注意：考試開始鈴響前，不得翻閱試題，

並不得書寫、畫記、作答。

國立清華大學 111 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

科目代碼：2501

考試科目：資訊安全

—作答注意事項—

1. 請核對答案卷（卡）上之准考證號、科目名稱是否正確。
2. 考試開始後，請於作答前先翻閱整份試題，是否有污損或試題印刷不清，得舉手請監試人員處理，但不得要求解釋題意。
3. 考生限在答案卷上標記「⬇ 由此開始作答」區內作答，且不可書寫姓名、准考證號或與作答無關之其他文字或符號。
4. 答案卷用盡不得要求加頁。
5. 答案卷可用任何書寫工具作答，惟為方便閱卷辨識，請儘量使用藍色或黑色書寫；答案卡限用 2B 鉛筆畫記；如畫記不清（含未依範例畫記）致光學閱讀機無法辨識答案者，其後果一律由考生自行負責。
6. 其他應考規則、違規處理及扣分方式，請自行詳閱准考證明上「**國立清華大學試場規則及違規處理辦法**」，無法因本試題封面作答注意事項中未列明而稱未知悉。

國立清華大學 111 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共__8__頁，第__1__頁　　*請在【答案卷、卡】作答

Part I (90%) Please select correct answers according to the question (2 points/each).

1. Which of the following web application attacks are caused by compromising a vulnerable web site and uploading malicious code or using malicious links to get a user's sensitive information?
A. CSRF attack
B. XSS attack
C. Injection attack
D. Defacing attack

2. Which of the following could make a web application vulnerable to an XSS attack? (Choose two.)
A. Weak encryption algorithm
B. Use of Flash, VBScript, or JavaScript
C. Malformed HTML requests
D. Malformed TCP segments

3. Which of the following are small files located on a host that contain session information about visited web sites?
A. Cookies
B. .html files
C. Session keys
D. Applets

4. What types of applications do local shared objects support?
A. Java applets
B. Operating system executable files
C. Microsoft Office content
D. Adobe Flash content

5. All of the following are mitigations against HTML attachment attacks, *except*:
A. Stripping e-mail attachments containing HTML files
B. Encrypting HTML attachments during transmission
C. Preventing Internet connections from HTML attachments
D. Cautioning users not to click HTML attachments

6. Manipulating ________________ is one way to embed malicious commands and directives into HTTP traffic sent back and forth between a client and web server.
A. request packets
B. response segments
C. HTTP headers
D. flash cookies

7. Which network device is used to send traffic to different physical networks, based upon logical addressing?

A. Router
B. Switch
C. Load balancer
D. Firewall

8. Which type of device is used to provide network protection and security by preventing hosts from connecting to the organization's infrastructure unless they meet certain criteria?

A. Switch
B. NAT device
C. Firewall
D. NAC device

9. You need to install a new network for a customer, and you are looking at different ways to design the perimeter network and entry points. You determine that you will need a firewall, border router, and two separate network segments off of the firewall for Internet-accessible-servers. Which one of the following architectures best describes your network design?

A. Bastion host
B. VLAN
C. DMZ
D. Subnetwork

10. Which of the following statements is true about subnetting?

A. Adding network bits to the subnet mask creates more networks but fewer hosts.
B. Adding network bits to the subnet mask creates more networks and hosts.
C. Adding host bits to the subnet masks creates more networks but fewer hosts.
D. Adding host bits to the subnet masks creates more hosts and networks.

11. All of the following characteristics describe VLANs, *except*:

A. VLANs require routing between them.
B. VLANs separate hosts into logical networks.
C. VLANs can be used to apply security policies and filtering to different segments.
D. VLANs allow any host plugged into the switch to become a member of the virtual segment.

12. Which of the following allows you to map a single public IP address to a pool of private IP addresses?

A. Virtual LAN
B. Port Address Translation
C. Network Access Control
D. Static NAT

13. One of your coworkers has recently reconfigured the firewall rule set, and users immediately began to report that they cannot receive any traffic at all from the Web. You examine the firewall rule set for issues. Which of the following could be considered a likely issue that would prevent all traffic from passing through the firewall?

A. Implicit deny
B. Explicit allow at the bottom of the rule set
C. Explicit deny at the top of the rule set
D. Implicit allow at the top of the rule set

14. Which of the following would be needed to block excessive traffic from a particular protocol?

A. Flood guard
B. Loop protection
C. ACL
D. 802.1X

15. Which of the following issues must be addressed in any remote access method or technology? (Choose two.)

A. Encryption
B. Loop protection
C. Authentication
D. Traffic flooding

16. Which one of the following terms is used for impersonating a host or user?

A. Smurf attack
B. Man-in-the-middle
C. Session hijacking
D. Spoofing

17. All of the following are characteristics of a man-in-the-middle (MITM) attack, *except*:

A. Intercepting data
B. Altering and retransmitting data
C. Spoofing both sides of the communications session
D. Flooding the network with ICMP packers

18. Intercepting a user's credentials and retransmitting them in the hopes of authenticating as a ____________ attack.

A, session hijacking
B. replay
C. man-in-the-middle
D. spoofing

19. Which of the following can be used to conduct a denial-of-service attack? (Choose all that apply.)
    A. Specially crafted traffic
    B. Malware
    C. Large amounts of traffic
    D. Man-in-the middle attacks

20. You have received reports that a user's host is very sluggish and unresponsive. After troubleshooting other items, you decide to use a sniffer to examine the network traffic coming into the host. You see that large amounts of ICMP traffic, in the form of ping replies, are being sent to the host. The host is having trouble processing all of this traffic, causing it to slow down. Which of the following is the most likely explanation for this?
    A. Faulty network card
    B. Man-in-the-middle attack
    C. Smurf attack
    D. SYN flood

21. In a SYN food attack, which of the following is a receiving host expecting back as a reply to complete the TCP three-way handshake?
    A. Repeated SYN segments
    B. A SYN/ACK segment
    C. A SYN segment
    D. An ACK segment

22. Which of the following would be considered a distributed denial-of-service attack?
    A. An attacker uses her own machine to attack another machine.
    B. An attacker uses a network of 20 malware-infected hosts to attack a web server.
    C. An attacker uses a SYN flood attack against a target's external router.
    D. An attacker uses a MITM attack against an unsuspecting rival hacker.

23. Which of the following describes a network device that intercepts user or host requests and then makes those requests to other hosts or networks on behalf of the user?
    A. Proxy
    B. Firewall
    C. NIDS
    D. NIPS

24. Which of the following is an advanced form of proxy and can also perform content filtering and web application attack prevention functions?
    A. NIPS
    B. Firewall
    C. Web security gateway
    D. NIDS

25. Which of the following types of connections does a VPN concentrator control? (Choose two.)
   A. Device VPN
   B. Client VPN
   C. User VPN
   D. Site-to-site VPN

26. A NIPS is considered a __________________ type of control.
   A. detective
   B. preventative
   C. network
   D. host

27. Which of the following types of systems detects network attacks based upon how they compare with a baseline of traffic patterns that are considered normal for the network?
   A. Pattern-based
   B. Rule-based
   C. Signature-based
   D. Behavior-based

28. Which of the following is used to intercept and examine network traffic based upon protocol
   A. Sniffer
   B. NIDS
   C. NIPS
   D. Proxy

29. Which of the following does MAC filtering use as its filtering criteria?
   A. Hardware address
   B. Software address
   C. Logical address
   D. IP address

30. You are configuring a network device. You want to be able to manage the device remotely using only the Secure Shell (SSH) protocol. If enabled by default, you should disable all of the following ports, protocols, and services, *except*:
   A. Telnet
   B. UDP port 69
   C. TCP port 22
   D. RDP

31. Which of the following techniques can be used to detect rogue or unauthorized hosts? (Choose all that apply.)
 A. DHCP address assignment logs
 B. NAC
 C. Switch port and VLAN connection logs
 D. IP address

32. Which of the following terms refers to combination of multifunction security devices?
 A. NIDS/NIPS
 B. Application firewall
 C. Web security gateway
 D. Unified Threat Management

33. Which of the following would describe an attack in which the attacker sets up a malicious access point configured almost identically to a legitimate one?
 A. Impersonation attack
 B. Evil twin attack
 C. Spoofing attack
 D. Rogue traffic attack

34. Which of the following can happen if an attacker sets the power levels on a rogue access point to overpower the wireless transmissions of a legitimate access point?
 A. Jamming
 B. Beaconing
 C. Deauthentication
 D. Spoofing

35. Which of the following older attacks involves marking attributes of wireless access points on walls or the sidewalk?
 A. AP tagging
 B. Geo-tagging
 C. Wardriving
 D. Warchalking

36. Which of the following actions may be considered illegal, depending upon where they take place? (Choose two.)
 A. Wardriving
 B. Warchalking
 C. Jamming attacks
 D. Deauthentication attacks

37. You are installing a wireless network for a small business. You decide to sniff traffic on the wireless network to see if it is secure. You can read all the traffic through your wireless sniffer program. Which of the following should you configure on the wireless network to prevent packet sniffing?
   A. Encryption settings
   B. Username and password
   C. Private IP address
   D. Access point power settings

38. Which of the following technologies requires that two devices be touching each other in order to communicate
   A. 802.11i
   B. WPA
   C. Bluetooth
   D. NFC

39. Which of the following describes an attack in which an attacker captures credentials and transmits them to another host for authentication?
   A. Replay attack
   B. Rogue access point
   C. IV attack
   D. Packet sniffing

40. All of the following are valid security issues that allow attacks on WEP, *except*:
   A. 24-bit initialization vectors
   B. Implementation of RC4
   C. Repeated keys
   D. Use of AES

41. Which of the following is an attack vector on networks that use WPA or WPA2?
   A. Use of RC4
   B. Weak passphrases
   C. 24-bit initialization vectors
   D. Use of AES

42. Which of the following attacks enables a malicious person to steal data via Bluetooth devices?
   A. Bluesneaking
   B. Bluejacking
   C. Bluesnarfing
   D. Rogue access point

43. Which of the following was the first attempt at developing a security protocol for early wireless networks?
   A. WPA2
   B. WPA
   C. WEP
   D. RC4

44. How many characters can a WPA/WPA2 passphrase be? (Choose two.)
   A. 6 or 10 characters
   B. 64 hexadecimal characters
   C. 8 to 63 ASCII characters
   D. 64 ASCII characters

45. Which of the following items should be examined when performing a wireless site survey (Choose all that apply.)
   A. Antenna placement
   B. Authentication protocols
   C. Physical environment
   D. Capacity planning

Part II (10%) Please answer the following question.

46.Show the ciphertext stealing technique in ECB mode and CBC mode respectively. (8 points)

47.Explain why there is no need for ciphertext stealing in CFB, OFB, and CTR modes. (2 points)