312-50V11Q&As

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v11.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Correct Answer: B

QUESTION 2

A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to

the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple

connections and keeps waiting for the requests to complete.

Which attack is being described here?

A. Desynchronization

B. Slowloris attack

C. Session splicing

D. Phlashing

Correct Answer: B

Developed by Robert "RSnake" Hansen, Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server\\'s web server only, with almost no side effects on other services and ports.Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.x and 2.x.Over the years, Slowloris has been credited with variety of high-profile server takedowns. Notably, it had been used extensively by Iranian `hackivists\\' following the 2009 Iranian presidential election to attack Iranian government internet sites .Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, expecting each of the attack requests to be completed.Periodically, the Slowloris sends subsequent HTTP headers for every request, but never actually completes the request. Ultimately, the targeted server\\'s maximum concurrent connection pool is filled, and extra (legitimate) connection attempts are denied.By sending partial, as against malformed, packets, Slowloris can easily elapse traditional Intrusion Detection systems.Named after a kind of slow- moving Asian primate, Slowloris really does win the race by moving slowly and steadily. A Slowloris attack must await sockets to be released by legitimate requests before consuming them one by one.For a high-volume internet site , this will take a while . the method are often further slowed if legitimate sessions are reinitiated. But within the end, if the attack is unmitigated, Slowloris--like the tortoise--wins the race.If undetected or unmitigated, Slowloris attacks also can last for long periods of your time . When attacked sockets outing , Slowloris simply reinitiates the connections, continuing to reach the online server until mitigated.Designed for stealth also as efficacy, Slowloris are often modified to send different host headers within the event that a virtual host is targeted, and logs are stored separately for every virtual host.More importantly, within the course of an attack, Slowloris are often set to suppress log file creation. this suggests the attack can catch unmonitored servers off-guard, with none red flags appearing in log file entries.Methods of mitigationImperva\\'s security services are enabled by reverse proxy technology, used for inspection of all incoming requests on their thanks to the clients\\' servers.Imperva\\'s secured proxy won\\'t forward any partial connection requests--rendering all Slowloris DDoS attack attempts completely and utterly useless.

QUESTION 3

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.

A. use of command-line interface

B. Data staging

C. Unspecified proxy activities

D. Use of DNS tunneling

Correct Answer: C

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.

QUESTION 4

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

A. Block port 25 at the firewall.

B. Shut off the SMTP service on the server.

C. Force all connections to use a username and password.

D. Switch from Windows Exchange to UNIX Sendmail.

E. None of the above.

Correct Answer: E

QUESTION 5

Which of the following is an extremely common IDS evasion technique in the web world?

A. Spyware

B. Subnetting

C. Unicode Characters

D. Port Knocking

Correct Answer: C