Exam #3 CNSE M55 (Ch 11 to 15)

Candidate: Ethan Bonavida (suborange)
Date: 12/10/2022 8:23:36 pm • **Time Spent:** 28:20

Score: 100%

Question 1: ✔ Correct

Which of the following commands would allow you to see whether a remote computer is reachable?

- ipconfig
- **ping**
- ifconfig
- ip addr ping
- netstat

Explanation

ping is a useful utility used to test whether a remote computer is reachable via a TCP/IP network. **ping** sends an ICMP packet to a remote host requesting a reply.

ifconfig and **ip addr** are commands that allow you to view and set interface specific network information such as IP addresses and subnet masks. They do not help you test connectivity. (**ip addr** does not have a ping option.)

ipconfig is not a Linux command; it is a Microsoft Windows command used to view IP address settings.

netstat is not used to test connectivity. **netstat** displays information about your local computer's network connections.

References

12.2.6 Network Configuration Facts

q_net_trb_lp5_01.question.fex

Question 2: ✔ Correct

What is the full path to the directory that contains log files, including secure, messages, [application], and kern.log?

/var/log ✔

Explanation

The /var/log directory contains log files, including secure, messages, [application], and kern.log.

- /var/log/secure logs any attempts to log in as the root user or attempts to use the **su** command.
- /var/log/messages is the default file for storing system messages on systems running init.
- /var/log/[application] stores application specific log entries.
- /var/log/kern.log store kernel specific log entries.

References

11.1.2 Log File Facts

q_log_com_f_01.question.fex

Question 3: ✔ Correct

Which network service would you use to get the IP address from the Fully Qualified Domain Name (FQDN) hostname?

- NAT
- DHCP
- FTP
- ➡ DNS

Explanation

Use the Domain Name System (DNS) to get the IP address from a given host name. The fully qualified domain name (FQDN) is the full DNS name for the computer.

Use DHCP to assign IP address and other configuration information to hosts automatically. Use FTP to transfer files. Use NAT to connect a private network to the internet.

References

1.1.4 Server Roles Facts

12.5.1 Hostname and DNS Configuration

q_dns_lp5_10.question.fex

Question 4: ✔ Correct

For Linux systems where physical access could be compromised, which of the following best practices should be implemented to prevent a user from booting into single user mode with root access?

- ➡ ◉ Set a bootloader password.
- ○ Separate sensitive data from the operation system.
- ○ Set a UEFI/BIOS password.
- ○ Disable Ctrl+Alt+Delete.

Explanation

A best practice is to set a password in a bootloader such as GRUB. These passwords help prevent others from booting to Linux, entering single user mode, and compromising the system.

References

15.12.1 Security Best Practices

15.12.2 Security Best Practices Facts

q_sec_prac_lp5_boot_pswd.question.fex

Question 5: ✔ Correct

What does the **netstat -a** command show?

- All network users
- ➡ All listening and non-listening sockets
- All listening sockets
- All connected hosts

Explanation

The **netstat -a** command shows the status of all listening and non-listening sockets.

References

15.4.3 Network Security Facts

q_netsec_f_lp5_01.question.fex

Question 6: ✔ Correct

Which utility would you use to view current connections and active sessions and ports on a computer?

- **nslookup**
- **netstat**
- **ip route**
- **ipconfig**

Explanation

netstat shows IP-related statistics, including:

- Current connections
- Incoming and outgoing connections
- Active sessions, ports, and sockets
- The local routing table

ipconfig displays IP configuration information for network adapters. Use **ipconfig** to view IP address, subnet mask, and default gateway configuration. Use **ipconfig /all** to view detailed configuration information including the MAC address and the DHCP server used for configuration.

nslookup resolves (looks up) the IP address of a hostname. **ip route** shows the routes in the routing table.

References

12.7.4 Troubleshooting Tool Facts

q_net_trb_lp5_05.question.fex

Question 7: ✔ Correct

What do you enter at the command prompt to prevent the shell from using too much of the system's resources?

ulimit ✔

Explanation

Use **ulimit** to limit computer resources used for applications launched from the shell. Limits can be hard or soft limits. Soft limits can be temporarily exceeded up to the hard limit setting. Users can modify soft limits, but only root can modify hard limits. Options include the following:

- **-c** limits the size of a core dump file. The value is in blocks.
- **-f** limits the file size of files created using the shell session. The value is in blocks.
- **-n** limits the maximum number of open files.
- **-t** limits the amount of CPU time a process can use. This is set in seconds.
- **-u** limits the number of concurrent processes a user can run.
- **-d** limits the maximum amount of memory a process can use. The value is in kilobytes.
- **-H** sets a hard resource limit.
- **-S** sets a soft resource limit.
- **-a** displays current limits. The default shows soft limits.

References

15.2.5 User Security Facts

q_usr_restrict_lp5_04.question.fex

Question 8: ✔ Correct

A technician executed a command that collects various OS usage statistics, provides report capability, and saves system activity information. Which of the following commands produced the following output?

```
Linux 3.10.0-957.5.1.el7.x86_64 (centos7.localdomain)   02/28/2019      _x86_64_        (1 CPU)

02:10:02 PM     CPU     %user     %nice   %system   %iowait    %steal     %idle
02:20:01 PM     all      1.07      0.00      0.41      0.03      0.00     98.49
02:30:01 PM     all      0.09      0.00      0.13      0.03      0.00     99.75
02:40:01 PM     all      0.38      0.08      0.35      0.02      0.00     99.18
02:50:01 PM     all      0.08      0.00      0.12      0.01      0.00     99.79
03:00:02 PM     all      0.71      0.00      0.25      0.02      0.00     99.01
Average:        all      0.47      0.02      0.25      0.02      0.00     99.25
```

- free
- vmstat
- **sar**
- iostat

Explanation

sar collects CPU usage, memory usage, swap space usage, overall I/O activity, individual device I/O, and network statistics.

iostat reports CPU statistics and input/output for devices and partitions but does not produce the output.

free displays information about the total amount of free and used physical and swap memory. It does not show other information in the output.

vmstat displays information about processes, memory, paging, block I/O, traps, disks, and CPU activity.

References

11.2.3 Resource Monitoring Facts

q_res_mon_lp4_sar.question.fex

Question 9: ✔ Correct

Out of concern for security, you convinced your boss to stop allowing Telnet access to the network. Now, remote connections are only made through ssh.

Which port must you allow through the firewall for ssh access?

- 22
- 23
- 24
- 25

Explanation

ssh uses port 22 by default.

References

12.1.8 IP Port Facts

q_com_port_lp5_01.question.fex

Question 10: ✔ Correct

Which of the following describes the function of the **export** command?

- Makes the command history available to a child process.
- Spawns a new subshell for command execution.
- ➡ Sets environment variables.
- Makes a mount point available to a remote server.

Explanation

The **export** command sets or converts a shell variable into an inheritable environment variable.

References

- 2.5.1 Environment Variables
- 2.5.2 Manage Environment Variables
- 2.5.3 Environment Variable Facts
- 14.1.1 Bash Scripting Overview
- 14.1.2 Bash Script Execution
- 14.2.1 Bash Shell Environments and Shell Variables
- 14.2.2 Bash Shell Parameters, User Variables and Expansions
- 14.2.3 Bash Shell Variables and Parameters
- 14.2.4 User Variables and Shell Arithmetic
- 14.2.5 Arrays and Expansions
- 14.2.6 Shell Environments, Bash Variables and Parameters Facts

q_env_var_param_lp5_export.question.fex

Question 11: ✔ Correct

Which is the most correct description for 3DES?

- 3DES is a very secure mode of the DES algorithm encryption method that encrypts data three times using a 168-bit key.
- 3DES means running the DES algorithm three times for maximum encryption.
- 3DES is derived from Microsoft's Windows Encrypted File System (EFS).
- 3DES is a third-generation version of DES, the Data Encryption Standard cipher.

Explanation

3DES is a secure mode of the DES algorithm that encrypts data with three different 56-bit keys in three different encryption passes (for a total of 168 key bits). 3DES is not derived from Microsoft's EFS. Running a DES algorithm three times is not the same as 3DES. 3DES does not mean it is the third generation of DES.

References

15.12.1 Security Best Practices

15.12.2 Security Best Practices Facts

q_encrypt_type_stand_lp5_01.question.fex

Question 12: ✔ Correct

There are two types of hypervisors, Type 1 and Type 2.

Which of the following describes those two types? (Choose TWO.)

- [x] A type 2 hypervisor runs on an operating system.
- [ ] A type 1 hypervisor is a software application that runs on top of a conventional operating system.
- [x] A type 1 hypervisor runs on bare metal hardware and is referred to as a native hypervisor.
- [ ] A type 2 hypervisor is an operating system that runs the hypervisor as a dedicated system.

Explanation

A Type 1 hypervisor runs on bare metal hardware and is referred to as a native hypervisor. Microsoft Hyper-V and VMware ESX are examples of a Type 1 hypervisor.

A Type 2 hypervisor runs on an operating system such as Windows, MacOS, or Linux. VMware Workstation, Oracle VM VirtualBox, Parallels Desktop for Mac, and open source QEMU are examples of Type 2 hypervisors.

References

13.1.1 Cloud and Virtualization Overview: Part 1

13.1.3 Install Hypervisor

13.1.4 Linux Cloud and Virtualization Facts

q_virt_lp5_hypervisor_types.question.fex

Question 13: ✔ Correct

Which of the following commands shows failed login attempts on the system?

- **lastb**
- **sar**
- **lastlog**
- **tail**

Explanation

lastb shows all failed login attempts on the system.

lastlog shows a list of the dates and times for the last login for each user.

sar views system statistics.

tail shows the last 10 lines of a file.

References

11.1.7 Log File Display Facts

q_log_com_f_lp5_lastb.question.fex

Question 14: ✔ Correct

When using templates to deploy virtual machines, one challenge is that all VMs will have the same settings, such as hostname, security identifiers, and even the same IP address.

Which of the following allow a VM to be provisioned with unique settings and configurations?

- OVA template
- OVF template
- bootstrapping
- container images

Explanation

Bootstrapping is the automated process of provisioning a virtual machine with unique settings and configurations. Bootstrapping customizes a virtual machine during installation (or, more specifically, when the virtual machine first boots) without requiring user input.

A container image is used to create multiple similar containers when copied, each running the same applications.

An OVF and OVA template will not provide unique settings when provisioning a VM.

References

13.2.2 Virtual Machine Concepts: Part 2

13.2.4 Virtual Machine Facts

q_virt_mach_lp5_bootstrapping.question.fex

Question 15: ✔ Correct

Anna, a system administrator, created a new virtual machine that she would like to provision on additional hypervisors.

Which of the following will provide a VM template that is open and can be used by hypervisors from different vendors?

- OVF
- XEN
- .vmx
- .vmdk

Explanation

OVF stands for Open Virtualization Format and provides an open standard to package virtual machine files for use on other systems as a template for creating a virtual machine.

.vmx is a hypervisor file format.

.vmdk is a hypervisor file that represents a disk drive.

XEN is a Type 1 hypervisor.

References

13.2.1 Virtual Machine Concepts: Part 1

13.2.4 Virtual Machine Facts

q_virt_mach_lp5_ovf.question.fex

Question 16: ✔ Correct

You are an application developer. You are writing a program to exchange video files through a TCP/IP network. You need to select a transport protocol that will guarantee delivery.

Which TCP/IP protocol would you implement that provides this capability?

- TFTP
- RIP
- IP
- TCP
- UDP

Explanation

Write the application to use the Transmission Control Protocol (TCP). TCP guarantees delivery through error checking and acknowledgments.

References

12.1.2 IP Protocol Facts

q_ports_f_lp5_03.question.fex

Question 17: ✔ Correct

A script developer is working on some new features for the administering Linux servers and wants to add the features without changing the master branch.

Which of the following is the BEST command to use?

- **git branch**
- **git merge**
- **git config**
- **git pull**

Explanation

git branch is used to list all the local branches in the current repository and allows a branch from the master.

git config is used to set the author name and email address to be used for commits.

git merge is used to merge a specified branch's history into the current branch.

git pull is used to get and merge the changes on the remote server to the local directory.

References

- **14.4.1 Git Concepts**
- **14.4.2 Installing Git**
- **14.4.3 Using a Git Repository**
- **14.4.4 Version Control Using Git Facts**

q_ver_ctrl_git_lp5_branch.question.fex

Question 18: ✔ Correct

When creating a bash script, it is important to document the purpose of the script.

Which of the following is a valid comment?

- // Comment text
- $ Comment text
- # Comment text
- !! Comment text

Explanation

Comments begin with a number sign (#). The shell ignores these lines when running the script. Comments help communicate how the script was constructed and what it is designed to do.

// will return the error "Is a directory."

$ and !! will both return the error "Command not found."

References

14.1.1 Bash Scripting Overview

14.1.4 Scripting Facts

q_script_lp5_comment.question.fex

Question 19: ✔ Correct

You have logged in as a regular user when a frantic phone call comes in. The ABCD process must be started on the server now, but can only be run by root.

Which command would you use to start this process?

- **sudo ABCD**
- **su ABCD**
- **exit ABCD**
- **ABCD /root**

Explanation

Use the **sudo** utility to run the specified utility as the superuser (root). This same task can be accomplished with the command **su -c ABCD**, but not with **su ABCD** (which attempts to change you to a user named ABCD).

References

15.1.4 root User Facts

q_usrrootu_lp5_02.question.fex

Question 20: ✔ Correct

You need to block all users from logging in to the Linux system while you resolve a serious issue. You first need to force all active users to logout.

Which command should you enter to display a list of all active users?

w ✔

Explanation

Use the **w** command to view all active user accounts. Administrators can prevent users from logging in to a Linux computer while resolving serious issues and can display a message to users who attempt to log in. To force all users to log out of the system:

1. Log in directly as the root user.
2. Use the **w** command to view all active user accounts.
3. Use **pkill -KILL -u *user*** to force the user to log out for each active user.

References

15.3.3 Login Blocking Facts

q_login_sec_f_lp5_03.question.fex

Question 21: ✔ Correct

You have used **su** to switch to the root user account to do system administration tasks. Now you want to revert back to your regular user account.

Which command should you use?

- **logoff**
- **off**
- **exit**
- **break**

Explanation

Use the **exit** command to terminate the su shell and revert back to the user you previously logged in as.

References

15.1.4 root User Facts

q_usrrootu_lp5_03.question.fex

Question 22: ✔ Correct

Mary, a technician, is troubleshooting memory and performance issues on a system. Mary executed a command to show information about processes, memory, paging, block IO, traps, disks, and CPU activity.

Which of the following commands did Mary use to produce the output below?

```
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 3  0      0 3238656   2280 920816    0    0   324    60    5  347  4  4 92  0  0
 0  0      0 3238624   2280 920816    0    0     0     0    1  156  2  0 98  0  0
 0  0      0 3238672   2280 920816    0    0     0     0    0  145  1  0 98  0  0
 0  0      0 3239764   2280 920444    0    0     0     2    5  131  1  1 99  0  0
 0  0      0 3239896   2280 920444    0    0     0     5    1  152  1  0 98  0  0
```

- top
- **vmstat**
- iostat
- free

Explanation

vmstat displays information about processes, memory, paging, block I/O, traps, disks, and CPU activity.

free displays information about the total amount of free and used physical and swap memory. It does not display other information.

iostat reports CPU statistics and input/output for devices and partitions, but does not produce the output shown.

top reports dynamic information on system processes, but does not produce this output.

References

8.4.3 Swap Area Management

q_res_mon_lp5_vmstat.question.fex

Question 23: ✔ Correct

Which of the following commands manages, compresses, renames, and deletes log files based on a specific criteria such as size or date?

- **logrotate**
- **dmesg**
- **lastlog**
- **logger**

Explanation

logrotate manages, compresses, renames, and deletes log files based on specific criteria (such as size or date).

lastlog shows a list of the dates and times for the last login for each user.

logger changes the message severity and where logged messages are sent.

dmesg views the boot logs and troubleshoots hardware errors. The **dmesg** command shows information about all the hardware controlled by the kernel and displays error messages as they occur.

References

11.1.9 logrotate Facts

q_logs_lp5_logrotate.question.fex

Question 24: ✔ Correct

When implementing a network gateway, implementing a firewall, or increasing performance, multiple NICs can be added to a computer.

Which of the following can be implemented on VMs to provide this capability?

- A bridged network
- An switch in isolated mode
- ➡ Dual-homed NICs
- An overlay network

Explanation

Physical computers can have multiple NICs connected to multiple subnets to increase performance, use the computer as a network gateway, or use the computer as a network firewall. Virtual machines can also be configured as a multi-homed system with multiple virtual NICs. Depending on your requirements, you can connect each NIC to a separate virtual switch or connect multiple NICs to a single virtual switch. You can link each physical NIC on the host machine to a different virtual switch, or you could link several physical NICs to one virtual switch.

References

13.2.3 Creating a Virtual Machine

13.3.1 Virtual Networking Concepts

13.3.2 Configuring Networking on a Virtual Machine

13.3.3 Virtual Networking Facts

q_virt_net_lp5_dual_homed.question.fex

Question 25: ✔ Correct

You are writing a bash script that lists the contents of a file. You would like to have any stderr messages sent to a file.

Which of the following commands will write the error message to a file?

- **cat projects 1> projects.err**
- **cat projects > projects.err**
- **cat projects 2>&1 projects.err**
- **cat projects 2> projects.err**

Explanation

cat projects 2> projects.err redirects *stderr* to *projects.err*.

cat projects > projects.err redirects the output of the command to *projects.err*. It does not redirect *stderr* to the file.

cat projects 1> projects.err redirects the output to the file, not the stderr.

cat projects 2>&1 projects.err redirects *stderr* to *stdout* and displays any error on *stdout*. The file will not contain error messages.

References

14.1.4 Scripting Facts

14.3.1 Bash Scripting Logic

14.3.3 Exit Codes

14.3.5 Bash Scripting Logic Facts

q_script_logic_lp5_stderr.question.fex