Hacking con Metasploit

Introduzione

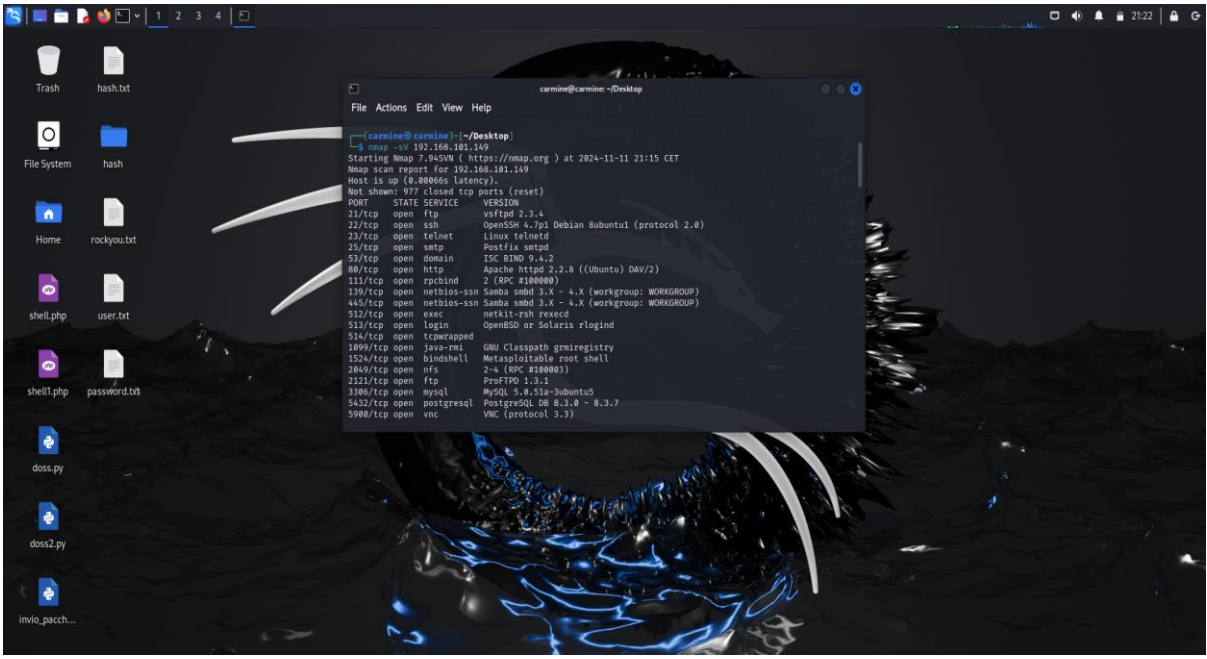
Nell'ambito di uno studio sulla sicurezza informatica, abbiamo condotto un esperimento per valutare la vulnerabilità del servizio vsftpd. Abbiamo utilizzato una macchina virtuale Metasploitable2, configurata con l'indirizzo IP 192.168.101.149/24, per simulare un ambiente di produzione. L'obiettivo era dimostrare come un attaccante, sfruttando una vulnerabilità nota, potesse ottenere l'accesso non autorizzato a un sistema e compiere azioni dannose. Dopo aver modificato l'indirizzo IP della macchina virtuale per isolarla, abbiamo utilizzato Metasploit per eseguire l'attacco e ottenere una shell interattiva. Una volta all'interno del sistema, abbiamo creato una nuova cartella per verificare il nostro accesso.

Preparazione dell'Ambiente

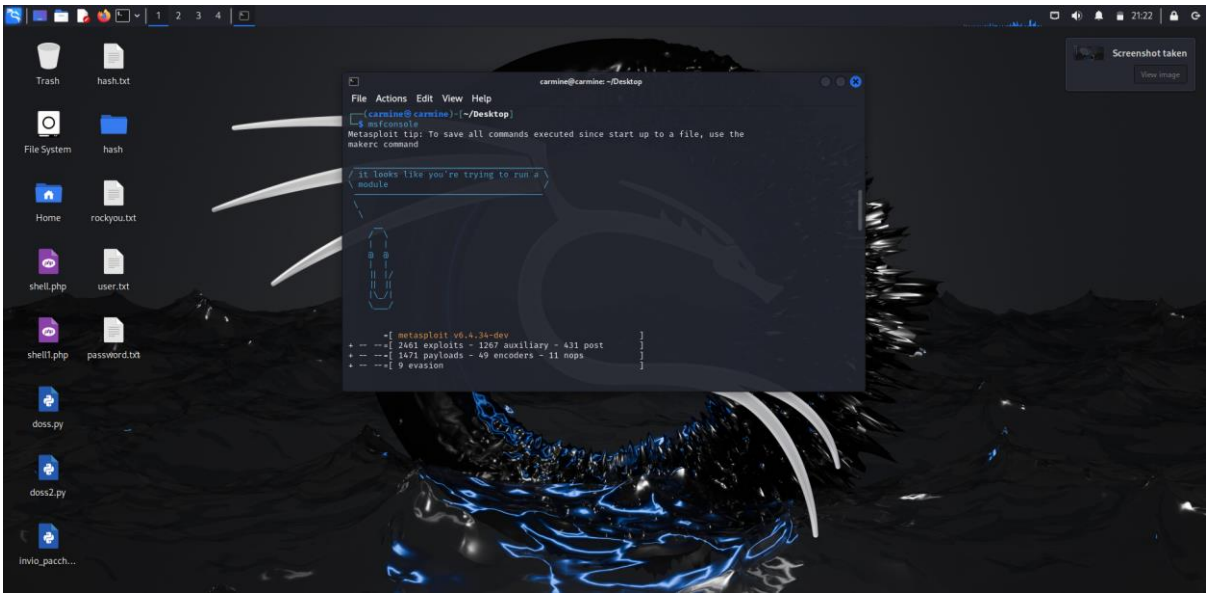
- **Configurazione di Metasploitable2:**
  - **Cambio di Indirizzo IP:**
    - Per garantire un isolamento maggiore e una migliore simulazione di un ambiente reale, è stato modificato l'indirizzo IP della macchina Metasploitable2.
  - **Verifica della Connettività:** Dopo la modifica dell'indirizzo IP, è stata verificata la raggiungibilità della macchina tramite ping .

Svolgimento dell'Attacco

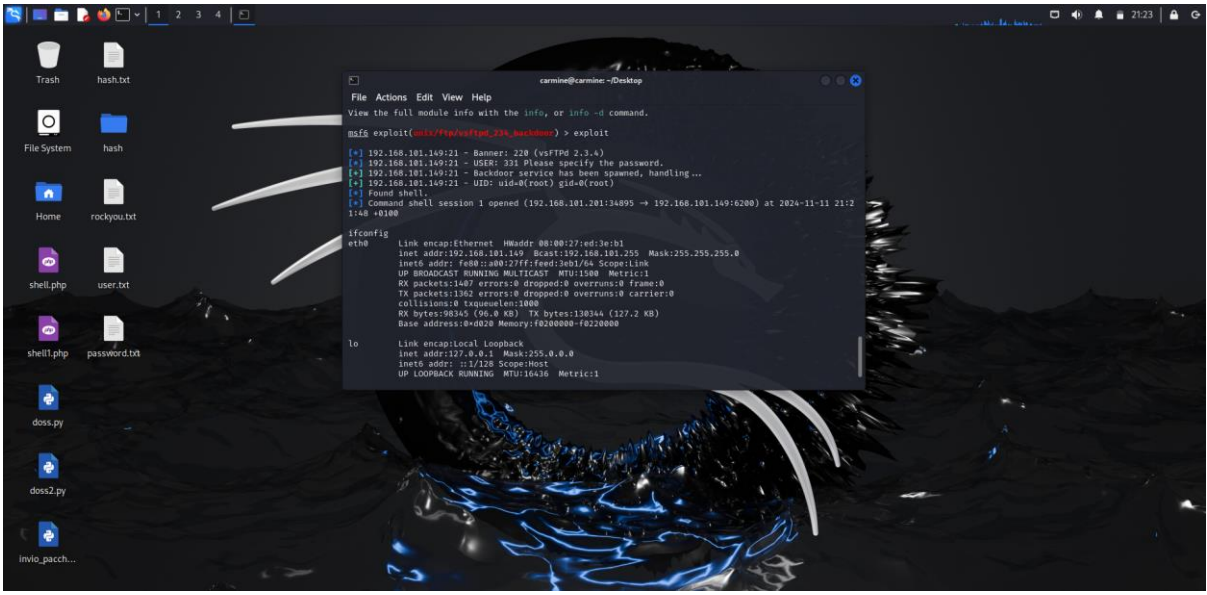
- **Identificazione della Vulnerabilità:**
  - È stata condotta una scansione iniziale della macchina Metasploitable2 per identificare i servizi in esecuzione e le eventuali vulnerabilità presenti.
  - *[Per la scansione delle porte abbiamo usato il comando nmap –sV 192.168.101.149*
  - In particolare, è stata individuata una vulnerabilità nel servizio vsftpd.



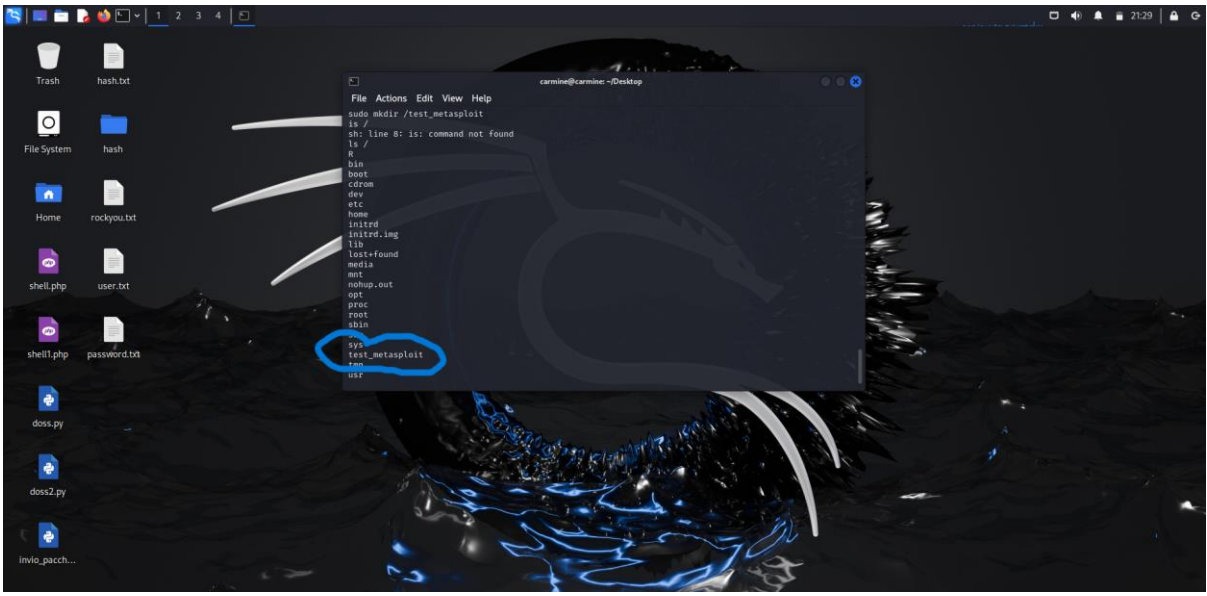
- **Sfruttamento della Vulnerabilità:**
  - Utilizzando il framework Metasploit, è stato selezionato un exploit appropriato per la vulnerabilità identificata.



- **Ottenimento dell'Accesso:**
  - A seguito dell'esecuzione dell'exploit, è stata ottenuta una shell interattiva sulla macchina vittima.



- **Creazione della Cartella:**
    - Utilizzando i comandi della shell, ci si è spostati nella directory root (`/`) e si è creata una nuova cartella chiamata `test_metasploit` utilizzando il comando sudo `mkdir /test_metasploit`.



Conclusioni

L'attacco condotto su Metasploitable2 ha evidenziato l'importanza di mantenere aggiornati i sistemi e di configurare correttamente i servizi. Sfruttando una vulnerabilità presente nel servizio vsftpd, siamo riusciti a ottenere una shell interattiva sulla macchina vittima. Questo ci ha permesso di eseguire comandi arbitrari, incluso la creazione della cartella 'test_metasploit' nella directory root. L'esperimento sottolinea come un attaccante, con le giuste competenze e strumenti, possa compromettere la sicurezza di un sistema anche attraverso vulnerabilità apparentemente minori