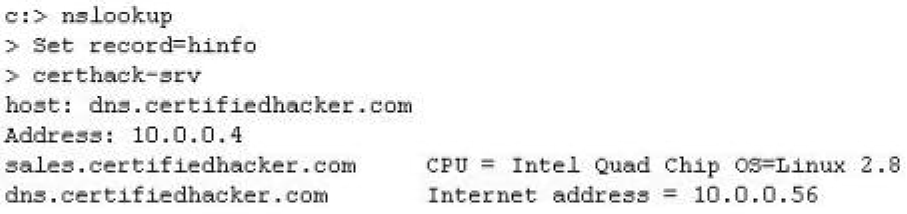
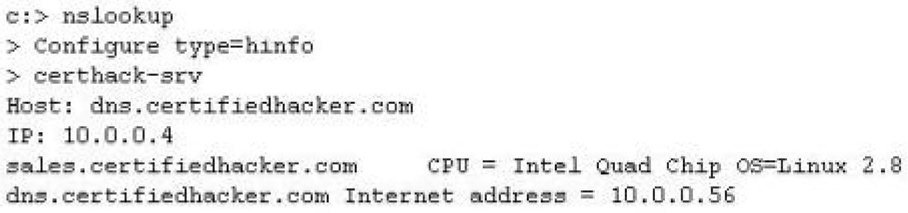


```
c:> nslookup
> Set record=hinfo
> certhack-srv
host: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

D.



```
c:> nslookup
> Configure type=hinfo
> certhack-srv
Host: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
```

Correct Answer: A

QUESTION 83

Bret is a web application administrator and has just read that there are a number of surprisingly common web application vulnerabilities that can be exploited by unsophisticated attackers with easily available tools on the Internet. He has also read that when an organization deploys a web application, they invite the world to send HTTP requests. Attacks buried in these requests sail past firewalls, filters, platform hardening, SSL, and IDS without notice because they are inside legal HTTP requests. Bret is determined to weed out vulnerabilities. What are some of the common vulnerabilities in web applications that he should be concerned about?

A. Non-validated parameters, broken access control, broken account and session management, cross-site scripting and buffer overflows are just a few common vulnerabilities.

B. Visible clear text passwords, anonymous user account set as default, missing latest security patch, no firewall filters set and no SSL configured are just a few common vulnerabilities.

C. No SSL configured, anonymous user account set as default, missing latest security patch, no firewall filters set and an inattentive system administrator are just a few common vulnerabilities.

D. No IDS configured, anonymous user account set as default, missing latest security patch, no firewall filters set and visible clear text passwords are just a few common vulnerabilities.

Correct Answer: A

QUESTION 84

What is War Dialing?

A. War dialing involves the use of a program in conjunction with a modem to penetrate the modem/PBX-based systems.

B. War dialing is a vulnerability scanning technique that penetrates Firewalls.
C. It is a social engineering technique that uses Phone calls to trick victims.
D. Involves IDS Scanning Fragments to bypass Internet filters and stateful Firewalls.

Correct Answer: A

QUESTION 85

Steven the hacker realizes the network administrator of Acme Corporation is using Syskey in Windows 2008 Server to protect his resources in the organization. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by Syskey before he can attempt to use brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2008 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch the attack. How many bits does Syskey use for encryption?

A. 40-bit encryption
B. 128-bit encryption
C. 256-bit encryption
D. 64-bit encryption

Correct Answer: B

QUESTION 86

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

A. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card.
B. Educate and enforce physical security policies of the company to all the employees on a regular basis.
C. Setup a mock video camera next to the special card reader adjacent to the secure door.
D. Post a sign that states, “no tailgating" next to the special card reader adjacent to the secure door.

Correct Answer: B

QUESTION 87

Ursula is a college student at a University in Amsterdam. Ursula originally went to college to study engineering but later changed to marine biology after spending a month at sea with her friends. These friends frequently go out to sea to follow and harass fishing fleets that illegally fish in foreign waters. Ursula eventually wants to put companies practicing illegal fishing out of business. Ursula decides to hack into the parent company's computers and destroy critical data knowing fully well that, if caught, she probably would be sent to jail for a very long time. What would Ursula be considered?

A. Ursula would be considered a gray hat since she is performing an act against illegal activities.
B. She would be considered a suicide hacker.
C. She would be called a cracker.
D. Ursula would be considered a black hat.

Correct Answer: B

QUESTION 88

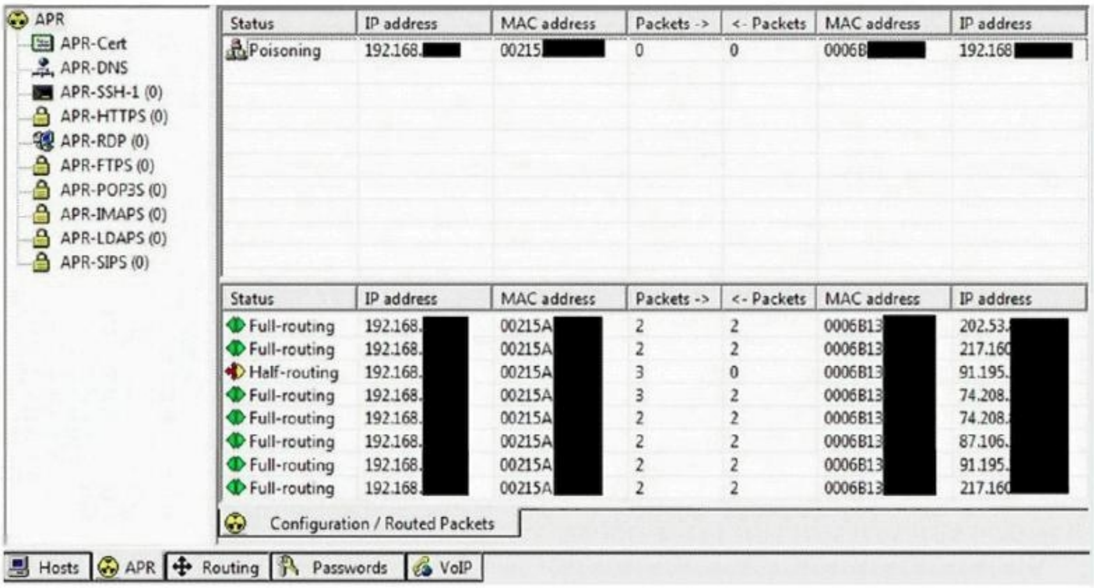
Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system. Which of the following is NOT an example of default installation?

A. Many systems come with default user accounts with well-known passwords that administrators forget to change.
B. Often, the default location of installation files can be exploited which allows a hacker to retrieve a file from the system.
C. Many software packages come with "samples" that can be exploited, such as the sample programs on IIS web services.
D. Enabling firewall and anti-virus software on the local system.

Correct Answer: D

QUESTION 89

This tool is widely used for ARP Poisoning attack. Name the tool.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.[redacted]	00215[redacted]	0	0	0006B[redacted]	192.168[redacted]

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	202.53.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	217.160[redacted]
Half-routing	192.168.[redacted]	00215A[redacted]	3	0	0006B13[redacted]	91.195.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	3	2	0006B13[redacted]	74.208.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	74.208.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	87.106.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	91.195.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	217.160[redacted]

A. Cain and Able

B. Beat Infector

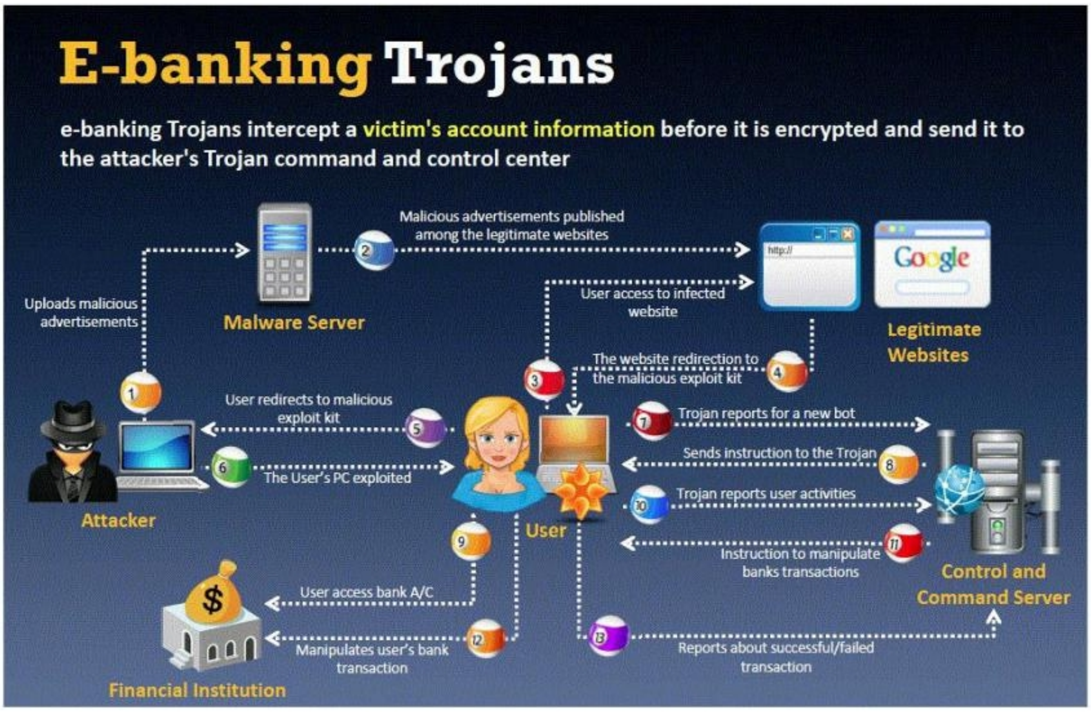
C. Poison Ivy

D. Webarp Infector

Correct Answer: A

QUESTION 90

BankerFox is a Trojan that is designed to steal users' banking data related to certain banking entities. When they access any website of the affected banks through the vulnerable Firefox 3.5 browser, the Trojan is activated and logs the information entered by the user. All the information entered in that website will be logged by the Trojan and transmitted to the attacker's machine using covert channel. BankerFox does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer. What is the most efficient way an attacker located in remote location to infect this banking Trojan on a victim's machine?



E-banking Trojans

e-banking Trojans intercept a victim's account information before it is encrypted and send it to the attacker's Trojan command and control center

Uploads malicious advertisements
1
Malware Server
2
Malicious advertisements published among the legitimate websites
User access to infected website
3
Legitimate Websites
The website redirection to the malicious exploit kit
4
User redirects to malicious exploit kit
5
6
The User's PC exploited
Attacker
User
7
Trojan reports for a new bot
Sends instruction to the Trojan
8
Trojan reports user activities
10
Instruction to manipulate banks transactions
11
Control and Command Server
9
User access bank A/C
12
Manipulates user's bank transaction
13
Reports about successful/failed transaction
Financial Institution

A. Physical access - the attacker can simply copy a Trojan horse to a victim's hard disk infecting the machine via Firefox add-on extensions.

B. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer.

C. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer.

D. Custom packaging - the attacker can create a custom Trojan horse that mimics the appearance of a program that is unique to that particular computer.

E. Downloading software from a website. An attacker can offer free software, such as shareware programs and pirated mp3 files.

Correct Answer: E

QUESTION 91

In the context of password security: a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive - though slow. Usually, it tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary combined together to have variations of words, what would you call such an attack?

A. Full Blown Attack

B. Thorough Attack