QUESTION 67
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 Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool

should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy
C. Blooover
D. BBCrack

Correct Answer: B

QUESTION 68
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

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

Correct Answer: A

QUESTION 69
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C

QUESTION 70
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering

B. Eavesdropping
C. Scanning
D. Sniffing

Correct Answer: A

QUESTION 71
Which system consists of a publicly available set of databases that contain domain name registration contact information?

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

Correct Answer: A

QUESTION 72
Why is a penetration test considered to be more thorough than vulnerability scan?

  A. Vulnerability scans only do host discovery and port scanning by default.
  B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
  C. It is not – a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
  D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Correct Answer: B

QUESTION 73
Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

  A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
  B. This is a scam because Bob does not know Scott.
  C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
  D. This is probably a legitimate message as it comes from a respectable organization.

Correct Answer: A

QUESTION 74
env x='(){ ::};echo exploit' bash –c 'cat/etc/passwd'

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

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

Correct Answer: D

QUESTION 75
Which of the following is assured by the use of a hash?

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

Correct Answer: D

QUESTION 76
Which results will be returned with the following Google search query? site:target.com – site:Marketing.target.com accounting

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

Correct Answer: D

QUESTION 77
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
B. UPGRADETLS
C. FORCETLS
D. STARTTLS

Correct Answer: D

QUESTION 78
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

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

Correct Answer: C

QUESTION 79
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.srcport= = 514 && ip.src= = 192.168.0.99 B.
tcp.srcport= = 514 && ip.src= = 192.168.150 C. tcp.dstport= =
514 && ip.dst= = 192.168.0.99 D. tcp.dstport= = 514 &&
ip.dst= = 192.168.0.150

Correct Answer: D

QUESTION 80
What two conditions must a digital signature meet?

A. Has to be the same number of characters as a physical signature and must be unique.
B. Has to be unforgeable, and has to be authentic.
C. Must be unique and have special characters.
D. Has to be legible and neat.

Correct Answer: B

QUESTION 81
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

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

Correct Answer: B

QUESTION 82
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.

Correct Answer: A

QUESTION 83
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat this action so that it escalates to a DoS attack.
D. He will repeat the same attack against all L2 switches of the network.

Correct Answer: A