412-79$^{\text{Q\&As}}$

EC-Council Certified Security Analyst (ECSA)

Pass EC-COUNCIL 412-79 Exam with 100% Guarantee

QUESTION 1

To preserve digital evidence, an investigator should ____________________

A. Make tow copies of each evidence item using a single imaging tool

B. Make a single copy of each evidence item using an approved imaging tool

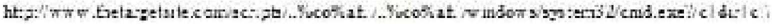
C. Make two copies of each evidence item using different imaging tools

D. Only store the original evidence item

Correct Answer: C

QUESTION 2

What will the following URL produce in an unpatched IIS Web Server?



http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Execute a buffer flow in the C: drive of the web server

B. Insert a Trojan horse into the C: drive of the web server

C. Directory listing of the C:\windows\system32 folder on the web server

D. Directory listing of C: drive on the web server

Correct Answer: D

QUESTION 3

Study the log given below and answer the following question: Apr 24 14:46:46 [4663]: spp_portscan:

portscan detected from 194.222.156.169 Apr 24 14:46:46 [4663]: IDS27/FIN Scan:

194.222.156.169:56693 -> 172.16.1.107:482 Apr 24 18:01:05 [4663]: IDS/DNS-version-query:

212.244.97.121:3485 -> 172.16.1.107:53 Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval:

194.222.156.169:1425 -> 172.16.1.107:21 Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53 Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53 Apr 25 02:08:07

[5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53 Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111 Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard:

198.173.35.164:4221 -> 172.16.1.107:80 Apr 26

05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53 Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53 Apr 26 06:44:25 victim7 PAM_pwdb [12509]: (login) session opened for

user simple by (uid=0) Apr 26 06:44:36 victim7 PAM_pwdb[12521]:

(su) session opened for user simon by simple(uid=506) Apr 26 06:45:34 [6283]: IDS175/socks-probe:

24.112.167.35:20 -> 172.16.1.107:1080 Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect:

172.16.1.107:23

-> 213.28.22.189:4558 Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A.

Disallow UDP53 in from outside to DNS server

B.

Allow UDP53 in from DNS server to outside

C.

Disallow TCP53 in from secondaries or ISP server to DNS server

D.

Block all UDP traffic

Correct Answer: A

QUESTION 4

The newer Macintosh Operating System is based on:

A. OS/2

B. BSD Unix

C. Linux

D. Microsoft Windows

Correct Answer: B

QUESTION 5

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall

B. Packet filtering firewall

C. Application-level proxy firewall

D. Statefull firewall

Correct Answer: D