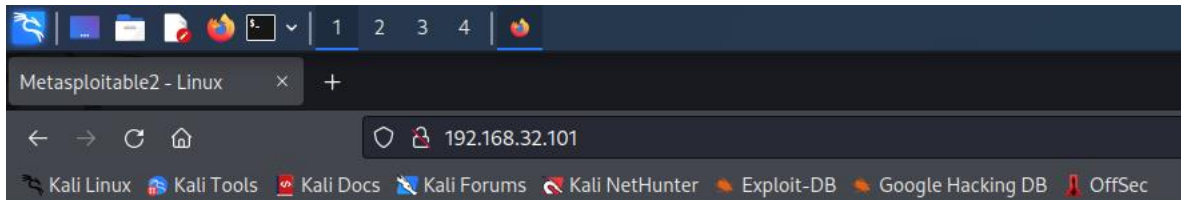


ENUMERAZIONE METODI HTTP ABILITATI

Creazione del programma in Python per mostrare i metodi http abilitati nella pagina web /phpMyAdmin.html del server.



Warning: Never expose this VM to an untrusted network!

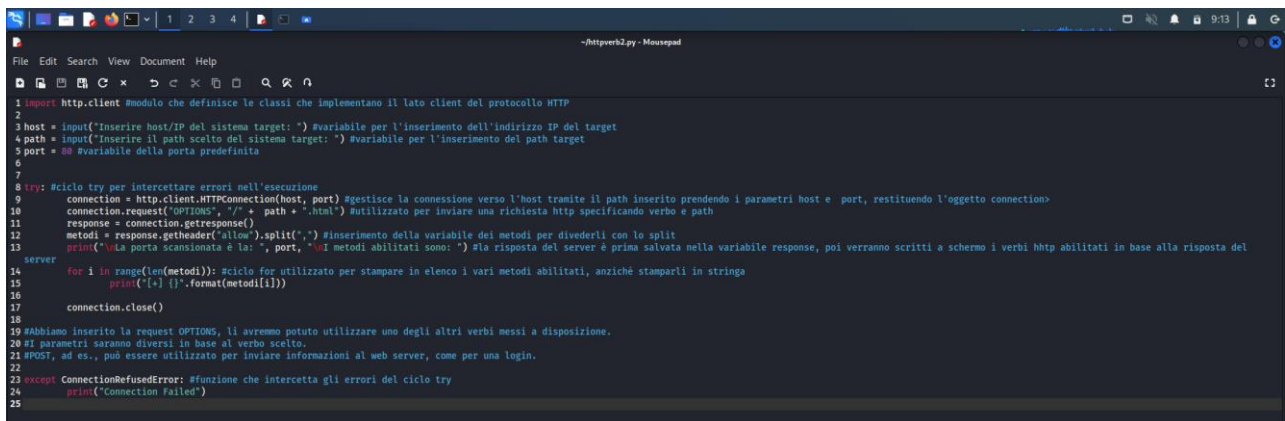
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Il programma, così compilato, è composto da:

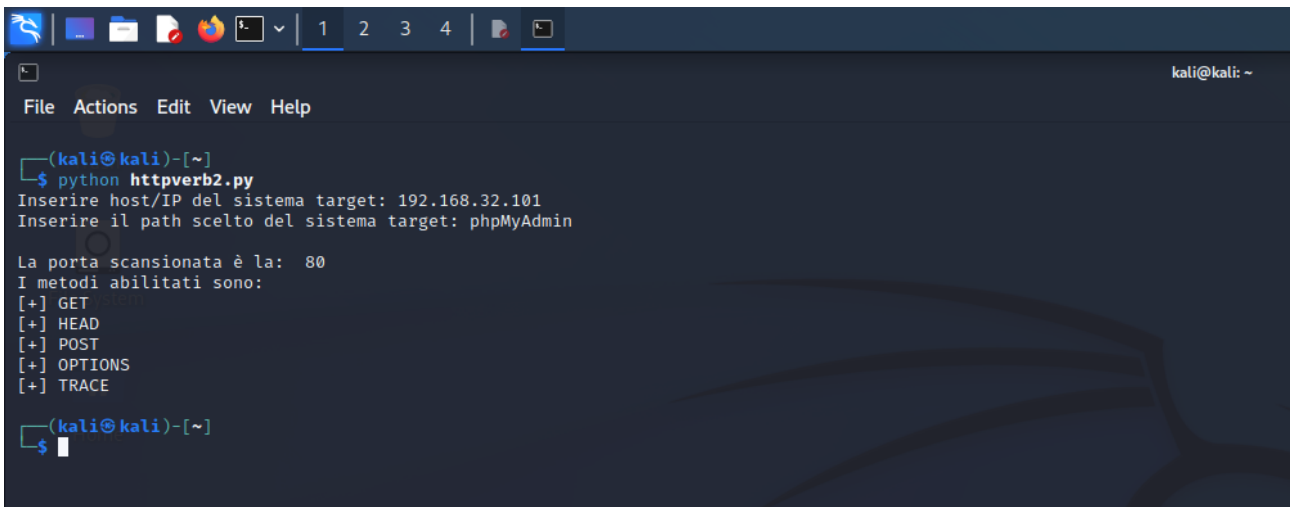
- Inserimento della libreria http.client già presente su Kali Linux per poter utilizzarne le funzioni;
- Inserimento delle variabili con le funzioni input dell'utente;
- Ciclo try per intercettare errori di esecuzione con la funzione except;
- Ciclo for per la compilazione in elenco dei metodi abilitati, anziché in stringa.



Tramite il programma si è riscontrato che i metodi http abilitati, sulla porta predefinita 80, sono:

- GET
- HEAD

- POST
- OPTIONS
- TRACE



```
(kali@kali)-[~]
$ python httpverb2.py
Inserire host/IP del sistema target: 192.168.32.101
Inserire il path scelto del sistema target: phpMyAdmin

La porta scansionata è la: 80
I metodi abilitati sono:
[+] GET
[+] HEAD
[+] POST
[+] OPTIONS
[+] TRACE

(kali@kali)-[~]
$
```

Il metodo GET può essere inteso come un servizio di richiesta, creato per inviare e ricevere informazioni su vari server e client web. Questo metodo è considerato inadatto e insicuro per la trasmissione di informazioni sensibili.

Il metodo HEAD è analogo a GET, ma restituisce solo i campi dell'header, ad esempio per verificare la data di modifica del file.

Il metodo POST scrive i parametri URL nella richiesta HTTP indirizzata al server, celandoli però alla vista dell'utente. Le richieste POST non prevedono un limite massimo di grandezza.

Con il metodo OPTIONS il client può richiedere quali metodi supporta il server per il file in questione.

Il metodo TRACE può essere usato per ricostruire il percorso di una richiesta HTTP fino al server e di ritorno dal server al client, ossia il browser in utilizzo.