D. Nmap -u -o -w2 <host>
- E. Nmap -sS -0p targe

Answer: B

NEW QUESTION 677

- (Exam Topic 6)

Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

- A. Preparation phase
- B. Containment phase
- C. Recovery phase
- D. Identification phase

Answer: A

NEW QUESTION 678

- (Exam Topic 6)

It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that

reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

- A. SNMP
- B. ICMP
- C. SYSLOG
- D. SMS

Answer: C

NEW QUESTION 683

- (Exam Topic 6)

What does a type 3 code 13 represent? (Choose two.)

- A. Echo request
- B. Destination unreachable
- C. Network unreachable
- D. Administratively prohibited
- E. Port unreachable
- F. Time exceeded

Answer: BD

NEW QUESTION 684

- (Exam Topic 6)

Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

- A. NIST SP 800-53
- B. PCI-DSS
- C. EU Safe Harbor
- D. HIPAA

Answer: A

NEW QUESTION 687

- (Exam Topic 6)

There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

- A. Collision
- B. Collusion
- C. Polymorphism
- D. Escrow

Answer: A

NEW QUESTION 689

- (Exam Topic 6)

Name two software tools used for OS guessing? (Choose two.)

- A. Nmap
- B. Snadboy
- C. Queso
- D. UserInfo
- E. NetBus

Answer: AC

NEW QUESTION 690

- (Exam Topic 6)

Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

- A. Metasploit
- B. Wireshark
- C. Maltego
- D. Cain & Abel

Answer: C

NEW QUESTION 693

- (Exam Topic 6)

Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?

- A. 1433
- B. 161
- C. 445

D. 3389

Answer: C

NEW QUESTION 695

- (Exam Topic 6)

Jack was attempting to fingerprint all machines in the network using the following Nmap syntax: `invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24`
TCP/IP fingerprinting (for OS scan) xxxxxxxx xxxxxx xxxxxxxxxx. QUITTING! Obviously, it is not going through. What is the issue here?

- A. OS Scan requires root privileges
- B. The nmap syntax is wrong.
- C. The outgoing TCP/IP fingerprinting is blocked by the host firewall
- D. This is a common behavior for a corrupted nmap application

Answer: A

NEW QUESTION 700

- (Exam Topic 6)

Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

- A. Shellshock
- B. Rootshell
- C. Rootshock
- D. Shellbash

Answer: A

NEW QUESTION 702

- (Exam Topic 6)

A big company, who wanted to test their security infrastructure, wants to hire elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What should you do?

- A. Share reports, after NDA is signed
- B. Share full reports, not redacted
- C. Decline but, provide references
- D. Share full reports with redactions

Answer: C

NEW QUESTION 707

- (Exam Topic 6)

What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5?

- A. `nmap -T4 -F 10.10.0.0/24`
- B. `nmap -T4 -q 10.10.0.0/24`
- C. `nmap -T4 -O 10.10.0.0/24`
- D. `nmap -T4 -r 10.10.1.0/24`

Answer: A

NEW QUESTION 708

- (Exam Topic 6)

One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?

- A. Interview all employees in the company to rule out possible insider threats.
- B. Establish attribution to suspected attackers.
- C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
- D. Start the Wireshark application to start sniffing network traffic.

Answer: C

NEW QUESTION 710

- (Exam Topic 6)

An nmap command that includes the host specification of `202.176.56-57.*` will scan number of hosts.

- A. 2
- B. 256
- C. 512
- D. Over 10, 000

Answer: C

NEW QUESTION 712

- (Exam Topic 6)

If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

- A. Running a network scan to detect network services in the corporate DMZ
- B. Reviewing the need for a security clearance for each employee
- C. Using configuration management to determine when and where to apply security patches
- D. Training employees on the security policy regarding social engineering

Answer: A

NEW QUESTION 713

- (Exam Topic 6)

You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

- A. TCP/IP doesn't support ICMP
- B. ARP is disabled on the target server
- C. ICMP could be disabled on the target server
- D. You need to run the ping command with root privileges

Answer: C

NEW QUESTION 714

- (Exam Topic 6)

Which service in a PKI will vouch for the identity of an individual or company?

- A. KDC
- B. CA
- C. CR
- D. CBC

Answer: B

NEW QUESTION 717

- (Exam Topic 6)

A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.

77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

- A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
- B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
- C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
- D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Answer: B

NEW QUESTION 721

- (Exam Topic 6)

What kind of risk will remain even if all theoretically possible safety measures would be applied?

- A. Residual risk
- B. Inherent risk
- C. Impact risk
- D. Deferred risk

Answer: A

NEW QUESTION 722

- (Exam Topic 6)

Which of the following command line switch would you use for OS detection in Nmap?

- A. -D
- B. -O
- C. -P
- D. -X

Answer: B

NEW QUESTION 724

- (Exam Topic 6)

Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol would you implement?

- A. TACACS+
- B. DIAMETER
- C. Kerberos

D. RADIUS

Answer: D

NEW QUESTION 728

- (Exam Topic 6)

What attack is used to crack passwords by using a precomputed table of hashed passwords?

- A. Brute Force Attack
- B. Hybrid Attack
- C. Rainbow Table Attack
- D. Dictionary Attack

Answer: C

NEW QUESTION 733

- (Exam Topic 7)

E- mail scams and mail fraud are regulated by which of the following?

- A. 18 U.S.
- B. pa
- C. 1030 Fraud and Related activity in connection with Computers
- D. 18 U.S.
- E. pa
- F. 1029 Fraud and Related activity in connection with Access Devices
- G. 18 U.S.
- H. pa
- I. 1362 Communication Lines, Stations, or Systems
- J. 18 U.S.
- K. pa
- L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 735

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-50v10 Exam with Our Prep Materials Via below:

<https://www.certleader.com/312-50v10-dumps.html>