Bryant Watkins

2/6/26

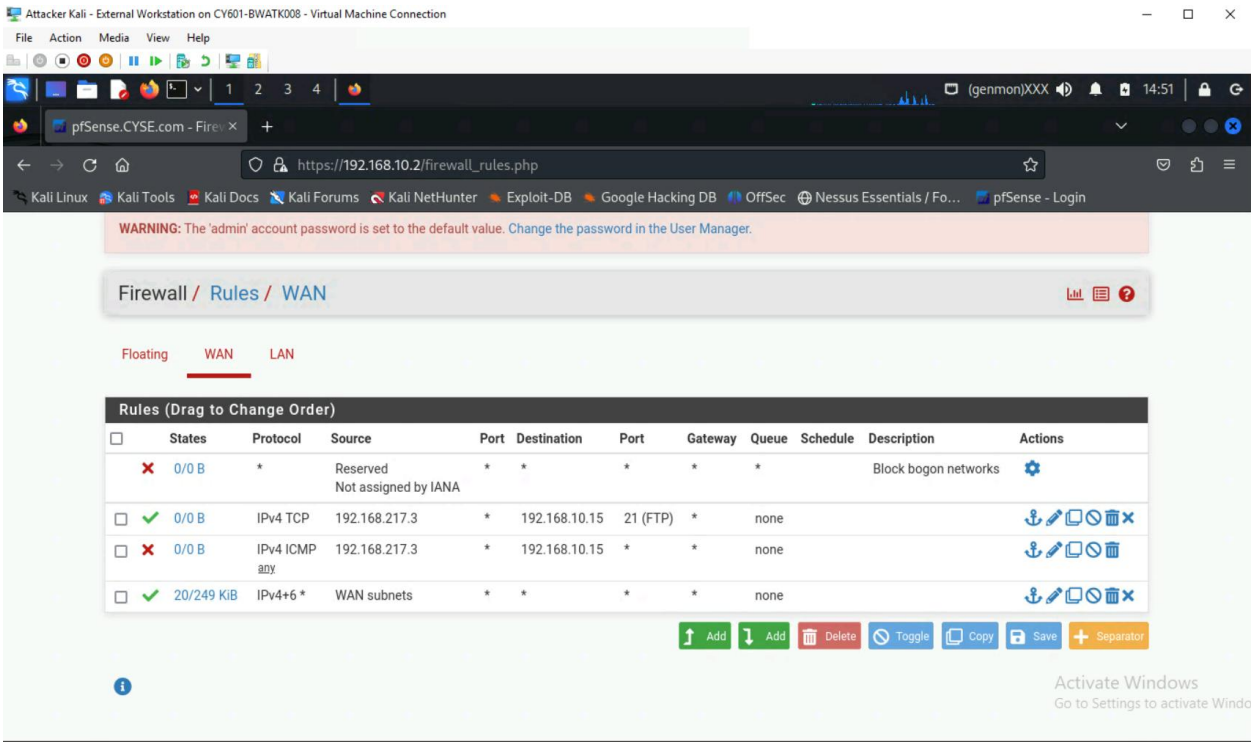
PFSENSE LAB REPORT

CYSE 601

Relevant Systems

- pfSense firewall VM (IP: 192.168.10.2).
- External Kali Linux machine (IP: 192.168.217.3).
- Internal Windows Server 2008 machine (IP: 192.168.10.15).

Firewall Configurations

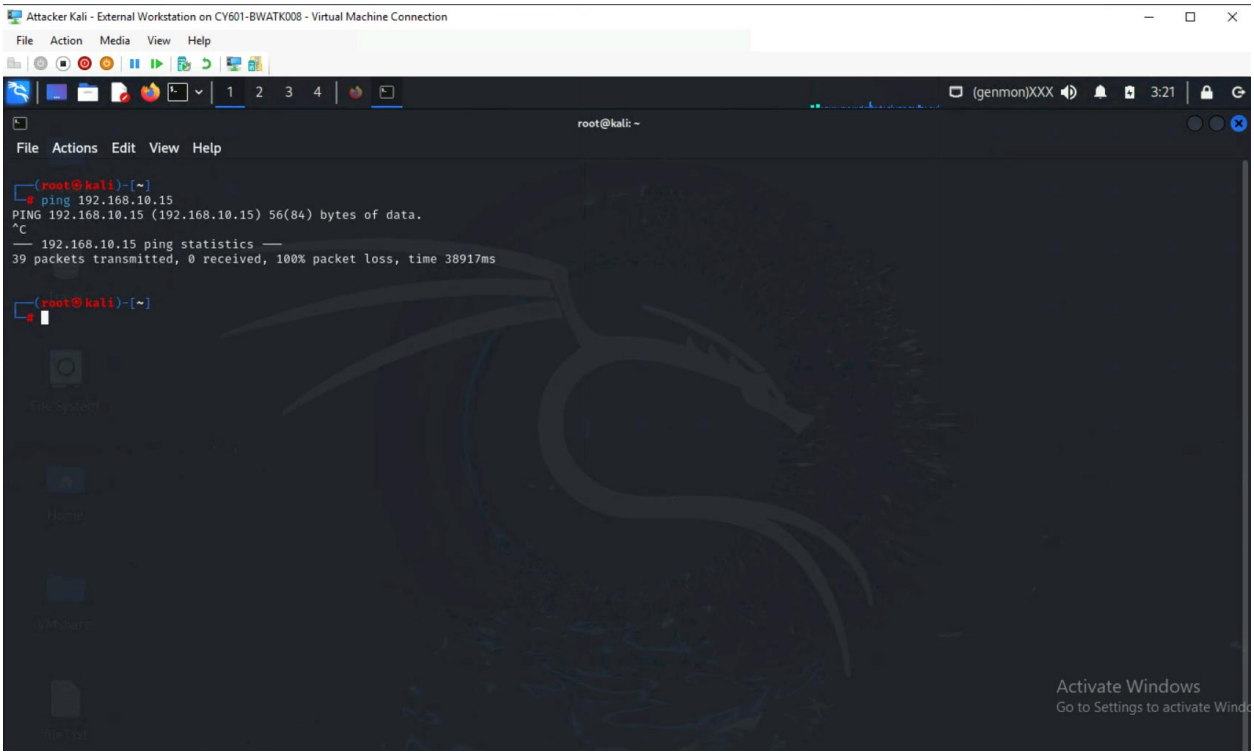


The above image displays four different rules established through the pfSense platform. Two of the four rules were implemented by me, both a Block and a Pass rule. The Pass rule functions by allowing FTP traffic to travel from the source address (Ext Kali Linux/192.168.217.3) to the destination address (Windows Server 2008/192.168.10.15). Being that the addresses involved are IPv4 and transmitted by way of TCP – the IPv4 TCP protocol was chosen of the available options. Port 21 was specifically chosen because it belongs to FTP. The Block rule implements a cessation of all ICMP traffic (including any subtype) traveling from the source address (Ext Kali Linux/192.168.217.3) to the destination address (Windows Server 2008/192.168.10.15). Wan was the chosen interface due to its posture of denying by default. The asterisks amongst all rules represent “any”. It is also imperative that the Pass rule precedes the

Block rule in sequential order, as the system executes the listed rules in order and placing the Pass rule below the Block rule would essentially render it meaningless/ineffective.

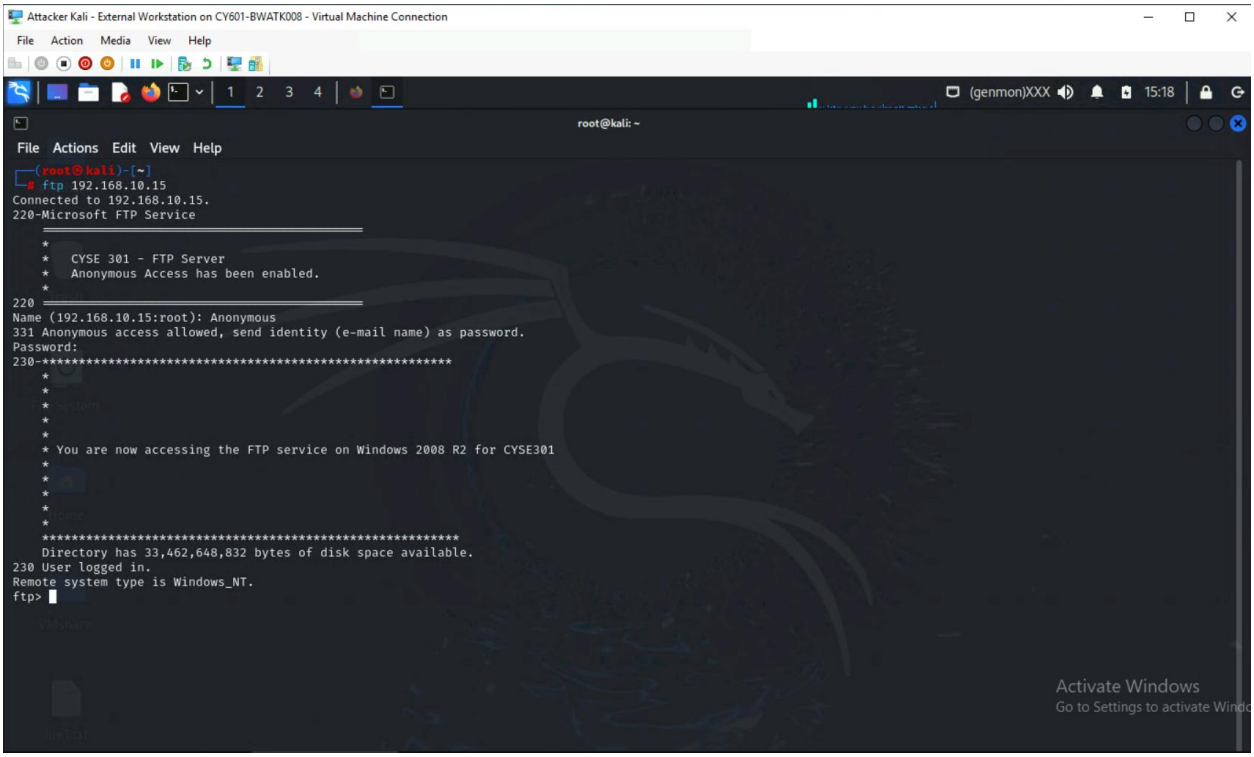
Testing and Validation

ICMP Block Test



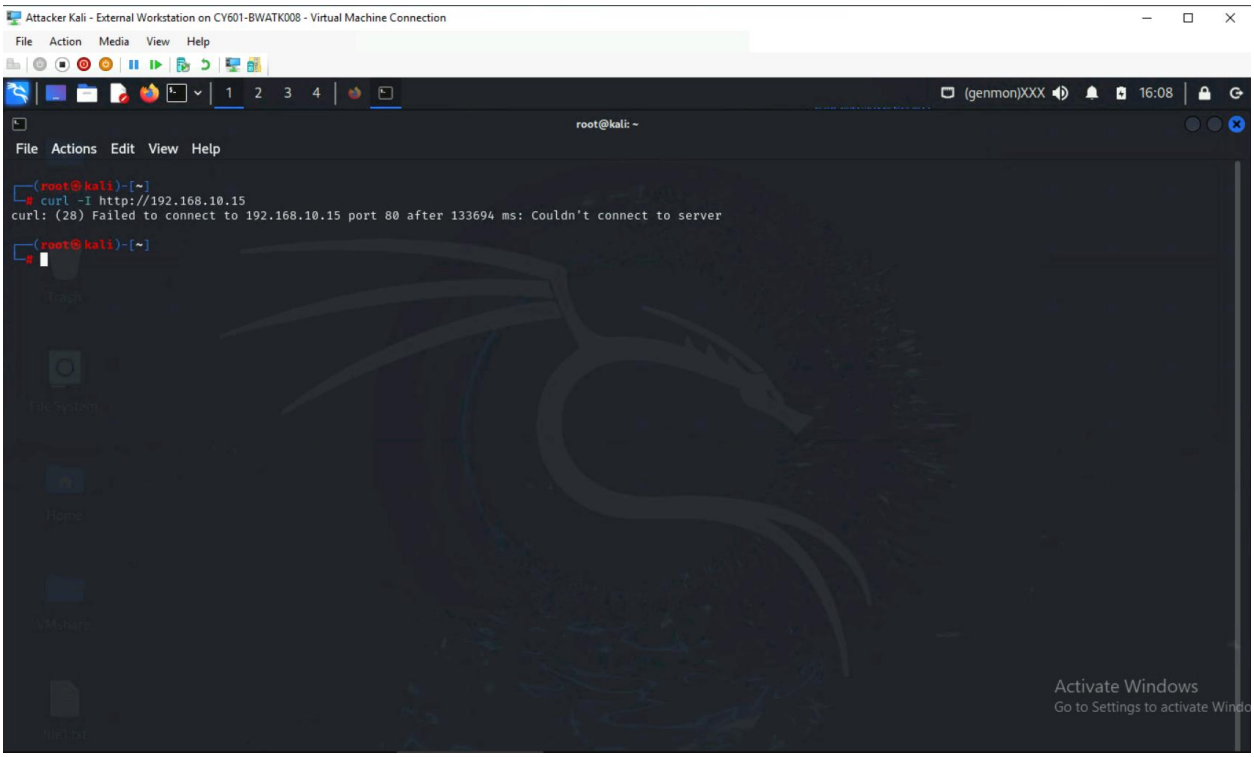
The above image displays the successful effect of the Block ICMP firewall rule. The source address (192.168.217.3) attempted to establish an ICMP, by way of the *ping* command, with the destination address (192.168.10.15). The attempted communication was successfully blocked by the firewall rule implemented, as indicated by the “100% packet loss” message.

FTP Allowance



FTP is a protocol primarily used for transferring files between a client and a server. In the above image, an FTP connection can be seen successfully establishing an FTP connection, from the source address (192.168.217.3) to the destination address (192.168.10.15). This communication was enabled due to the Pass rule implemented, allowing traffic to flow through FTP port 21. The successful connection also includes a login. The username of *Anonymous* and password of *xxx* were successfully accepted, which allowed for the source address to login to the destination address – as seen with the "230 User logged in" message.

Other Traffic



The above image displays an unsuccessful attempt to establish an HTTP protocol connection between the source address (192.168.217.3) and the destination address (192.168.10.15). Due to the firewall configurations lack of explicit permission for other protocols, such as HTTP in this case, no connection has been allowed. The unsuccessful attempt is described with the output statement “Failed to connect to 192.168.10.15 port 80... Couldn’t connect to server”.