Active Directory Attacks –

Advanced Edition

Connecting to the lab

Table of Contents

Connecting using OpenVPN	2
Download VPN Config	2
Windows setup:	3
Ubuntu/Kali setup:	4
MacOSX Setup:	5
Login using web browser	7
Copying text from host machine to lab VM	9
Copying text from Lab VM to host machine	11
Copy files from host machine to lab VM	12
Copy files from lab VM to host machine	14
ri-dec	

Connecting using OpenVPN

Download Credentials and VPN Config

Please login to the lab portal (https://advancedbootcamp.enterprisesecurity.io/) using your registered Google account and download the VPN config. If the email you used to purchase the lab is not connected to a Google account, please sign-up for one and share that with us.

You have to login over OpenVPN server and then using the Windows/Ubuntu/MacOSX host machine take a remote desktop connection to the dedicated VM in the lab with the credentials below. Noted that X is your userID. If you are studentuser41, your machine is 192.168.100.41 and your username is studentuser41:

VPN credentials: Username: studentuserX Password: Tdh13SheXS3PnCeC

VM credentials (to be used after connecting to the VPN): IP: 192.168.100.X Username: us\studentuserX Password: iWVUCsY36P8xUfTs

nideor.

Windows setup:

- 1. First of all download OpenVPN from following website: https://openvpn.net/community-downloads/
- 2. Install the OpenVPN client (default options are fine).
- 3. After completing the installation, copy the OpenVPN config files that you got to OpenVPN directory "C:\Users\<username>\OpenVPN\config\" or "C:\Program Files\OpenVPN\config"
- 4. Run OpeVPN GUI as administrator. After running, you can find it in the system tray at bottom right, and click on Connect. If you have existing configurations, choose the one for this lab.
- 5. Enter the VPN credentials in the credential prompt. If everything is fine, you will be connected to the lab.
- 6. Now you can RDP to your dedicated VM 192.168.100.X in the lab using mstsc or any other RDP client.



Ubuntu/Kali setup:

1. Install openvpn and rdesktop on the machine using following command:

```
sudo apt-get install openvpn -y
sudo apt-get install rdesktop
```

2. Go ahead and connect to the VPN server using openvpn config files. Extract the VPN config archive that you got and use it with the below command:

```
sudo openvpn --config <yourlabconfigfile>.ovpn
```

3. Use rdesktop to connect to your dedicated VM 192.168.100.X in the lab

```
rdesktop -d us -u studentuserX -p iWVUCsY36P8xUfTs 179.168.100.
Х
```

Alternatively, You can use xfreerdp to connect with the dedicated VM -

1. Install xfreerdp package on your machine using the following command -

sudo apt install freerdp2-x11

2. Use xfreedp to connect to your dedicated VM 192.168.100.X in the lab

```
xfreerdp /u:'us\studentuserX' /p:<Password> /cert-ignore
/drive:Tools,/home/user/Desktop/Tools /v:192.168.100.X
+clipboard
```

Note - Change the path "/home/user/Desktop/Tools" accordingly, to share local folder with your student VM

MacOSX Setup:

- Install Tunnelblick and Microsoft Remote desktop
 <u>https://tunnelblick.net/</u>
 <u>https://itunes.apple.com/in/app/microsoft-remote-desktop/id715768417?mt=12</u>
- 2. Now go ahead and add OpenVPN config file using Tunnelblick





3. Next, click on Connect to connect to the lab



- 4. Enter the VPN credentials in the credential prompt. If everything is fine, you will be connected to the lab.
- 5. Use Remote desktop application and configure the IP (PC name) and credentials. Click on start to connect.

See Microsoft's documentation for more details: https://docs.microsoft.com/en-us/windowsserver/remote/remote-desktop-services/clients/remote-desktop-mac

nideo1.ir

Login using web browser

Step 1: Browse to the server URL 'https://<ServerIP>:Port' and accept the certificate warning to open the login page:



Step 2: Enter the username and password shared with you or generated in the portal to login:



Step 3: Enter the Windows username and password shared with you. You can now access the lab VM without needing anything else.



nide01.i.

Copying text from host machine to lab VM

Step 1: After login, use **Ctrl + Alt + Shift** on the browser to open clipboard:

Studentuser	2 studentuser	•
Clipboard Text copied/cut within Guacamole will appear the text below will affect the remote clipboard	here. Changes to	〒 File Explorer me Share View ↑ ⑦ Quick access > ccess ~ Frequent folders (4) obp 0 Desktop ioads ~ This PC ments . .
Devices Shared Drive	B	es * ~ Recent files (0)

Step 2: Copy text from host machine and paste in the clipboard:

Studentuser	-
Clipboard Text copied/cut within Guacamole will appear here. Changes to the text below will affect the remote clipboard.	
This is the text from host machine	me Share View ↑
Devices Shared Drive	k

Step 3: Press **Ctrl + Alt + Shift** on the browser to copy the text to lab VM's clipboard.

Step 4: Press Ctrl + v to paste the text in notepad or any other application on the lab VM. It is recommended to use notepad when copying multiline commands.



Copying text from Lab VM to host machine

Step 1: Copy text from the lab VM.

Step 2: Press Ctrl + Alt + Shift to open the clipboard. The text you copied from the lab VM will be there.

Studentuser	👱 studentuser 🐌 👻	
Clipboard		
Text copied/cut within Guacamole will appear he the text below will affect the remote clipboard.	here. Changes to	
inis is the text from lad vm	$\leftarrow \rightarrow \checkmark \uparrow \checkmark > Quick access >$	
	File Edit Format View Help This is the text from Lab VM	
Devices		
Shared Drive	· · · · · · · · · · · · · · · · · · ·	
Input method		

Step 3: Copy the text from the clipboard using Ctrl + c and paste it in any application on your host machine.

Copy files from host machine to lab VM

Step 1: Press **Ctrl + Alt + Shift** in the browser window and click on Shared Drive. Click on 'Upload Files' and browse to the file that you want to upload:



Step 2: You can check the file transfer status at the bottom right corner:





Step 3: Access the file from a folder called 'Shared' on user Desktop on lab VM.

nideor.ir

Copy files from lab VM to host machine

Step 1: Copy the file you want to download to the folder named 'Shared' on user Desktop on the lab VM. Press **Ctrl + Alt + Shift** on the browser window and click on 'Shared Drive'. The file you copied to the 'Shared' folder will be visible:



Step 2: Double click the file you want to download:

← → ♂ ☆ \$	🛈 🐔 https://51.89.7.105/#/dient/ZW1wbG5	95ZWUxMABjAGRIZmF1bHQ=				… ⊠ ☆
Shared Drive	Upload Files 🗸 Back					
=						
FileFromVM.txt						
		. 📙 🖓 😽 🖛 Shar	red			
		File Home S	Share View			
		y → ~ ↑ 📙	> Shared			
		- Ouistansee	Name	Date modified	Туре	Size
		Desktop	FileFromVM	9/20/2019 7:18 AM	Text Document	1 KB
		🕹 Downloads	*			
		😫 Documents	*			
		E Pictures	Opening FileFromVM.txt		×	
		This PC	You have chosen to open:			
		- Inis Pe	FileFromVM.txt			
		- Network	which is: Text Document from: https://51.89.7.105			
			What should Firefox do with t	his file? fault)		
			Save File	(and the second s		
			Do this automatically for	files like this from now on.		
				OK Cancel		