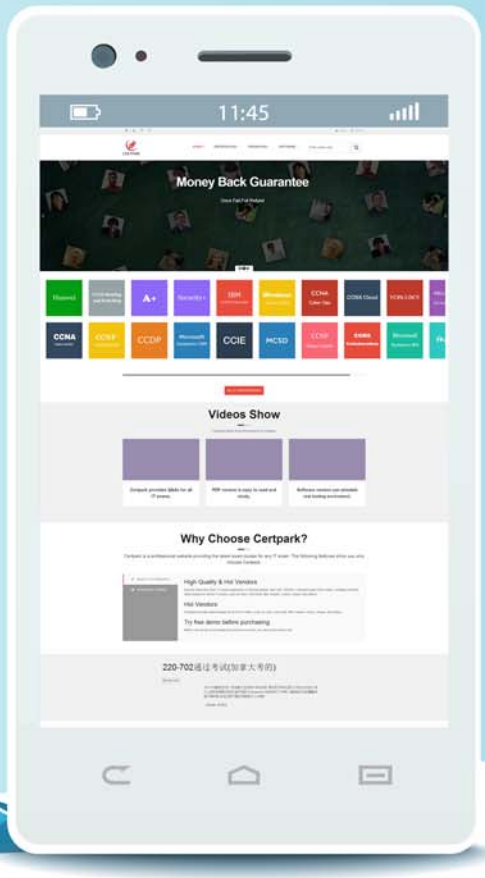
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **SEC504**

Title : Hacker Tools, Techniques, Exploits and Incident Handling

Version : DEMO

1.Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?
A. Preparation phase
B. Eradication phase
C. Identification phase
D. Recovery phase
E. Containment phase
Answer: A

2.Which of the following statements are true about netcat?
Each correct answer represents a complete solution. Choose all that apply.
A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.
B. It can be used as a file transfer solution.
C. It provides outbound and inbound connections for TCP and UDP ports.
D. The nc -z command can be used to redirect stdin/stdout from a program.
Answer: A,B,C

3.Which of the following is a reason to implement security logging on a DNS server?
A. For preventing malware attacks on a DNS server
B. For measuring a DNS server's performance
C. For monitoring unauthorized zone transfer
D. For recording the number of queries resolved
Answer: C

4.The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?
A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Answer: C

5.You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?
Each correct answer represents a complete solution. Choose all that apply.
A. Misconfiguration (e.g. open mail relay, missing patches, etc.)
B. Vulnerabilities that allow a remote cracker to control sensitive data on a system
C. Vulnerabilities that allow a remote cracker to access sensitive data on a system

D. Vulnerabilities that help in Code injection attacks
Answer: A,B,C