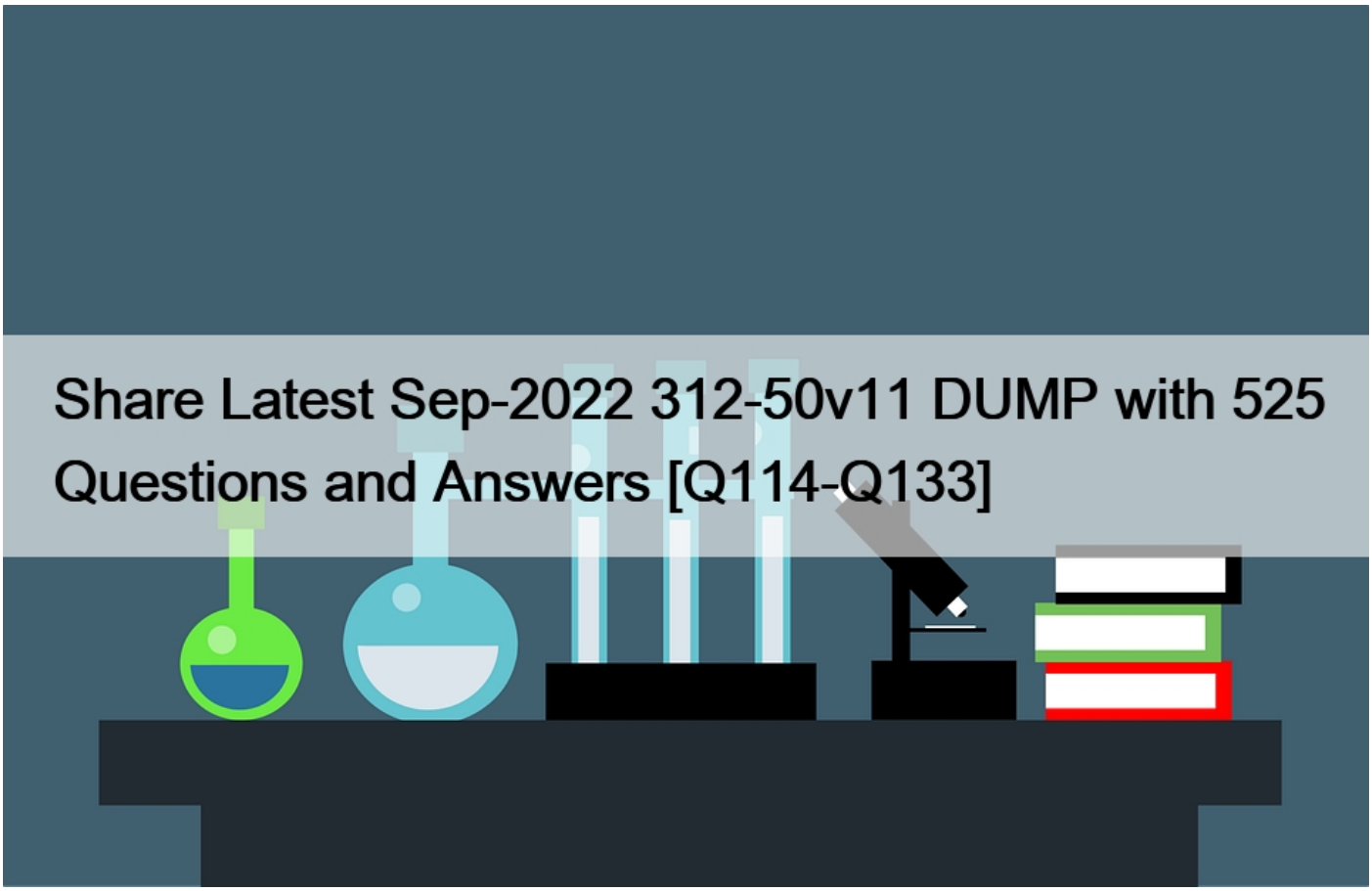
Share Latest Sep-2022 312-50v11 DUMP with 525 Questions and Answers [Q114-Q133



Share Latest Sep-2022 312-50v11 DUMP with 525 Questions and Answers
PDF Dumps 2022 Exam Questions with Practice Test

NEW QUESTION 114

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?
* Side-channel attack
* Denial-of-service attack
* HMI-based attack
* Buffer overflow attack

NEW QUESTION 115

You have gained physical access to a Windows 2008 R2 server, which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu

9.10 Linux LiveCD. Which Linux-based tool can change any user’s password or activate disabled Windows accounts?
* John the Ripper
* SET
* CHNTPW
* Cain & Abel

NEW QUESTION 116

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?
* -T5
* -O
* -T0
* -A

Explanation/Reference:

NEW QUESTION 117

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.
* Spear phishing
* Whaling
* Vishing
* Phishing

NEW QUESTION 118

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?
* The use of security agents in clients’ computers
* The use of DNSSEC
* The use of double-factor authentication
* Client awareness

NEW QUESTION 119

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?
* Key archival
* Key escrow.
* Certificate rollover
* Key renewal

NEW QUESTION 120

Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```


From the options below, choose the exploit against which this rule applies.

* WebDav
* SQL Slammer
* MS Blaster
* MyDoom

NEW QUESTION 121

Study the snort rule given below and interpret the rule. alert tcp any any –> 192.168.1.0/24 111 (content:”|00 01 86 a5|”; msG. “mountd access”;)

* An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
* An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
* An alert is generated when a TCP packet is originated from port 111 of any IP address to the

192.168.1.0 subnet

* An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

NEW QUESTION 122

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SVN ping scan?

* nmap -sn -pp < target ip address >
* nmap -sn -PO < target IP address >
* Anmap -sn -PS < target IP address >
* nmap -sn -PA < target IP address >

NEW QUESTION 123

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

* The attacker queries a nameserver using the DNS resolver.
* The attacker uses TCP to poison the DNS resolver.
* The attacker makes a request to the DNS resolver.
* The attacker forges a reply from the DNS resolver.

NEW QUESTION 124

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

* Wardriving
* KRACK attack
* jamming signal attack
* aLTEr attack

aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.

NEW QUESTION 125

Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_____to encrypt the message, and Bryan uses_____to confirm the digital signature.

* Bryan’s public key; Bryan’s public key
* Alice’s public key; Alice’s public key
* Bryan’s private key; Alice’s public key
* Bryan’s public key; Alice’s public key

NEW QUESTION 126

Which of the following tactics uses malicious code to redirect users’ web traffic?

* Spimming
* Pharming
* Phishing
* Spear-phishing

NEW QUESTION 127

By using a smart card and pin, you are using a two-factor authentication that satisfies

* Something you are and something you remember
* Something you have and something you know
* Something you know and something you are
* Something you have and something you are

NEW QUESTION 128

Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp’s lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

* He must perform privilege escalation.
* He needs to disable antivirus protection.
* He needs to gain physical access.
* He already has admin privileges, as shown by the “501” at the end of the SID.

NEW QUESTION 129

Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization’s OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?
* nmap -Pn -sT –scan-delay 1s –max-parallelism 1 -p < Port List > < Target IP >
* nmap -Pn -sU -p 44818 –script enip-info < Target IP >
* nmap -Pn -sT -p 46824 < Target IP >
* nmap -Pn -sT -p 102 –script s7-info < Target IP >

NEW QUESTION 130

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.

What is the type of attack Jason performed in the above scenario?
* Web server misconfiguration
* Server-side request forgery (SSRF) attack
* Web cache poisoning attack
* Website defacement

NEW QUESTION 131

Attacker Steve targeted an organization’s network with the aim of redirecting the company’s web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website.

What is the technique employed by Steve to gather information for identity theft?
* Pharming
* Skimming
* Pretexting
* Wardriving

NEW QUESTION 132

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources. What is the framework used by James to conduct footprinting and reconnaissance activities?
* WebSploit Framework
* Browser Exploitation Framework
* OSINT framework
* SpeedPhish Framework

NEW QUESTION 133

There are multiple cloud deployment options depending on how isolated a customer’s resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.

What is this cloud deployment option called?
* Private
* Community
* Public
* Hybrid

Since 2003, the EC-Council 312-50 exam has been assisting the world to have profoundly able and seasoned ethical hackers. The latest exam version, 312-50v11, is on the floor now and is all set to bestow a brand-new set of learning & expertise to ambitious specialists. Those who have challenged such an exam and have contrived success are fortuitously placed in the industry and are enjoying a promising career.

Dumps for Free 312-50v11 Practice Exam Questions: https://www.topexamcollection.com/312-50v11-vce-collection.html]