Exam Name – Certified Professional Ethical Hacker (CPEH)™

Exam Code – CPEH-001

Sample Exam

(Question): You just noticed a member of your pen test team sending an email to an address that you know does not exist within the company for which you are contracted to perform the penetration test. Why is he doing this?

(A): To determine who is the holder of the root account
(B): To determine if the email server is vulnerable to a relay attack
(C): To test the network's IDS systems
(D): To generate a response back that will reveal information about email servers

(Correct): D

(Question): What is the range for dynamic random ports?

(A): 1024-49151
(B): 1-1024
(C): 49152-65535
(D): 0-1023

(Correct): C

(Question): You would like to perform a port scan that would allow you to determine if a stateless firewall is being used. Which of the following would be the best option?

(A): XMAS scan
(B): Idle scan
(C): Stealth scan
(D): ACK scan

(Correct): D

(Question): You have become concerned that someone could attempt to poison your DNS server. What determines how long cache poisoning would last?

(A): A record
(B): CNAME
(C): SOA
(D): MX

(Correct): C

(Question): Which of the following Trojans uses port 6666?

(A): Subseven
(B): NetBus
(C): Amitis
(D): Beast

(Correct): D

(Question): Which of the following best describes a wrapper?

(A): Wrappers are used as tunneling programs.
(B): Wrappers are used to cause a Trojan to self execute when previewed within email.
(C): Wrappers are used as backdoors to allow unauthenticated access.
(D): Wrappers are used to package covert programs with overt programs

(Correct): D

(Question): Loki uses which of the following by default?

(A): ICMP
(B): UDP 69
(C): TCP 80
(D): IGRP

(Correct): A

(Question): You have become concerned that one of your workstations might be infected with a malicious program. Which of the following netstat switches would be the best to use?

(A): netstat -an
(B): netstat -r
(C): netstat -p
(D): netstat –s

(Correct): A

(Question): You have just completed a scan of your servers, and you found port 12345 open.

Which of the following programs uses that port by default?

(A): Donald Dick
(B): Back Orifice
(C): Subseven
(D): NetBus

(Correct): D