# Threat Report Summary based on firewall log report.

Date: 2023-03-15

Time: 06:26:45 - 06:35:27

Source IP: 192.168.1.105-192.168.1.106-192.168.1.108-192.168.1.110-192.168.1.112

Destination IP: 192.168.1.255-203.0.113.5-198.51.100.24-203.0.113.10-10.10.10.10-192.168.1.230

Protocols: UDP, TCP, ICMP

Ports: 138, 44347, 22, 44348, 80, 44350, 1433, 44353, 161,

Info: Local Broadcast, SSH Attempt, Client Hello, SQL Server Access Attempt, Destination Unreachable, SNMP Access Attempt

Summary:

The ABC firewall detected six potential threats on 2023-03-15 between 06:26:45 and 06:35:27. All the threats originated from the source IP address, 192.168.1.105-192.168.1.106-192.168.1.108-192.168.1.110-192.168.1.112

1. The first threat was a UDP broadcast packet on port 138. This type of packet is commonly used by malware to spread across a network.
2. The second threat was an SSH attempt on port 22. SSH is a secure shell protocol that is often used to access remote servers. This threat could be an attempt to gain unauthorized access to a server on the network.
3. The third threat was a Client Hello packet on port 443. This type of packet is used to initiate a TLS connection. This threat could be an attempt to exploit a vulnerability in a web server on the network.
4. The fourth threat was a SQL Server Access Attempt on port 1433. SQL Server is a database management system. This threat could be an attempt to gain unauthorized access to a SQL Server database on the network.
5. The fifth threat was an ICMP activity with the "Destination Unreachable" message. ICMP (Internet Control Message Protocol) is commonly used for

network diagnostics, but in this context, it indicates a potential issue in reaching the specified destination (10.10.10.10). The "Destination Unreachable" message suggests that the network encountered difficulties reaching the intended destination. This threat could be DDOS attack.

6. The sixth threat was an SNMP Access Attempt on port 161. SNMP is a network management protocol that is used to monitor and manage network devices. This threat could be an attempt to gain unauthorized access to a network device on the network.

Recommendations:

- Block all traffic from the source IP address, 192.168.1.105-192.168.1.106-192.168.1.108-192.168.1.110-192.168.1.112
- Investigate the source IP address to determine the source of the threats.
- Update all software and firmware on the network to the latest versions.
- Implement a security information and event management (SIEM) system to monitor network traffic for suspicious activity.
- Consider using a network intrusion detection system (NIDS) to detect and block malicious traffic.
- Implement a network access control (NAC) system to restrict access to the network to authorized users and devices.
- Conduct regular security audits to identify and mitigate security vulnerabilities.