ECCouncil

Exam 312-50v8

Certified Ethical Hacker v8 Exam

Version: 7.0

[Total Questions: 357]

Topic break down

Topic	No. of Questions
Topic 1: Background	38
Topic 3: Security	57
Topic 4: Tools /Systems /Programs	74
Topic 5: Procedures/ Methodology	47
Topic 6: Regulations / Policy	10
Topic 7: Ethics	131

Topic 1, Background

Question No : 1 - (Topic 1)

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

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

Answer: C

Question No : 2 - (Topic 1)

A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Information reporting
B. Vulnerability assessment
C. Active information gathering
D. Passive information gathering

Answer: D

Question No : 3 - (Topic 1)

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

Question No : 4 - (Topic 1)

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

Question No : 5 - (Topic 1)

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

Question No : 6 - (Topic 1)

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

Question No : 7 - (Topic 1)

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

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

Answer: C

Question No : 8 - (Topic 1)

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

Question No : 9 - (Topic 1)

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

Question No : 10 - (Topic 1)

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

Question No : 11 - (Topic 1)

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

Question No : 12 - (Topic 1)

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

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

Answer: B

Question No : 13 - (Topic 1)

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

Question No : 14 - (Topic 1)

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

Question No : 15 - (Topic 1)

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

Question No : 16 - (Topic 1)

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

Question No : 17 - (Topic 1)

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

Question No : 18 - (Topic 1)

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Reflective
C. Active
D. Distributive

Answer: C

Question No : 19 - (Topic 1)

Which of the following is an application that requires a host application for replication?

A. Micro
B. Worm
C. Trojan
D. Virus

Answer: D

Question No : 20 - (Topic 1)

Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

Answer: C

Question No : 21 - (Topic 1)

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

Question No : 22 - (Topic 1)

A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the