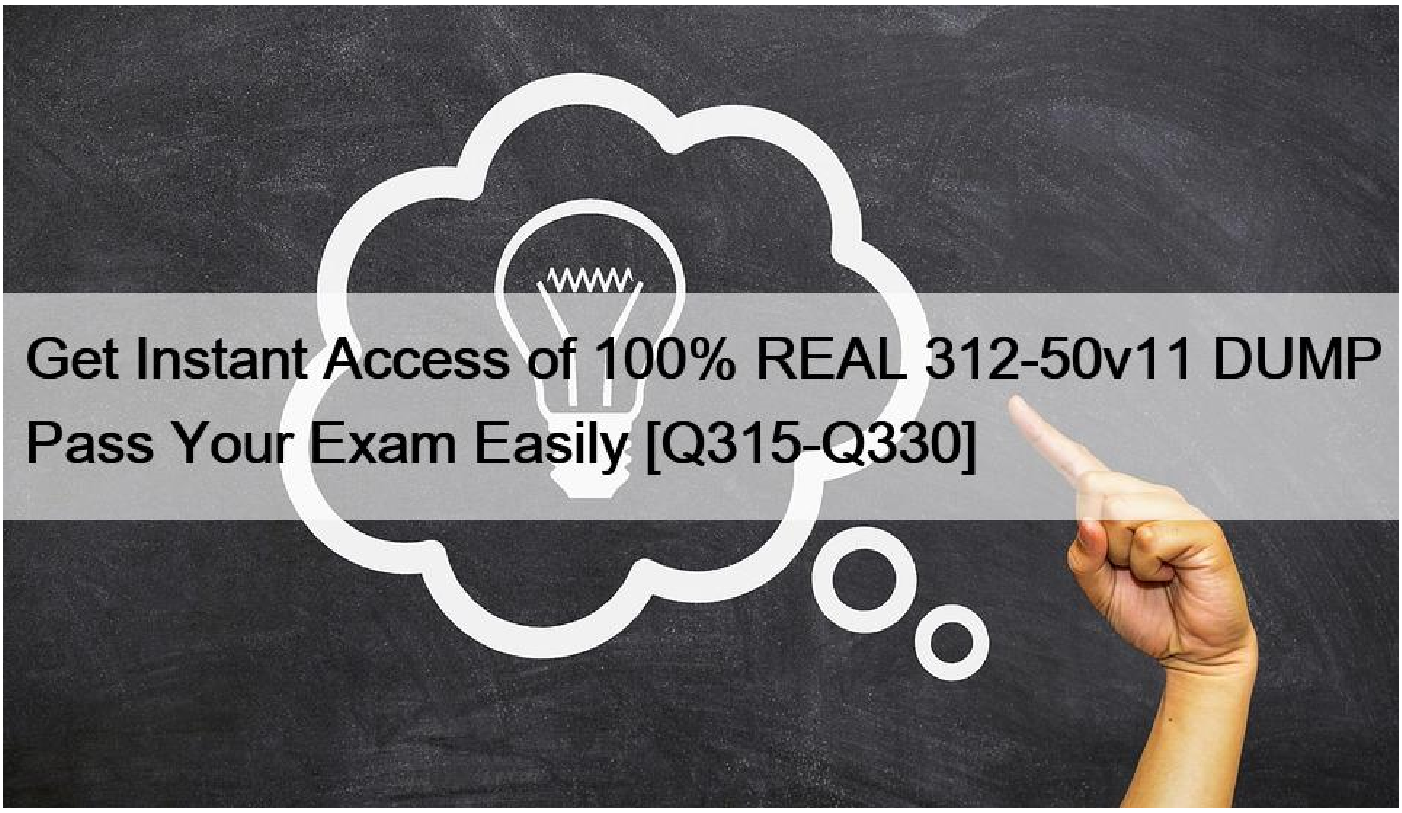
Get Instant Access of 100% REAL 312-50v11 DUMP Pass Your Exam Easily [Q315-Q330



Get Instant Access of 100% REAL 312-50v11 DUMP Pass Your Exam Easily
312-50v11 Free Exam Questions with Quality Guaranteed

Q315. What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
* Black-box
* Announced
* White-box
* Grey-box

Q316. Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.

Identify the behavior of the adversary in the above scenario.
* Unspecified proxy activities
* Use of command-line interface
* Data staging
* Use of DNS tunneling

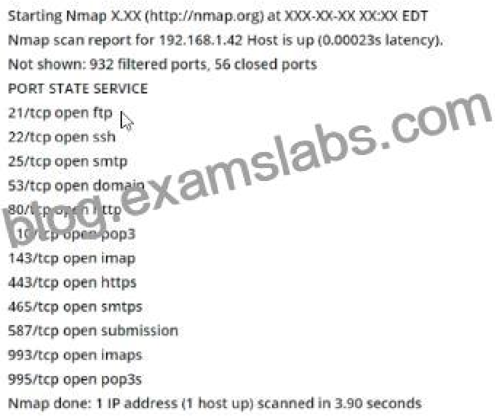
Q317. What is the following command used for?

sqlmap.py-u ,,http://10.10.1.20/?p=1&forumaction=search&#8221; -dbs
* Creating backdoors using SQL injection
* A Enumerating the databases in the DBMS for the URL
* Retrieving SQL statements being executed on the database
* Searching database statements at the IP address given

Q318. Widespread fraud ac Enron. WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?
* Fed RAMP
* PCIDSS
* SOX
* HIPAA
The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies.Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.

The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

Q319. Consider the following Nmap output:



```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

what command-line parameter could you use to determine the type and version number of the web server?
* -sv
* -Pn
* -V
* -ss

Q320. Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization&#8217;s vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?
* Medium
* Low

* Critical
* High

Rating	CVSS Score
None	0.0
Low	0.1 &#8211; 3.9
Medium	4.0 &#8211; 6.9
High	7.0 &#8211; 8.9
Critical	9.0 &#8211; 10.0

Q321. A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?
* Credentialed assessment
* Database assessment
* Host-based assessment
* Distributed assessment

Explanation

The host-based vulnerability assessment (VA) resolution arose from the auditors&#8217; got to periodically review systems. Arising before the net becoming common, these tools typically take an &#8220;administrator&#8217;s eye&#8221; read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal.

UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.

What it Measures Host

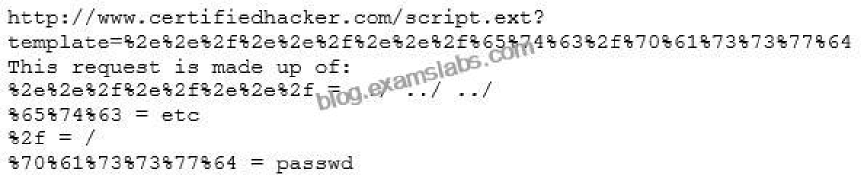
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally &#8220;dormant&#8221; vulnerabilities &#8211; those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

Q322. Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?
* AOL
* ARIN
* DuckDuckGo
* Baidu

Q323. Which of the following is the primary objective of a rootkit?
* It opens a port to provide an unauthorized service
* It creates a buffer overflow
* It replaces legitimate programs
* It provides an undocumented opening in a program

Q324. 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&#8217;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 &#8211;scan-delay 1s &#8211;max-parallelism 1 -p < Port List > < Target IP >
* nmap -Pn -sU -p 44818 &#8211;script enip-info < Target IP >
* nmap -Pn -sT -p 46824 < Target IP >
* nmap -Pn -sT -p 102 &#8211;script s7-info < Target IP >

Q325. Take a look at the following attack on a Web Server using obstructed URL:



```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?
* Configure the Web Server to deny requests involving &#8220;hex encoded&#8221; characters
* Create rules in IDS to alert on strange Unicode requests
* Use SSL authentication on Web Servers
* Enable Active Scripts Detection at the firewall and routers

Q326. 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

Q327. You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees&#8217; emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?
* Reconnaissance
* Command and control
* Weaponization
* Exploitation

Explanation

This stage coupling exploit with backdoor into deliverable payload

Next, attackers can re-engineer some core malware to suit their functions victimization subtle techniques.

counting on the requirements and talents of the assaulter, the malware might exploit antecedently unknown vulnerabilities, aka &#8220;zero-day&#8221; exploits, or some combination of vulnerabilities, to quietly defeat a network&#8217;s defenses. By reengineering the malware, attackers scale back the probability of detection by ancient security solutions. This method typically involves embedding specially crafted malware into Associate in Nursing otherwise benign or legitimate document, like a press release or contract document, or hosting the malware on a compromised domain.

Q328. Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.

What is the type of web-service API mentioned in the above scenario?
* RESTful API
* JSON-RPC
* SOAP API
* REST API

Q329. You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees&#8217; emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?
* Reconnaissance
* Command and control
* Weaponization
* Exploitation
Explanation

Weaponization

The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary: o Identifying appropriate malware payload based on the analysis o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability o Creating a phishing email campaign o Leveraging exploit kits and botnets

Q330. What is the proper response for a NULL scan if the port is open?
* SYN
* ACK
* FIN
* PSH
* RST
* No response

Training Courses **For better 312-50v11 exam readiness, it is wise to join a training course endorsed by the vendor. Overall, there are many official live online classes so here are the best picks:** - CEH MasterClass Program - To master the exam domains and acquire noteworthy practical as well as conjectural subject matter cognizance, join the CEH MasterClass Program. This package includes CEH e-courseware, exam insurance information, and live labs so it is worth a try.- CEH Exam Prep ? Live Online - This training course covers the CEH exam content and details via a skilled instructor through online live sessions.

312-50v11 Free Exam Files Downloaded Instantly: https://www.examslabs.com/EC-COUNCIL/CEH-v11/best-312-50v11-exam-dumps.html]