Certified Ethical Hacker Exam (CEH v10)

1. Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

A. She is using John the Ripper to crack the passwords in the secret.txt file.

B. She is using ftp to transfer the file to another hacker named John.

C. She is encrypting the file.

D. She is using John the Ripper to view the contents of the file.

Answer(s): A

---

2. Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PEM

B. PPP

C. IPSEC

D. SET

Answer(s): C

---

3. In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

A. Transport layer port numbers and application layer headers

B. Presentation layer headers and the session layer port numbers

C. Application layer port numbers and the transport layer headers

D. Network layer headers and the session layer port numbers

Answer(s): A

---

4. A software tester is randomly generating invalid inputs in an attempt to crash the program. Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?

A. Bounding

B. Randomizing

C. Mutating

D. Fuzzing

Answer(s): D

---

5. While

A. Web Parameter Tampering

B. Cookie Tampering

C. XSS Reflection

D. SQL injection

Answer(s): A

---

6. Your company was hired by a small healthcare provider to perform a technical assessment on the network.

A. Use a scan tool like Nessus

B. Use the built-in Windows Update tool

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Answer(s): A

---

7. You are using NMAP to resolve domain names into IP addresses for a ping sweep later.

A. >host -t a hackeddomain.com

B. >host -t soa hackeddomain.com

C. >host -t ns hackeddomain.com

D. >host -t AXFR hackeddomain.com

Answer(s): A

---

8. Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

A. [link:]

B. [site:]

C. [inurl:]

D. [cache:]

Answer(s): B

---

9. Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Remote access policy

B. Network security policy

C. Access control policy

D. Information protection policy

Answer(s): A

---

10. The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.

A. Wireshark

B. Nessus

C. Netcat

D. Netstat

Answer(s): A

---

11. Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

A. A man in the middle attack

B. A denial of service attack

C. A sniffing attack

D. A spoofing attack

Answer(s): A

---

12. A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

A. The host is likely a printer.

B. The host is likely a Windows machine.

C. The host is likely a Linux machine.

D. The host is likely a router.

Answer(s): A

---

13. Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries.) More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

A. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.

B. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.

C. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.

D. Algorithm is not the secret, key is the secret.

Answer(s): B

---

14. A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks.

A. SSDP Scanning

B. UDP Scanning

C. Banner Grabbing

D. IDLE/IPID Scanning

Answer(s): C

---

15. An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

A. The network devices are not all synchronized.

B. Proper chain of custody was not observed while collecting the logs.

C. The attacker altered or erased events from the logs.

D. The security breach was a false positive.

Answer(s): A

---

16. The "black box testing" methodology enforces which kind of restriction?

A. Only the external operation of a system is accessible to the tester.

B. Only the internal operation of a system is known to the tester.

C. The internal operation of a system is only partly accessible to the tester.

D. The internal operation of a system is completely known to the tester.

Answer(s): A

---

17. The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.

A. Private

B. Public

C. Shared

D. Root

Answer(s): A

---

18. Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark

B. Nessus

C. Metasploit

D. Maltego

Answer(s): C

19. Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?

A. My Doom

B. Astacheldraht

C. R-U-Dead-Yet?(RUDY)

D. LOIC

Answer(s): C

---

20. Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide.

A. External scripts have direct access to the company servers and can steal the data from there

B. External scripts increase the outbound company data traffic which leads greater financial losses

C. External script contents could be maliciously modified without the security team knowledge

D. There is no risk at all as the marketing services are trustworthy

Answer(s): C