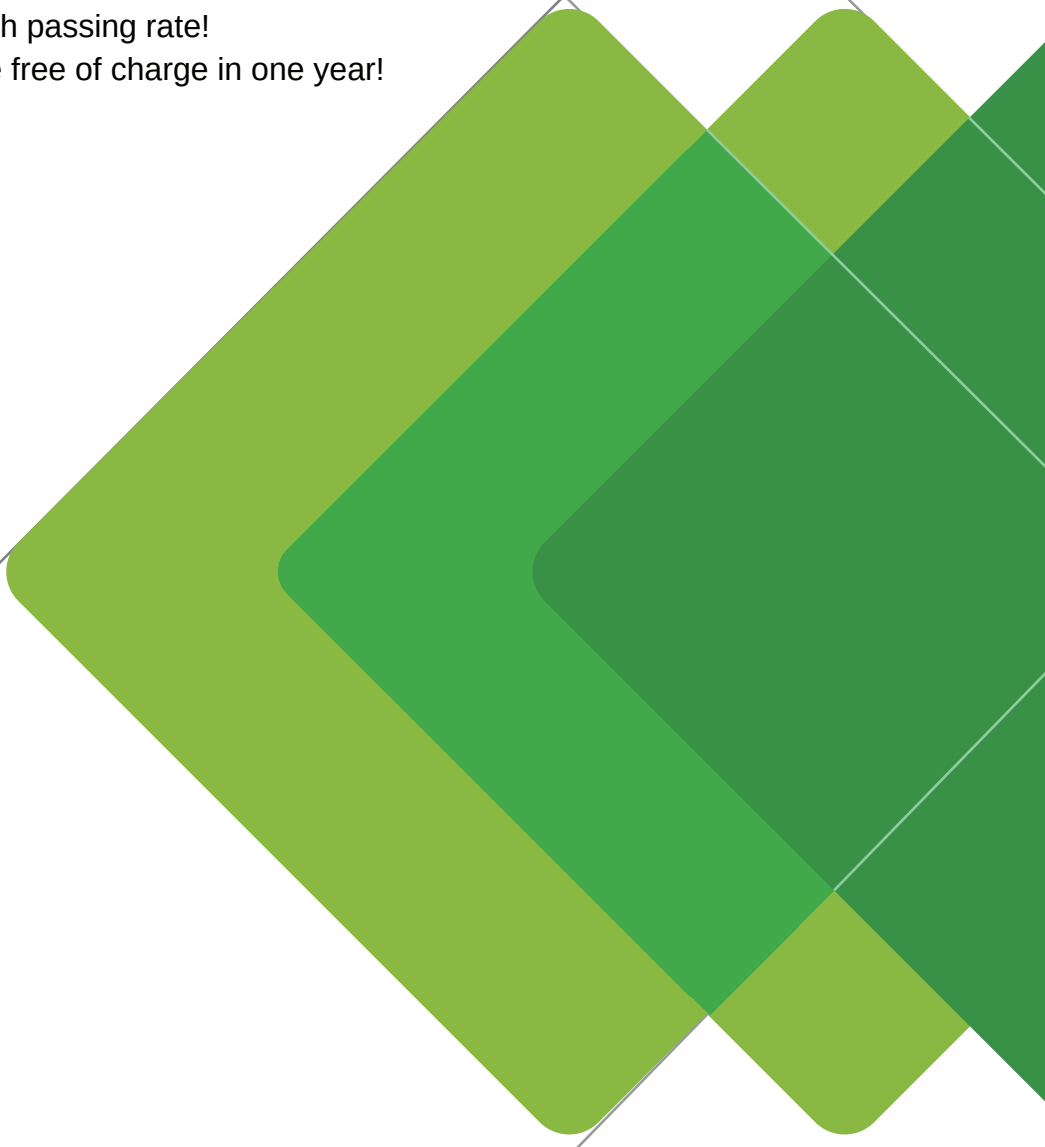
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!



Exam : **NO0-002**

Title : Nokia Security Administrator

Version : DEMO

1.What are the advantages of an external syslog server Vs data log files (Choose three):

A. External backup of logs in case of malicious activity
B. Guaranteed delivery of logs
C. Multiple indexing and searching of logs
D. Ability to see more information and select what outputs including internal facility and severity fields?
E. Allows a user to see Object ID
Answer: A,C,D
Incorrect answers:
B - There is no guarantee of delivery. The NAP could be down, or the syslog daemon failed.
E - You will not see Object ID's. What you would be able to see is the remote device IP and hostname.

2.You want to live messages in the log file. What command would you use via clish (Choose one):

A. Vi -e /var/log/messages
B. Tail -200 /var/db/messages
C. Tail - t /var/log/messages |more
D. Fw log -nft
E. Tail -f /var/log/messages
Answer: E
Tail -f views messages in real-time. Fw log views the Firewall connection logs in real-time

3.What commands can display interface statistics (Choose one):

A. Ifconfig -a (iclid)
B. Ipconfig -a (clish)
C. Show interface (clish)
D. Ifconfig -a (clish)
E. Show interface (iclid)
Answer: D, E

4.When using voyager what will make permanent changes after a reboot (Choose one):

A. Clicking apply
B. Clicking apply and then save
C. Saving changes from advanced fw config
D. Clicking apply and rebooting the NAP

Answer: B
Clicking apply only saves changes to the running configuration. Which are overwritten at startup by /config/db/inital

5.To what location/directory does Voyager make changes
(Choose one):

A. /config/db
B. /conf/
C. /var/conf
D. /var/admin
Answer: A

6.You can no longer gain access to your Nokia firewall via secure communications. What command will give you access and reset http:

A. Voyager -e 0 80
B. Set voyager ssl-level 0
C. Apachd -0 httpd.conf
D. Set Httpd -r -s
Answer: A, B

7.User UID of 0 will give:

A. Admin permissions of root on the machine
B. Backup user permissions on the enforcement module
C. Monitor user permissions
Answer: A
Setting the UID of 0 from the Voyager or the CLI will give the same machine permissions as the root user on a Nokia IPSO device

8.What ICLID command will show the version of the OS:

A. Show running config
B. Copy run start
C. Show version
D. Fw Ver
Answer: C

9.Misuse is accepted as non-attack activity from inside the company itself:

A. False
B. True
Answer: B

10.The Default priority for VRRP:

A. 100
B. 10
C. 110
D. 1
Answer: A

11.At what value must the TTL for a VRRP packet be set to:

A. 250
B. 255
C. 10
D. 100
Answer: B

12.What are the correct duplex settings. Which gives the more complete answer.

A. Console - Half Duplex and Full Duplex for a Serial connection
B. Cat6 Always full duplex
C. Serial always full duplex
D. Full Duplex - Switch and Half Duplex - Hub
Answer: D
The most correct answer in this case would be Full Duplex for a switch, Half Duplex for a hub

13.The correct switch for single user mode from Boot manager on an IP440 is:

A. -s
B. Boot-p
C. b-f
D. -singlemode
Answer: A

14.What are invalid commands in the boot manager (Choose one):

A. Boot
B. Set-defaults
C. Ls
D. setRAID
E. setenv
Answer: D

15.Commands to terminate an ICLID session are:

A. Close
B. Exit
C. Stop
D. Quit
Answer: B, D

16.'What is correct of DNS and hostfiles on IPSO (Choose all that apply):

A. The hostfile is located in /etc/resolv.conf
B. Can use a hostfile if DNS is disabled
C. Checkpoint uses when retrieving policy with Checkpoint Policy Provider
D. A hostname must be an FQDN
E. Required for Checkpoint Licencing
Answer: A, B, D, E

17.What is not true of DNS on IPSO with Checkpoint NG (Choose one):

A. Checkpoint needs this in case of domain usage in policy
B. Reduces the number of hostname file assignments (less IP's required to be entered manually)
C. Requires least one host entry of the machine itself, for Checkpoint
D. DNS must be enabled at startup for the NAP to function correctly
Answer: D

18.What is the location of the hosts file on IPSO (Choose one):

A. /var
B. /var/config
C. /etc/hosts
Answer: C

19.What is the correct flow of data on a NAP. Consider there is a fresh installation of Checkpoint NG installed (Choose the best answer):

A. Wire - Ethernet Driver - FWrulebase - Routing- NAT- Ethernet Driver -Wire
B. Wire - Ethernet Driver -FW rulebase&NAT - Routing- FW1- Ethernet Driver- Wire
C. Wire - FW Rulebase - Routing - NAT - Ethernet Driver - Wire
D. Wire - FW1rulebase - NAT - Routing - Ethernet Driver - Wire
Answer: B

20.What command will allow you to view the current connections table (Choose two):

A. fw tab -t connections -s
B. fwconn -i
C. fwtable -i
D. cpconntab -t
Answer: A, C