Task 4: Linux Server Hardening

Objective

Capture and analyze live network traffic to identify credentials or suspicious activity. Apply Linux server hardening techniques using Ubuntu, UFW, Fail2ban, and SSH.

Before State

- Firewall (UFW): Inactive
- Fail2ban: Not installed ("Unit fail2ban.service could not be found")
- SSH configuration: Root login allowed, password authentication enabled
- Open Ports: 22 (SSH), 80 (HTTP), 3306 (MySQL – exposed)
- Traffic Capture Findings: Cleartext HTTP traffic observed with 'Authorization: Basic' headers (credentials leaked)

Actions Applied

- Installed and enabled UFW, set default deny incoming, allow outgoing
- Allowed only necessary ports (22/tcp for SSH, 80/tcp for HTTP, 443/tcp for HTTPS)
- Installed and configured Fail2ban with SSH jail (bantime=3600s, maxretry=5)
- Hardened SSH configuration: Disabled root login, disabled password authentication, enforced key-based login
- Updated system packages and removed unnecessary services (e.g., telnet)
- Performed post-hardening packet capture: No cleartext credentials observed

After State

- Firewall (UFW): Active with deny incoming / allow outgoing policy
- Fail2ban: Installed, running, protecting SSH (verified with 'fail2ban-client status')
- SSH configuration: Root login disabled, password authentication disabled, key-based login enabled
- Open Ports: 22 (SSH, limited), 80 (HTTP), 443 (HTTPS), MySQL (3306) blocked externally
- Traffic Capture Findings: No cleartext credentials detected after hardening

Risk Reduction

Brute force attacks are mitigated with Fail2ban and UFW rate limiting. Password-based SSH authentication is disabled, removing exposure to credential guessing attacks. Unnecessary services removed and MySQL external exposure blocked. Plaintext credential leakage reduced; migration to HTTPS is still recommended for full protection.

Deliverables

1. Before/After state summary (included in this document)
2. Applied commands list (see applied_commands.sh file)
3. Screenshots:
   - UFW before/after status
   - Fail2ban before (not found) and after (active jail)
   - SSH config before/after
   - Tcpdump/Tshark showing credentials before and absence after hardening