ECCouncil

Exam 412-79v8

EC-Council Certified Security Analyst (ECSA)

Version: 10.3

[Total Questions: 196]

Question No : 1

Identify the person who will lead the penetration-testing project and be the client point of contact.

A. Database Penetration Tester
B. Policy Penetration Tester
C. Chief Penetration Tester
D. Application Penetration Tester

Answer: C
Reference:http://www.scribd.com/doc/133635286/LPTv4-Module-15-Pre-Penetration-Testing-Checklist-NoRestriction(page 15)

Question No : 2

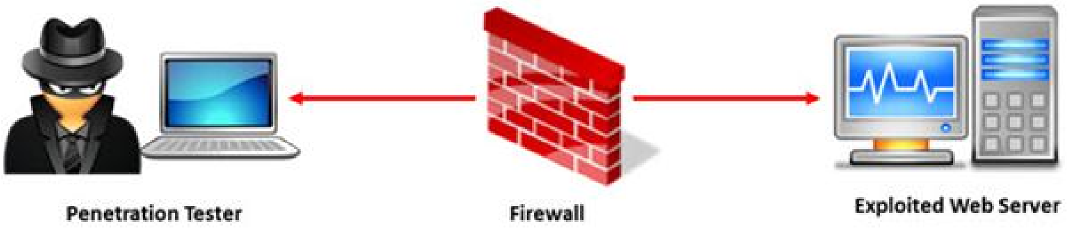
Which of the following statements is true about the LM hash?

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

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

Question No : 3

A penetration test will show youthe vulnerabilities in the target system and the risks associated with it. An educated valuation of the risk will be performed so that the vulnerabilities can be reported as High/Medium/Low risk issues.



What are the two types of ‘white-box’ penetration testing?

A. Announced testing and blind testing
B. Blind testing and double blind testing
C. Blind testing and unannounced testing
D. Announced testing and unannounced testing

Answer: D

Question No : 4

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

Question No : 5

Metasploit framework in an open source platform for vulnerability research, development, and penetration testing. Which one of the following metasploit options is used to exploit multiple systems at once?

A. NinjaDontKill
B. NinjaHost

C. RandomNops
D. EnablePython

Answer: A

Question No : 6

John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

A. C:\Windows\System32\Boot
B. C:\WINNT\system32\drivers\etc
C. C:\WINDOWS\system32\cmd.exe
D. C:\Windows\System32\restore

Answer: B
Reference:http://en.wikipedia.org/wiki/Hosts_(file) (location in the file system, see the table)

Question No : 7

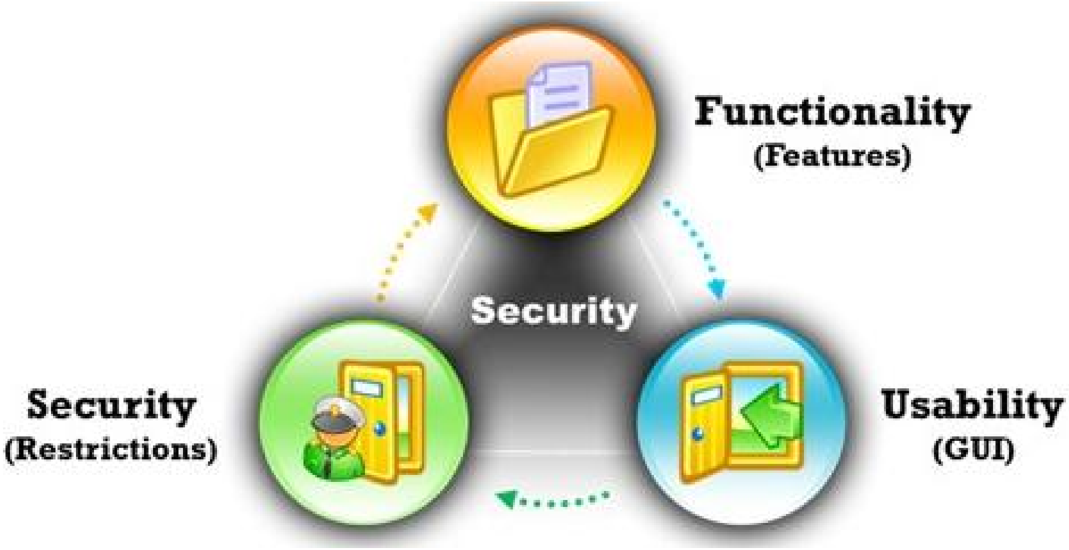
Which one of the following commands is used to search one of more files for a specific pattern and it helps in organizing the firewall log files?

A. grpck
B. grep
C. gpgv
D. gprn

Answer: B

Question No : 8

Today, most organizations would agree that their most valuable IT assets reside within applications and databases. Most would probably also agree that these are areasthat have the weakest levels of security, thus making them the prime target for malicious activity from system administrators, DBAs, contractors, consultants, partners, and customers.



Which of the following flaws refers to an application using poorlywritten encryption code to securely encrypt and store sensitive data in the database and allows an attacker to steal or modify weakly protected data such as credit card numbers, SSNs, and other authentication credentials?

A. SSI injection attack
B. Insecure cryptographic storage attack
C. Hidden field manipulation attack
D. Man-in-the-Middle attack

Answer: B

Question No : 9

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

Question No : 10

DNS information records provide important data about:

A. Phone and Fax Numbers
B. Location and Type of Servers
C. Agents Providing Service to Company Staff
D. New Customer

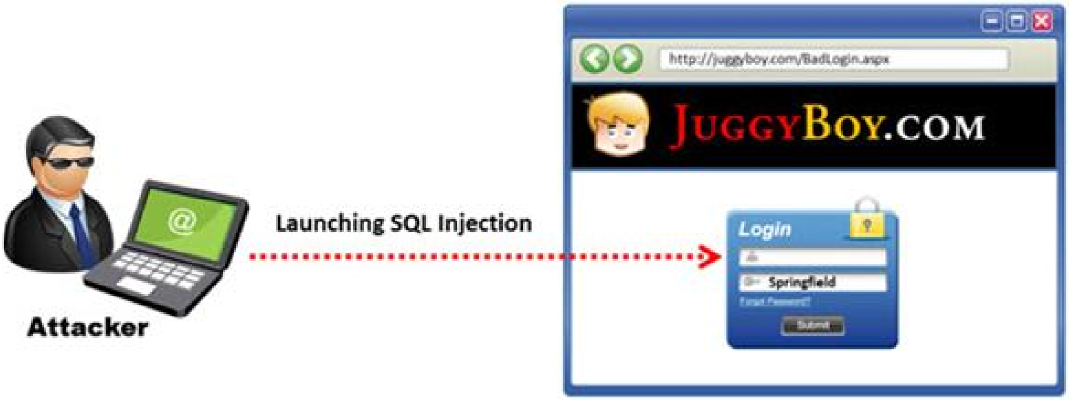
Answer: B

Question No : 11

SQL injection attacks are becoming significantly more popular amongst hackers and there has been an estimated 69 percent increase of this attack type.

This exploit is used to great effect by the hacking community since it is the primary way to steal sensitive data from web applications. It takes advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database.

The below diagram shows how attackers launched SQL injection attacks on web applications.



Which of the following can the attacker use to launch an SQL injection attack?

A. Blah' “2=2 –“

B. Blah' and 2=2 --
C. Blah' and 1=1 --
D. Blah' or 1=1 --

Answer: D

Explanation:

QUESTIONNO: 127

What threat categories should you use to prioritize vulnerabilities detected in the pen testing report?

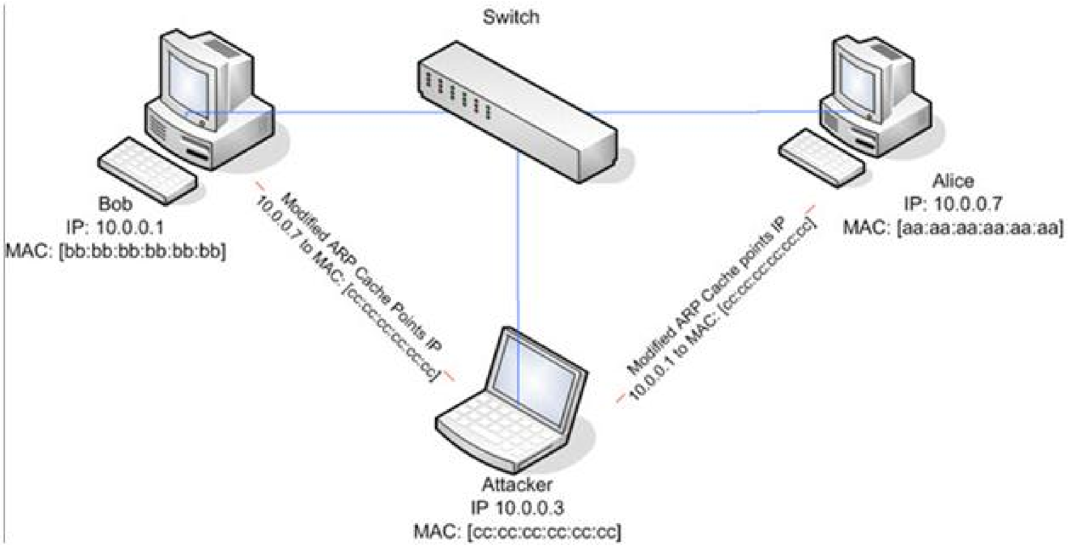
A. 1, 2, 3, 4, 5
B. Low, medium, high, serious, critical
C. Urgent, dispute, action, zero, low
D. A, b, c, d, e

Answer: B

Question No : 12

ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address ResolutionProtocol (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.


Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP 10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP 10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

What type of attack would you launch after successfully deploying ARP spoofing?

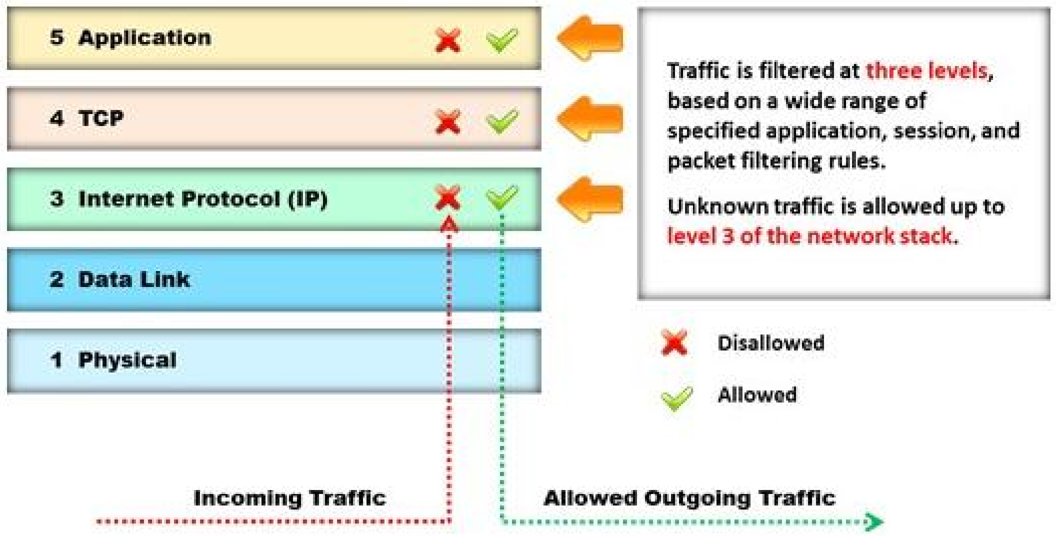
A. Parameter Filtering
B. Social Engineering
C. Input Validation
D. Session Hijacking

Answer: D

ence:http://en.wikipedia.org/wiki/ARP_spoofing

Question No : 13

Identify the type of firewall represented in the diagram below:


5 Application
4 TCP
3 Internet Protocol (IP)
2 Data Link
1 Physical
Traffic is filtered at three levels, based on a wide range of specified application, session, and packet filtering rules.
Unknown traffic is allowed up to level 3 of the network stack.
Disallowed
Allowed
Incoming Traffic
Allowed Outgoing Traffic

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

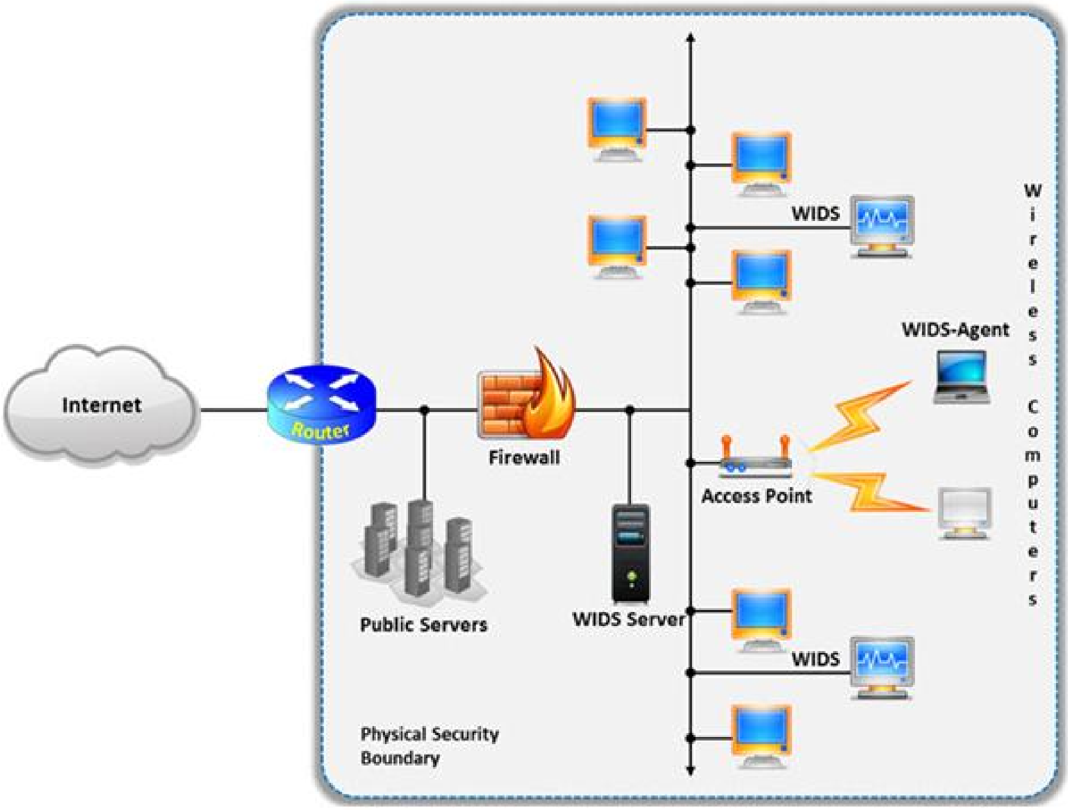
Answer: A
Reference:http://www.technicolorbroadbandpartner.com/getfile.php?id=4159(page 13)

Question No : 14

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected.

Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Which of the following attacks can be detected with the help ofwireless intrusion detection system (WIDS)?



A. Social engineering
B. SQL injection
C. Parameter tampering
D. Man-in-the-middle attack

Answer: D

Reference:http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf(page 5)

Question No : 15

Security auditors determine the use of WAPs on their networks with Nessus vulnerability scanner which identifies the commonly used WAPs. One of the plug-ins that the Nessus Vulnerability Scanner uses is ID #11026 and is named “Access Point Detection”. This plug-in uses four techniques to identify the presence of a WAP. Which one of the following techniques is mostly used for uploading new firmware images while upgrading the WAP device?

A. NMAP TCP/IP fingerprinting