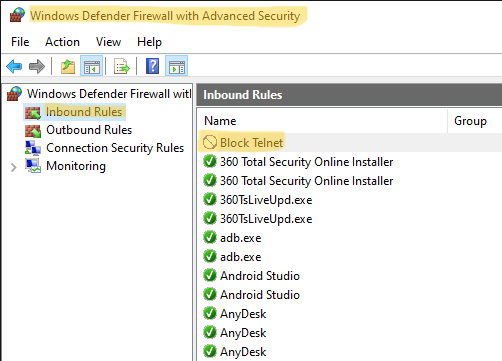
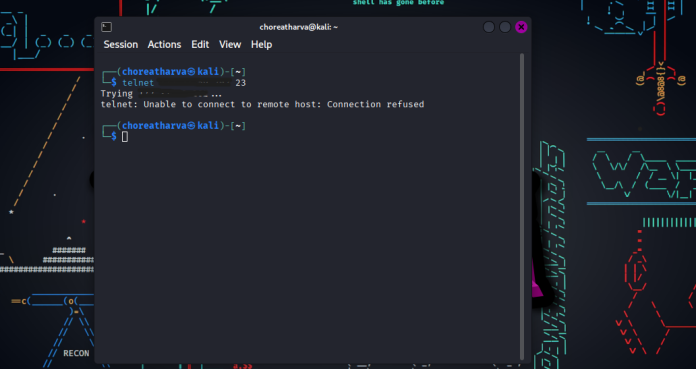
***ELEVATE LABS CYBER SECURITY INTERNSHIP***

***TASK 4: Setup and use a Firewall on Window/Linux***

******

***Here we started with Windows Defender Firewall with Advacned Security. After that , in Inbound rule on left side panel, here are rules set for the firewall to work. Here we set a new rule for this task i.e to block telnet on port 23, so we set new rule named “Block telnet”.***

******

***After setting the rule we need a different machine on the same network as our host PC, so I have used Kali Linux Virtual Machine as another machine on same network, we start with pinging the machine and after successful one, we use command “telnet [ip address] 23, here we have used telnet and 23 is the port that we have block on. As in the image after command is executed the result shows connection is refused.***

***That shows that the new rule that we have set worked successfully.***

***Interview Questions***

**1. What is a firewall?**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on a set of predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network, like the internet.

**2. What is the difference between a stateful and a stateless firewall?**

* Stateless Firewall: A stateless firewall inspects each data packet individually, without any knowledge of its context or connection to other packets. It makes decisions solely based on rules like source/destination IP addresses and port numbers. It's fast but can be less secure because it doesn't recognize legitimate connections.
* Stateful Firewall: A stateful firewall keeps track of the state of active network connections in a state table. Once a connection is established, it recognizes all subsequent packets belonging to that connection as legitimate traffic, making it more efficient and secure.

**3. What are inbound and outbound rules?**

* **Inbound Rules**: These rules control traffic that is **entering** your network. They determine what external services or devices are allowed to access resources on your internal network.
* **Outbound Rules**: These rules control traffic that is **leaving** your network. They define what internal devices or applications are allowed to connect to the outside world.

**4. How does UFW simplify firewall management?**

UFW, or Uncomplicated Firewall, simplifies firewall management on Linux by providing a user-friendly command-line interface. It acts as a front-end for the more complex iptables utility, allowing users to easily add, delete, and manage firewall rules with simple commands.

**5. Why block port 23 (Telnet)?**

Port 23 is used by the Telnet protocol, which transmits data, including usernames and passwords, in plain text. This makes it highly vulnerable to eavesdropping and man-in-the-middle attacks. Blocking this port forces users to rely on more secure, encrypted protocols like SSH (Secure Shell).

**6. What are common firewall mistakes?**

* **Misconfiguration**: Leaving unnecessary ports open or mistakenly blocking essential services.
* **Default Rules**: Using overly permissive default rules that allow too much traffic.
* **Neglecting Updates**: Failing to update the firewall's software and rules to defend against new threats.
* **Lack of Monitoring**: Not regularly checking firewall logs for suspicious activity.

**7. How does a firewall improve network security?**

A firewall improves security by creating a protective boundary around a network. It enforces a security policy, filters out malicious traffic, and prevents unauthorized access. By logging activity, it also provides a record for security analysis and incident response.

**8. What is NAT in firewalls?**

**NAT (Network Address Translation)** is a service that translates private IP addresses of devices on an internal network into a single public IP address when they communicate with the internet. This technique helps conserve public IP addresses and adds a layer of security by hiding the internal network's structure from the outside world.