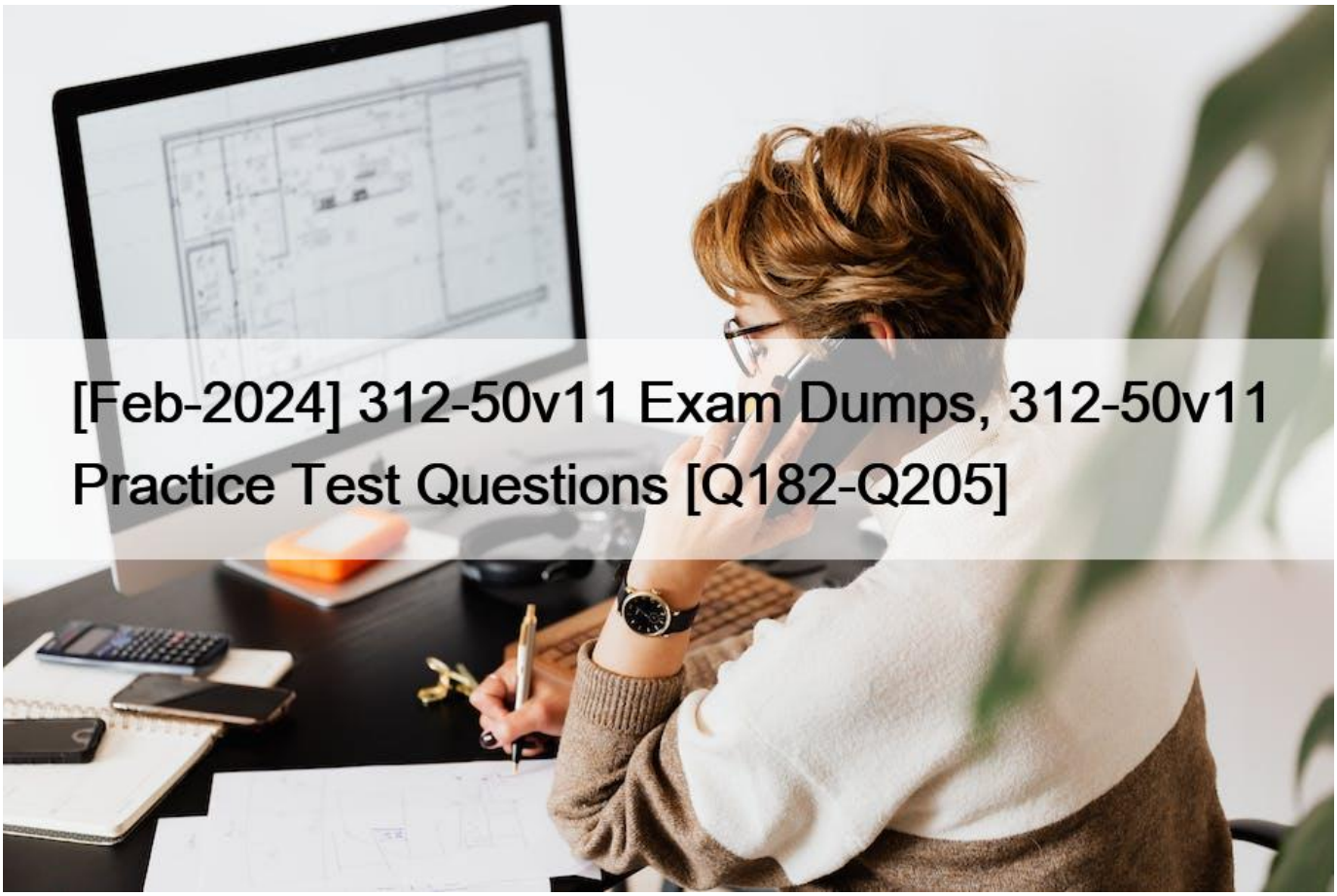
[Feb-2024 312-50v11 Exam Dumps, 312-50v11 Practice Test Questions [Q182-Q205



[Feb-2024] 312-50v11 Exam Dumps, 312-50v11 Practice Test Questions
Attested 312-50v11 Dumps PDF Resource [2024]

Q182. 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

Q183. Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company’s email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

What is the first thing that Nedved needs to do before contacting the incident response team?
* Leave it as it Is and contact the incident response te3m right away

* Block the connection to the suspicious IP Address from the firewall
* Disconnect the email server from the network
* Migrate the connection to the backup email server

Q184. An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network’s external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?
* Protocol analyzer
* Network sniffer
* Intrusion Prevention System (IPS)
* Vulnerability scanner

Q185. _____ 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

Q186. 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/Rep 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
* -sS
* -Pn
* -V

Q187. Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?
* Rootkit
* Trojan
* A Worm
* Adware

Q188. Attacker Rony installed a rogue access point within an organization’s perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by johnson in the above scenario?
* Host-based assessment
* Wireless network assessment
* Application assessment
* Distributed assessment

Wireless network assessment determines the vulnerabilities in an organization’s wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization’s perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

Q189. If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?
* Birthday
* Brute force
* Man-in-the-middle
* Smurf

Q190. John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?
* DNS cache snooping
* DNSSEC zone walking
* DNS tunneling method
* DNS enumeration

Explanation

DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it’s become a well-liked but effective tool in many attacks.Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi.On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voila, we’ve internet access.This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow.Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances…) to line up an immediate and unmonitored communications channel on an organisation’s network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool… you name it.To make it even more worrying, there’s an outsized amount of easy to use DNS tunneling tools out there.There’s even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it).As a pentester all this is often great, as a network admin not such a lot .

How does it work:For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person’s name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people’s names.For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is:* A Record: Maps a website name to an IP address.example.com ? 12.34.52.67* NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers.example.com ? server1.example.com, server2.example.comWho is involved in DNS tunneling?* Client. Will launch DNS requests with data in them to a website .* One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.* Server. this is often the defined nameserver which can ultimately receive the DNS requests.The 6 Steps in DNS tunneling (simplified):1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com2. The DNS request goes bent a DNS server.3. The DNS server finds out the A register of your domain with the IP address of your server.4. The request for mypieceofdata.server1.example.com is forwarded to the server.5. The server processes regardless of the mypieceofdata was alleged to do. Let’s assume it had been an HTTP request.6. The server replies back over DNS and woop woop, we’ve got signal.

Q191. What would be the purpose of running “wget 192.168.0.15 -q -S” against a web server?
* Performing content enumeration on the web server to discover hidden folders
* Using wget to perform banner grabbing on the webserver
* Flooding the web server with requests to perform a DoS attack
* Downloading all the contents of the web page locally for further examination

-q, –quiet quiet (no output)

-S, –server-response print server response

Q192. Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?
* ARIN
* APNIC
* RIPE
* LACNIC

Q193. ping-* 6 192.168.0.101

Output:

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101: bytes=32 time<1ms TTL=128

Reply from 192.168.0.101:

Ping statistics for 192.168.0101

Packets: Sent = 6, Received = 6, Lost = 0 (0% loss).

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

What does the option * indicate?
* t
* s
* a
* n

Q194. A zone file consists of which of the following Resource Records (RRs)?
* DNS, NS, AXFR, and MX records
* DNS, NS, PTR, and MX records
* SOA, NS, AXFR, and MX records
* SOA, NS, A, and MX records

Q195. A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.
* Use port security on his switches.
* Use a tool like ARPwatch to monitor for strange ARP activity.
* Use a firewall between all LAN segments.
* If you have a small network, use static ARP entries.
* Use only static IP addresses on all PC’s.

Q196. Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.

What is the port scanning technique used by Sam to discover open ports?
* Xmas scan

* IDLE/IPID header scan
* TCP Maimon scan
* ACK flag probe scan

Q197. Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.

Which of the following tiers of the container technology architecture is Abel currently working in?
* Tier-1: Developer machines
* Tier-2: Testing and accreditation systems
* Tier-3: Registries
* Tier-4: Orchestrators

Q198. Which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?
* Botnet
* Intrusion detection system
* Firewall
* Honeypot

Q199. 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.
* use of command-line interface
* Data staging
* Unspecified proxy activities
* Use of DNS tunneling

Explanation

A proxy server acts as a gateway between you and therefore the internet. It’s an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy.If you’re employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you’ll see the page in your browser.

Q200. A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm’s public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html

Accept-Ranges: bytes

Last Modified: Wed, 28 Dec 2010 15:32:21 GMT

ETag:”b0aac0542e25c31:89d”

Content-Length: 7369

Which of the following is an example of what the engineer performed?
* Banner grabbing
* SQL injection
* Whois database query
* Cross-site scripting

Q201. Which service in a PKI will vouch for the identity of an individual or company?
* KDC
* CR
* CBC
* CA

Q202. Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?
* btlejack-f 0x129f3244-j
* btlejack -c any
* btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
* btlejack -f 0x9c68fd30 -t -m 0x1 fffffffff

Q203. Steve, an attacker, created a fake profile on a social media website and sent a request to Stell a. Stella was enthralled by Steve’s profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?
* Diversion theft
* Baiting
* Honey trap
* Piggybacking

The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company’s logo, thereby tricking

end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.

For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label “Employee Salary Information 2019” and a legitimate company’s logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim’s system, giving the attacker access.

Q204. Let’s imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?
* Install DNS logger and track vulnerable packets
* Disable DNS timeouts
* Install DNS Anti-spoofing
* Disable DNS Zone Transfer

Q205. Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.

Which of the following tools is used by Wilson in the above scenario?
* Factiva
* Netcraft
* infoga
* Zoominfo

The CEH v11 certification program is ideal for professionals who are interested in pursuing a career in cybersecurity, particularly in the field of ethical hacking. Certified Ethical Hacker Exam (CEH v11) certification program provides a comprehensive understanding of various hacking techniques, tools, and methodologies that are commonly used by cybercriminals. The program also covers topics such as network security, web application security, mobile security, and cloud security.

The CEH v11 exam covers a wide range of topics, including ethical hacking techniques, network security concepts, and information security management. 312-50v11 exam is based on the latest industry trends and technologies, ensuring that individuals are equipped with the latest knowledge and skills to stay ahead in the field.

Latest 312-50v11 Actual Free Exam Questions Updated 525 Questions:
https://www.validexam.com/312-50v11-latest-dumps.html]