Secure Network Architecture Design

Raymond A. Vejar
Grand Canyon University

CYB -525: Technology Implementation of Security Solutions

Professor Jean-Pierre Nziaga

January 10, 2024

Part 1:

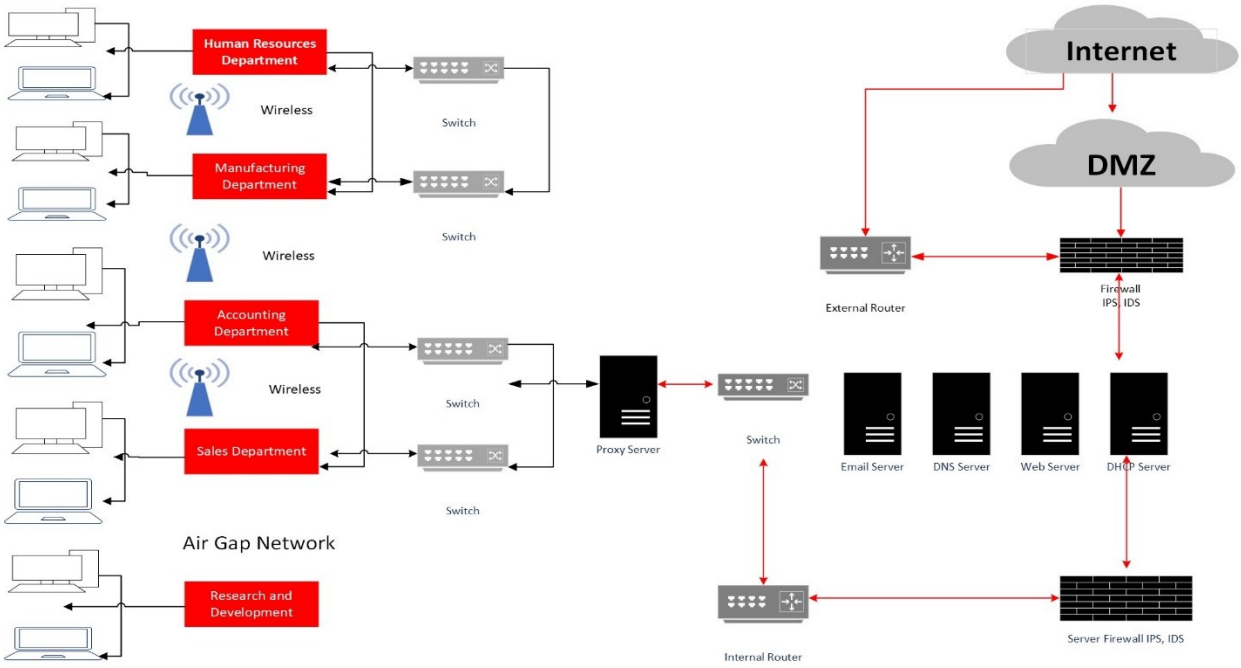
Design a secure architecture for a fictional company:

Design a corporate infrastructure diagram in Visio or another network mapping tool (this deliverable must be readable by your professor; Cisco Packet Tracer is not acceptable). Your network diagram must include a minimum of 2 routers, 2 firewalls, 4 switches, 1 IDS, 1 IPS, a proxy server, an email server, a DHCP server, a DMZ, and finally, 5 separate departments utilizing network segmentation with a minimum of 25 clients per department. You must also include an air gapped system for your R&D department to utilize:

Notes:

“All manner of fictional businesses exist in books, film, television, games, comics and other forms of media. Fictional companies are sometimes parodies of real-life businesses and often times they may be wholly original with their own interesting histories and unique logos!”(Fictional Companies, 2023).

Fictional Company Diagram Design:

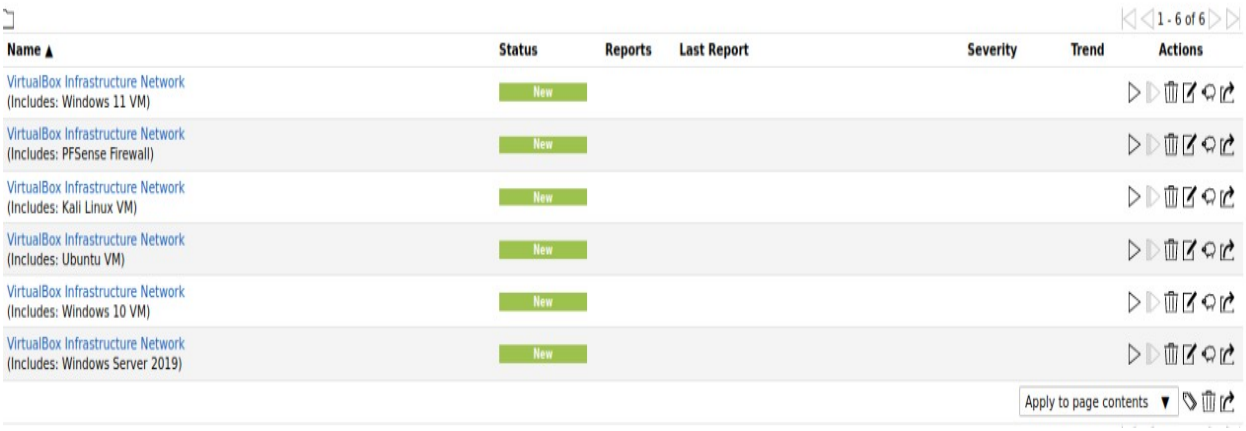


Using your Kali Linux VM, perform a GVM Full and Fast vulnerability scan of your entire VirtualBox infrastructure:

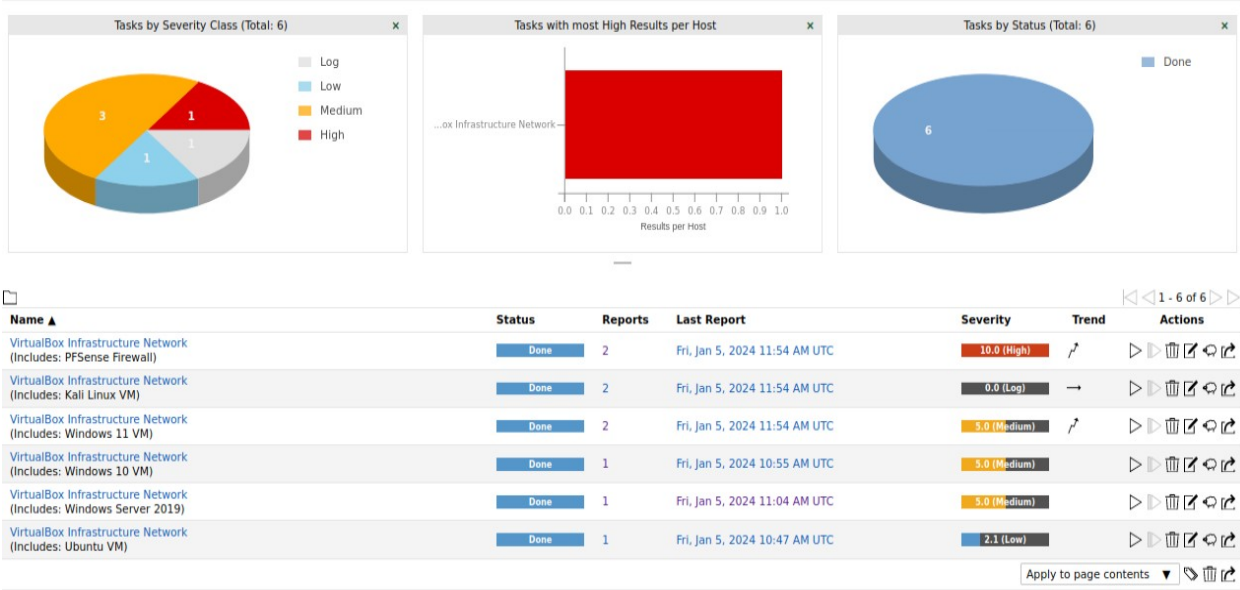
OpenVAS

Open Vulnerability Assessment Scanner

“OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test. The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates.”(OpenVas, 2023).

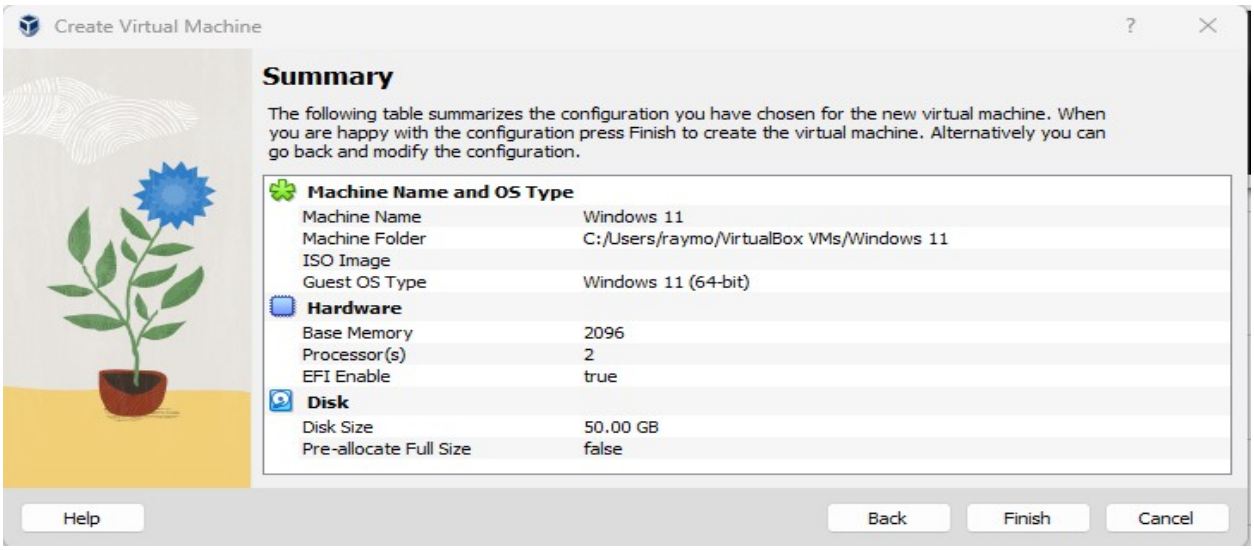


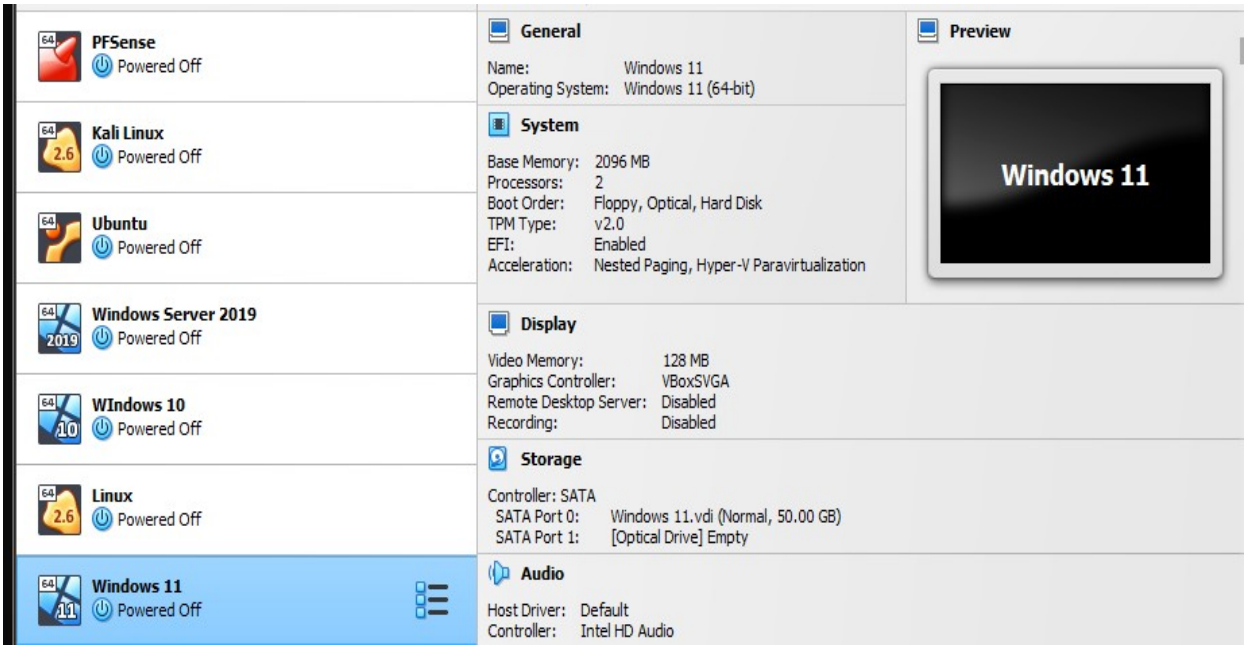
The VirtualBox infrastructure included: Windows 11 VM, Windows 10 VM, Windows Server 2019, Kali Linux VM, Ubuntu VM, and our PFsense Firewall. Scans were created and configured from our OpenVAS vulnerability scanner distrusted by GreenBoone Networks in our Kali Linux VM.

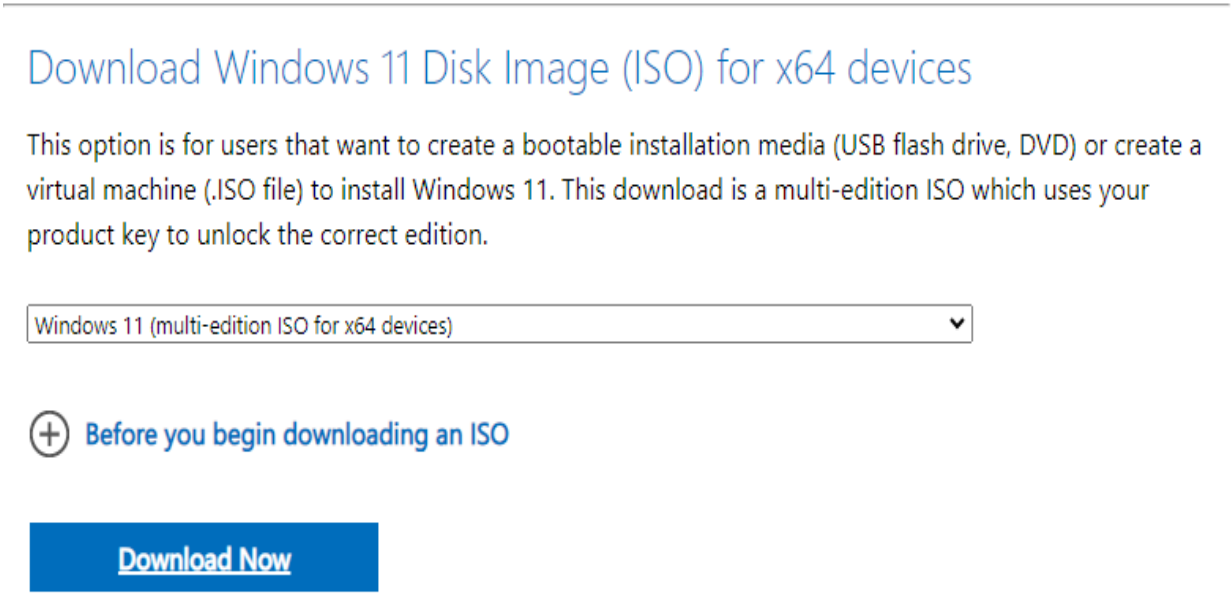


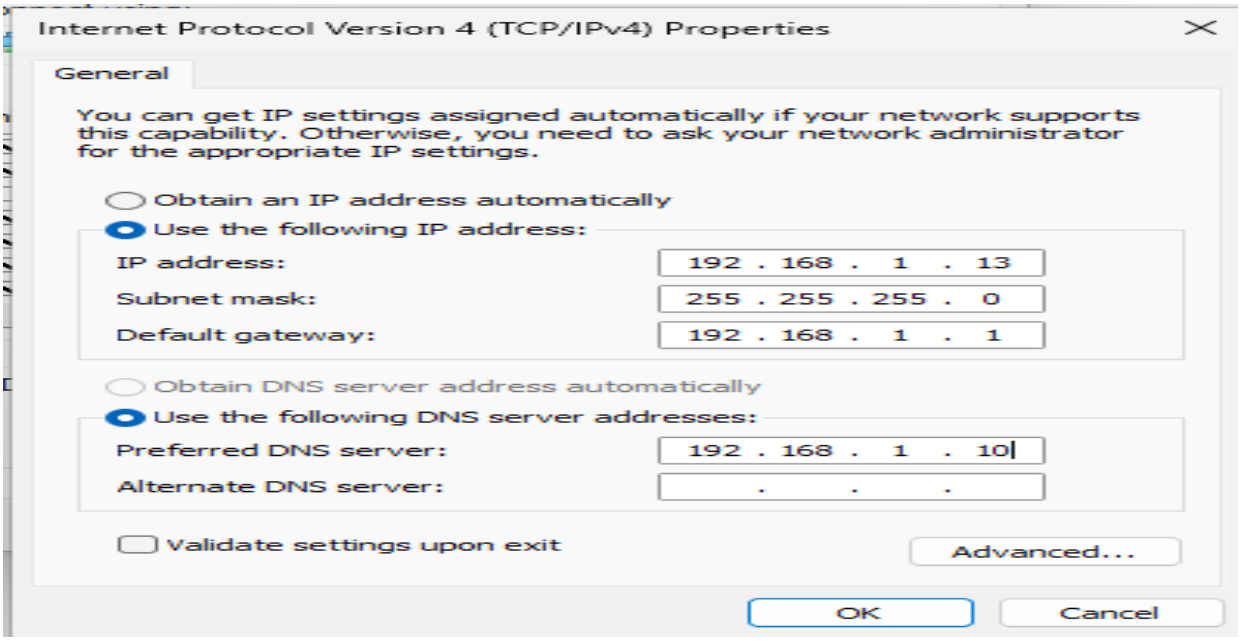
Perform the following tasks to complete the VirtualBox infrastructure:

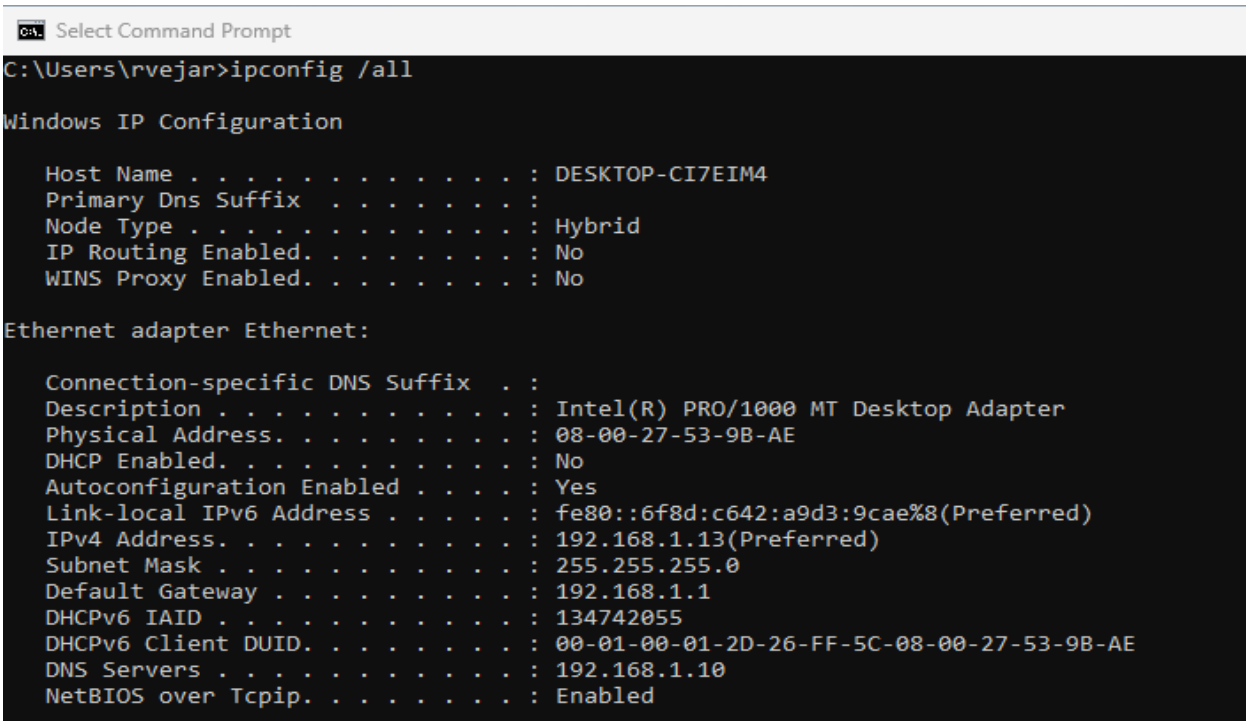
Create a Windows 11 VM and join it to the domain._In a Microsoft Word document, supply screenshots demonstrating the successful creation of both VMs:

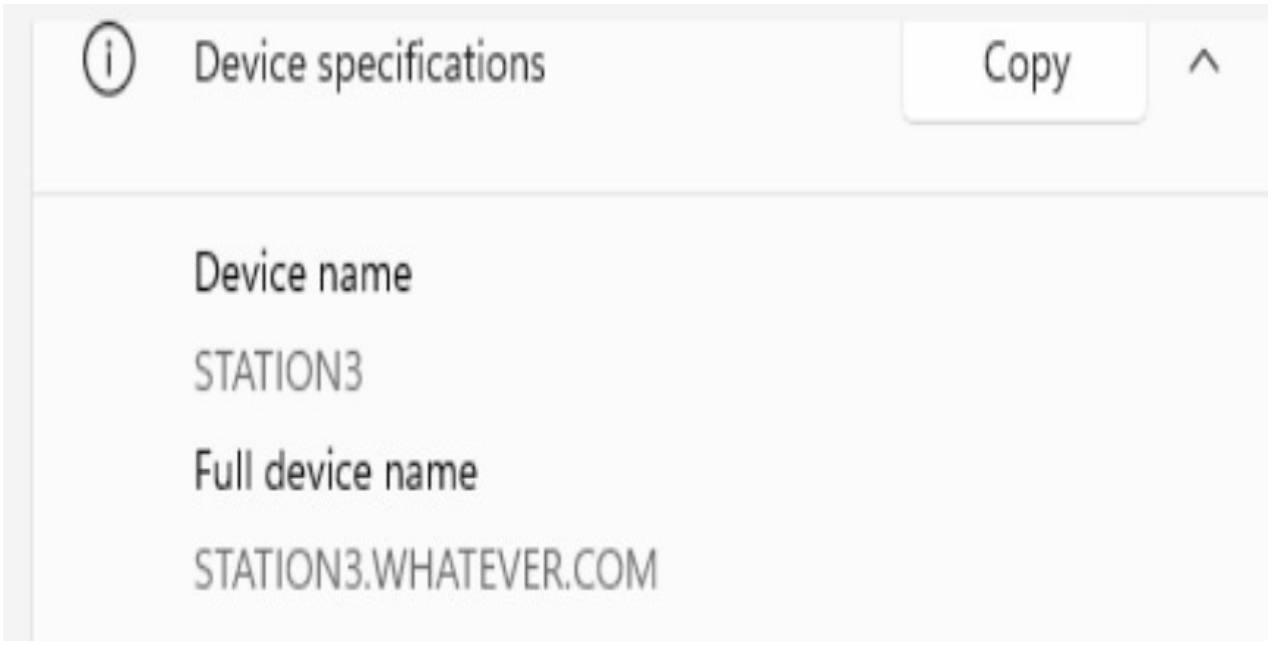


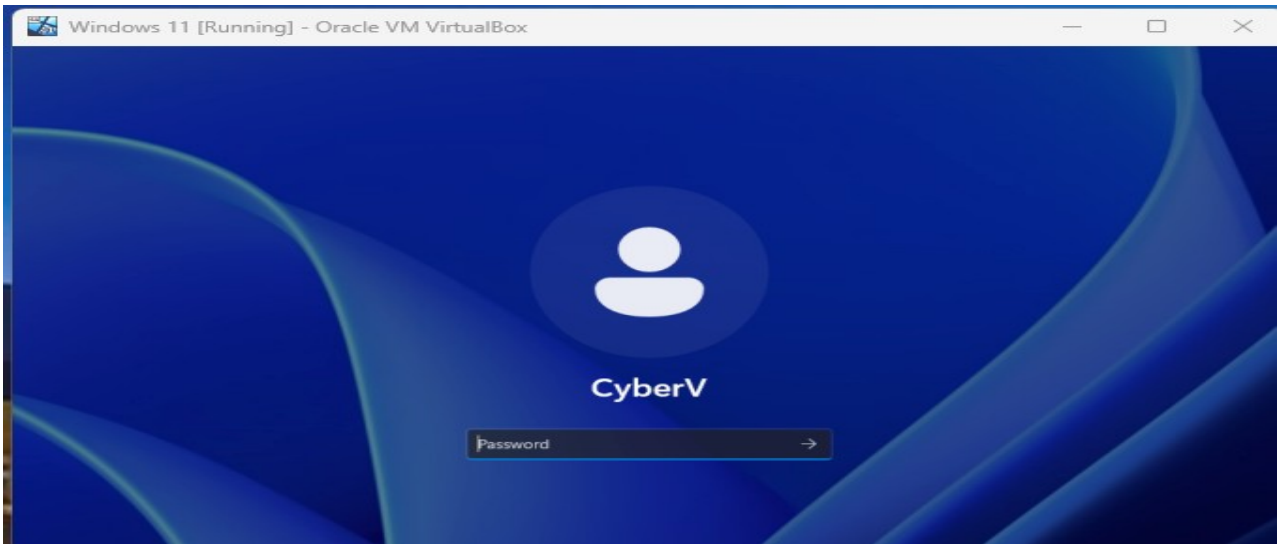

PFSense
Powered Off
Kali Linux
Powered Off
Ubuntu
Powered Off
Windows Server 2019
Powered Off
WIndows 10
Powered Off
Linux
Powered Off
Windows 11
Powered Off
General
Name: Windows 11
Operating System: Windows 11 (64-bit)
System
Base Memory: 2096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
TPM Type: v2.0
EFI: Enabled
Acceleration: Nested Paging, Hyper-V Paravirtualization
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: Windows 11.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Empty
Audio
Host Driver: Default
Controller: Intel HD Audio
Preview
Windows 11


Download Windows 11 Disk Image (ISO) for x64 devices
This option is for users that want to create a bootable installation media (USB flash drive, DVD) or create a virtual machine (.ISO file) to install Windows 11. This download is a multi-edition ISO which uses your product key to unlock the correct edition.
Windows 11 (multi-edition ISO for x64 devices)
Before you begin downloading an ISO
Download Now

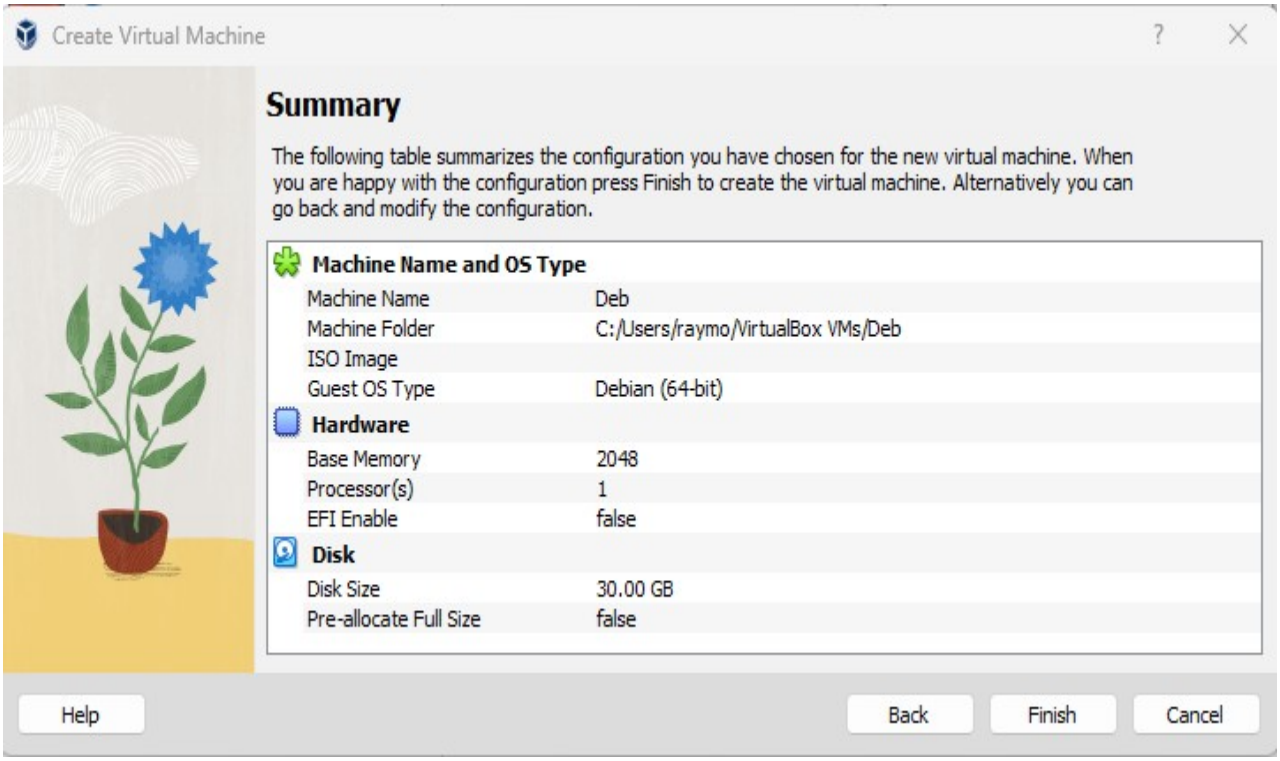

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 13
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 10
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

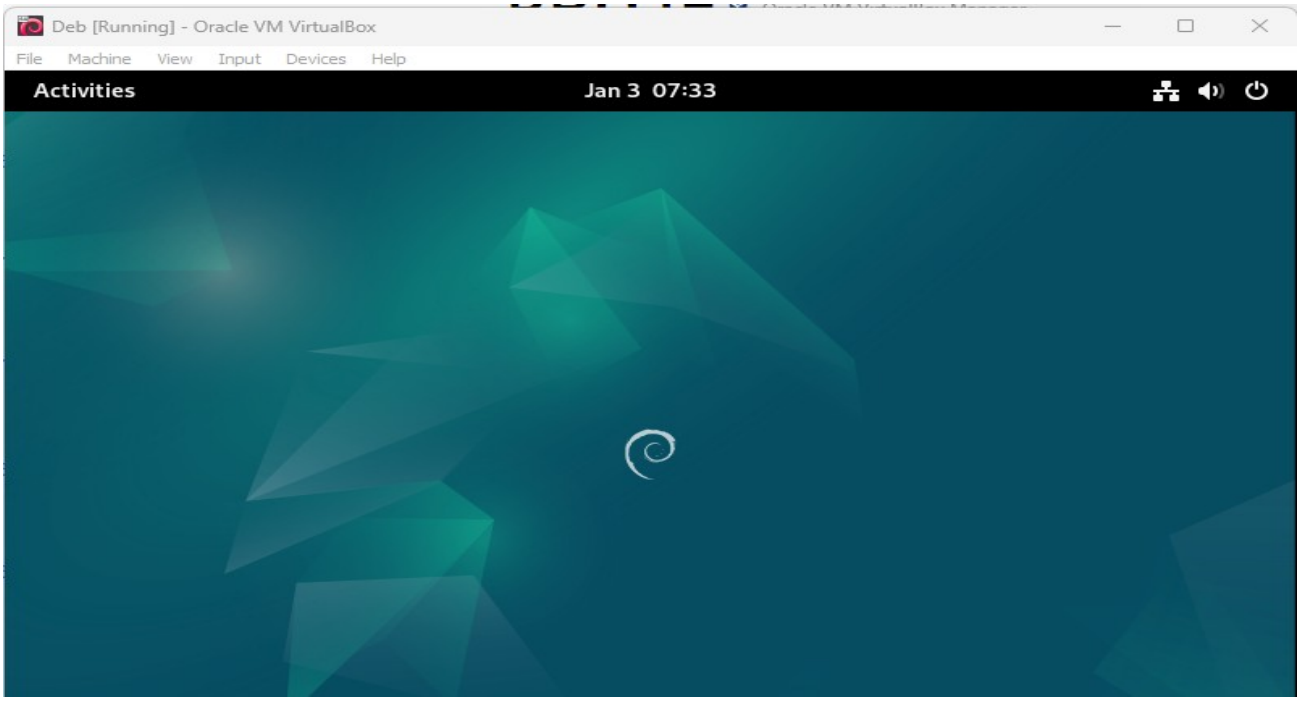

Select Command Prompt
C:\Users\rvejar>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-CI7EIM4
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-53-9B-AE
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6f8d:c642:a9d3:9cae%8(Preferred)
IPv4 Address. . . . . : 192.168.1.13(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 134742055
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-26-FF-5C-08-00-27-53-9B-AE
DNS Servers . . . . . : 192.168.1.10
NetBIOS over Tcpip. . . . . : Enabled

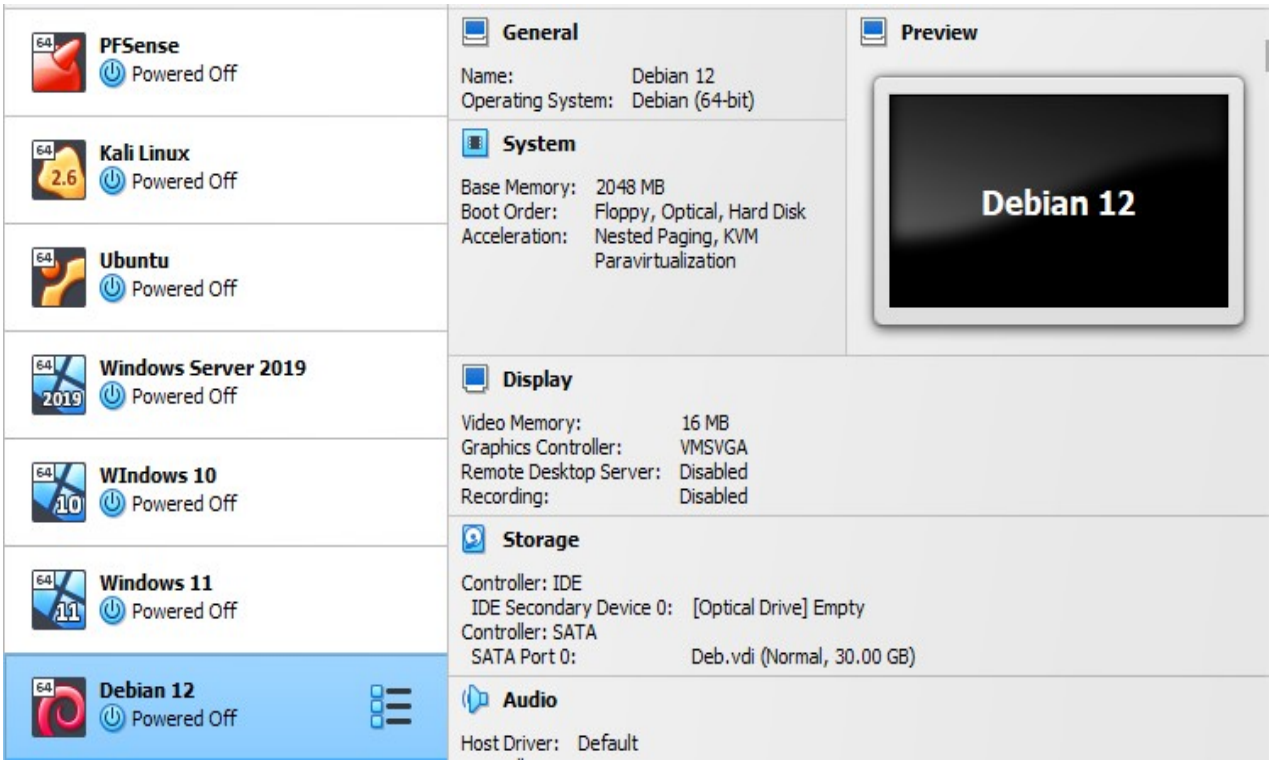

Device specifications
Copy
Device name
STATION3
Full device name
STATION3.WHATEVER.COM


Windows 11 [Running] - Oracle VM VirtualBox
CyberV
Password

Create a VM using an operating system of your choice that has not been created yet. It could be a different version of Windows or Linux. It is not necessary to join this VM to the domain:




Deb [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Jan 3 07:33


PFSense
Powered Off
Kali Linux
Powered Off
Ubuntu
Powered Off
Windows Server 2019
Powered Off
WIndows 10
Powered Off
Windows 11
Powered Off
Debian 12
Powered Off
General
Name: Debian 12
Operating System: Debian (64-bit)
System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM
Paravirtualization
Preview
Debian 12
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Deb.vdi (Normal, 30.00 GB)
Audio
Host Driver: Default

Select 2-3 intellectual tools (e.g., Suricata, pfSense, Snort, etc.) and demonstrate how they work together to create a framework. Make sure to include them in your secure network design. Do not use Suricata, pfSense, or Snort for this part of the assignment:

The three intellectual tools that were selected Included Cisco Secure Firewall, Cisco Secure IPS, and OSSEC IDS:

- “Cisco Secure Firewall provides unified management of firewalls, application control, intrusion prevention, URL filtering, and malware defense policies. Secure Firewall provides faster threat protection with industry leading Snort 3 Intrusion Detection and Prevention System (IDS/IPS)”(Cisco, 2023).
- “Cisco NGIPS markets their Secure IPS product as a next generation intrusion prevention system (NGIPS) with over 35,000 built-in IPS rules and broad capabilities for detecting and blocking anomalous traffic. Secure IPS can be integrated with other Cisco devices or deployed as a stand-alone IPS.”(Samson, 2023).
- “OSSEC is a host-based IDS that is produced by a long-running open-source project. It’s been widely downloaded and used — the project receives more than 500,000 downloads a year — and works on Windows, macOS, and a host of Unix-like systems, including Linux. OSSEC monitors the logs various system components generate in real time, and can detect changes to individual files, including all-important Windows registry files. While primarily an IDS, OSSEC can also respond to attacks, using both its own capacities and integration with third-party tools”(Fruhlinger, 2020).

Cybersecurity tools, are selected and implemented as protective measures and controls, which aid individuals and companies in maintaining online privacy and security to their computer systems and networks. The goal, is to select and implement several safeguards to provide a Defense in Depth security strategy. The main idea of this strategy is designed, so that if one line of defense has been compromised. Additional layers or tools that are installed will ensure that the threat is contained.

For example, the Cisco Secure Firewall would be implemented to monitor incoming and outgoing network traffic from the public internet to our Fictional Company's private network, and would be based on a defined set of security rules, and these rules will decide whether to allow or block specific traffic.

In addition, to the Cisco Secure Firewall, Cisco NGIP Intrusion Protective System and OSSEC Intrusion Detection System will continuously monitor our network for malicious activity and take action to prevent it. These tools work together to provide layers of security on our network, as part of an individual or organizations security framework.

Part 2:

Create a 5– to 7-minute screencast addressing the following:

Explain all components and how they interact with each other within the secure network design created.

Discuss the results of the GVM scan.

Describe and discuss the security issues and implications of advanced and novel networks and protocols. Ensure your discussion applies to both current and new network technologies:

https://youtu.be/M-u0vCBGysA

References:

Cisco. (2023). Cisco Secure Firewall At a Glance. Retrieved from, https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/at-a-glance-c45-736624.html

Fruhlinger, Josh. 12 top IDS/IPS Tools. Retrieved from, https://www.csoonline.com/article/569085/12-top-idsips-tools.html#:~:text=OSSEC%20monitors%20the%20logs%20various,integration%20with%20third%2Dparty%20tools.

Samson, R.(2023). Top 10 Intrusion Detection and Prevention System. Retrieved from, https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/