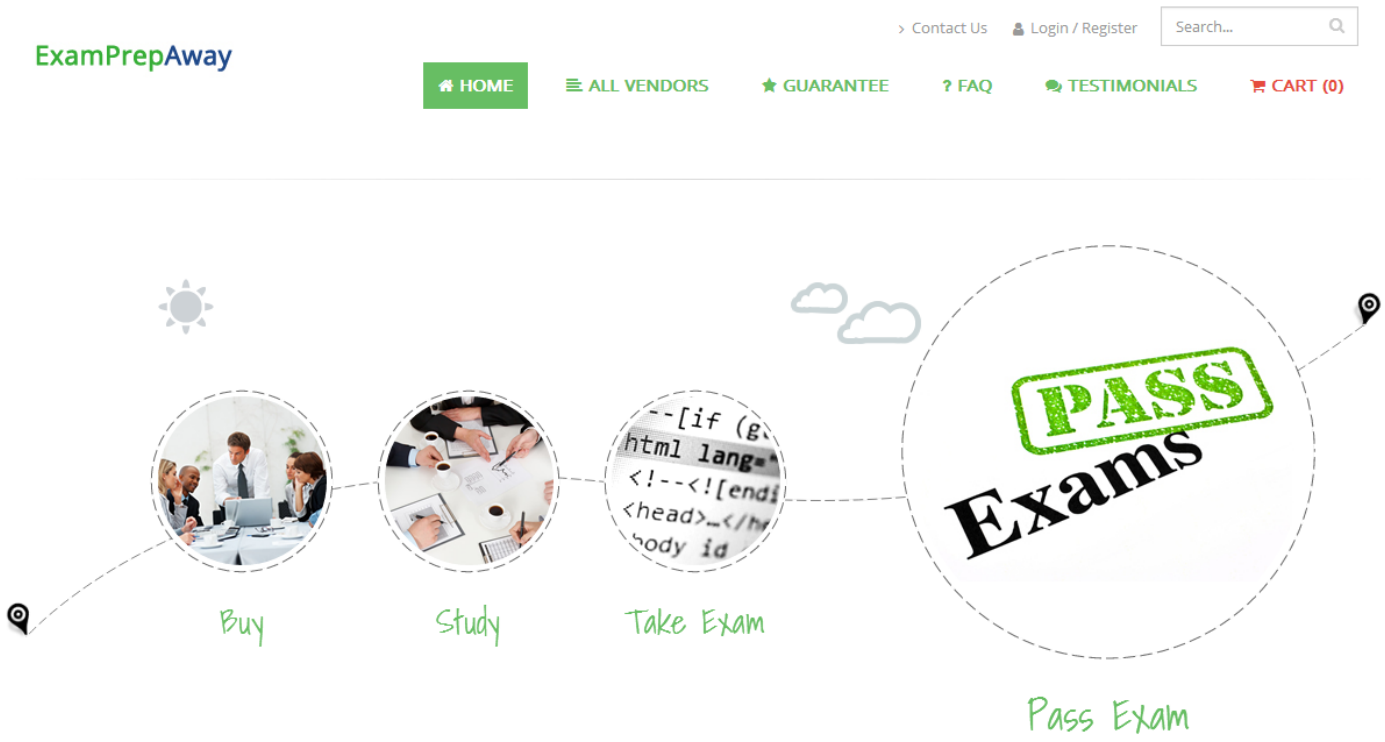
ExamPrepAway



Try **Online Engine** before you buy

We're not the only ones **happy** about ExamPrepAway Practice Material ...

56295+ customers in 100+ countries use ExamPrepAway Test Engine. Meet our customers.

GetCustom JET ORANGE iCompany Paradoxx iMessenger VOREED

http://www.examprepaway.com/

Latest Exam Guide & Learning Materials

Exam : **412-79v8**

Title : EC-Council Certified Security Analyst (ECSA)

Vendor : EC-COUNCIL

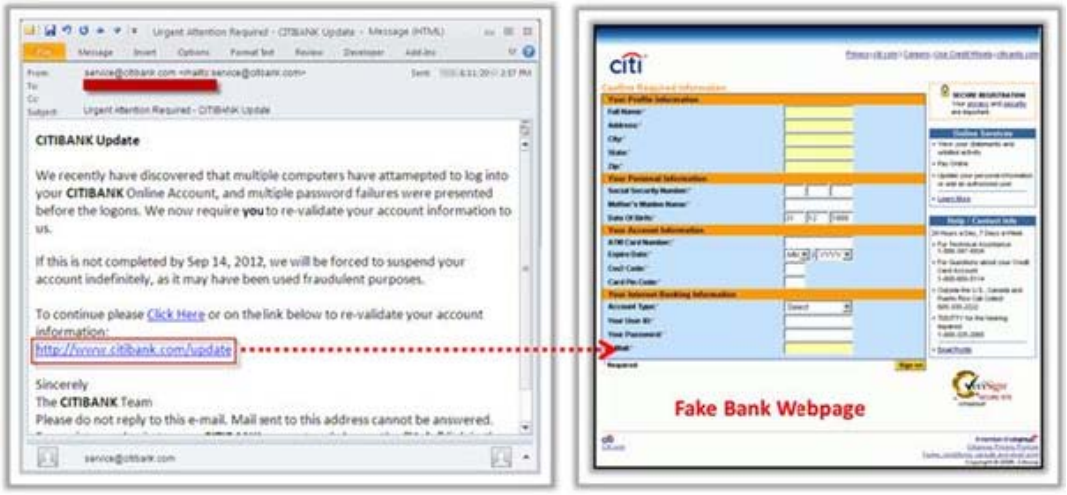
Version : DEMO

NO.1 A security policy is a document or set of documents that describes, at a high level, the security controls that will be implemented by the company.
Which one of the following policies forbids everything and restricts usage of company computers, whether it is system usage or network usage?
A. Paranoid Policy
B. Prudent Policy
C. Promiscuous Policy
D. Information-Protection Policy
Answer: A

NO.2 Variables are used to define parameters for detection, specifically those of your local network and/or specific servers or ports for inclusion or exclusion in rules. These are simple substitution variables set with the var keyword. Which one of the following operator is used to define metavariables?
A. "$"
B. "#"
C. "*"
D. "?"
Answer: A

NO.3 In which of the following firewalls are the incoming or outgoing packets blocked from accessing services for which there is no proxy?
A. Circuit level firewalls
B. Packet filters firewalls
C. Stateful multilayer inspection firewalls
D. Application level firewalls
Answer: D
Reference:http://www.vicomsoft.com/learning-center/firewalls/

NO.4 Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.



What characteristics do phishing messages often have that may make them identifiable?
A. Invalid email signatures or contact information
B. Suspiciously good grammar and capitalization
C. They trigger warning pop-ups
D. Suspicious attachments
Answer: C

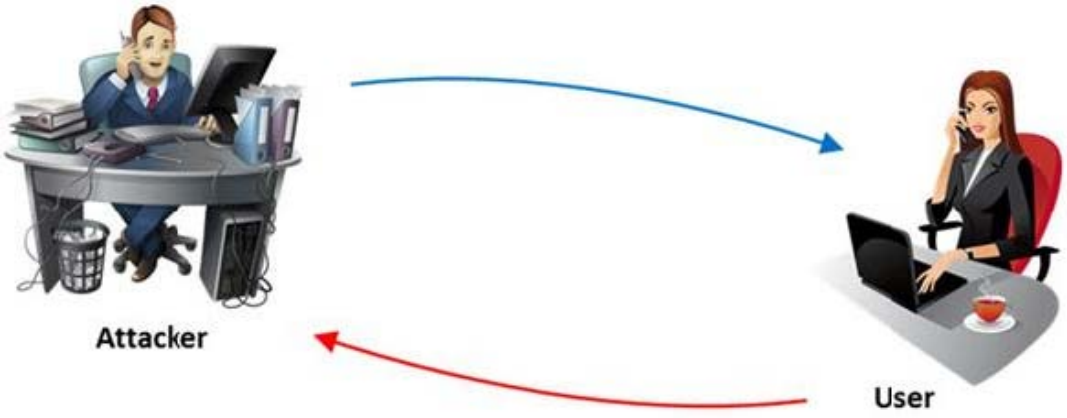
NO.5 Which of the following scan option is able to identify the SSL services?
A. -sS
B. -sV
C. -sU
D. -sT
Answer: B
Reference:https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001) (blackboxtest and example, second para)

NO.6 Network scanning is used to identify the available network resources. Which one of the following is also known as a half-open scan, because a full TCP connection is never completed and it is used to determine which ports are open and listening on a target device?
A. SYN Scan
B. TCP Connect Scan
C. XMAS Scan
D. Null Scan
Answer: A

NO.7 A firewall's decision to forward or reject traffic in network filtering is dependent upon which of the following?
A. Destination address
B. Port numbers
C. Source address
D. Protocol used

Answer: D
Reference:http://www.vicomsoft.com/learning-center/firewalls/(what does afirewall do)

NO.8 The term social engineering is used to describe the various tricks used to fool people (employees, business partners, or customers) into voluntarily giving away information that would not normally be known to the general public.



What is the criminal practice of social engineering where an attacker uses the telephone system in an attempt to scam the user into surrendering private information?
A. Phishing
B. Spoofing
C. Tapping
D. Vishing
Answer: D

NO.9 Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing. Management decide to block all such web sites using URL filtering software.

How can employees continue to see the blocked websites?
A. Using session hijacking
B. Using proxy servers
C. Using authentication
D. Using encryption
Answer: B

NO.10 Many security and compliance projects begin with a simple idea: assess the organization's risk, vulnerabilities, and breaches. Implementing an IT security risk assessment is critical to the overall

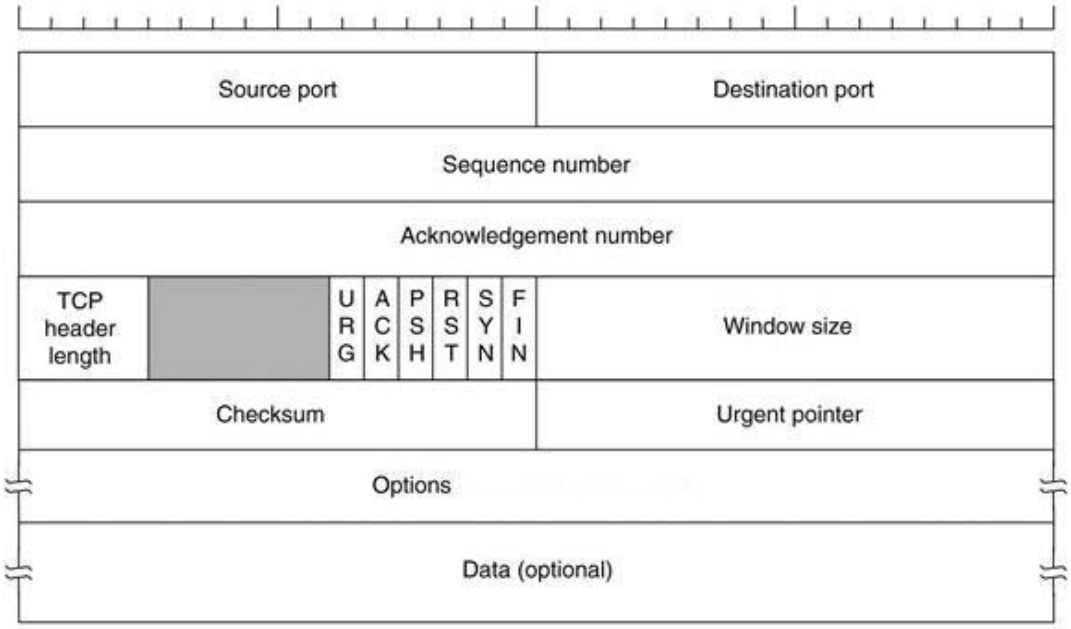
security posture of any organization.
An effective security risk assessment can prevent breaches and reduce the impact of realized breaches.

What is the formula to calculate risk?
A. Risk = Budget x Time
B. Risk = Goodwill x Reputation
C. Risk = Loss x Exposure factor
D. Risk = Threats x Attacks
Answer: C

NO.11 Which of the following is the objective of Gramm-Leach-Bliley Act?
A. To ease the transfer of financial information between institutions and banks
B. To protect the confidentiality, integrity, and availability of data
C. To set a new or enhanced standards for all U.S. public company boards, management and public accounting firms
D. To certify the accuracy of the reported financial statement
Answer: A
Reference:http://www.itap.purdue.edu/security/policies/glb_safeguards_rule_training_general.pdf

NO.12 Transmission control protocol accepts data from a data stream, divides it into chunks, and

adds a
TCP header creating a TCP segment.
The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints. For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side
The below diagram shows the TCP Header format:

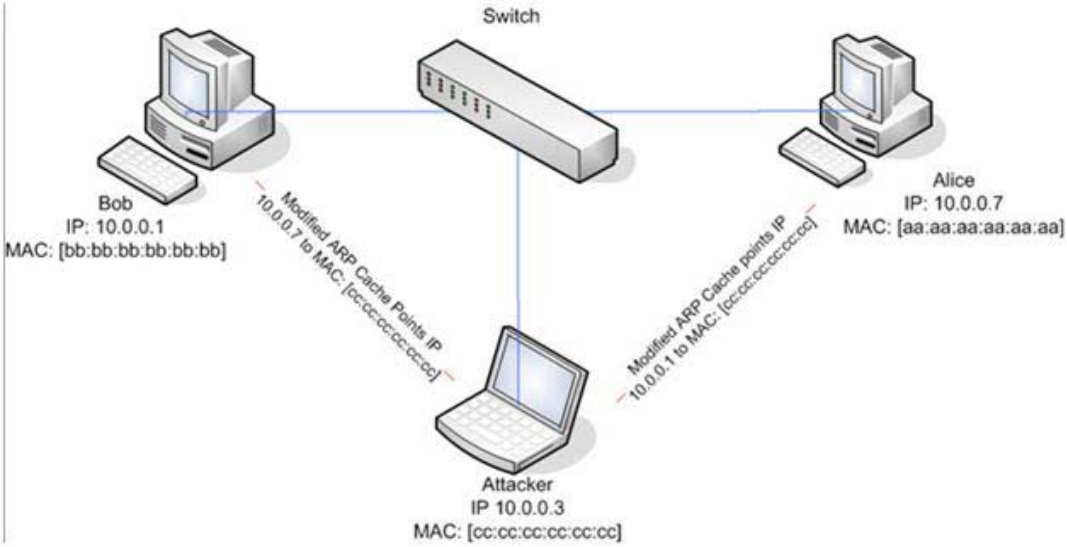


How many bits is a acknowledgement number?
A. 16 bits
B. 32 bits
C. 8 bits
D. 24 bits
Answer: B
Reference:http://en.wikipedia.org/wiki/Transmission_Control_Protocol(acknowledgement number)

NO.13 Assessing a network from a hacker's point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?
A. Network Assessments
B. Application Assessments
C. Wireless Network Assessments
D. External Assessment
Answer: D
Reference:http://controlcase.com/managed_compliance_pci_vulnerability_scan.html

NO.14 ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic

meant for that IP address to be sent to the attacker instead.
ARP spoofing attack is used as an opening for other attacks.



What type of attack would you launch after successfully deploying ARP spoofing?
A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking
Answer: D
ence:http://en.wikipedia.org/wiki/ARP_spoofing

NO.15 The first phase of the penetration testing plan is to develop the scope of the project in consultation with the client. Pen testing test components depend on the client's operating environment, threat perception, security and compliance requirements, ROE, and budget. Various components need to be considered for testing while developing the scope of the project.

Which of the following is NOT a pen testing component to be tested?
A. System Software Security
B. Intrusion Detection
C. Outside Accomplices
D. Inside Accomplices
Answer: C