   A penetration tester is conducting a gray box penetration test. She notices that one of the branch offices of the organization uses a caching-only DNS server to handle name resolution requests. She sends a bogus reply to a name resolution request from

the caching-only DNS server, using a spoofed source address in the reply packets. The bogus name resolution records point users to a fake web server that is used to harvest authentication credentials. What is this exploit called?

Step 1: Answer with Example

Answer: option **C.**DNS cache poisoning

Explanation:

Another example of DNS cache poisoning is this. In this case, the caching-only DNS server's cache has been tainted rather than the local DNS cache on workstations. Until the TTL value is achieved, the poisoned entries will remain in the cache.

Step 2: Explanation for incorrect option

The highly deceptive cyberattack known as DNS poisoning, often referred to as DNS cache poisoning or DNS spoofing, involves hackers diverting online traffic to phishing websites and bogus web servers.

Sending malicious ARP packets to a default gateway on a LAN in order to alter the pairings in its IP to MAC address table is known as ARP Poisoning (also known as ARP Spoofing), and it is a sort of cyberattack used across Local Area Networks (LANs). IP addresses are converted into MAC addresses by the ARP Protocol.

A cyberattack known as a man-in-the-middle (MiTM) attack involves the perpetrator discreetly intercepting and relaying messages between two parties who believe they are speaking directly to one another. The attack is a form of eavesdropping in which the assailant overhears the full discussion before taking control of it.

 You are performing a gray box penetration test for a medium-sized organization. You have used reconnaissance techniques to identify a help desk employee and a payroll employee. You craft an email to the payroll employee that appears to come from the help desk employee directing the payroll employee to reset her password. When she clicks the link provided in the email, she is redirected to your own website where her credentials are captured to a text file. What kind of exploit did you use?

**A.**Phishing

**B.**Interrogation

**C.**Spear phishing

**D.**Whaling

Step 1: Answer with Explanation

Answer: option **C.**Spear phishing

Explanation:

Because the infected email was created especially for a particular employee, a spear phishing assault was used in this instance. On the other hand, a generic phishing assault would have been launched indiscriminately to a huge number of workers within the company.

Step 2: Explanation for incorrect option

Phishing is an assault that tries to steal your money or your identity by tricking you into disclosing personal information on websites that look authentic but are actually fake, such as credit card numbers, bank account information, or passwords.

When investigating computer crimes, interrogations are conducted in accordance with practical guidelines created by criminalistics

Employees of information system owners and users typically do the initial detection of illicit activities involving computer information. Eyewitness testimony may provide a description of these actions' characteristics.

A whale attack, often referred to as a whaling phishing attack or a whaling phishing, is a particular kind of phishing attempt that targets prominent workers, such as the chief executive officer or chief financial officer, in order to acquire confidential data from a business.

You are performing a black box penetration test for a medium-sized organization that sells imported motorcycles and ATVs through its online storefront. You need to discover who owns the organization's domain. Which tool in your penetration testing toolkit should you use?  
  
A. nslookup  
B. whois  
C. Shodan  
D. Maltego

Step 1: Answer with Explanation

Answer: B. whois

Explanation

Whois Pentest

To find out who owns a specific domain, use the whois command to search public data.

The protocol known as "whois" is used to query the Regional Internet Registries' servers, which house data on each resource (IP address or domain name) registered on the Internet. You can learn the following details about a resource: Owner company's name.

Step 2: Explanation for incorrect option

The application known as "nslookup" enables any computer user or Internet server administrator to enter a host name (for instance, "whatis.com") and discover the related IP address or domain name system (DNS) record.

With the help of a number of filters, users of the search engine Shodan can look for various internet-connected servers, such as cameras, routers, and servers. A search engine of service banners, which are metadata that the server delivers back to the client, is another way that it has been characterised.

Maltego is a comprehensive tool for graphical link studies that provides real-time data mining and information collection in addition to the depiction of this data on a node-based graph, making patterns and multiple order relationships between said data easily discernible.