Windows security

Exercise 4 – Module 3 – Section 3

June 2020  
V1.2

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

[Windows communication protocols hardening 1](#_Toc44075602)

[Abstract and learning objectives 1](#_Toc44075603)

[Overview 2](#_Toc44075604)

[Requirements 2](#_Toc44075605)

[Before the exercise 3](#_Toc44075606)

[List of VM to start 3](#_Toc44075607)

[How to start and connect to a VM 4](#_Toc44075608)

[Exercise 1: Strengthen TLS server configuration 6](#_Toc44075609)

[Task 1: Assess the existing 6](#_Toc44075610)

[Task 2: Remediate weak SChannel configuration 7](#_Toc44075611)

[Task 3: Assess remediated configuration 8](#_Toc44075612)

[Exercise 2: Strengthen SMB configuration 9](#_Toc44075613)

[Task 1: Assess the existing 9](#_Toc44075614)

[Task 2: Remediate weak SMB configuration – Part 1 10](#_Toc44075615)

[Task 3: Assess remediated configuration 11](#_Toc44075616)

[After the Lab 12](#_Toc44075617)

[Task 1: Stop and deallocated all the VMs 12](#_Toc44075618)

[Annex 1 – Wireshark 13](#_Toc44075619)

[Wireshark Panels 13](#_Toc44075620)

[Starting a capture 13](#_Toc44075621)

[Starting a capture with a filter 14](#_Toc44075622)

[Stop Capture 14](#_Toc44075623)

[Restart Capture 15](#_Toc44075624)

[Annex 2 - Troubleshooting 16](#_Toc44075625)

[No Internet connectivity 16](#_Toc44075626)

[NLA Issues 16](#_Toc44075627)

[Issues with the Ubuntu environment 16](#_Toc44075628)

# Windows communication protocols hardening

## Abstract and learning objectives

This training is designed to train yourself in hardening some of the communications protocol used in Windows. The lab exercises will cover SMB and TLS protocols.

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

* Assess an existing SMB or TLS deployment using commonly available tools
* Deploy a hardened configuration for these protocols
* Assess the new configuration

## Overview

This lab exercise is a very simple environment consisting in a Windows 10 client and Windows Server 2016 server. Both are member of an ActiveDirectory domain seclab.local. The server provides an SMB share and an HTTPS website.

## 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

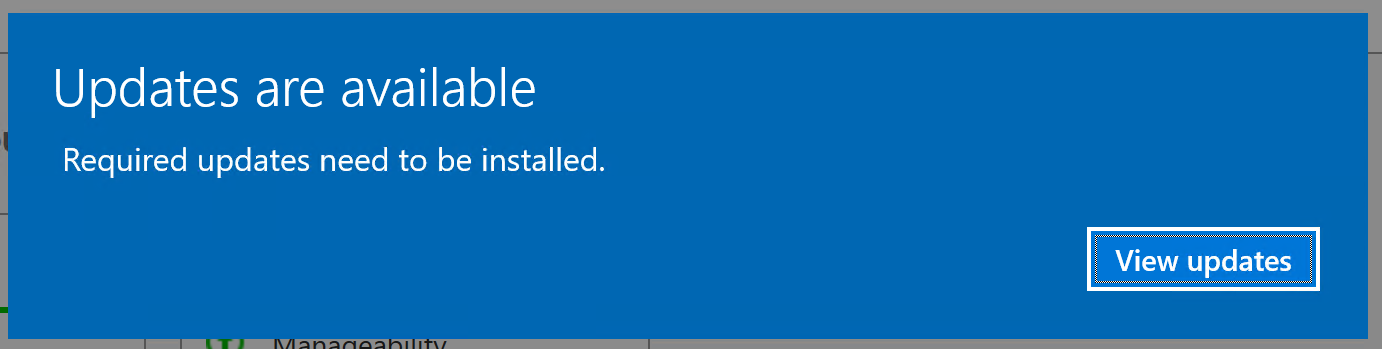
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

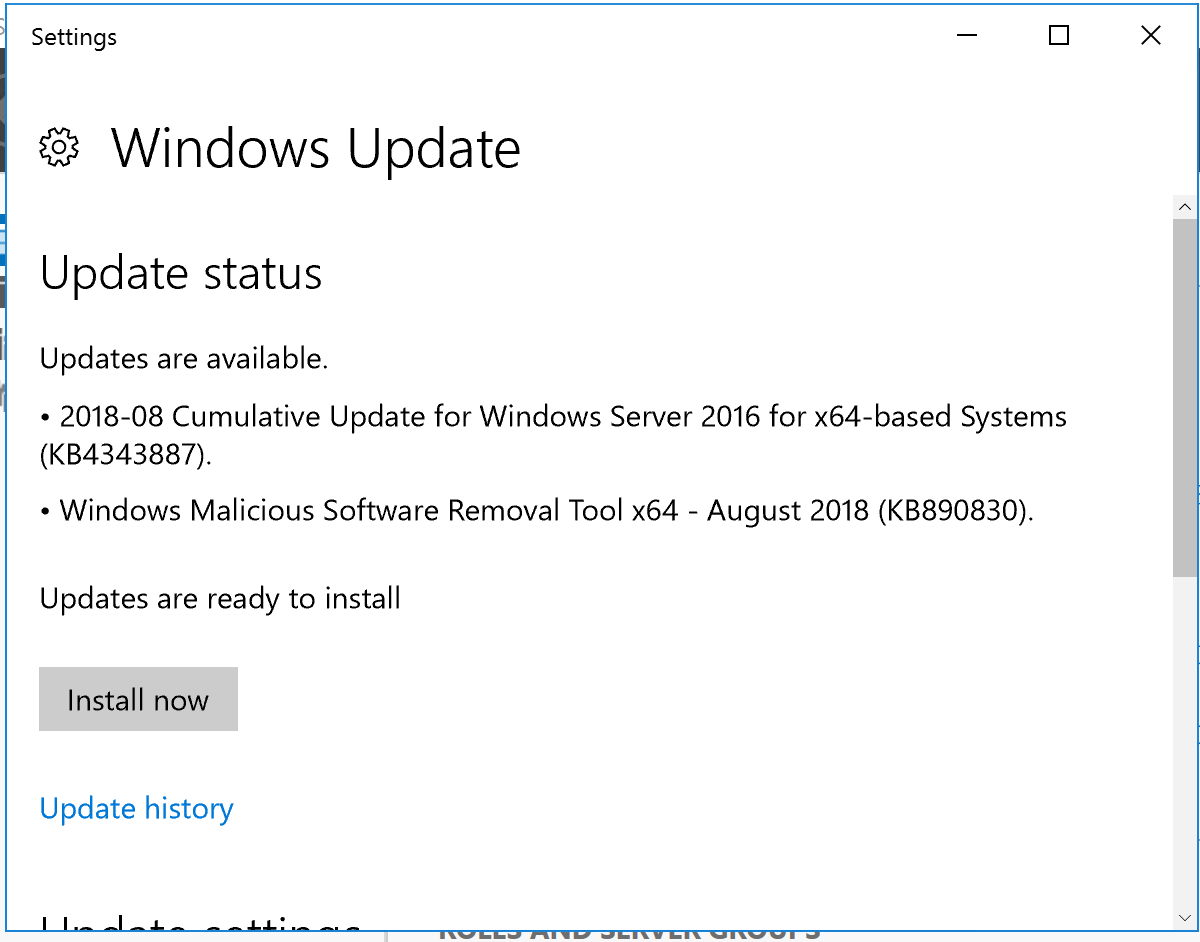
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

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.



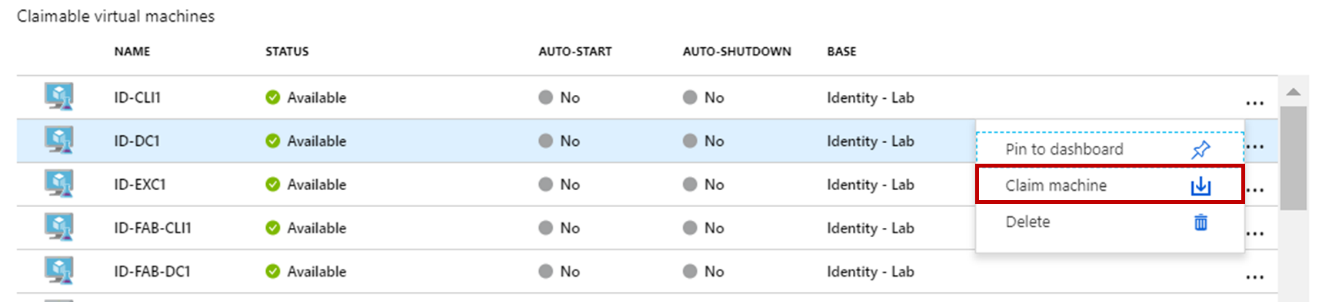
We do not need the latest updates for these labs so you can close this window.

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

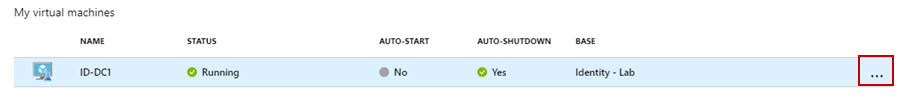
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



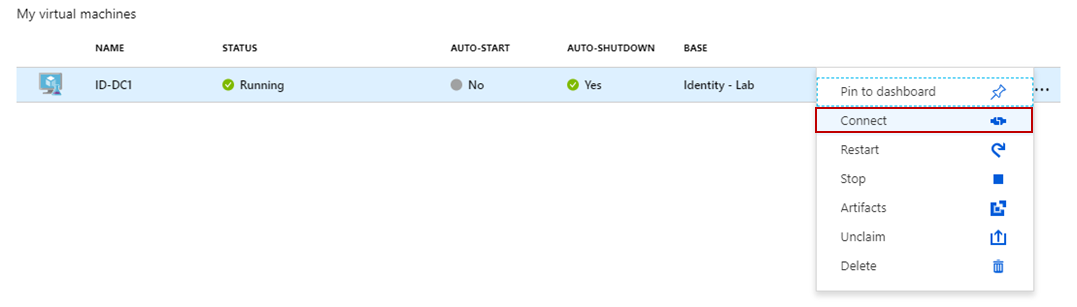
1. To start a VM, click on “Claim machine”



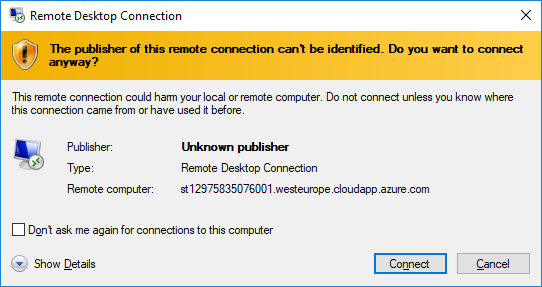
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



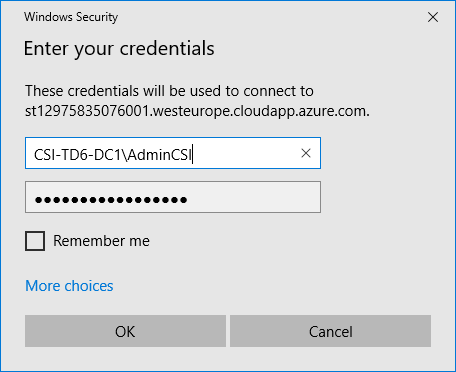
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



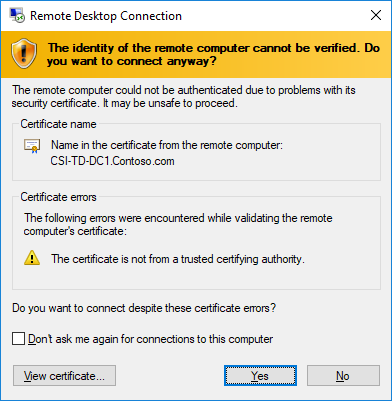
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Strengthen TLS server configuration

Duration: 45 minutes

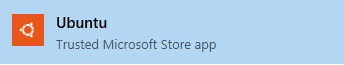
Synopsis: In this exercise, you will learn how to assess a Windows SChannel configuration regarding enabled protocols and cipher suite. Then, you will learn how to configure these settings in order to meet certain security requirements. Concerning TLS, the main security challenge is to get rid of obsolete cipher suites, algorithms and protocol versions.

For all connection tests, you can use :

* TLS Server: csw2-srv.seclab.local or IP address = 10.0.0.5
* TCP Port: 443

#### Task 1: Assess the existing

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

1. Sign in **CSW2-WKS** with following credentials  
    Username: CSW2-WKS\local\_student  
    Password: 08Fc720C!0eK2
2. Once the session is ready, open the Start memu and launch the Ubuntu application  
   
3. To assess current TLS configuration of the server, you will be using the openssl -s\_client command. Now, take time to review the available options. Documentation is located here: <https://www.openssl.org/docs/man1.0.2/apps/openssl-s_client.html>
4. OpenSSL is already installed in your Ubuntu environment. Use the command from previous step to assess various TLS protocol versions and cipher suites family

Additional Questions:

1. Is the server accepting connections for the following TLS protocol versions?
   1. TLS 1.2 ?
   2. TLS 1.1 ?
   3. TLS 1.0 ?
2. Is the server accepting cipher suites containing the following algorithms?
   1. 3-DES?
   2. RC4?
   3. MD5?
   4. SHA1?
3. Copy-paste the output of openssl -s\_client command when connecting to the server using TLS 1.0 protocol and using a 3-DES based cipher suite.

#### Task 2: Remediate weak SChannel configuration

In this task, you will be learning how to configure enabled TLS protocols versions and cipher suites

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Using the course material and <https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc>, implement the following security requirements:
   1. The only version of TLS allowed is 1.2
   2. DES based algorithms, SHA1, MD5 and RC4 are not allowed
3. Using the course material, restrict allowed TLS cipher suite list so that it meet these requirements:
   1. No suite containing an obsolete algorithm (RC4, SHA, MD5, 3DES)
   2. No NULL encryption
   3. Only ephemeral variants of the Diffie-Helman key exchange algorithms

Additional Questions:

1. Explain how you implemented the security requirements

#### Task 3: Assess remediated configuration

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

1. Reboot server **CSW2-SRV** to ensure new configuration is used
2. Using the same commands as in Task #1, ensure TLS 1.0, TLS 1.1 are not enabled anymore.
3. Using the same commands as in Task #1, ensure server is not accepting cipher suites containing any of 3-DES, RC4, SHA1, MD5 algorithms

Additional Questions:

1. Copy-paste the output of openssl -s\_client command when connecting to the server using TLS 1.0 protocol and using a 3-DES based cipher suite.

## Exercise 2: Strengthen SMB configuration

Duration: 45 minutes

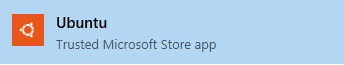
Synopsis: In this exercise, you will learn how to assess a Windows SMB configuration regarding enabled protocols and support for encryption and signing. Then, you will learn how to configure these settings to meet certain security requirements. Concerning SMB, the main security challenge is to get rid of SMB1 and enforce signing and encryption

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 configuration of the SMB protocol on the file server (csw2-srv.seclab.local)

1. Sign in **CSW2-WKS** with following credentials  
    Username: CSW2-WKS\local\_student  
    Password: 08Fc720C!0eK2
2. Once the session is ready, open the Start memu and launch the Ubuntu application  
   
3. To assess current SMB configuration of the server, you will be using the smbclient command. Now, take time to review the available options. Documentation is located here: <https://www.samba.org/samba/docs/current/man-html/smbclient.1.html>
4. Start a network capture using Wireshark. Set a capture filter equals to :  
    tcp port 445 and host 10.0.0.5  
   *Note: Help on Wireshark is provided in Annex 1*
5. Samba is already installed in your Ubuntu environment. Use the command from previous step to assess acceptance of all 3 versions of SMB protocol by the server.
6. Stop the network capture

Additional Questions:

1. Is the server accepting a connection for the following SMB protocol versions?
   1. SMB 1?
   2. SMB 2?
   3. SMB 3?
2. Using information from the network capture, make a screenshot from the Packet Details window of wireshark where the protocol version which is going to be used appears clearly.  
   *Note: Use these as reference :*[*https://msdn.microsoft.com/en-us/library/cc246561.aspx*](https://msdn.microsoft.com/en-us/library/cc246561.aspx)[*https://msdn.microsoft.com/en-us/library/ee441946.aspx*](https://msdn.microsoft.com/en-us/library/ee441946.aspx)
   1. SMB1:  
       <insert screenshot here>
   2. SMB2:  
       <insert screenshot here>
   3. SMB3:  
       <insert screenshot here>

#### Task 2: Remediate weak SMB configuration – Part 1

In this task, you will be learning how to disable version 1 of the SMB protocol and enforce signing and encryption on the ‘Share’ shared folder

1. Sign in **CSW2-SRV** with following credentials  
    Username: SECLAB\student  
    Password: 08Fc720C!0eK2
2. Using the course material, perform the following actions:
   1. Disable version 1 of the SMB protocol
   2. Enable Signature requirement
   3. Enable Encryption for the ‘Share’ shared folder

Additional Questions:

1. Explain how you implemented the security requirements

#### Task 3: Assess remediated configuration

In this task, you will test the settings you’ve applied in previous task to ensure security requirements are enforced.

1. Reboot server CSW2-SRV to ensure new configuration is properly applied
2. Start a network capture using Wireshark. Set a capture filter equals to:  
    tcp port 445 and host 10.0.0.5  
   *Note: Help on Wireshark is provided in Annex 1*
3. Using the same commands as in Task #1, ensure SMB1 is not enabled anymore
4. Using Wireshark, ensure Signing and Encryption are enforced
5. Stop the network capture

Additional Questions:

1. Regarding SMB1:
   1. What is the result of the smbclient command when you try SMB1 protocol?
   2. Copy-paste the command and its output
2. Regarding SMB2:
   1. Was the user able to connect to the server?
   2. How was it handled differently from an SMB1 connection?
   3. Copy-paste the command and its output during an SMB2 connection test

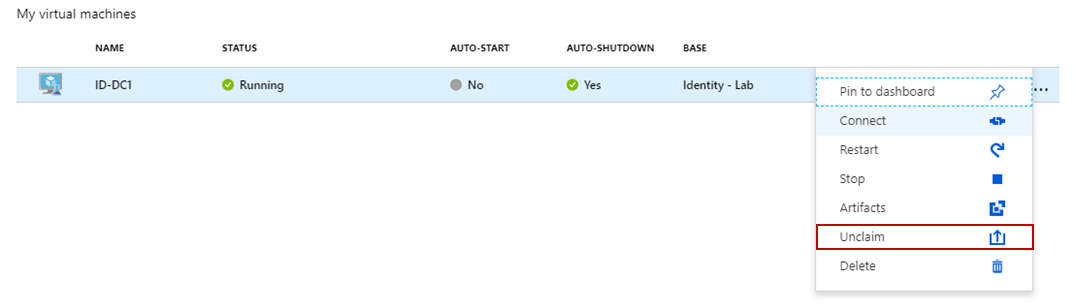
## After the Lab

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

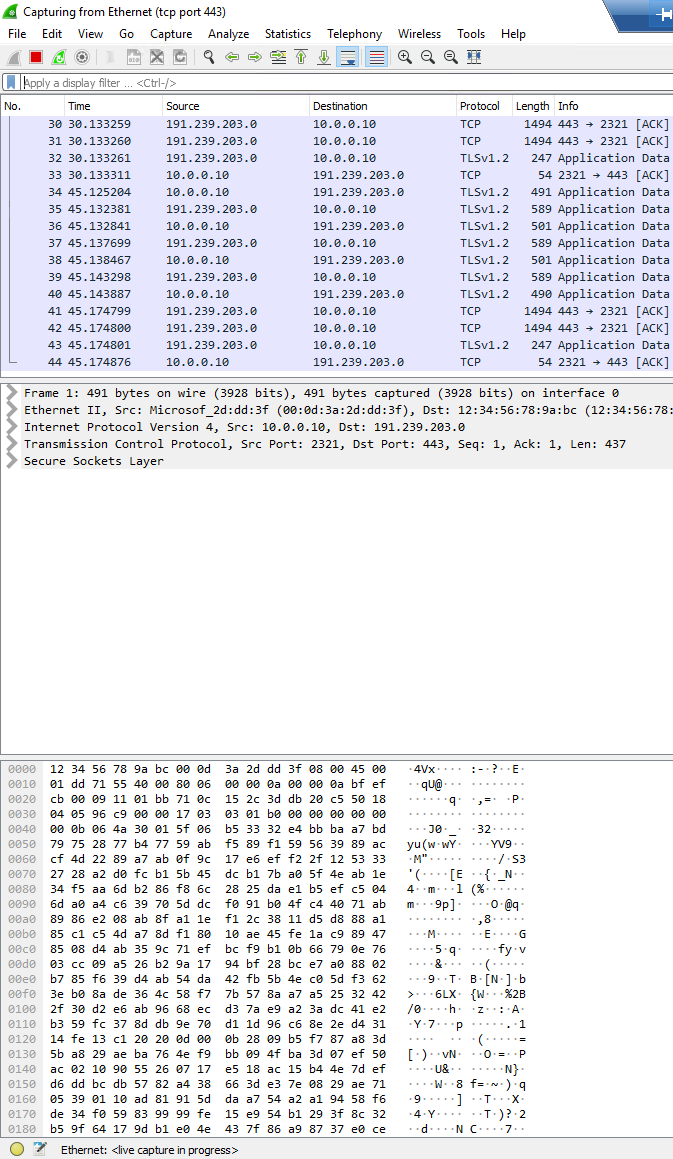
1. Properly shutdown all the VMs
2. Deallocate the VM in the Azure Portal
3. To Stop a VM, simply click on Unclaim.



## Annex 1 – Wireshark

Wireshark is already installed on CSW2-WKS machine.

#### Wireshark Panels

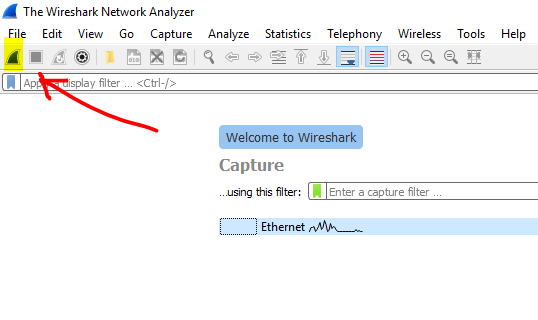


Packet Bytes

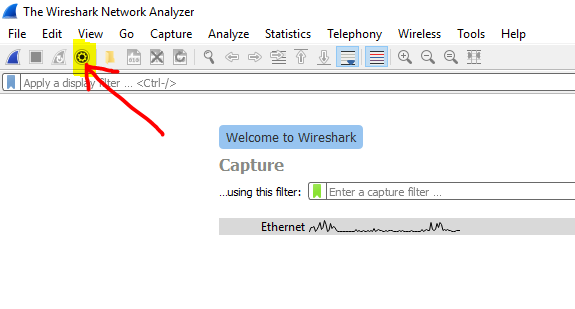
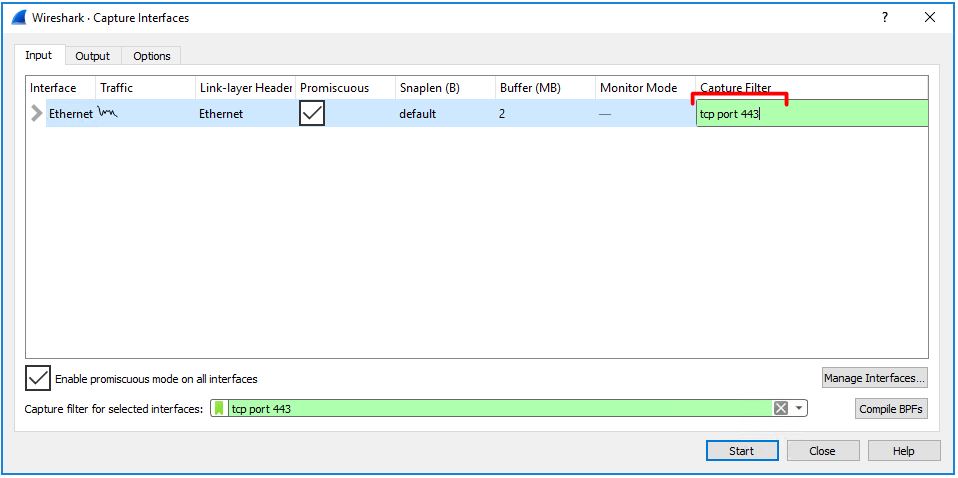
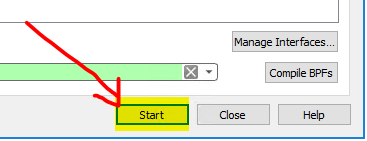
Packet Details

Packet List

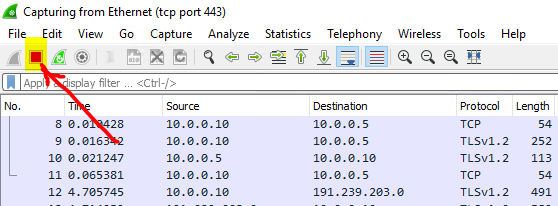
#### Starting a capture



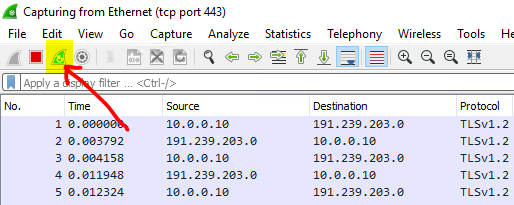
#### Starting a capture with a filter

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

#### Stop Capture



#### Restart Capture



## Annex 2 - Troubleshooting

#### No Internet connectivity

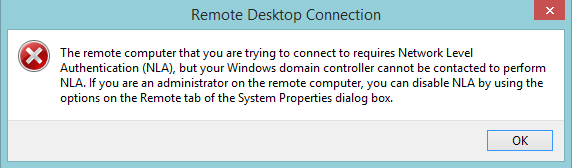
**Symptom**: You cannot access any resource on the Internet from the lab machines

**Cause**: The lab is an ActiveDirectory environment. The CSW2-DC machine acts as a DNS server for all other machines. If CSW2-DC is not running, no VM can access Internet resources

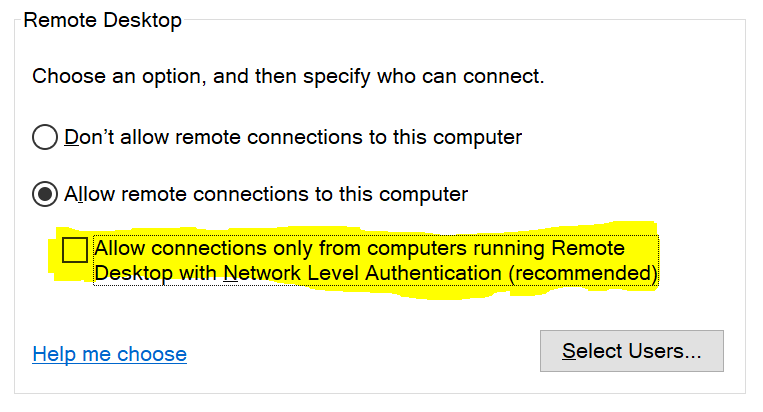
**Resolution**: When you start working in your lab, ensure CSW2-DC is always turned on

#### NLA Issues

**Symptom**: When connecting to a VM, the connection fails with an error message like:



**Resolution**: Disable NLA on the machine you want to connect to by using the following steps:

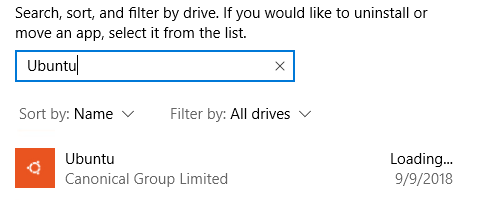
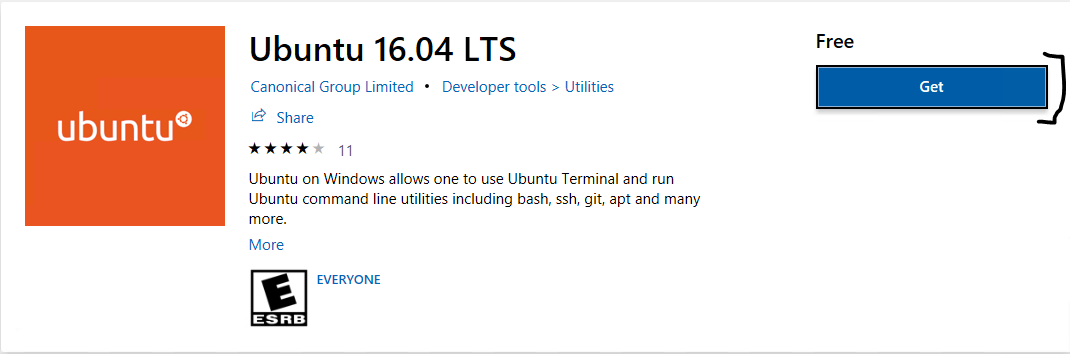
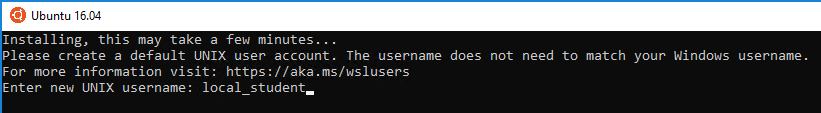
1. Sign-in the machine using these local credentials:  
   Username : . CSW2-SRV\local\_student  
   Password: 08Fc720C!0eK2  
   *Replace CSW2-WKS with the name of the machine if different (eg. CSW2-WKS\local\_student)*
2. Open the **Run** dialog box by right-clocking the Start Menu icon and select **Run**
3. In the **Open** field, type **sysdm.cpl** and hit Enter
4. In the **System Properties** window, select the **Remote** tab
5. In the **Remote Desktop** section, ensure that the box named **Allow connections only from computer running Remote Desktop with Network Level Authentication** is left unchecked:  
   
6. Sign-off and resume the lab where you left off

#### Issues with the Ubuntu environment

**Symptom**: Starting the Ubuntu application ends with an error like



**Resolution**: Reinstall the Ubuntu application by using the following steps:

1. Right-click the **Start Menu** icon and selectr **Apps and Features**
2. In the **Apps & features** section, type **Ubuntu** in the **Search this list** text box  
   
3. Click the Ubuntu icon and select **Uninstall**
4. Confirm uninstallation when prompted
5. When the uninstall process is complete, start the **Windows Store** application 
6. Click the **Search** button located in the top right corner
7. Type **Ubuntu** in the text box
8. Select **Ubuntu 16.04 LTS** from the list
9. On the application page, select **Get**  
   
10. When asked to sign-in with a Microsoft account, select **No, thanks** option
11. Wait for the installation process to complete. It can takes some time if the VM was not started recently and other applications are updating in the background
12. When the installation is complete, launch the Ubuntu application. First start can take many minutes to complete.
13. At the end of Ubuntu initialization, you’ll be prompted for a UNIX name. Type local\_student and hit **Enter**  
    
14. When prompted for a password, type 08Fc720C!0eK2
15. Confirm the password
16. Resume the lab where you left off