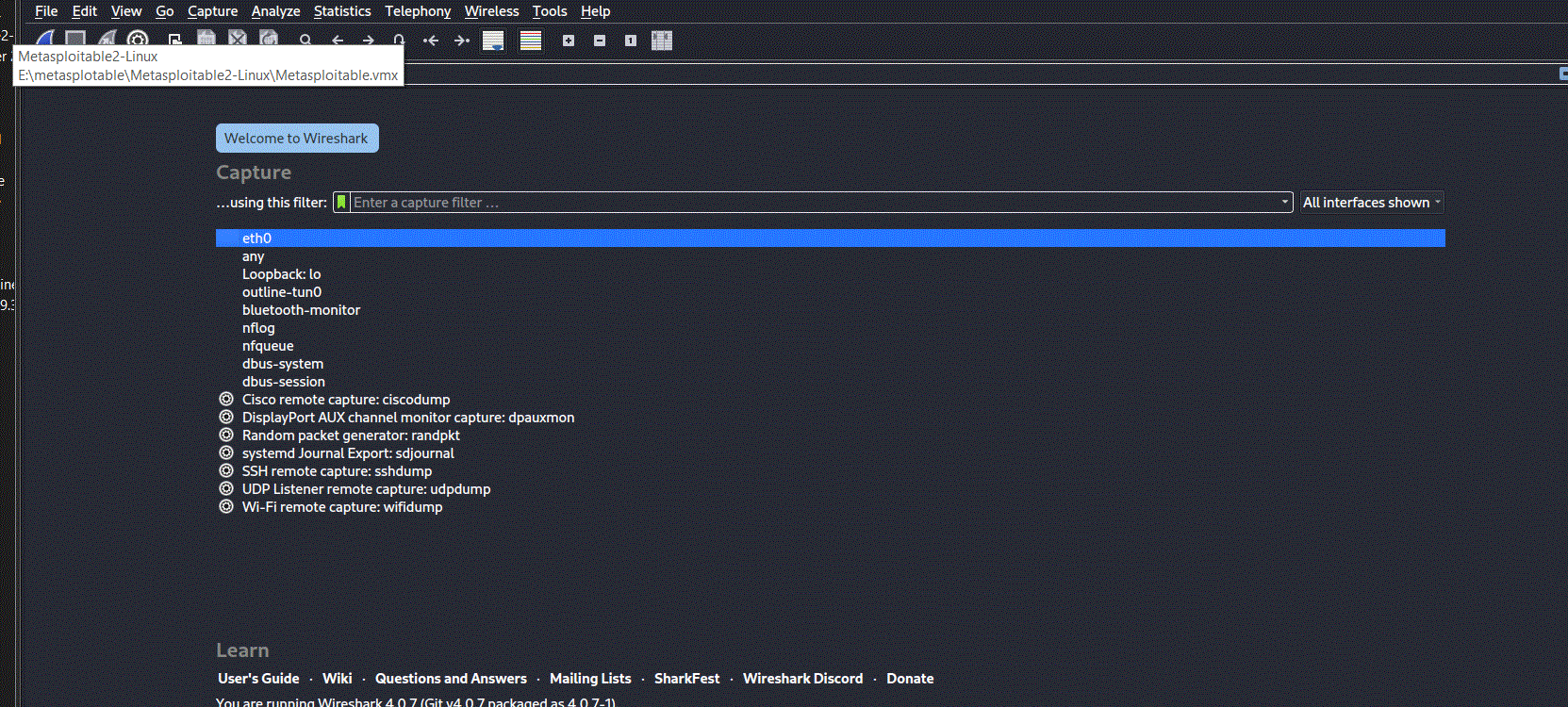
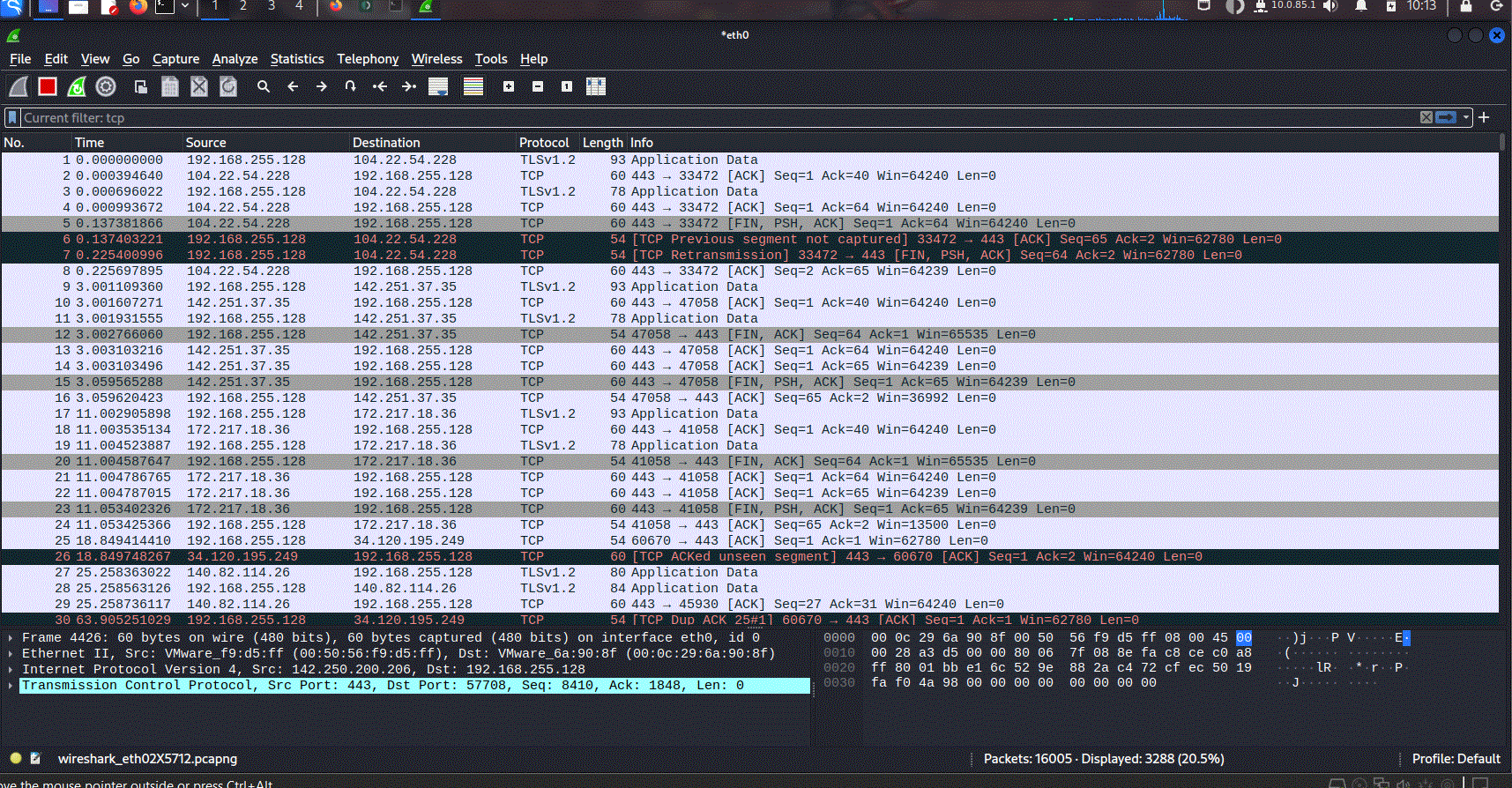
***Network Traffic Analysis Using Wireshark***

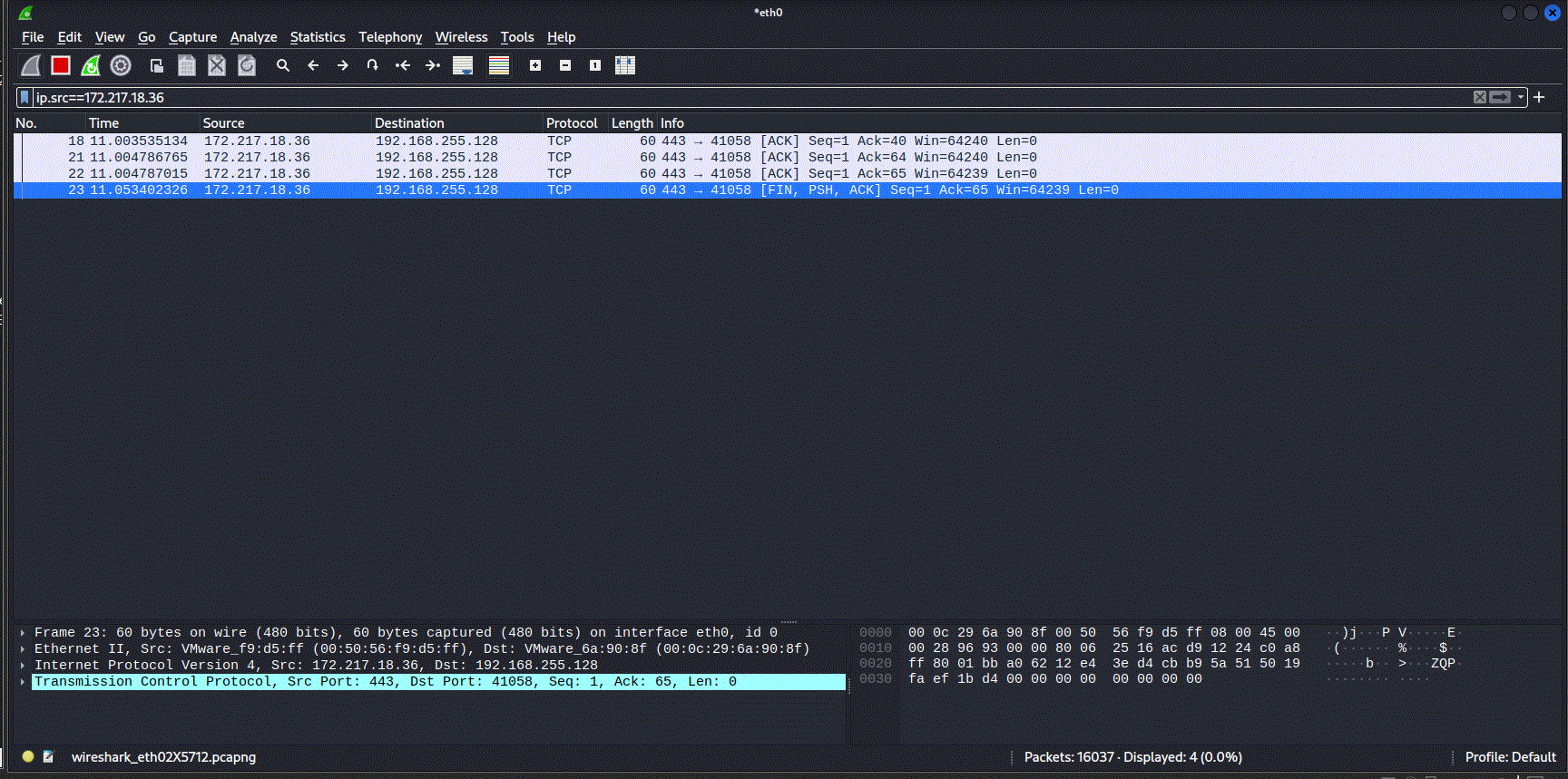
Wireshark is a powerful network protocol analyzer used for capturing and inspecting network traffic in real time. It helps cybersecurity professionals, network administrators, and developers analyze network communications, detect security threats, troubleshoot issues, and monitor data packets. Wireshark supports various protocols and provides detailed insights into network behavior, making it a valuable tool for network security and performance analysis.

-First Users must select the network interface they wish to monitor, such as eth0, Ethernet or WIFI.

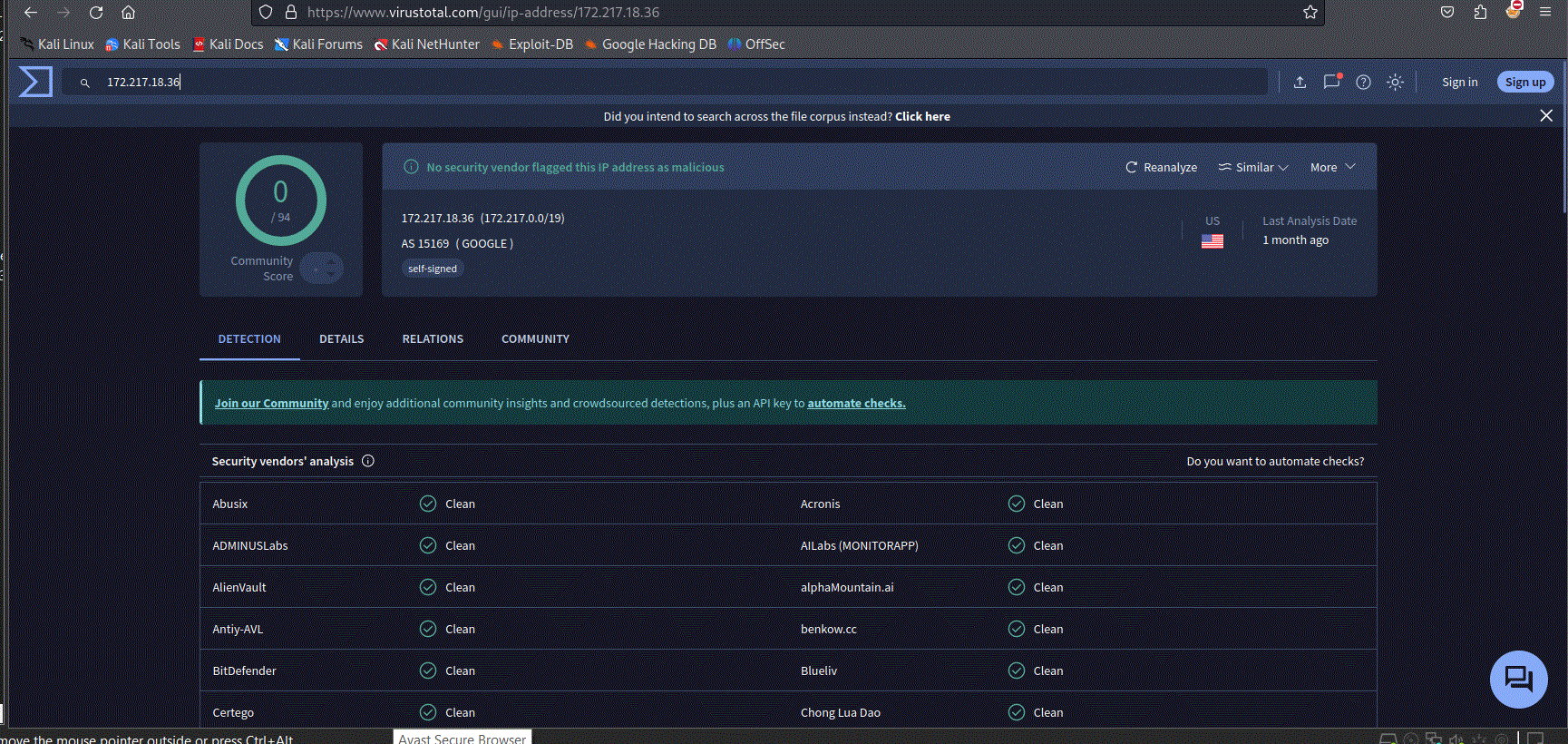


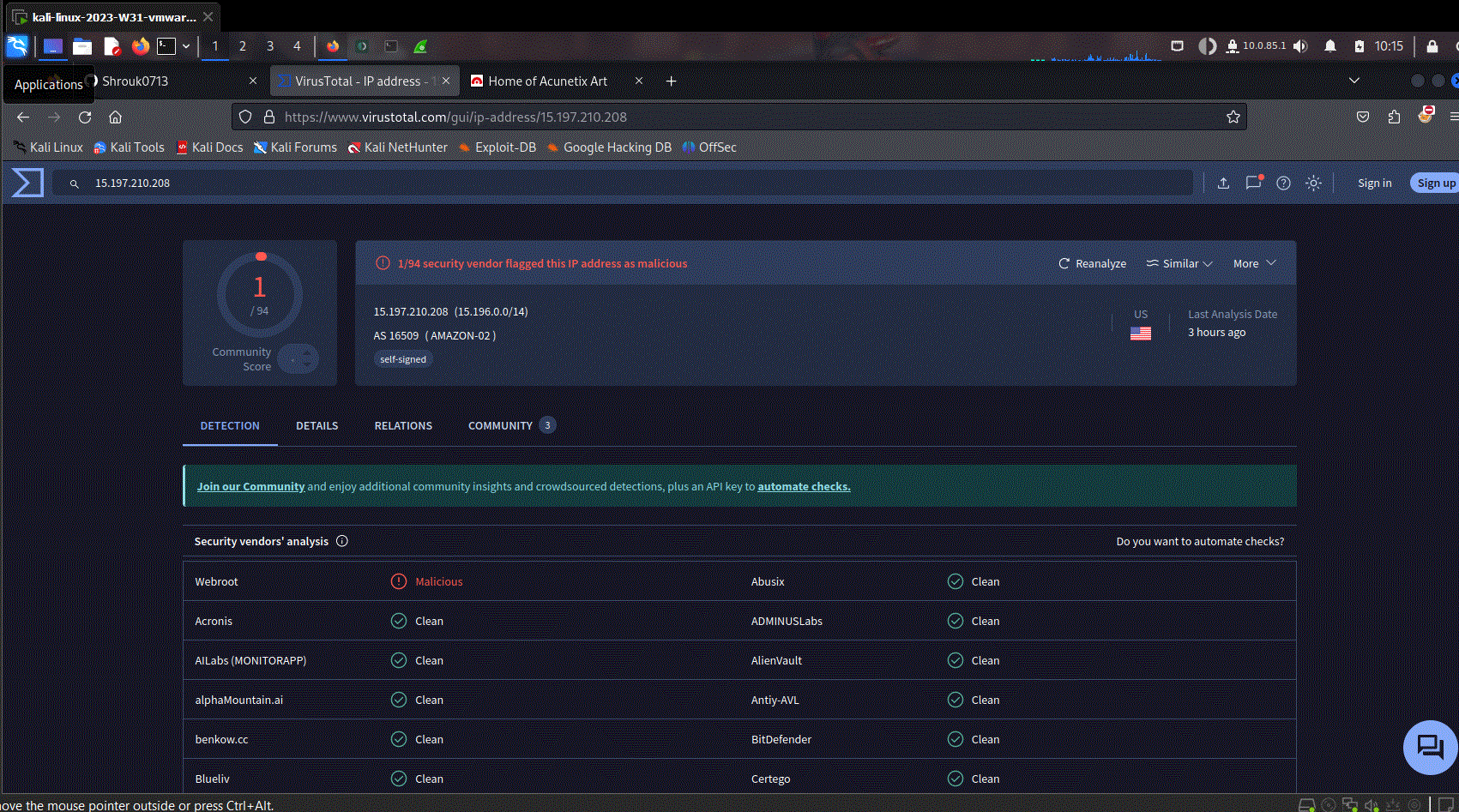
After capturing data packets, users can utilize Wireshark’s advanced filtering capabilities to analyze specific types of traffic. The display filter bar at the top of the interface allows users to apply filters based on criteria like IP addresses, protocols (such as HTTP or TCP), and port numbers. For example, using the filter “ip.addr == 172.217.18.36” as shown in the pictures will isolate packets associated with that particular IP, making it easier to focus on relevant network activity and streamline the analysis process.





When detecting suspicious IP addresses, it is essential to verify their authenticity. Tools like VirusTotal and Talos are highly useful for this purpose. By entering an IP address on the VirusTotal website, users can access data collected from various threat intelligence sources. The results help determine if the IP is linked to malicious activities, allowing for more informed security decisions.





-Network traffic analysis involves monitoring and inspecting data packets to detect suspicious activities, security threats, or anomalies. This report documents identified suspicious activities and provides recommendations to mitigate potential risks.

***Identified Suspicious Activities***

1-Unusual Outbound Traffic:

* High volume of data being sent to an unknown external IP.
* Possible indication of data exfiltration or compromised system.

2-Repeated Failed Login Attempts:

* Multiple failed authentication attempts from a single IP address.
* Possible brute-force attack on login credentials.

3-Communication with Malicious IPs:

* Traffic detected to known malicious domains or blacklisted IPs.
* Potential malware infection or command-and-control (C2) communication.

4-Use of Unauthorized Protocols or Ports:

* Detection of non-standard protocols (e.g., FTP, RDP) on unexpected ports.
* Possible data transfer attempts bypassing security controls.

***- Recommendations for Mitigation***

1-Monitor and Block Suspicious Traffic:

* Implement firewall rules to restrict outbound communication with untrusted IPs and block unauthorized ports.

2-Enhance Authentication Security:

* Enforce strong password policies, enable multi-factor authentication (MFA), and limit login attempts to prevent brute-force attacks.

3-Deploy Intrusion Detection and Prevention Systems (IDS/IPS):

* Use tools like Snort or Suricata to detect and block malicious activities in real time.

4-Regularly Update Threat Intelligence Feeds:

* Keep firewall, antivirus, and security tools updated with the latest threat intelligence to detect known malicious IPs.

4-Conduct Network Traffic Audits:

* Periodically review network logs using tools like Wireshark or Zeek to identify unusual patterns and ensure security compliance.

-This proactive approach will help minimize risks, strengthen network security, and prevent potential cyber threats.