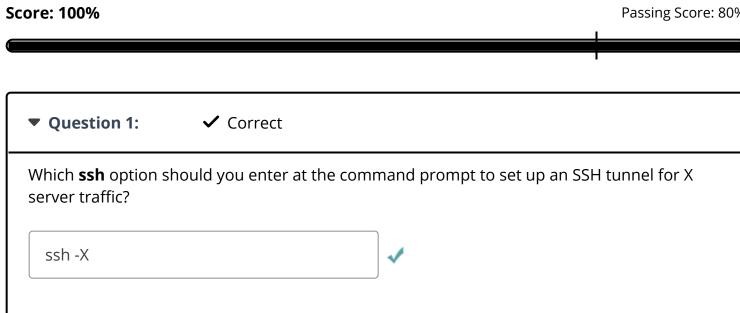
TestOut LabSim 12/9/22, 12:26 AM

# 15.7.4 Practice Questions

Candidate: Ethan Bonavida (suborange) Date: 12/9/2022 12:26:48 am • Time Spent: 00:42

Passing Score: 80%



# **Explanation**

Use **ssh** -X to set up an SSH tunnel from the client to the server for X server traffic. Be aware of the following options:

- -I specifies the username of the user account on the remote system.
- **server** specifies the server name and domain running the SSH daemon.

For example, ssh -X -I mtrance hn3.mydomain.com sets up an SSH port tunnel for X server traffic.

### References



q\_port\_tunn\_lp5\_01.question.fex

#### ✓ Correct **▼** Question 2:

What is the purpose of the **-N** option in the following command?

# ssh -f -N -L 2345:mail.mydomain.com:110 userbob@mail.mydomain.com

- To specify the port numbers and server name.
- To ensure that SSH does not execute a remote command.
  - To specify the default port for non-secure protocol.
  - To run SSH in the background after the password prompt.

# **Explanation**

ssh -N ensures that SSH does not execute a remote command. Among other tasks, use ssh to set up an SSH tunnel from the client to the server for textual traffic. Be aware of the following options:

- **-f** runs SSH in the background after the password prompt.
- **-N** ensures that SSH does not execute a remote command.
- **-L** specifies the port numbers and server name.
- **-g** overrides configuration file settings and creates a tunnel if needed.
- *tunnelport* specifies the SSH port for the encrypted data. Only the root user can set the SSH port to a privileged port (port 1024 or lower.)
- **server** specifies the server running the SSH daemon.
- **port** specifies the default port for non-secure protocol.

For example, ssh -f -N -L 2345:mail.mydomain.com:110 userbob@mail.mydomain.com sets up an SSH port tunnel for POP3 mail traffic over port 2345.

## References

15.7.3 SSH Port Tunneling Facts

q\_port\_tunn\_lp5\_02.question.fex

▼ Question 3: ✓ Correct
When configuring the SSH daemon using the <code>/etc/ssh/sshd_config</code> file, which options can be set to either prevent or allow unrestricted access to all GUI features on the client? (Select TWO).
AllowXServerForwarding
TrustX11
→ ✓ ForwardX11Trusted
XServerForwarding
→ X11Forwarding
Explanation
In the /etc/ssh/sshd_config file, the <b>X11Forwarding</b> or <b>ForwardX11Trusted</b> option (depending on which Linux distribution you are running) needs to be set to <i>yes</i> to allow unrestricted access to all GUI features on the client. This option should be set in the configuration file before the sshd.service is started. If the SSH deamon is already running, the sshd.service will need to be restarted before the configuration change will take effect.
References

15.7.3 SSH Port Tunneling Facts

q\_port\_tunn\_lp5\_03.question.fex



You would like to use SSH port tunneling to work on a remote system. You also need to ensure that all data that you send to the remote system is encrypted.

Which SSH configuration option, in the /etc/ssh/sshd\_config file, needs to be set yet to yes?

$\Rightarrow$	AllowTCPForwarding
	7 111 O T T T C T T O T T C T C T C T C T C T

- AllowSSHForwarding
- AllowSSHTunneling
- AllowTCPTunneling

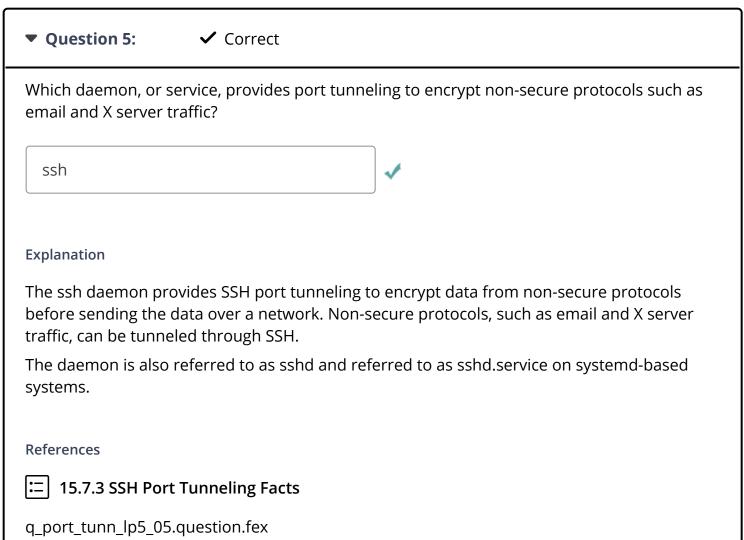
# **Explanation**

In the /etc/ssh/sshd\_config file, the AllowTCPForwarding option needs to be set to yes for SSH port tunneling to work. This option should be set in the configuration file before the sshd.service is started. If the SSH deamon is already running, the sshd.service will need to be restarted before the configuration change will take effect.

### References

15.7.3 SSH Port Tunneling Facts

q\_port\_tunn\_lp5\_04.question.fex



**Copyright © 2022 TestOut Corporation All rights reserved.**