Security Awareness

1. 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(s): D

---

2. Which type of vulnerability assessment tool provides security to the IT system by testing for vulnerabilities in the applications and operation system?

A. Active/Passive Tools

B. Application-layer Vulnerability Assessment Tools

C. Location/Data Examined Tools

D. Scope Assessment Tools

Answer(s): D

---

3. Which of the following policies states that the relevant application owner must authorize requests for additional access to specific business applications in writing to the IT Department/resource?

A. Special-Access Policy

B. User Identification and Password Policy

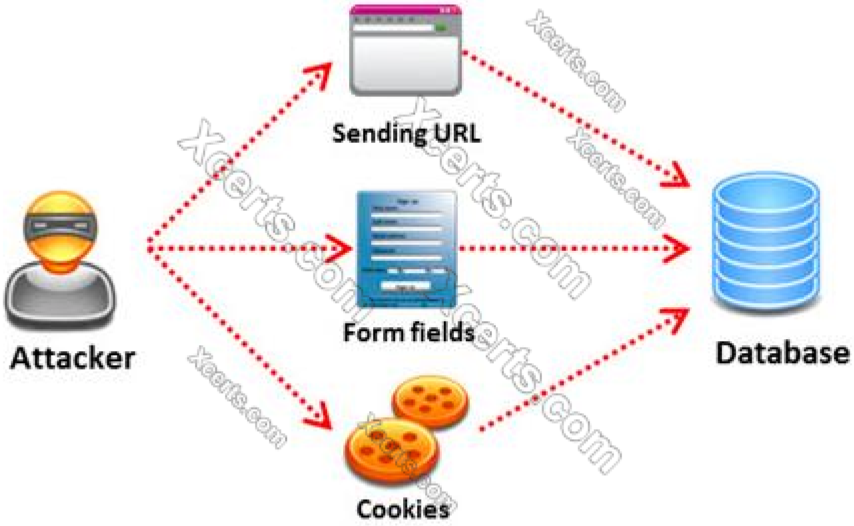
C. Personal Computer Acceptable Use Policy

D. User-Account Policy

Answer(s): B

---

4. SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application.
A successful SQL injection attack can:
i) Read sensitive data from the database iii)Modify database data (insert/update/delete)
iii) Execute administration operations on the database (such as shutdown the DBMS)
iv) Recover the content of a given file existing on the DBMS file system or write files into the file system v) Issue commands to the operating system



Pen tester needs to perform various tests to detect SQL injection vulnerability. He has to make a list of all input fields whose values could be used in crafting a SQL query, including the hidden fields of POST requests and then test them separately, trying to interfere with the query and to generate an error.
In which of the following tests is the source code of the application tested in a non-runtime environment to detect the SQL injection vulnerabilities?

A. Automated Testing

B. Function Testing

C. Dynamic Testing

D. Static Testing

Answer(s): D

---

5. 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

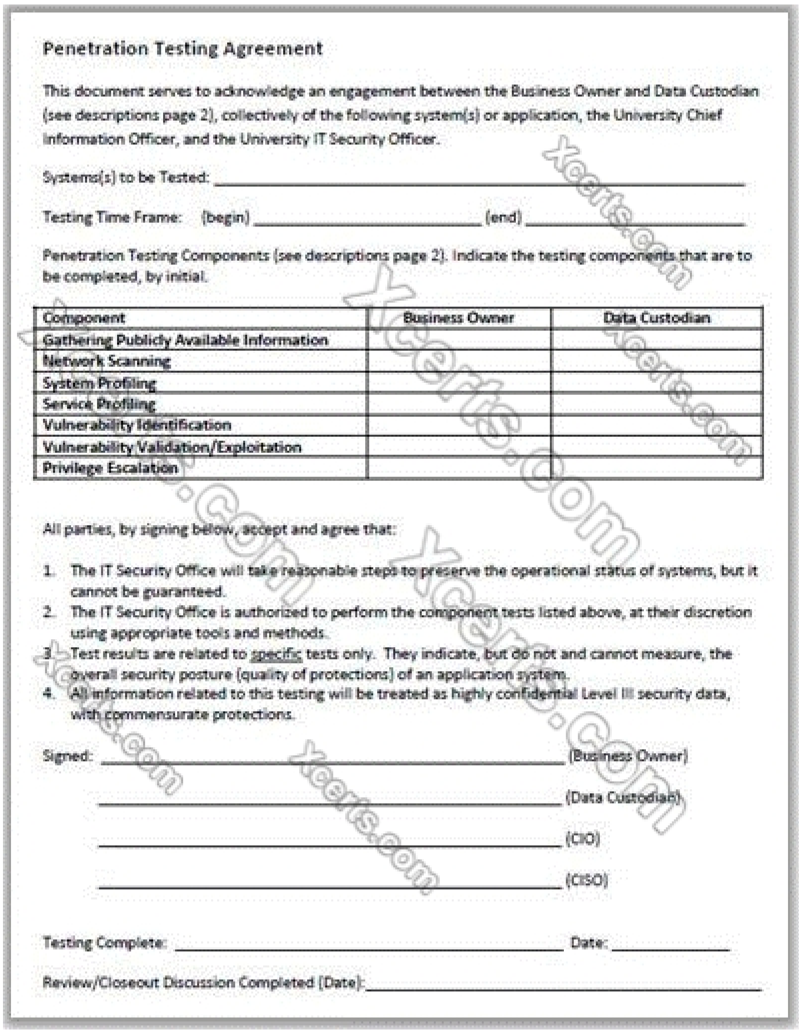
C. Liability Insurance

D. Non-Disclosure Agreement

Answer(s): D

---

6. Why is a legal agreement important to have before launching a penetration test?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be Tested: ______________________________

Testing Time Frame: (begin) ____________________ (end) ____________________

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component	Business Owner	Data Custodian
Gathering Publicly Available Information		
Network Scanning		
System Profiling		
Service Profiling		
Vulnerability Identification		
Vulnerability Validation/Exploitation		
Privilege Escalation		

All parties, by signing below, accept and agree that:

1. The IT Security Office will take reasonable steps to preserve the operational status of systems, but it cannot be guaranteed.
2. The IT Security Office is authorized to perform the component tests listed above, at their discretion using appropriate tools and methods.
3. Test results are related to specific tests only. They indicate, but do not and cannot measure, the overall security posture (quality of protections) of an application system.
4. All information related to this testing will be treated as highly confidential Level III security data, with commensurate protections.

Signed: ______________________________ (Business Owner)

______________________________ (Data Custodian)

______________________________ (CIO)

______________________________ (CISO)

Testing Complete: ______________________________ Date: ____________

Review/Closeout Discussion Completed (Date): ______________________________

A. Guarantees your consultant fees

B. Allows you to perform a penetration test without the knowledge and consent of the organization's upper management

C. It establishes the legality of the penetration test by documenting the scope of the project and the consent of the company.

D. It is important to ensure that the target organization has implemented mandatory security policies

Answer(s): C

---

7. A security policy is a document or set of documents that describes, at a high level, the security controls that will be implemented by the company. Which one of the following policies forbids everything and restricts usage of company computers, whether it is system usage or network usage?

A. Paranoid Policy

B. Prudent Policy

C. Promiscuous Policy

D. Information-Protection Policy

Answer(s): A

---

8. Which of the following protocol's traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

A. Reverse Gossip Transport Protocol (RGTP)

B. Real-time Transport Protocol (RTP)

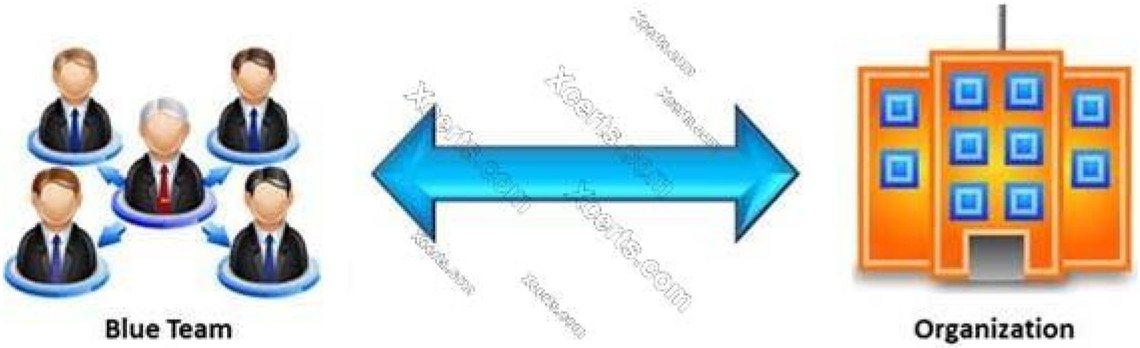
C. Remote Desktop Protocol (RDP)

D. Session Initiation Protocol (SIP)

Answer(s): C

---

9. In the context of penetration testing, what does blue teaming mean?



A. A penetration test performed with the knowledge and consent of the organization's IT staff

B. It is the most expensive and most widely used

C. It may be conducted with or without warning

D. A penetration test performed without the knowledge of the organization's IT staff but with permission from upper management

Answer(s): A

---

10. James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf

B. Trinoo

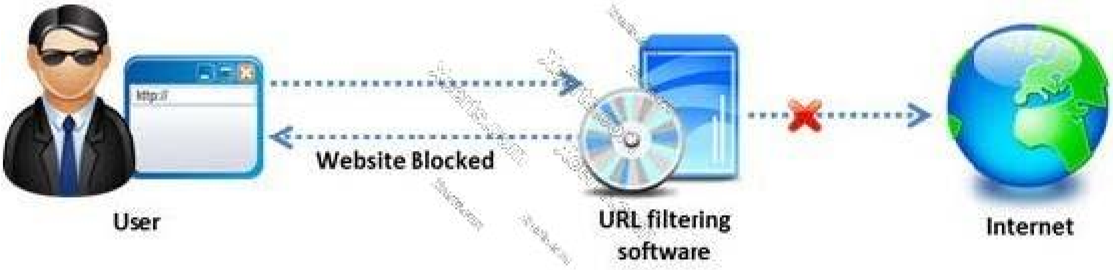
C. Fraggle

D. SYN flood

Answer(s): A

---

11. Amazon, an IT based company, conducts a survey on the usage of the Internet. They found that company employees spend most of the time at work surfing the web for their personal use and for inappropriate web site viewing.
Management decide to block all such web sites using URL filtering software.



How can employees continue to see the blocked websites?

A. Using session hijacking

B. Using proxy servers

C. Using authentication

D. Using encryption

Answer(s): B

---

12. Nessus can test a server or a network for DoS vulnerabilities. Which one of the following script tries to kill a service?

A. ACT_DENIAL

B. ACT_FLOOD

C. ACT_KILL_HOST

D. ACT_ATTACK

Answer(s): A

---

13. Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81

B. Port 443

C. Port 0

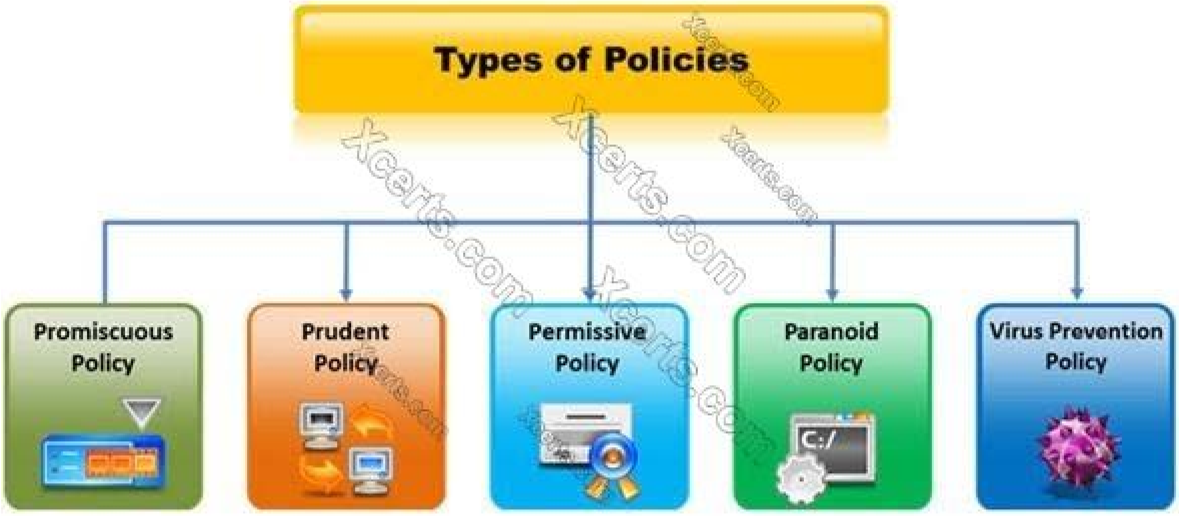
D. Port21

Answer(s): C

---

14. Which type of security policy applies to the below configuration?
i) Provides maximum security while allowing known, but necessary, dangers
ii) All services are blocked; nothing is allowed
iii) Safe and necessary services are enabled individually
iv) Non-essential services and procedures that cannot be made safe are NOT allowed

v)Everything is logged



A. Paranoid Policy

B. Prudent Policy

C. Permissive Policy

D. Promiscuous Policy

Answer(s): B

---

15. 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(s): A

---

16. Snort, an open source network-based intrusion detection sensor, is the most widely installed NIDS in the world. It can be configured to run in the four modes. Which one of the following modes reads the packets off the network and displays them in a continuous stream on the console (screen)?

A. Packet Sniffer Mode

B. Packet Logger Mode

C. Network Intrusion Detection System Mode

D. Inline Mode

Answer(s): A

---

17. What is the difference between penetration testing and vulnerability testing?

A. Penetration testing goes one step further than vulnerability testing; while vulnerability tests check for known vulnerabilities, penetration testing adopts the concept of ‘in-depth ethical hacking’

B. Penetration testing is based on purely online vulnerability analysis while vulnerability testing engages ethical hackers to find vulnerabilities

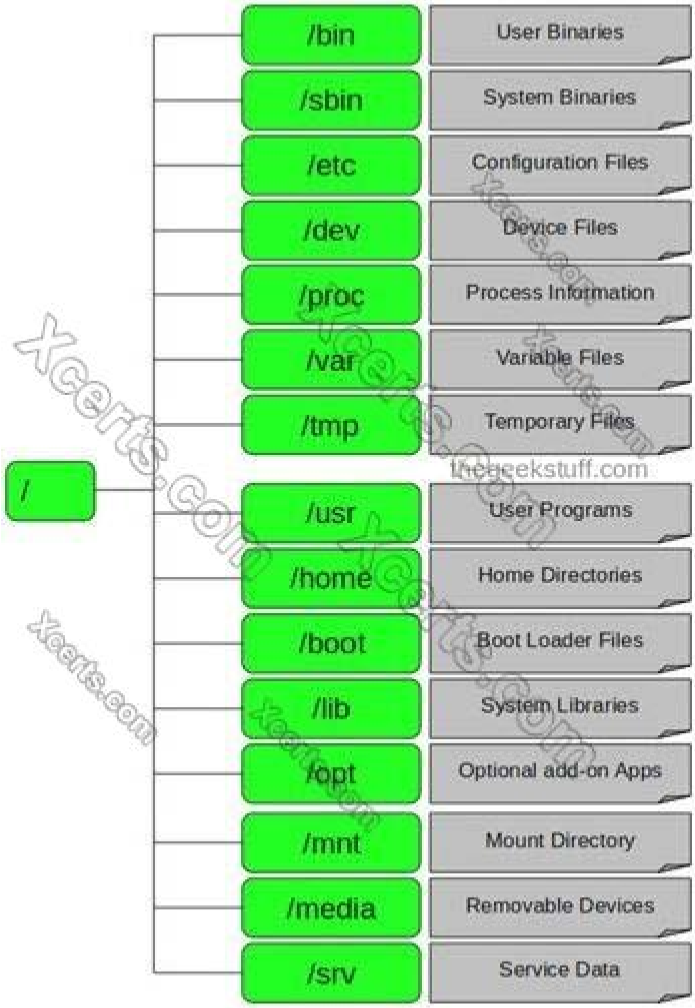
C. Vulnerability testing is more expensive than penetration testing

D. Penetration testing is conducted purely for meeting compliance standards while vulnerability testing is focused on online scans

Answer(s): A

---

18. In Linux, /etc/shadow file stores the real password in encrypted format for user’s account with added properties associated with the user’s password.



In the example of a /etc/shadow file below, what does the bold letter string indicate?
Vivek: $1$fnffc$GteyHdicpGOfffXX40w#5:13064:0:99999:7

A. Number of days the user is warned before the expiration date

B. Minimum number of days required between password changes

C. Maximum number of days the password is valid

D. Last password changed

Answer(s): B

---

19. The first and foremost step for a penetration test is information gathering. The main objective of this test is to gather information about the target system which can be used in a malicious manner to gain access to the target systems.

Which of the following information gathering terminologies refers to gathering information through social engineering on-site visits, face-to-face interviews, and direct questionnaires?

A. Active Information Gathering

B. Pseudonymous Information Gathering

C. Anonymous Information Gathering

D. Open Source or Passive Information Gathering

Answer(s): A

---

20. DMZ is a network designed to give the public access to the specific internal resources and you might want to do the same thing for guests visiting organizations without compromising the integrity of the internal resources. In general, attacks on the wireless networks fall into four basic categories. Identify the attacks that fall under Passive attacks category.(Select all that apply)

A. Wardriving

B. Spoofing

C. Sniffing

D. Network Hijacking

Answer(s): A