**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** The Pen Test: Putting It All Together

|  |  |  |
| --- | --- | --- |
| 答案 | 編號 | 題目 |
|  | 1. | Incident response (IR) is an important part of organizational security. In what step of the incident-handling process would IR team members disable or delete user accounts and change firewall rules?  **A.**   Detection and analysis　**B.**   Classification and prioritization  **C.**   Containment　　　　　　**D.**   Forensic investigation |
|  | 2. | A software company puts an application through stringent testing and, on the date of release, is confident the software is free of known vulnerabilities. An organization named BigBiz purchases the software at a premium cost, with a guarantee of service, maintenance, and liability. Which risk management method is in use by the BigBiz organization?  **A.**   Accept　　　　**B.**   Transfer  **C.**   Avoid　　　　　**D.**   Mitigate |
|  | 3. | Which of the following provide automated pen test–like results for an organization? (Choose all that apply.)  **A.**   Metasploit　　**B.**   Nessus　　**C.**   Core Impact  **D.**   CANVAS　　　**E.**   SAINT　　**F.**   GFI LanGuard |
|  | 4. | Which of the following best describes an assessment against a network segment that tests for existing vulnerabilities but does not attempt to exploit any of them?  **A.**   Penetration test　　　　　　　**B.**   Partial penetration test  **C.**   Vulnerability assessment　　　**D.**   Security audit |
|  | 5. | You are a member of a pen test team conducting tests. Your team has all necessary scope, terms of engagement, and nondisclosure and service level agreements in place. You gain access to an employee’s system and during further testing discover child pornography on a hidden drive folder. Which of the following is the best course of action for the ethical hacker?  **A.**   Continue testing without notification to anyone, but ensure the information is included in the final out-brief report.  **B.**   Continue testing without interruption, but completely remove all hidden files and the folder containing the pornography.  **C.**   Stop testing and notify law enforcement authorities immediately.  **D.**   Stop testing and remove all evidence of intrusion into the machine. |
|  | 6. | In which phase of a pen test is scanning performed?  **A.**   Pre-attack　　　　**B.**   Attack  **C.**   Post-attack　　　　**D.**   Reconnaissance |
|  | 7. | Which of the following describes risk that remains after all security controls have been implemented to the best of one’s ability?  **A.**   Residual　　　　**B.**   Inherent  **C.**   Deferred　　　　**D.**   Remaining |
|  | 8. | Which of the following statements are true regarding OSSTMM? (Choose all that apply.)  **A.**   OSSTMM is a nonprofit, international research initiative dedicated to defining standards in security testing and business integrity testing.  **B.**   OSSTMM recognizes ten types of controls, which are divided into two classes.  **C.**   ISECOM maintains the OSSTMM.  **D.**   OSSTMM defines three types of compliance. |
|  | 9. | Which of the following is an open source project produced by OISSG (Open Information Systems Security Group) intended to provide security testing assistance?  **A.**   OSSTMM　**B.**   OWASP　**C.**   COBIT　**D.**   ISSAF |
|  | 10. | NIST SP 800-30 defines steps for conducting a risk assessment. Which of the following statements is true regarding the process?  **A.**   Threats are identified before vulnerabilities.  **B.**   Determining the magnitude of impact is the first step.  **C.**   Likelihood is determined after the risk assessment is complete.  **D.**   Risk assessment is not a recurring process. |
|  | 11. | In which phase of a pen test will the team penetrate the perimeter and acquire targets?  **A.**   Pre-attack  **B.**   Attack  **C.**   Post-attack  **D.**   None of the above |
|  | 12. | Which of the following is a legitimate communication path for the transfer of data?  **A.**   Overt　　**B.**   Covert　　**C.**   Authentic  **D.**   Imitation　**E.**   Actual |
|  | 13. | An organization participates in a real-world exercise designed to test all facets of its security systems. An independent group is hired to assist the organization’s security groups, assisting in the defense of assets against the attacks from the attacking group. Which of the following statements is true?  **A.**   The group assisting in the defense of the systems is referred to as a blue team.  **B.**   The group assisting in the defense of the systems is referred to as a red team.  **C.**   The group assisting in the defense of the systems is known as a white-hat group.  **D.**   The team attacking the systems must provide all details of any planned attack with the defense group before launching to ensure security measures are tested appropriately. |
|  | 14. | Sally is part of a penetration test team and is starting a test. The client has provided a network drop on one of their subnets for Sally to launch her attacks from. However, they did not provide any authentication information, network diagrams, or other notable data concerning the systems. Which type of test is Sally performing?  **A.**   External, white box　　　**B.**   External, black box  **C.**   Internal, white box　　　**D.**   Internal, black box |
|  | 15. | Your pen test team is discussing services with a potential client. The client indicates they do not see the value in penetration testing. Which of the following is the correct response from your team?  **A.**   Run a few tests and display the results to the client to prove the value of penetration testing.  **B.**   Provide detailed results from other customers you’ve tested, displaying the value of planned testing and security deficiency discovery.  **C.**   Provide information and statistics regarding pen testing and security vulnerabilities from reliable sources.  **D.**   Perform the penetration test anyway in case they change their mind. |
|  | 16. | In which phase of a penetration test would you compile a list of vulnerabilities found?  **A.**   Pre-attack　　　　**B.**   Attack  **C.**   Post-attack　　　　**D.**   Reconciliation |
|  | 17. | Which of the following has a database containing thousands of signatures used to detect vulnerabilities in multiple operating systems?  **A.**   Nessus　**B.**   Hping　**C.**   LOIC　**D.**   SNMPUtil |
|  | 18. | Cleaning registry entries and removing uploaded files and tools are part of which phase of a pen test?  **A.**   Covering tracks　**B.**   Pre-attack  **C.**   Attack　　　　　**D.**   Post-attack |
|  | 19. | Which of the following are true statements regarding a pen test? (Choose all that apply.)  **A.**   Pen tests do not include social engineering.  **B.**   Pen tests may include unannounced attacks against the network.  **C.**   During a pen test, the security professionals can carry out any attack they choose.  **D.**   Pen tests always have a scope.  **E.**   A list of all personnel involved in the test is not included in the final report. |
|  | 20. | Which of the following causes a potential security breach?  **A.**   Vulnerability　　**B.**   Threat　　**C.**   Exploit　　**D.**   Zero day |
|  | 21. | Which Metasploit payload type operates via DLL injection and is difficult for antivirus software to pick up?  **A.**   Inline　　**B.**   Meterpreter　　**C.**   Staged　　**D.**   Remote |
|  | 22. | Metasploit is a framework allowing for the development and execution of exploit code against a remote host and is designed for use in pen testing. The framework consists of several libraries, each performing a specific task and set of functions. Which library is considered the most fundamental component of the Metasploit framework?  **A.**   MSF Core　**B.**   MSF Base　**C.**   MSF interfaces　**D.**   Rex |
|  | 23. | Which of the following may be effective countermeasures against an inside attacker? (Choose all that apply.)  **A.**   Enforce elevated privilege control.  **B.**   Secure all dumpsters and shred collection boxes.  **C.**   Enforce good physical security practice and policy.  **D.**   Perform background checks on all employees. |