312-50V8^{Q&As}

Certified Ethical Hacker v8

Pass NetApp 312-50V8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/312-50v8.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by NetApp
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

What is the proper response for a NULL scan if the port is open?

A. SYN

B. ACK

C. FIN

D. PSH

E. RST

F. No response

Correct Answer: F

QUESTION 2

Say that "abigcompany.com" had a security vulnerability in the javascript on their website in the past. They recently fixed the security vulnerability, but it had been there for many months.

Is there some way to 4go back and see the code for that error? Select the best answer.

A. archive.org

B. There is no way to get the changed webpage unless you contact someone at the company

C. Usenet

D. Javascript would not be in their html so a service like usenet or archive wouldn\\'t help you

Correct Answer: A

QUESTION 3

It isan entity or event with the potential to adversely impact a system through unauthorized access destruction disclosures denial of service or modification of data.

Which of the following terms best matches this definition?

A. Threat

B. Attack

C. Risk

D. Vulnerability

Correct Answer: A

QUESTION 4

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.

B. They send alerts to security monitors.

C. They use the same packet analysis engine.

D. They use the same packet capture utility.

Correct Answer: D

QUESTION 5

Jason\\'s Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet.

Identify the remote server\\'s port number by decoding the packet?

A. Port 1890 (Net-Devil Trojan)

B. Port 1786 (Net-Devil Trojan)

C. Port 1909 (Net-Devil Trojan)

D. Port 6667 (Net-Devil Trojan)

Correct Answer: D

QUESTION 6

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?

A. Symmetric system

B. Combined system

C. Hybrid system

D. Asymmetric system

Correct Answer: C

QUESTION 7

Tess King, the evil hacker, is purposely sending fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65, 536 bytes. From the information given, what type of attack is Tess King attempting to perform?

A. Syn flood

B. Smurf

C. Ping of death

D. Fraggle

Correct Answer: C

QUESTION 8

Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance

B. Bit length

C. Key strength

D. Entropy

Correct Answer: A

QUESTION 9

A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but in addition to the expected function steals information or harms the system.
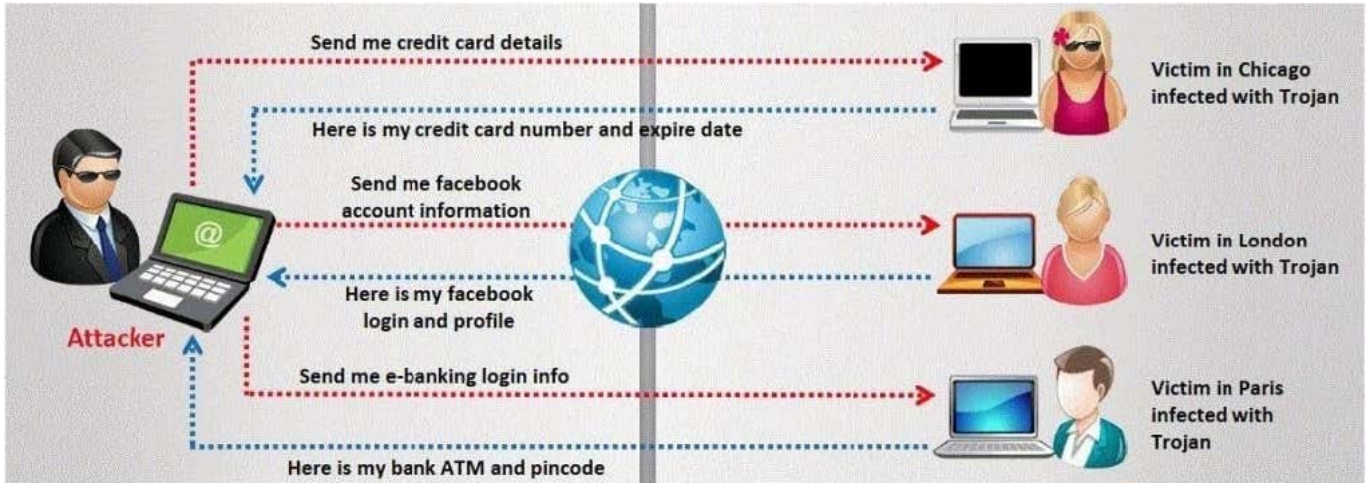
The challenge for an attacker is to send a convincing file attachment to the victim, which gets easily executed on the victim machine without raising any suspicion. Today\'s end users are quite knowledgeable about malwares and viruses. Instead of sending games and fun executables, Hackers today are quite successful in spreading the Trojans using Rogue security software.

What is Rogue security software?

A. A flash file extension to Firefox that gets automatically installed when a victim visits rogue software disabling websites

B. A Fake AV program that claims to rid a computer of malware,but instead installs spyware or other malware onto the computer. This kind of software is known as rogue security software.

C. Rogue security software is based on social engineering technique in which the attackers lures victim to visit spear phishing websites

D. This software disables firewalls and establishes reverse connecting tunnel between the victim\'s machine and that of the attacker

Correct Answer: B

QUESTION 10

What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.

B. LM hashes are based on AES128 cryptographic standard.

C. Uppercase characters in the password are converted to lowercase.

D. LM hashes are not generated when the password length exceeds 15 characters.

Correct Answer: D

QUESTION 11

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known wardriving.

Which algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)

B. Temporal Key Integrity Protocol (TRIP)

C. Wi-Fi Protected Access (WPA)

D. Wi-Fi Protected Access 2(WPA2)

Correct Answer: A

QUESTION 12

Melissa is a virus that attacks Microsoft Windows platforms.

To which category does this virus belong?

A. Polymorphic

B. Boot Sector infector

C. System

D. Macro

Correct Answer: D

QUESTION 13

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company\\'s network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you. He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain

B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks

C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks

D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to

bypass the filters in your gateway

Correct Answer: A

QUESTION 14

What does FIN in TCP flag define?

A. Used to abort a TCP connection abruptly

B. Used to close a TCP connection

C. Used to acknowledge receipt of a previous packet or transmission

D. Used to indicate the beginning of a TCP connection

Correct Answer: B

QUESTION 15

Which of these options is the most secure procedure for strong backup tapes?

A. In a climate controlled facility offsite

B. Inside the data center for faster retrieval in afireproof safe

C. In a cool dry environment

D. On a different floor in the same building

Correct Answer: A

[312-50V8 VCE Dumps](#)   [312-50V8 Practice Test](#)   [312-50V8 Study Guide](#)