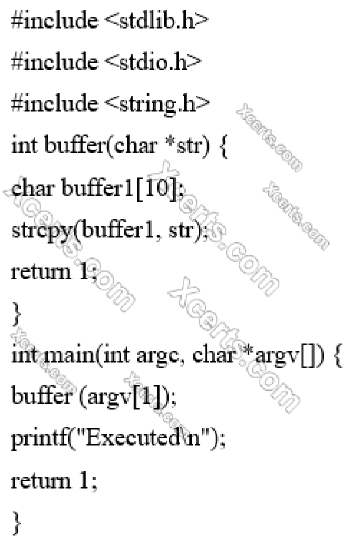
EC-Council Certified Security Analyst (ECSA)

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

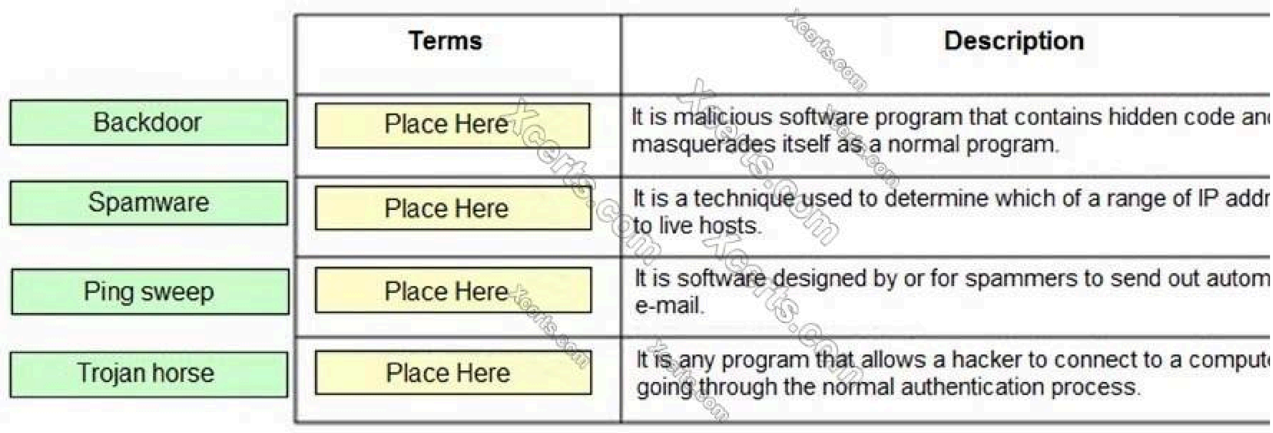
C. Buffer overflow

D. Cross site scripting

Answer(s): C

---

2. DRAG DROP (Drag and Drop is not supported)
Drag and drop the terms to match with their descriptions.
Select and Place:



	Terms	Description
Backdoor	Place Here	It is malicious software program that contains hidden code an masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addr to live hosts.
Ping sweep	Place Here	It is software designed by or for spammers to send out autom e-mail.
Trojan horse	Place Here	It is any program that allows a hacker to connect to a comput going through the normal authentication process.

A. See Explanation section for answer.

Answer(s): A

---

3. FILL BLANK
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.

A. NetRanger

Answer(s): A

---

4. FILL BLANK
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.

A. biometric

Answer(s): A

---

5. 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(s): A C

---

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(s): C D

---

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(s): C

---

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(s): D

---

9. FILL BLANK
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.

A. Network reconnaissance

Answer(s): A

---

10. FILL BLANK
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.

A. DCAP

Answer(s): A

---

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(s): C

---

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(s): A

---

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(s): C

---

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(s): B

---

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(s): C

---

16. Which of the following is a protocol that describes an approach to providing "streamlined" support of OSI application services on top of TCP/IP-based networks for some constrained environments?

A. Network News Transfer Protocol

B. Lightweight Presentation Protocol

C. Internet Relay Chat Protocol

D. Dynamic Host Configuration Protocol

Answer(s): B

---

17. You are an Administrator for a network at an investment bank. You are concerned about individuals breeching your network and being able to steal data before you can detect their presence and shut down their access. Which of the following is the best way to address this issue?

A. Implement a strong password policy.

B. Implement a strong firewall.

C. Implement a honeypot.

D. Implement network based antivirus.

Answer(s): C

---

18. Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.

☐ A. E-mail spam

☐ B. Junk mail

☐ C. Email spoofing

☐ D. Email jamming

Answer(s): A B

---

19. FILL BLANK
Fill in the blank with the appropriate word. The________________ risk analysis process analyzes the effect of a risk event deriving a numerical value.

A. quantitative

Answer(s): A

---

20. Which of the following is a tool that runs on the Windows OS and analyzes iptables log messages to detect port scans and other suspicious traffic?

A. Nmap

B. Hping

C. NetRanger

D. PSAD

Answer(s): D