C. Hybrid Attack
D. BruteDict Attack

Correct Answer: C

QUESTION 92
You receive an e-mail with the following text message. "Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible." You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service". What category of virus is this?

A. Virus hoax
B. Spooky Virus
C. Stealth Virus
D. Polymorphic Virus

Correct Answer: A

QUESTION 93
Choose one of the following pseudo codes to describe this statement:

"If we have written 200 characters to the buffer variable, the stack should stop because it cannot hold any more data."

A. If (I > 200) then exit (1)
B. If (I < 200) then exit (1)
C. If (I <= 200) then exit (1)
D. If (I >= 200) then exit (1)

Correct Answer: D

QUESTION 94
One of the effective DoS/DDoS countermeasures is 'Throttling'. Which statement correctly defines this term?

A. Set up routers that access a server with logic to adjust incoming traffic to levels that will be safe for the server to process.
B. Providers can increase the bandwidth on critical connections to prevent them from going down in the event of an attack.
C. Replicating servers that can provide additional failsafe protection.
D. Load balance each server in a multiple-server architecture.

Correct Answer: A

QUESTION 95
Attackers footprint target Websites using Google Hacking techniques. Google hacking is a term that refers to the art of creating complex search engine queries. It detects websites that are vulnerable to numerous exploits and vulnerabilities. Google operators are used to locate specific strings of text within the search results. The configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database. WordPress uses config.php that stores the database Username and Password. Which of the below Google search string brings up sites with "config.php" files?

A. Search:index config/php
B. Wordpress:index config.php
C. intitle:index.of config.php
D. Config.php:index list

Correct Answer: C

QUESTION 96

Which of the following tool would be considered as Signature Integrity Verifier (SIV)?

A. Nmap
B. SNORT
C. Virus SCAN
D. Tripwire

Correct Answer: D

QUESTION 97

Bob has set up three web servers on Windows Server 2008 IIS 7.0. Bob has followed all the recommendations for securing the operating system and IIS. These servers are going to run numerous e-commerce websites that are projected to bring in thousands of dollars a day. Bob is still concerned about the security of these servers because of the potential for financial loss. Bob has asked his company's firewall administrator to set the firewall to inspect all incoming traffic on ports 80 and 443 to ensure that no malicious data is getting into the network. Why will this not be possible?

A. Firewalls cannot inspect traffic coming through port 443.
B. Firewalls can only inspect outbound traffic.
C. Firewalls cannot inspect traffic at all, they can only block or allow certain ports.
D. Firewalls cannot inspect traffic coming through port 80.

Correct Answer: C

QUESTION 98

Which of the following statement correctly defines ICMP Flood Attack? (Select 2 answers)

The attacker sends ICMP ECHO requests with spoofed source addresses
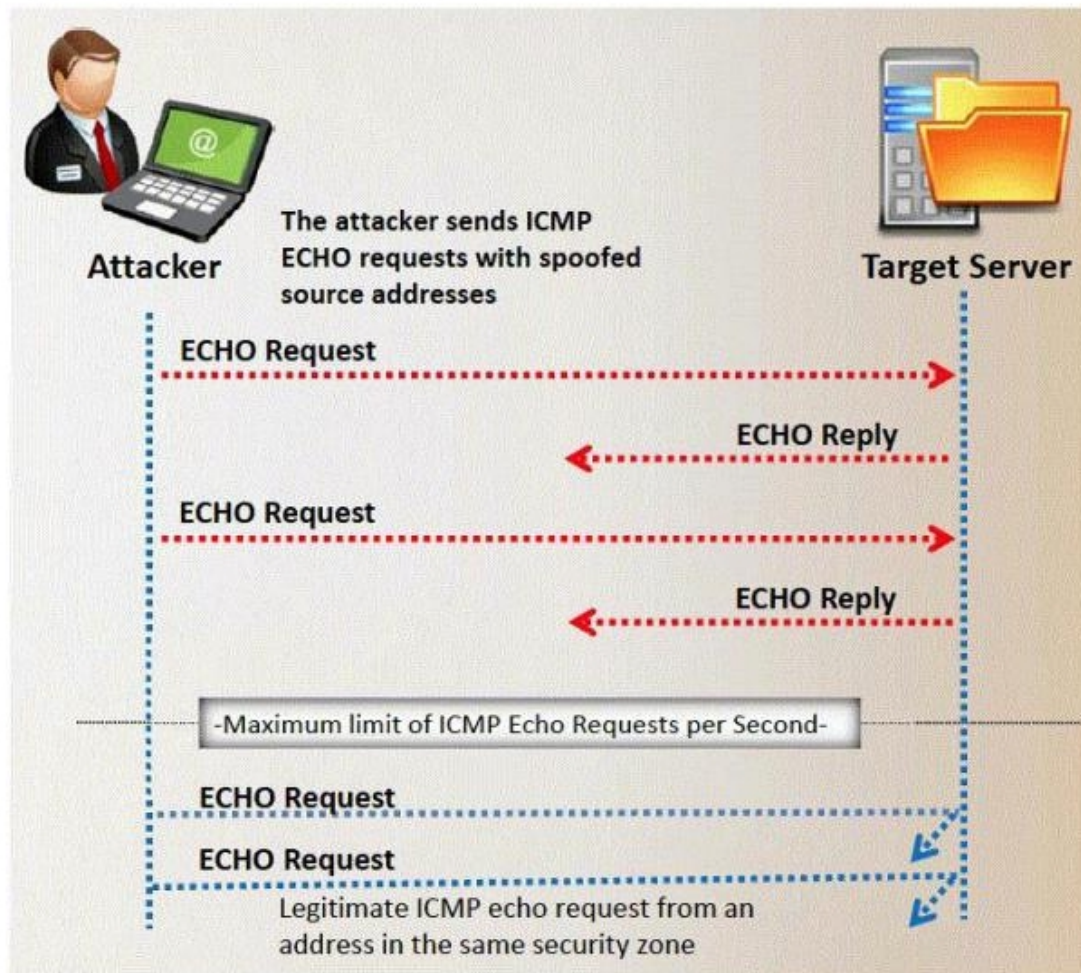
A. Bogus ECHO reply packets are flooded on the network spoofing the IP and MAC address
B. The ICMP packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network
C. ECHO packets are flooded on the network saturating the bandwidth of the subnet causing denial of service
D. A DDoS ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets to the victim system.

Correct Answer: BD

QUESTION 99
Which type of scan does NOT open a full TCP connection?

A. Stealth Scan
B. XMAS Scan
C. Null Scan
D. FIN Scan