

ECCouncil

Exam ECSAv8

EC-Council Certified Security Analyst (ECSA)

Version: 10.3

[Total Questions: 200]

Question No : 1

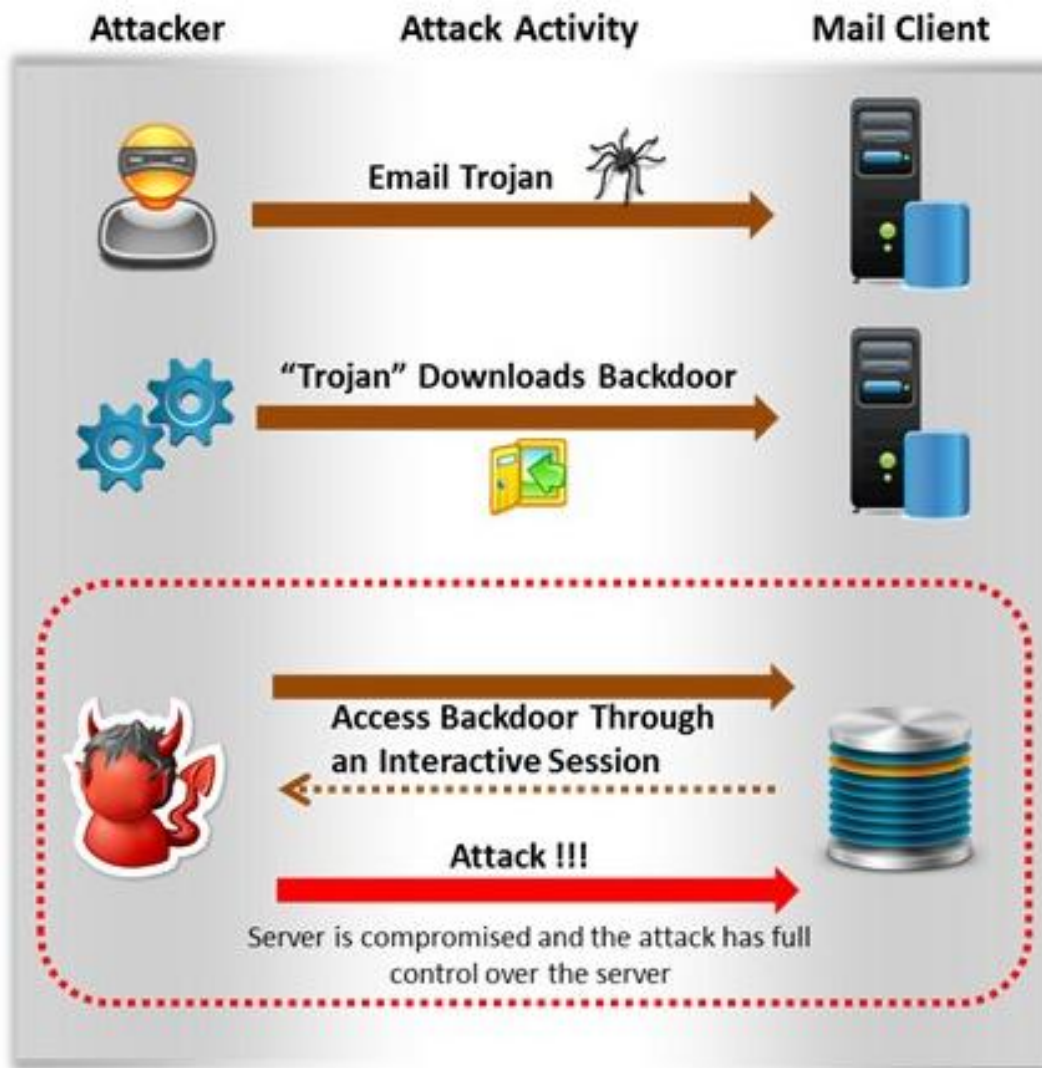
Which one of the following tools of trade is an automated, comprehensive penetration testing product for assessing the specific information security threats to an organization?

- A. Sunbelt Network Security Inspector (SNSI)
- B. CORE Impact
- C. Canvas
- D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

Question No : 2

Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.



Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

- A. Internal network mapping to map the internal network of the target machine
- B. Port scanning to determine what ports are open or in use on the target machine
- C. Sniffing to monitor all the incoming and outgoing network traffic
- D. Social engineering and spear phishing attacks to install malicious programs on the target machine

Answer: D

Question No : 3

Which of the following reports provides a summary of the complete pen testing process, its outcomes, and recommendations?

- A. Vulnerability Report
- B. Executive Report
- C. Client-side test Report
- D. Host Report

Answer: B

Question No : 4

Which of the following statements is true about the LM hash?

- A. Disabled in Windows Vista and 7 OSs
- B. Separated into two 8-character strings
- C. Letters are converted to the lowercase
- D. Padded with NULL to 16 characters

Answer: A

Reference: http://www.onlinehashcrack.com/how_to_crack_windows_passwords.php (first paragraph of the page)

Question No : 5

A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?

- A. Shoulder surfing
- B. Phishing
- C. Insider Accomplice
- D. Vishing

Answer: A

Question No : 6

During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

- A. Examine Source of the Available Pages
- B. Perform Web Spidering
- C. Perform Banner Grabbing
- D. Check the HTTP and HTML Processing by the Browser

Answer: D

Question No : 7

Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

- A. 3001-3100
- B. 5000-5099
- C. 6666-6674
- D. 0 – 1023

Answer: D

Reference: <https://www.ietf.org/rfc/rfc1700.txt> (well known port numbers, 4th para)

Question No : 8

Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businessService, bindingTemplate, and tModel?

- A. Web Services Footprinting Attack
- B. Service Level Configuration Attacks
- C. URL Tampering Attacks
- D. Inside Attacks

Answer: A

Reference: <http://www.scribd.com/doc/184891017/CEHv8-Module-13-Hacking-Web-Applications-pdf> (page 99)

Question No : 9

Which of the following statements is true about Multi-Layer Intrusion Detection Systems (mIDSs)?

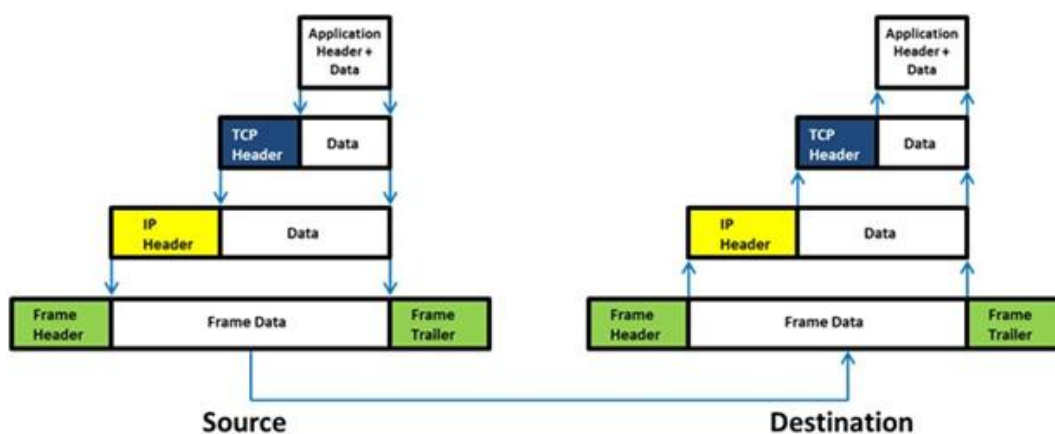
- A. Decreases consumed employee time and increases system uptime
- B. Increases detection and reaction time
- C. Increases response time
- D. Both a and c

Answer: A

Reference: <http://www.symantec.com/connect/articles/multi-layer-intrusion-detection-systems> (economic advantages, first para)

Question No : 10

Which of the following statement holds true for TCP Operation?



- A. Port numbers are used to know which application the receiving host should pass the data to
- B. Sequence numbers are used to track the number of packets lost in transmission
- C. Flow control shows the trend of a transmitting host overflowing the buffers in the receiving host
- D. Data transfer begins even before the connection is established

Answer: D

Question No : 11

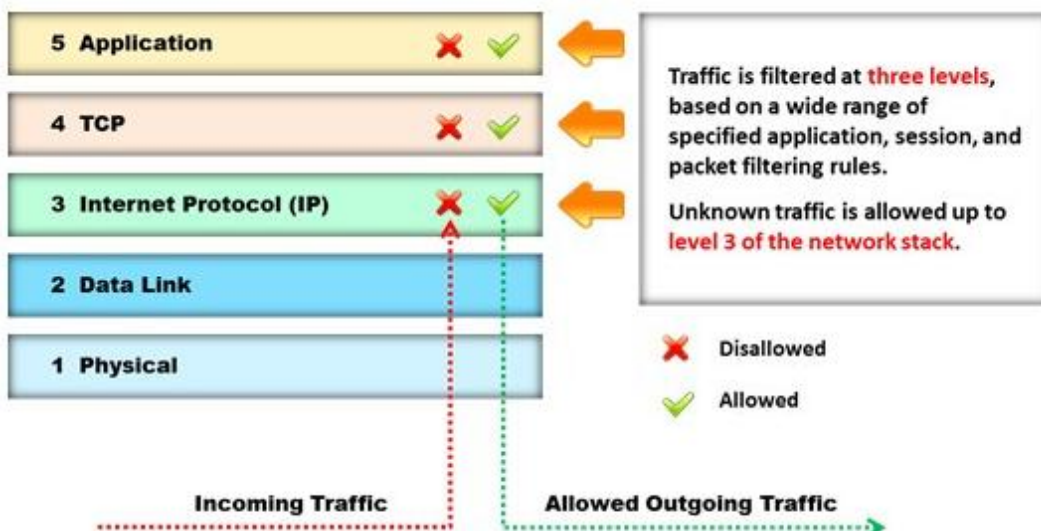
Logs are the record of the system and network activities. Syslog protocol is used for delivering log information across an IP network. Syslog messages can be sent via which one of the following?

- A. UDP and TCP
- B. TCP and SMTP
- C. SMTP
- D. UDP and SMTP

Answer: A

Question No : 12

Identify the type of firewall represented in the diagram below:



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

Answer: A

Reference: <http://www.technicolorbroadbandpartner.com/getfile.php?id=4159> (page 13)

Question No : 13

Timing is an element of port-scanning that can catch one unaware. If scans are taking too long to complete or obvious ports are missing from the scan, various time parameters may need to be adjusted. Which one of the following scanned timing options in NMAP's scan is useful across slow WAN links or to hide the scan?

- A. Paranoid
- B. Sneaky
- C. Polite
- D. Normal

Answer: C

Question No : 14

Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

- A. Reverse Address Resolution Protocol (RARP)
- B. HTTP (Hypertext Transfer Protocol)
- C. SMTP (Simple Mail Transfer Protocol)
- D. Telnet

Answer: A

Question No : 15

Which of the following approaches to vulnerability assessment relies on the administrator providing baseline of system configuration and then scanning continuously without incorporating any information found at the time of scanning?



- A. Service-based Assessment Solutions
- B. Product-based Assessment Solutions
- C. Tree-based Assessment
- D. Inference-based Assessment

Answer: C

Reference: http://www.netsense.info/downloads/security_wp_mva.pdf (page 12, tree-based assessment technology, second para)

Question No : 16

Which of the following documents helps in creating a confidential relationship between the pen tester and client to protect critical and confidential information or trade secrets?

- A. Penetration Testing Agreement
- B. Rules of Behavior Agreement
- C. Liability Insurance
- D. Non-Disclosure Agreement

Answer: D

Question No : 17

Internet Control Message Protocol (ICMP) messages occur in many situations, such as whenever a datagram cannot reach the destination or the gateway does not have the buffering capacity to forward a datagram. Each ICMP message contains three fields: type, code, and checksum. Different types of Internet Control Message Protocols (ICMPs) are identified by a TYPE field. If the destination is not reachable, which one of the following are generated?

- A. Type 8 ICMP codes
- B. Type 12 ICMP codes
- C. Type 3 ICMP codes
- D. Type 7 ICMP codes

Answer: C

Question No : 18

Which one of the following acts makes reputational risk of poor security a reality because it requires public disclosure of any security breach that involves personal information if it is unencrypted or if it is reasonably believed that the information has been acquired by an unauthorized person?

- A. California SB 1386
- B. Sarbanes-Oxley 2002
- C. Gramm-Leach-Bliley Act (GLBA)
- D. USA Patriot Act 2001

Answer: A

Question No : 19

Which one of the following components of standard Solaris Syslog is a UNIX command that is used to add single-line entries to the system log?

- A. "Logger"
- B. "/etc/syslog.conf"
- C. "Syslogd"
- D. "Syslogd.conf"