Oggi siamo andati ad exploitare il servizio Telnet di metasploitable.

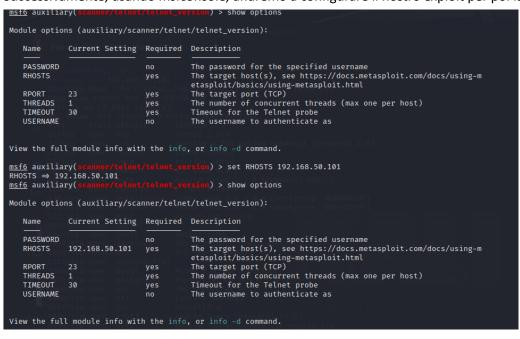
Cosa è un exploit? Gli exploit sono vettori di attacco che vengono utilizzati per sfruttare le vulnerabilità trovate nelle fase precedenti di un pentesting.

Nel nostro caso, abbiamo effettuato una scansione con nmap per vedere i servizi attivi.

```
kali@kali: ~
File Actions Edit View Help
 —(kali⊕kali)-[~]
 -$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:42 CET
Nmap scan report for 192.168.50.101
Host is up (0.014s latency).
Not shown: 978 closed tcp ports (conn-refused)
        STATE SERVICE
                           VERSION
21/tcp
        open ftp
                           vsftpd 2.3.4
22/tcp
        open ssh
                           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp
        open telnet
                           Linux telnetd
25/tcp
                           Postfix smtpd
        open smtp
53/tcp
        open domain
                           ISC BIND 9.4.2
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp
        open
              http
111/tcp
        open rpcbind
                           2 (RPC #100000)
139/tcp
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
        open
        open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp
512/tcp
              exec
                           netkit-rsh rexecd
        open
513/tcp
        open login?
                           Netkit rshd
514/tcp open shell
              java-rmi GNU Classpath grmiregistry
1099/tcp open
2049/tcp open nfs
                           2-4 (RPC #100003)
              ccproxy-ftp?
2121/tcp open
3306/tcp open mysql
                           MySQL 5.0.51a-3ubuntu5
              postgresql
5432/tcp open
                           PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc
                           VNC (protocol 3.3)
6000/tcp open
                           (access denied)
                          UnrealIRCd
6667/tcp open irc
8009/tcp open ajp13
                           Apache Jserv (Protocol v1.3)
                           Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open http
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:li
nux:linux_kernel
```

Una volta effettuata la scansione, possiamo notare che sulla porta 23 è attivo il servizio telnet.

Successivamente, usando msfconsole, andremo a configurare il nostro exploit per poi lanciarlo.



Per configurare il nostro exploit, andremo a controllare quali sono i dati necessari e non già presenti, come da screen: Una volta eseguita la configurazione (qua siamo solo andati a configurare il campo "RHOSTS" inserendo l'ip del nostro Metasploitable) eseguiremo il nostro exploit. Il risultato sarà il seguente:

Come possiamo notare, nel corpo dell'exploit vengono mostrate le credenziali per poter accedere a metasploitable. Consideriamo quindi l'exploit eseguito con successo.