Windows security

Exercise 3 – Module 2 – Section 1

June 2020  
V1.1

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only, and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

This training uses various tools and utilities downloaded from the Internet for the classroom environment.   
Downloading any tools, installing and using them should only be done at your own risk security checked the tools in a test environment.

© 2020 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Contents

[Implementation of security mechanisms 1](#_Toc44075534)

[Abstract and learning objectives 1](#_Toc44075535)

[Overview 2](#_Toc44075536)

[Requirements 2](#_Toc44075537)

[Before the exercise 3](#_Toc44075538)

[List of VM to start 3](#_Toc44075539)

[How to start and connect to a VM 5](#_Toc44075540)

[Exercise 1: Prevent anonymous enumeration of accounts 7](#_Toc44075541)

[Task 1: Assess the existing 7](#_Toc44075542)

[Task 2: Remediate weak SAM remote configuration 7](#_Toc44075543)

[Task 3: Assess remediated configuration – part 1 9](#_Toc44075544)

[Exercise 2: Implement DACL 10](#_Toc44075545)

[Task 1: Assess the existing 10](#_Toc44075546)

[Task 2: Implement file permissions 10](#_Toc44075547)

[Exercise 3: Implement Audit 12](#_Toc44075548)

[Task 1: Implement Logon/Logoff auditing 12](#_Toc44075549)

[Task 2: Implement File Access auditing 13](#_Toc44075550)

[Task 3: Enable Registry auditing 14](#_Toc44075551)

[Task 4: Create an auditing GPO 14](#_Toc44075552)

[After the Lab 16](#_Toc44075553)

[Task 1: Stop and deallocated all the VMs 16](#_Toc44075554)

[Annex 1 – Wireshark 17](#_Toc44075555)

[Wireshark Panels 17](#_Toc44075556)

[Starting a capture 17](#_Toc44075557)

[Starting a capture with a filter 18](#_Toc44075558)

[Stop Capture 18](#_Toc44075559)

[Restart Capture 19](#_Toc44075560)

# Implementation of security mechanisms

## Abstract and learning objectives

This training is designed to train yourself in implementing some of the most important security mechanisms built into Windows.

At the end of this training, you will able to:

* Ensure anonymous enumeration of SAM accounts is not permitted
* Implement access control on files
* Implement audit strategies

## Overview

This lab exercise is a very simple environment consisting in a Windows 10 client and Windows Server 2016 servers. Both are member of an Active Directory domain seclab.local. The server provides fictious SMB share for users’ personal files and team projects.

## Requirements

1. Attendee’s machine:
   1. Ideal resolution 1920 x 1080
   2. An Internet browser
   3. An RDP client
   4. Internet access without restriction on outbound connections.   
      The following outbound TCP port must be accessible :

* **TCP/80 and TCP/443** to reach Azure Portal
* **TCP/3389** to establish RDP remote connection to virtual machines exposed directly to Internet

or

* **TCP/(49152 to 65535)** to establish RDP remote connection to virtual machines exposed by a Load Balancer

## Before the exercise

Duration: 10 minutes

Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

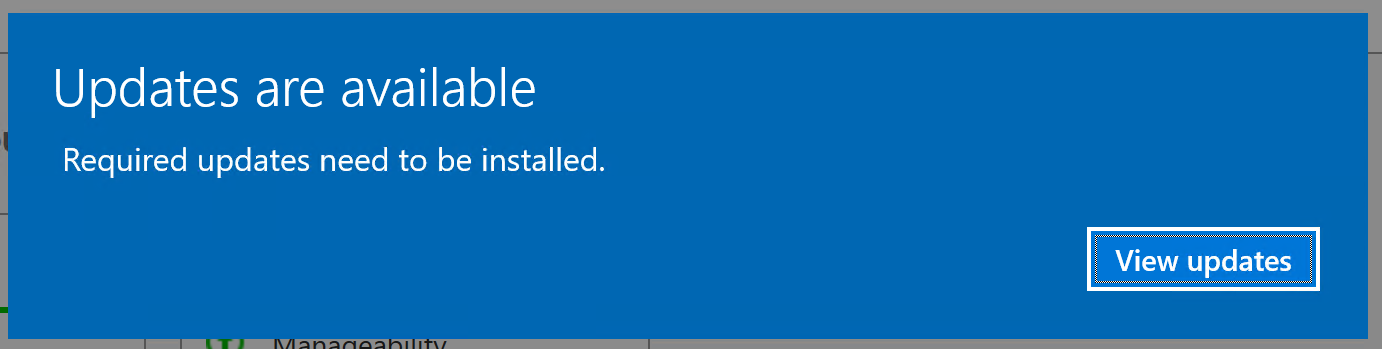
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| CSW2-WKS | CSW2-WKS | Windows 10 Enterprise | Workstation |
| CSW2-SRV | CSW2-SRV | Windows Server 2016 Datacenter | Server |
| CSW2-DC | CSW2-DC | Windows Server 2016 Datacenter | DC |

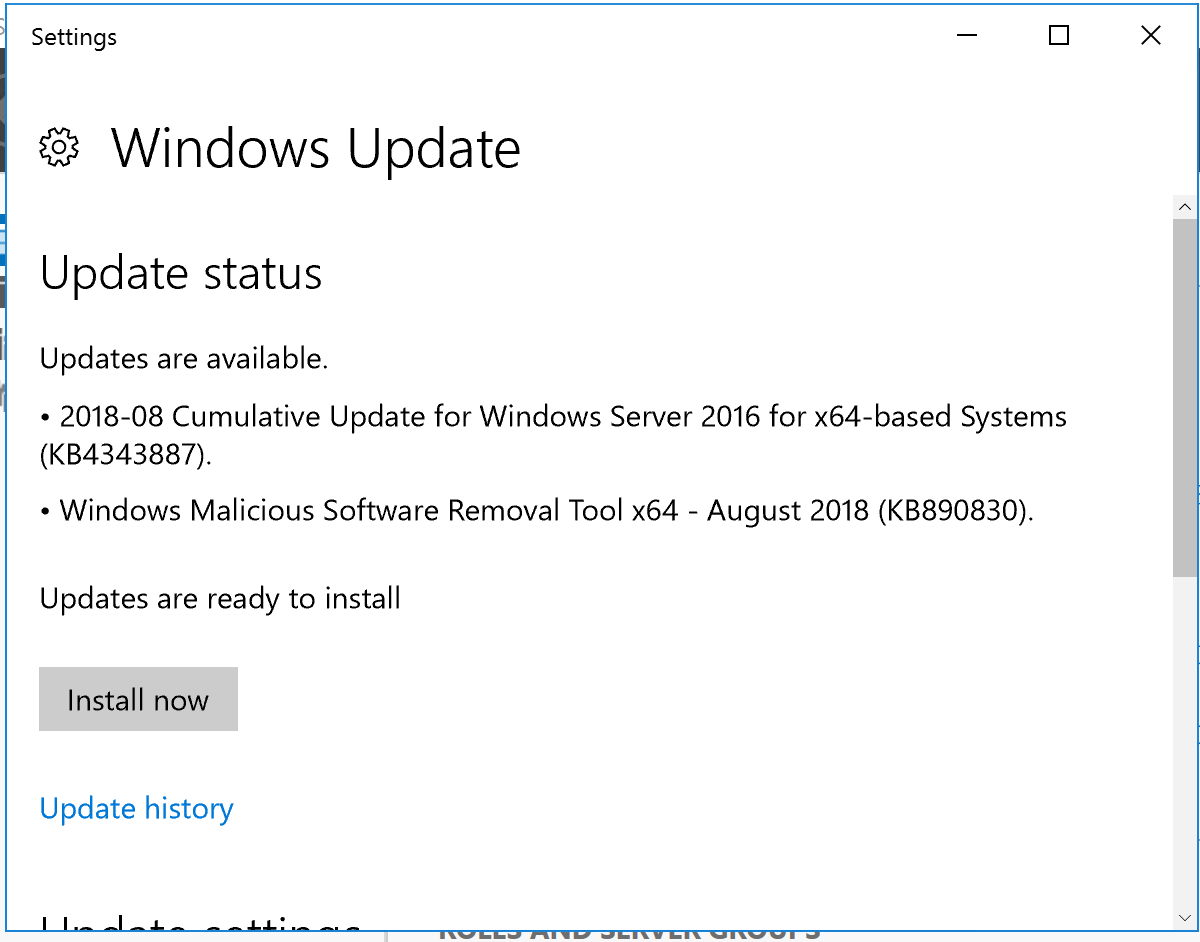
**Additional Accounts**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | FIRST NAME | LAST NAME | LogonName | Password |
| 1. | Cleveland | McFadden | SECLAB\U64543 | N?07\*F3sDj |
| 2. | Josefina | Neal | SECLAB\U64542 | N?07\*F3sDj |
| 3. | Kris | Rios | SECLAB\U64541 | N?07\*F3sDj |
| 4. | Leah | Hooper | SECLAB\U64540 | N?07\*F3sDj |
| 5. | Patrice | Koch | SECLAB\U64539 | N?07\*F3sDj |
| 6. | Isabelle | Barry | SECLAB\U64538 | N?07\*F3sDj |
| 7. | Michele | Best | SECLAB\U64537 | N?07\*F3sDj |
| 8. | Andre | Robledo | SECLAB\U64536 | N?07\*F3sDj |
| 9. | Margie | Clarke | SECLAB\U64535 | N?07\*F3sDj |
| 10. | Trevor | Alfonso | SECLAB\U64534 | N?07\*F3sDj |

Note that the machines have been provisioned in March 2020.   
Therefore, it is possible to see the following message while connecting for the first time to the servers:



In this case, click on View updates.



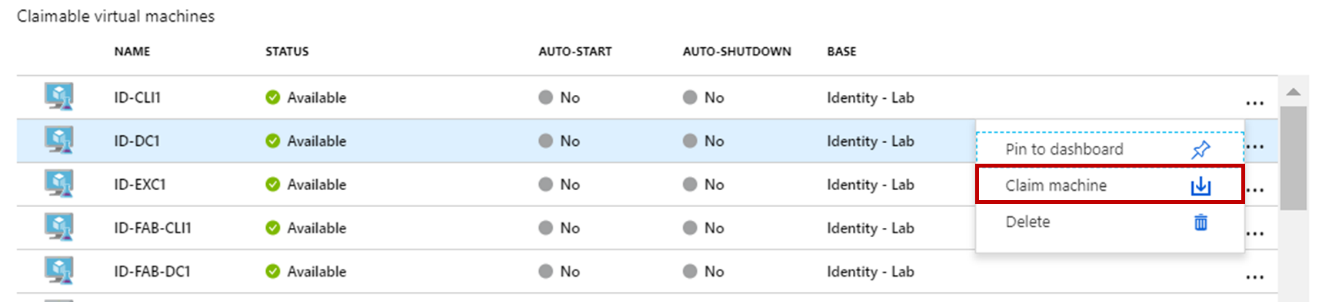
We do not need the latest updates for these labs so you can close this window.

#### How to start and connect to a VM

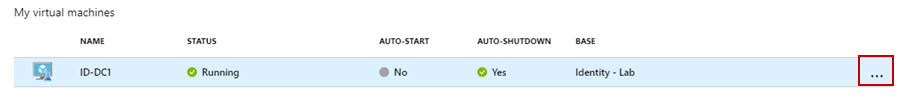
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



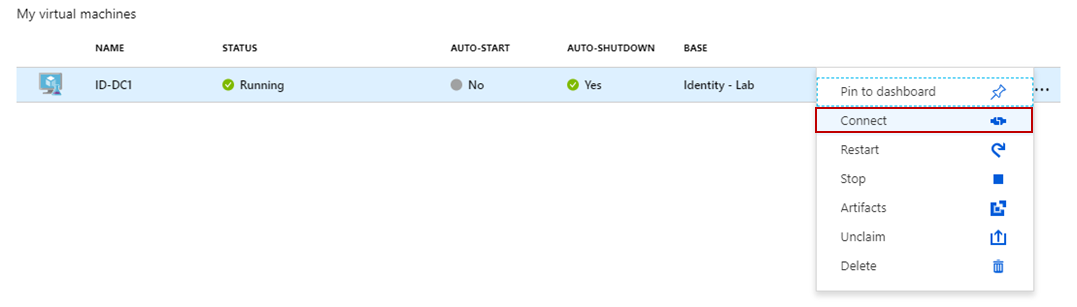
1. To start a VM, click on “Claim machine”



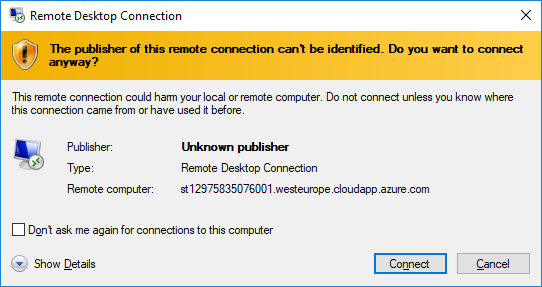
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



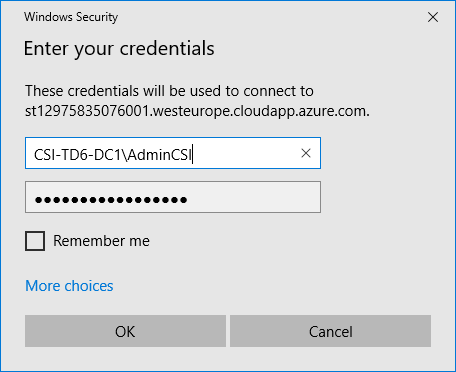
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



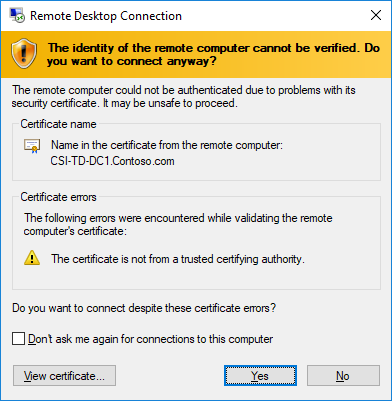
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



1. Enter the user name and password to connect to the Virtual Machine detailed in each exercise below.   
   (Do not use your student or organizational account.)



1. A warning on the self-issued certificate is displayed. You can safely ignore this warning by clicking on Yes.



## Exercise 1: Prevent anonymous enumeration of accounts

Duration: 30 minutes

Synopsis: In this exercise, you will learn how to assess the configuration of remote SAM accounts database. Then, you will learn how to properly configure the SAM database to prevent anonymous enumeration of accounts.

Because the SAM is available on both domain controllers and any member server or workstation, you will perform the assessment and remediation both on the lab DC and server:

* Server: csw2-srv.seclab.local or IP address = 10.0.0.5
* DC: csw2-dc.seclab.local or IP address = 10.0.0.4

#### Task 1: Assess the existing

In this task, you will assess the current configuration of the SAM database

1. Sign in **CSW2-WKS** with following credentials  
    Username: CSW2-WKS\local\_student  
    Password: 08Fc720C!0eK2
2. Once the session is ready, open a command prompt ‘as administrator’. This can be achieved in two ways:
   1. Right-click the **Start** menu and select **Command Prompt (Admin)**
   2. Open the **Start** menu, type **cmd**, right click on the **Command Prompt** tile and select **Run as Administrator**
3. To assess current SAM configuration, you will be using the **nmap** utility. Now, take time to review the nmap script you are going to use. Documentation is located here: https://nmap.org/nsedoc/scripts/smb-enum-users.html
4. NMap is already installed in your environment. The command to use to test a particular server is:  
    nmap -script=smb-enum-users -p445 *hostname\_or\_IP*
5. Start a network capture using Wireshark. Set a capture filter equals to :  
    tcp port 445 and host a.b.c.d  
    *Where a.b.c.d is either the IP address of the DC or the address of the server*  
   *Note: Help on Wireshark is provided in Annex 1*
6. Run the script for both the member server and the DC
7. Stop the network capture

Additional Questions:

1. What is the output of the nmap command for the DC?
2. What is the output of the nmap command for the member server?
3. Using the network capture, copy-paste the network frame details which display an anonymous connection. Do that only once; choose either the DC or the member server.

#### Task 2: Remediate weak SAM remote configuration

In this task, you will be learning how to prevent remote anonymous access to the SAM database. For the purpose of the lab, a weak security configuration has been applied to all machines in the seclab.local domain. For simplicity, the configuration was done in the *Default Domain Policy* group policy.

1. Review security options in the category “Network Access” documented at <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-options>. Pay attention to the 2 ***Network access: Do not allow anonymous enumeration of SAM accounts*** settings. They will be discussed later.
2. Sign in **CSW2-DC** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
3. Open the *Default Domain Policy*
   1. From **Server Manager**, open the **Tools** menu in the top right corner
   2. Select **Group Policy Management** from the drop-down menu
   3. In **Group Policy Management** console, expand the following node: **Group Policy Management, Forest: seclab.local, Domains, seclab.local**
   4. Right click **Default Domain Policy** node and select **Edit**
4. Set the Security Options of the GPO so that the following security requirements are met:
   1. No anonymous access to SAM
   2. No anonymous access to named pipes or shares
   3. No anonymous translations of names or SIDs.
   4. Only Administrator should be able to access SAM remotely

Additional Questions:

1. Does the ***Network access: Do not allow anonymous enumeration of SAM accounts*** settings applies to DC and Why?
2. Explain how you implemented the security requirements

#### Task 3: Assess remediated configuration – part 1

In this task, you will test if your configuration meets the security requirements.

1. Reboot server **CSW2-SRV** and **CSW2-DC** to ensure new configuration is used
2. Start a network capture using Wireshark. Set a capture filter equals to:  
    tcp port 445 and host a.b.c.d  
    Where a.b.c.d is either the IP address of the DC or the address of the server  
   *Note: Help on Wireshark is provided in Annex 1*
3. Using the same commands as in Task #1, ensure anonymous enumeration of users for both DC and member server is not possible
4. Stop the network capture

Additional Questions:

1. Copy-paste at least one screenshot of a *packet details* view of wireshark demonstrating the anonymous attempt is blocked

## Exercise 2: Implement DACL

Duration: 15 minutes

Synopsis: In this exercise, you will train yourself in setting DACL on an existing file structure. For this lab, a fictious file structure (C:\Share) has been created on CSW2-SRV to support the exercise.

For all connection tests, you can use:

* File server: csw2-srv.seclab.local or IP address = 10.0.0.5
* File share: [\\csw2-srv.seclab.local\Share](file://csw2-srv.seclab.local/Share)
* User account: SECLAB\student
* User password: 08Fc720C!0eK2

#### Task 1: Assess the existing

In this task, you will assess the current permissions of the file server (csw2-srv.seclab.local)

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Find a way to display the current permissions of folder C:\Share using the graphical user interface.
3. Find a way to display the current permissions of folder C:\Share using a command line tool.

Additional Questions:

1. What are the current permissions on the C:\Share folder?
2. Copy-paste the output of the command line tool you used to display folder permissions

#### Task 2: Implement file permissions

In this task, you will learn how to set permissions on a folder

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Using the security rules below, set the proper permissions on folders in C:\Share:

|  |  |  |
| --- | --- | --- |
| ID# | Folder | Policy description |
| 0 | C:\Projects\Cucumber | For the need of backup and administration, SYSTEM and SECLAB\Domain Admins must have full control on the folder and all child files and folders. |
| 1 | C:\Projects\Cucumber | User SECLAB\U64536 has full control on this folder |
| 2 | C:\Projects\Cucumber | User SECLAB\U64537 can create new files/folders and edit existing files but cannot delete any file |
| 3 | C:\Projects\Cucumber | User SECLAB\U64538 can only read files |
| 4 | C:\Projects\Cucumber | Except the users referenced above, no other user must be able to access files in the foler |
| 5 | C:\Share\Users | Each user can have a personal folder which only the user can access. The folder is named after the logon name of the user |
| 6 | C:\Share\Users | Users must not be able to delete other users’ personal folder |
| 7 | C:\Share\Users | In his/her personal folder, the user has full permissions |
| 8 | C:\Share\Users | For the need of backup and administration, SYSTEM and SECLAB\Domain Admins must have full control on all files and folders in the Users folder |
| 9 | C:\Share\Users | In case the user’s folder does not exist, user should be able to create his folder by himself. *Hint: use the CREATOR OWNER special user* |

Additional Questions:

1. Take a screenshot of the Advanced Security Settings window of the C:\Share\Projects\Cucumber folder.
2. Take a screenshot of the Advanced Security Settings window of the C:\Share\Users folder
3. Take a screenshot of the Advanced Security Settings window of the C:\Share\Users\U64536 folder
4. What permissions did you apply implement rule #9?

## Exercise 3: Implement Audit

Duration: 45 minutes

Synopsis: In this exercise, you will train yourself in implementing basic auditing scenarios as well as deploy an audit policy.

#### Task 1: Implement Logon/Logoff auditing

In this task, you will implement auditing of user logon & logoff events on server **CSW2-SRV**. For this first exercise, you will only enable auditing locally, using the auditpol.exe command

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Right-click the **Start** menu and select **Command Prompt (admin)**
3. Run the following commands:  
   auditpol /set /subcategory:Logon /success:enable  
   auditpol /set /subcategory:Logoff /success:enable
4. In order to end existing file sharing sessions, restart the **Server** service using the command:  
   net stop srv && net start srv
5. Sign in **CSW2-WKS** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
6. Use the file explorer to access **\\CSW2-SRV\Share**
7. Go back to **CSW2-SRV** and open the event viewer  
   *Note: the event viewer can easily be opened by right clicking the start menu and selecting Event Viewer.*
8. Using the course material, locate the security event which correspond to your attempt to access the shared folder

Additional Questions:

1. Copy-paste a screenshot of the security event from step 8
2. Have a look at this event and answer these questions:
   1. What is the type of this logon?
   2. What does the logon type means?
   3. List all other Logon Types.
3. How can the 2 auditpol commands be modified so that Logon Failures can also be audited?

#### Task 2: Implement File Access auditing

In this task, you will learn how to enable auditing of files and folder usage. For the purpose of the lab, you will be using the fictious folder hierarchy on CSW-SRV located at C:\Share

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Using file explorer, open the folder **C:\Share\Projects**
3. Right click folder **Artichoke** and select **Properties**
4. Select the **Security** Tab and click **Advanced**
5. Select the **Auditing** tab
6. Click the **Add** button
7. Click **Select a principal**, type **Everyone** in the text box and click **OK**
8. In the **Basic permissions** list field, tick the **Write** checkbox
9. Click **OK**
10. In the **Advanced Security Settings Window**, click **Apply** and **OK**
11. Right-click the **Start** menu and select **Command Prompt (admin)**
12. Run the following command:  
    auditpol /set /subcategory:"File System" /success:enable /failure:enable
13. Modify one of the files contained in the **C:\Share\Projects\Artichoke** folder to generate an audit event

Additional Questions:

1. What is the ID of the security event which traced the modification event?
2. You will notice the same event is generated whether the file was opened for reading or Writing. Using the event contained data, how can you discriminate a read access from a write access?
3. Now, we want to audit permission changes and deletion of files and folders in the same project folder.
   1. How should you modify the SACL?
   2. Which security events will be generated?
   3. What is the issue with the event marking the real deletion?
   4. How can you link it with the file name?

#### Task 3: Enable Registry auditing

In this task, you will learn how to enable audit registry keys and values accesses.

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Open registry editor by launching regedit.exe
3. Create this registry key: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Test**
4. Using the same basic principles as previous assignments, set-up auditing so that every operation can be audited for all users
5. Try to create a new DWORD value in this key in order to generate an audit event.

Additional Questions:

1. Take a screenshot of the auditing permissions you set up and paste it here.
2. Explain how you changed the audit policy so that registry accesses can be audited.
3. What security event will be generated when
   1. key will be read or enumerated?
   2. a value will be modified inside the key?

#### Task 4: Create an auditing GPO

In this task, you will learn how auditing settings can be deployed using a GPO – *Group Policy Objects*.

1. Sign in **CSW2-DC** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Open the roup policy management console (From the **Server Manager** application, select the **Tools** menu, then **Group Policy Management**)
3. In the **Group Policy Management** console, unfold the nodes: **Group Policy Management\Forest: seclab.local\Domains\seclab.local\Group Policy Objects**
4. Right click **Group Policy Objects** and select **New**
5. Give a name to your GPO. For instance, **Domain Auditing Policy**
6. Right click the new GPO and select **Edit**
7. In the Group Policy Management Editor console, **unfold Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration**
8. Using the course material, edit your GPO so that the use of sensitive privileges and failure to acquire those privileges are audited
9. Link your GPO to the domain. From the **Group Policy Management** console, right click the **seclab.local** node and select **Link an existing GPO**. Then, choose your auditing GPO and click **OK**.
10. Sign in **CSW2-SRV** with following credentials  
     Username: SECLAB\student  
     Password: 08Fc720C!0eK2
11. Right-click the **Start** menu and select **Command Prompt (admin)**
12. Run **gpupdate** to ensure GPO gets refreshed
13. Run **robocopy C:\Share\Projects\Artichoke C:\Backup \*.\* /E /B**

Additional Questions:

1. Which command can you run to ensure audit policy got successfully deployed on the system?
2. What privilege is activated by the robocopy command?
3. What actions can be performed when this privilege is hold?

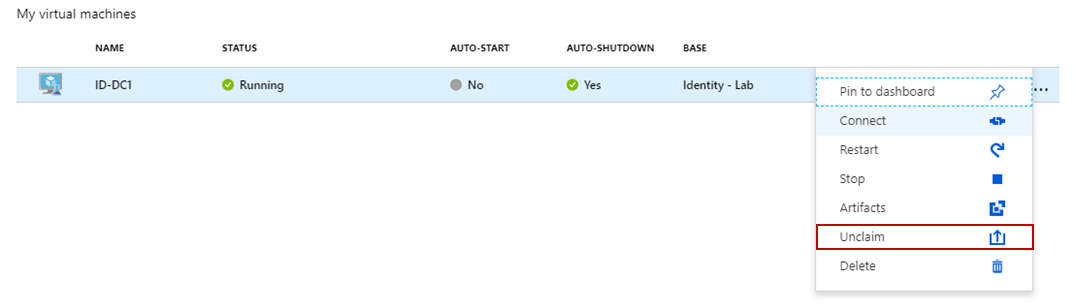
## After the Lab

Duration: 10 minutes

In this exercise, attendees will deprovision any Azure resources that were created in support of the lab.

#### Task 1: Stop and deallocated all the VMs

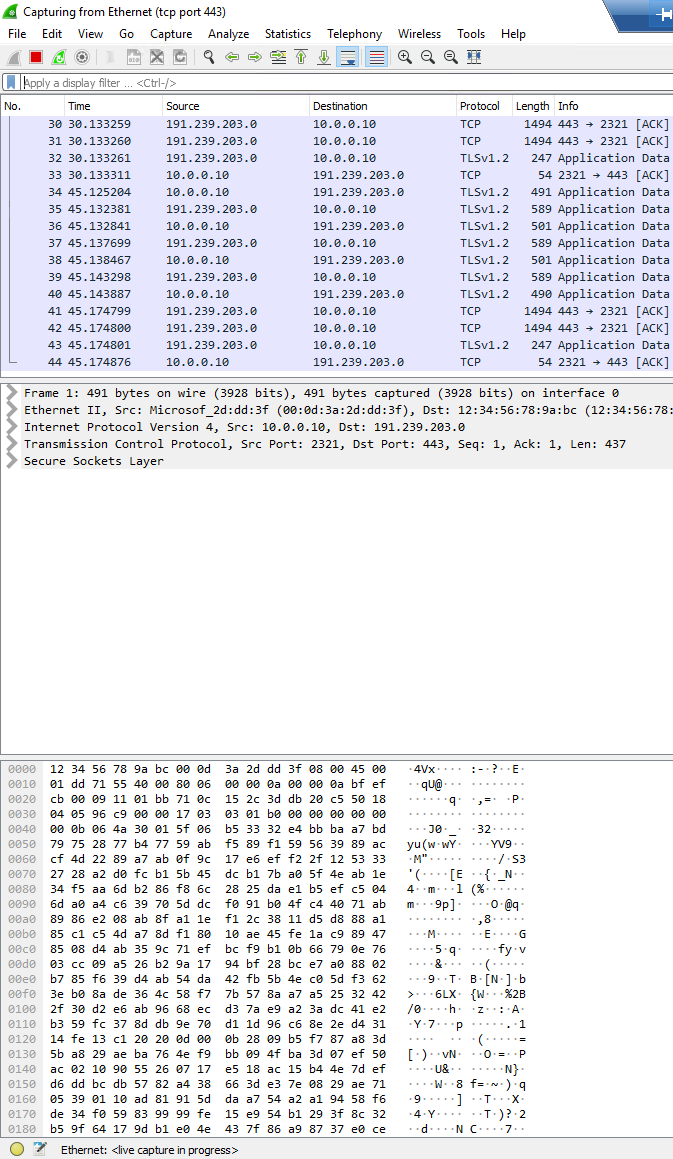
1. Properly shutdown all the VMs
2. Deallocate the VM in the Azure Portal
3. To Stop a VM, simply click on Unclaim.



## Annex 1 – Wireshark

Wireshark is already installed on CSW2-WKS machine.

#### Wireshark Panels

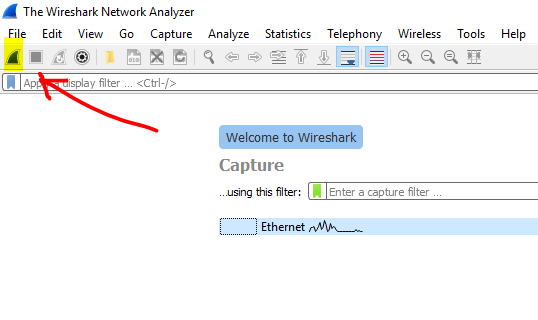


Packet Bytes

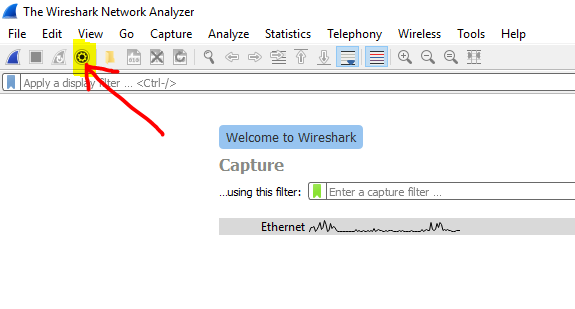
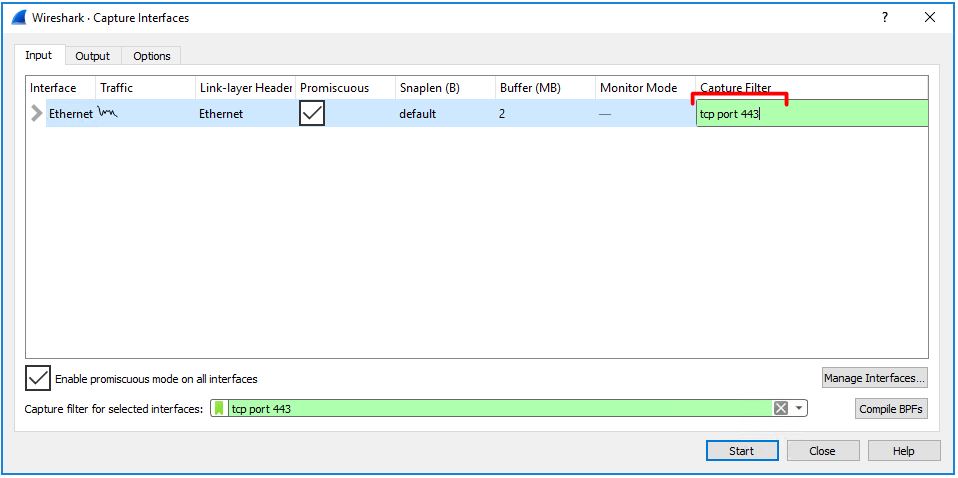
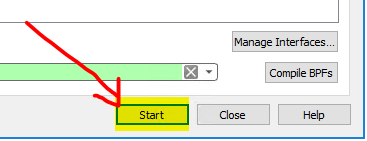
Packet Details

Packet List

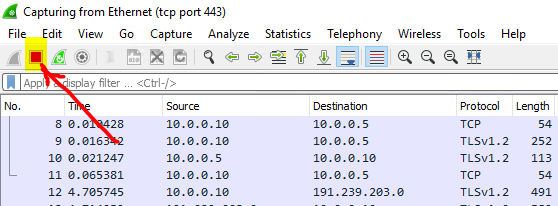
#### Starting a capture



#### Starting a capture with a filter

1. Edit options  
   
2. Input filter  
   
3. Start Capture  
   

#### Stop Capture



#### Restart Capture

