**Task 2: SSL/TLS Implementation Report**

# Environment Setup

- Server: Kali Linux VM running Apache2  
- Attacker: Kali Linux VM for testing  
- Both on same virtual network (Bridged/NAT)

# Tools Used

- Apache2 — Web server  
- OpenSSL — To create self-signed certificate  
- curl — To test HTTPS traffic

# Steps

1. Created a self-signed certificate and private key:  
 sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \  
 -keyout /etc/ssl/private/apache-selfsigned.key \  
 -out /etc/ssl/certs/apache-selfsigned.crt  
  
2. Configured Apache to use the certificate:  
 Edited /etc/apache2/sites-available/default-ssl.conf  
 Set:  
 SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt  
 SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key  
  
3. Enabled SSL module and default SSL site:  
 sudo a2enmod ssl  
 sudo a2ensite default-ssl  
 sudo systemctl restart apache2  
  
4. Configured HTTP to redirect to HTTPS:  
 Edited /etc/apache2/sites-available/000-default.conf:  
 Added inside <VirtualHost \*:80>:  
 Redirect "/" "https://192.168.85.134/"  
  
 Restarted Apache:  
 sudo systemctl restart apache2

# Tests

Tested HTTP redirect:  
 curl -I http://192.168.85.134/  
 Expected: HTTP/1.1 301/302 redirect to HTTPS.  
  
 Tested HTTPS response:  
 curl -kI https://192.168.85.134/  
 Expected: HTTP/1.1 200 OK  
  
 Verified with browser: Accessed https://192.168.85.134/  
 Browser showed warning (self-signed) and loaded page.

# Evidence

Attached:  
- Screenshot of HTTP request showing redirect (302 Found)  
- Screenshot of HTTPS curl showing 200 OK  
- Screenshot of browser accessing https://192.168.85.134/

# Conclusion

SSL/TLS was successfully implemented with a self-signed certificate. HTTP traffic is redirected to HTTPS, ensuring data in transit is encrypted. Tested with curl and browser; verified working.