QUESTION 10
How do you defend against ARP Spoofing? Select three.

A. Use ARPWALL system and block ARP spoofing attacks.
B. Tune IDS Sensors to look for large amount of ARP traffic on local subnets.
C. Use private VLANS.
D. Place static ARP entries on servers, workstation and routers.

Correct Answer: ABD

QUESTION 11
TCP SYN Flood attack uses the three-way handshake mechanism.

1. An attacker at system A sends a SYN packet to victim at system B.
2. System B sends a SYN/ACK packet to victim A.
3. As a normal three-way handshake mechanism system A should send an ACK packet to system B, however, system A does not send an ACK packet to system B. In this case client B is waiting for an ACK packet from client A.

This status of client B is called _____.

A. "half-closed"
B. "half open"
C. "full-open"
D. "xmas-open"

Correct Answer: B

QUESTION 12
Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company. She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them, only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special

software to further examine the pictures and finds that each one had hidden text that was stored in each picture. What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

A. The Kiley Innovators employee used cryptography to hide the information in the emails sent.
B. The method used by the employee to hide the information was logical watermarking.
C. The employee used steganography to hide information in the picture attachments.
D. By using the pictures to hide information, the employee utilized picture fuzzing.

Correct Answer: C

QUESTION 13

You run nmap port Scan on 10.0.0.5 and attempt to gain banner/server information from services running on ports 21, 110 and 123. Here is the output of your scan results:

```
PORT        STATE       SERVICE     VERSION
21/tcp      open        ftp         vsftpd 2.0.7
110/tcp     open        pop3        Courier pop3d
123/tcp     closed      ntp

Device type: general purpose
Running: Linux 2.8.X

OS details: Linux 2.8.18, Linux 2.8.20 - 2.8.24
Uptime: 65.658 days (since Mon Jun 19 00:43:29 2011)
Network Distance: 0 hops
Service Info: OS: Unix
```

Which of the following nmap command did you run?

A. nmap -A -sV -p21,110,123 10.0.0.5
B. nmap -F -sV -p21,110,123 10.0.0.5
C. nmap -O -sV -p21,110,123 10.0.0.5
D. nmap -T -sV -p21,110,123 10.0.0.5

Correct Answer: C

QUESTION 14

How do you defend against Privilege Escalation?

A. Use encryption to protect sensitive data.
B. Restrict the interactive logon privileges.
C. Run services as unprivileged accounts.

D. Allow security settings of IE to zero or Low.
E. Run users and applications on the least privileges.

Correct Answer: ABCE

QUESTION 15
What does ICMP (type 11, code 0) denote?

A. Source Quench
B. Destination Unreachable
C. Time Exceeded
D. Unknown Type

Correct Answer: C

QUESTION 16
You are the security administrator of Jaco Banking Systems located in Boston. You are setting up e-banking website (http://www.ejacobank.com) authentication system. Instead of issuing banking customer with a single password, you give them a printed list of 100 unique passwords. Each time the customer needs to log into the e-banking system website, the customer enters the next password on the list. If someone sees them type the password using shoulder surfing, MiTM or keyloggers, then no damage is done because the password will not be accepted a second time. Once the list of 100 passwords is almost finished, the system automatically sends out a new password list by encrypted e-mail to the customer. You are confident that this security implementation will protect the customer from password abuse. Two months later, a group of hackers called "HackJihad" found a way to access the one-time password list issued to customers of Jaco Banking Systems. The hackers set up a fake website (http://www.e-jacobank.com) and used phishing attacks to direct ignorant customers to it. The fake website asked users for their e-banking username and password, and the next unused entry from their one-time password sheet. The hackers collected 200 customer's username/passwords this way. They transferred money from the customer's bank account to various offshore accounts. Your decision of password policy implementation has cost the bank with USD 925, 000 to hackers. You immediately shut down the e-banking website while figuring out the next best security solution. What effective security solution will you recommend in this case?

A. Implement Biometrics based password authentication system. Record the customers face image to the authentication database.
B. Configure your firewall to block logon attempts of more than three wrong tries.
C. Enable a complex password policy of 20 characters and ask the user to change the password immediately after they logon and do not store password histories.
D. Implement RSA SecureID based authentication system.

Correct Answer: D

QUESTION 17

More sophisticated IDSs look for common shellcode signatures. But even these systems can be bypassed, by using polymorphic shellcode. This is a technique common among virus writers. It basically hides the true nature of the shellcode in different disguises. How does a polymorphic shellcode work?

A. They encrypt the shellcode by XORing values over the shellcode,using loader code to decrypt the shellcode,and then executing the decrypted shellcode.
B. They convert the shellcode into Unicode,using loader to convert back to machine code then executing them.
C. They reverse the working instructions into opposite order by masking the IDS signatures.
D. They compress shellcode into normal instructions,uncompress the shellcode using loader code and then executing the shellcode.

Correct Answer: A

QUESTION 18

SYN Flood is a DOS attack in which an attacker deliberately violates the three-way handshake and opens a large number of half-open TCP connections. The signature of attack for SYN Flood contains:

A. The source and destination address having the same value.
B. A large number of SYN packets appearing on a network without the corresponding reply packets.
C. The source and destination port numbers having the same value.
D. A large number of SYN packets appearing on a network with the corresponding reply packets.

Correct Answer: B

QUESTION 19

Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?

A. Port Scanning
B. Single Scanning
C. External Scanning
D. Vulnerability Scanning

Correct Answer: D

QUESTION 20

The following script shows a simple SQL injection. The script builds an SQL query by concatenating hard-coded strings together with a string entered by the user:

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

The user is prompted to enter the name of a city on a Web form. If she enters Chicago, the query assembled by the script looks similar to the following:

SELECT * FROM OrdersTable WHERE ShipCity = 'Chicago'

How will you delete the OrdersTable from the database using SQL Injection?

A. Chicago'; drop table OrdersTable --
B. Delete table'blah'; OrdersTable --
C. EXEC; SELECT * OrdersTable > DROP --
D. cmdshell'; 'del c:\sql\mydb\OrdersTable' //

Correct Answer: A

QUESTION 21

What are the limitations of Vulnerability scanners? (Select 2 answers)

A. There are often better at detecting well-known vulnerabilities than more esoteric ones.
B. The scanning speed of their scanners are extremely high.
C. It is impossible for any, one scanning product to incorporate all known vulnerabilities in a timely manner.
D. The more vulnerabilities detected, the more tests required.
E. They are highly expensive and require per host scan license.

Correct Answer: AC

QUESTION 22

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website http://www.jeansclothesman.com. He tries random URLs on the company's website and