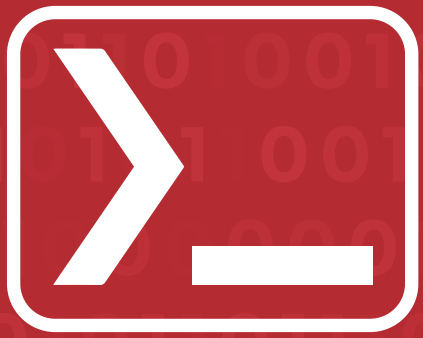




IMPACKET EXEC COMMANDS

CHEAT SHEET

ATEXEC.PY

atexec.py domain/username:password@[hostname | IP] command

- Requires a command to execute; shell not available
- Creates and subsequently deletes a **Scheduled Task** with a random 8-character mixed-case alpha string
- Runs cmd.exe with arguments of "/C" followed by the command specified by the user, followed by "C:\Windows\Temp\xxxxxxx.tmp 2>&1"
- Where "xxxxxxx" is the SAME random 8-character mixed-case alpha string used for the Scheduled Task name
- Subsequently deletes the .tmp file containing command output from C:\Windows\Temp
- NOT detected and blocked by Windows Defender by default

Windows Event Log Residue:

- **Two rounds of:**
 - Event ID 4776 in Security on target (for user specified in command)
 - Event ID 4672 in Security on target (for user specified in command)
 - Event ID 4624 Type 3 in Security on target (for user specified in command)
- [IF ENABLED] Event ID 4698 in Security on target
- Event ID 186, 325, 129, 180, 280, 118, 141, 111, 201, 102 in Microsoft-Windows-TaskScheduler/Operational on target
- [IF ENABLED] Event ID 4688 in Security on target:
 - svchost.exe → cmd.exe /C command > C:\Windows\Temp\xxxxxxx.tmp 2>&1
- [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- [IF ENABLED] Event ID 4699 in Security on target
- [IF ENABLED AND EXTERNAL BINARY IS CALLED] Event ID 4688 in Security on target:
 - cmd.exe → xxx.exe (the command specified via atexec.py)
- **Two rounds of:**
 - Event ID 4634 Type 3 in Security on target (for user specified in command)
- [IF EXTERNAL BINARY IS CALLED, 201/102 MAY APPEAR LATER] Event ID 201, 102 in Microsoft-Windows-TaskScheduler/Operational on target

PSEXEC.PY

psexec.py domain/username:password@[hostname | IP] command

- Can specify a command to run, or leave blank for shell
- PSEXEC like functionality example using RemComSvc
- Creates and subsequently deletes a **Windows Service** with a random 4-character mixed-case alpha name referencing an 8-character mixed-case alpha .exe file in %systemroot%
- Detected and blocked by Windows Defender by default

Windows Event Log Residue:

- Event ID 4776 in Security on target (for user specified in command)
- Event ID 4672 in Security on target (for user specified in command)
- Event ID 4624 Type 3 in Security on target (for user specified in command)
- Event ID 7045 in System on target (service installation: 4-character mixed-case alpha name referencing an 8-character mixed-case alpha .exe file):
 - %systemroot%\xxxxxxx.exe
- Event ID 7036 in System on target
- Event ID 7036 in System on target
- [IF ENABLED] Event ID 4688 in Security on target:
 - services.exe → C:\Windows\xxxxxxx.exe
- Event ID 4776 in Security on target (for user specified in command)
- Event ID 4672 in Security on target (for user specified in command)
- Event ID 4624 Type 3 in Security on target (for user specified in command)
- Event ID 4776 in Security on target (for user specified in command)
- Event ID 4672 in Security on target (for user specified in command)
- Event ID 4624 Type 3 in Security on target (for user specified in command)
- Event ID 4776 in Security on target (for user specified in command)
- Event ID 4672 in Security on target (for user specified in command)
- Event ID 4624 Type 3 in Security on target (for user specified in command)
- [IF ENABLED] Event ID 4688 in Security on target:
 - C:\Windows\xxxxxxx.exe → command
- [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- ... numerous other 4624, 4634, 4672 events

WMIEXEC.PY

wmiexec.py domain/username:password@[hostname | IP] command

- Can specify a command to run, or leave blank for shell
- Executes a semi-interactive shell using Windows Management Instrumentation
- Uses **UNIX Epoch Time** in commands
- NOT detected and blocked by Windows Defender by default

Windows Event Log Residue:

- **Multiple rounds of:**
 - Event ID 4776 in Security on target (for user specified in command)
 - Event ID 4672 in Security on target (for user specified in command)
 - Event ID 4624 Type 3 in Security on target (for user specified in command)
- **Always present:**
 - [IF ENABLED] Event ID 4688 in Security on target:
 - wmiprvse.exe → cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN\$__ssssssssss.sssssss 2>&1
 - (where "s" is the UNIX Epoch Time at which the command ran)
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- [IF ENABLED] Event ID 4688 in Security on target:
 - wmiprvse.exe → cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$__ssssssssss.sssssss 2>&1
- [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- [IF ENABLED] Event ID 4688 in Security on target:
 - wmiprvse.exe → cmd.exe /Q /c command 1> \\127.0.0.1\ADMIN\$__ssssssssss.sssssss 2>&1
- [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- Event ID 4634 Type 3 in Security on target (for user specified in command)
- [MAY BE PRESENT] Event ID 5857/5858 in Microsoft-Windows-WMI-Activity/Operational on target

DCOMEXEC.PY

dcomexec.py -object [ShellWindows | ShellBrowserWindow | MMC20] domain/username:password@[hostname | IP] command

- Can specify a command to run, or leave blank for shell
- Executes a semi-interactive shell using DCOM objects
- Must specify 'ShellWindows', 'ShellBrowserWindow', 'MMC20' via the -object parameter
- Uses first 5 digits of **UNIX Epoch Time** in commands
- NOT detected and blocked by Windows Defender by default

Windows Event Log Residue:

- **Two rounds of:**
 - Event ID 4776 in Security on target (for user specified in command)
 - Event ID 4672 in Security on target (for user specified in command)
 - Event ID 4624 Type 3 in Security on target (for user specified in command)
- [IF ENABLED] Event ID 4688 in Security on target:
 - svchost.exe → mmc.exe -Embedding
- Event ID 4776 in Security on target (for user specified in command)
- Event ID 4672 in Security on target (for user specified in command)
- Event ID 4624 Type 3 in Security on target (for user specified in command)
- **Always present:**
 - [IF ENABLED] Event ID 4688 in Security on target:
 - mmc.exe → cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN\$__sssss 2>&1
 - (where "s" is the first 5 digits of the UNIX Epoch Time at which the command ran)
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
 - [IF ENABLED] Event ID 4688 in Security on target:
 - mmc.exe → cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$__sssss 2>&1
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- **User specified commands:**
 - [IF ENABLED] Event ID 4688 in Security on target:
 - mmc.exe → cmd.exe /Q /c command 1> \\127.0.0.1\ADMIN\$__sssss 2>&1
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- **Two rounds of:**
 - Event ID 4634 Type 3 in Security on target (for user specified in command)

SMBEXEC.PY

smbexec.py domain/username:password@[hostname | IP]

- No option to specify a command to run; you only get shell
- Creates and subsequently deletes a **Windows Service** named "BTOBTO" referencing execute.bat for EVERY command entered into the shell
 - In May of 2023, the default service name of "BTOBTO" for smbexec.py was replaced with a random 8-character mixed-case alpha string
- Detected and blocked by Windows Defender by default

Windows Event Log Residue:

- Event ID 4776 in Security on target (for user specified in command)
- Event ID 4672 in Security on target (for user specified in command)
- Event ID 4624 Type 3 in Security on target (for user specified in command)
- Event ID 7045 in System on target (service installation: "BTOBTO" or random 8-character mixed-case alpha string for the default service name, but can be changed to custom value):
 - %COMSPEC% /Q /c echo cd ^> \\127.0.0.1\C\$__output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
- **Always present:**
 - [IF ENABLED] Event ID 4688 in Security on target:
 - services.exe → cmd.exe /Q /c echo cd ^> \\127.0.0.1\C\$__output 2^>^&1 > C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → cmd.exe /Q /c C:\Windows\TEMP\execute.bat
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- **Present if commands are issued in lieu of an interactive shell:**
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe /Q /c echo command ^> \\127.0.0.1\C\$__output 2^>^&1 > C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → cmd.exe /Q /c C:\Windows\TEMP\execute.bat
 - [IF ENABLED] Event ID 4688 in Security on target:
 - cmd.exe → conhost.exe 0xffffffff -ForceV1
- **If interactive shell is used, when shell exits:**
 - Event ID 4634 Type 3 in Security on target (for user specified in command)

