Logical Operations

Exam CFR-210

Logical Operations CyberSec First Responder

Verson: Demo

[Total Questions: 10]

Question No : 1

Which of the following are legally compliant forensics applications that will detect ADS or a file with an incorrect file extension? (Choose two.)

A. Regedit
B. EnCase
C. dd
D. FTK
E. Procmon

Answer: A,C

Question No : 2

Which of the following could an attacker use to perpetrate a social engineering attack? (Choose two.)

A. Keylogger
B. Yagi
C. Company uniform
D. Blackdoor
E. Phone call

Answer: A,E

Question No : 3

A high-level government official uses anonymous bank accounts to transfer a requested amount of funds to individuals in another country. These individuals are known for defacing government websites and exfiltrating sensitive data. Which of the following BEST describes the involved threat actors?

A. State-sponsored hackers
B. Gray hat hackers
C. Hacktivists
D. Cyber terrorists

Answer: D

Question No : 4

An organization’s firewall has recently been bombarded with an excessive amount of failed requests. A security analyst has been tasked with providing metrics on any failed attempts to ports above 1000. Which of the following regular expressions will work BEST to identify an IP address with the desired port range?

A. /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):({4,5}\d+)\b/
B. /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([4]\D+)\b/
C. /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([4]\d+)\b/
D. /\b^(?\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):(\d{1,5})\b/

Answer: C

Question No : 5

A Windows system user reports seeing a command prompt window pop up briefly during each login. In which of the following locations would an incident responder check to explain this activity?

A. rc.d
B. HKLM “RunOnce” key
C. c:\temp
D. /etc/init.d/

Answer: C

Question No : 6

An intruder gains physical access to a company’s headquarters. The intruder is able to access the company’s network via a visitor’s office. The intruder sets up an attack device, under the visitor’s office desk, that impersonates the corporate wireless network. Users at headquarters begin to notice slow browsing speeds from their company laptops. Which of the following attacks is MOST likely occurring?

A. Man-in-the-middle
B. Denial of service
C. Social engineering
D. ARP table poisoning

Answer: D

Question No : 7

An incident responder has captured packets associated with malware. The source port is 8765 and the destination port is 7653. Which of the following commands should be used on the source computer to help determine which program is responsible for the connection?

A. services.msc
B. psexec
C. msconfig
D. fport

Answer: D

Question No : 8

During an investigation on Windows 10 system, a system administrator needs to analyze Windows event logs related to CD/DVD-burning activities. In which of the following paths will the system administrator find these logs?

A. \Windows\Systems32\winevt\logs\System.evt
B. \Windows\System32\winevt\Logs\System.evtx
C. \Windows\Systems\winevt\Evtlogs\System.evtx
D. \Windows\System\winevt\Logs\System.evt

Answer: B

Question No : 9

Customers are reporting issues connecting to a company’s Internet server. Which of the following device logs should a technician review in order to help identify the issue?

A. WIPS
B. SSH
C. WAP
D. WAF

Answer: A

Question No : 10

Which of the following enables security personnel to have the BEST security incident recovery practices?

A. Crisis communication plan
B. Disaster recovery plan
C. Occupant emergency plan
D. Cyber incident response plan

Answer: D