CertNexus

CFR-410
CyberSec First Responder (CFR) Exam

Questions & Answers PDF

Latest Version: 6.0

Question: 1

Which of the following types of attackers would be MOST likely to use multiple zero-day exploits executed against high-value, well-defended targets for the purposes of espionage and sabotage?

A. Cybercriminals
B. Hacktivists
C. State-sponsored hackers
D. Cyberterrorist

Answer: C

Question: 2

Malicious code designed to execute in concurrence with a particular event is BEST defined as which of the following?

A. Logic bomb
B. Rootkit
C. Trojan
D. Backdoor

Answer: A

Reference: https://searchsecurity.techtarget.com/definition/Malware-Glossary

Question: 3

In which of the following attack phases would an attacker use Shodan?

A. Scanning
B. Reconnaissance
C. Gaining access
D. Persistence

Answer: A

Question: 4

During a malware-driven distributed denial of service attack, a security researcher found excessive requests to a name server referring to the same domain name and host name encoded in hexadecimal. The malware author used which type of command and control?

A. Internet Relay Chat (IRC)
B. Dnscat2
C. Custom channel
D. File Transfer Protocol (FTP)

Answer: D

Reference: https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on- the-internet.html

Question: 5

Nmap is a tool most commonly used to:

A. Map a route for war-driving
B. Determine who is logged onto a host
C. Perform network and port scanning
D. Scan web applications

Answer: C