0:00 - 5:00 (First 5 Minutes: Preparation)

- **Task**: Split the team into roles for simultaneous execution.
- Assign roles:
  - Password changes.
  - Service and port scanning.
  - Backups and defensive software installation.
  - Stopping unnecessary services and enabling firewalls.
  - Monitoring and steady-state setup.

5:00 - 20:00 (Password Changes & Initial Scanning)

- **Password Changes**:
  - Use a password manager or script to set strong passwords for all system accounts.
  - Document new passwords securely for the team.
- **Service and Port Discovery**:
  - Linux: Use `netstat`, `ss`, or nmap to list services and open ports.
  - Windows: Use `netstat`, PowerShell commands, or tools like Advanced Port Scanner.

20:00 - 35:00 (Backup & Defensive Software)

- **Create Backups**:
  - Backup key configuration files (e.g., `/etc/` on Linux, `C:\Windows\System32\` on Windows).
  - Run the "generic_bkup.sh" script on Linux
- **Install Defensive Software**:
  - Linux:
    - Install and configure `ClamAV`, `rkhunter`, and `fail2ban`.
    - Run initial scans where feasible.
  - Windows:
    - Ensure Antivirus (Windows Defender) is installed and up-to-date.

35:00 - 45:00 (Stop Unnecessary Services & Enable Firewalls)

- **Stop Unnecessary Services**:
  - Linux:
    - Use `systemctl` or `service` commands to identify and disable non-critical services.
  - Windows:
    - Use `services.msc` or PowerShell to disable services.
- **Enable Firewalls**:
  - Linux:
    - Configure `iptables` or `ufw` rules.
  - Windows:
    - Configure Windows Firewall with strict inbound/outbound rules.

45:00 - 55:00 (Establish Steady State)

- Confirm all critical services are running and secured.
- Set up centralized monitoring for logs:
  - Linux: Configure `syslog` or `journald`.
  - Windows: Set Event Viewer alerts.
- Check defensive tools for anomalies.
- CONSTANTLY monitor the logs (/var/log/messages or syslog)

55:00 - 60:00 (Final Check & Monitoring)

- Conduct a final sweep for vulnerabilities (e.g., quick re-scan ports and services).
- Test backups.
- Designate a team member to monitor logs and alerts in real-time.

This plan assumes parallel execution to maximize efficiency and leverages team members' expertise.