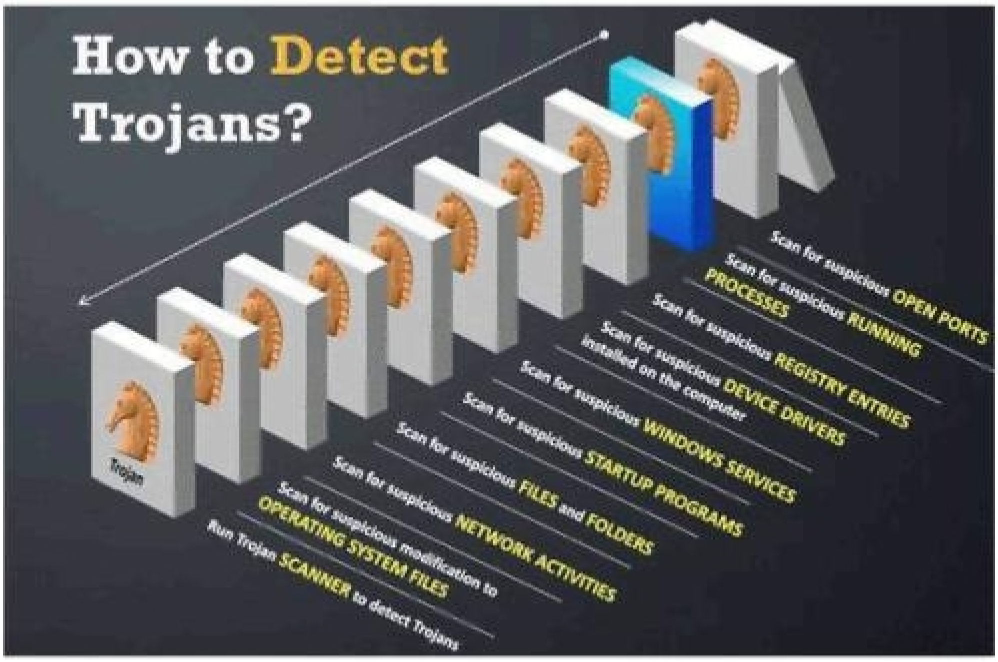

How to Detect Trojans?
Trojan
Scan for suspicious OPEN PORTS
Scan for suspicious RUNNING PROCESSES
Scan for suspicious REGISTRY ENTRIES
Scan for suspicious DEVICE DRIVERS installed on the computer
Scan for suspicious WINDOWS SERVICES
Scan for suspicious STARTUP PROGRAMS
Scan for suspicious FILES and FOLDERS
Scan for suspicious NETWORK ACTIVITIES
Scan for suspicious modification to OPERATING SYSTEM FILES
Run Trojan SCANNER to detect Trojans

A. Scan for suspicious startup programs using msconfig.
B. Scan for suspicious network activities using Wireshark.
C. Scan for suspicious device drivers in c:\windows\system32\drivers.
D. Scan for suspicious open ports using netstat.

Correct Answer: C

QUESTION 53

Which type of hacker represents the highest risk to your network?

A. black hat hackers
B. grey hat hackers
C. disgruntled employees
D. script kiddies

Correct Answer: C

QUESTION 54

Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security. No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices. What type of insider threat would Shayla be considered?

A. She would be considered an Insider Affiliate.
B. Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate.
C. Shayla is an Insider Associate since she has befriended an actual employee.
D. Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider.

Correct Answer: A

QUESTION 55
What port number is used by Kerberos protocol?

A. 88
B. 44
C. 487
D. 419

Correct Answer: A

QUESTION 56
What does FIN in TCP flag define?

A. Used to abort a TCP connection abruptly.
B. Used to close a TCP connection.
C. Used to acknowledge receipt of a previous packet or transmission.
D. Used to indicate the beginning of a TCP connection.

Correct Answer: B

QUESTION 57
Annie has just succeeded in stealing a secure cookie via a XSS attack. She is able to replay the cookie even while the session is invalid on the server. Why do you think this is possible?

A. It works because encryption is performed at the application layer (single encryption key).
B. The scenario is invalid as a secure cookie cannot be replayed.
C. It works because encryption is performed at the network layer (layer 1 encryption).
D. Any cookie can be replayed irrespective of the session status.

Correct Answer: A

QUESTION 58

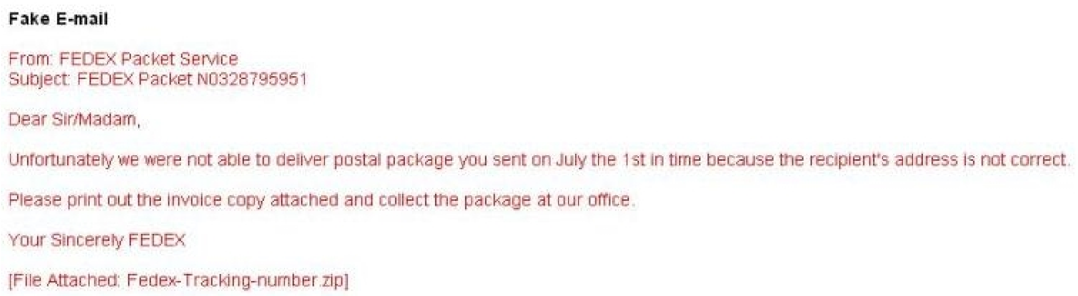
This attack technique is used when a Web application is vulnerable to an SQL Injection but the results of the Injection are not visible to the attacker.

A. Unique SQL Injection
B. Blind SQL Injection
C. Generic SQL Injection
D. Double SQL Injection

Correct Answer: B

QUESTION 59

A common technique for luring e-mail users into opening virus-launching attachments is to send messages that would appear to be relevant or important to many of their potential recipients. One way of accomplishing this feat is to make the virus-carrying messages appear to come from some type of business entity retailing sites, UPS, FEDEX, CITIBANK or a major provider of a common service. Here is a fraudulent e-mail claiming to be from FedEx regarding a package that could not be delivered. This mail asks the receiver to open an attachment in order to obtain the FEDEX tracking number for picking up the package. The attachment contained in this type of e-mail activates a virus.



Fake E-mail

From: FEDEX Packet Service
Subject: FEDEX Packet N0328795951

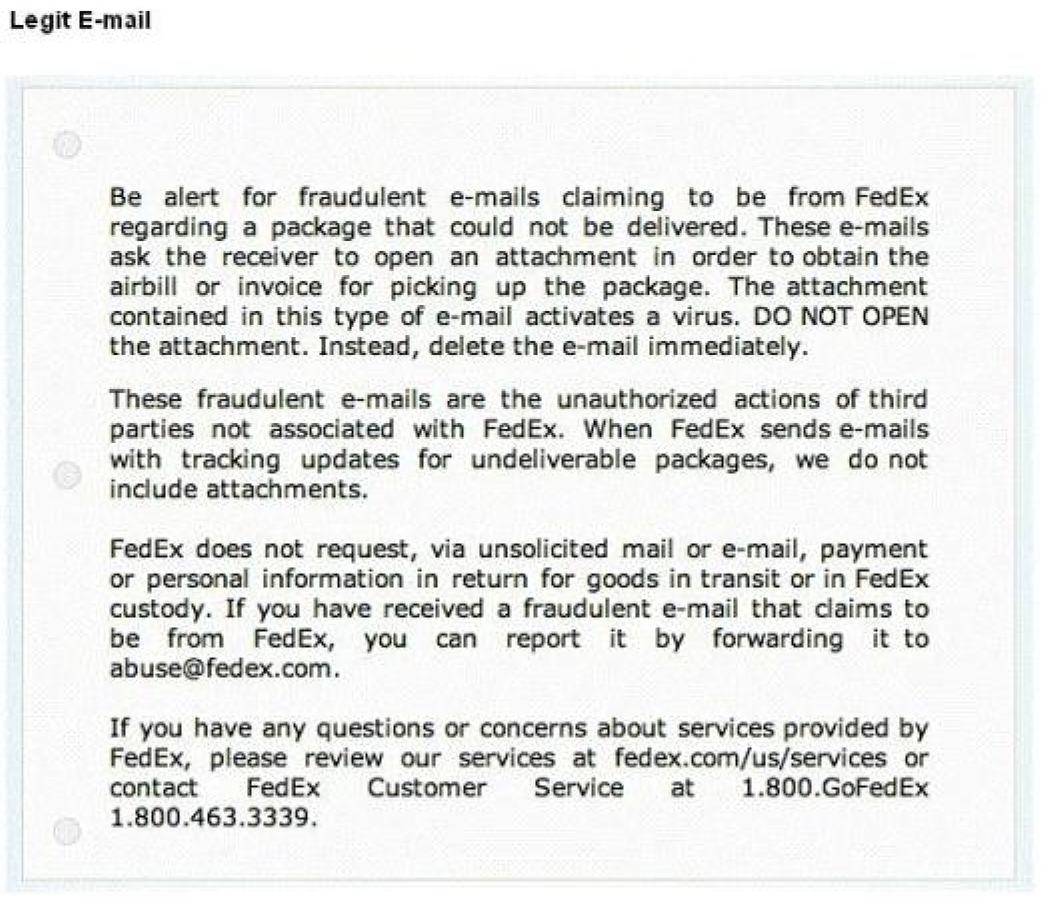
Dear Sir/Madam,

Unfortunately we were not able to deliver postal package you sent on July the 1st in time because the recipient's address is not correct.

Please print out the invoice copy attached and collect the package at our office.

Your Sincerely FEDEX

[File Attached: Fedex-Tracking-number.zip]



Legit E-mail

○

Be alert for fraudulent e-mails claiming to be from FedEx regarding a package that could not be delivered. These e-mails ask the receiver to open an attachment in order to obtain the airbill or invoice for picking up the package. The attachment contained in this type of e-mail activates a virus. DO NOT OPEN the attachment. Instead, delete the e-mail immediately.

These fraudulent e-mails are the unauthorized actions of third parties not associated with FedEx. When FedEx sends e-mails with tracking updates for undeliverable packages, we do not include attachments.

○

FedEx does not request, via unsolicited mail or e-mail, payment or personal information in return for goods in transit or in FedEx custody. If you have received a fraudulent e-mail that claims to be from FedEx, you can report it by forwarding it to abuse@fedex.com.

If you have any questions or concerns about services provided by FedEx, please review our services at fedex.com/us/services or contact FedEx Customer Service at 1.800.GoFedEx 1.800.463.3339.

○

Vendors send e-mails like this to their customers advising them not to open any files attached with the mail, as they do not include attachments. Fraudulent e-mail and legit e-mail that arrives in your inbox contain the fedex.com as the sender of the mail. How do you ensure if the e-mail is authentic and sent from fedex.com?

A. Verify the digital signature attached with the mail, the fake mail will not have Digital ID at all.
B. Check the Sender ID against the National Spam Database (NSD).
C. Fake mail will have spelling/grammatical errors.
D. Fake mail uses extensive images, animation and flash content.

Correct Answer: A

QUESTION 60

What file system vulnerability does the following command take advantage of?

```
type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.exe
```

A. HFS
B. Backdoor access
C. XFS

D. ADS

Correct Answer: D

QUESTION 61

You are the Security Administrator of Xtrinity, Inc. You write security policies and conduct assessments to protect the company's network. During one of your periodic checks to see how well policy is being observed by the employees, you discover an employee has attached cell phone 3G modem to his telephone line and workstation. He has used this cell phone 3G modem to dial in to his workstation, thereby bypassing your firewall. A security breach has occurred as a direct result of this activity. The employee explains that he used the modem because he had to download software for a department project. How would you resolve this situation?

A. Reconfigure the firewall
B. Enforce the corporate security policy
C. Install a network-based IDS
D. Conduct a needs analysis

Correct Answer: B

QUESTION 62

In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design
B. Elimination
C. Incorporation
D. Replication
E. Launch
F. Detection

Correct Answer: E

QUESTION 63

What is a sniffing performed on a switched network called?

A. Spoofed sniffing
B. Passive sniffing
C. Direct sniffing
D. Active sniffing