



ubuntu - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

- nixKali
- Debian 13.x 64-bit
- pfsense(firewall)
- ubuntu

Activities

Terminal

Dec 24 18:12

```
waltro@ubuntu: ~  
Setting up python3-pkg-resources (59.6.0-1.2ubuntu0.22.04.3) ...  
Setting up libgs9-common (9.55.0~dfsg1-0ubuntu5.13) ...  
Setting up libexpat1:amd64 (2.4.7-1ubuntu0.6) ...  
Setting up libgsf-1-common (1.14.47-1ubuntu0.1) ...  
Setting up powermgmt-base (1.36ubuntu0.22.04.1) ...  
Setting up bubblewrap (0.6.1-1ubuntu0.1) ...  
Setting up gcc-11-base:amd64 (11.4.0-1ubuntu1~22.04.2) ...  
Setting up libapparmor1:amd64 (3.0.4-2ubuntu2.5) ...  
Setting up pci.ids (0.0~2022.01.22-1ubuntu0.1) ...  
Setting up apt-utils (2.4.14) ...  
Setting up linux-base (4.5ubuntu9+22.04.1) ...  
Setting up libmpg123-0:amd64 (1.29.3-1ubuntu0.1) ...  
Setting up openvpn (2.5.11-0ubuntu0.22.04.1) ...  
Setting up cups-server-common (2.4.10p1-1ubuntu4.16) ...  
Setting up libdebuginfod-common (0.186-1ubuntu0.1) ...  
Setting up libfontembed1:amd64 (1.28.15-0ubuntu1.5) ...  
Setting up linux-hwe-6.8-headers-6.8.0-90 (6.8.0-90.91~22.04.1) ...  
Setting up libgbm1:amd64 (23.2.1-1ubuntu3.1~22.04.3) ...  
Setting up alsa-ucm-conf (1.2.6.3-1ubuntu1.12) ...  
Setting up fonts-noto-color-emoji (2.047-0ubuntu0.22.04.1) ...  
Setting up linux-firmware (20220329.git681281e4-0ubuntu3.40) ...  
update-initramfs: Generating /boot/initrd.img-6.8.0-40-generic  
  
Progress: [ 56%] [#####.....]
```

To direct input to this VM, click inside or press Ctrl+G.



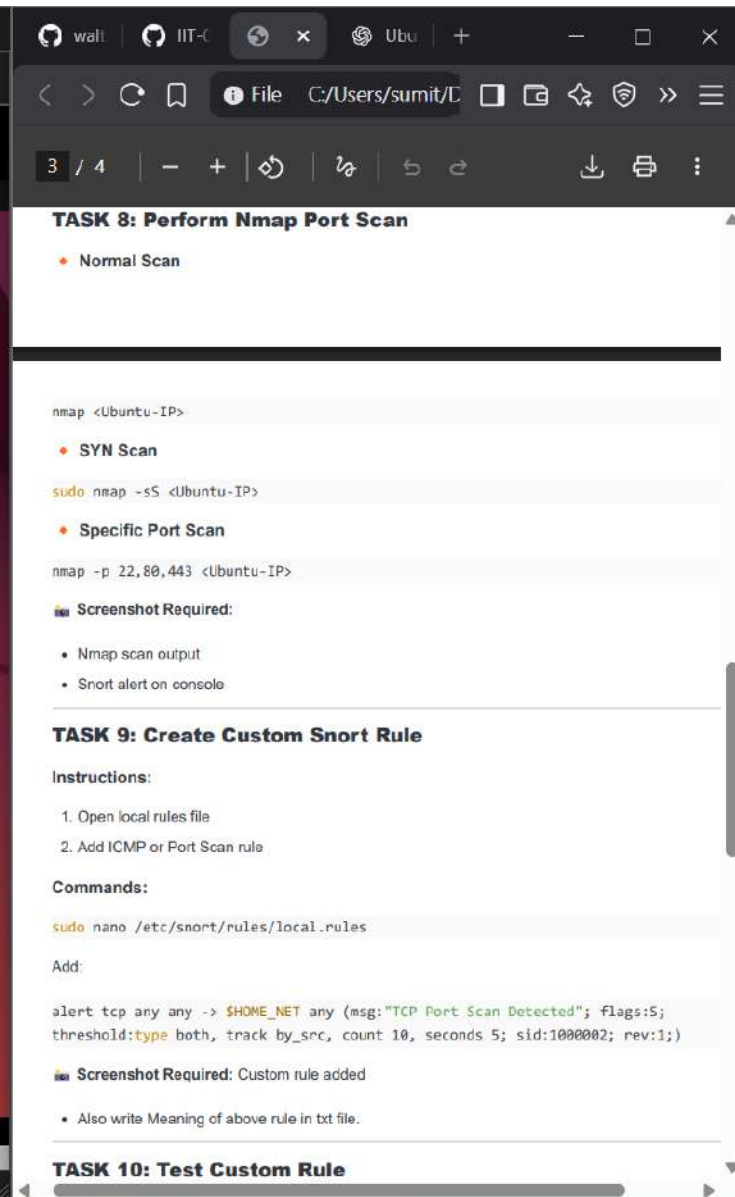
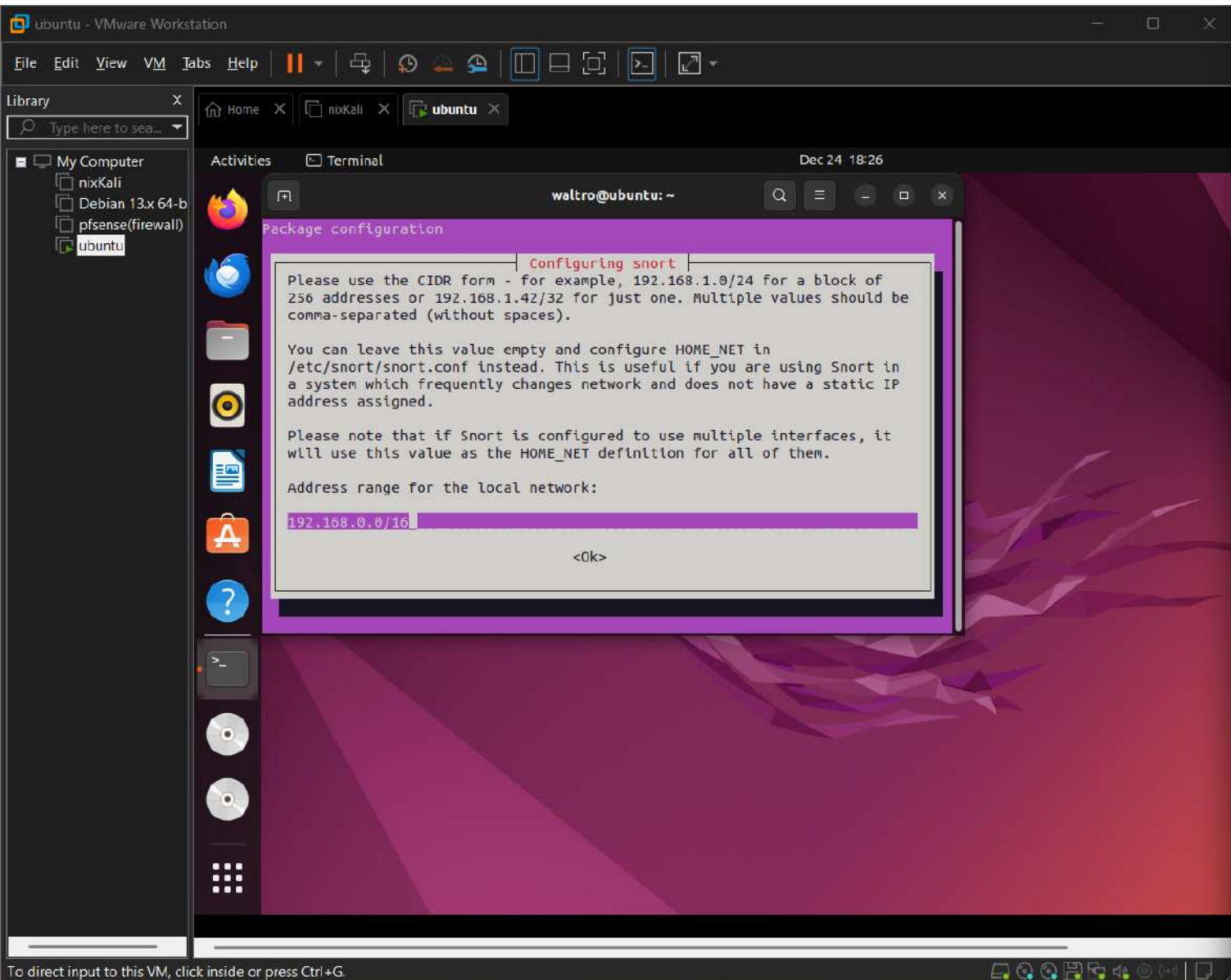
Search



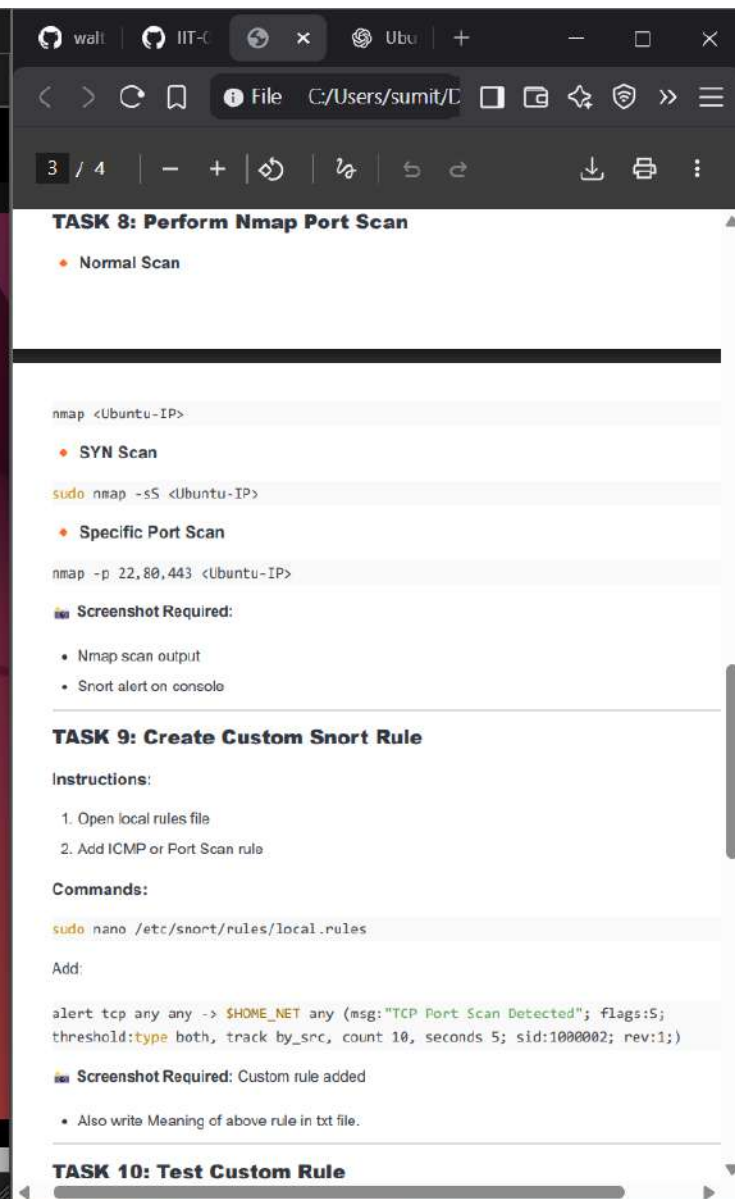
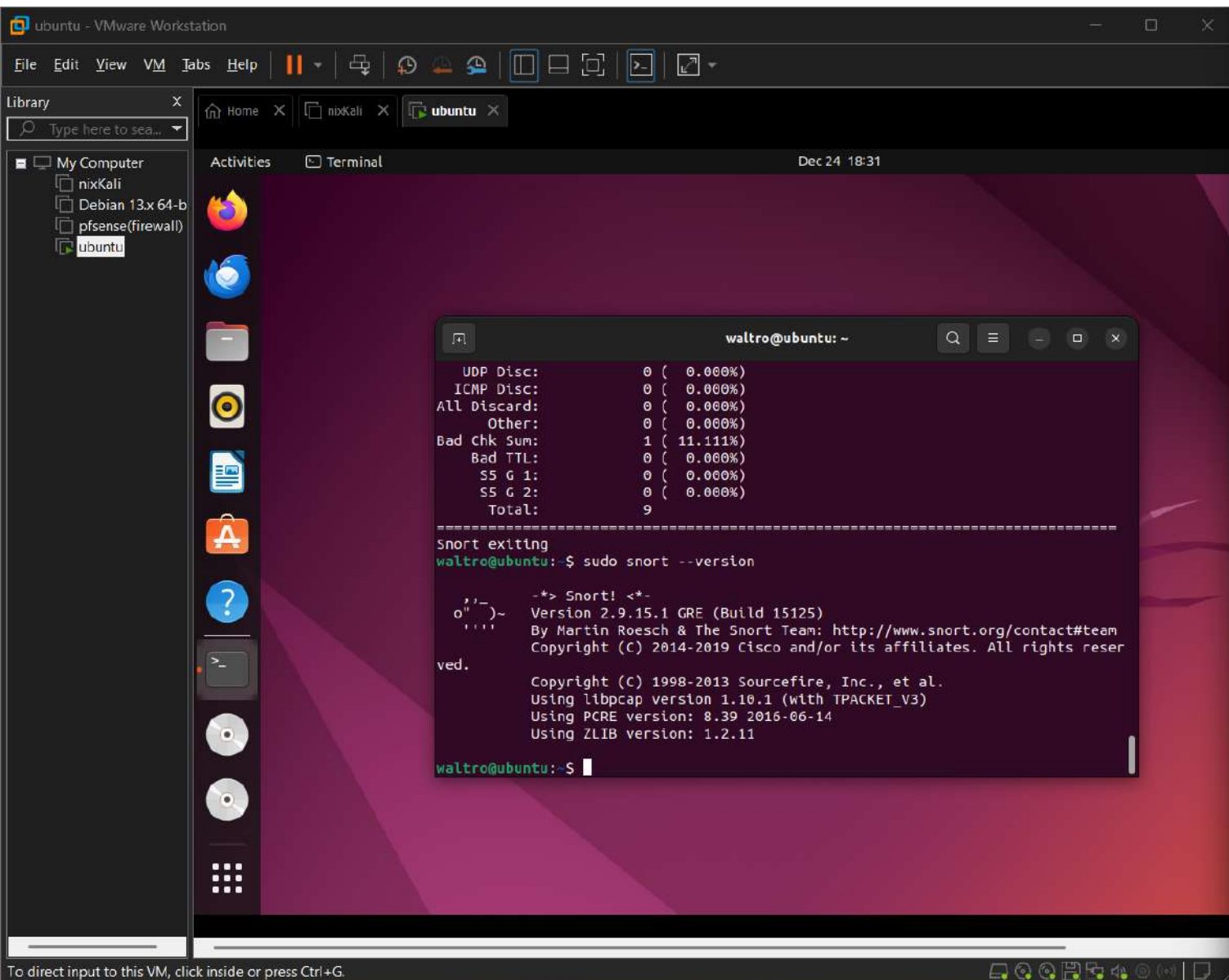
ENG
IN

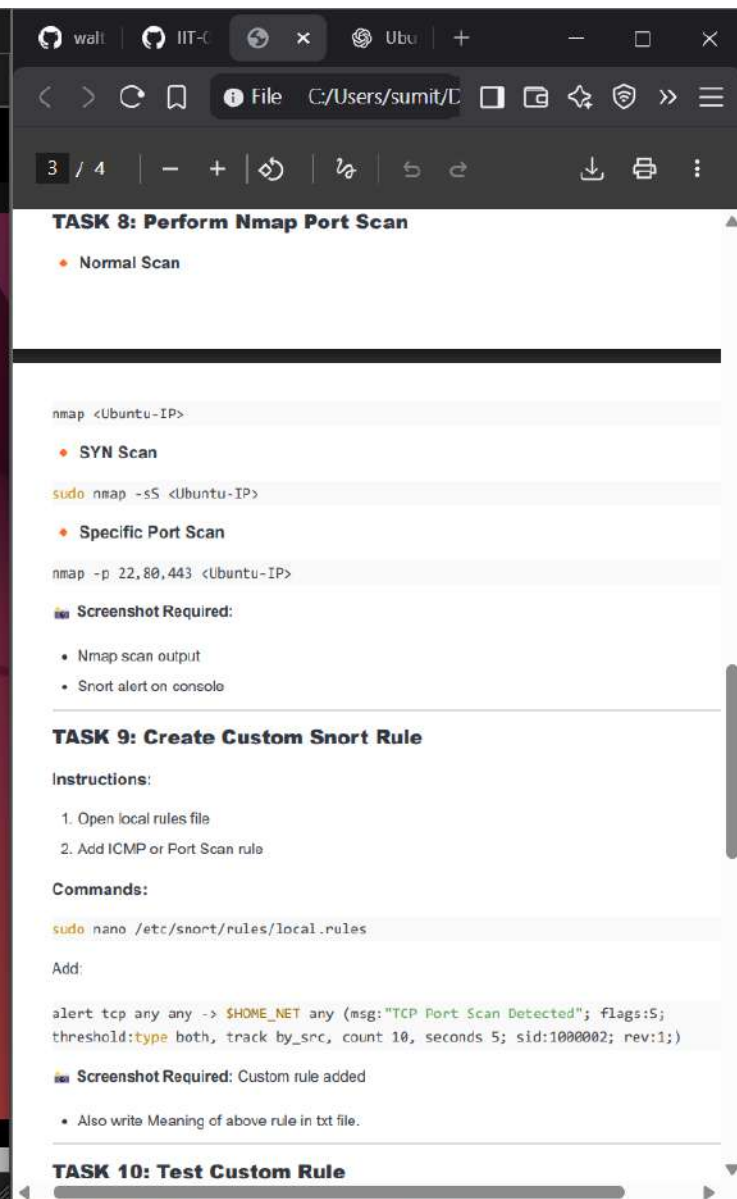
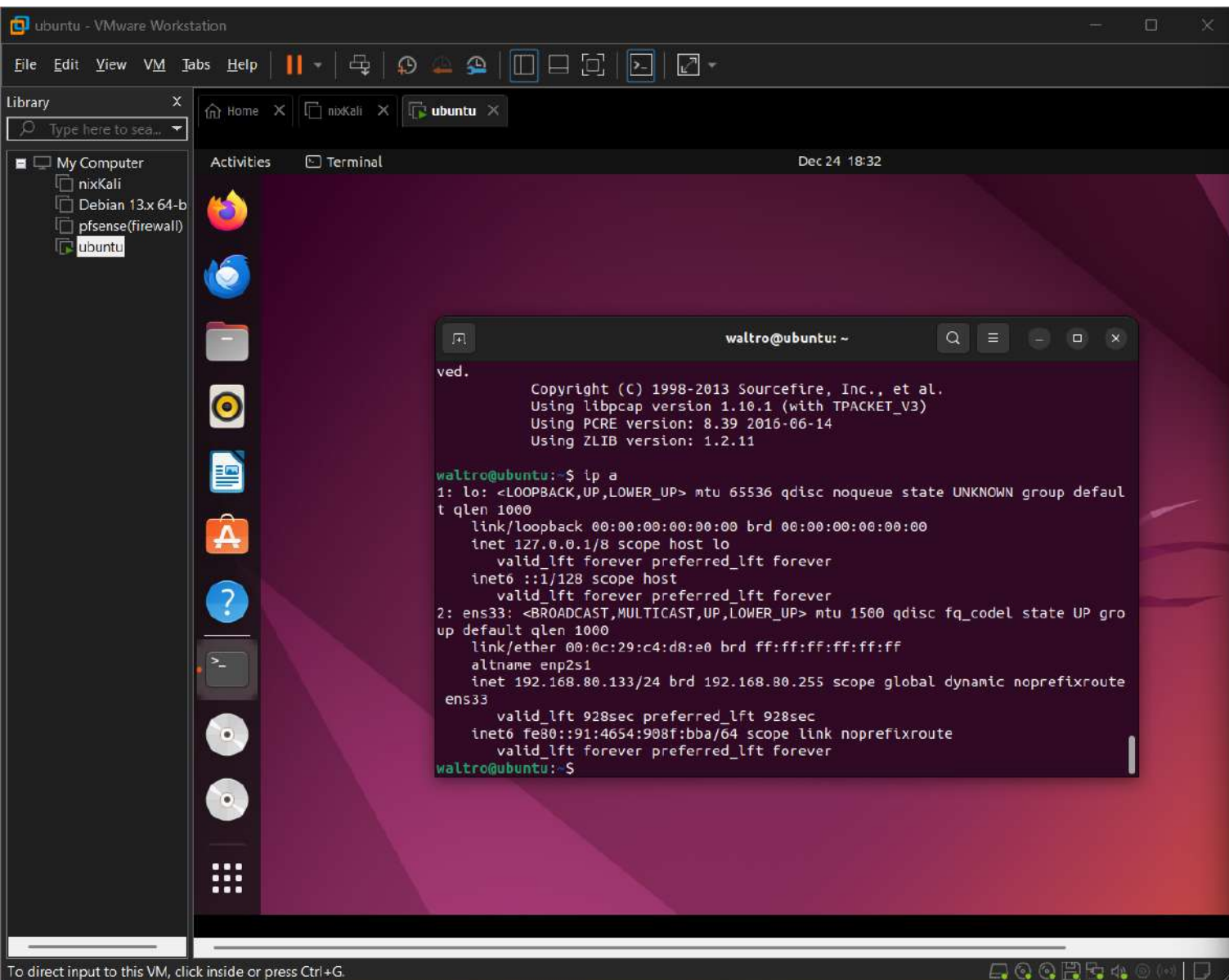


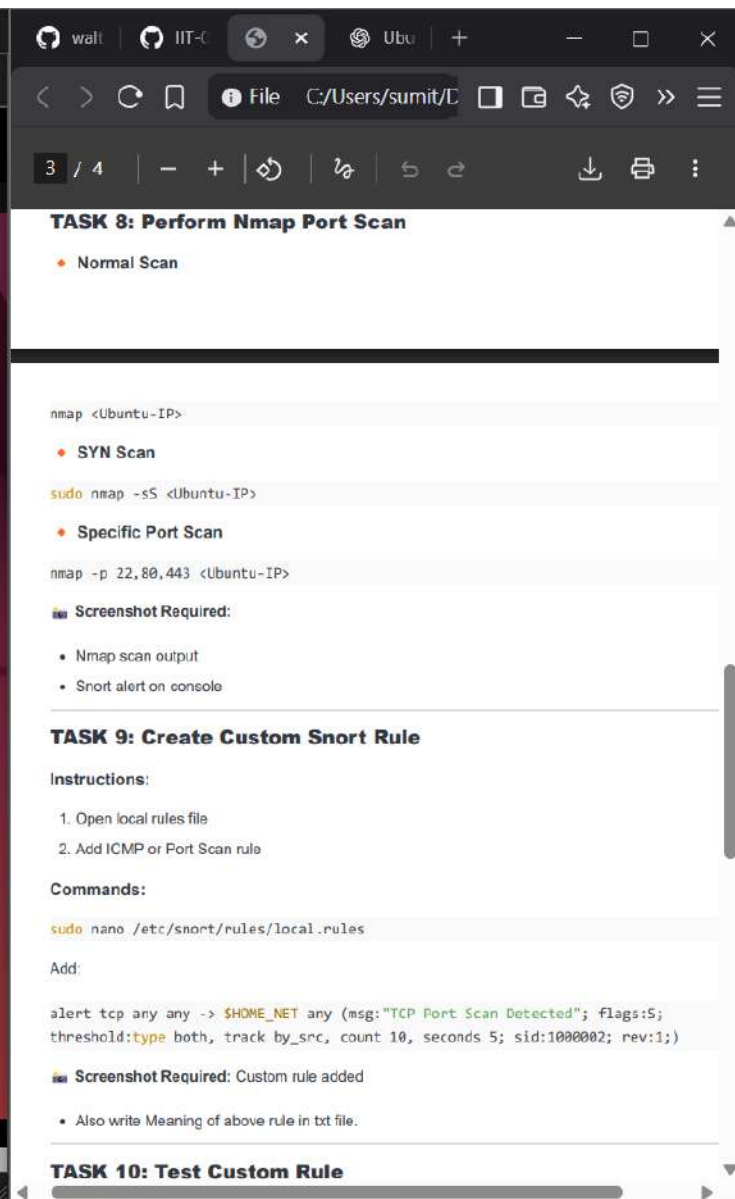
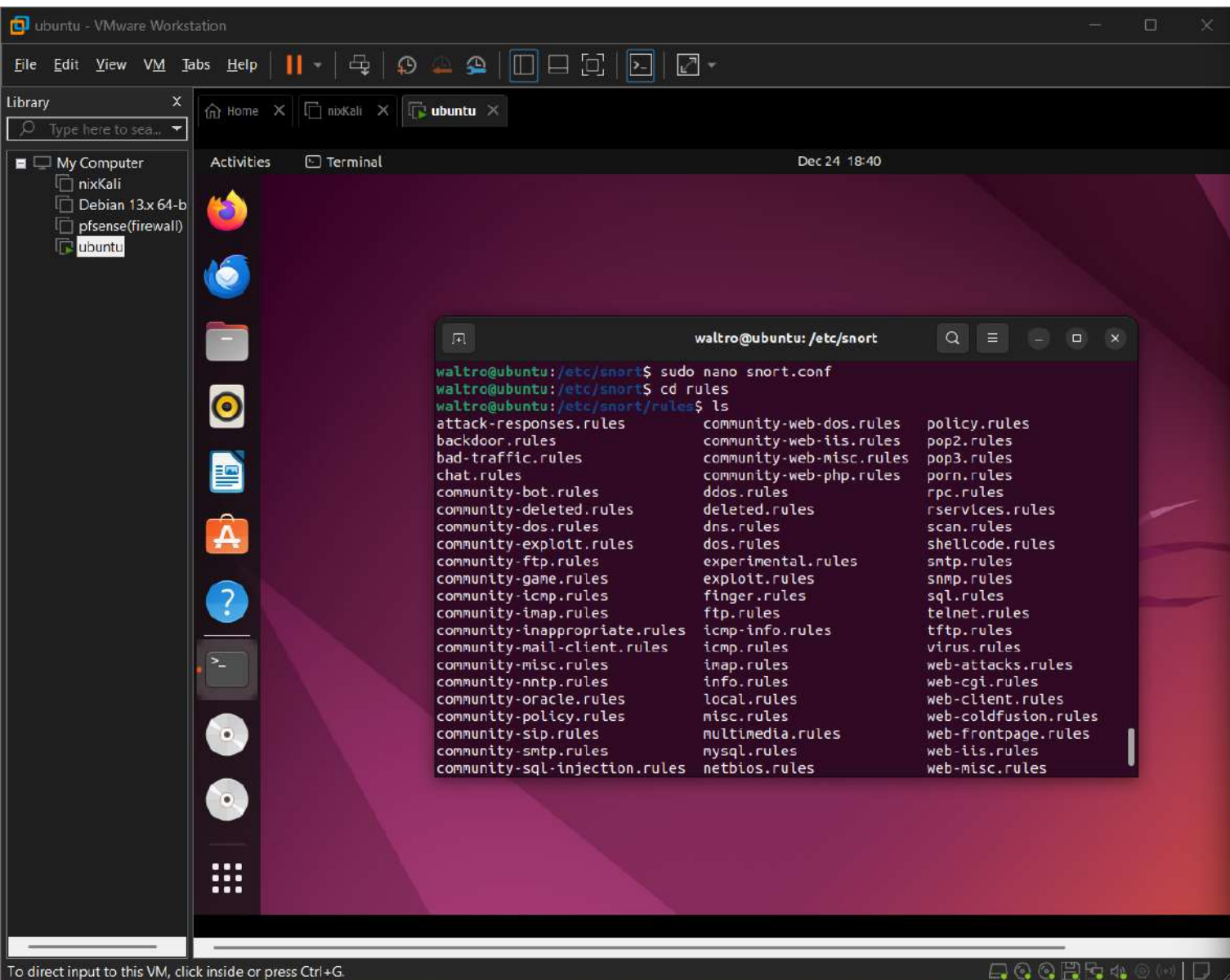
6:12 PM
12/24/2025

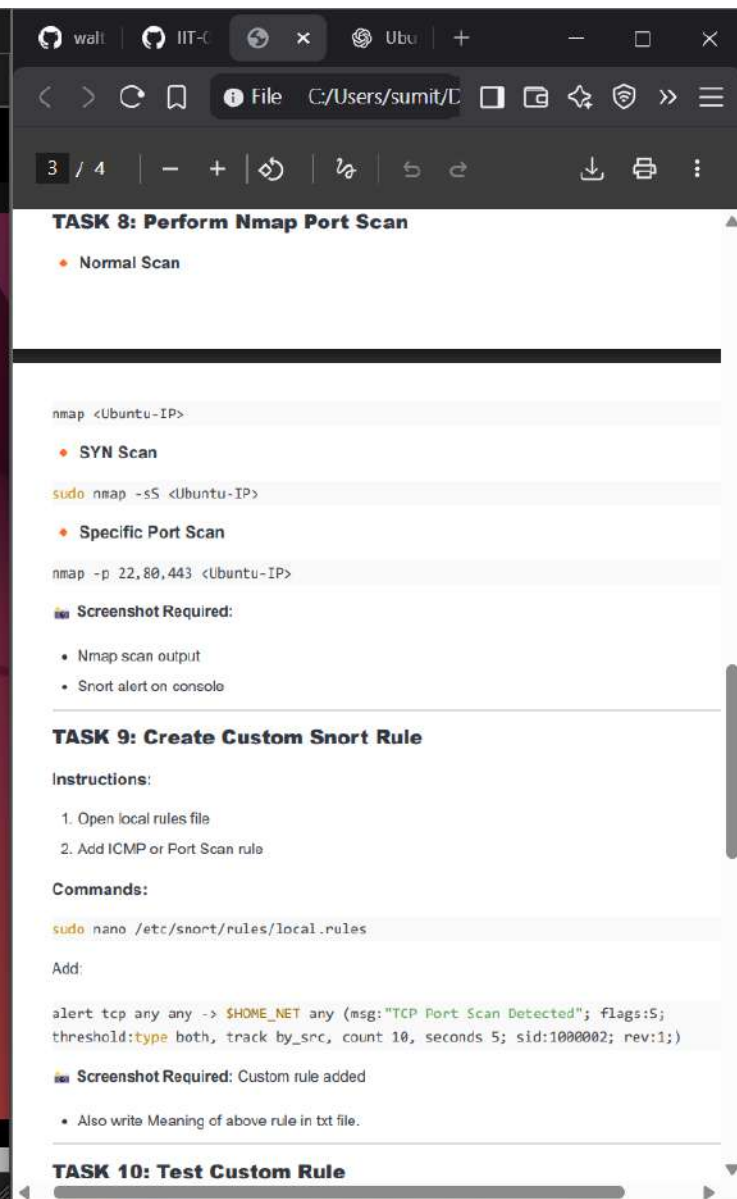
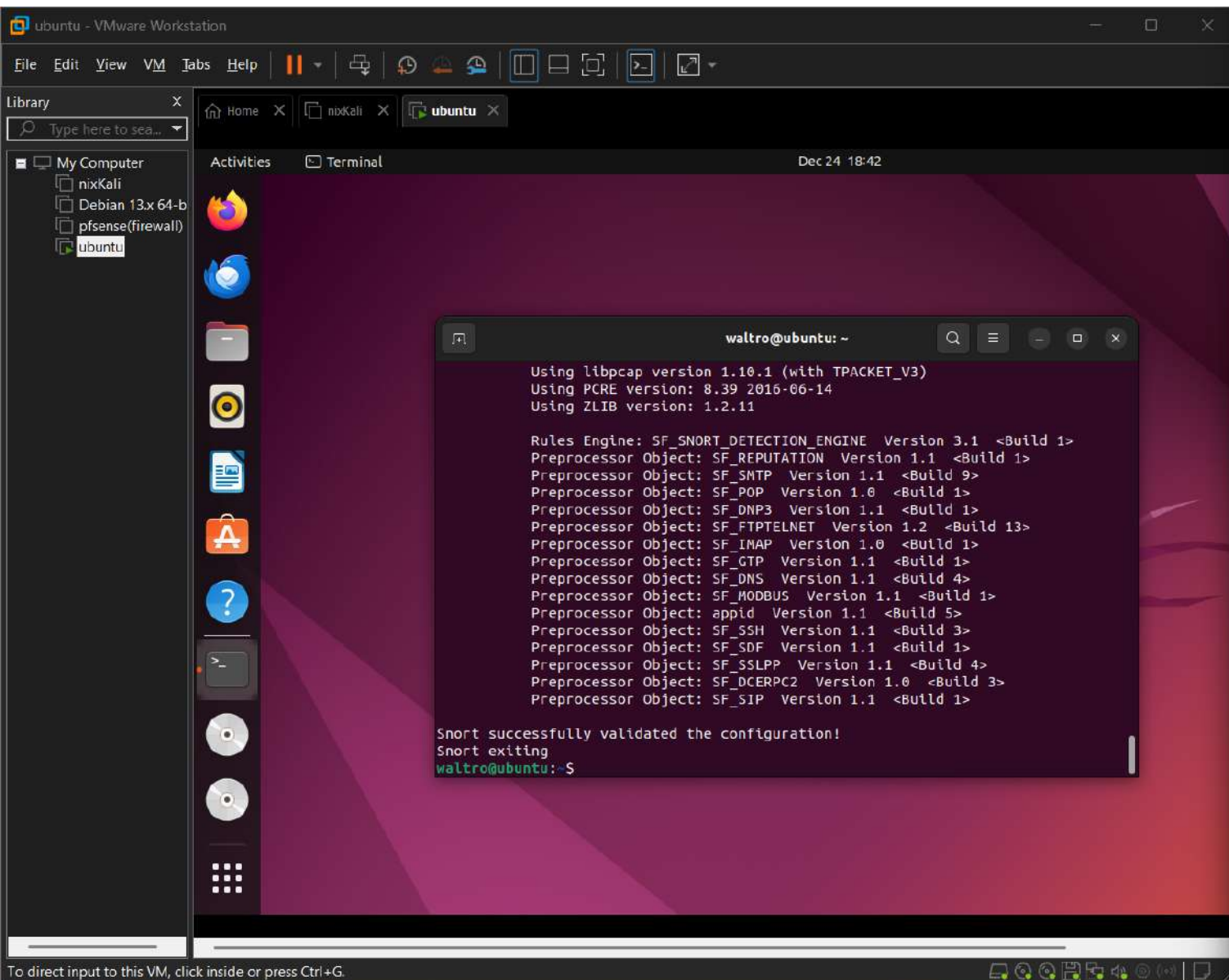


To direct input to this VM, click inside or press Ctrl+G.

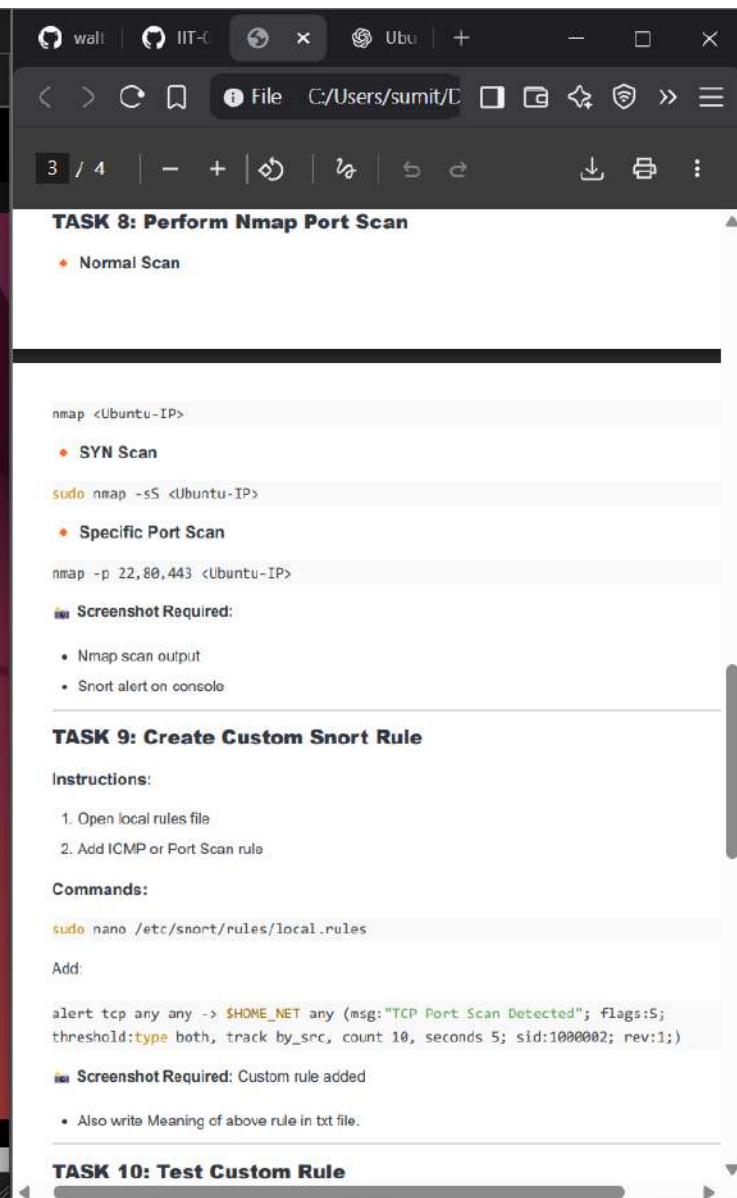
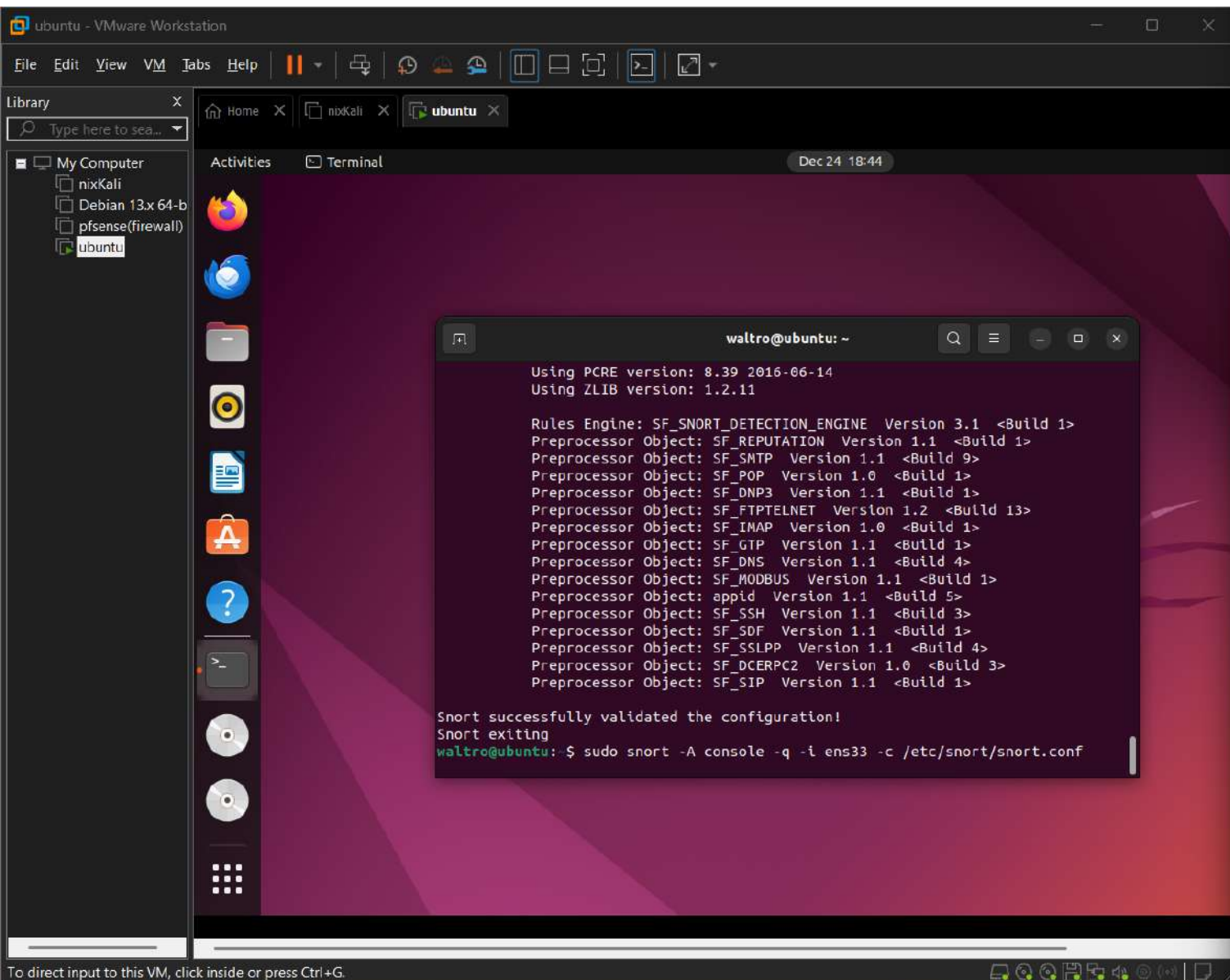




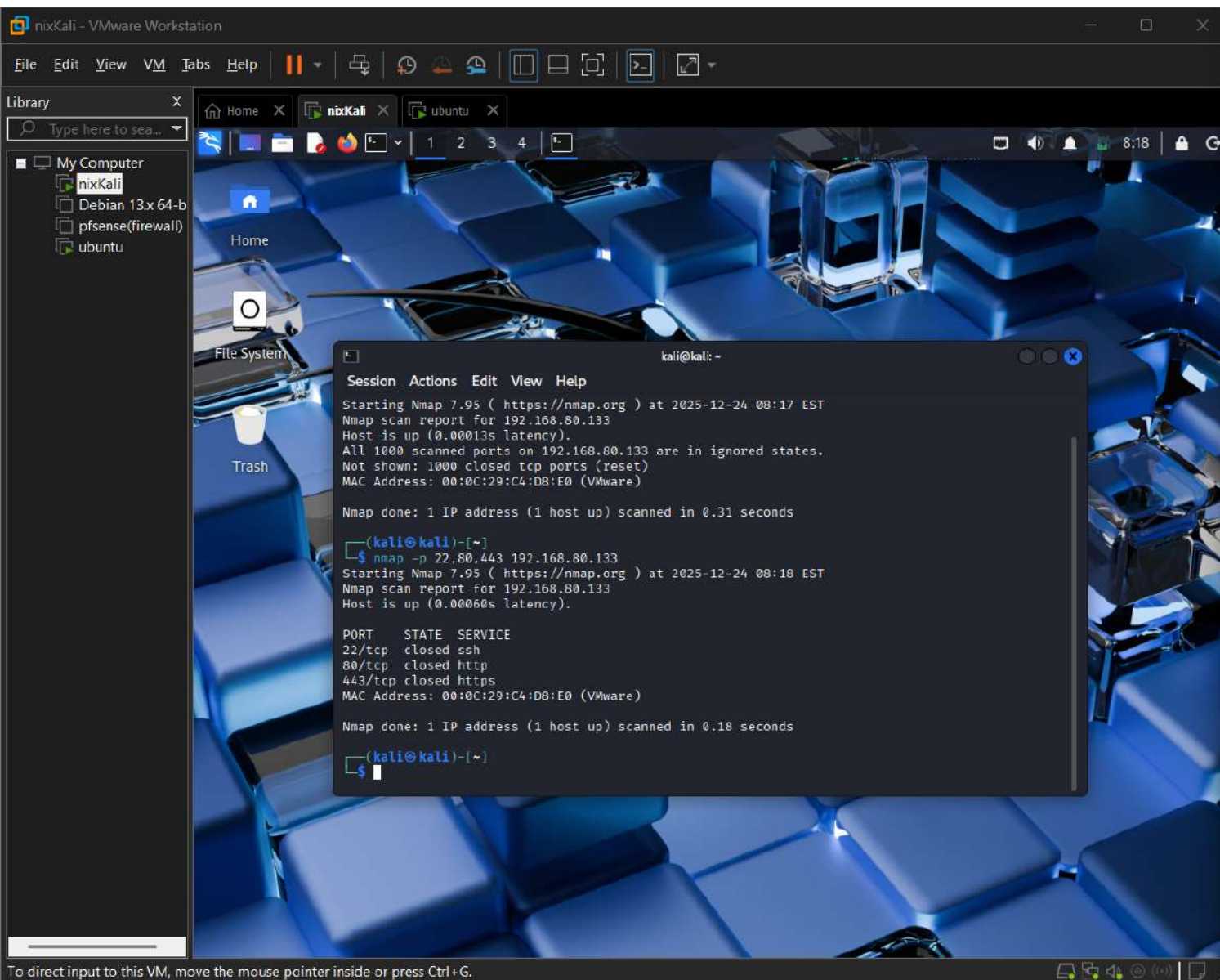




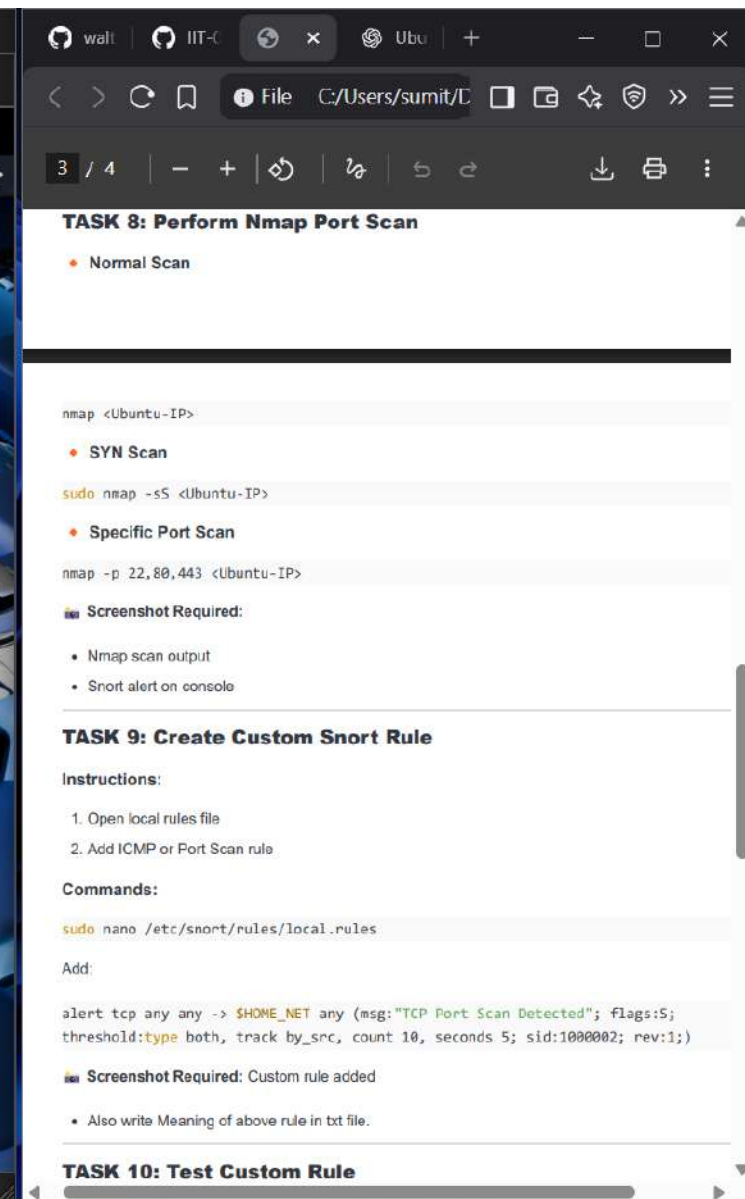
To direct input to this VM, click inside or press Ctrl+G.

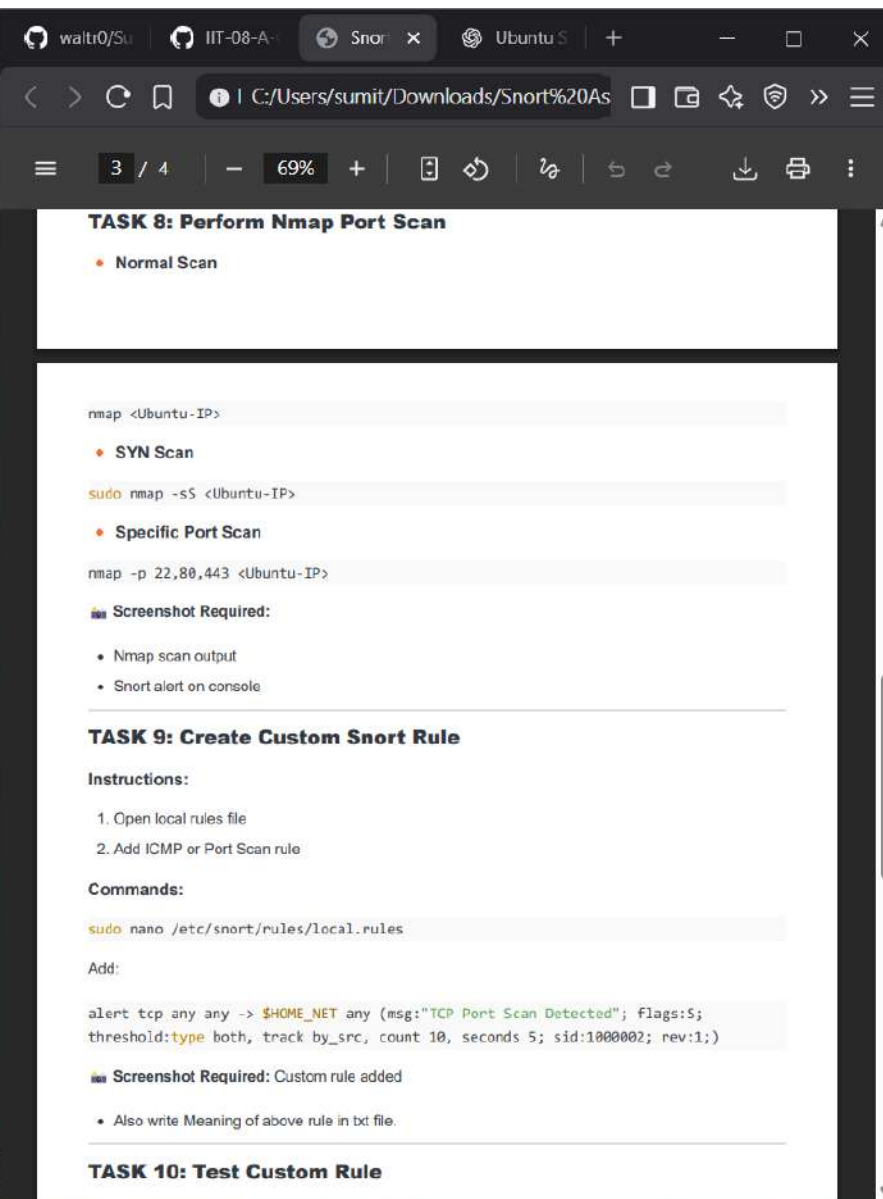
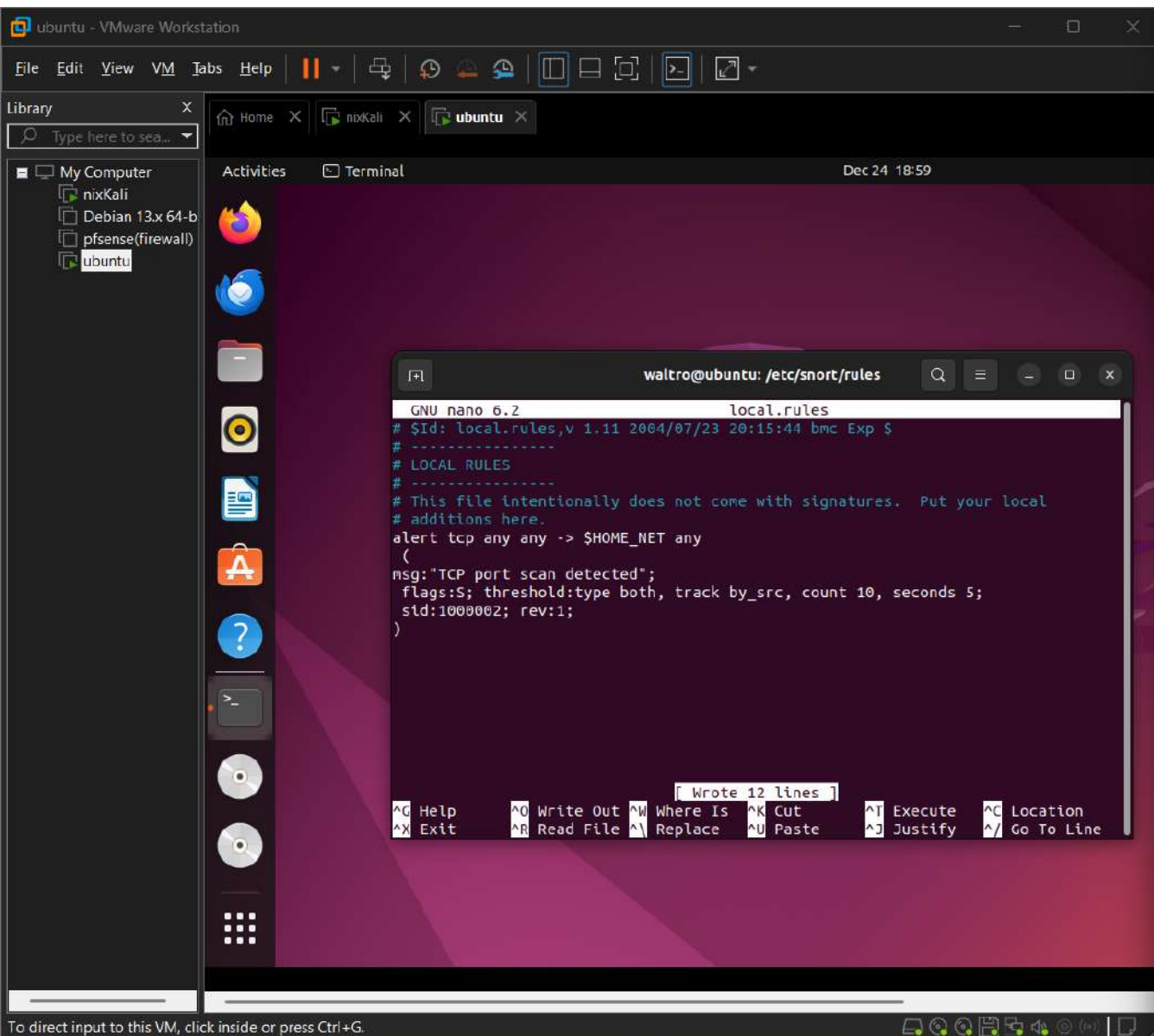


To direct input to this VM, click inside or press Ctrl+G.



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





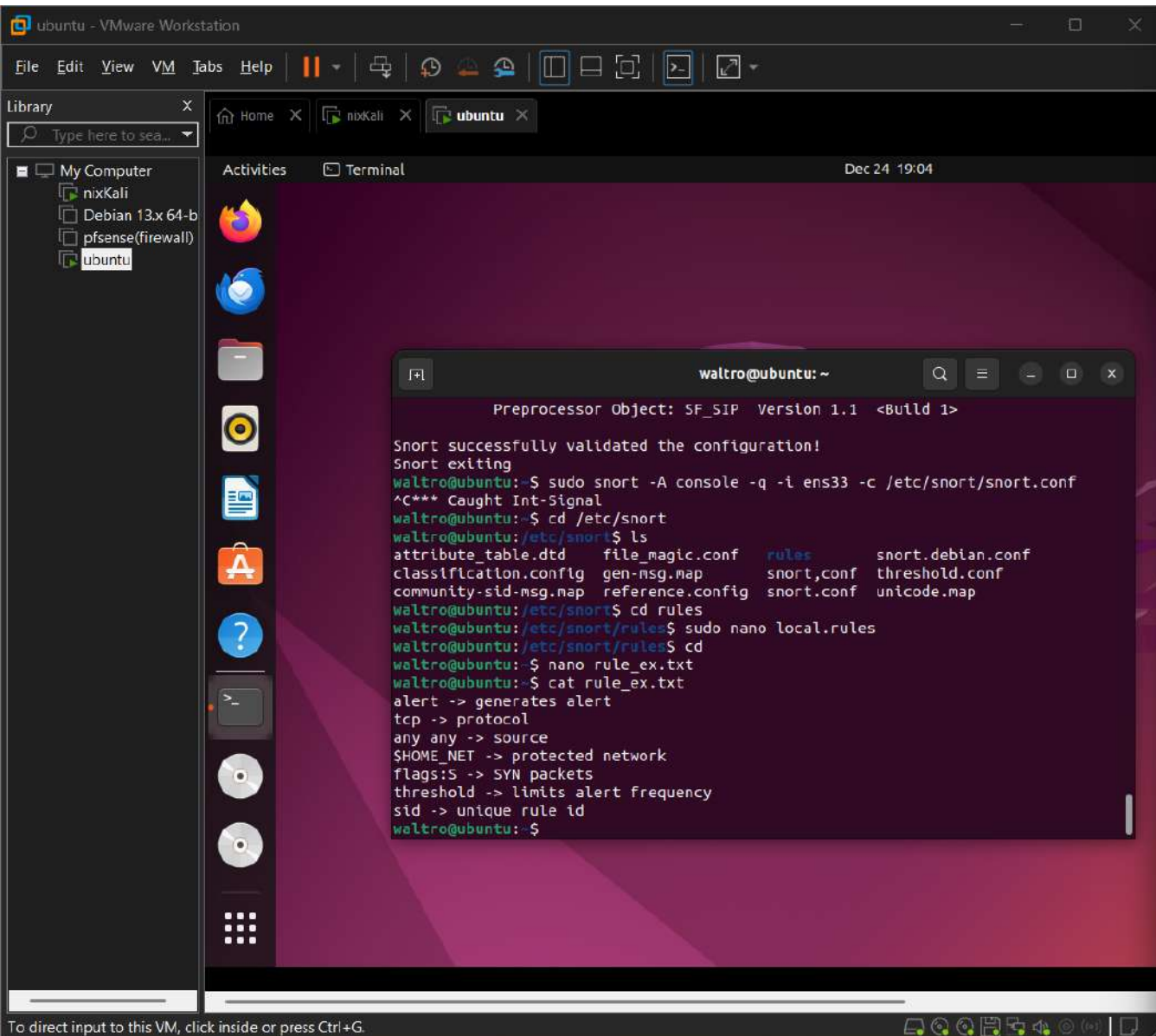
Search



ENG
IN



6:59 PM
12/24/2025



To direct input to this VM, click inside or press Ctrl+G.

waltro0/Su | IIT-08-A- | Snort | Ubuntu S | +

C:/Users/sumit/Downloads/Snort%20As

3 / 4 | 69% +

TASK 8: Perform Nmap Port Scan

- Normal Scan

```
nmap <Ubuntu-IP>
```

- SYN Scan

```
sudo nmap -sS <Ubuntu-IP>
```

- Specific Port Scan

```
nmap -p 22,80,443 <Ubuntu-IP>
```

Screenshot Required:

- Nmap scan output
- Snort alert on console

TASK 9: Create Custom Snort Rule

Instructions:

- Open local rules file
- Add ICMP or Port Scan rule

Commands:

```
sudo nano /etc/snort/rules/local.rules
```

Add:

```
alert tcp any any -> $HOME_NET any (msg:"TCP Port Scan Detected"; flags:S;  
threshold:type both, track by_src, count 10, seconds 5; sid:1000002; rev:1;)
```

Screenshot Required: Custom rule added

- Also write Meaning of above rule in txt file.

TASK 10: Test Custom Rule



Search



ENG
IN



7:04 PM
12/24/2025



The screenshot shows a VMware Workstation interface with an Ubuntu VM. The terminal window is open, displaying the output of the 'sudo snort -A console -q -i ens33 -c /etc/snort/snort.conf' command. The output shows that Snort successfully validated the configuration and then exited. Following this, a series of alerts are displayed, indicating multiple 'TCP port scan detected' events from the IP address 192.168.80.128 to 192.168.80.133. The alerts are timestamped with the date and time 12/25-09:02:28.

```

waltro@ubuntu: /etc/snort/rules
Snort successfully validated the configuration!
Snort exiting
waltro@ubuntu:/etc/snort/rules$ sudo snort -A console -q -i ens33 -c /etc/snort/snort.conf

12/25-09:02:28.110548  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:445
12/25-09:02:28.113447  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:21
12/25-09:02:28.114929  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:2718
12/25-09:02:28.117574  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:1044
12/25-09:02:28.120018  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:2045
12/25-09:02:28.121238  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:10000
12/25-09:02:28.122518  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:3827
12/25-09:02:28.125205  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:2869
12/25-09:02:28.125844  [**] [1:1:1] TCP port scan detected [**] [Priority: 0] {TCP} 1
192.168.80.128:41361 -> 192.168.80.133:2241

```




Control Panel



This PC



Recycle Bin

ubuntu - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
 - nixKali
 - Debian 13.x 64-b
 - pfsense(firewall)
 - ubuntu

Activities

Terminal

Dec 25 09:08

```
waltro@ubuntu: /var/log/snort
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57396 -> 239.255.255.250:1900
12/24-19:05:43.204562 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57400 -> 239.255.255.250:1900
12/24-19:05:44.139287 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57396 -> 239.255.255.250:1900
12/24-19:05:44.216369 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57400 -> 239.255.255.250:1900
12/24-19:05:45.141166 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57396 -> 239.255.255.250:1900
12/24-19:05:45.218970 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57400 -> 239.255.255.250:1900
12/24-19:05:46.151518 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57396 -> 239.255.255.250:1900
12/24-19:05:46.228120 1:1917:6 SCAN UPnP service discover attempt 1:1917:6
Classification: Detection of a Network Scan [Priority: 3] {UDP} 192.168.80.1:57400 -> 239.255.255.250:1900
waltro@ubuntu: /var/log/snort$
```

Home

To direct input to this VM, click inside or press Ctrl+G.



Search



ENG
IN



9:08 AM
12/25/2025

