Report: Analisi delle Vulnerabilità in DVWA

Obiettivo dell'esercitazione

- Caricare una shell PHP su DVWA (Damn Vulnerable Web Application) per dimostrare una vulnerabilità nell'upload di file.
- Eseguire comandi sulla macchina remota utilizzando la shell caricata.
- Intercettare e analizzare il traffico HTTP con Burp Suite per comprendere il flusso delle richieste e individuare eventuali vulnerabilità.

Passaggi eseguiti

1. Preparazione dell'ambiente

- Configurate due macchine virtuali:
- Kali Linux: utilizzata per eseguire l'attacco.
- Metasploitable: macchina bersaglio con DVWA installato.
- Verificata la connessione tra le due macchine con un semplice ping.

2. Caricamento della shell PHP

- Creato un file PHP (shell.php) con il seguente contenuto:
  <?php system($_REQUEST["cmd"]); ?>
- Ho impostato 'DVWA Security' in low
- Acceduto alla sezione File Upload di DVWA.
- Caricato il file PHP con successo. Ho annotato il percorso del file caricato.

3. Esecuzione della shell

- Acceduto alla shell PHP tramite il browser utilizzando l'URL del file caricato.
- Eseguiti diversi comandi tramite il parametro cmd, come:
  - ls: per elencare i file nella directory corrente.
  - pwd: per vedere il percorso della directory corrente.

4. Intercettazione e analisi con Burp Suite

- Configurato il browser per passare attraverso il proxy di Burp Suite.
- Intercettato il traffico HTTP durante il caricamento del file e l'esecuzione dei comandi sulla shell.
- Analizzate le richieste HTTP/HTTPS per:

- Osservare la struttura delle richieste POST durante l'upload.
- Identificare i parametri utilizzati per inviare comandi alla shell.

Vulnerabilità individuate

1. Insufficiente validazione dei file:
   - Nessun controllo sul tipo di file caricato.
   - Permesso di caricare file PHP, che consente l'esecuzione remota di comandi.
2. Esecuzione remota di comandi:
   - È stato possibile eseguire comandi arbitrari sul server bersaglio.
3. Richieste HTTP non sicure:
   - I dati sensibili, come il percorso del file e i comandi inviati, sono stati facilmente intercettati tramite Burp Suite.

Conclusioni

L'esercitazione ha dimostrato come una configurazione insicura di un modulo di upload possa compromettere gravemente un sistema web. Questo tipo di vulnerabilità è comune nelle applicazioni web mal configurate e può essere mitigato con:

- Validazione del tipo di file.
- Restrizioni sui permessi di esecuzione per i file caricati.
- Uso di protocolli sicuri (HTTPS) per proteggere i dati in transito.

In allegato gli screenshot.