BUILD WEEK - NETWORK FOR THETA

The Build Week project involved implementing a network for the Theta company. The goal was to connect 120 devices, a NAS server, a web server, a perimeter firewall, and 3 IDS/IPS, organized into subnets. The devices were distributed across 6 floors, with 20 on each floor.

After the requirements were outlined, we focused on preparing a budget that included labor costs for configuration. The total estimated cost amounts to €174,490.58, well within the initial budget of €285,000. Below is a list of links to the selected components:

Budget for Theta Company

SWITCH:

- S3700-24T4F 24 PORT
- UNIT COST: €254.98
- TOTAL FOR 8 DEVICES: €2,039.84

OPTICAL FIBER CABLE

- TOTAL COST: €2,225.73

SERVER:

- TOWER POWEREDGE T160
- COST: €4,135.54

PC:

- HP PRO TOWER 400 G9
- UNIT COST: €947.00
- TOTAL FOR 120 DEVICES: €113,640

MONITOR:

- SAMSUNG S31C
- UNIT COST: €89.90
- TOTAL FOR 120 DEVICES: €10,788

FIREWALL:

- NSG-5220
- COST: €5,936.52

IPS/IDS:

- CISCO 4260
- UNIT COST: €1,696.50
- TOTAL FOR 3 DEVICES: €5,089.50

NAS:

- SYNOLOGY DISKSTATION DS1823xs+
- COST: €1,941.52

ROUTER:

- CISCO C891FW-E-K9
- COST: €1,080.50

LABOR AND INTERNET PROVIDER:

- €20,000
- 20 DAYS FOR NETWORK DESIGN AND INSTALLATION (THROUGH AN EXTERNAL COMPANY)
- €7,620 FOR 12 MONTHS OF INTERNET SERVICE, INCLUDING FIXED COSTS

Network Design and Distribution

The network is organized by floor as follows:

- 1st Floor: Reception and Front Desk (VLAN-Floor-1)
- 2nd Floor: Marketing (VLAN-Floor-2)
- 3rd Floor: Management (VLAN-Floor-3, VLAN-NAS, VLAN-WEBSERVER)
- 4th Floor: Sales Department (VLAN-Floor-4)
- 5th Floor: Logistics (VLAN-Floor-5)
- 6th Floor: Finance (VLAN-Floor-6)

Each floor has 20 devices connected to a switch, totaling 120 devices and 6 switches. These switches are linked to a router gateway positioned on the 3rd floor to minimize cable length and signal loss. Additionally, the 3rd floor houses the NAS, the web server, the firewall, and the 3 IDS/IPS units, for easy centralized access.

IDS and IPS are strategically placed: two IDS protect the NAS and Management devices, which contain sensitive data, while still allowing employee access. An IPS defends the web server, ensuring security against external threats. The firewall is hardware-based and configured at the perimeter to handle a high volume of connected devices, minimizing potential disruptions. It employs application filtering with a DMZ inside the firewall.

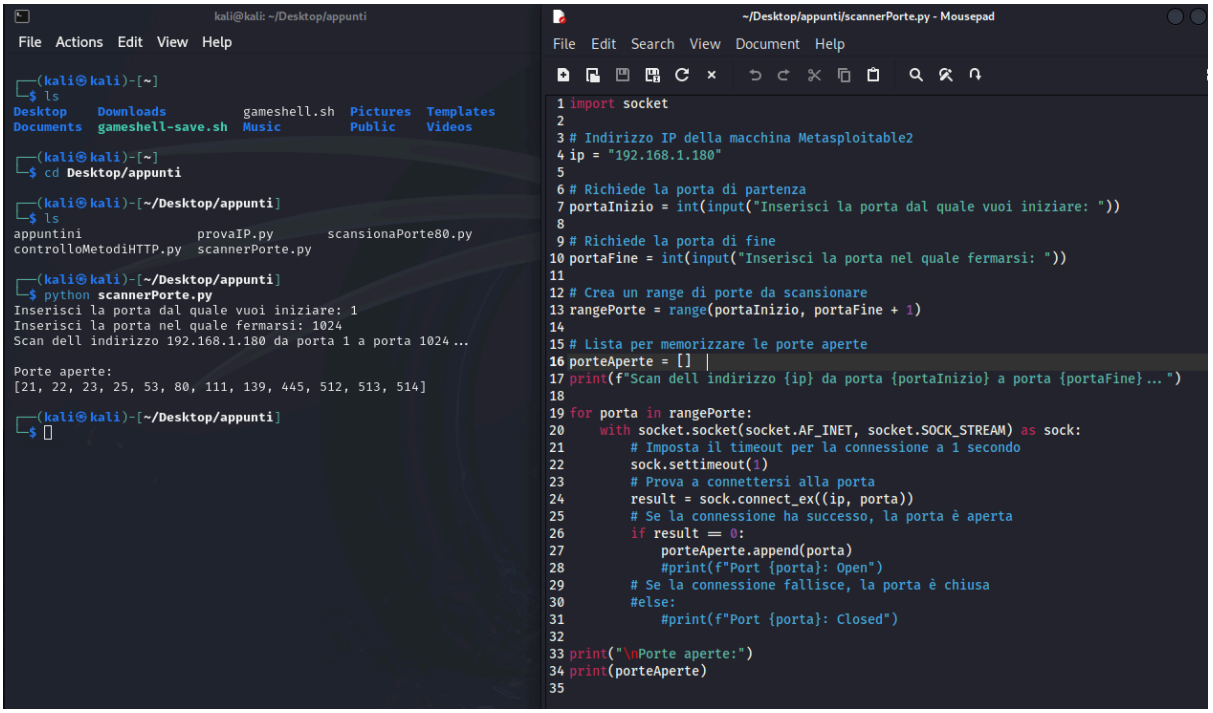
For network segmentation, we chose a /27 subnet mask, providing 32 IP addresses per subnet, with 30 available for hosts, reserving one for the gateway. This decision, based on Cisco's guidelines, supports the 20 devices per floor while allowing for potential future expansions of up to 54 additional devices.

VLANs were configured for each subnet to compartmentalize information and optimize traffic flow across departments. Switches handle data exchange within the same subnet, while the gateway router allows communication between subnets. To simplify network management for the company, which lacks an in-house IT technician, we assigned intuitive names to the VLANs for easy identification.

The NAS and web servers are placed in a separate subnet with a /29 mask, providing 8 IP addresses, of which 5 are available for hosts. This choice isolates the servers from the rest of the network, enhancing security. The lower number of devices means this subnet is appropriately sized without excess.

Network Testing

Beyond the initial ping to the Metasploitable machine to identify its IP address, the first network test verified open ports on this device, represented by the Metasploitable machine. Using a custom network scanner to scan a port range for a given IP address, we compiled a list of currently open ports. This is useful for verifying that necessary services are available and identifying any critical vulnerabilities.



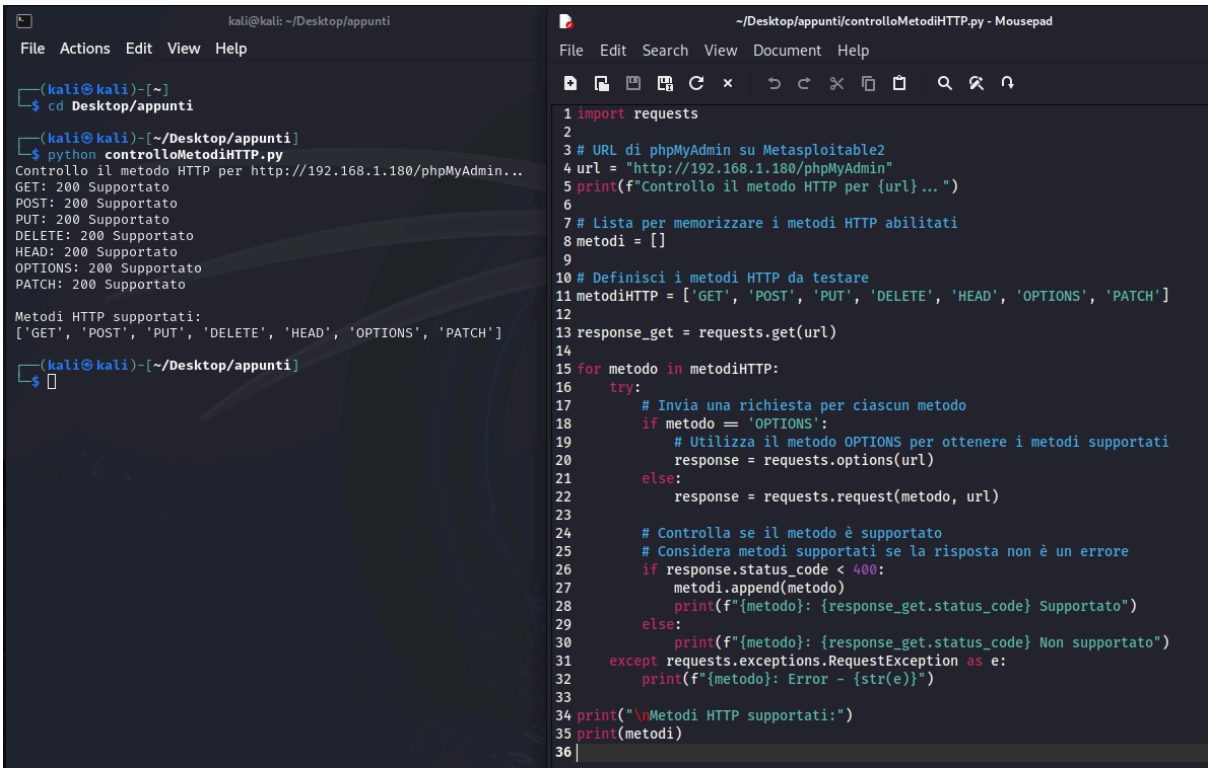
The test found the following ports open: 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, and 514. Below is a list of the most relevant:

- 21 (FTP) - File Transfer Protocol
- 22 (SSH) - Secure Remote Access
- 23 (Telnet) - Unsecured Remote Access (data transmitted in plain text)
- 25 (SMTP) - Email Transmission
- 80 (HTTP) - Unsecured Web Traffic

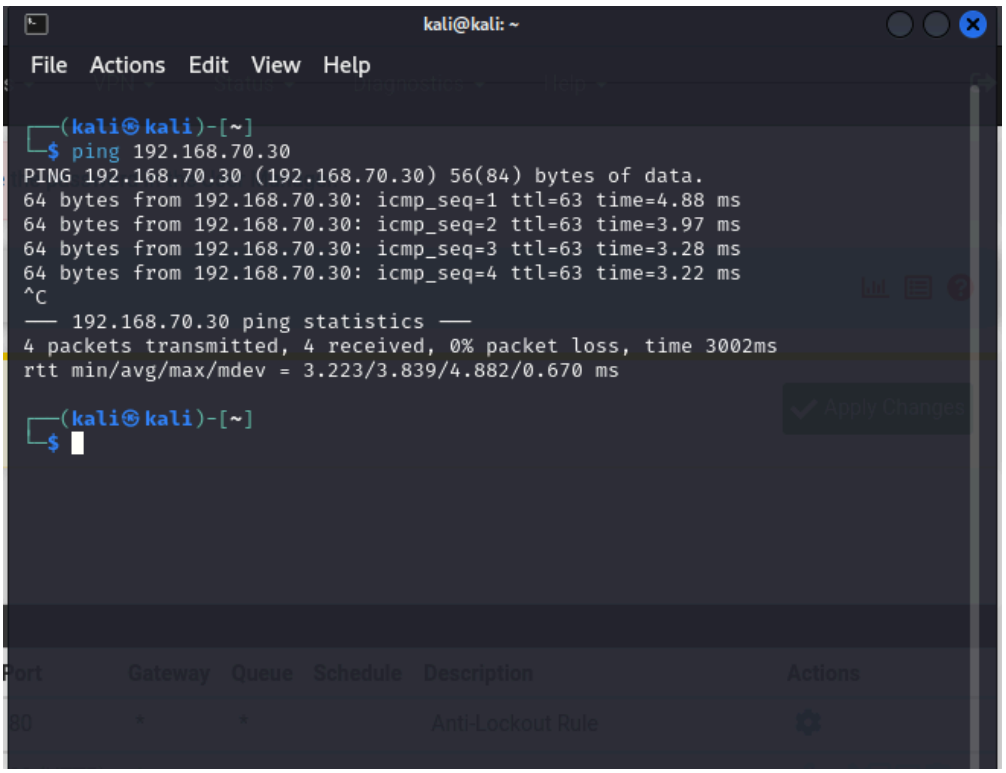
As expected, we identified port 80 (HTTP) as open, representing a vulnerability since it is the "insecure" version of HTTPS.

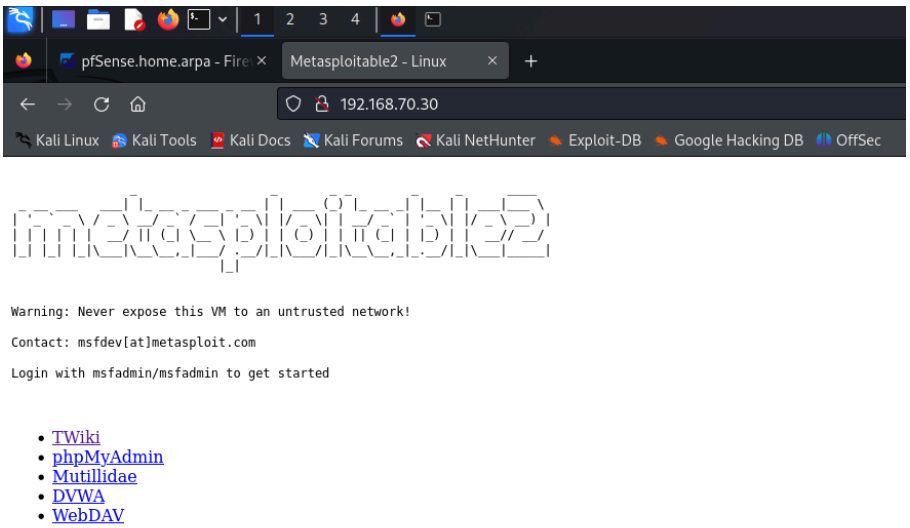
Based on this finding, we proceeded to verify the HTTP methods for the same IP address on the Metasploitable machine. The program first defines the IP address, creates a list to store request results by "method," and sets the HTTP methods to test. The `requests` module, imported at the beginning (chosen for its practicality and speed with HTTP requests), is used

within a for-loop that iterates through both defined lists. Using if/else constructs, we set conditions to send requests for each method and check if the method is supported. The results show that all methods are supported in this case.

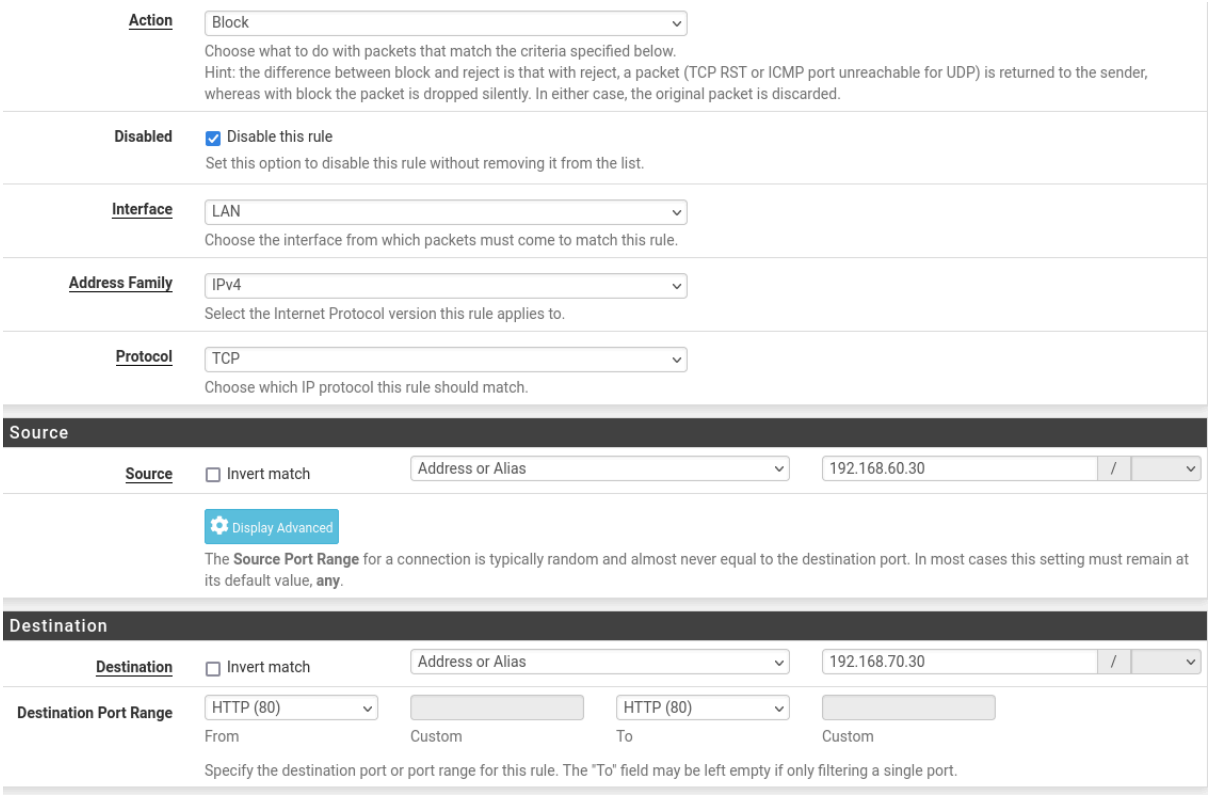


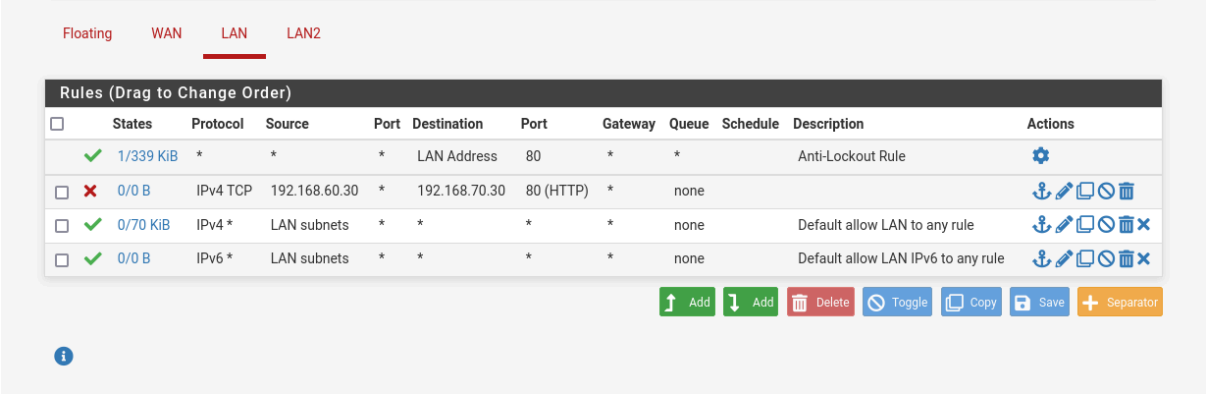
Finally, as required, we simulated device communication (pfsense, Metasploitable, and Kali) in a virtual environment. Packet transmission occurred without loss.



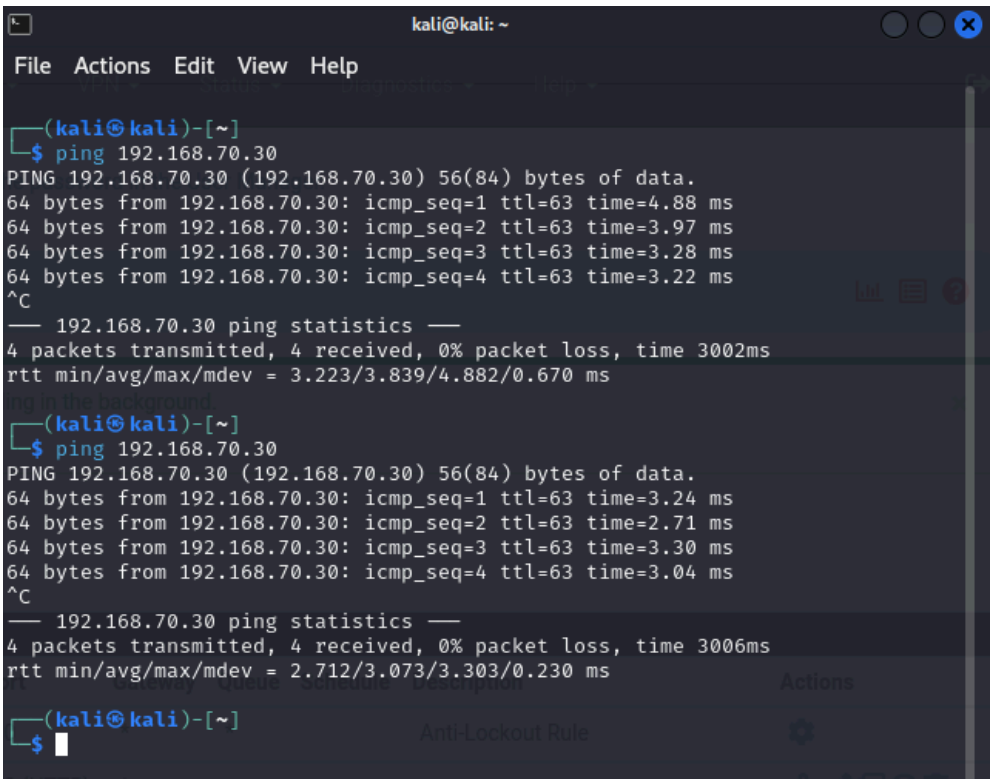


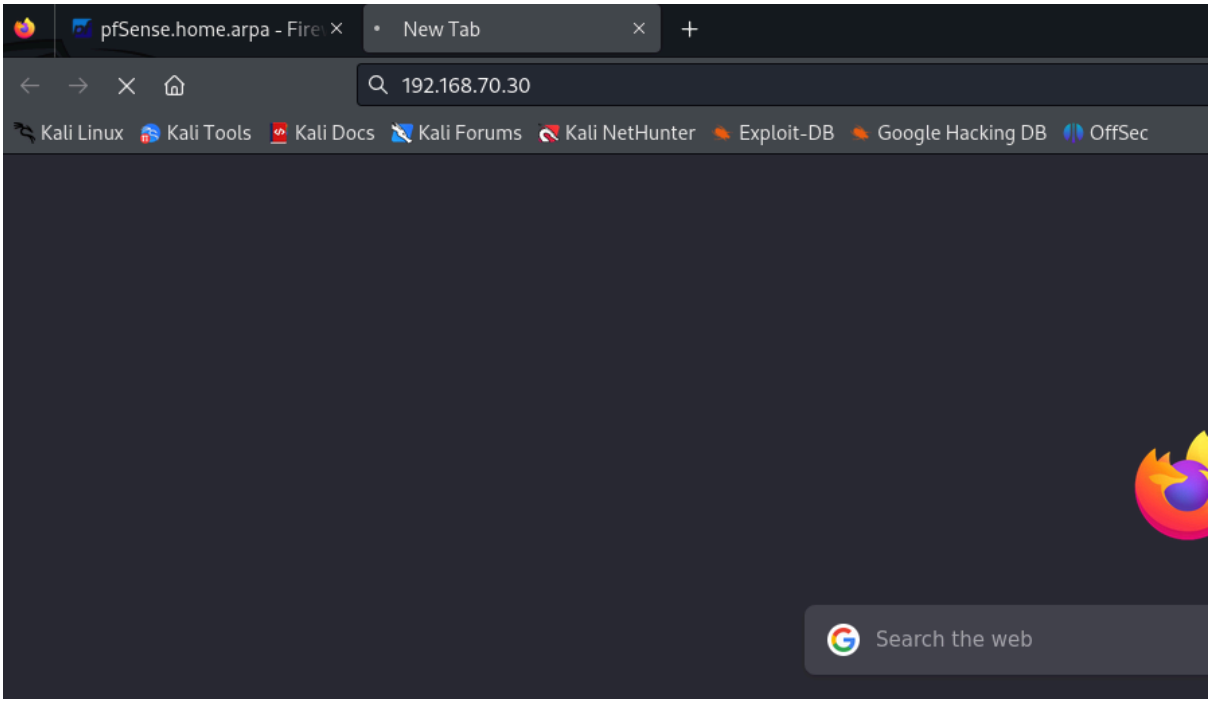
Once the network configuration was confirmed, we applied a blocking rule on port 80 through the pfsense GUI to prevent communication between Kali and the DVWA.





We tested this rule using a final ping:





As expected, communication was blocked, allowing us to confirm that we mitigated the vulnerability on port 80. Additionally, we noted that HTTP methods PUT and DELETE, which are currently active, pose significant vulnerabilities by allowing any user to freely add or delete code. This could lead to serious issues if malicious actions were taken. We recommend that the company mitigate risks by disabling these HTTP methods.