A white text on a black background

Description automatically generated

**Background of Company:**

The Sirius Cybernetics Corporation is the primary manufacturer and supplier of androids, robots, automatic doors, digital watches, operating systems and autonomic assistants in the United States. They are known for their catchy jingles and catchphrases, which are created by their Marketing Department. Their primary claim to fame seems to be constructing just about everything with advanced robotics and software, from doors to lifts, toaster ovens, drink machines and even vacuum cleaners. Sirius Cybernetics has 342 employees, most working at the headquarters while some employees work remotely.

**Network Overview:**

Many of the users login into company Linux machines remotely.

10.10.10.1 – 10.10.10.100 are user machines

10.234.125.254 – Software repo; Maintains Foxy Fitzroy ROS

10.121.70.151 – Internal FTP Server

Separate 192.168.0.1/24 subnet for software develop of critical software

**Audit Findings:**

A recent audit has found that Sirius Cybernetics does not have a VPN setup for employees to connect to the network from home securely. In workgroup environments, users are given file share access with admin credentials. Employees are using their own various RDP solutions to remotely connect to their office workstations so RDP ports are open to the internet. Furthermore, they do not have a log management tool or centralized logging system in place. Sirius Cybernetics does not have any Data Loss Protection solution, nor does it perform regular penetration testing on its network infrastructure. No disaster recovery or incident response plan is in place. There is no monitoring for suspicious log-in activity. No documented security framework is being utilized. They also use Windows Automatic Updates to handle patching instead of a dedicated solution, which creates a lack of visibility across an environment of current patch status. You also scanned their Web Server for vulnerabilities and the report is provided.

**Threat Hunting / Forensics:**

Perform a threat hunt with the logs and evidence given to see if there are any additional findings. You have several PCAPs and a log of user logins. Review them to see if there are any exposures or incidents. Hint: There was an attack! You job is to hunt down the root cause of the attack and describe what happened along each step of the way. You should ask for evidence if you need it. Specifically, we can get bash history for some users at certain time intervals. Submit the request for evidence. Based on the bash history, you may want to request more evidence.