Certified Incident Handler (ECIH)

1. You have just attempted to perform DNS poisoning on the local network DNS server and did not succeed; you decide to launch an attack against routing tables instead.
Which of the following would NOT be an effective way of attempting to manipulate the routing table on the local network or through its gateway?

A. By using a source route attack

B. By using ICMP redirect messages

C. By advertising bogus OSDF routes

D. By advertising bogus RIP routes

Answer(s): C

---

2. Why is it so challenging to block packets from Remote Access Troans that use port 80 for network communications? Choose three.

- [ ] A. To a firewall, the traffic appears simply to be from an internal user making an innocuous HTTP GET request.
- [ ] B. Port 80 outbound is normally open on corporate firewalls
- [ ] C. Stateful inspection firewalls will block unsolicited inbound HTTP GET requests
- [ ] D. Not all firewalls are capable of inspecting data in the HTTP data fields for evidence of tunneling

Answer(s): A B D

---

3. Which of the following statements would best describe the act of signing a message with a Digital Signature?

A. The sender creates a hash value of the message he wishes to send He uses his private key to encrypt the hash value.The message and the encrypted hash value are sent to the receiver.

B. The sender creates a hash value of the message he wishes to send. He uses his public key to encrypt the hash value.The message and the encrypted has value are sent to the receiver.

C. The sender creates a hash value of the message he wishes to send. The message and the hash value are sent to the receiver.

D. The sender uses his public key to create a digital signature. The digital signature is sent along with the text message.The receiver will use the sender private key to validate the signature.

Answer(s): A

---

4. One of the last steps taken by an attacker will be to configure permanent access to a compromised system.
However, the installation of a backdoor, installation of new processes, and changes to key files could be very quickly detected by an administrator.
What tool would assist the attacker in preventing the administrator from detecting changes to files, new processes that are running, or other signs that the system might have been compromised?

A. A Trojan horse

B. A Rootkit

C. A Backdoor

D. A privilege escalation tool

Answer(s): B

---

5. Which of the following tools can detect hidden Alternative Data Streams on an NTFS file or folder? Choose all that apply.

- [ ] A. Lns.exe
- [ ] B. Lads.exe
- [ ] C. FileAlyzer
- [ ] D. ADSCheker

Answer(s): A B C

---

6. In order to identify a unique record within a database what would you use?

A. A foreign key

B. A primary key

C. A view

D. A unique key

Answer(s): B

---

7. Why is it important to the security of a network to create a complex password for the SA account on a MSSQL server installation?

A. The SA account is a pseudo-account and does not have any privileges.

B. The SA account can add/delete or change Domain User accounts.

C. The SA account can have privileges of the local administrators group on the host OS.

D. The SA account is the most powerful account on the domain controller.

Answer(s): C

---

8. Bryce, who is a great security professional with a perfect track record, has just been called into his supervisor's office.
His supervisor has the sad task of letting him know that has the next position being cut in their downsizing effort. Bryce has been known to be a mellow type of person but the version of being unemployed after working for 25 years at the same company is just a bit too much for him. He cannot understand why newer employees with only a few years of experience have not been fired before him and why he is the one that must leave. Bryce tells himself that is employer is going to pay dearly for this and has planning to use his skills to cause disruption within the company infrastructure.
Which of the following term would best describe the reaction of Bryce?

A. Cracker

B. Disgruntled Employee

C. Ethical Hacker

D. Revenge Master

Answer(s): B

---

9. Using Netcat what would be the syntax to setup a listening back door from a compromised Windows Server that will spawn a shell when connecting to the remote server on port 777?

A. nc |p 777 e cmd.exe

B. nc sh p 777 e cmd.exe

C. nc |p 777 sh cmd.exe

D. nc |p 777 exec cmd.exe

Answer(s): A

---

10. Duane is a clever attacker, he has penetrated a system and wishes to hide some files within other files on the file system. Which of the following could be used by Duane to attempt hiding files within the file system?

A. Attrib

B. HideNSeek

C. Chgrp

D. Alternate Data Stream

Answer(s): D

---

11. Which of the following penetration framework is Open Source and offers features that are similar to some of its rival commercial tools?

A. CANVAS

B. CORE IMPACT

C. METASPLOIT

D. DEEP HOLE

Answer(s): C

---

12. Software Restriction Policies, if implemented correctly, can help protect against what kinds of threats? Choose two.

- [ ] A. Trojans
- [ ] B. Malware
- [ ] C. Spam
- [ ] D. Smurf Attacks

Answer(s): A B

---

13. If the DS Client software has been installed on Windows 95,Windows 98,and NT 4 computers, what setting of the LanMan Authentication level should be applied to counteract LanMan hash sniffing and offline cracking? Choose the best

A. Send NTLM v2/Refuse LM & NTML

B. Send NTLM only

C. Send LM & NTLM responses

D. Send NTLM v2/Refuse LM

Answer(s): A

---

14. Ping utilities can be used for basic network connectivity test; the ping command sends out an ICMP Echo Request packets and the destination host will reply with an ICMP Echo Reply packets if the host is alive.
However, in some cases the host might be alive and responses are not received.
What is the most likely cause of such behavior?

A. The packet suffers from time exceeded in transit

B. The packet did not reach the destination gateway

C. A filtering device is dropping the packets

D. The remote device OS does not support the ping command.

Answer(s): C

---

15. When doing a Half-Open Scan what packet type would be expected as a response if the port being probed is closed?

A. FIN

B. ACK

C. RST

D. RST/ACK

Answer(s): D

---

16. Mae i a keen system administration; she constantly monitors the mailing list for best practices that are being used out in the field. On the servers that she maintains, Mae has renamed the administrator account to another name to avoid abuse from crackers. However, she found out that it was possible using the sid2user tool to find the new name she used for the administrator account. Mae does not understand; she has NOT shared this name with anyone. How can this be? What is the most likely reason?

A. Her system have been compromised

B. Renaming the administrator account does not change the SID

C. She has not applied all of the patches

D. Someone social engineered her

Answer(s): B

---

17. What built-in Windows command can be used to help find remote access trojans? Choose the best

A. Netstat a

B. Ipconfig/displaydns

C. Nbtstat c

D. Netdiag

Answer(s): A

---

18. Under the Windows platform, there is something referred to as Null Session.
Which of the following statements would best describe what a null session consists of?

A. It is a session where zero bytes of traffic have been transferred

B. It is a session where erroneous commands are being used showing the a lack of knowledge of the user connected.

C. It is a remote session that is established anonymously to a window machine

D. It is a anonymous FTP session under the Windows platform

Answer(s): C

---

19. Why is tunneling-based trojan software so useful for hackers if it is installed inside a corporate network? Choose the best

A. Tunneling software uses ports that are not well knwon,eg.12345

B. Stateful inspection firewalls can only filter Server ports of 1-1023

C. It makes network penetration trivial the tunneling occurs using Whatever port(s) the firewall is configured to allow

D. Anti-trojan software do not have signatures for tunneling trojans, therefore it is easy to have end-users install tunneling trojans.

Answer(s): C

---

20. On a Linux system, which of the following files would contain the list of user accounts, their shell, and their home directories?

A. useradd

B. shadow

C. passwd

D. group

Answer(s): C
