Information Assurance and Security

Prelim Test Sample

January 2009

1. (15 percent) Explain the three methods of system authentication and give at least one example of each. Explain two-factor authentication.

2. (20 percent) Three common techniques used to store password “hashes” are LANMAN, NTLM, and MD5. Explain each method. Which method of these three is the most secure? Defend your answer.

3. (10 percent) In network traffic analysis, what would explain a TCP packet with all flags set or with illogical combinations of flags set?

4. (15 percent) In public key cryptography, explain how a user named Bob would send an encrypted message to Alice. Explain how Alice would send a digitally signed message to Bob and how Bob would verify the signature.

5. (5 percent) Explain multilateral and multilevel security and give an example of each.

6. (15 percent) Software accounts for a large majority of vulnerabilities in computer and network security. Explain three common software vulnerabilities.

7. (20 percent) Describe the design of a secure computer network with the following requirements: 1) the network connects to the Internet, 2) the network has a Web server and a Mail relay server that both must access the Internet directly, 3) the network contains several internal systems that process extremely sensitive data. In your description, a diagram might be useful to illustrate your design.

Ph.D. Prelim Exam
Information Assurance
April 17, 2009

1. Which one of the following commands is useful for network port scanning as well as Operating System fingerprinting?

    a. nmap
    b. nc
    c. netstat
    d. tftp

2. What is the fundamental difference between assurance and acceptance?

    a. Assurance has to do with security and acceptance is how well-liked it is.
    b. Assurance is whether a system will work and acceptance is how you convince other people that the system works.
    c. Assurance is a measure of security of a system and acceptance is a management decision to deploy a system.
    d. Assurance is a grade assigned by at least three evaluators that shows the reliability of a system and acceptance is determined if this system's grade exceeds a minimum threshold determined by the system's owner.

3. What is the value of the minimum decimal number that can be represented by a 32-bit unsigned integer?

    a. 0
    b. -32768
    c. -2147483648
    d. -1024

4. _____ are where a transaction is carried out in two or more stages, and it is possible for someone to alter the transaction after the stage that involves verifying access rights.

    a. Denial of service attacks
    b. Buffer overflow attacks
    c. Race conditions
    d. Trojan horse attacks

5. Which one of the logs listed below is NOT one of the three basic event logs found in Microsoft Windows 2000?
    a. Application
    b. System
    c. Security

d. Syslog

6. Why should egress filters be utilized at the network perimeter?

    a. To minimize network traffic
    b. To limit information leakage and prevent “ET Phone Home” Trojans
    c. To punish your employees
    d. So that you can use ingress filter

7. Which one of the following best describes what happens when a buffer is overflowed?

    a. The program will crash with a segmentation fault
    b. The person performing the buffer overflow will be given access to the computer running the vulnerable program
    c. The program will provide incorrect results
    d. Nothing bad will happen
    e. Results vary based upon exactly what information is overwritten

8. Which one of the following would be displayed by the ls command for a file with the permissions 6766 on a Linux system?

    a. –rwsrwSrw-
    b. -rwxrwsrws
    c. –rwsrwsrw-
    d. –rwxrwxrw-

9. The _____ attack is, simply, to send a large number of SYN packets and never acknowledge any of the replies.

    a. Smurf
    b. Trojan horse
    c. SYN flood
    d. SPAM

10. Which one of the following is NOT an accepted software testing methodology?

    a. Hybrid approach
    b. Bell-LaPadula
    c. Top Down methodology
    d. Bottom up methodology

11. _____ attacks are those aimed at gaining access to data without the authorization of the data owner.

    a. Integrity
    b. Accountability
    c. Availability
    d. Confidentiality

12. When digitally signing a message using PGP, what key is used to sign the message and which key is used by the recipient to verify the signature?

    a. Sign: recipient's public key, verify: sender's private key
    b. Sign: sender's private key, verify: sender's public key
    c. Sign: sender's public key, verify: recipient's private key
    d. Sign: recipient's public key, verify: recipient's private key

13. Which one of the following Microsoft Windows file systems support access control lists?

    a. FAT
    b. FAT32
    c. NTFS
    d. Floppy

14. Which one of the following is NOT a common cause of software security vulnerabilities?

    a. Poor documentation
    b. Buffer overflows
    c. Timing windows
    d. Insecure default configurations
    e. Bad protocols

15. If your network has never been successfully hacked, what can be said about your Risk Level?

    a. It is Very Low because your security controls must be adequate to keep out the bad guys, since you have never been hacked.
    b. It is at a Medium level

c. It is at a High level because you are overdue for a successful attack
d. You don't know what your Risk level is until you perform a Risk Assessment.

16. One technique that can be used to improve the software testing process is to introduce a number of errors into the code at random. This is know as:

    a. Fault injection
    b. Test metrics manipulation
    c. Harassment
    d. Engineering management

17. Which of the following is NOT a commonly accepted method for securing software applications?

    a. Obfuscate the source code
    b. Chroot or "jail" the application
    c. Tunnel application communications via SSH
    d. Application level access control lists and/or application level authentication

18. When executing a format string attack, what format string is used to "store" a new value into the application's memory address space?

    a. `%n`
    b. `%s`
    c. `%d`
    d. `%x`

19. The format string vulnerability is basically:

    a. A buffer overflow.
    b. An error in the type assigned to a string variable in the C language.
    c. A misuse of the printf function
    d. An error in the way that a software developer formats his source code that causes the complier to produce an insecure executable.

20. _____ attacks include manipulation of data, such as changing a patient's health data.

    a. Integrity
    b. Accountability
    c. Availability
    d. Confidentiality

21. Which one of the following lines (note: the whole line is not displayed) from the `/etc/shadow` file on a Linux machine represents an account that CAN be logged into with no password required?

    a. `lp:*:`
    b. `sys:LK:`
    c. `paul::`
    d. `bin:locked:`
    e. `ftp:NP:`

22. Which one of the following statements is NOT true concerning backups?

    a. Backups should be performed on at least two different types of media.
    b. Backups should be stored off-site for protection from natural disasters
    c. Backups should be tested periodically for verification purposes.
    d. Backup media should be protected in a secure environment.

23. What type of testing is performed by security professionals to verify system vulnerabilities?

    a. Reconnaissance
    b. Scanning
    c. Penetration testing
    d. Hybrid approach

24. _____ attacks erase or destroy evidence as to who caused a problem. These attacks could also result in the placement of false data on the system in order to implicate an innocent party.

    a. Integrity
    b. Accountability
    c. Availability
    d. Confidentiality

25. _____ attacks prevent access to a target machine or network or a particular service.

    a. Integrity
    b. Accountability
    c. Availability
    d. Confidentiality

26. Unauthorized use of “valid” accounts, escalation of privilege, and physical compromise are examples of _____ attacks.

    a. remote
    b. network
    c. local
    d. denial of service

27. Why is telnet a very dangerous utility from a security perspective?

    a. It is an old protocol and has not kept up-to-date.
    b. It is only available on a very few platforms.
    c. It transmits both the username and the password in clear text.
    d. It is extremely difficult to learn how to use and thus the poorly trained telnet user is dangerous from a security point of view.

28. What is the absolute minimum security control that a system administrator should perform to help secure his machines from buffer overflow attacks?

    a. Only use “secure” software.
    b. When a buffer overflow is found, uninstall the software and ask your users to select another product that will meet their needs.
    c. Nothing. Your computer is not likely to be attacked.
    d. Keep your systems and software products fully patched and up-to-date.

29. When using vulnerability scanners, what is a “false negative”?

    a. The vulnerability scanner fails to report a vulnerability that actually exists on the system.
    b. The vulnerability scanner reports that a vulnerability “might” exist on the system.
    c. The vulnerability scanner reports that a Linux machine has a Microsoft Windows vulnerability.
    d. The term “false negative” does not make since, and thus does not exist in this context.

30. Why are escalation of privilege attacks performed?

    a. Because the attacker wants to prove his hacker “worthiness”.
    b. Because the attacker needs to perform an operation on the machine for which he does not currently have the privilege to execute.
    c. No particular reason.
    d. So that he can access the machine again tomorrow.

31. Which one of the following will NOT help to produce better (more secure) software?

    a. Train the software developers about buffer overflows and how to avoid them.
    b. Security awareness training for the developers.
    c. Code reviews.
    d. Decrease development time. The less time a code developer has to generate software, the less likely he is to make mistakes.
    e. Automated code checking tools.

32. _____ goes beyond the initial penetration into the system and includes the installation of root kits and other methods for keeping access to the system.

    a. Scanning
    b. Exploitation
    c. Foot-printing
    d. Reconnaissance

33. Using multiple security controls to protect your valuable information is known as:

    a. a “good job”
    b. spending more money than you really should for security
    c. defense-in-depth
    d. being overstaffed

34. The Chinese-wall is an example of _____.
    a. Multi-user security
    b. Multi-level security
    c. Multi-lateral security
    d. Multi-protocol security

35. Which one of the following is an example of 2-factor authentication?

    a. Username & Password
    b. Retina scan & fingerprint
    c. Password & PIN
    d. Password & Retina scan

36. Password cracking is performed using what 3 methods?

a. brute strength, cunning, good guesses
b. brute force, hybrid, dictionary
c. brute force, dictionary, encyclopedia
d. hydra, crack, l0pht

37. Passwords for most modern Operating Systems are protected using _____.

a. Public Key Infrastructure (PKI)
b. One-way hash
c. Shared key encryption
d. Two-way hash

38. In UNIX or Linux, what file normally is used to store password hashes?

a. /password
b. /etc/password
c. /etc/passwd
d. /etc/shadow
e. /root/shadow

39. When digitally signing a message using PGP, what key is used to sign the message and which key is used by the recipient to verify the signature?

a. Sign: recipient's public key, verify: sender's private key
b. Sign: sender's private key, verify: sender's public key
c. Sign: sender's public key, verify: recipient's private key
d. Sign: recipient's public key, verify: recipient's private key

40. A Denial of Service (DoS) is an attack against the _____ of the information system.

a. Owner
b. System manager
c. Integrity
d. Availability

Ph.D. Preliminary Examination

Information Assurance

October 16, 2009

1. Preventative intrusion detection systems:

   A.) Are far more expensive and effective than other types

   B.) Can only monitor activity on the host itself

   C.) Were the first types of IDSs

   D.) Are designed to stop malicious activity from occurring

2. An IDS is most like:

   A.) A dead-bolt

   B.) A burglar alarm

   C.) A pressure sensor

   D.) An electric gate

3. What are the main types of IDS signatures? (Choose only one answer.)

   A.) Active and reactive

   B.) Context-based and content-based

   C.) Active and passive

   D.) Network-based and file-based

4. What does a host-based IDS examine?

   A.) Feeds from network capture devices such as sniffers

B.) Honeypot activity

C.) Firewall activity records

D.) Activity on the local host

5. Detecting and responding to malicious traffic on a network segment requires:

   A.) An active host-based IDS

   B.) A passive host-based IDS

   C.) An active network-based IDS

   D.) A passive network-based IDS

   Answer: **C**.

6. What are the two main types of intrusion detection systems?

   A.) Signature-based and event-based

   B.) Network-based and host-based

   C.) Active and reactive

   D.) Intelligent and passive

7. Honeypots are primarily used to:

   A.) Collect evidence for law enforcement

   B.) Research behavior of attackers using virtual targets

   C.) Process events from firewalls and routers

   D.) Attract customers to e-commerce sites

8. Which of the following is true for host-based IDSs?

   A.) They are not application-specific.

B.) They cannot determine whether or not an alarm really applies to the local system.

C.) They use local system resources.

D.) They are not operating system–specific.

9. A port scan is…

A.) An attack involving large ICMP packets

B.) A method for breaking into Web servers

C.) A reconnaissance activity

D.) Only effective against firewalls and routers

10. In a UNIX operating system, the master services daemon is called…

A.) Firmware

B.) An Access Control List

C.) inetd

D.) netstat

11. TCP wrappers do what?

A.) Help secure the system by restricting network connections

B.) Help prioritize network traffic for optimal throughput

C.) Encrypt outgoing network traffic

D.) Strip out excess input to defeat buffer overflow attacks

12. File permissions under UNIX consist of what three types?

A.) Modify, read, and execute

B.) Read, write, and execute

C.) Full control, read-only, and run

D.) Write, read, and open

13. Picking the first letter of each word in a sentence to create a password is a…

A.) Baseline

B.) Password policy

C.) Wrapper

D.) Passphrase

14. Which of the following would make the best password?

A.) Snorkel1

B.) TommyJones

C.) Inlk9

D.) Iltdm69m!

15. Users should change their passwords:

A.) Once a year

B.) Every six months

C.) Every 120 to 180 days

D.) Every 60 to 90 days

16. Microsoft's way of bundling updates, fixes, and new functions into a large, self-installing package is called a…

A.) Service pack

B.) Hotfix

C.) Upgrade

D.) Firmware update

17. Applying the latest patches is important for maintaining the security of:

A.) Applications only

B.) Operating systems and applications

C.) Firmware only

D.) Buffer overflows

18. To stop a particular service or program running on a UNIX operating system, you might use the ____ command.

A.) Netstat

B.) Ps

C.) Kill

D.) Inetd

19. An attack conducted by supplying more data than is expected is called:

A.) A buffer overflow

B.) Relaying

C.) Smurfing

D.) Access list trashing

20. A SYN flood is an example of what type of attack?

    A.) Malicious code

    B.) Denial-of-Service

    C.) Man-in-the-middle

    D.) Spoofing

21. An attack in which attackers place themselves in the middle of two other hosts that are communicating in order to view and/or modify the traffic is known as…

    A.) A man-in-the-middle attack

    B.) A Denial-of-Service attack

    C.) A sniffing attack

    D.) A backdoor attack

22. Which attack takes advantage of a trusted relationship that exists between two systems?

    A.) Spoofing

    B.) Password guessing

    C.) Sniffing

    D.) Brute force

23. In what type of attack does an attacker resend the series of commands and codes used in a financial transaction in order to cause the transaction to be conducted multiple times?

    A.) Spoofing

    B.) Man-in-the-middle

    C.) Replay

    D.) Backdoor

24. The trick in both spoofing and TCP/IP hijacking is in trying to…

A.) Provide the correct authentication token

B.) Find two systems between which a trusted relationship exists

C.) Guess a password or brute force a password to gain initial access to the system or network

D.) Maintain the correct sequence numbers for the response packets

25. The most ominous aspect of the Slammer worm was the fact that…

A.) It exploited a vulnerability that had previously not been known

B.) It spread so quickly, affecting 90 percent of vulnerable systems in less than 10 minutes

C.) It affected multiple platforms and multiple operating systems as it utilized a segment of mobile code

D.) It contained a malicious payload that was not detected until over a week after the initial attack

26. The ability of an attacker to crack passwords is directly related to the method the user employed to create the password in the first place, as well as…

A.) The length of the password

B.) The size of the character set used in generating the password

C.) The speed of the machine cracking the password

D.) The dictionary and rules used by the cracking program

27. A piece of malicious code that must attach itself to another file in order to replicate is known as…

A.) A worm

B.) A virus

C.) A logic bomb

D.) A Trojan

28. A piece of code that attempts to propagate through penetration of networks and computer systems is known as…

A.) A worm

B.) A virus

C.) A logic bomb

D.) A Trojan

29. An attack in which the attackers attempt to lie and misrepresent themselves in order to gain access to information that can be useful in an attack is known as what?

A.) Social science

B.) White-hat hacking

C.) Social engineering

D.) Social manipulation

30. The best way to minimize possible avenues of attack for your system is to…

A. Install a firewall and check the logs daily

B. Monitor your intrusion detection system for possible attacks

C. Limit the information that can be obtained on your organization and the services that are run by your Internet-visible systems

D. Ensure that all patches have been applied for the services that are offered by your system

31. What is the value of the minimum decimal number that can be represented by a 32-bit unsigned integer?

A. -32768
B. -2147483648
C. 0
D. -1024

32. Which one of the logs listed below is NOT one of the three basic event logs found in Microsoft Windows 2000?

A. Syslog
B. Application
C. System
D. Security

33. Which one of the following would be displayed by the ls command for a file with the permissions 6766 on a Linux system?

A. -rwxrwsrws
B. –rwsrwsrw-
C. –rwsrwSrw-
D. –rwxrwxrw-

34. Which one of the following Microsoft Windows file systems support access control lists?

A. FAT
B. FAT32
C. NTFS
D. Floppy

35. One technique that can be used to improve the software testing process is to introduce a number of errors into the code at random. This is know as:

A. Engineering management
B. Test metrics manipulation
C. Fault injection
D. Harassment