**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** Trojans and Other Attacks

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | Bart receives an e-mail that appears to be from his lawyer containing a ZIP file named Courtdoc.zip. Bart double-clicks the ZIP file to open it, and a message stating “This word document is corrupt” appears. In the background, a file named Courtdoc.doc.exe runs and copies itself to the local APPDATA directory. It then begins beaconing to an external server. Which of the following best describes the malware Bart installed?  **A.**   Worm  **B.**   Virus  **C.**   Trojan  **D.**   Macro |
|  | 2. | You have established a Netcat connection to a target machine. Which flag can be used to launch a program?  **A.**   -p  **B.**   -a  **C.**   -l  **D.**   -e |
|  | 3. | Claire is surfing the Web and, after some time, a message pops up stating her system has been infected by malware and offering a button to click for removal of the virus. After she clicks the button, another message window appears stating the system has been quarantined due to the nature of the infection and provides a link with instructions to pay in order to regain control and to clear the virus. Which of the following best describes this infection?  **A.**   Spyware  **B.**   Ransomware  **C.**   Trojan  **D.**   Adware |
|  | 4. | Matty is examining malware as part of a security effort. She performs analysis of the malware executable without running or installing it. Instead, she examines source and binary code to find data structures, function calls, and other indicators of malicious behavior. Which of the following best describes the type of malware analysis Matty is performing?  **A.**   Static  **B.**   Dynamic  **C.**   File fingerprinting  **D.**   Code emulation |
|  | 5. | Pen test team member Amy attempts to guess the ISN for a TCP session. Which attack is she most likely carrying out?  **A.**   XSS  **B.**   Session splicing  **C.**   Session hijacking  **D.**   Multipartite attack |
|  | 6. | An attacker wants to make his malware as stealthy and undetectable as possible. He employs an effort that uses compression to reduce the file size of the malware. Which of the following best describes this?  **A.**   Crypter  **B.**   Wrapper  **C.**   Packer  **D.**   Compressor |
|  | 7. | An attacker is attempting a DoS attack against a machine. She first spoofs the target’s IP address and then begins sending large amounts of ICMP packets containing the MAC address FF:FF:FF:FF:FF:FF. What attack is underway?  **A.**   ICMP flood  **B.**   Ping of death  **C.**   SYN flood  **D.**   Smurf  **E.**   Fraggle |
|  | 8. | An attacker makes use of the Beacon implant on a target system to hijack a browser session. Which of the following best describes this attack?  **A.**   Man in the browser  **B.**   Man in the middle  **C.**   Man in the pivot  **D.**   IE hijacking |
|  | 9. | Claire’s Windows system at work begins displaying strange activity, and she places a call to the IT staff. On investigation, it appears Claire’s system is infected with several viruses. The IT staff removes the viruses, deleting several file and folder locations and using an AV tool, and the machine is reconnected to the network. Later in the day, Claire’s system again displays strange activity and the IT staff is called once again. Which of the following are likely causes of the re-infection? (Choose all that apply.)  **A.**   Claire revisits a malicious website.  **B.**   Claire opens her Microsoft Outlook e-mail client and newly received e-mail is loaded to her local folder (.pst file).  **C.**   Claire uses a system restore point to regain access to deleted files and folders.  **D.**   Claire uses the organization’s backup application to restore files and folders. |
|  | 10. | In regard to Trojans, which of the following best describes a wrapper?  **A.**   The legitimate file the Trojan is attached to  **B.**   A program used to bind the Trojan to a legitimate file  **C.**   A method of obfuscation using compression  **D.**   A software tool that uses encryption and code manipulation to hide malware |
|  | 11. | In May of 2017, this ransomware took advantage of a Windows SMB vulnerability known as the Eternal Blue exploit and spread worldwide in a matter of hours. A hidden kill switch inside the coding was quickly discovered, halting its spread. Which of the following best fits this description?  **A.**   Petya  **B.**   WannaCry  **C.**   Zeus  **D.**   Botnet |
|  | 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. | In what layer of the OSI reference model is session hijacking carried out?  **A.**   Data Link layer  **B.**   Transport layer  **C.**   Network layer  **D.**   Physical layer |
|  | 14. | A pen test team member types the following command:  nc222.15.66.78 –p 8765  Which of the following statements is true regarding this attempt?  **A.**   The attacker is attempting to connect to an established listening port on a remote computer.  **B.**   The attacker is establishing a listening port on his machine for later use.  **C.**   The attacker is attempting a DoS against a remote computer.  **D.**   The attacker is attempting to kill a service on a remote machine. |
|  | 15. | Examine the partial command-line output listed here:  Images  Which of the following is a true statement regarding the output?  **A.**   This is output from a **netstat -an** command.  **B.**   This is output from a **netstat -b** command.  **C.**   This is output from a **netstat -e** command.  **D.**   This is output from a **netstat -r** command. |
|  | 16. | You are discussing malware with a new pen test member who asks about restarting executables. Which registry keys within Windows automatically run executables and instructions? (Choose all that apply.)  **A.**   HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce  **B.**   HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices  **C.**   HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce  **D.**   HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run |
|  | 17. | Which of the following is a true statement?  **A.**   Sequence prediction attacks are specific to TCP.  **B.**   Using a protocol in a way it is not intended to be used is an example of an overt channel.  **C.**   All DoS and DDoS attacks are specific to TCP.  **D.**   Fraggle is a TCP-based attack. |
|  | 18. | Which denial-of-service attack involves using multiple intermediary and secondary machines to contribute to the DoS effort?  **A.**   SYN flood  **B.**   DRDoS  **C.**   Application-level flood  **D.**   LOIC |
|  | 19. | Which of the following takes advantage of weaknesses in the fragment reassembly functionality of TCP/IP?  **A.**   Teardrop  **B.**   SYN flood  **C.**   Smurf attack  **D.**   Ping of death |
|  | 20. | IPSec is an effective preventative measure against session hijacking. Which IPSec mode encrypts only the data payload?  **A.**   Transport  **B.**   Tunnel  **C.**   Protected  **D.**   Spoofed |
|  | 21. | What provides for both authentication and confidentiality in IPSec?  **A.**   AH  **B.**   IKE  **C.**   OAKLEY  **D.**   ESP |
|  | 22. | Which of the following statements best describes the comparison between spoofing and session hijacking?  **A.**   Spoofing and session hijacking are the same thing.  **B.**   Spoofing interrupts a client’s communication, whereas hijacking does not.  **C.**   Hijacking interrupts a client’s communication, whereas spoofing does not.  **D.**   Hijacking emulates a foreign IP address, whereas spoofing refers to MAC addresses. |
|  | 23. | Which of the following is an effective deterrent against TCP session hijacking?  **A.**   Install and use an HIDS on the system.  **B.**   Install and use Tripwire on the system.  **C.**   Enforce good password policy.  **D.**   Use unpredictable sequence numbers. |
|  | 24. | Which of the following is a group of Internet computers set up to forward transmissions to other computers on the Internet without the owner’s knowledge or permission?  **A.**   Botnet  **B.**   Zombie  **C.**   Honeypot  **D.**   DDoS |
|  | 25. | Within a TCP packet dump, a packet is noted with the SYN flag set and a sequence number set at A13F. What should the acknowledgment number in the return SYN/ACK packet be?  **A.**   A131  **B.**   A130  **C.**   A140  **D.**   A14F |
|  | 26. | When is session hijacking performed?  **A.**   Before the three-step handshake  **B.**   During the three-step handshake  **C.**   After the three-step handshake  **D.**   After a FIN packet |