NTS103 Malware Removal Lab Assignment

Mohanad Horani

University of Advancing Technology



To begin with, I changed the theme, which, ideally, would only take a few seconds, in order to view everything properly. The theme that the malware had by default made it extremely hard to read the screen, so this makes optimizing the VM much easier.

uttons	Pointers	Pointer Options	Wheel	Hardware	
Butto	n configura	tion	-		
	witch prima	ry and secondary	buttons		an a
Selec	t this chee	k box to make the	button o	n the	10
as se	lecting and	dragging.	Incuons s		
					-
Doub	le-click spe	eed			
Doub	le-click the	folder to test you	setting.	lf the	
folder	does not a	open or close, try u	using a sl	ower	100
Spee	d: Slow	O		st	6
	N 17		1204		
Click	Lock				
	um on Clic	Lock		Se	ttings
Enab	les you to l	nighlight or drag w	ithout hol	ding down the n	nouse
butto	n. To set, b e button ad	priefly press the mo gain.	ouse butto	on. To release, o	lick the

Next, I quickly opened up the mouse properties and set the mouse options to normal. By default, the malware switched the left and right mouse buttons, so being able to use the mouse normally allows more comfort, ensuring efficiency while attempting to stop the malware from spreading.

2 Change Your Password	
😋 🔿 = 🤽 - Control Parini - Usiar Veccounts and Fearly Solidy - User Accounts - Usinge Your Parsmant	Search Control Panel
Change your password	
The password hirt will be visible to everyone who uses this computer.	

Next, I changed the default password, "P@ssw0rd" to a custom password, so that the "hacker" can't get access via the main administrator account. This helps to prevent another way for the hacker to get into the system.



In the meanwhile of accomplishing all of this, I have been deleting all of the command prompts that have been appearing as annoyances every minute, before I have been able to stop the scheduled tasks, in order to prevent lag, in the meanwhile, for more efficiency.



At a certain point, I finally deleted all of the scheduled tasks in the task scheduler. This stops the scheduled annoying four command prompts every minute as well as stops the updating hacker user accounts and the hacker files showing up in several places in the system every five minutes.

```
Administrator: C:\Windows\System32\cmd.exe
                                                                                                        0
                                                                                                                    23
Hacker82
                                     Hacker83
                                                                          Hacker84
                                                                                                                       .
                                                                         Hacker87
Hacker85
                                     Hacker86
Hacker88
                                    Hacker89
                                                                         Hacker9
Hacker90
                                    Hacker91
                                                                         Hacker92
Hacker93
Hacker96
                                    Hacker94
                                                                         Hacker95
                                    Hacker97
                                                                         Hacker98
theAdmin
The command completed successfully.
                                                                                                                      Ε
C:\Windows\system32>net User Hacker98,Hacker97 /delete
The syntax of this command is:
NET USER
[username [password | *] [options]] [/DOMAIN]
username {password | *} /ADD [options] [/DOMAIN]
username [/DELETE] [/DOMAIN]
username [/TIMES:{times | ALL}]
C:\Windows\system32>net user Hacker98 /delete
The command completed successfully.
C:\Windows\system32>net user Hacker97 /delete
```



Next, I deleted all of the hacker accounts, which can be used in order to gain access to the main administrator accounts via the command line, as they are all administrator accounts as well. I deleted them one by one in the command line using the command "net user <ACCOUNT> /delete" for every account. An alternative which could take much less time would be to create a batch file that runs a script to delete all of the accounts, but I thought of this AFTER I deleted all of the accounts, so I did not do that.

Drganize 🔻 🛛 🛜 Open	Share with 🔻 New fold	er			8== *	
Favorites	Name	Date modi	fied Type	Size		
E Desktop	lol	Re21 Team	n O Cloc File folder			
Downloads	Hacker.1.30822	Re21 Team	n O Cloc 30822 File	1 KB		
🖳 Recent Places	Hacker.2.30822	Re21 Team	n O Cloc 30822 File	1 KB		
	Hacker.3.30822	Re21 Team	n O Cloc 30822 File	1 KB		
Libraries	Hacker.4.30822	Re21 Team	O Cloc 30822 File	1 KB		
Documents	Hacker.5.30822	Re21 Team	O Cloc 30822 File	1 KB		
J Music	Hacker.6.30822	Re21 Team	O Cloc 30822 File	1 KB		
Pictures	Hacker.7.30822	Re21 Team	O Cloc 30822 File	1 KB		
Videos	Hacker.8.30822	Re21 Team	n O Cloc 30822 File	1 KB		
	Hacker.9.30822	Re21 Team	O Cloc 30822 File	1 KB		
📮 Computer	Hacker.10.30822	Re21 Team	n O Cloc 30822 File	1 KB		
🚮 Local Disk (C:)	Hacker.11.30822	7.7	o	1 KB		
DVD Drive (D:) GSP1	Hacker.12.30822	7-Zip	oc 30822 File	1 KB		
	Hacker.13.30822	CRC SHA	oc 30822 File	1 KB		
Network	Hacker.14.30822	Share with	• oc 30822 File	1 KB		
	Hacker.15.30822	Sendto	oc 30822 File	1 KB		
	Hacker.16.30822	Send to	oc 30822 File	1 KB		
	Hacker.17.30822	Cut	oc 30822 File	1 KB		
	Hacker.18.30822	Сору	oc 30822 File	1 KB		
	Hacker.19.30822	Create shortcut	oc 30822 File	1 KB		
	Hacker.20.30822	PEIEte	oc 30822 File	1 KB		
		Rename				
		Properties				

Next, now that these Hacker files are no longer being added every five minutes, I deleted all of them from the system, showing a more clean look without as much influence from the "hacker". This could potentially be a way for the hacker to get into the system, so it is important to finally delete all of the files.



In this screenshot, I turned off network discovery as well as file and printer sharing. The reason for that was to defend against the malware for this lab primarily. This was done simply by going to the control panel and then clicking on network and internet settings as displayed in the screenshot.



In this screenshot, I deleted all the unnecessary text of the hosts file. The reason for that was

primarily in order to connect to the internet on the VM properly.

	000 MT Network Conne	ection
		Configure
his connection uses	the following items:	
Client for Mic	crosoft Networks	
GoS Packet	Scheduler	Networks
Internet Protect	ocol Version 6 (TCP/IP)	v6)
Internet Prot	ocol Version 4 (TCP/IP)	(4)
🗌 🔺 Link-Layer T	opology Discovery Map	per I/O Driver
📥 Link-Laver T	opology Discovery Res	ponder
Install	Lipingtal	Properties
Install	Uninstall	Properties
Install Description	Uninstall	Properties

In this screenshot, I changed the internet settings and turned off the unnecessary settings that were not required. The purpose of doing so was in order to connect to the internet on the Virtual Machine properly.

	Alternate Configuration				
You car this car for the	n get IP settings assigned a pability. Otherwise, you ne appropriate IP settings.	automatically if ed to ask your	your r netwo	network si rk adminis	upports strator
0	btain an IP address automa	atically			
- O U:	se the following IP address	-			
IP address:				,	
Subr	net mask:			,	
Defa	ault gateway:		- 54		1
Pref	btain DNS server address a se the following DNS server erred DNS server:	addresses:	0.	0.1]
FICI					
Alter	mate DNS server:			•	

In this screenshot, I changed the IPv4 settings and enabled the option for the DNS server to be obtained automatically. This also was to cause the Virtual Machine to connect to the internet properly since it was not doing so beforehand. In addition, it was set at the wrong address causing the internet to not work on the VM.