312-50V9$^{Q\&As}$

Certified Ethical Hacker Exam V9

Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee

QUESTION 1

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. PKI

B. single sign on

C. biometrics

D. SOA

Correct Answer: A Section: (none)

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

References: https://en.wikipedia.org/wiki/Public_key_infrastructure

QUESTION 2

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

A. $146

B. $1320

C. $440

D. $100

Correct Answer: A Section: (none)

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000. In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

QUESTION 3

This asymmetry cipher is based on factoring the product of two large prime numbers.

What cipher is described above?

A. RSA

B. SHA

C. RC5

D. MD5

Correct Answer: A Section: (none)

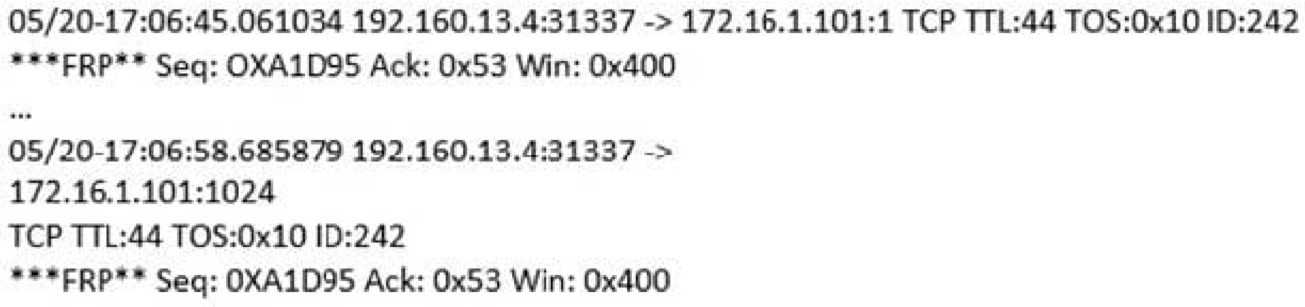
RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

QUESTION 4

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.). Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal? What is odd about this attack? Choose the best answer.



```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.

B. This is back orifice activity as the scan comes from port 31337.

C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.

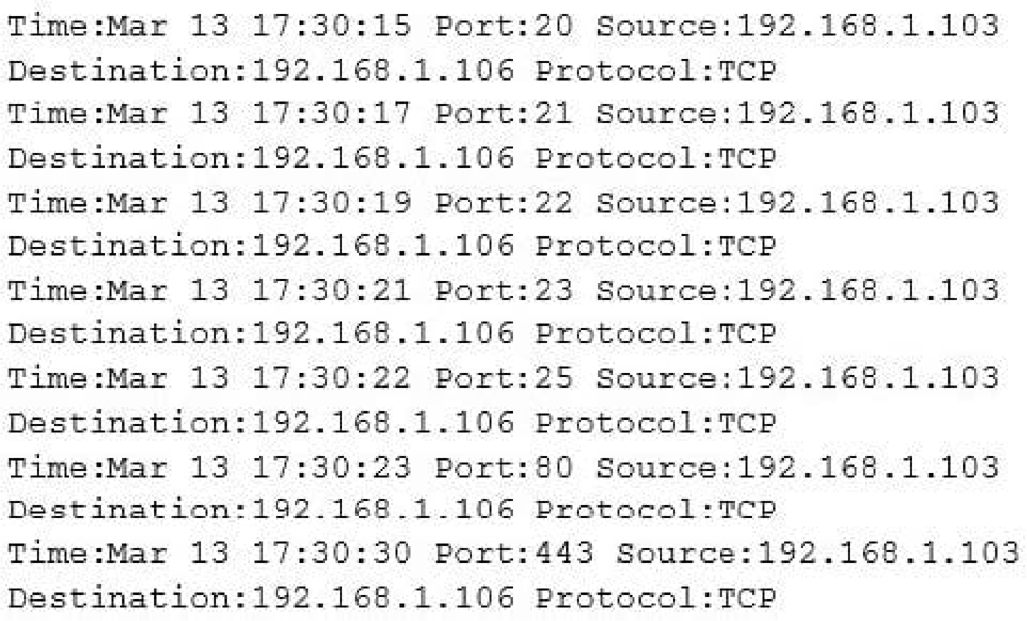
D. These packets were crafted by a tool, they were not created by a standard IP stack.

Correct Answer: B Section: (none)

QUESTION 5

The following is part of a log file taken from the machine on the network with the IP address of

192.168.1.106:



```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

A. Port scan targeting 192.168.1.103

B. Teardrop attack targeting 192.168.1.106

C. Denial of service attack targeting 192.168.1.103

D. Port scan targeting 192.168.1.106

Correct Answer: D Section: (none)

312-50V9 Practice Test 312-50V9 Study Guide 312-50V9 Braindumps