Vendor: EC-Council

Exam Code: 312-38

Exam Name: EC-Council Network Security Administrator (ENSA)

Version: DEMO

QUESTION 1
John works as a C programmer. He develops the following C program:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str)
{
char buffer1[10];
strcpy(buffer1, str);
return 1;
}
int main(int argc, char *argv[]) {
buffer (argv[1]);
printf("Executed\n");
return 1;
}
```

His program is vulnerable to a _____ attack.

A. SQL injection
B. Denial-of-Service
C. Buffer overflow
D. Cross site scripting

Answer: C

QUESTION 2
Fill in the blank with the appropriate term. _____is the complete network configuration and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

Answer: NetRanger

QUESTION 3
Fill in the blank with the appropriate term. A _____device is used for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Answer: biometric

QUESTION 4
Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution.
Choose all that apply.

A. Wireless sniffer
B. Spectrum analyzer
C. Protocol analyzer
D. Performance Monitor

Answer: AC

QUESTION 5
Drag and drop the terms to match with their descriptions.

Terms		Description
Backdoor	Place Here	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Place Here	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Place Here	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Answer:

Terms		Description
Backdoor	Trojan horse	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

QUESTION 6
In which of the following conditions does the system enter ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.

A. The router does not have a configuration file.
B. There is a need to set operating parameters.
C. The user interrupts the boot sequence.
D. The router does not find a valid operating system image.

Answer: CD

QUESTION 7
Which of the following protocols is used for exchanging routing information between two gateways in a network of autonomous systems?

A. IGMP
B. ICMP
C. EGP
D. OSPF

Answer: C

QUESTION 8
Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?

A. Sequence Number
B. Header Length
C. Acknowledgment Number
D. Source Port Address

Answer: D

QUESTION 9
Fill in the blank with the appropriate term. _____ is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.

Answer: Network reconnaissance

QUESTION 10
Fill in the blank with the appropriate term. The _____is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions.

Answer: DCAP

QUESTION 11
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd
B. Kismet
C. AirSnort
D. Cain

Answer: C

QUESTION 12
Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?

A. Incident response
B. Incident handling
C. Incident management
D. Incident planning

Answer: A

QUESTION 13
Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?

A. Fire sprinkler
B. Fire suppression system
C. Fire alarm system
D. Gaseous fire suppression

Answer: C

QUESTION 14
Which of the following is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces?

A. IPS
B. HIDS
C. DMZ
D. NIDS

Answer: B

QUESTION 15
Which of the following types of VPN uses the Internet as its main backbone, allowing users, customers, and branch offices to access corporate network resources across various network architectures?

A. PPTP VPN
B. Remote access VPN
C. Extranet-based VPN
D. Intranet-based VPN

Answer: C

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and
VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: BDNT2014