# Esercitazione W16D1 - Pratica 2

# Exploit Twiki

Fabio Benevento - 21/02/2024

## 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 precedente, se dovessero esserci problemi è consentito "fare l'hacker"

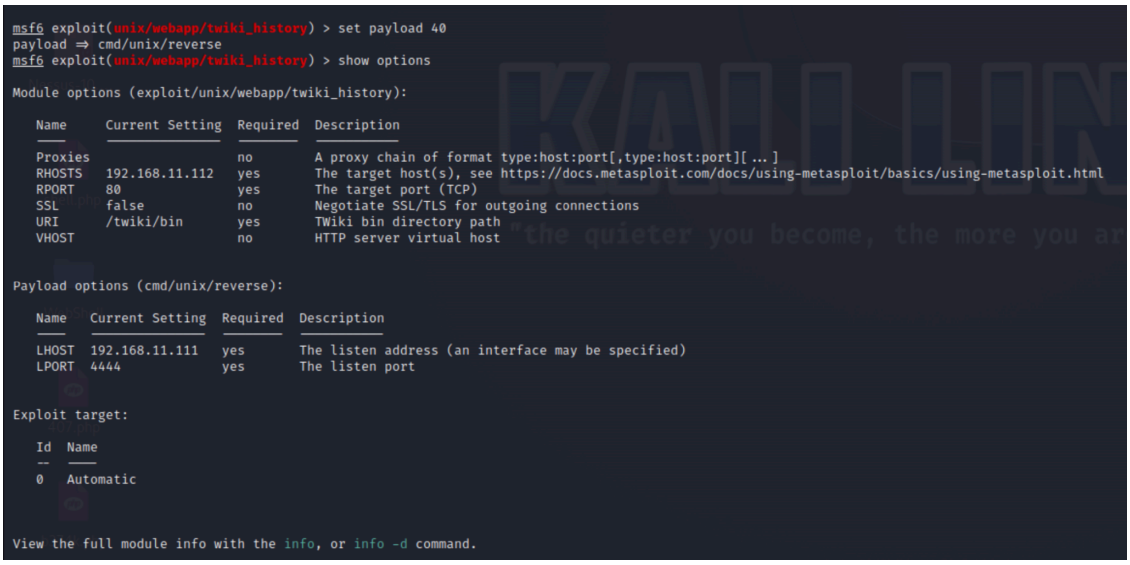
## Implementazione

Dopo aver avviato il tool Metaspoloit con il comando `search telnet_version` ho ricercato l'exploit `auxiliary/scanner/telnet/version` visto a lezione e l'ho selezionato tramite il comando `use 1`.

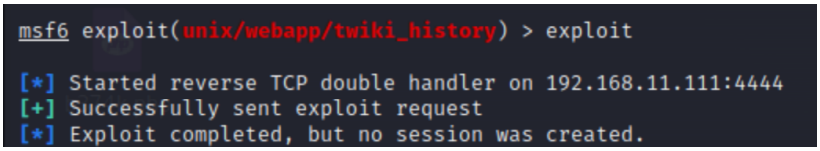
```
msf6 > search twiki

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw        2012-12-30       manual     Yes    MoinMoin twikidraw Action Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins         2014-10-09       excellent  Yes    TWiki Debugenableplugins Remote Code Execution
   2  exploit/unix/webapp/twiki_history             2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parameter Command Exec
ution
   3  exploit/unix/webapp/twiki_maketext            2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search              2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Command Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search

msf6 >
msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
```

Tramite il comando show payloads ho analizzato i payload disponibili e selezionato il payload cmd/unix/reverse

Ho quindi analizzato i parametri richiesti tramite il comando `show options`.
L'unico parametro obbligatorio non settato è il parametro RHOSTS che ho impostato con l'indirizzo della macchina target Metasploitable ovvero 192.168.11.112. Il resto dei parametri vanno bene nella configurazione di default.
Ho riverificato la correttezza dei parametri eseguendo nuovamente il comando `show options`




Ho eseguito l'exploit con il comando exploit. Il comando, come mostrato in figura restituisce l'errore "" ad indicare che l'exploit con il payload prescelto non va a buon fine.




I motivi possono essere molteplici:
1) Mancata corrispondenza tra payload e architettura dell'exploit
2) Mancata corrispondenza in LHOST / SRVHOST
3) Dispositivo dietro NAT
4) Politica restrittiva del firewall
5) Presenza di antivirus
6) L'exploit non funziona correttamente o è obsoleto