QUESTION 980
Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites
B. Improper input handling
C. DLL injection
D. Certificate signing flaws

Answer: B

QUESTION 981
An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?

A. Wipe the hard drive.
B. Shred the hard drive.
C. Sanitize all of the data.
D. Degauss the hard drive.

Answer: B

QUESTION 982
A technician is designing a solution that will be required to process sensitive information, including classified government data. The system needs to be common criteria certified. Which of the following should the technician select?

A. Security baseline
B. B Hybrid cloud solution
C. Open-source software applications
D. Trusted operating system

Answer: D

QUESTION 983
A security administrator has generated an SSH key pair to authenticate to a new server. Which of the following should the security administrator do NEXT to use the keys securely for authentication? Choose 2

A. Install the public key on the server
B. Install the private key on the server.

C. Encrypt the public key.
D. Encrypt the private key.
E. Install both keys on the server.
F. Securely wipe the certificate signing request.

Answer: CE

QUESTION 984
A company has just experienced a malware attack affecting a large number of desktop users. The antivirus solution was not able to block the malware, but the HIDS alerted to C2 calls as 'Troj.Generic'. Once the security team found a solution to remove the malware, they were able to remove the malware files successfully, and the HIDS stopped alerting. The next morning, however, the HIDS once again started alerting on the same desktops, and the security team discovered the files were back. Which of the following BEST describes the type of malware infecting this company's network?

A. Trojan
B. Spyware
C. Rootkit
D. Botnet

Answer: A

QUESTION 985
An organization wants to host an externally accessible web server that will not contain sensitive user information. Any sensitive information will be hosted on file servers. Which of the following is the BEST architecture configuration for this organization?

A. Host the web server in a DMZ and the file servers behind a firewall
B. Host the web server and the file servers in a DMZ
C. Host the web server behind a firewall and the file servers in a DMZ
D. Host both the web server and file servers behind a firewall

Answer: A

QUESTION 986
a technician is recommending preventive physical security controls for a server room. Which of the following would the technician most likely recommend? (select two)

A. GEO fencing
B. Video surveillance
C. Protected Cabinets
D. Mantrap
E. Key exchange
F. Authorized personnel signage

Answer: BF

QUESTION 987
A company posts a sign indicating its server room is under video surveillance. Which of the following control types is represented?

A. Administrative
B. Detective
C. Technical
D. Deterrent

Answer: A

QUESTION 988
A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files. the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?

A. DDoS
B. DoS
C. Zero day
D. Logic bomb

Answer: A

QUESTION 989
A network administrator was provided the following output from a vulnerability scan:

Plugin ID	Severity	Count	Description	Risk Score
10	Critical	1	CentOS 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0670)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?

A. 10
B. 11
C. 12
D. 13
E. 14

Answer: A

QUESTION 990
A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

Answer: B

QUESTION 991
A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the Internet?

A. VLAN
B. Air gap

C. NAT
D. Firewall

Answer: B

QUESTION 992
Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization.
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

Answer: A