Ashwin Belbase BSc. (Hons) Computer Networking & IT Security
<np01nt4a180030@islingtoncollege.edu.np>

Multiple Choice Questions

Google Forms <forms-receipts-noreply@google.com> 20 April 2021 at 09:31
To: np01nt4a180030@islingtoncollege.edu.np

Thanks for filling in Multiple Choice Questions

Here's what we've received from you:

View score

Multiple Choice Questions

Answer all questions

Your email address (**np01nt4a180030@islingtoncollege.edu.np**) was recorded when you submitted this form.

Full Name *

Ashwin Belbase

Select your Group *

N1

1. What are the basic phases of attack that can be used by a virus or worm in sequential order? *

○ paralyze, probe, penetrate, persist, and propagate

● probe, penetrate, persist, propagate, and paralyze

○ penetrate, persist, propagate, paralyze, and probe

○ persist, propagate, paralyze, probe, and penetrate

2. What occurs during a spoofing attack? *

● One device falsifies data to gain access to privileged information

○ Large amounts of network traffic are sent to a target device to make resources unavailable to intended users

○ Improperly formatted packets are forwarded to a target device to cause the target system to crash.

○ A program writes data beyond the allocated memory to enable the execution of malicious code.

3. Which phase of worm mitigation requires compartmentalization and segmentation of the network to slow down or stop the worm and prevent currently infected hosts from targeting and infecting other systems? *

● containment phase

○ inoculation phase

○ quarantine phase

○ treatment phase

4. A disgruntled employee is using Wireshark to discover administrative Telnet usernames and passwords. What type of network attack does this describe *

○ Denial of Service

○ port redirection

● reconnaissance

○ trust exploitation

5. What are three goals of a port scan attack? (Choose three.) *

□ disable used ports and services

☑ determine potential vulnerabilities

☑ identify active services

□ identify peripheral configurations

☑ identify operating systems

□ discover system passwords

6. Which two statements describe access attacks? (Choose two.) *

□ Port redirection attacks use a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.

☑ Password attacks can be implemented using brute-force attack methods, Trojan Horses, or packet sniffers.

□ Buffer overflow attacks write data beyond the allocated buffer memory to overwrite valid data or exploit systems to execute malicious code.

□ Port scanning attacks scan a range of TCP or UDP port numbers on a host to detect listening services.

☑ Trust exploitation attacks can use a laptop acting as a rogue access point to capture and copy all network traffic in a public location on a wireless hotspot

7. What are the three components of information security? (Choose three.) *

☑ availability

□ connectivity

☑ confidentiality

□ disclosure

☑ integrity

□ safety

8. Which domain of network security would contain a document that specifies the level of access that college staff have to the student records server? *

○

○ asset management

○ communication and network management

○ risk assessment

● Security policy

9. Which three areas of router security must be maintained to secure an edge router at the network perimeter? (Choose three.) *

☑ physical security

□ flash security

□ operating system security

☑ remote access security

☑ router hardening

□ zone isolation

10. What is the minimum recommended modulus key length for keys generated to use with SSH? *

○ 256

○ 512

○ 768

○ 1024

● 2048

11. Why is local database authentication preferred over a password-only login? *

○ It specifies a different password for each line or port.

● It provides for authentication and accountability.

○ It requires a login and password combination on console, vty lines, and aux ports.

○ It is more efficient for users who only need to enter a password to gain entry to a device.

12. Due to implemented security controls, a user can only access a server with FTP. Which AAA component accomplishes this? *

○ accessibility

○ accounting

○ aduiting

● authentication

○ authorization

13. What is a zero-day attack? *

○ an extortion threat directed against a bank, and demanding a huge amount of money within a short response time, typically within a day

○ a type of DoS attack that launches within 24 hours after it first infects multiple computers around the world

○ a rapid exploit attack of employee login credentials via the use of social engineering techniques

● an attack that targets software vulnerabilities unknown or unpatched by the software vendor

14. What is a disadvantage of a pattern-based detection mechanism? *

○ Its configuration is complex

○ It cannot detect unknown attacks

○ It is difficult to deploy in a large network.

● The normal network traffic pattern must be profiled first

15. What information must an IPS track in order to detect attacks matching a composite signature? *

○ the total number of packets in the attack

○

○ the attacking period used by the attacker

○ the network bandwidth consumed by all packets

● the state of packets related to the attack

16. A system analyst is configuring and tuning a recently deployed IPS appliance. By examining the IPS alarm log, the analyst notices that the IPS does not generate alarms for a few known attack packets. Which term describes the lack of alarms by the IPS? *

○ true negative

○ false positive

● false negative

○ true positive

17. A security specialist configures an IPS so that it will generate an alert when an attack is first detected. Alerts for the subsequent detection of the same attack are suppressed for a pre-defined period of time. Another alert will be generated at the end of the period indicating the number of the attack detected. Which IPS alert monitoring mechanism is configured *

○ composite alert

○ atomic alert

● summary alert

○ correlation alert

18. What are two shared characteristics of the IDS and the IPS? (Choose two.) *

☑ Both use signatures to detect malicious traffic

□ Both analyze copies of network traffic

□ Both have minimal impact on network performance

□ Both rely on an additional network device to respond to malicious traffic.

□

☑ Both are deployed as sensors

19. Which item is the great majority of software vulnerabilities that have been discovered? *

○ Stack vulnerabilities

○ Heap overflows

○ Software overflows

● Buffer overflows

20. Select four types of Layer 2 attacks? *

☑ MAC address spoofing

□ MAC address table overflows

□ LAN Tear Worm Attack

□ LAN storms

☑ VLAN attacks

21. A network administrator detects unknown sessions involving port 21 on the network. What could be causing this security breach? *

● An FTP Trojan Horse is executing

○ A reconnaissance attack is occurring

○ A denial of service attack is occurring.

○ Cisco Security Agent is testing the network.

22. Which two network security solutions can be used to mitigate DoS attacks? (Choose two.) *

□ virus scanning

□ data encryption

☑ anti-spoofing technologies

□ intrusion protection systems

☑ applying user authentication

23. Which phase of worm mitigation involves terminating the worm process, removing modified files or system settings that the worm introduced, and patching the vulnerability that the worm used to exploit the system? *

□ containment

□ inoculation

□ quarantine

☑ treatment

24. Which statement accurately characterizes the evolution of network security? *

● Internal threats can cause even greater damage than external threats

○ Internet architects planned for network security from the beginning

○ Early Internet users often engaged in activities that would harm other users.

○ Threats have become less sophisticated while the technical knowledge needed by an attacker has grown

25. An attacker is using a laptop as a rogue access point to capture all network traffic from a targeted user. Which type of attack is this? *

○ trust exploitation

○ buffer overflow

● man in the middle

○ port redirection

26. Which security organization would most likely coordinate communication between security experts in various US agencies when a security attack has been

launched? *

● CERT

○ CIS

○ (ISC)2

○ SANS

27. How would limiting the type and number of input characters on a web page help with network security? *

● It provides content filtering

○ It deters hacking

○ It protects from DoS attacks

○ It prevents open ports from being used in an improper manner

28. Which of the following is the most secure? *

○ PAP

○ CHAP

○ MS-CHAP

● MS-CHAP2

29. To protect against malicious attacks, what should you think like? *

● hacker

○ network admin

○ auditor

○ spoofer

30. Which of the following factors should you consider when evaluating assets to a company? (Select the two best answers.) *

☑ Its value to the company

□ Where they were purchased from

☑ Its replacement cost

□ Their salvage value

31. Which of the following is placed in an application by programmers either knowingly or inadvertently to bypass normal authentication? *

○ Input validation

○ Sandbox

● Backdoor

○ virus

32. NAT is also known as IP masquerading. *

● True

○ False

33. An intranet enables sister companies to access a secure area of a company's network. *

● True

○ False

34. A DMZ is a special area of the network accessed by clients on the Internet. *

● True

○ False

35. Which of the following ways can help secure a modem? (Select the two best answers.) *

☑ Use the callback feature

□ Mount the modem to the floor.

□ Use telnet

☑ use strong password

36. Your boss wants you to secure your web server's transactions. Which protocol and port number should you use to accomplish this? *

○ POP3-110

○ LDAP-389

○ RDP-3389

● HTTPS-44361

37. Which of the following is not a denial-of-service attack? *

○ Smurf attack

○ Teardrop attack

● replay attack

○ fork bomb

38. Which of the following can best be described as the exploitation of a computer session in an attempt to gain unauthorized access to data? *

○ DoS

● session hijacking

○ null session

○ domain name hiding

39. A MAC flood is when a person accesses a single port of a switch that was not physically secured. *

○ True

● False

40. Which of the following RAID versions offers the least amount of performance degration when a disk in the array fails? *

○ RAID 0

○ RAID 1

○ RAID 4

● RAID 5

41. Which of the following can facilitate a full recovery within minutes? *

○ Warm site

○ Cold site

○ Reestablishing a mirror

● Hot site

42. Which of the following tape backup methods enables daily backups, weekly full backups, and monthly full backups? *

○ Towers of Hanoi

○ Incremental

● Grandfather-father-son

○ differential

43. Of the following, what is the worst place to store a backup tape? *

○

○ Near a bundle of fiber-optic cables

● Near a power line

○ Near a server

○ Near an LCD screen

44. An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to combine the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal? *

● Unified Threat Management

○ Virtual Private Network

○ Single sign on

○ Role-based management

45. The system administrator is tasked with changing the administrator password across all 2000 computers in the organization. Which of the following should the system administrator implement to accomplish this task? *

○ A security group

● A group policy

○ Key escrow

○ Certificate revocation

Create your own Google Form
Report Abuse