312-50V12$^{Q\&As}$

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What does the following command in netcat do? nc -l -u -p55555

A. logs the incoming connections to /etc/passwd file

B. loads the /etc/passwd file to the UDP port 55555

C. grabs the /etc/passwd file when connected to UDP port 55555

D. deletes the /etc/passwd file when connected to the UDP port 55555

Correct Answer: C

QUESTION 2

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 could not detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication between the victim machine and the CandC server. What is the technique employed by John to bypass the firewall?

A. DNS cache snooping

B. DNSSEC zone walking

C. DNS tunneling method

D. DNS enumeration

Correct Answer: C

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 voil? 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.

QUESTION 3

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a

session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to

test the randomness of session tokens.

Which of the following tools is used by Gregory in the above scenario?

A. Nmap

B. Burp Suite

C. CxSAST

D. Wireshark

Correct Answer: B

QUESTION 4

What piece of hardware on a computer\\'s motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU

B. GPU

C. UEFI

D. TPM

Correct Answer: D

The TPM is a chip that\\'s part of your computer\\'s motherboard -- if you bought an off-the-shelf PC, it\\'s soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The

TPM generates encryption keys, keeping part of the key to itself

QUESTION 5

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA

B. -sX

C. -sT

D. -sF

Correct Answer: A

Latest 312-50V12 Dumps 312-50V12 Study Guide 312-50V12 Exam Questions