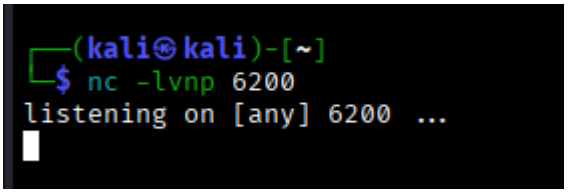
INDICE

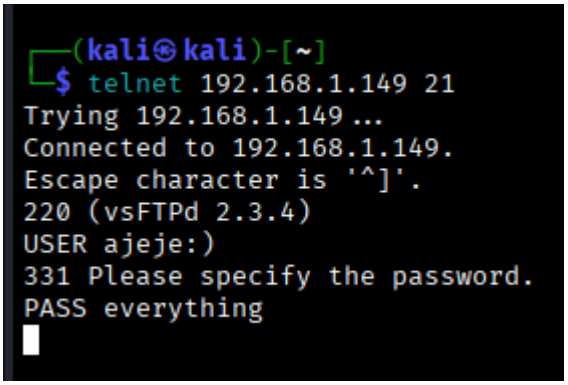
INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il laboratorio facoltativo ha l'obiettivo di approfondire il funzionamento interno di una vulnerabilità nota del servizio FTP vsftpd, andando oltre l'utilizzo automatico di framework di exploitation.
L'attività si concentra sull'analisi del comportamento dell'exploit a livello applicativo e di rete, evidenziando come una sequenza specifica di interazioni con il servizio possa innescare l'attivazione di una backdoor.
Questo approccio consente di comprendere in modo più consapevole le dinamiche di compromissione, mettendo in relazione codice, protocollo e impatto operativo sul sistema bersaglio.

OBIETTIVO: analizzare il codice dell'exploit vsftpd 2.3.4 e riprodurne manualmente il comportamento utilizzando strumenti di base di interazione di rete, dimostrando l'apertura di una shell remota con privilegi elevati. L'attività mira a rafforzare la comprensione dei meccanismi di exploitation e delle implicazioni di sicurezza derivanti dall'esposizione di servizi vulnerabili.



A supporto della riproduzione manuale dell'exploit, è stata predisposta una sessione di ascolto su una porta di rete specifica, coerente con il comportamento osservato durante l'analisi del codice dell'exploit. Questa fase ha lo scopo di intercettare l'eventuale connessione in ingresso generata dal servizio compromesso, consentendo di verificare in modo diretto l'attivazione della backdoor.
L'apertura del listener rappresenta un passaggio cruciale, in quanto permette di distinguere chiaramente tra la fase di innesco della vulnerabilità e la successiva fase di interazione con la shell remota.
La corretta messa in ascolto conferma inoltre la comprensione del flusso di rete previsto dall'exploit, dimostrando che l'accesso remoto non dipende dal framework di automazione, ma da una comunicazione di rete esplicita avviata dal sistema bersaglio.



In questa fase viene stabilita una connessione diretta al servizio FTP esposto dalla macchina bersaglio, identificato come vsftpd versione 2.3.4. L'interazione con il servizio avviene attraverso l'invio di una sequenza controllata di credenziali, costruita in modo da sfruttare una debolezza nota del software.
Questo passaggio non ha come obiettivo l'autenticazione legittima, bensì l'attivazione di un comportamento anomalo interno al servizio, che porta all'avvio di una backdoor in ascolto su una porta di rete non standard.
La risposta del servizio conferma che la comunicazione è stata accettata e che la sequenza di input è stata elaborata correttamente, creando le condizioni necessarie per la successiva esposizione di una shell remota.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 6200 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-22 08:02 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.0014s latency).

PORT     STATE SERVICE
6200/tcp open  lm-x
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

A seguito dell'interazione con il servizio FTP, è stata eseguita una verifica mirata sullo stato delle porte di rete della macchina bersaglio.
L'analisi ha evidenziato l'apertura di una porta precedentemente non esposta, riconducibile al meccanismo di backdoor associato alla vulnerabilità analizzata; la presenza della porta in stato di ascolto conferma che il servizio compromesso ha attivato correttamente una shell remota, rendendo il sistema accessibile dall'esterno senza ulteriori fasi di autenticazione. Questo riscontro rappresenta un'evidenza chiara dell'avvenuta compromissione e consente di distinguere in modo netto la fase di innesco della vulnerabilità dalla fase di accesso operativo al sistema.

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.149 6200
whoami
root
cd /test_metasploit
pwd
/test_metasploit
ls -la
total 8
drwx------  2 root root 4096 Jan 20 16:00 .
drwxr-xr-x 22 root root 4096 Jan 20 16:00 ..
```

Una volta confermata l'esposizione della porta associata alla backdoor, è stato stabilito l'accesso alla shell remota generata dal servizio compromesso.
La sessione ottenuta ha consentito di interagire direttamente con il sistema bersaglio, verificando il contesto di esecuzione e la posizione all'interno del filesystem.
Le informazioni restituite dalla shell indicano chiaramente che l'accesso avviene con privilegi massimi di sistema, permettendo operazioni complete sul filesystem, inclusa la navigazione nella directory root e la gestione delle risorse di sistema.
La presenza della directory precedentemente creata costituisce una conferma operativa dell'effettivo controllo del sistema remoto.
Questa fase dimostra in modo inequivocabile l'impatto della vulnerabilità analizzata, evidenziando come una semplice interazione con un servizio esposto possa portare all'ottenimento di accesso amministrativo completo, con conseguenze critiche in termini di sicurezza, integrità e riservatezza del sistema.

CONCLUSIONE

L’attività condotta ha evidenziato come la presenza di un servizio FTP vulnerabile possa rappresentare un punto di ingresso critico per la compromissione completa di un sistema. Lo sfruttamento della vulnerabilità associata a vsftpd 2.3.4 ha permesso di attivare una backdoor e ottenere accesso remoto con privilegi di amministrazione, dimostrando un impatto elevato sulla sicurezza complessiva dell’infrastruttura e la possibilità di instaurare una shell remota con privilegi root senza l’uso di credenziali valide mette in luce gravi carenze in termini di controllo degli accessi e gestione delle superfici esposte. I
n uno scenario reale, una vulnerabilità di questo tipo consentirebbe a un attaccante di eseguire operazioni arbitrarie sul sistema, compromettendo dati, servizi e continuità operativa.
L’analisi conferma quindi la necessità di adottare politiche rigorose di aggiornamento dei servizi, riduzione dell’esposizione delle porte di rete e monitoraggio attivo delle anomalie di traffico ed infine la mancata mitigazione di vulnerabilità note può tradursi rapidamente in incidenti di sicurezza ad alto impatto, con conseguenze significative per l’organizzazione sotto il profilo operativo, reputazionale e di conformità.