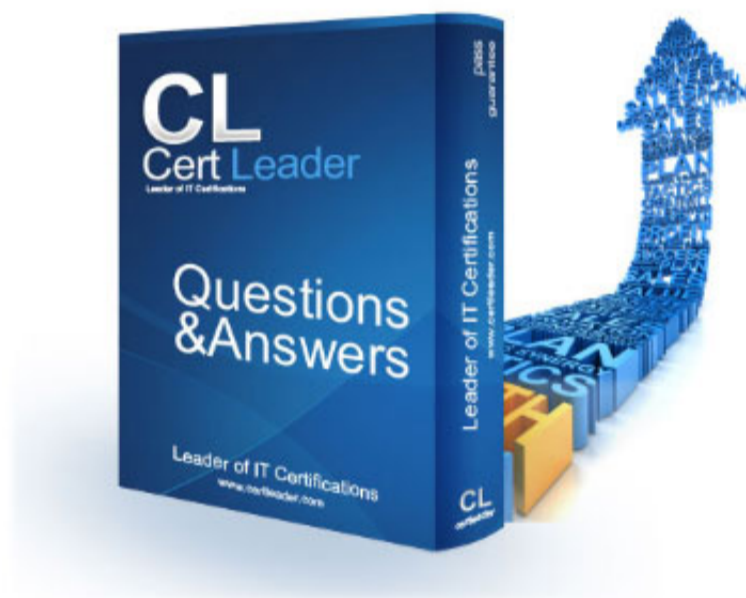


312-50v10 Dumps

Certified Ethical Hacker v10

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



NEW QUESTION 1

- (Exam Topic 1)

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 2

- (Exam Topic 1)

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

What is the main security risk associated with this scenario?

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

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

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 4

- (Exam Topic 1)

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/1.1Host: 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 5

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

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

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

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

Answer: D

NEW QUESTION 7

- (Exam Topic 1)

Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

- A. [cache:]
- B. [site:]
- C. [inurl:]
- D. [link:]

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

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 9

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 11

- (Exam Topic 1)

Cross-site request forgery involves:

- A. A request sent by a malicious user from a browser to a server
- B. Modification of a request by a proxy between client and server
- C. A browser making a request to a server without the user's knowledge
- D. A server making a request to another server without the user's knowledge

Answer: C

NEW QUESTION 15

- (Exam Topic 1)

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

- A. Banner Grabbing
- B. IDLE/IPID Scanning

- C. SSDP Scanning
- D. UDP Scanning

Answer: A

NEW QUESTION 20

- (Exam Topic 2)

The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

- A. Physical
- B. Procedural
- C. Technical
- D. Compliance

Answer: B

NEW QUESTION 22

- (Exam Topic 2)

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 27

- (Exam Topic 2)

What are the three types of authentication?

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

Answer: B

NEW QUESTION 28

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 30

- (Exam Topic 2)

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 31

- (Exam Topic 2)

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 35

- (Exam Topic 2)

A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company's building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

- A. Man trap
- B. Tailgating
- C. Shoulder surfing
- D. Social engineering

Answer: B

NEW QUESTION 36

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 40

- (Exam Topic 2)

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 45

- (Exam Topic 2)

If the final set of security controls does not eliminate all risk in a system, what could be done next?

- A. Continue to apply controls until there is zero risk.
- B. Ignore any remaining risk.
- C. If the residual risk is low enough, it can be accepted.
- D. Remove current controls since they are not completely effective.

Answer: C

NEW QUESTION 46

- (Exam Topic 2)

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

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

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

Answer: A

NEW QUESTION 47

- (Exam Topic 2)

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 51

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 56

- (Exam Topic 2)

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

- A. Host
- B. Stateful
- C. Stateless
- D. Application

Answer: C

NEW QUESTION 59

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 62

- (Exam Topic 2)

Bluetooth uses which digital modulation technique to exchange information between paired devices?

- A. PSK (phase-shift keying)
- B. FSK (frequency-shift keying)
- C. ASK (amplitude-shift keying)
- D. QAM (quadrature amplitude modulation)

Answer: A

Explanation:

Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK.

References:

<http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php>

NEW QUESTION 64

- (Exam Topic 2)

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 68

- (Exam Topic 2)

Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

- A. DataThief
- B. NetCat
- C. Cain and Abel
- D. SQLInjector

Answer: A

NEW QUESTION 71

- (Exam Topic 2)

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP

address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

Answer: D

NEW QUESTION 72

- (Exam Topic 2)

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 74

- (Exam Topic 2)

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus
- B. Multipart virus
- C. Macro virus
- D. Stealth virus

Answer: C

Explanation:

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.

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

NEW QUESTION 77

- (Exam Topic 2)

Which of the following is a symmetric cryptographic standard?

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

Answer: D

NEW QUESTION 81

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 86

- (Exam Topic 2)

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 90

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 95

- (Exam Topic 2)

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 97

- (Exam Topic 3)

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 101

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 103

- (Exam Topic 3)

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 105

- (Exam Topic 3)

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 108

- (Exam Topic 3)

Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

- A. Cross-site scripting
- B. SQL injection
- C. VPath injection
- D. XML denial of service issues

Answer: D

NEW QUESTION 112

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 116

- (Exam Topic 3)

Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

- A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
- B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
- C. Hashing is faster compared to more traditional encryption algorithms.
- D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Answer: D

NEW QUESTION 117

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 120

- (Exam Topic 3)

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Hping
- B. Traceroute
- C. TCP ping
- D. Broadcast ping

Answer: A

NEW QUESTION 123

- (Exam Topic 3)

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 124

- (Exam Topic 3)

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 127

- (Exam Topic 3)

A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

- A. Say nothing and continue with the security testing.
- B. Stop work immediately and contact the authorities.
- C. Delete the pornography, say nothing, and continue security testing.
- D. Bring the discovery to the financial organization's human resource department.

Answer: B

NEW QUESTION 131

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 133

- (Exam Topic 3)

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 137

- (Exam Topic 3)

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 140

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 142

- (Exam Topic 3)

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 147

- (Exam Topic 3)

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 148

- (Exam Topic 3)

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

- A. Implementing server-side PKI certificates for all connections

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

Answer: C

NEW QUESTION 152

- (Exam Topic 4)

When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.

What command will help you to search files using Google as a search engine?

- A. site: target.com filetype:xls username password email
- B. inurl: target.com filename:xls username password email
- C. domain: target.com archive:xls username password email
- D. site: target.com file:xls username password email

Answer: A

Explanation:

If you include site: in your query, Google will restrict your search results to the site or domain you specify. If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms “web,” “page,” “evaluation,” and “checklist.”

References:

http://www.googleguide.com/advanced_operators_reference.html

NEW QUESTION 154

- (Exam Topic 4)

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 159

- (Exam Topic 4)

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

- A. Private
- B. Public
- C. Shared
- D. Root

Answer: A

Explanation:

The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.

An attack may also reveal private keys of compromised parties. References: <https://en.wikipedia.org/wiki/Heartbleed>

NEW QUESTION 163

- (Exam Topic 4)

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

What type of firewall is inspecting outbound traffic?

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

Answer: A

Explanation:

An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control

the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

References:

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

NEW QUESTION 166

- (Exam Topic 4)

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 171

- (Exam Topic 4)

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 176

- (Exam Topic 4)

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

- A. Burpsuite
- B. Maskgen
- C. Dimitry
- D. Proxychains

Answer: A

Explanation:

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

References: <https://portswigger.net/burp/>

NEW QUESTION 177

- (Exam Topic 4)

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

What is this style of attack called?

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

Answer: A

Explanation:

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

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

NEW QUESTION 182

- (Exam Topic 4)

Which of the following is assured by the use of a hash?

- A. Integrity
- B. Confidentiality
- C. Authentication
- D. Availability

Answer: A

Explanation:

An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

References: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

NEW QUESTION 187

- (Exam Topic 4)

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. tcpdump
- B. nessus
- C. etherea
- D. Jack the ripper

Answer: A

Explanation:

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP

and other packets being transmitted or received over a network to which the computer is attached. References: <https://en.wikipedia.org/wiki/Tcpdump>

NEW QUESTION 189

- (Exam Topic 4)

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- A. PKI
- B. single sign on
- C. biometrics
- D. SOA

Answer: A

Explanation:

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates [1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

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

NEW QUESTION 192

- (Exam Topic 4)

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

Which of the following terms best matches the definition?

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

Answer: A

Explanation:

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

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

NEW QUESTION 197

- (Exam Topic 4)

It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.

Which of the following terms best matches the definition?

- A. Threat
- B. Attack
- C. Vulnerability
- D. Risk

Answer: A

Explanation:

A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

References: [https://en.wikipedia.org/wiki/Threat_\(computer\)](https://en.wikipedia.org/wiki/Threat_(computer))

NEW QUESTION 201

- (Exam Topic 4)

While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

Which type of vulnerability is present on this site?

- A. Web Parameter Tampering
- B. Cookie Tampering
- C. XSS Reflection
- D. SQL injection

Answer: A

Explanation:

The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

NEW QUESTION 205

- (Exam Topic 4)

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Hosts
- B. Sudoers
- C. Boot.ini
- D. Networks

Answer: A

Explanation:

The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.

References: [https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file))

NEW QUESTION 207

- (Exam Topic 5)

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

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

Answer: A

Explanation:

A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

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

NEW QUESTION 212

- (Exam Topic 5)

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

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

Answer: A

Explanation:

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

References:

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

NEW QUESTION 216

- (Exam Topic 5)

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security

policies. Which one of the following tools would most likely be used in such an audit?

- A. Vulnerability scanner
- B. Protocol analyzer
- C. Port scanner
- D. Intrusion Detection System

Answer: A

Explanation:

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

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

NEW QUESTION 220

- (Exam Topic 5)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 225

- (Exam Topic 5)

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

What is the most likely cause?

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

Answer: A

Explanation:

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

References:

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

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

NEW QUESTION 229

- (Exam Topic 5)

In Risk Management, how is the term "likelihood" related to the concept of "threat?"

- A. Likelihood is the probability that a threat-source will exploit a vulnerability.
- B. Likelihood is a possible threat-source that may exploit a vulnerability.
- C. Likelihood is the likely source of a threat that could exploit a vulnerability.
- D. Likelihood is the probability that a vulnerability is a threat-source.

Answer: A

Explanation:

The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.

References:

<http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attac>

NEW QUESTION 233

- (Exam Topic 5)

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

- A. Civil
- B. International

- C. Criminal
- D. Common

Answer: A

NEW QUESTION 238

- (Exam Topic 5)

An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

- A. Insufficient input validation
- B. Insufficient exception handling
- C. Insufficient database hardening
- D. Insufficient security management

Answer: A

Explanation:

The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

References: https://www.owasp.org/index.php/Testing_for_Input_Validation

NEW QUESTION 243

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 244

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 249

- (Exam Topic 5)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

- A. Kismet
- B. Nessus
- C. Netstumbler
- D. Abel

Answer: A

Explanation:

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: [https://en.wikipedia.org/wiki/Kismet_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))

NEW QUESTION 254

- (Exam Topic 5)

Which method of password cracking takes the most time and effort?

- A. Brute force
- B. Rainbow tables
- C. Dictionary attack
- D. Shoulder surfing

Answer: A

Explanation:

Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be

attempted before brute force.

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

NEW QUESTION 257

- (Exam Topic 5)

By using a smart card and pin, you are using a two-factor authentication that satisfies

- A. Something you know and something you are
- B. Something you have and something you know
- C. Something you have and something you are
- D. Something you are and something you remember

Answer: B

NEW QUESTION 262

- (Exam Topic 5)

Which of the following security operations is used for determining the attack surface of an organization?

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

Answer: A

Explanation:

For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

References:

<http://meisecurity.com/home/consulting/consulting-network-scanning/>

NEW QUESTION 266

- (Exam Topic 5)

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- A. tcptrace
- B. tcptraceroute
- C. Nessus
- D. OpenVAS

Answer: A

Explanation:

tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

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

NEW QUESTION 269

- (Exam Topic 5)

Which of the following statements regarding ethical hacking is incorrect?

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

Answer: A

Explanation:

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

References:

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

NEW QUESTION 273

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 277

- (Exam Topic 5)

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

- A. Only using OSPFv3 will mitigate this risk.
- B. Make sure that legitimate network routers are configured to run routing protocols with authentication.
- C. Redirection of the traffic cannot happen unless the admin allows it explicitly.
- D. Disable all routing protocols and only use static routes.

Answer: B

NEW QUESTION 278

- (Exam Topic 5)

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

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

Answer: A

Explanation:

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

References:

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

NEW QUESTION 279

- (Exam Topic 5)

In order to have an anonymous Internet surf, which of the following is best choice?

- A. Use SSL sites when entering personal information
- B. Use Tor network with multi-node
- C. Use shared WiFi
- D. Use public VPN

Answer: B

NEW QUESTION 284

- (Exam Topic 5)

What is correct about digital signatures?

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

Answer: A

NEW QUESTION 289

- (Exam Topic 5)

What is the role of test automation in security testing?

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

Answer: A

NEW QUESTION 294

- (Exam Topic 5)

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

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 296

- (Exam Topic 5)

Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.

What technique is Ricardo using?

- A. Steganography
- B. Public-key cryptography
- C. RSA algorithm
- D. Encryption

Answer: A

Explanation:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

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

NEW QUESTION 297

- (Exam Topic 5)

The security concept of "separation of duties" is most similar to the operation of which type of security device?

- A. Firewall
- B. Bastion host
- C. Intrusion Detection System
- D. Honeypot

Answer: A

Explanation:

In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References:

<http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-d>

NEW QUESTION 298

- (Exam Topic 5)

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

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

Answer: A

Explanation:

Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

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

NEW QUESTION 302

- (Exam Topic 6)

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

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

Answer: C

NEW QUESTION 306

- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 308

- (Exam Topic 6)

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

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

Answer: B

NEW QUESTION 312

- (Exam Topic 6)

Which of the following is a wireless network detector that is commonly found on Linux?

- A. Kismet
- B. Abel
- C. Netstumbler
- D. Nessus

Answer: A

NEW QUESTION 313

- (Exam Topic 6)

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

Fill in the blank with appropriate choice.

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

Answer: B

NEW QUESTION 316

- (Exam Topic 6)

Which of the following commands runs snort in packet logger mode?

- A. ./snort -dev -h ./log
- B. ./snort -dev -l ./log
- C. ./snort -dev -o ./log
- D. ./snort -dev -p ./log

Answer: B

NEW QUESTION 318

- (Exam Topic 6)

While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

- A. The port will send an ACK
- B. The port will send a SYN
- C. The port will ignore the packets
- D. The port will send an RST

Answer: C

NEW QUESTION 323

- (Exam Topic 6)

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

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

Answer: C

NEW QUESTION 325

- (Exam Topic 6)

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139.

What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP
- C. Samba
- D. SMB

Answer: D

NEW QUESTION 329

- (Exam Topic 6)

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

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

Answer: B

NEW QUESTION 330

- (Exam Topic 6)

What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?

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

Answer: B

NEW QUESTION 335

- (Exam Topic 6)

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

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

Answer: B

NEW QUESTION 340

- (Exam Topic 6)

It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

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

Answer: C

NEW QUESTION 342

- (Exam Topic 6)

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

- A. Role Based Access Control (RBAC)
- B. Discretionary Access Control (DAC)
- C. Windows authentication
- D. Single sign-on

Answer: D

NEW QUESTION 343

- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 347

- (Exam Topic 6)

Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

- A. Nothing, but suggest to him to change the network's SSID and password.
- B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
- C. Log onto to his network, after all it's his fault that you can get in.
- D. Only use his network when you have large downloads so you don't tax your own network.

Answer: A

NEW QUESTION 351

- (Exam Topic 6)

It is a short-range wireless communication technology that allows mobile phones, computers and other devices to connect and communicate. This technology intends to replace cables connecting portable devices with high regards to security.

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

Answer: A

NEW QUESTION 354

- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 355

- (Exam Topic 6)

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

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

Answer: C

NEW QUESTION 358

- (Exam Topic 6)

Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

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

Answer: D

NEW QUESTION 360

- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 363

- (Exam Topic 6)

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

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

Answer: B

NEW QUESTION 364

- (Exam Topic 6)

What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of \$300 given that the technician who charges \$10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

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

Answer: D

NEW QUESTION 369

- (Exam Topic 6)

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

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

Answer: D

NEW QUESTION 370

- (Exam Topic 7)

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

Answer: B

NEW QUESTION 372

- (Exam Topic 7)

This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Hybrid
- B. Linear
- C. Symmetric
- D. Brute Force

Answer: A

NEW QUESTION 374

- (Exam Topic 7)

Within the context of Computer Security, which of the following statements describes Social Engineering best?

- A. Social Engineering is the act of publicly disclosing information
- B. Social Engineering is the means put in place by human resource to perform time accounting
- C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
- D. Social Engineering is a training program within sociology studies

Answer: C

NEW QUESTION 377

- (Exam Topic 7)

One of your team members has asked you to analyze the following SOA record. What is the version? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

Answer: A

NEW QUESTION 378

- (Exam Topic 7)

Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

- A. Take over the session
- B. Reverse sequence prediction
- C. Guess the sequence numbers
- D. Take one of the parties offline

Answer: C

NEW QUESTION 380

- (Exam Topic 7)

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

- A. BA810DBA98995F1817306D272A9441BB
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. 0182BD0BD4444BF836077A718CCDF409
- D. CEC52EB9C8E3455DC2265B23734E0DAC
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: BE

NEW QUESTION 382

- (Exam Topic 7)

What is a NULL scan?

- A. A scan in which all flags are turned off
- B. A scan in which certain flags are off
- C. A scan in which all flags are on
- D. A scan in which the packet size is set to zero
- E. A scan with an illegal packet size

Answer: A

NEW QUESTION 383

- (Exam Topic 7)

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
- D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NEW QUESTION 384

- (Exam Topic 7)

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

If these switches' ARP cache is successfully flooded, what will be the result?

- A. The switches will drop into hub mode if the ARP cache is successfully flooded.
- B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
- C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
- D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

NEW QUESTION 385

- (Exam Topic 7)

Which definition among those given below best describes a covert channel?

- A. A server program using a port that is not well known.
- B. Making use of a protocol in a way it is not intended to be used.
- C. It is the multiplexing taking place on a communication link.
- D. It is one of the weak channels used by WEP which makes it insecure

Answer: B

NEW QUESTION 390

- (Exam Topic 7)

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

Answer: C

NEW QUESTION 394

- (Exam Topic 7)

Which of the following tools can be used to perform a zone transfer?

- A. NSLookup
- B. Finger
- C. Dig
- D. Sam Spade
- E. Host
- F. Netcat
- G. Neotrace

Answer: ACDE

NEW QUESTION 399

- (Exam Topic 7)

Which of the following are well known password-cracking programs?

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

Answer: AE

NEW QUESTION 402

- (Exam Topic 7)

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: `nmap -Pn -p- -si kiosk.adobe.com www.riaa.com`. `kiosk.adobe.com` is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

- A. Conduct stealth scan
- B. Conduct ICMP scan
- C. Conduct IDLE scan
- D. Conduct silent scan

Answer: A

NEW QUESTION 405

- (Exam Topic 7)

An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: `netcat -l -p -s password 1234 < testfile` Machine B: `netcat <machine A IP> 1234`
- B. Machine A: `netcat -l -e magickey -p 1234 < testfile` Machine B: `netcat <machine A IP> 1234`
- C. Machine A: `netcat -l -p 1234 < testfile -pw password` Machine B: `netcat <machine A IP> 1234 -pw password`
- D. Use cryptcat instead of netcat

Answer: D

NEW QUESTION 406

- (Exam Topic 7)

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *  
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as a user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

Answer: C

NEW QUESTION 408

- (Exam Topic 7)

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

- A. Do not reply to email messages or popup ads asking for personal or financial information
- B. Do not trust telephone numbers in e-mails or popup ads
- C. Review credit card and bank account statements regularly
- D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
- E. Do not send credit card numbers, and personal or financial information via e-mail

Answer: D

NEW QUESTION 409

- (Exam Topic 7)

In Trojan terminology, what is a covert channel?



- A. A channel that transfers information within a computer system or network in a way that violates the security policy
- B. A legitimate communication path within a computer system or network for transfer of data
- C. It is a kernel operation that hides boot processes and services to mask detection
- D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Answer: A

NEW QUESTION 410

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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