C. g++ -i hackersExploit.pl -o calc.exe
D. g++ --compile -i hackersExploit.cpp -o calc.exe

Correct Answer: A

QUESTION 310
A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.
B. Create a document that will crash the computer when opened and send it to friends.
C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Correct Answer: D

QUESTION 311
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Correct Answer: B

QUESTION 312
The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?
A. Investigate based on the maintenance schedule of the affected systems.
B. Investigate based on the service level agreements of the systems.
C. Investigate based on the potential effect of the incident.
D. Investigate based on the order that the alerts arrived in.

Correct Answer: C

QUESTION 313

A corporation hired an ethical hacker to test if it is possible to obtain users' login credentials using methods other than social engineering. Access to offices and to a network node is granted. Results from server scanning indicate all are adequately patched and physical access is denied, thus, administrators have access only through Remote Desktop. Which technique could be used to obtain login credentials?

A. Capture every users' traffic with Ettercap.
B. Capture LANMAN Hashes and crack them with LC6.
C. Guess passwords using Medusa or Hydra against a network service.
D. Capture administrators RDP traffic and decode it with Cain and Abel.

Correct Answer: D

QUESTION 314

Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

A. Microsoft Security Baseline Analyzer
B. Retina
C. Core Impact
D. Microsoft Baseline Security Analyzer

Correct Answer: D

QUESTION 315

Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Correct Answer: D

QUESTION 316

Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date.
B. Username and Password.

C. Digital Certificate and Hardware Token.
D. Fingerprint and Smartcard ID.

Correct Answer: D

QUESTION 317
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Correct Answer: B

QUESTION 318
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed.
Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
80/tcp open http
139/tcp open netbios-ssn
515/tcp open
631/tcp open ipp
9100/tcp open
MAC Address: 00:00:48:0D:EE:89

A. The host is likely a Windows machine.
B. The host is likely a Linux machine.
C. The host is likely a router.
D. The host is likely a printer.

Correct Answer: D

QUESTION 319

What is the outcome of the comm”nc -I -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Correct Answer: B

QUESTION 320

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Correct Answer: D

QUESTION 321

Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing
B. Social engineering
C. Vulnerability scanning
D. Access control list reviews

Correct Answer: A

QUESTION 322
When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap
B. Layer 3 switch
C. Network bridge
D. Application firewall

Correct Answer: A

QUESTION 323
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Correct Answer: A

QUESTION 324
Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

Correct Answer: C

QUESTION 325
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected