- **Vendor:** EC-Council
- **Exam Code:** 312-38
- **Exam Name:** EC-Council Certified Network Defender Certification Exam
- **New Updated Questions from Braindump2go**
- **(Updated in December/2021)**

QUESTION 611
A network designer needs to submit a proposal for a company, which has just published a web portal for its clients on the internet. Such a server needs to be isolated from the internal network, placing itself in a DMZ. Faced with this need, the designer will present a proposal for a firewall with three interfaces, one for the internet network, another for the DMZ server farm and another for the internal network. What kind of topology will the designer propose?

A. Screened subnet
B. Multi-homed firewall
C. Bastion host
D. DMZ, External-Internal firewall

Answer: B

QUESTION 612
You are tasked to perform black hat vulnerability assessment for a client. You received official written permission to work with: company site, forum, Linux server with LAMP, where this site hosted. Which vulnerability assessment tool should you consider to use?

A. dnsbrute
B. hping
C. OpenVAS
D. wireshark

Answer: C

QUESTION 613
What is the best way to describe a mesh network topology?

A. A network in which every computer in the network has a connection to each and every computer in the network.
B. A network in which every computer meshes together to form a hybrid between a star and bus topology.
C. A network in which every computer in the network can communicate with a single central computer.
D. A network that is extremely cost efficient, offering the best option for allowing computers to communicate amongst each other.

Answer: A

QUESTION 614
The security network team is trying to implement a firewall capable of operating only in the session layer, monitoring the TCP inter-packet link protocol to determine when a requested session is legitimate or not. Using this type of firewall, they could be able to intercept the communication, making the external network see that the firewall is the source, and facing the user, who responds from the outside is the firewall itself. They are just limiting a requirements previous listed, because they already have a packet filtering firewall and they must add a cheap solution that meets the objective. What kind of firewall would you recommend?

A. Packet Filtering with NAT
B. Circuit Level Gateway
C. Application Proxies
D. Application Level Gateways

Answer: B

QUESTION 615
If a network is at risk resulting from misconfiguration performed by unskilled and/or unqualified individuals, what type of threat is this?

A. External Threats
B. Unstructured Threats
C. Structured Threats
D. Internal Threats

Answer: B

QUESTION 616
John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization’s network. Which of following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt? (Choose all that apply.)

A. tcp.flags=0x00
B. tcp.options.wscale_val==20
C. tcp.flags==0x2b
D. tcp.options.mss_val<1460

Answer: ACD

QUESTION 617
Michael decides to view the ________ to track employee actions on the organization’s network.

A. Firewall policy
B. Firewall settings
C. Firewall log
D. Firewall rule set

Answer: C

QUESTION 618
Which of the following systems includes an independent NAS Head and multiple storage arrays?

A. FreeNAS
B. None of these
C. Gateway NAS System

D. Integrated NAS System

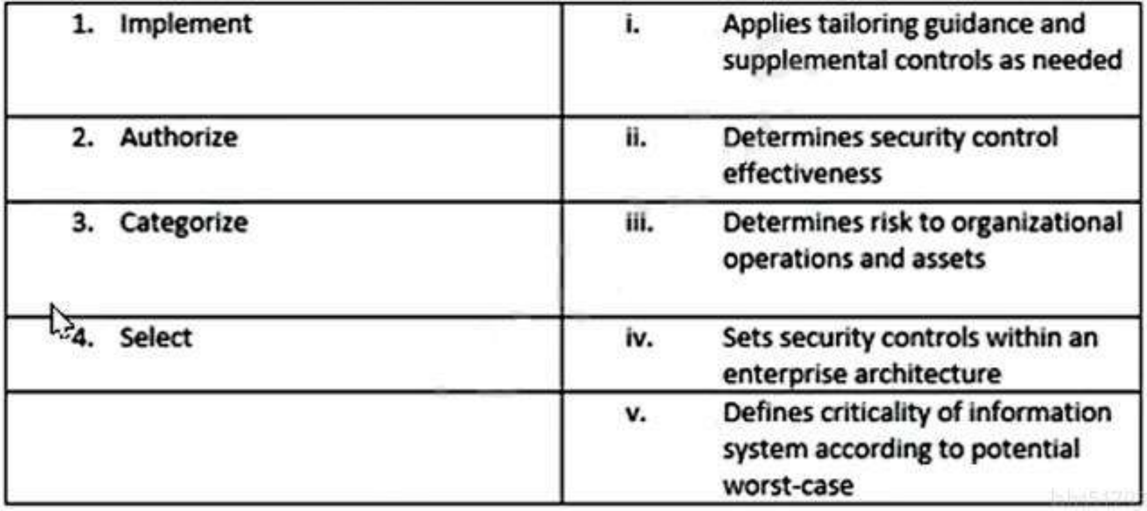
Answer: C

QUESTION 619
Which of the following can be used to suppress fire from Class K sources?

A. Water
B. Carbon dioxide
C. Foam
D. Dry Chemical

Answer: C

QUESTION 620
Match the following NIST security life cycle components with their activities:



1. Implement	i.	Applies tailoring guidance and supplemental controls as needed
2. Authorize	ii.	Determines security control effectiveness
3. Categorize	iii.	Determines risk to organizational operations and assets
4. Select	iv.	Sets security controls within an enterprise architecture
	v.	Defines criticality of information system according to potential worst-case

A. 1-iv, 2- iii,3-v,4-i
B. 1-ii,2-i,3-v,4-iv
C. 1-i,2-v,3-iii,4-ii
D. 1-iii,2-iv,3-v,4-i

Answer: A

QUESTION 621
What is the correct order of activities that a IDS is supposed to attempt in order of detect an intrusion?

A. Prevention, Intrusion Monitoring, intrusion Detection, Response
B. Intrusion Detection, Response, Prevention, Intrusion Monitoring
C. Intrusion Monitoring, Intrusion Detection, Response, Prevention
D. Prevention, intrusion Detection, Response, Intrusion Monitoring

Answer: A

QUESTION 622
Larry is a network administrator working for a manufacturing company in Detroit. Larry is responsible for the entire company's network which consists of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to cut back on costs and bring the email control internal. Larry likes this idea because it will give him more control over email. Larry wants to purchase a server for email but he does not want the server to be on the internal network because this might cause security risks. He decides to place the email server on the outside of the

company’s internal firewall. There is another firewall connected directly to the Internet that will protect some traffic from accessing the email server; the server will essentially be place between the two firewalls. What logical area is Larry going to place the new email server into?

A. He is going to place the server in a Demilitarized Zone (DMZ).
B. He will put the email server in an IPSec zone.
C. For security reasons, Larry is going to place the email server in the company’s Logical Buffer Zone (LBZ).
D. Larry is going to put the email server in a hot-server zone.

Answer: A

QUESTION 623
Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user’s email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?

A. Usability
B. Confidentiality
C. Availability
D. Data Integrity

Answer: D

QUESTION 624
Which of the following interfaces uses hot plugging technique to replace computer components without the need to shut down the system?

A. SATA
B. SCSI
C. IDE
D. SDRAM

Answer: B

QUESTION 625
Alex is administering the firewall in the organization’s network. What command will he use to check all the remote addresses and ports in numerical form?

A. netstat -a
B. netstat -ao
C. netstat -o
D. netstat -an

Answer: D

QUESTION 626
Which type of wireless network attack is characterized by an attacker using a high gain amplifier from a nearby location to drown out the legitimate access point signal?

A. Rogue access point attack
B. Ad Hoc Connection attack
C. Jamming signal attack
D. Unauthorized association

Answer: C

QUESTION 627
Which of the following RAID storage techniques divides the data into multiple blocks, which are further written across the RAID system?

A. Striping
B. None of these
C. Parity
D. Mirroring

Answer: A

QUESTION 628
Management decides to implement a risk management system to reduce and maintain the organization's risk to an acceptable level. Which of the following is the correct order in the risk management phase?

A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review
B. Risk Identification, Risk Assessment, Risk Monitoring & Review, Risk Treatment
C. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment
D. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification

Answer: A

QUESTION 629
You want to increase your network security implementing a technology that only allows certain MAC addresses in specific ports in the switches; which one of the above is the best choice?

A. Port Security
B. Port Authorization
C. Port Detection
D. Port Knocking

Answer: A

QUESTION 630
An IDS or IDPS can be deployed in two modes. Which deployment mode allows the IDS to both detect and stop malicious traffic?

A. passive mode
B. inline mode
C. promiscuous mode
D. firewall mode

Answer: B

QUESTION 631
Which protocol could choose the network administrator for the wireless network design, if he need to satisfied the minimum requirement of 2.4 GHz, 22 MHz of bandwidth, 2 Mbits/s stream for data rate and use DSSS for modulation.

A. 802.11n
B. 802.11g
C. 802.11b
D. 802.11a

Answer: C

QUESTION 632
Physical access controls help organizations monitor, record, and control access to the information assets and facility. Identify the category of physical security controls which includes security labels and warning signs.

A. Technical control
B. Environmental control
C. Physical control
D. Administrative control

Answer: D

QUESTION 633
Which Internet access policy starts with all services blocked and the administrator enables safe and necessary services individually, which provides maximum security and logs everything, such as system and network activities?

A. Internet access policy
B. Paranoid policy
C. Permissive policy
D. Prudent policy

Answer: D

QUESTION 634
Daniel who works as a network administrator has just deployed an IDS in his organization's network. He wants to calculate the False Positive rate for his implementation. Which of the following formulas will he use, to calculate the False Positive rate?

A. False Negative/True Negative+True Positive
B. False Positive/False Positive+True Negative
C. True Negative/False Negative+True Positive
D. False Negative/False Negative+True Positive

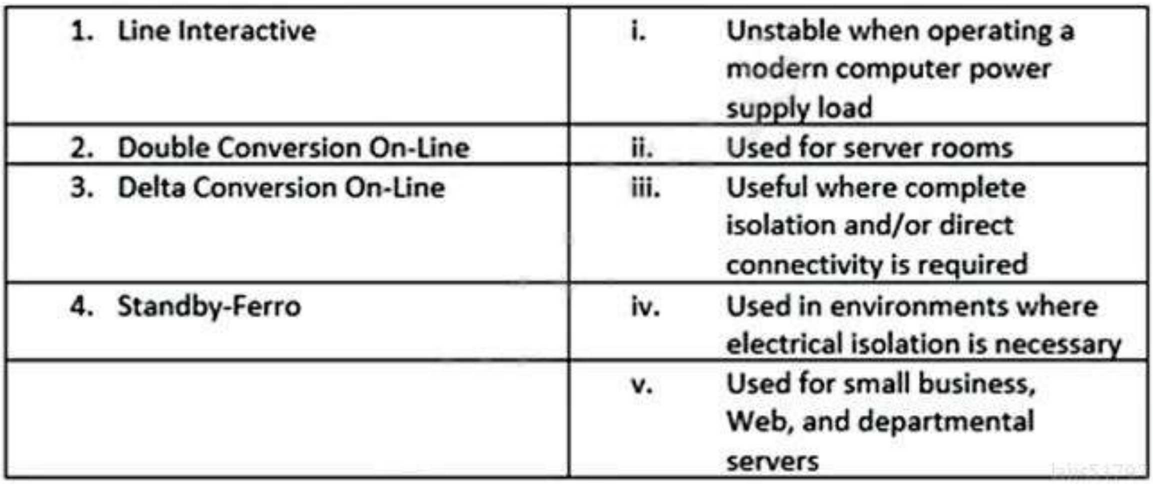
Answer: B

QUESTION 635
The SNMP contains various commands that reduce the burden on the network administrators. Which of the following commands is used by SNMP agents to notify SNMP managers about an event occurring in the network?

A. INFORM
B. RESPONSE
C. TRAPS
D. SET

Answer: C

QUESTION 636
Your company is planning to use an uninterruptible power supply (UPS) to avoid damage from power fluctuations. As a network administrator, you need to suggest an appropriate UPS solution suitable for specific resources or conditions. Match the type of UPS with the use and advantage:



1. Line Interactive	i.	Unstable when operating a modern computer power supply load
2. Double Conversion On-Line	ii.	Used for server rooms
3. Delta Conversion On-Line	iii.	Useful where complete isolation and/or direct connectivity is required
4. Standby-Ferro	iv.	Used in environments where electrical isolation is necessary
	v.	Used for small business, Web, and departmental servers

A. 1-i,2-iv,3-ii,4-v
B. 1-v,2-iii,3-i,4-ii
C. 1-ii,2-iv,3-iii,4-i
D. 1-iii,2-iv,3-v,4-iv

Answer: C

QUESTION 637
Which filter to locate unusual ICMP request an Analyst can use in order to detect a ICMP probes from the attacker to a target OS looking for the response to perform ICMP based fingerprinting?

A. (icmp.type==9 && ((!(icmp.code==9))
B. (icmp.type==8 && ((!(icmp.code==8))
C. (icmp.type==12) | | (icmp.type==15| |(icmp.type==17)
D. (icmp.type==14) | | (icmp.type==15| |(icmp.type==17)

Answer: B