Exam Code: 156-515

Exam Name: Check Point Certified Security Expert Plus NGX

Vendor: Check Point

Version: DEMO

Part: A

1: Which files should be acquired from a Windows 2003 Server system crash with a Dr. Watson error?
A.drwtsn32.log
B.vmcore.log
C.core.log
D.memory.log
E.info.log
Correct Answers: A

2: VPN debugging information is written to which of the following files?
A.FWDIR/log/ahttpd.elg
B.FWDIR/log/fw.elg
C.$FWDIR/log/ike.elg
D.FWDIR/log/authd.elg
E.FWDIR/log/vpn.elg
Correct Answers: C

3: fw monitor packets are collected from the kernel in a buffer. What happens if the buffer becomes full?
A.The information in the buffer is saved and packet capture continues, with new data stored in the buffer.
B.Older packet information is dropped as new packet information is added.
C.Packet capture stops.
D.All packets in it are deleted, and the buffer begins filling from the beginning.
Correct Answers: D

4: Which file provides the data for the host_table output, and is responsible for keeping a record of all internal IPs passing through the internal interfaces of a restricted hosts licensed Security Gateway?
A.hosts.h
B.external.if
C.hosts
D.fwd.h
E.fwconn.h
Correct Answers: D

5: You modified the *def file on your Security Gateway, but the changes were not applied. Why?
A.There is more than one *.def file on the Gateway.
B.You did not have the proper authority.
C.*.def files must be modified on the SmartCenter Server.
D.The *.def file on the Gateway is read-only.
Correct Answers: C

6: Assume you have a rule allowing HTTP traffic, on port 80, to a specific Web server in a Demilitarized Zone (DMZ). If an external host port scans the Web server's IP address, what information will be revealed?
A.Nothing; the NGX Security Server automatically block all port scans.
B.All ports are open on the Security Server.
C.All ports are open on the Web server.
D.The Web server's file structure is revealed.
E.Port 80 is open on the Web server.
Correct Answers: E

7: Which of the following types of information should an Administrator use tcpdump to view?
A.DECnet traffic analysis
B.VLAN trunking analysis
C.NAT traffic analysis
D.Packet-header analysis
E.AppleTalk traffic analysis
Correct Answers: D

8: Which statement is true for route based VPNs?
A.IP Pool NAT must be configured on each gateway
B.Route-based VPNs replace domain-based VPNs
C.Route-based VPNs are a form of partial overlap VPN Domain
D.Packets are encrypted or decrypted automatically
E.Dynamic-routing protocols are not required
Correct Answers: E

9: The list below provides all the actions Check Point recommends to troubleshoot a problem with an NGX product.
A.List Possible Causes
B.Identify the Problem
C.Collect Related Information
D.Consult Various Reference Sources
E.Test Causes Individually and Logically
Select the answer that shows the order of the recommended actions that make up Check Point's troubleshooting guidelines?
A.B, C, A, E, D
B.A, E, B, D, C
C.A, B, C, D, E
D.B, A, D, E, C
E.D, B, A, C, E
Correct Answers: A

10: NGX Wire Mode allows:

A.Peer gateways to establish a VPN connection automatically from predefined preshared secrets.
B.Administrators to verify that each VPN-1 SecureClient is properly configured, before allowing it access to the protected domain.
C.Peer gateways to fail over existing VPN traffic, by avoiding Stateful Inspection.
D.Administrators to monitor VPN traffic for troubleshooting purposes.
E.Administrators to limit the number of simultaneous VPN connections, to reduce the traffic load passing through a Security Gateway.
Correct Answers: C

11: Which of the following commands identifies whether or not a Security Policy is installed or the Security Gateway is operating with the Initial Policy?
A.fw monitor
B.cp policy
C.cp stat
D.fw policy
E.fw stat
Correct Answers: E

12: A SecuRemote/SecureClient tunnel test uses which port?
A.UDP 18233
B.UDP 2746
C.UDP 18234
D.TCP 18231
E.UDP 18321
Correct Answers: C

13: Which of the following vpn debug options purges ike.elg and vpnd.elg, and creates a time stamp before starting ike debug and vpn debug at the same time?
A.ike on
B.timeon
C.trunc
D.ikefail
E.mon
Correct Answers: C

14: Gus is troubleshooting a problem with SMTP. He has enabled debugging on his Security Gateway and needs to copy the *.elg files into an archive to send to Check Point Support. Which of the following files does Gus NOT need to send?
A.fwd.elg
B.mdq.elg
C.diffserv.elg
D.asmtpd.elg
Correct Answers: C

15: How can you view cpinfo on a SecurePlatform Pro machine?
A.snoop -i
B.infotab
C.tcpdump
D.Text editor, such as vi
E.infoview
Correct Answers: D

16: When VPN-1 NGX starts after reboot, with no installed Security Policy, which of these occurs?
A.All traffic except HTTP connections is blocked.
B.All traffic except SmartDefense Console connections is blocked.
C.All traffic is blocked.
D.All traffic except SmartConsole/SmartCenter Server connections is blocked.
E.All traffic is allowed.
Correct Answers: D

17: Which of the following commands would you run to debug a VPN connection?
A.debug vpn ike
B.debug vpn ikeon
C.vpn debug ike
D.debug vpn ike on
E.vpn debug ikeon
Correct Answers: E

18: Which one of these is a temporary pointer log file?
A.$FWDIR/log/xx.logptr
B.$FWDIR/log/xx.log
C.$FWDIR/log/xx.logaccount_ptr
D.$FWDIR/log/xx.logLuuidDB
Correct Answers: D

19: When collecting information relating to the perceived problem, what is the most important question to ask?
A.Is this problem repeatable?
B.Is this problem software or hardware related?
C.Under what circumstances does this problem occur?
D.What action or state am I trying to achieve?
E.Does the problem appear random or can you establish a pattern?
Correct Answers: C

20: The virtual machine inspects each packet at the following points:
-Before the virtual machine, in the inbound direction (i or PREIN)
-After the virtual machine, in the inbound direction (I or POSTIN)

-Before the virtual machine, in the outbound direction (o or PREOUT)
-After the virtual machine, in the outbound direction (O or POSTOUT)
If Ethereal displays a packet with i, I, o, and O entries, what does that likely indicate?
A.The packet was rejected by the Rule Base.
B.The packet was destined for the Gateway.
C.Nothing unusual; the o and O entries only appear if there is a kernel-level error.
D.The packet was rerouted by the Gateway's OS.
E.The packet arrived at the kernel and left the Security Gateway successfully.
Correct Answers: E