LAB – 10 prelab

- ☐ **All screenshots, must have your username at command prompt and screenshot should be legible.** Snipping tool is advised for the screen shots, no full page screenshot.
- ☐ **For LAB REPORT, The screenshots should be pasted in Word Document in order of the lab questions and submitted in Blackboard as a single document only. Plagiarism is awarded zero.**
- ☐ Refer to course details posted in BB for more info on Lab report and screenshots.
- ☐ **Do NOT login as root or user with UID=0 to do the lab, use sudo ONLY when required.**

If *nnnn* is specified in the lab, it is your last four digits of your humberid which starts with n

- ☐ **Do not use changeme username** to do the lab, the lab(s) MUST be done using your own username as specified in PART-B of LAB-1
- ☐ **Strictly NO screenshots with full screen of terminal or desktop or partly taken screenshots**
- ☐ **It is highly required to following naming conventions and instructions and it would affect evaluation.**

Reference to your course resources could be required

PART-A: WINDOWS NETWORKING

1. In command prompt, type **ipconfig /all** and note the available information **(SCREENSHOT)**
2. Display the routing table using **route** and **netstat** command **(SCREENSHOT)** and find various options available with **route** and **netstat** command and try it out

   (SCREENSHOT doskey /HISTORY)

PART-B: LINUX NETWORKING

MONTREAL VM

3. Check if toronto VM's full hostname and short hostname are mapped to toronto IP in montreal VM's /etc/hosts, if not need to be mapped.**(SCREENSHOT)**
4. Display the ip address, MAC address, packet statistics, netmask, broadcast address of NIC ens192. **(SCREENSHOT)**
5. Display your hostname, using **hostname**, **hostnamectl**, **uname** and **nmcli** commands. **(SCREENSHOT)**
6. Use **hostname** command to find short hostname, long hostname (FQDN), addresses for the hostname, all addresses for the domain name. **(SCREENSHOT)**
7. Use **nmcli** command with options of general, connection, networking, radio and device. **(SCREENSHOT)**
8. In montreal, **ping** (4 lines only) to toronto using IP address, hostname and short hostname of toronto. **(SCREENSHOT)**
9. Use **ip** command with addr, neigh, route **(SCREENSHOT).** Familiarise with various options available with **ip**
10. Add the following network 10.1.1.0/24 and make it static / persistent (**SCREENSHOT** of routing table and the file configured to be static) **(SCREENSHOT history |grep ip)**

TORONTO VM

11. Check if montreal VM's full hostname and short hostname are mapped to montreal IP in toronto VM's /etc/hosts, if not need to be mapped.**(SCREENSHOT)**

prof benann nathan

LAB – 10 prelab

12. In toronto, **ping** (4 lines only) to montreal using IP address, hostname and short hostname of montreal**(SCREENSHOT)**
13. Add the following network 10.2.2.0/24 and make it static / persistent (**SCREENSHOT** of routing table and the file configured to be static)
14. Type **nmcli device show ens192** and note the information given **(SCREENSHOT)**
15. Type **nmcli connection show ens192** and not the information given **(SCREENSHOT)**
16. Type **nmcli –help** and note the options available and also read **man nmcli**

PART-D Windows Firewall

17. In DC2022 VM, go to Windows Firewall with Advanced Security and familiarize with the outgoing rules, incoming rules, Connection Security Rules and Monitoring.
18. Configure DC2022 VM such that incoming pings are blocked and test it from WS2019 **(SCREENSHOT)**
19. How many profiles are there for each rule in Windows Firewall ?
20. Configure DC2022 VM such that incoming pings are ALLOWED and test it from WS2019**(SCREENSHOT)**

PART-E: LINUX Firewall

in MONTREAL VM

21. List the firewalld packages installed, display firewalld service if it is enabled & active ,
22. List firewalld config file, config file directory and firewalld templates
23. Display default firewalld zone using command line.
24. List the firewall services allowed
25. Display state of firewalld

    (SCREENSHOT: history |grep -E 'firewalld' | 'firewall-cmd')

in **TORONTO VM**

26. Display default firewalld zone using command line.
27. List the firewall services allowed
28. Allow tcp ports 443 to firewalld and list the firewall ports
29. Add smtp services to firewalld and list the firewall services
30. Allow TCP IPv4 192.168.1.21 to firewalld
31. Allow Network 192.168.2.0/24 to firewalld
32. List the services, ports, sources of firewalld in single command line**(SCREENSHOT)**
33. Display all the zones using command line **(SCREENSHOT)**
34. Display active zones using comamnd line **(SCREENSHOT)**
35. Remove tcp port 443 from firewalld
36. Remove smtp services

prof benann nathan

LAB – 10 prelab

37. Remove TCP IPv4 192.168.1.21 and list it

38. Remove Network 192.168.2.0/24 and list it

39. List the services, ports, sources of firewalld**(SCREENSHOT)**

40. Add nfs, samba to zone trusted **(SCREENSHOT)**

41. Make trusted as default zone **(SCREENSHOT)**

42. Block network 192.168.5.0/24 and display it **(SCREENSHOT)**

43. Make public as default zone **(SCREENSHOT)**

44. Remove nfs, samba from zone trusted & list services in trusted zone **(SCREENSHOT)**

45. Remove blocked access for network 192.168.5.0/24 and confirm it is removed**(SCREENSHOT)**

(SCREENSHOT: history |grep -E 'firewalld | firewall-cmd')

==========