QUESTION 201

To see how some of the hosts on your network react, Winston sends out SYN packets to an IP range. A number of IPs respond with a SYN/ACK response. Before the connection is established he sends RST packets to those hosts to stop the session. Winston has done this to see how his intrusion detection system will log the traffic. What type of scan is Winston attempting here?

A. Winston is attempting to find live hosts on your company's network by using an XMAS scan.
B. He is utilizing a SYN scan to find live hosts that are listening on your network.
C. This type of scan he is using is called a NULL scan.
D. He is using a half-open scan to find live hosts on your network.

Correct Answer: D

QUESTION 202

John runs a Web server, IDS and firewall on his network. Recently his Web server has been under constant hacking attacks. He looks up the IDS log files and sees no intrusion attempts but the Web server constantly locks up and needs rebooting due to various brute force and buffer overflow attacks but still the IDS alerts no intrusion whatsoever. John becomes suspicious and views the Firewall logs and he notices huge SSL connections constantly hitting his Web server. Hackers have been using the encrypted HTTPS protocol to send exploits to the Web server and that was the reason the IDS did not detect the intrusions. How would John protect his network from these types of attacks?

A. Install a proxy server and terminate SSL at the proxy.
B. Enable the IDS to filter encrypted HTTPS traffic.
C. Install a hardware SSL "accelerator" and terminate SSL at this layer.
D. Enable the Firewall to filter encrypted HTTPS traffic.

Correct Answer: AC

QUESTION 203

Jane wishes to forward X-Windows traffic to a remote host as well as POP3 traffic. She is worried that adversaries might be monitoring the communication link and could inspect captured traffic. She would like to tunnel the information to the remote end but does not have VPN capabilities to do so. Which of the following tools can she use to protect the link?

A. MD5
B. PGP
C. RSA
D. SSH

Correct Answer: D

QUESTION 204

NTP allows you to set the clocks on your systems very accurately, to within 100ms and sometimes-even 10ms. Knowing the exact time is extremely important for enterprise security. Various security protocols depend on an accurate source of time information in order to prevent "playback" attacks. These protocols tag their communications with the current time, to prevent attackers from replaying the same communications, e.g., a login/password interaction or even an entire communication, at a later date. One can circumvent this tagging, if the clock can be set back to the time the communication was recorded. An attacker attempts to try corrupting the clocks on devices on your network. You run Wireshark to detect the NTP traffic to see if there are any irregularities on the network. What port number you should enable in Wireshark display filter to view NTP packets?

A. TCP Port 124
B. UDP Port 125
C. UDP Port 123
D. TCP Port 126

Correct Answer: C

QUESTION 205

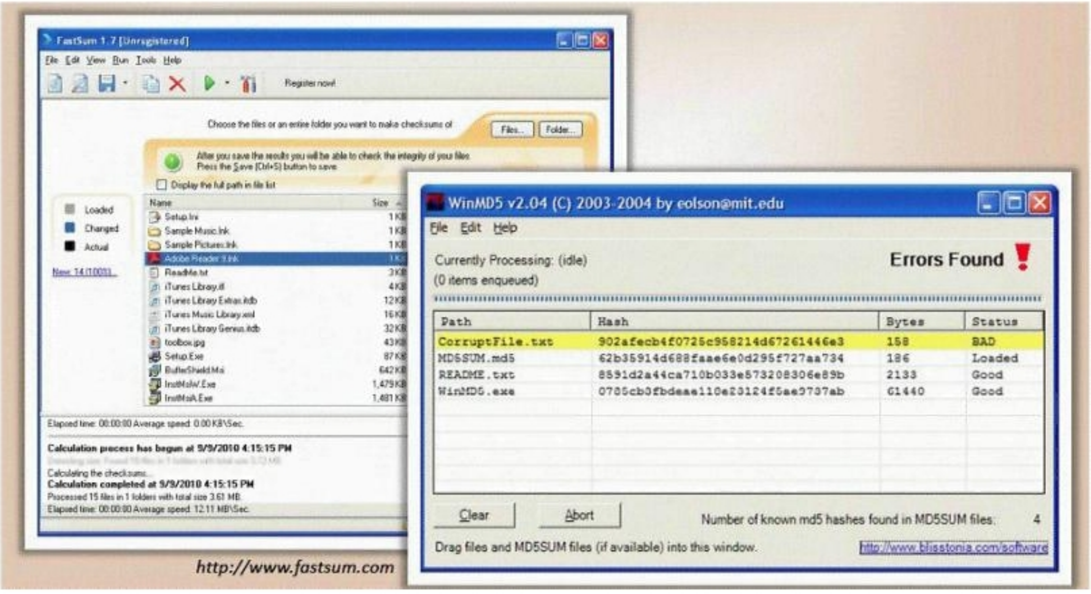
Bill is a security analyst for his company. All the switches used in the company's office are Cisco switches. Bill wants to make sure all switches are safe from ARP poisoning. How can Bill accomplish this?

A. Bill can use the command: ip dhcp snooping.
B. Bill can use the command: no ip snoop.
C. Bill could use the command: ip arp no flood.
D. He could use the command: ip arp no snoop.

Correct Answer: A

QUESTION 206

You generate MD5 128-bit hash on all files and folders on your computer to keep a baseline check for security reasons. What is the length of the MD5 hash?


FastSum 1.7 [Unregistered]
File Edit View Run Tools Help
Register now!
Files...
Folder...
Loaded
Changed
Actual
New: 14 (100%)
WinMD5 v2.04 (C) 2003-2004 by eolson@mit.edu
File Edit Help
Clear
Abort
http://www.blisstonia.com/software
http://www.fastsum.com

Choose the files or an entire folder you want to make checksums of

After you save the results you will be able to check the integrity of your files
Press the Save (Ctrl+S) button to save

☐ Display the full path in file list

Name	Size
Setup.lnk	1 KB
Sample Music.lnk	1 KB
Sample Pictures.lnk	1 KB
Adobe Reader 9.lnk	1 KB
ReadMe.txt	3 KB
iTunes Library.itl	4 KB
iTunes Library Extras.itdb	12 KB
iTunes Music Library.xml	16 KB
iTunes Library Genius.itdb	32 KB
toolbox.jpg	43 KB
Setup.Exe	87 KB
BulletShield.Msi	642 KB
InstMsiW.Exe	1,479 KB
InstMsiA.Exe	1,481 KB

Elapsed time: 00:00:00 Average speed: 0.00 KB\Sec.

Calculation process has begun at 9/9/2010 4:15:15 PM
Calculating the checksums...
Calculation completed at 9/9/2010 4:15:15 PM
Processed 15 files in 1 folders with total size 3.61 MB
Elapsed time: 00:00:00 Average speed: 12.11 MB\Sec.

Currently Processing: (idle)
(0 items enqueued)

Errors Found !

Path	Hash	Bytes	Status
CorruptFile.txt	902afecb4f0725c958214d67261446e3	158	BAD
MD5SUM.md5	62b35914d688faae6e0d295f727aa734	186	Loaded
README.txt	8591d2a44ca710b033e573208306e89b	2133	Good
WinMD5.exe	0785cb3fbdeae110e23124f5ae9737ab	61440	Good

Number of known md5 hashes found in MD5SUM files: 4

Drag files and MD5SUM files (if available) into this window.

A. 32 character
B. 64 byte
C. 48 char
D. 128 kb

Correct Answer: A

QUESTION 207

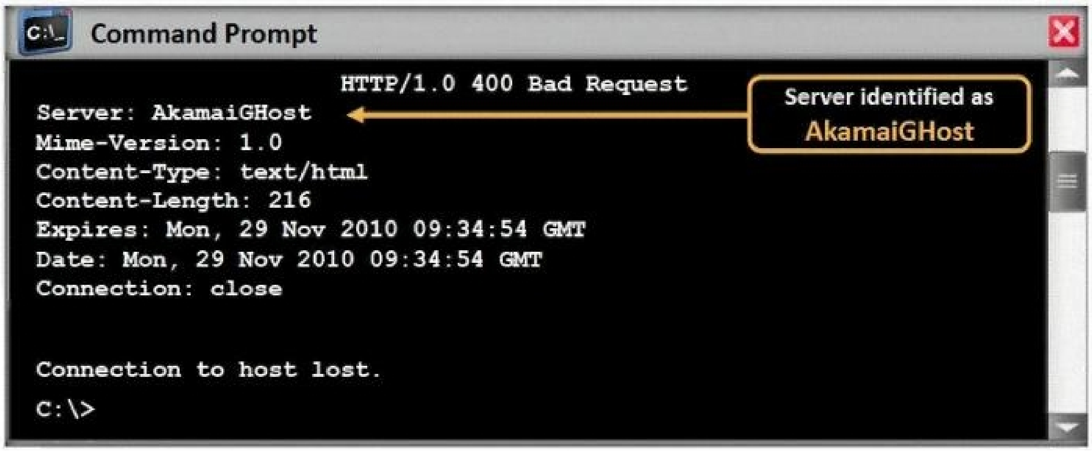
Which type of password cracking technique works like dictionary attack but adds some numbers and symbols to the words from the dictionary and tries to crack the password?

A. Dictionary attack
B. Brute forcing attack
C. Hybrid attack
D. Syllable attack
E. Rule-based attack

Correct Answer: C

QUESTION 208

What command would you type to OS fingerprint a server using the command line?

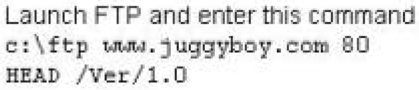


```
                    HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 216
Expires: Mon, 29 Nov 2010 09:34:54 GMT
Date: Mon, 29 Nov 2010 09:34:54 GMT
Connection: close


Connection to host lost.
C:\>
```

Server identified as AkamaiGHost

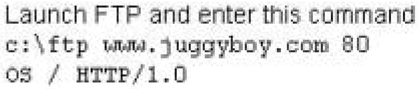
A.



Launch FTP and enter this command

```
c:\ftp www.juggyboy.com 80
HEAD /Ver/1.0
```

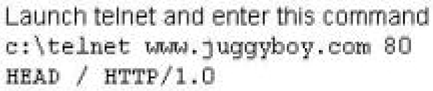
B.



Launch FTP and enter this command

```
c:\ftp www.juggyboy.com 80
OS / HTTP/1.0
```

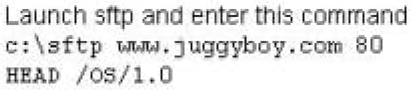
C.



Launch telnet and enter this command

```
c:\telnet www.juggyboy.com 80
HEAD / HTTP/1.0
```

D.



Launch sftp and enter this command

```
c:\sftp www.juggyboy.com 80
HEAD /OS/1.0
```

Correct Answer: C

QUESTION 209

What do you call a pre-computed hash?

A. Sun tables

B. Apple tables

C. Rainbow tables

D. Moon tables

Correct Answer: C

QUESTION 210

Why attackers use proxy servers?

A. To ensure the exploits used in the attacks always flip reverse vectors.

B. Faster bandwidth performance and increase in attack speed.

C. Interrupt the remote victim's network traffic and reroute the packets to attackers machine.

D. To hide the source IP address so that an attacker can hack without any legal corollary.

Correct Answer: D

QUESTION 211

The SNMP Read-Only Community String is like a password. The string is sent along with each SNMP Get-Request and allows (or denies) access to a device. Most network vendors ship their equipment with a default password of "public". This is the so-called "default public community string". How would you keep intruders from getting sensitive information regarding the network devices using SNMP? (Select 2 answers)

A. Enable SNMPv3 which encrypts username/password authentication.

B. Use your company name as the public community string replacing the default 'public'.

C. Enable IP filtering to limit access to SNMP device.

D. The default configuration provided by device vendors is highly secure and you don't need to change anything.

Correct Answer: AC

QUESTION 212

You are writing security policy that hardens and prevents Footprinting attempt by Hackers. Which of the following countermeasures will NOT be effective against this attack?

A. Configure routers to restrict the responses to Footprinting requests.

B. Configure Web Servers to avoid information leakage and disable unwanted protocols.

C. Lock the ports with suitable Firewall configuration.

D. Use an IDS that can be configured to refuse suspicious traffic and pick up Footprinting patterns.

E. Evaluate the information before publishing it on the Website/Intranet.

F. Monitor every employee computer with Spy cameras, keyloggers and spy on them.

G. Perform Footprinting techniques and remove any sensitive information found on DMZ sites.

H. Prevent search engines from caching a Webpage and use anonymous registration services.

I. Disable directory and use split-DNS.

Correct Answer: F