

Expert Reference Series of IT Security White Papers

CEH Practice Exam

www.thesolutionfirm.com

CEH PRACTICE EXAM

Alice Perales

Here are a few questions for those of you that are preparing for the CEH exam.

1. If you receive a RST packet while doing an ACK scan it indicates that the port is OPEN?
 - a. TRUE
 - b. FALSE

2. How would someone determine if an LM hash from a password had less than 8 characters?
 - a. The has value always starts with MGD3B
 - b. The leftmost portion of the Hash is always the same
 - c. The rightmost portion of the Hash is always the same
 - d. Because it is a hash it cannot be reversed

3. If you receive an ICMP packet while doing an ACK scan it indicates that the port is CLOSED?
 - a. TRUE
 - b. FALSE

4. In the context of password, what is a brute force attack?
 - a. You blackmail someone to make them give up their password
 - b. You create hashes of a large number of words and compare it with the encrypted password value
 - c. You try every single possibility
 - d. You wait until the password expires

5. Which type of NMAP port scan is considered stealthy?
 - a. -sT
 - b. -sU
 - c. -s0
 - d. -sS

6. During a recent test NMAP has not been able to identify a remote OS and did not give you any results, what else could you do to identify the OS?
 - a. Attempt to grab service banners on the host
 - b. Attempt to perform a XProbe2 scan
 - c. Attempt to perform a Traceroute using different protocols
 - d. Attempt to do a TDP scan of the remote host
 - e. Attempt to do a Reverse Scan

7. Which of the following represents the RID of the Microsoft XP administrator?
 - a. S-1-5-21-343818398-789336058-1343024091-1000 administrator
 - b. S-1-5-21-343818398-789336058-1343024091-501 guest
 - c. S-1-5-21-343818398-789336058-1343024091-500 jack
 - d. S-1-5-21-343818398-789336058-1343024091-1010 contractor

8. Which of the following is a good example of passive fingerprinting?

- a. Nmap Scan
- b. Traceroute
- c. EDGAR search
- d. Host Scanning

9. Why is it that an IDS system dislikes a large quantity of small fragmented packets?

- a. It must buffer the traffic, therefore it slows communication.
- b. It has to rebuild the stream to make sense of the message or communication.
- c. This process requires the intervention of an employee to make a go / no go decision
- d. It must pass the traffic without inspection

10. What ports would you block on your firewall to ensure that NetBIOS traffic is NOT coming through the firewall if you have a mixed Windows NT, 2000, and 2003 environment?
(Choose all that apply)

- a. 21
- b. 25
- c. 53
- d. 110
- e. 111
- f. 135
- g. 139
- h. 389
- h. 445
- i. 1024
- j. 1434

11. Your assessment team is conducting a pen test against a company's internal website. One of the team members received the following errors while reviewing the site: *Microsoft OLE DB Provider for ODBC Drivers error "80040e14."* What does this mean?

- a. The site is vulnerable to the Unicode exploit.
- b. The site is vulnerable to SQL injection.
- c. The team member has attempted to access the global.asa file and has caused a buffer overflow.
- d. The team member has accessed a web page that contains a web bug or error.

12. Tushar is attempting to determine the owner and location of an address he has found in his Snort logs. He has decided to use IANA.net and RIPE.net to begin his search. Can the RIPE Database be searched by domain name?

- a. Yes
- b. No

END OF TEST

CEH EXAM ANSWERS

1. If you receive a RST packet while doing an ACK scan it indicates that the port is OPEN?

- a. **TRUE**
- b. FALSE

2. How would someone determine if an LM hash from a password had less than 8 characters?

- a. The has value always starts with MGD3B
- b. The leftmost portion of the Hash is always the same
- c. The rightmost portion of the Hash is always the same (i.e. 1404EE)**
- d. Because it is a hash it cannot be reversed

3. If you receive an ICMP packet while doing an ACK scan it indicates that the port is CLOSED?

- a. **TRUE**
- b. FALSE

4. In the context of password, what is a brute force attack?

- a. You blackmail someone to make them give up their password
- b. You create hashes of a large number of words and compare it with the encrypted password value
- c. You try every single possibility**
- d. You wait until the password expires

5. Which type of NMAP port scan is considered stealthy?

- a. -sT
- b. -sU
- c. -s0
- d. -sS**

6. During a recent test NMAP has not been able to identify a remote OS and did not give you any results, what else could you do to identify the OS?

- a. Attempt to grab service banners on the host**
- b. Attempt to perform an XProbe2 scan
- c. Attempt to perform a Traceroute using different protocols
- d. Attempt to do a TDP scan of the remote host
- e. Attempt to do a Reverse Scan

7. Which of the following represents the RID of the Microsoft XP administrator?

- a. S-1-5-21-343818398-789336058-1343024091-1000 administrator

- b. S-1-5-21-343818398-789336058-1343024091-501 guest
- c. S-1-5-21-343818398-789336058-1343024091-500 jack**
- d. S-1-5-21-343818398-789336058-1343024091-1010 contractor

8. Which of the following is a good example of passive fingerprinting?

- a. Nmap Scan
- b. Traceroute
- c. EDGAR search**
- d. Host Scanning

9. Why is it that an IDS system dislikes a large quantity of small fragmented packets?

- a. It must buffer the traffic, therefore it slows communication.
- b. It has to rebuild the stream to make sense of the message or communication.**
- c. This process requires the intervention of an employee to make a go / no go decision
- d. It must pass the traffic without inspection

10. What ports would you block on your firewall to ensure that NetBIOS traffic is NOT coming through the firewall if you have a mixed Windows NT, 2000, and 2003 environment?
(Choose all that apply)

- a. 21
- b. 25
- c. 53
- d. 110
- e. 111
- f. 135**
- g. 139**
- h. 389
- h. 445**
- i. 1024
- j. 1434

11. Your assessment team is conducting a pen test against a company's internal website. One of the team members received the following errors while reviewing the site: *Microsoft OLE DB Provider for ODBC Drivers error "80040e14."* What does this mean?

- a. The site is vulnerable to the Unicode exploit.
- b. The site is vulnerable to SQL injection.**
- c. The team member has attempted to access the global.asa file and has caused a buffer overflow.
- d. The team member has accessed a web page that contains a web bug or error.

12. Tushar is attempting to determine the owner and location of an address he has found in his Snort logs. He has decided to use IANA.net and RIPE.net to begin his search. Can the RIPE Database be searched by domain name?

- a. Yes
- b. No**

About the Author

Alice Perales is the Training Development Director of Superior Solutions, Inc., a security assessment and training firm.