Step 11 – Remediation (Fixes for Identified Risks)

Device 1: 192.168.31.10

Port 22 – SSH (Medium Risk):

- Use strong passwords or SSH keys.
- Disable password login and use key-based authentication.
- Restrict SSH access to trusted IP addresses.
- Disable SSH entirely if not required.

Port 80 – HTTP (Medium Risk):

- Enable HTTPS instead of HTTP.
- Update any web server running on port 80.
- Disable the HTTP service if it is not needed.

Device 2: 192.168.31.238

Port 445 – SMB (High Risk):

- Turn off SMB file sharing if not needed.
- Block port 445 using the system firewall.
- Ensure the system is fully patched to prevent SMB vulnerabilities.
- Use strong passwords for shared folders.

Port 139 – NetBIOS (High Risk):

- Disable NetBIOS over TCP/IP.
- Turn off file and printer sharing.
- Block external access to this port using firewall rules.

Device 3: 192.168.31.70

Port 443 – HTTPS (Low Risk):

- Ensure SSL/TLS certificates are updated.

- Disable outdated protocols (SSLv2, SSLv3, TLS 1.0).

- Keep the web server fully updated.

Device 4: 192.168.31.22

Port 5555 – ADB (Critical Risk):

- Turn off ADB over Wi-Fi from Developer Options.

- Use USB debugging instead of wireless debugging.

- Never expose port 5555 on any network.

- Restart the device after disabling ADB over Wi-Fi.

Overall Network Security Recommendations:

- Close all unnecessary ports.

- Enable firewalls with strict inbound/outbound rules.

- Keep operating systems and firmware updated.

- Disable file sharing unless required.

- Use WPA2/WPA3 Wi-Fi encryption.

- Separate IoT devices onto a guest network.