EC-Council Security Awareness

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

Penetration Tester
Server

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

---

2. Hackers today have an ever-increasing list of weaknesses in the web application structure at their disposal, which they can exploit to accomplish a wide variety of malicious tasks.

New flaws in web application security measures are constantly being researched, both by hackers and by security professionals. Most of these flaws affect all dynamic web applications whilst others are dependent on specific application technologies.

In both cases, one may observe how the evolution and refinement of web technologies also brings about new exploits which compromise sensitive databases, provide access to theoretically secure networks, and

pose a threat to the daily operation of online businesses.
What is the biggest threat to Web 2.0 technologies?

A. SQL Injection Attacks

B. Service Level Configuration Attacks

C. Inside Attacks

D. URL Tampering Attacks

Answer(s): A

---

3. Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Filtered

B. Stealth

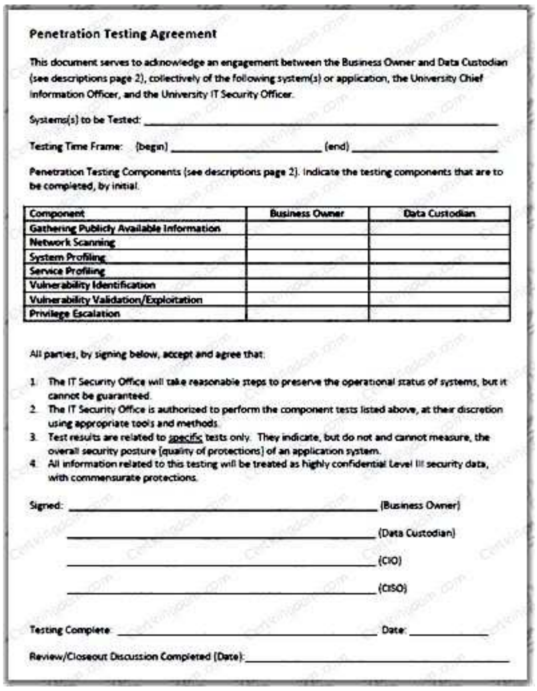
C. Closed

D. Open

Answer(s): D

---

4. 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

---

5. Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. OSPF

B. BPG

C. ATM

D. UDP

Answer(s): A

---

6. Which of the following is the range for assigned ports managed by the Internet Assigned Numbers Authority (IANA)?

A. 3001-3100

B. 5000-5099

C. 6666-6674

D. 0 1023

Answer(s): D

---

7. If a web application sends HTTP cookies as its method for transmitting session tokens, it may be vulnerable which of the following attacks?

A. Parameter tampering Attack

B. Sql injection attack

C. Session Hijacking

D. Cross-site request attack

Answer(s): D

---

8. Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\LSA

B. %systemroot%\repair

C. %systemroot%\system32\drivers\etc

D. %systemroot%\system32\LSA

Answer(s): B

---

9. Transmission Control Protocol (TCP) is a connection-oriented four layer protocol. It is responsible for breaking messages into segments, re-assembling them at the destination station, and re-sending. Which one of the following protocols does not use the TCP?

A. Reverse Address Resolution Protocol (RARP)

B. HTTP (Hypertext Transfer Protocol)

C. SMTP (Simple Mail Transfer Protocol)

D. Telnet

Answer(s): A

---

10. Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.
link:www.ghttech.net
What will this search produce?

A. All sites that link to ghttech.net

B. Sites that contain the code: link:www.ghttech.net

C. All sites that ghttech.net links to

D. All search engines that link to .net domains

Answer(s): A

---

11. Which one of the following 802.11 types uses either FHSS or DSSS for modulation?

A. 802.11b

B. 802.11a

C. 802.11n

D. 802.11-Legacy

Answer(s): D

---

12. Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

A. SYN Scan

B. Connect() scan

C. XMAS Scan

D. Null Scan

Answer(s): A

---

13. Which one of the following acts makes reputational risk of poor security a reality because it requires public disclosure of any security breach that involves personal information if it is unencrypted or if it is reasonably believed that the information has been acquired by an unauthorized person?

A. California SB 1386

B. Sarbanes-Oxley 2002

C. Gramm-Leach-Bliley Act (GLBA)

D. USA Patriot Act 2001

Answer(s): A

---

14. 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.

A. Wardriving

B. Spoofing

C. Sniffing

D. Network Hijacking

Answer(s): A

---

15. Which of the following attacks does a hacker perform in order to obtain UDDI information such as businessEntity, businesService, bindingTemplate, and tModel?

A. Web Services Footprinting Attack

B. Service Level Configuration Attacks

C. URL Tampering Attacks

D. Inside Attacks

Answer(s): A

---

16. Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase

B. Pre-Assessment Phase

C. Assessment Phase

D. Post-Assessment Phase

Answer(s): B

---

17. What are the security risks of running a "repair" installation for Windows XP?

A. There are no security risks when running the "repair" installation for Windows XP

B. Pressing Shift+F1 gives the user administrative rights

C. Pressing Ctrl+F10 gives the user administrative rights

D. Pressing Shift+F10 gives the user administrative rights

Answer(s): D

---

18. Software firewalls work at which layer of the OSI model?

A. Data Link

B. Network

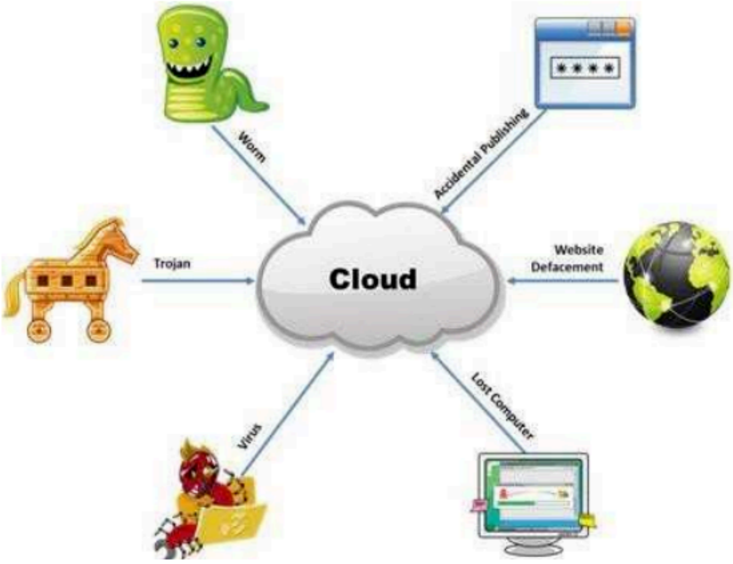
C. Transport

D. Application

Answer(s): A

---

19. The Internet is a giant database where people store some of their most private information on the cloud, trusting that the service provider can keep it all safe. Trojans, Viruses, DoS attacks, website defacement, lost computers, accidental publishing, and more have all been sources of major leaks over the last 15 years.



What is the biggest source of data leaks in organizations today?

A. Weak passwords and lack of identity management

B. Insufficient IT security budget

C. Rogue employees and insider attacks

D. Vulnerabilities, risks, and threats facing Web sites

Answer(s): C

---

20. Which one of the following log analysis tools is used for analyzing the server's log files?

A. Performance Analysis of Logs tool

B. Network Sniffer Interface Test tool

C. Ka Log Analyzer tool

D. Event Log Tracker tool

Answer(s): C