FCCH FOR REVIEW

1. What is a good security method to prevent unauthorized users from “tailgating” ?
   - 0 ✗ A. Electronic key systems
   - 0 ✓ B. Man trap
   - 0 ✗ C. Pick-resistant locks
   - 0 ✗ D. Electronic combination locks
2. 2.

   Andrew is an IT consultant who works for corporations and government agencies. Andrew plans on shutting down the city’s network using BGP devices and ombies? What type of Penetration Testing is Andrew planning to carry out?

   - 0 ✓ A. DoS Penetration Testing
   - 0 ✗ B. Firewall Penetration Testing
   - 0 ✗ C. Internal Penetration Testing
   - 0 ✗ D. Router Penetration Testing
3. 3.

   What is the military testing scenario called ?

   - 0 ✓ A. Red Box Testing
   - 0 ✗ B. Black Box Testing
   - 0 ✗ C. White Box Testing
   - 0 ✗ D. Grey Box Testing
4. 4.

   Julia is a senior security analyst for Bolton Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company’s main office in Iowa. She states that she needs the receptionist’s network user name and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use ?

   - 0 ✓ A. Reciprocation
   - 0 ✗ B. Social Validation
   - 0 ✗ C. Scarcity
   - 0 ✗ D. Friendship/Liking
5. 5.

   Is the tools and exploit codes during the penetration tests needed to be disclosed to the test sponsor prior before the penetration test ?

   - 0 ✓ A. True

- 0 ✗ B. False

6. 6.

   What are they key success factor in a penetration test ?

   - 0 ✓ A. The ability to show the depth of the impact.
   - 0 ✗ B. The ability to hack into the system.
   - 0 ✗ C. The ability to demonstrate the vulnerability.
   - 0 ✗ D. No correct answers.

7. 7.

   What is the default document that is the key requirement prior before starting a Penetration Testing Project ?

   - 0 ✓ A. Non Disclosure Agreement
   - 0 ✗ B. Security Policy Compliance
   - 0 ✗ C. Confidentiality Agreement
   - 0 ✗ D. All mention answers

8. 8.

   Cyber Crime Legal Clauses are mandatory when proposing testing projects.

   - 0 ✓ A. True
   - 0 ✗ B. False

9. 9.

   Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

   - 0 ✓ A. Tailgating
   - 0 ✗ B. Man trap attack
   - 0 ✗ C. Fuzzing
   - 0 ✗ D. Backtrapping

10. 10.

   Which of the following attacks combines dictionary and brute force attacks?

   - 0 ✗ A. Brute Force Attack
   - 0 ✓ B. Hybrid Attack
   - 0 ✗ C. Phishing Attack
   - 0 ✗ D. Replay Attack

11. 11.

When a major vulnerability in the security of a critical web server is discovered, immediate notification should be made to the:

- 0 ✓ A. System owner to take corrective action.
- 0 ✗ B. Incident response team to investigate.
- 0 ✗ C. Data owners to mitigate damage.
- 0 ✗ D. Development team to remediate.

12. 12.

What is the key difference of Black Box Penetration Testing & White Box Test ?

- 0 ✓ A. Black Box Test is a blinded test and a White Box is specific.
- 0 ✗ B. Key success factor is higher on Black Box Test.
- 0 ✗ C. Black Box Test requires more skills and White Box Test requires less.
- 0 ✗ D. A Black Box Test is a pronounced test and a White Box Test is a non pronounced.

13. 13.

A systems ability to identify a particular individual, track their actions, and monitor their behavior is known as:

- 0 ✓ A. Accountability
- 0 ✗ B. Auditing
- 0 ✗ C. Monitoring
- 0 ✗ D. Observing

14. 14.

Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

- 0 ✓ A. Change management
- 0 ✗ B. Patch management
- 0 ✗ C. Stress testing
- 0 ✗ D. Security baselines

15. 15.

When would be appropriate to to drop the project of Penetration Testing ?

- 0 ✓ A. During a feasibility assessment time.
- 0 ✗ B. During the risk management time.
- 0 ✗ C. During the project kick off time.
- 0 ✗ D. Anytime.

16. 16.

The MAIN goal of an information security strategic plan is to:

- 0 ✓ A. protect information assets and resources.
- 0 ✗ B. establish security governance.

- 0 ✗ C. develop a risk assessment plan.
- 0 ✗ D. develop a data protection plan.

17. 17.

An organization without any formal information security program that has decided to implement information security best practices should FIRST:

- 0 ✓ A. define high-level business security requirements.
- 0 ✗ B. benchmark similar organizations.
- 0 ✗ C. allocate budget based on best practices.
- 0 ✗ D. invite an external consultant to create the security strategy.

18. 18.

What are the common Reconnaissance phase which is referenced to a inactive intelligence gathering ?

- 0 ✓ A. Passive Information Gathering
- 0 ✗ B. Active Information Gathering
- 0 ✗ C. Social Engineering
- 0 ✗ D. Pilfering

19. 19.

When is the most appropriate time for conducting an Intrusive Test for a secure production environment ?

- 0 ✗ A. 9.00 am to 5.00 pm
- 0 ✗ B. During lunch time
- 0 ✗ C. During tea break
- 0 ✓ D. After office hour

20. 20.

Where would it be likely the test environment be set for remote testing for target servers ?

- 0 ✓ A. Spoofed Ip infrastructure
- 0 ✗ B. Undisclosed location
- 0 ✗ C. Home
- 0 ✗ D. Customer office

21. 21.

Penetration Testing which includes Social Engineering could be done without Managements approval ?

- 0 ✗ A. True
- 0 ✓ B. False

22. 22.

The last step of a Security Test is which of the below ?

- 0 ✓ A. Covering tracks
- 0 ✗ B. Backdooring

- 0 ✗ C. Pivoting
- 0 ✗ D. No correct answer

23. 23.

What is referred to a Penetration Testing Method which involves extensive testing to a privilege escalation test ?

- 0 ✗ A. Red Box Testing
- 0 ✗ B. White Box Testing
- 0 ✓ C. Grey Box Testing
- 0 ✗ D. Black Box Testing

24. 24.

Common exploitation methods use in modern security testing would be ?

- 0 ✓ A. Mobile Devices
- 0 ✗ B. USB Flash Disk
- 0 ✗ C. Wireless
- 0 ✗ D. Bluetooth

25. 25.

Bill is the accounting manager for Gerard and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through e-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection ?

- 0 ✗ A. PDF passwords can easily be cracked by software brute force tools.
- 0 ✓ B. PDF passwords are not considered safe by Sarbanes-Oxley.
- 0 ✗ C. PDF passwords are converted to clear text when sent through e-mail.
- 0 ✗ D. When sent through e-mail, PDF passwords are stripped from the document completely.

26. 26.

Where would the best place for testing which security landscape is relaxed ?

- 0 ✓ A. Disaster Recovery Site
- 0 ✗ B. VPN Networks
- 0 ✗ C. Mail Server Farm
- 0 ✗ D. All of the above

27. 27.

Keystroke logging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored:

- 0 ✗ A. Alternate between typing the login credentials and typing characters somewhere else in the focus window.
- 0 ✗ B. Type a wrong password first, later type the correct password on the login page defeating the key logger recording.

- 0 ✓ C. Type a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
- 0 ✗ D. The next key typed replaces selected text portion. E.g. if the password is“secret”, one could type “s”, then some dummy keys “asdfsd”.Then these dummies could be selected with mouse, and next character from the password “e” is typed, which replaces the dummies “asdfsd”.

28. 28.

What would the most easiest testing method to conduct but could prove disastrous if wrongly executed ?

- 0 ✓ A. Social Engineering
- 0 ✗ B. Physical Testing
- 0 ✗ C. Buffer Overflow
- 0 ✗ D. Side Channel Attack

29. 29.

Fiona, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning ?

- 0 ✗ A. A recent security breach in which passwords were cracked.
- 0 ✗ B. Implementation of configuration management processes.
- 0 ✓ C. Enforcement of password complexity requirements.
- 0 ✗ D. Implementation of account lockout procedures.

30. 30.

Which of the following security mechanisms is MOST effective in protecting classified data that have been encrypted to prevent disclosure and transmission outside the organization’s network ?

- 0 ✗ A. Configuration of firewalls
- 0 ✗ B. Strength of encryption algorithms
- 0 ✗ C. Authentication within application
- 0 ✓ D. Safeguards over keys

31. 31.

Contrary to popular believe, What is the actual function of an Ethical Hacker ?

- 0 ✗ A. System Level Tester
- 0 ✗ B. O/S level Tester
- 0 ✗ C. Source Code Tester
- 0 ✓ D. Infrastructure Tester

32. 32.

What is the benefit to the management if the senior management were to propose a Penetration Testing activity as a part of their security continuity project ?

- 0 ✗ A. Better Vulnerability Understanding.
- 0 ✓ B. Better Impact Assessment.
- 0 ✗ C. Better Visibility of Hacker Skills.
- 0 ✗ D. Better Exploit Understanding.

33. 33.

Backdooring a compromised system is a standard practice of penetration testing. Is it a standard practice ?

- 0 ✗ A. True
- 0 ✓ B. False

34. 34.

What is the best format of Penetration Testing Report for Final Delivery ?

- 0 ✗ A. Verbal communication
- 0 ✓ B. Hard copy
- 0 ✗ C. Soft copy
- 0 ✗ D. No correct answer

35. 35.

Would hiring an ex Black Hat Hacker be advisable to a penetration testing project ?

- 0 ✗ A. Yes - Advisable.
- 0 ✓ B. No - Not Advisable.