Lab 15 - Using Public Key Encryption to Secure Messages

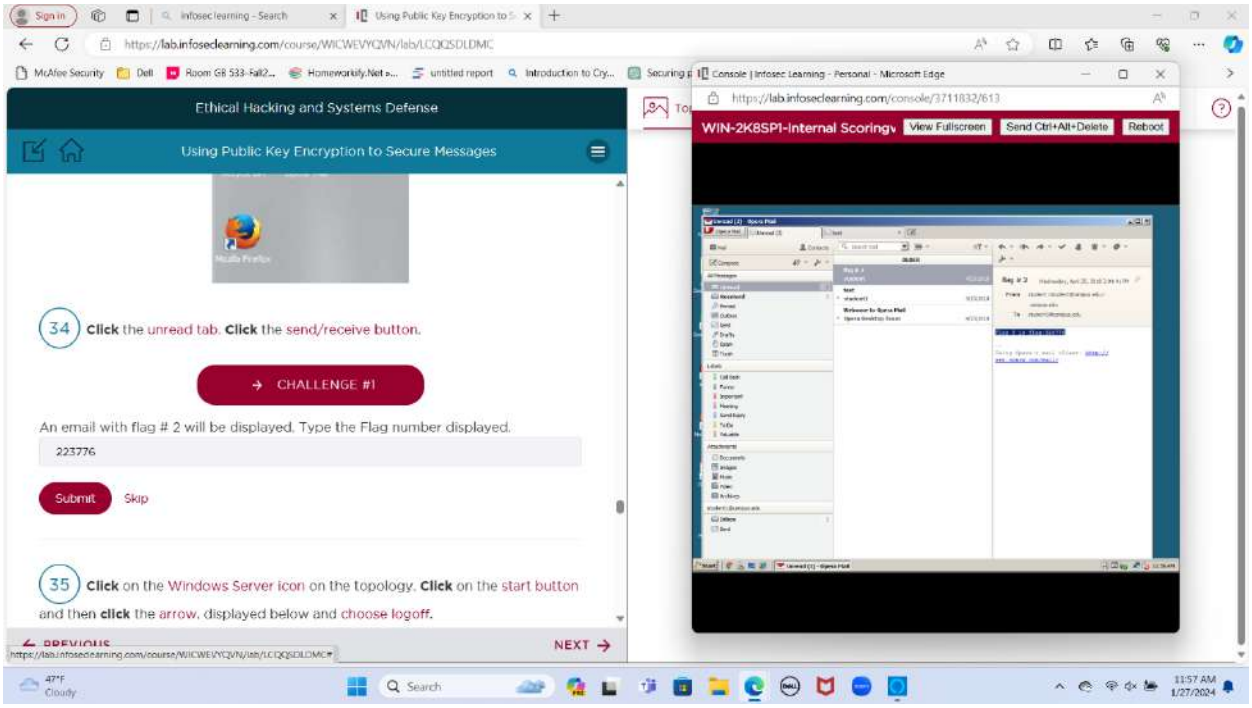
Objective:

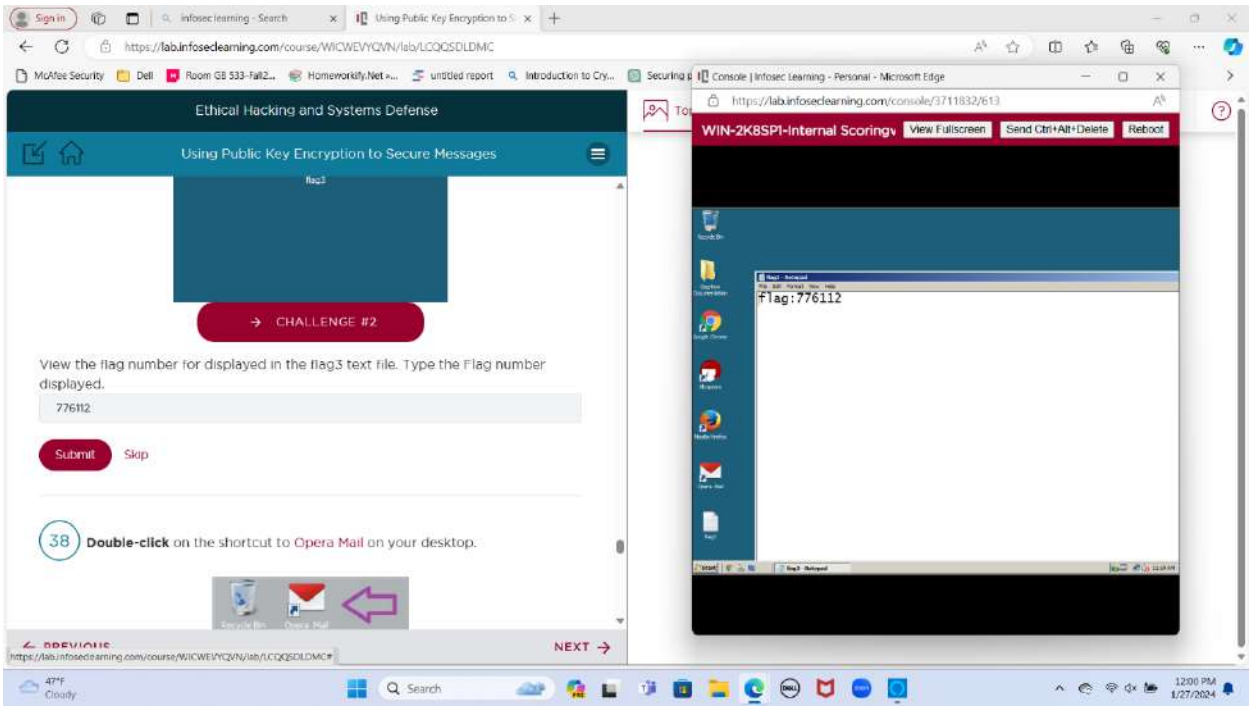
1. Creating the Certificate for Student
2. Creating the Certificate for Administrator
3. Encrypting and Decrypting the File

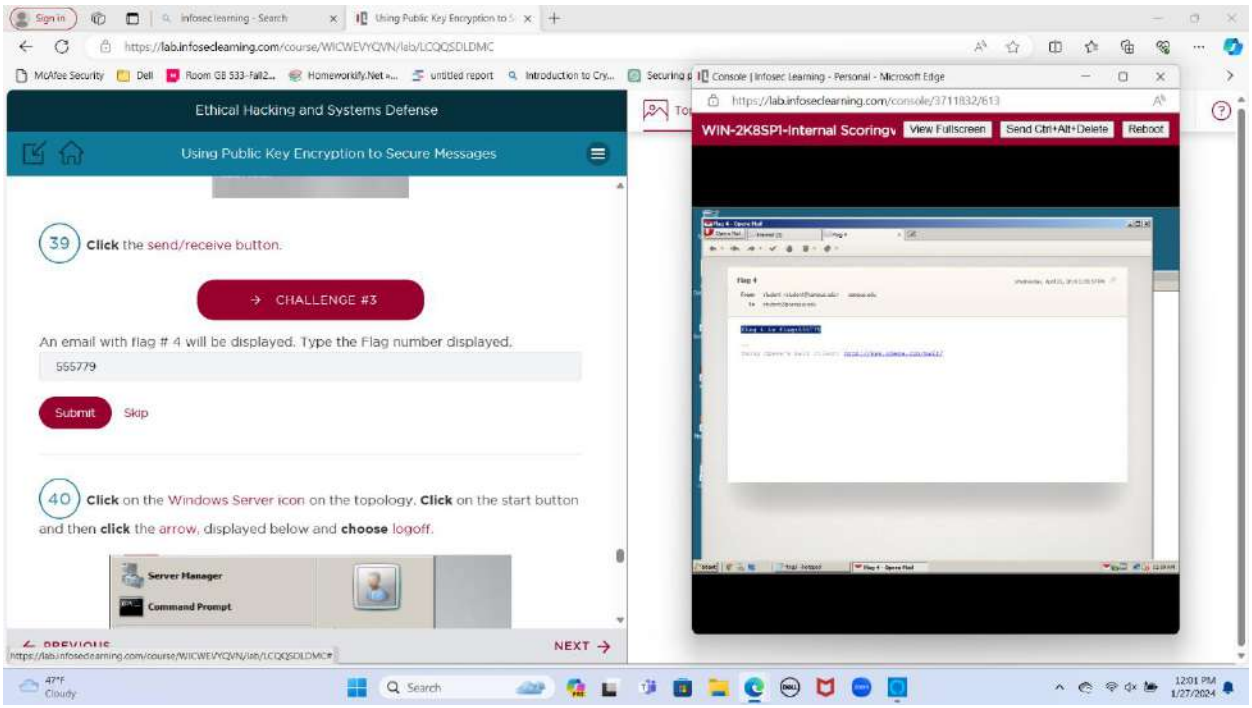
Takeaways:

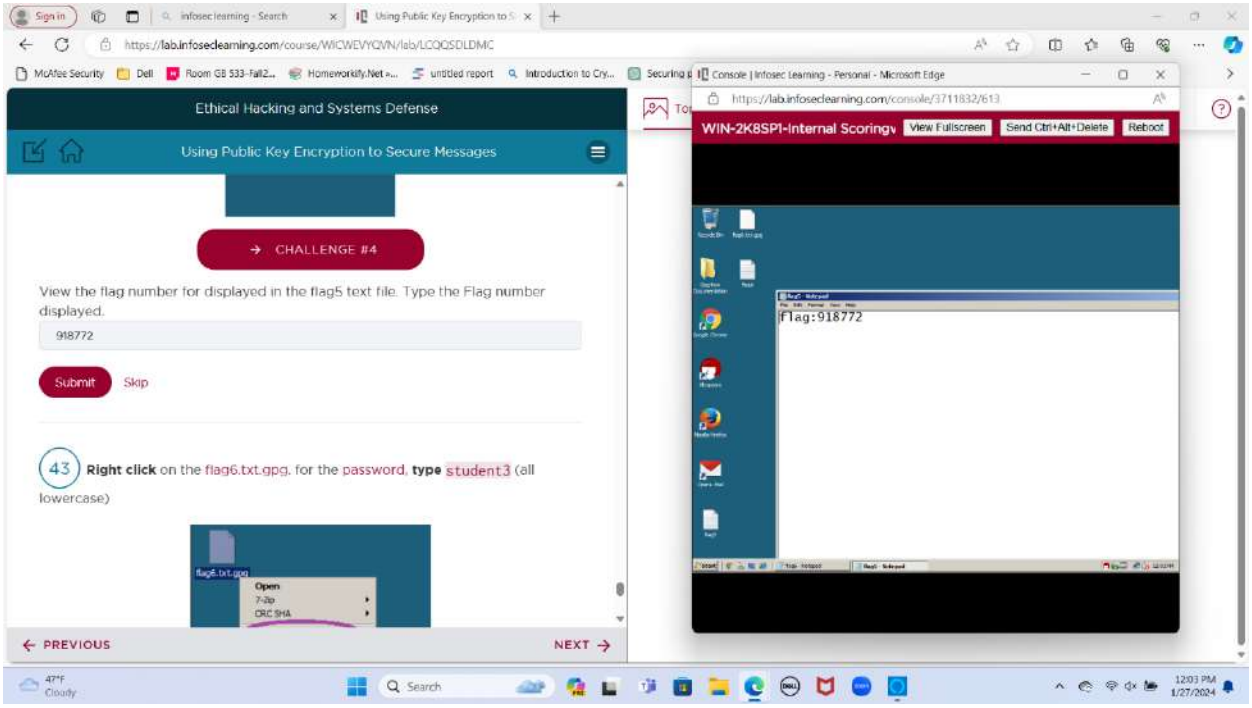
1. OpenPGP (Pretty Good Privacy) is an open-source encryption standard that enables secure and private communication using public-key cryptography for data encryption and digital signatures.
2. Kleopatra is a certificate manager and graphical user interface for GnuPG (GNU Privacy Guard), providing a user-friendly way to manage cryptographic keys and perform encryption-related tasks on Windows systems.
3. When creating a certificate, we are generating a digital document that includes a public key and information about the key owner, often used for secure communication, authentication, or digital signatures.
4. When encrypting a file, we typically use a symmetric key, which is a single secret key shared between the sender and recipient for both encryption and decryption.
5. When decrypting a file, we use the corresponding key to the one used for encryption, typically a symmetric key, to reverse the encryption process and reveal the original content.

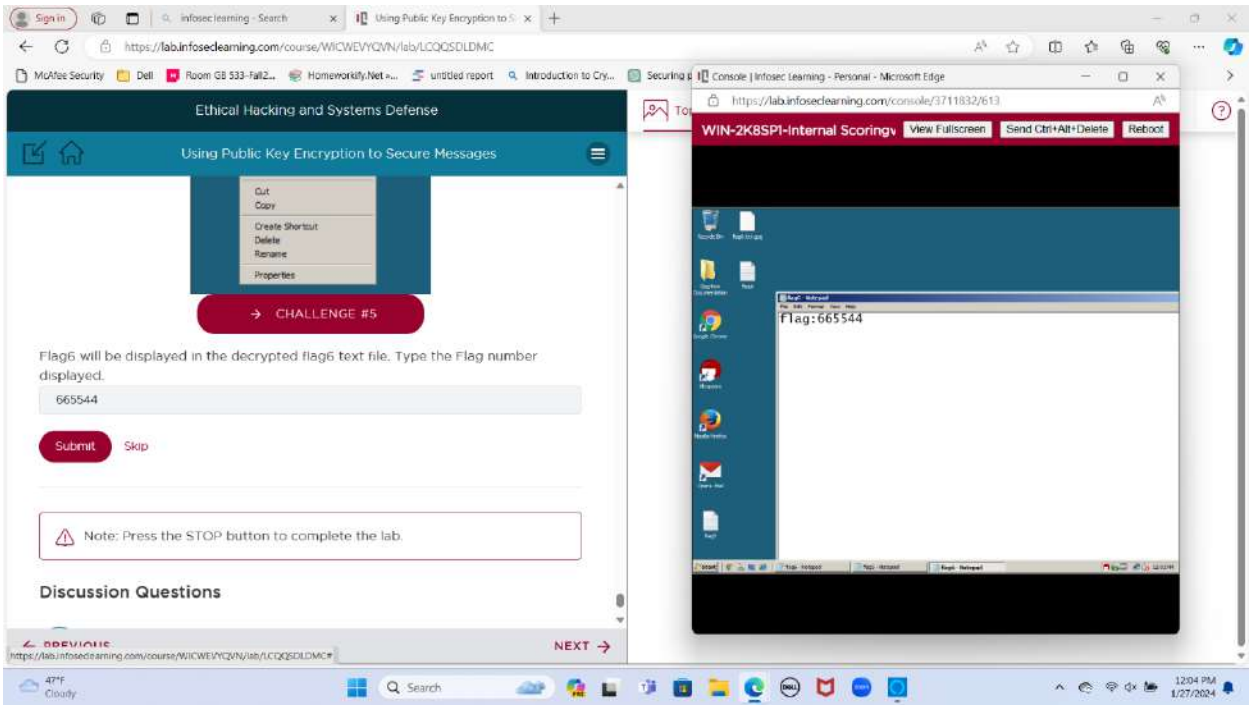
Challenges:


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
34 Click the unread tab. Click the send/receive button.
→ CHALLENGE #1
An email with flag # 2 will be displayed. Type the Flag number displayed.
223776
Submit
Skip
35 Click on the Windows Server icon on the topology. Click on the start button and then click the arrow, displayed below and choose logoff.
NEXT →
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

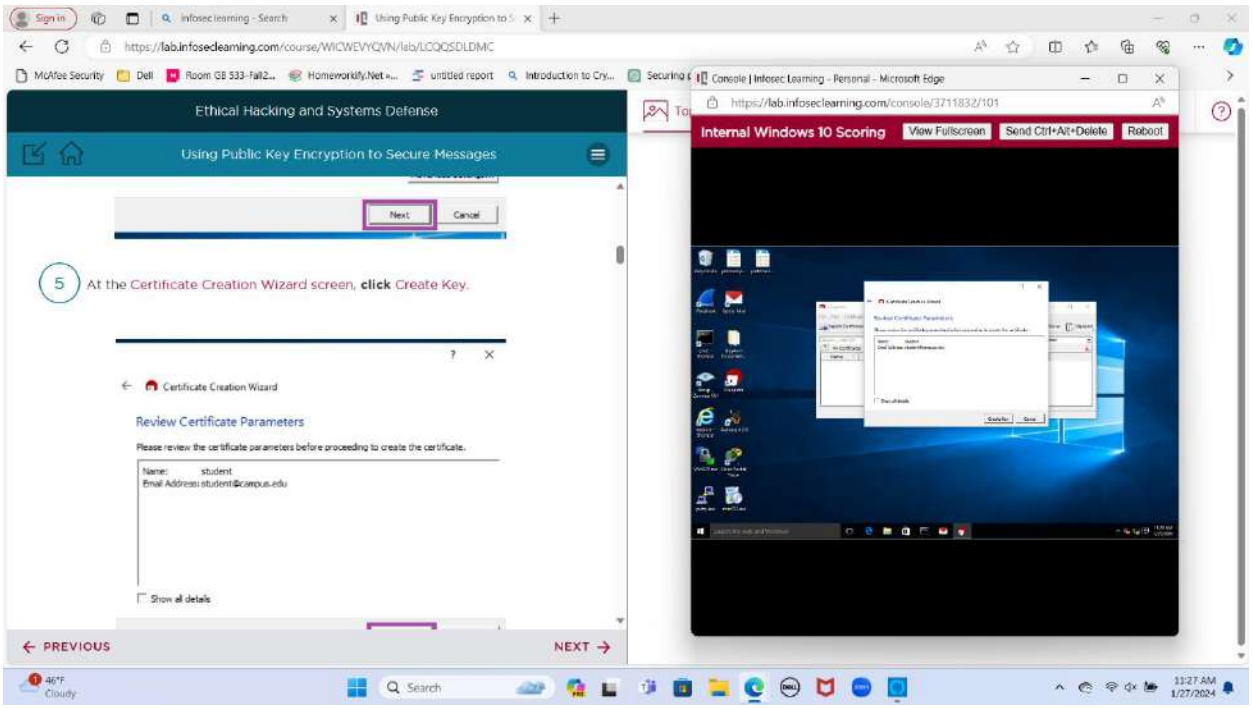

Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
flag3
→ CHALLENGE #2
View the flag number for displayed in the flag3 text file. Type the Flag number displayed.
776112
Submit
Skip
38 Double-click on the shortcut to Opera Mail on your desktop.
NEXT →
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
flag:776112

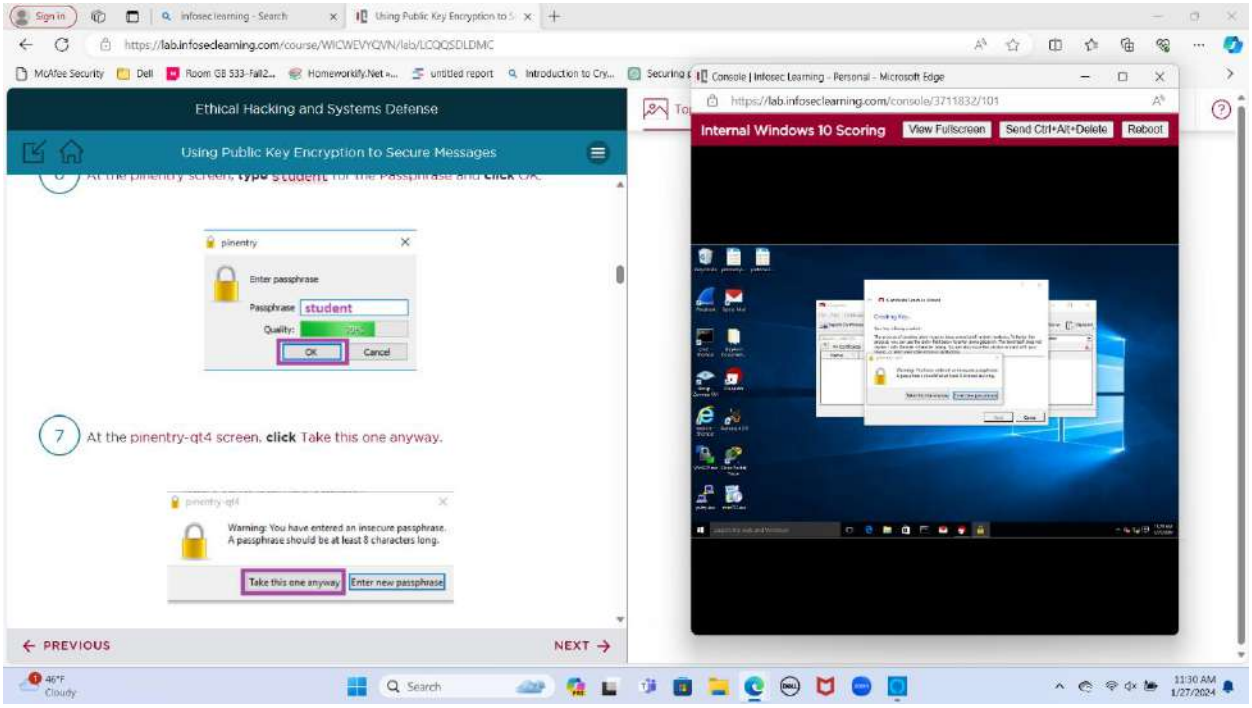

Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
39 Click the send/receive button.
→ CHALLENGE #3
An email with flag # 4 will be displayed. Type the Flag number displayed.
555779
Submit
Skip
40 Click on the Windows Server icon on the topology. Click on the start button and then click the arrow, displayed below and choose logoff.
Server Manager
Command Prompt
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecdearning.com/console/3711832/613
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

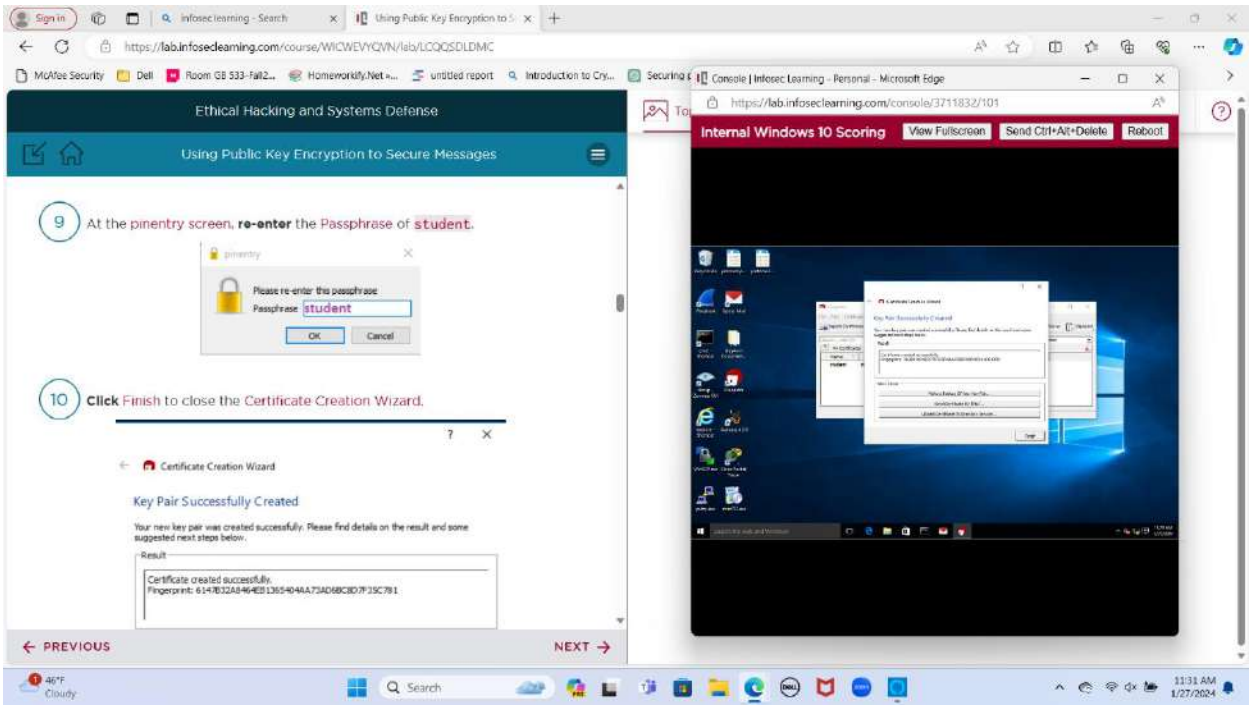

Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
→ CHALLENGE #4
View the flag number for displayed in the flag5 text file. Type the Flag number displayed.
918772
Submit
Skip
43 Right click on the flag6.txt.gpg, for the password, type student3 (all lowercase)
flag6.txt.gpg
Open
7-Zip
CRC SHA
← PREVIOUS
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecdearning.com/console/3711832/613
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Flag:918772

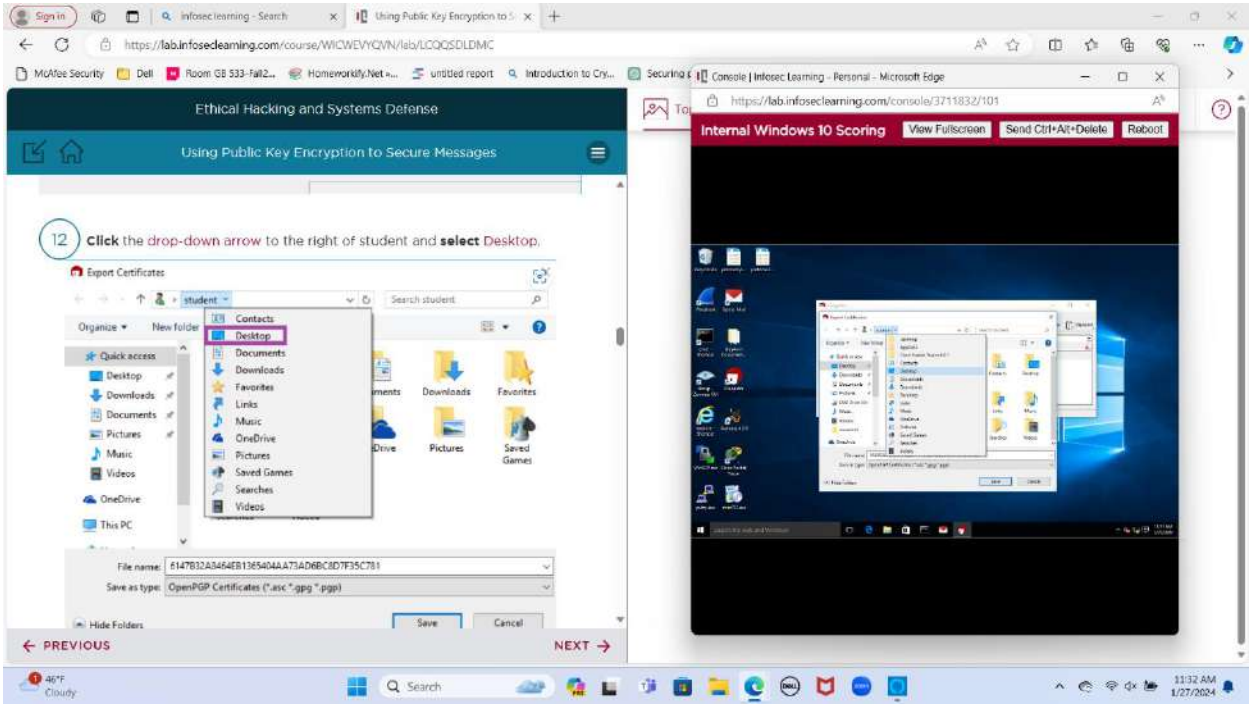


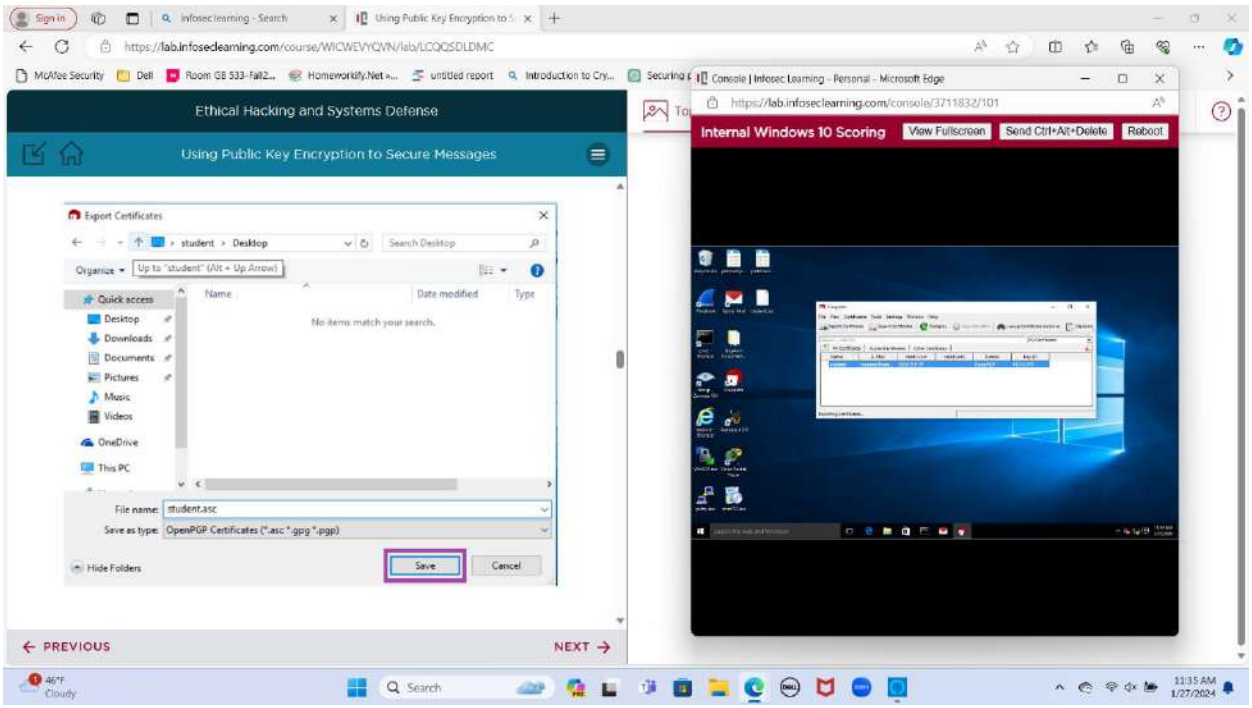
Screenshots:

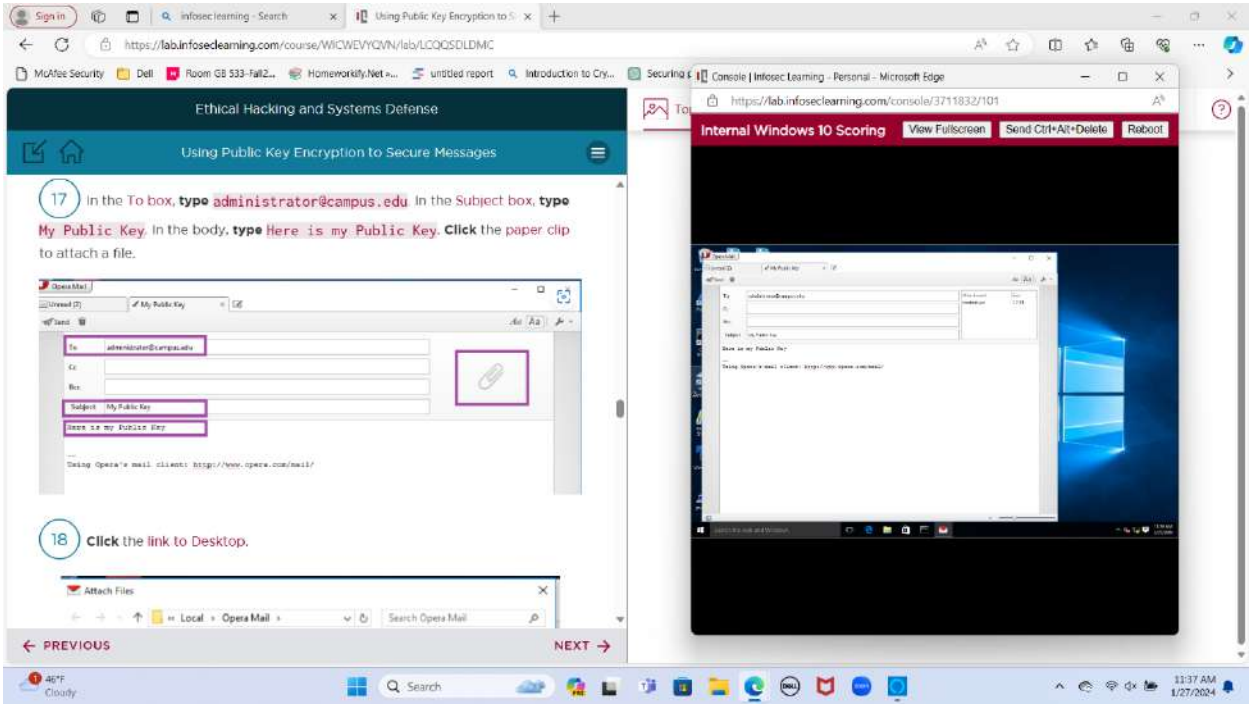

Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
Next
Cancel
5
At the Certificate Creation Wizard screen, click Create Key.
Certificate Creation Wizard
Review Certificate Parameters
Please review the certificate parameters before proceeding to create the certificate.
Name: student
Email Address: student@campus.edu
Show all details
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
pinentry
Enter passphrase
Passphrase student
Quality:
OK
Cancel
7
At the pinentry-qt4 screen, click Take this one anyway.
pinentry-qt4
Warning: You have entered an insecure passphrase.
A passphrase should be at least 8 characters long.
Take this one anyway
Enter new passphrase
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
9 At the pinentry screen, re-enter the Passphrase of student.
Please re-enter this passphrase
Passphrase: student
OK
Cancel
10 Click Finish to close the Certificate Creation Wizard.
Certificate Creation Wizard
Key Pair Successfully Created
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.
Result
Certificate created successfully.
Fingerprint: 6147B32A8464EB1365404AA73AD6BC8D7F35C781
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
12 Click the drop-down arrow to the right of student and select Desktop.
Export Certificates
student
Search student
Organize
New folder
Contacts
Desktop
Documents
Downloads
Favorites
Links
Music
OneDrive
Pictures
Saved Games
Searches
Videos
Quick access
This PC
File name: 6147B32A8464EB1365404AA73AD6BC8D7F35C781
Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)
Hide Folders
Save
Cancel
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
Export Certificates
student > Desktop
Search Desktop
Organize
Up to "student" (Alt + Up Arrow)
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Name
Date modified
Type
No items match your search.
File name: student.asc
Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)
Hide Folders
Save
Cancel
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
17 In the To box, type administrator@campus.edu In the Subject box, type My Public Key. In the body, type Here is my Public Key. Click the paper clip to attach a file.
18 Click the link to Desktop.
Attach Files
Local > Opera Mail
Search Opera Mail
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

21 **Click** on the Windows Server icon on the topology. After sending a control alt delete to the virtual machine, **log in** as `administrator` with the password of `P@ssw0rd`.

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

← PREVIOUS NEXT →

Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

23 **Type** the following command and **press** Enter to set the clock on the VM. When asked to set the clock, **type** Y.

C:\>`net time \\concord /set`

```
C:\>net time \\concord /set
Current time at \\concord is 9/15/2021 11:07:18 AM

The current local clock is 9/15/2021 3:15:05 AM
Do you want to set the local computer's time to match the
time at \\concord? (Y/N) [Y]: y
The command completed successfully.
```

24 **Double-click** on the shortcut to Opera Mail on your desktop.

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

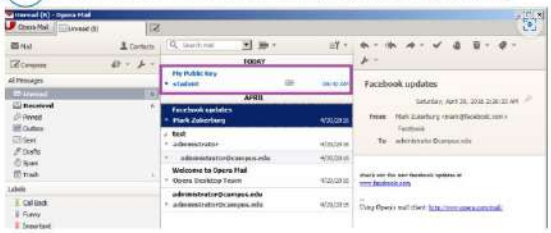
```
Microsoft Windows [Version 6.0.6001]
Copyright (C) 2006 Microsoft Corporation.  All rights reserved.

C:\>net time \\concord /set
Current time at \\concord is 1/27/2024 11:38:50 AM

The current local clock is 1/27/2024 11:38:50 AM
Do you want to set the local computer's time to match the
time at \\concord? (Y/N) [Y]: y
The command completed successfully.

C:\>
```

← PREVIOUS NEXT →

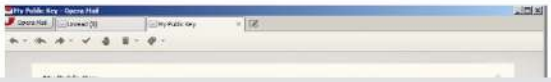
Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

26 **Double-click** on the email from student with the subject My Public Key.



27 **Click** the student.asc file and **select** Save As.

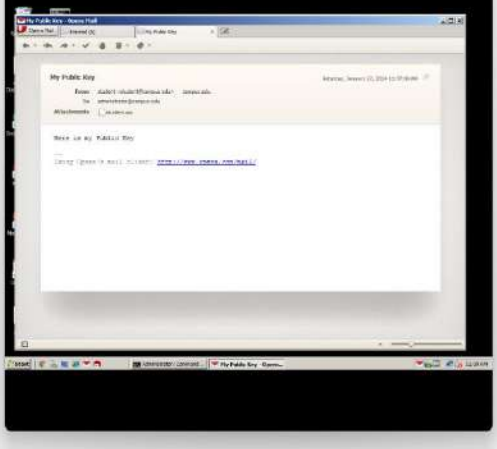


← PREVIOUS NEXT →

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv View Fullscreen Send Ctrl+Alt+Delete Reboot



Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

31 **Click** Opera Mail and then **select** Exit.

Discussion Questions

1 What is OpenPGP?

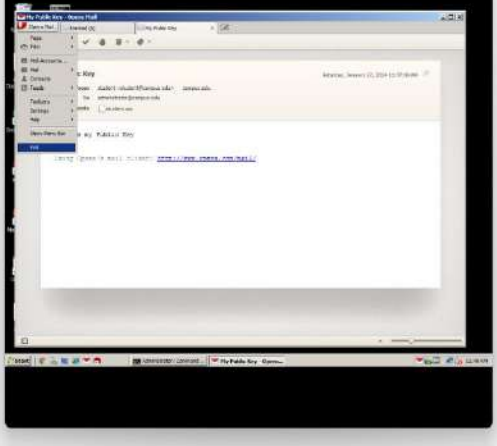
2 What is the application used to create a certificate for student?

← PREVIOUS NEXT →

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv View Fullscreen Send Ctrl+Alt+Delete Reboot



Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

2 From the Kleopatra menu, **select** File and **select** New Certificate.

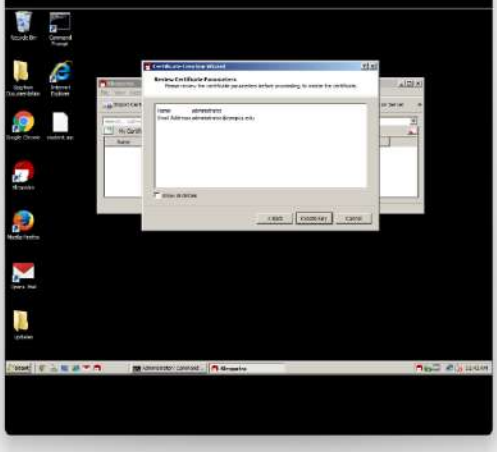
3 **Click** Create a personal OpenPGP key pair.

← PREVIOUS NEXT →

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv View Fullscreen Send Ctrl+Alt+Delete Reboot



Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

Take this one anyway Enter new passphrase

8 At the pinentry screen, **re-enter** the Passphrase of `administrator`

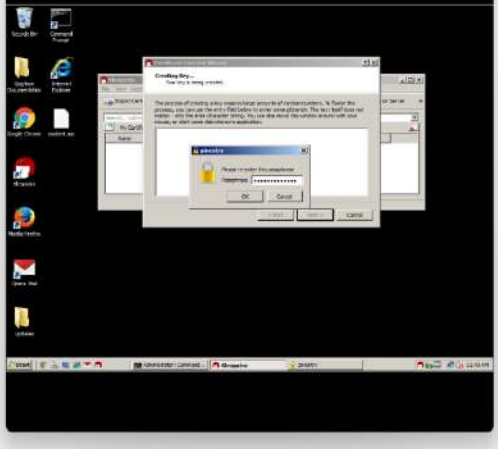
9 **Click** Finish to close the Certificate Creation Wizard.

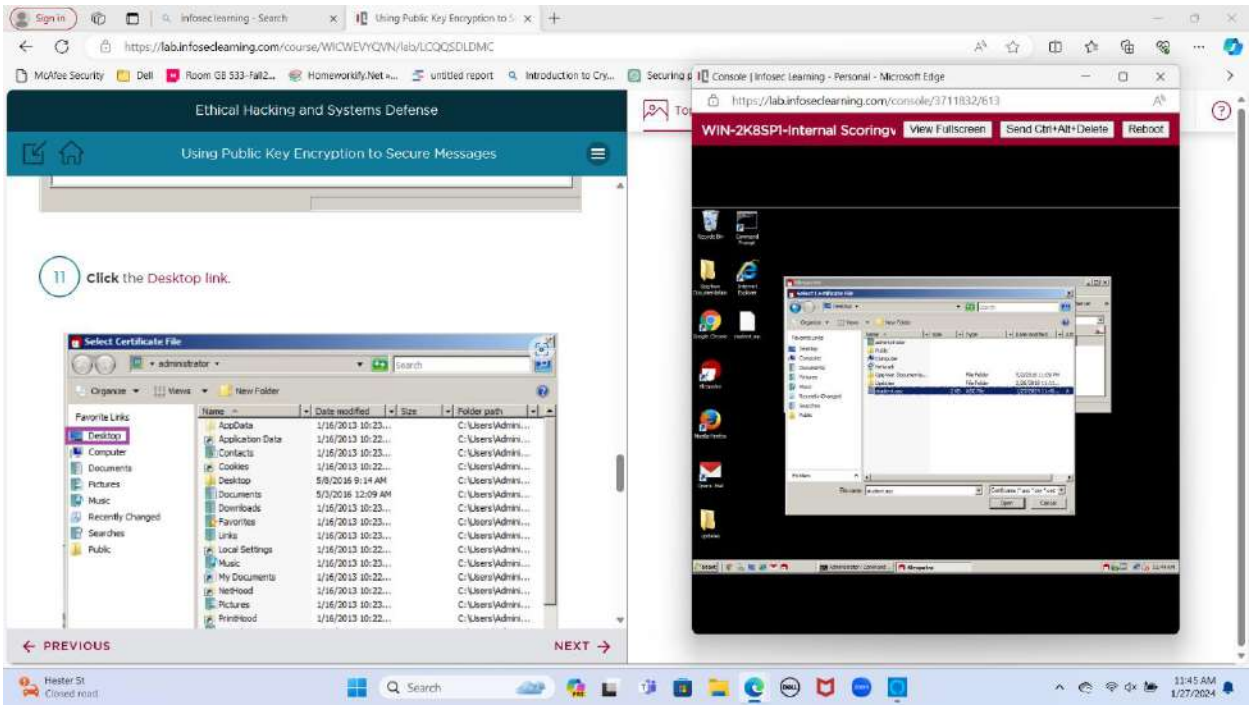
← PREVIOUS NEXT →

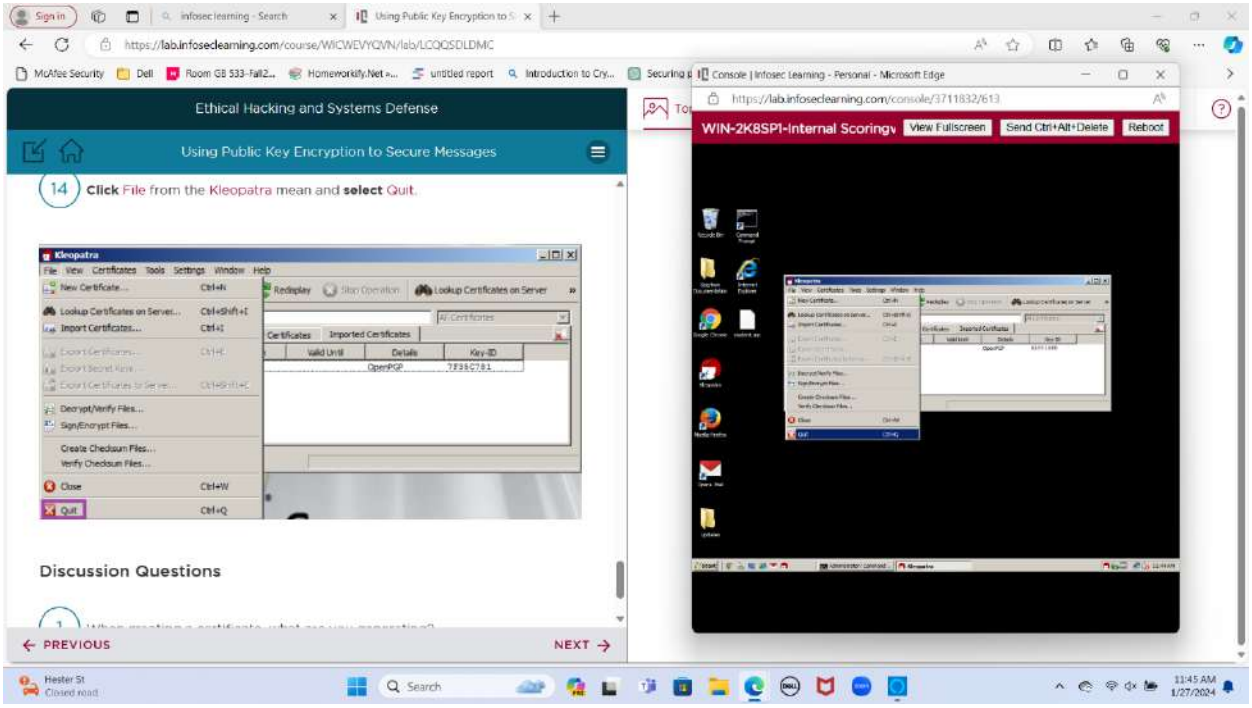
Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv View Fullscreen Send Ctrl+Alt+Delete Reboot




Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
11 Click the Desktop link.
Select Certificate File
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
14 Click File from the Kleopatra mean and select Quit.
Kleopatra
Discussion Questions
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
WIN-2K8SP1-Internal Scoringv
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

1 **Right-click** on the Windows Server desktop, **click** New then **select** Text Document.

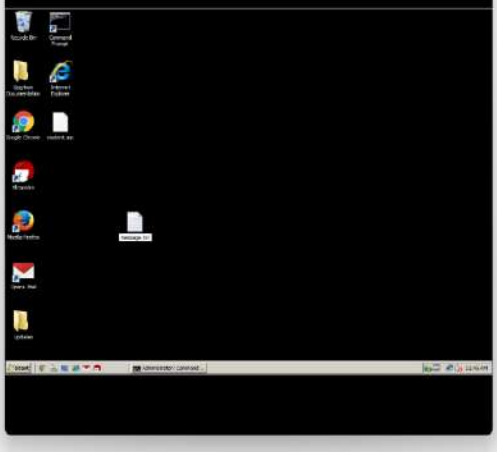
2 **Name** the file message.txt.

← PREVIOUS NEXT →

Console | Infosec Learning - Personal - Microsoft Edge

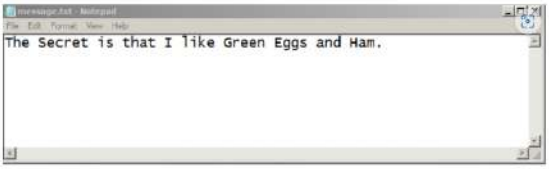
https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

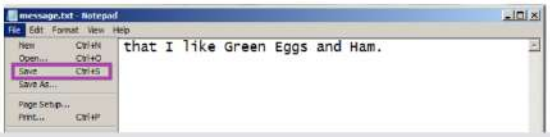


Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages



5 **Click** File from the Notepad menu and **select** Save.



← PREVIOUS NEXT →

Console | Infosec Learning - Personal - Microsoft Edge

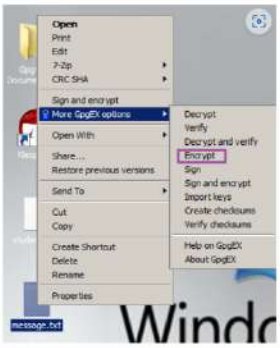
https://lab.infosecdearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

7 **Right-click** on message.txt and **select** More GpgEX options and then **select** Encrypt.

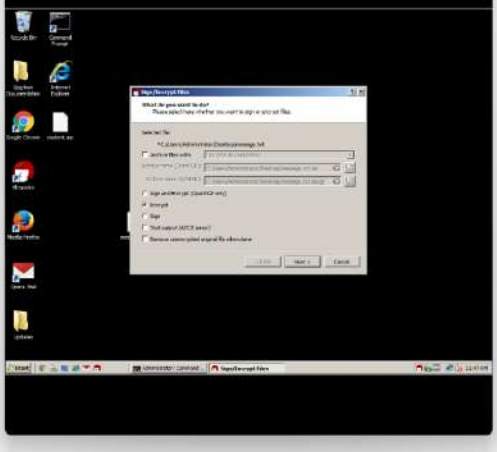


PREVIOUS NEXT

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecilearning.com/console/3711832/613

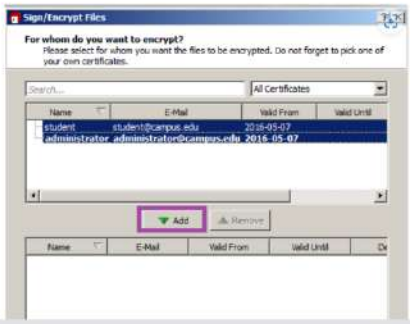
WIN-2K8SP1-Internal Scoringv View Fullscreen Send Ctrl+Alt+Delete Reboot



Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

9 **Hold down** Control to select the student and the administrator certificates. **Click** Add.

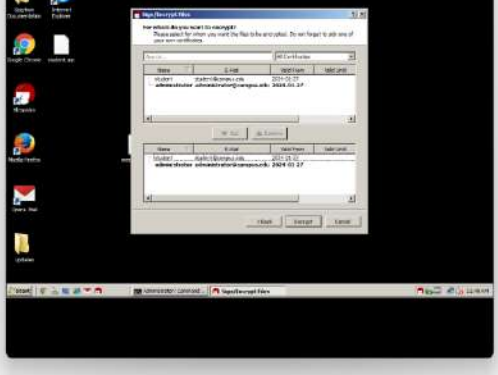


PREVIOUS NEXT

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infosecilearning.com/console/3711832/613

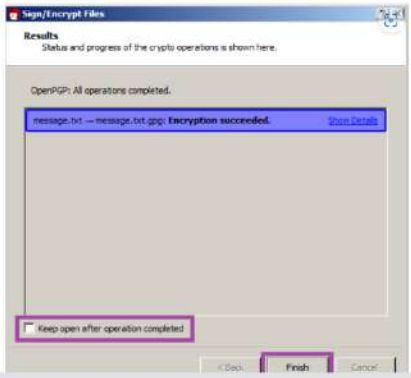
WIN-2K8SP1-Internal Scoringv View Fullscreen Send Ctrl+Alt+Delete Reboot



Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

11 You should see the message in blue that Encryption succeeded. **Remove** the check to Keep open after operation completed. **Click** the Finish button.

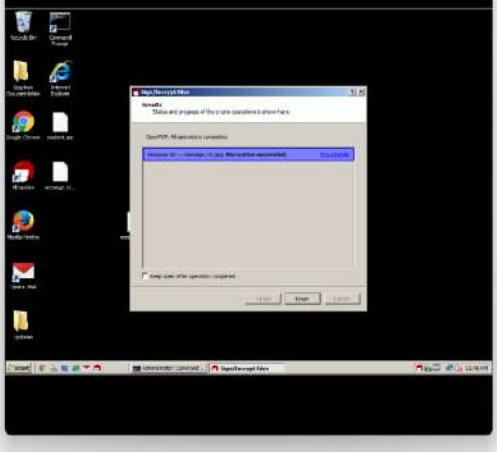


← PREVIOUS NEXT →

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3711832/613

WIN-2K8SP1-Internal Scoringv | View Fullscreen | Send Ctrl+Alt+Delete | Reboot



47°F Cloudy | Search | 11:49 AM 1/27/2024

Ethical Hacking and Systems Defense

Using Public Key Encryption to Secure Messages

16 **Click** the Send button to send the email.

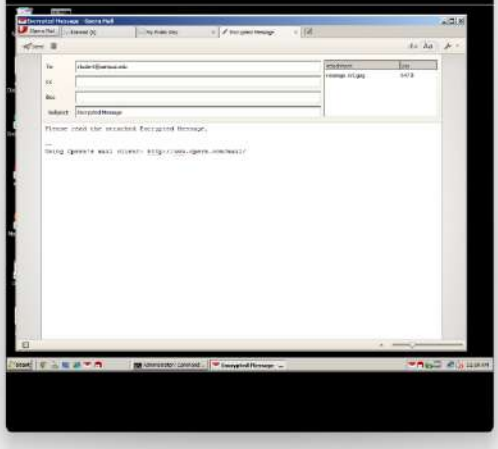
17 **Click** on the Windows 10 machine. If the Opera Mail program is not already open, **double-click** on the shortcut to Opera Mail.

← PREVIOUS NEXT →

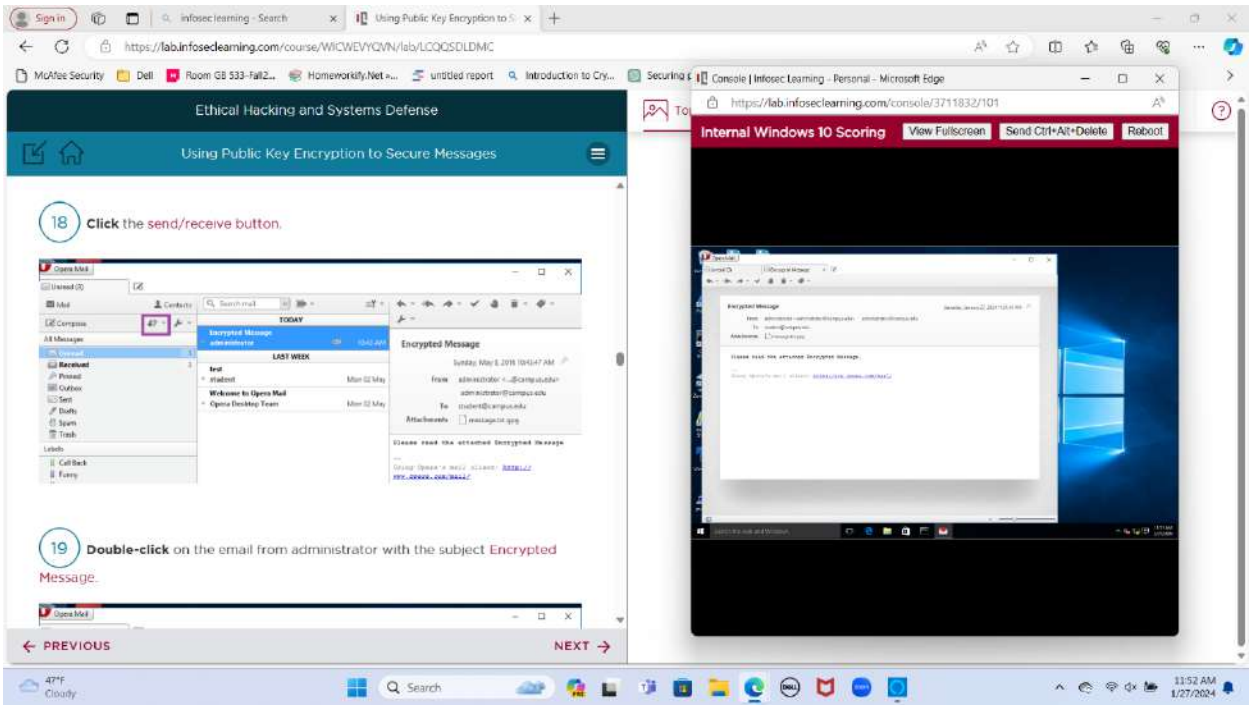
Console | Infosec Learning - Personal - Microsoft Edge

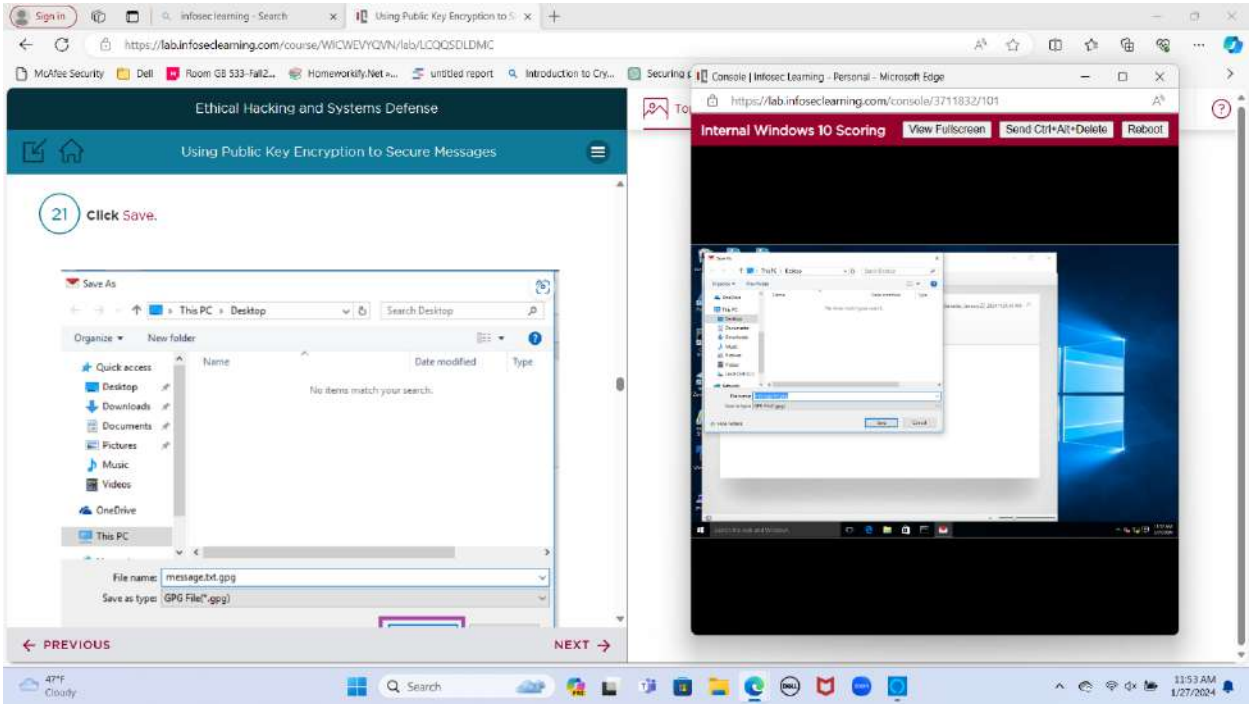
https://lab.infoseclearning.com/console/3711832/613

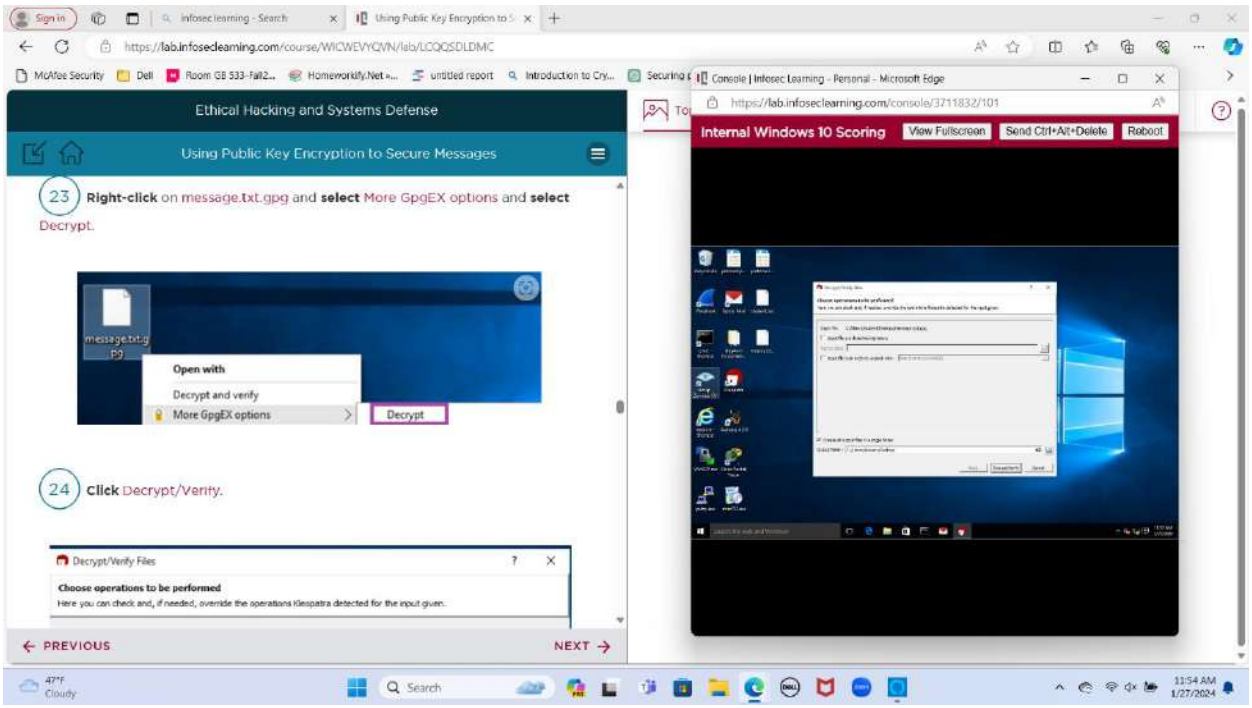
WIN-2K8SP1-Internal Scoringv | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

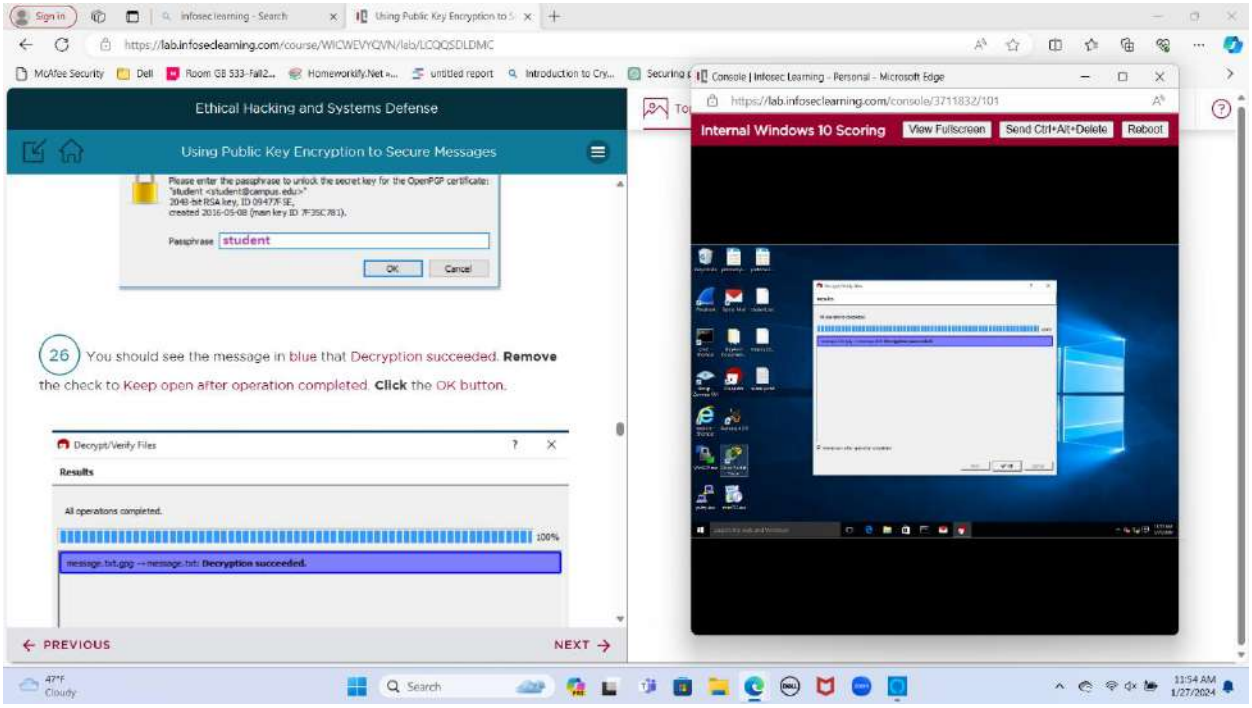


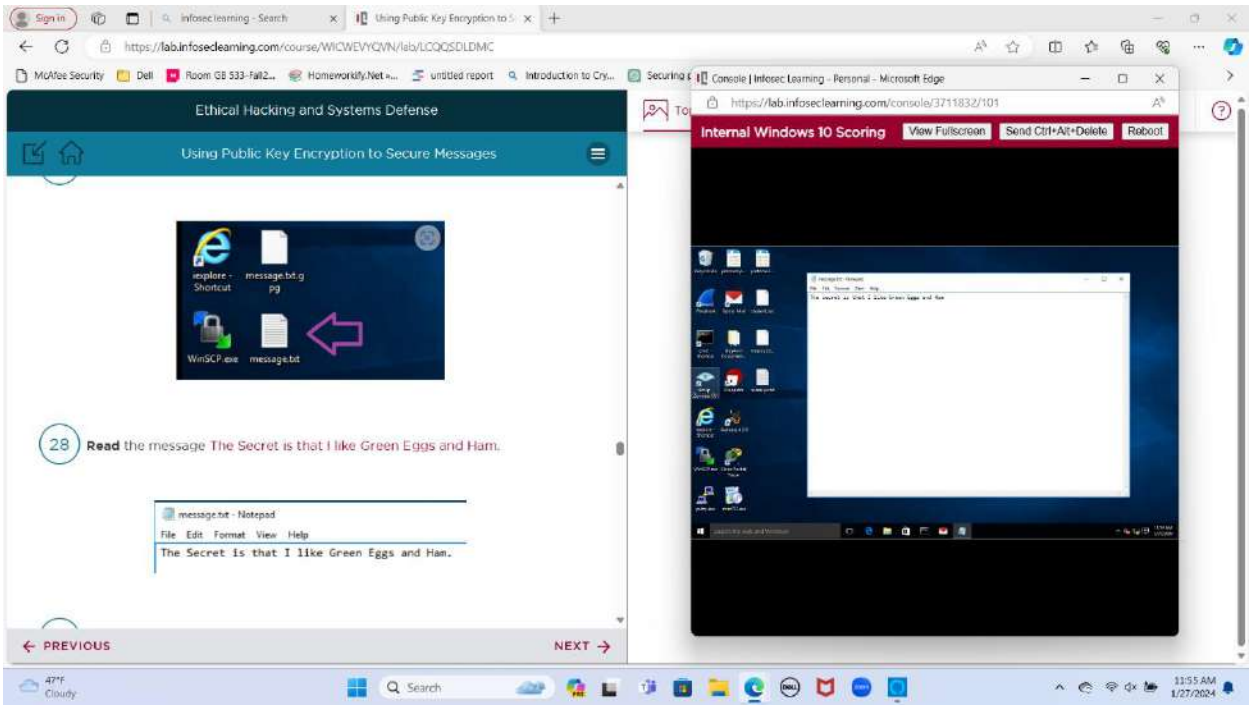
47°F Cloudy | Search | 11:51 AM 1/27/2024

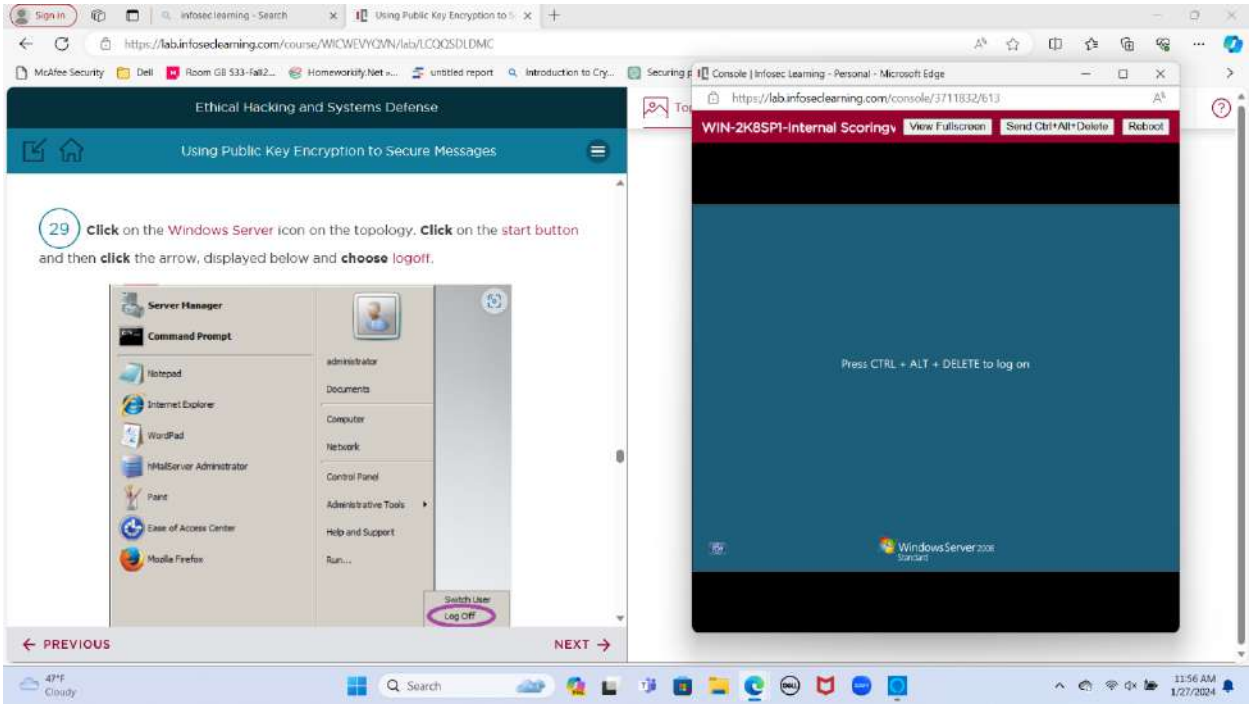

Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
18 Click the send/receive button.
19 Double-click on the email from administrator with the subject Encrypted Message.
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot

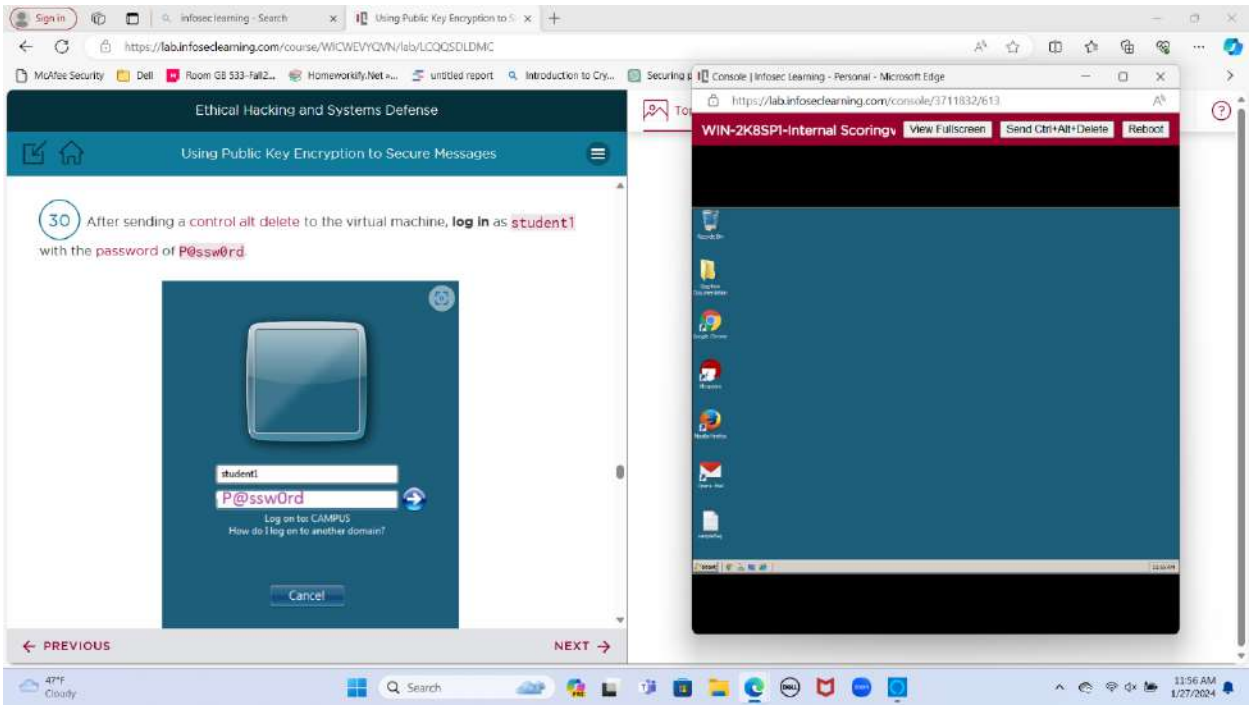

Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
21 Click Save.
Save As
This PC › Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Name
Date modified
Type
No items match your search.
File name: message.txt.gpg
Save as type: GPG File(*.gpg)
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3711832/101
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
23 Right-click on message.txt.gpg and select More GpgEX options and select Decrypt.
Open with
Decrypt and verify
More GpgEX options
Decrypt
24 Click Decrypt/Verify.
Decrypt/Verify Files
Choose operations to be performed
Here you can check and, if needed, override the operations Kleopatra detected for the input given.
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
Passphrase
student
OK
Cancel
26 You should see the message in blue that Decryption succeeded. Remove the check to Keep open after operation completed. Click the OK button.
Decrypt/Verify Files
Results
All operations completed.
100%
message.txt.gpg -- message.txt: Decryption succeeded.
PREVIOUS
NEXT
Console | Infosec Learning - Personal - Microsoft Edge
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
28 Read the message The Secret is that I like Green Eggs and Ham.
message.txt - Notepad
File Edit Format View Help
The Secret is that I like Green Eggs and Ham.
PREVIOUS
NEXT


Ethical Hacking and Systems Defense
Using Public Key Encryption to Secure Messages
WIN-2K8SP1-Internal Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
29 Click on the Windows Server icon on the topology. Click on the start button and then click the arrow, displayed below and choose logoff.
Server Manager
Command Prompt
Notepad
Internet Explorer
WordPad
hMailServer Administrator
Paint
Ease of Access Center
Mozilla Firefox
administrator
Documents
Computer
Network
Control Panel
Administrative Tools
Help and Support
Run...
Switch User
Log Off
Press CTRL + ALT + DELETE to log on
PREVIOUS
NEXT



This is the last screen before the end of this lab.