312-50v9

EC-Council Certified Ethical Hacker v9

Version: Demo

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

1.A common cryptographically tool is the use of XOR. XOR the following binary value:

10110001

00111010

A. 10001011

B. 10011101

C. 11011000

D. 10111100

Answer: A

2. An attacker gains access to a Web server’s database and display the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site\'s user login page that the software\'s designers did not expect to be entered. This is an example of what kind of software design problem?

A. Insufficient security management

B. Insufficient database hardening

C. Insufficient exception handling

D. Insufficient input validation

Answer: D

3. What does a firewall check to prevent particularports and applications from getting packets into an organizations?

A. Transport layer port numbers and application layer headers

B. Network layer headers and the session layer port numbers

C. Application layer port numbers and the transport layer headers

D. Presentation layer headers and the session layer port numbers

Answer: A

4. Which of the followingtypes of firewalls ensures that the packets are part of the established session?

A. Switch-level firewall

B. Stateful inspection firewall

C. Application-level firewall

D. Circuit-level firewall

Answer: B

5. To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

A. Bounding

B. Mutating

C. Puzzing

D. Randomizing

Answer: C

6. env x= '(){ :;};echo exploit ' bash –c 'cat/etc/passwd

What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

A. Add new user to the passwd file

B. Display passwd contents to prompt

C. Change all password in passwd

D. Remove the passwd file.

Answer: B

7. Which of the following describes the characteristics of a Boot Sector Virus?

A. Overwrites the original MBR and only executes the new virus code

B. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

Answer: C

8. You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Host-based IDS

B. Firewall

C. Network-Based IDS

D. Proxy

Answer: C

9. In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known wardriving.

Which algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)

B. Temporal Key Integrity Protocol (TRIP)

C. Wi-Fi Protected Access (WPA)

D. Wi-Fi Protected Access 2(WPA2)

Answer: A

10. An attacker changes the profile information of a particular user on a target website (the victim). The attacker uses this string to update the victim\'s profile to a text file and then submit the data to the attacker\'s database.

What is this type of attack (that can use either HTTP GET or HRRP POST) called?

A. Cross-Site Request Forgery

B. Cross-Site Scripting

C. SQL Injection

D. Browser Hacking

Answer: A

11. Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document.Upon execution, a windows appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\\local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?

A. Trojan

B. Worm

C. Key-Logger

D. Micro Virus

Answer: A

12. While using your bank\'s online servicing you notice the following stringin the URL bar:

"http://www.MyPersonalBank/Account?

Id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request,

that data on the web page reflect the changes.

What type of vulnerability is present on this site?

A. SQL injection

B. XSS Reflection

C. Web Parameter Tampering

D. Cookie Tampering

Answer: C

13. It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up windows, webpage,or email warning from what looks like an officialauthority. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again.

Which term best matches this definition?

A. Spyware

B. Adware

C. Ransomware

D. Riskware

Answer: C

14. Nation-state threat actors often discover vulnerabilitiesand hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability.

What is this style of attack called?

A. zero-hour

B. no-day

C. zero-day

D. zero-sum

Answer: C

15. The configuration allows a wired or wireless network interface controller to pass all trafice it receives to thecentral processing unit (CPU), rather than passing only the frames that the

controller is intended to receive.

Which of the following is being described?

A. WEM

B. Multi-cast mode

C. Promiscuous mode

D. Port forwarding

Answer: B

Relate Links

100% Pass Your 312-50v9 Exam with Exambible Prep Materials

http://www.exambible.com/312-50v9-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - http://www.exambible.com/