Windows security, Active Directory and Azure AD

TD08 – Module 1 – Section 2

July 2020  
V3.1

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

[Windows security, Active Directory and Azure AD Lab step-by-step 1](#_Toc43753772)

[Abstract and learning objectives 1](#_Toc43753773)

[Overview 2](#_Toc43753774)

[Requirements 2](#_Toc43753775)

[Before the exercise 3](#_Toc43753776)

[List of VM to start 3](#_Toc43753777)

[How to start and connect to a VM 4](#_Toc43753778)

[Exercise 1: Kill LSASS 6](#_Toc43753779)

[Prerequisite 6](#_Toc43753780)

[Prerequisite 6](#_Toc43753781)

[Task 1: Kill LSASS.exe 7](#_Toc43753782)

[Exercise 2: Kerberos and NTLM authentication 8](#_Toc43753783)

[Task 1: Kerberos Capture 8](#_Toc43753784)

[Task 2: NTLM Capture 9](#_Toc43753785)

[Questions: 11](#_Toc43753786)

[After the Lab 12](#_Toc43753787)

[Task 1: Stop and deallocated all the VMs 12](#_Toc43753788)

# Windows security, Active Directory and Azure AD Lab step-by-step

## Abstract and learning objectives

This training is designed to provide exposure to many of Microsoft Windows, Active Directory and Azure Active Directory security features.

## Overview

In this Lab, the attendees will have a closer look at the authentication protocols used in AD DS.

## 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.

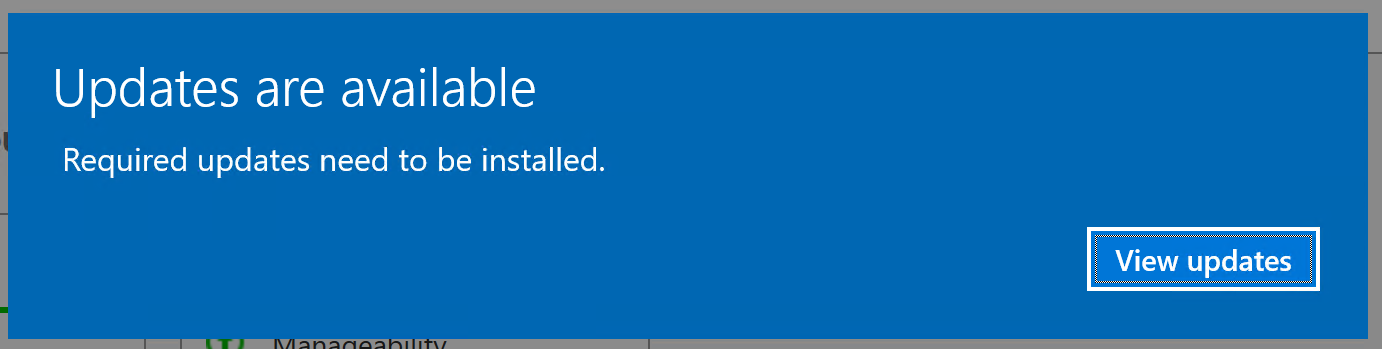
#### List of VM to start

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

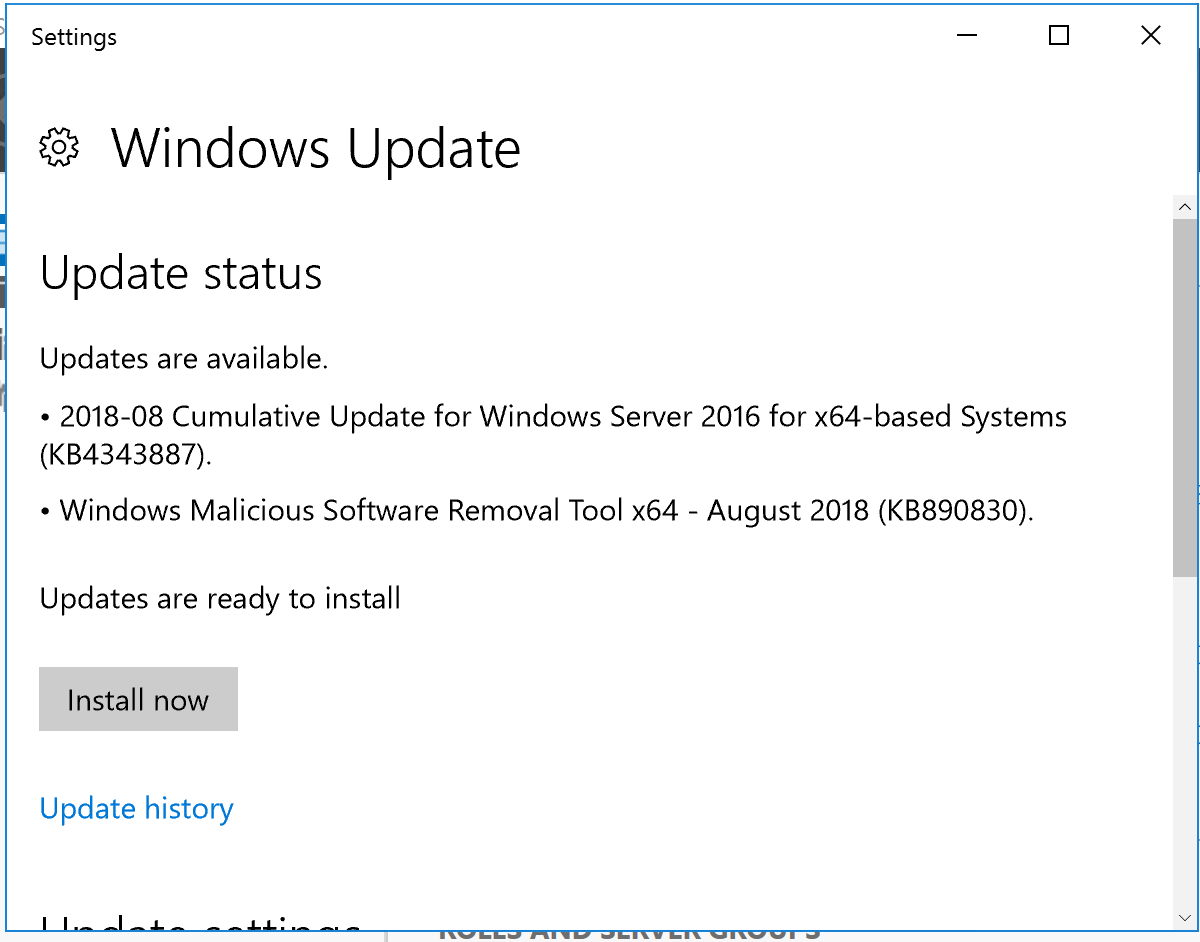
|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-DC1 | **ID-DC1** | Windows Server 2016 Standard | DC |
| ID-SRV1 | **ID-SRV1** | Windows Server 2016 Standard | Server |
| ID-CLI1 | **ID-CLI1** | Windows 10 Enterprise | Desktop |

Note that the IP addresses of the machines in this lab might be different for each attendee. For this reason, some of the exercises may ask you to determine what are the IP addresses used for your machines.

Also 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.



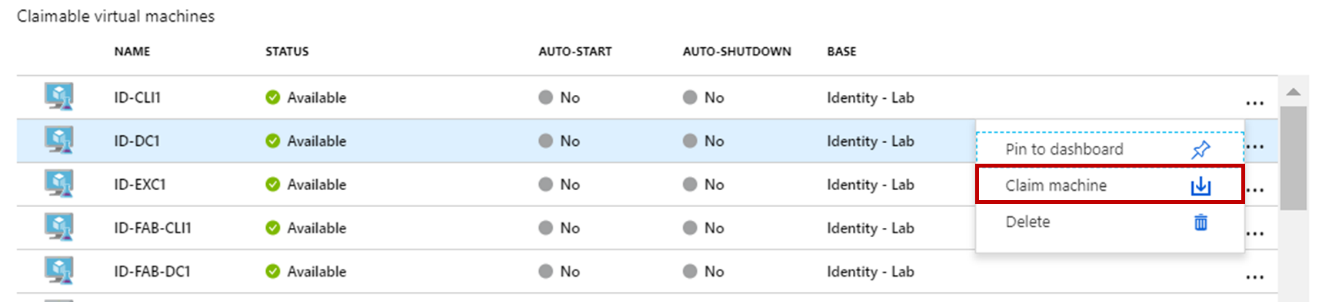
We do not need the latest updates for these labs so you can close this window.

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

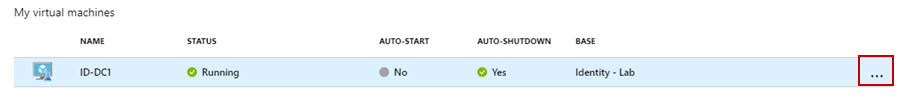
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



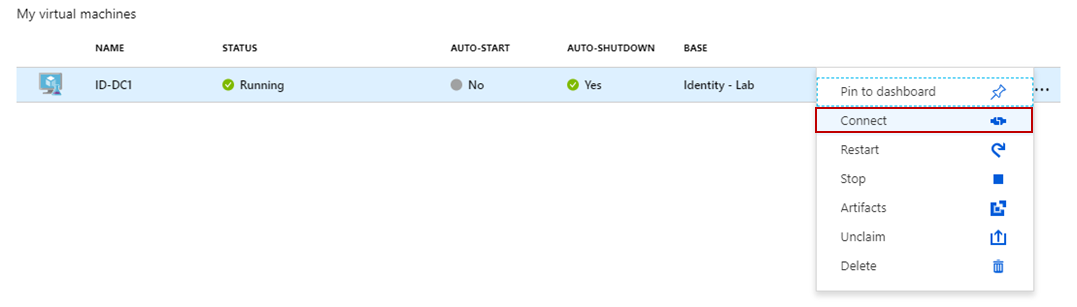
1. To start a VM, click on “Claim machine”



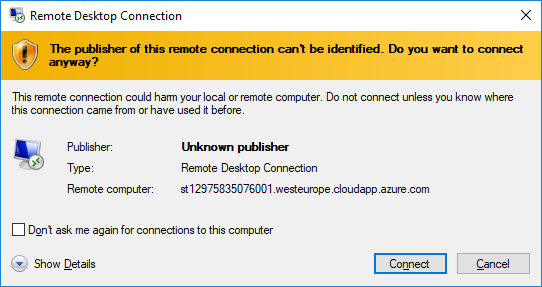
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



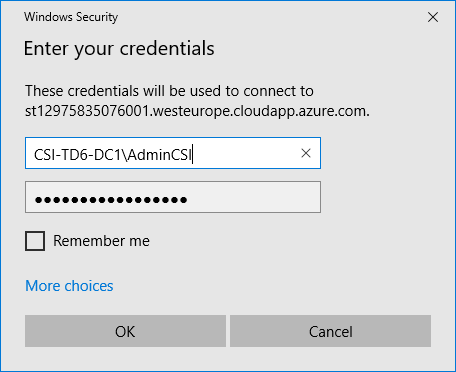
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



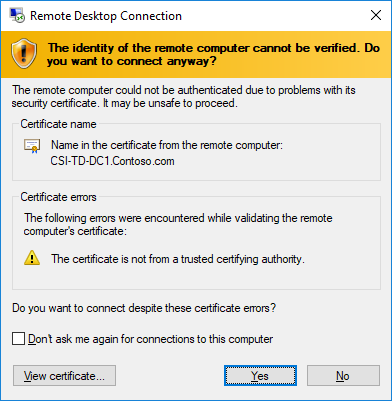
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Kill LSASS

Duration: 30 minutes

Synopsis: In this exercise, attendees will show the impact of killing LSASS.exe.

#### Prerequisite

For **each** machine check and if necessary, correct the IP address for the DNS Server

1. Right click on Windows button  on the taskbar and choose **Run**
2. Enter **cmd**
3. Enter **Ipconfig /all**
4. Ensure that the IP addresses for the DNS servers are
5. The correct configuration should be :
6. First IP : IP address of CSI-TD-DC1 -  **This server must be listed first**
7. 168.63.129.16 : This address should be the last address
8. If the DNS server addresses are not correct
9. Click on Windows button  on the taskbar and enter Network Connect

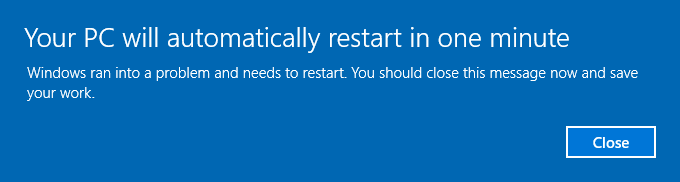
A screenshot of a cell phone

Description automatically generated

1. Select **Network Connections**
2. Right on the Network Card and choose **Properties**
3. Double Click on **Internet Protocol Version 4 (TCP/IPv4)**
4. Select Use the following DNS server addresses and enter the IP of the CSI-TD-DC1 in **Preferred DNS** **Server** and 168.63.129.16 in **Alternate**
5. Click **Ok** Twice
6. You're going to lost control of the VM and you need to restart using **DevTestLab**
7. Go to the **Azure Portal** in **DevTest Labs**, select **All virtual machines**, and click on the server
8. Click on **Restart**

#### Task 1: Kill LSASS.exe

1. Logon to **CSI-TD-CLI1**
   1. Username: [**Par\_User02@contoso.com**](mailto:Par_User02@contoso.com)
   2. Password: **Ilovesecu\*!**
2. Kill process **LSASS.exe**
   1. As **LSASS.exe** is longer securing the system, the computer will automatically reboot.



## Exercise 2: Kerberos and NTLM authentication

Duration: 45 minutes

Synopsis: In this exercise, attendees will perform Kerberos and NTLM authentication and analyze the network trace.

#### Task 1: Kerberos Capture

1. Logon to **CSI-TD-DC1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Add **Par\_User02@contoso.Com** to the local group **Administrators**
3. Sign out
4. Logon to **CSI-TD-CLI1**
   1. Username: [**Par\_User02@contoso.com**](mailto:Par_User02@contoso.com)
   2. Password: **Ilovesecu\*!**
5. Launch **Command line** as **Administrator** and check the Kerberos ticket using **Klist.exe**
   1. You should see at least two ticket
      1. **TGT**
      2. **LDAP**
6. Launch **Network Monitor as Administrator**
   1. If a dialog box asks for update, click N**o**
7. Start a **New Capture**
8. Purge Kerberos ticket for the user using **Klist**
   1. Access to share folder on **CSI-TD-SRV1** : [**\\CSI-TD-SRV1.contoso.com\public**](file://CSI-TD-SRV1.contoso.com/public)
   2. Open **File1.txt**
   3. Close File1.txt
9. Close the **Explorer** windows
10. **Stop** the capture
11. **Save** the Capture and named it **Kerberos**
12. Analysis the capture
    1. Apply the following filter
    2. **ipv4.address==10.0.0.4 or ipv4.address==10.0.0.5 or ipv4.address==10.0.0.9**
    3. **or**
    4. **TCP.port<>3389 and ProtocolName <> "TCP"**
13. Retrieve the IP Addresses of the following computers using Command Prompt and ipconfig command :
    1. CSI-TD-DC1 : ……… ……… ……… ………
    2. CSI-TD-CLI1 : ……… ……… ……… ………
    3. CSI-TD-SRV1 : ……… ……… ……… ………
14. In the next line, the IP addresses will be shown as :
    1. CSI-TD-DC1 : 10.0.0.a
    2. CSI-TD-CLI1 : 10.0.0.b
    3. CSI-TD-SRV1 : 10.0.0.c
    4. The name of the server may sometimes replace the IP address
15. Look for the following frame

|  |
| --- |
| **CSI-TD-CLI1 initiate the connection to CSI-TD-SRV1 and propose Negotiate as authentication method** |
| System 10.0.0.b 10.0.0.c SMB SMB:C; Negotiate, Dialect = NT LM 0.12, SMB 2.002, SMB 2.??? {SMBOverTCP:19, TCP:18, IPv4:17} |
| **CSI-TD-CLI1 ASRequest to obtain the TGT** |
| 10.0.0.b 10.0.0.a KerberosV5 KerberosV5:AS Request Cname: Par\_User02 Realm: CONTOSO.COM Sname: krbtgt/CONTOSO.COM {TCP:20, IPv4:14} |
| **First request failed because for Pre-auth required** |
| 10.0.0.a 10.0.0.b KerberosV5 KerberosV5:AS Request Cname: Par\_User02 Realm: CONTOSO.COM Sname: krbtgt/CONTOSO.COM {TCP:21, IPv4:14} |
| **CSI-TD-CLI1 ASRequest to obtain the TGT with pre-auth** |
| 10.0.0.b 10.0.0.a KerberosV5 KerberosV5:AS Response Ticket[Realm: CONTOSO.COM, Sname: krbtgt/CONTOSO.COM] {TCP:21, IPv4:14} |
| **KDC sent the TGT** |
| 10.0.0.a 10.0.0.b KerberosV5 KerberosV5:AS Response Ticket[Realm: CONTOSO.COM, Sname: krbtgt/CONTOSO.COM] {TCP:21, IPv4:14} |
| **Request for a TGS for CSI-TD-SRV1** |
| 10.0.0.b 10.0.0.a KerberosV5 KerberosV5:TGS Request Realm: CONTOSO.COM Sname: cifs/csi-td-srv1.contoso.com {TCP:22, IPv4:14} |
| **KDC send TGS for CSI-TD-SRV1** |
| 10.0.0.a 10.0.0.b KerberosV5 KerberosV5:TGS Response Cname: Par\_User02 {TCP:22, IPv4:14} |
| **Beginning of the SMB session** |
| 10.0.0.a 10.0.0.c SMB2 SMB2:C SESSION SETUP (0x1) {SMBOverTCP:8, TCP:7, IPv4:6} |

#### Task 2: NTLM Capture

1. Logon to **CSI-TD-SRV1** using
   1. On the credentials dialog box, enter :
      1. Username: **.\AdminCSI**
      2. Password: **PiKarAlR@AlBenMo1 (Note that l is a L in lower case)**
2. Open a command prompt as Administrator
3. Enable **Netlogon** login
4. Switch to **CSI-TD-CLI1**
5. Switch Network Monitor
6. Start a **New Capture**
7. Purge Kerberos tickets for the current user
8. Access to the shared folder on SRV1: [**\\10.0.0.c\public**](file:///\\10.0.0.c\public)
   1. Open **File1.txt**
9. Stop the capture
10. Save the Capture and named it **NTLM**
11. Capture Analysis
    1. Apply the following filter
    2. **TCP.port<>3389 and ProtocolName <> "TCP"**
12. Retrieve the IP Addresses of the following computers using Command Prompt and ipconfig command :
    1. CSI-TD-DC1 : ……… ……… ……… ………
    2. CSI-TD-CLI1 : ……… ……… ……… ………
    3. CSI-TD-SRV1 : ……… ……… ……… ………
13. In the next line, the IP addresses will be shown as :
    1. CSI-TD-DC1 : 10.0.0.a
    2. CSI-TD-CLI1 : 10.0.0.b
    3. CSI-TD-SRV1 : 10.0.0.c
    4. The name of the server may sometimes replace the IP address
14. Look for the following frame

|  |
| --- |
| **CSI-TD-CLI1 initiate the connection to CSI-TD-SRV1 and propose Negotiate as authentication method** |
| 10.0.0.b 10.0.0.c SMB SMB:C; Negotiate, Dialect = NT LM 0.12, SMB 2.002, SMB 2.??? {SMBOverTCP:19, TCP:18, IPv4:10} |
| |  | | --- | | **CSI-TD-CLI1 initiate the connection to CSI-TD-SRV1 and use NTM as authentication protocol**  **Check for the information in the Frame details** | | 10.0.0.b 10.0.0.c SMB2 SMB2:C SESSION SETUP (0x1) {SMBOverTCP:19, TCP:18, IPv4:10}  - SMB2: C SESSION SETUP (0x1)  - CSessionSetup:  - securityBlob:  - GSSAPI:  - InitialContextToken:  - InnerContextToken: 0x1  - SpnegoToken: 0x1  - NegTokenInit:  + MechToken: **NTLM NEGOTIATE MESSAGE** | |  | |

1. Why the authentication was NTLM and not Kerberos ?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

1. Go to **CSI-TD-SRV1**
2. Open the file **%windir%\debug\netlogon.log**
3. Analyze the path through authentication between **the CSI-TD-SRV1** and **CSI-TD-DC1**
4. Open a **command prompt as Administrator**
5. Disable Netlogon login

## Questions:

1. Why was the authentication NTLM and not Kerberos?

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

## After the Lab

Duration: 10 minutes

In this exercise, attendees will deallocate any Azure resources that were started 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.

