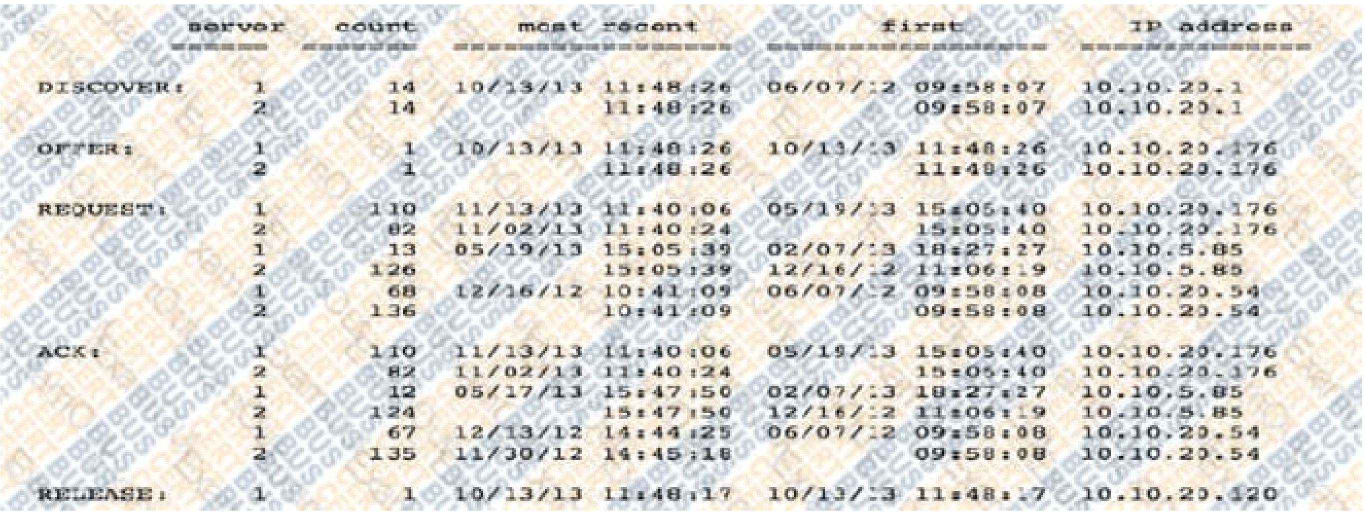
GCCC$^{Q\&As}$

GCCC - GIAC Critical Controls Certification (GCCC)

QUESTION 1

DHCP logging output in the screenshot would be used for which of the following?



```
                server     count       most recent            first              IP address
                ======    =======   ==================   ==================   ===============

DISCOVER:         1         14      10/13/13 11:48:26    06/07/12 09:58:07    10.10.20.1
                  2         14               11:48:26             09:58:07    10.10.20.1

OFFER:            1          1      10/13/13 11:48:26    10/13/13 11:48:26    10.10.20.176
                  2          1               11:48:26             11:48:26    10.10.20.176

REQUEST:          1        110      11/13/13 11:40:06    05/19/13 15:05:40    10.10.20.176
                  2         82      11/02/13 11:40:24             15:05:40    10.10.20.176
                  1         13      05/19/13 15:05:39    02/07/13 18:27:27    10.10.5.85
                  2        126               15:05:39    12/16/12 11:06:19    10.10.5.85
                  1         68      12/16/12 10:41:09    06/07/12 09:58:08    10.10.20.54
                  2        136               10:41:09             09:58:08    10.10.20.54

ACK:              1        110      11/13/13 11:40:06    05/19/13 15:05:40    10.10.20.176
                  2         82      11/02/13 11:40:24             15:05:40    10.10.20.176
                  1         12      05/17/13 15:47:50    02/07/13 18:27:27    10.10.5.85
                  2        124               15:47:50    12/16/12 11:06:19    10.10.5.85
                  1         67      12/13/12 14:44:25    06/07/12 09:58:08    10.10.20.54
                  2        135      11/30/12 14:45:18             09:58:08    10.10.20.54

RELEASE:          1          1      10/13/13 11:48:17    10/13/13 11:48:17    10.10.20.120
```

A. Enforcing port-based network access control to prevent unauthorized devices on the network.

B. Identifying new connections to maintain an up-to-date inventory of devices on the network.

C. Detecting malicious activity by compromised or unauthorized devices on the network.

D. Providing ping sweep results to identify live network hosts for vulnerability scanning.

Correct Answer: B

QUESTION 2

Which approach is recommended by the CIS Controls for performing penetration tests?

A. Document a single vulnerability per system

B. Utilize a single attack vector at a time

C. Complete intrusive tests on test systems

D. Execute all tests during network maintenance windows

Correct Answer: C

QUESTION 3

Which of the following items would be used reactively for incident response?

A. A schedule for creating and storing backup

B. A phone tree used to contact necessary personnel

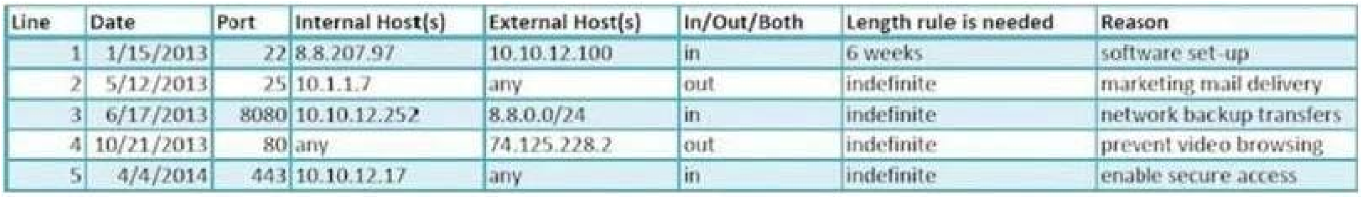
C. A script used to verify patches are installed on systems

D. An IPS rule that prevents web access from international locations

Correct Answer: B

QUESTION 4

Dragonfly Industries requires firewall rules to go through a change management system before they are configured. Review the change management log. Which of the following lines in your firewall ruleset has expired and should be removed from the configuration?



Line	Date	Port	Internal Host(s)	External Host(s)	In/Out/Both	Length rule is needed	Reason
1	1/15/2013	22	8.8.207.97	10.10.12.100	in	6 weeks	software set-up
2	5/12/2013	25	10.1.1.7	any	out	indefinite	marketing mail delivery
3	6/17/2013	8080	10.10.12.252	8.8.0.0/24	in	indefinite	network backup transfers
4	10/21/2013	80	any	74.125.228.2	out	indefinite	prevent video browsing
5	4/4/2014	443	10.10.12.17	any	in	indefinite	enable secure access

A. access-list outbound permit tcp host 10.1.1.7 any eq smtp

B. access-list outbound deny tcp any host 74.125.228.2 eq www

C. access-list inbound permit tcp 8.8.0.0 0.0.0.255 10.10.12.252 eq 8080

D. access-list inbound permit tcp host 8.8.207.97 host 10.10.12.100 eq ssh

Correct Answer: D

QUESTION 5

John is implementing a commercial backup solution for his organization. Which of the following steps should be on the configuration checklist?

A. Enable encryption if it \\'s not enabled by default

B. Disable software-level encryption to increase speed of transfer

C. Develop a unique encryption scheme

Correct Answer: A

GCCC VCE Dumps   GCCC Practice Test   GCCC Braindumps