Cybersecurity Incident Report

The network protocol analyzer logs indicate that port 443 is unreachable when attempting to access the secure employee background check website. Port 443 is normally used for HTTPS traffic. This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack on the web server.

The incident occurred earlier this morning when the human resources (HR) team reported that they could not reach the background check web portal. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 443, which is used for HTTPS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. Our next steps include checking the firewall configuration to see if port 443 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The HR team believes it is possible that a certain new hire may want to keep them from performing the background check. The network security team suspects this person might have launched an attack to crash the background check website.

Incident Report Summary

Incident: Port 443 unreachable for the secure employee background check website

Date/Time: Earlier this morning

Reported by: HR team

Impact:

- HR team unable to access the background check web portal
- Potential delay in hiring process
- Loss of sensitive employee data if the website is compromised

Cause:

- Unknown at this time
- Possible causes include:
    - Firewall misconfiguration

    - System outage on the web server
    - Malicious attack

Next steps:

- Check firewall configuration to see if port 443 is blocked
- Contact the system administrator for the web server to have them check the system for signs of an attack
- Investigate the possibility of a malicious attack by a new hire

Possible Mitigations:

- Implement additional security measures for the web server, such as:
    - Enabling SSL/TLS encryption
    - Implementing a web application firewall
    - Regularly patching the web server software
- Educate HR team on cybersecurity best practices, such as:
    - Using strong passwords
    - Being aware of phishing attacks
    - Not clicking on suspicious links
    - Reporting any suspicious activity to the IT department
- Monitor the network for suspicious activity, such as:
    - Unusual traffic patterns
    - Attempts to access unauthorized resources
    - Unauthorized changes to system files
- Review the organization's cybersecurity policies and procedures to ensure that they are adequate.