OLD DOMINION UNIVERSITY <u>CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS</u> <u>Assignment #1 Traffic Tracing and Analysis</u>

Clarence Kimbrell Jr. UIN 01207106

CYSE 301 Assignment 1

1. Power On the following VMs:

kimb002 - Google Chrome				· · · · · · // F 30 - F - 0	-0-5 45-4 0-5 40	15-1-11-01		C 45 - 4 0 - 5 40 45 - 6 46 00 - 64	4520-5-0 -0-6 45-4 0-5 4245-4-44	-00	-
inect.cova-ccl.org/nti	ps-9440/portai.tab.cova-cci.org/	console/lib/hovivc/vnc_auto.nt	mispatn=vik	/vm/1556a5e0-	eoeo-4580-occ5-115	45cre4rc0/pro	xyoduuid=1556a5e0-eoe	6-458d-6005-11545CTe410000101e	=15368560-6666-4580-6005-1154501641	tootattached=faise	anypervisorType=kKVm
d (encrypted) to: CYSE	-ckimb002										
	Eile Action View Help		-								
	Hyper-V Manaper										
	CYSE-CKIMB002	Virtual Machines							CVSE-CKIMB002	•	
		Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati	Quick Create		
		Attacker Kali - External Wo	Running	10%	8192 MB	00:01:52		9.0	New	,	
		Ubuntu 64-bit	Running	34%	4096 MB	00:01:26		9.0	Import Virtual Machine		
		Windows Server 2008 R2	Running	10%	2048 MB	00:01:22		9.0	Hyper-V Settings		
									Virtual Switch Manage		
									J Virtual SAN Manager		
									Edit Disk		
									Inspect Disk		
									Stop Service		
	-6								K Remove Server		
		Checkpoints							Befresh		
		E- By Windows Server 2008	R2 x64 - (7/29/	2021 - 11:32:44 PM					View	•	
		Now							Help		
									Windows Server 2008 R2 xb	-	
									Connect		
									Settings		
									Turn Off		
									Shut Down		
									Save Save		
									II Pause		
		Windows Server 2008 P2	~64						IÞ Reset		
		WINDOWS SERVER 2000 HZ									
		Created		7/24/2021 9:14:16	PM		Clustered:	No	5 Revert		
		Configur	ation Version:	9.0			Heartbeat:	No Contact	Move		
		Generat	ion:	1	200002				Export		
		notes.		192.168.10.11	200012				E Rename		
				Password: Password	r d123				I Help		
		a Harrison Harrison	1								
		Summary Memory Network	ung								
	- 0 H I	Hvper-V Manager 🛛 🛄 pF	sense - Firewal	16 🦭 Ubun	itu 64-bit on C 📃	Windows Serv	wr 20			8:00 PM	

The Hyper-V Manager displays all the virtual machines being powered on. Such Attacker Kali, pFense, Ubuntu, and Windows Server 2008.

2. Find the IP address of the following VMs:



In Ubuntu 64-bit, one way of finding out the IP address is by using the ifconfig command in the terminal. The result was 192.168.10.10.

Recycle Bin	Windows Server 2008 R2 xt File Action Media C Ba (a) (a) (a) (a) (a) (b) (b) (b) (b) (b) (b) (b) (b) (b) (b	4 on CYSE-CKIM8002 - Virtual Machine Con lipboard View Help ▶ 🔂 🕽 🖳 🏙	nection		×
	File Action View Help				
Diama di Antonio di An	(a = a) [] [] Server Manager (W2008R2) (i)] Roles (i)] Peatures (i)] Diagnostics (ii) Configuration	Server Manager (W2008R2)			
Zenmap GUI		Get an overview of the st	atus of this server, perform top management tasks, and add or ren	OMINION / ERSITY	
Nutaria SSR	(E) Es storage	Server Summary		Server Summary Help	-
Wirebank Virishali Login info		Computer Information Full Computer Information Full Computer Information Workgrauer Workgrauer WorkgrauerInformation ServerMagerRemote Newsgrammetic Preduction Control Alows me this canado	W2008K2 WCR6582C0,# 192, Hill, Di, 11 IPv4 address assigned by DHCP, IPv5 enabled Enabled Daabled S0645-365-2218K314-K322 (Activated) a st Jogan	Charge System Properties Charge System Properties Charge Renot Dealtoo Configure Renot Dealtoo Configure Server Manager Remote Heavypenett	
VMaare Workstaf		Security Information Windows Fremal: Windows Updates: Last checked for updates: Last instaled updates: Windows Updates: Exhanced Security Configure Last Refresh: Today at 5:53 PM. C	Public On Not configured Never Never Never Statistic On for Adventures Statistics Statistics	Cost Windows Prevail Configure Loaders for Each for Hear Roles for Check for Hear Roles for Startic Configure bit BSC	
	Arstart 🛃 🛃	lovs Explore		(b 5:53 PM 9/8/202	o, contact the ITS Help Desk: 92 itshelp@odu.edu 2 ■

Windows server 2008 makes it simple to figure out the IP address. Once the virtual machine is running within the server manager there is a server summary tab. Then it displays many things but we are looking for the IP address which is the third thing listed. The result was 192.168.10.10.



Attacker Kali virtual machine is similar to Ubuntu in that they use the same command to find the machine's IP address. The result was 192.168.10.13.



3. Verify the connection between Kali Linux VM and Ubuntu VM using the ping command.

For this, I used the ping command with the IP address of the other virtual machine. Not sure why it says host unreachable. Tried many other IP addresses, and the only one that seemed to work is the lo one which was 127.0.0.1. I thought this would only ping itself so there wasn't any communication between them. I'm still slightly confused by this.

Task B: Practice with Linux Commands



The image above is tasks 1-4. The first task is to display your directory in the terminal and mine is in the home directory. The second task requires you to echo your print name into the terminal. This is fairly simple and the echo command repeats what you type in a new line. Then the third task states you repeat the above command but split it into two separate lines. This is done by using the \n function in the command line. This will split the text where ever you place \n in this case it was in between first and last name.



To create a new file from the terminal, you can use the command line touch function, allowing you to create one without ever leaving it. The file size is 0.



Question 6 states to create a new directory named after your MIDAS ID which is done by the mkdir command followed by MIDAS ID. This will create a new file that is named after yourself in the home directory. The file size of this folder is 0, there is no data in it yet.



Task seven is to copy the /etc/passwd file into your home directory. This is done by using cp which stands for copy followed by /etc/passwd then where you want it to go. In this case, it is the home directory. Then the following step requires you to display the first six lines of the file. This can be done by using the head followed by a "- "and the number of lines you would like to see. Then the second task for this question is to do a keyword search in this file. This is done by using the grep function followed by the destination of the file. The results were that www appeared six times.