Instrukcja dla prowadzącego — Scenariusz 4 (HTTP Interception, Lab04)

Temat laboratorium

Przechwytywanie i modyfikowanie ruchu HTTP w środowisku kontenerowym Docker przy użyciu mitmproxy.

Cel dydaktyczny

Pokazać studentom, jak działa atak typu Man-in-the-Middle w warstwie aplikacji (HTTP), bez potrzeby wykonywania ARP/DNS spoofingu.
Scenariusz demonstruje:

- interceptowanie żądań HTTP i HTTPS,
- modyfikowanie odpowiedzi serwera w czasie rzeczywistym,
- ekstrakcję danych POST (np. loginów),
- logowanie ruchu do plików,
- wdrożenie własnego skryptu MITM w Pythonie.

Co sprawdzać podczas zajęć

Prowadzący powinien zweryfikować:

1. Czy projekt został sklonowany poprawnie i struktura plików jest zgodna z repo.
2. Czy kontenery uruchamiają się i tworzą sieć zgodną z docker-compose-scenario4.yml.
3. Czy interceptor działa, czyli:
    - logi w /app/logs/requests.log i responses.log powstają,
    - dane POST są widoczne,
    - wykryta jest modyfikacja HTML (iniekcja JS).
4. Czy student potrafi uzasadnić, dlaczego HTTPS chroni przed takim atakiem MITM, a HTTP nie.

Co ma zrobić prowadzący podczas demonstracji

- pokazać działające proxy MITM: docker logs -f advanced_interceptor
- pokazać logi: docker exec advanced_interceptor cat /app/logs/requests.log
- omówić zagrożenia bezpieczeństwa i typowe zabezpieczenia (HSTS, TLS).

Zasady oceniania (dla prowadzącego)

Element	Opis	Punkty
1. Poprawne uruchomienie środowiska Docker	Kontenery + sieć działają	2
2. Działanie proxy MITM	Interceptor startuje bez błędów	2
3. Logowanie żądań HTTP/POST	W plikach pojawiają się dane POST	2
4. Modyfikacja odpowiedzi HTML	Iniekcja JS widoczna	2
5. Analiza wyników i wnioski	Student potrafi wyjaśnić zagrożenia i obronę	2
RAZEM		**10 punktów**