Professional information security and training service

REDTEAM
HACKER ACADEMY
www.redteamacademy.com

Joystick
Penetration Test Report

RED TEAM HACK ACADEMY

October 05th, 2023

Submitted by : **Abin cv**

Submitted to : **Sneha**

Table of Contents

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 JOYSTCK 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. Unfortunatly 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).

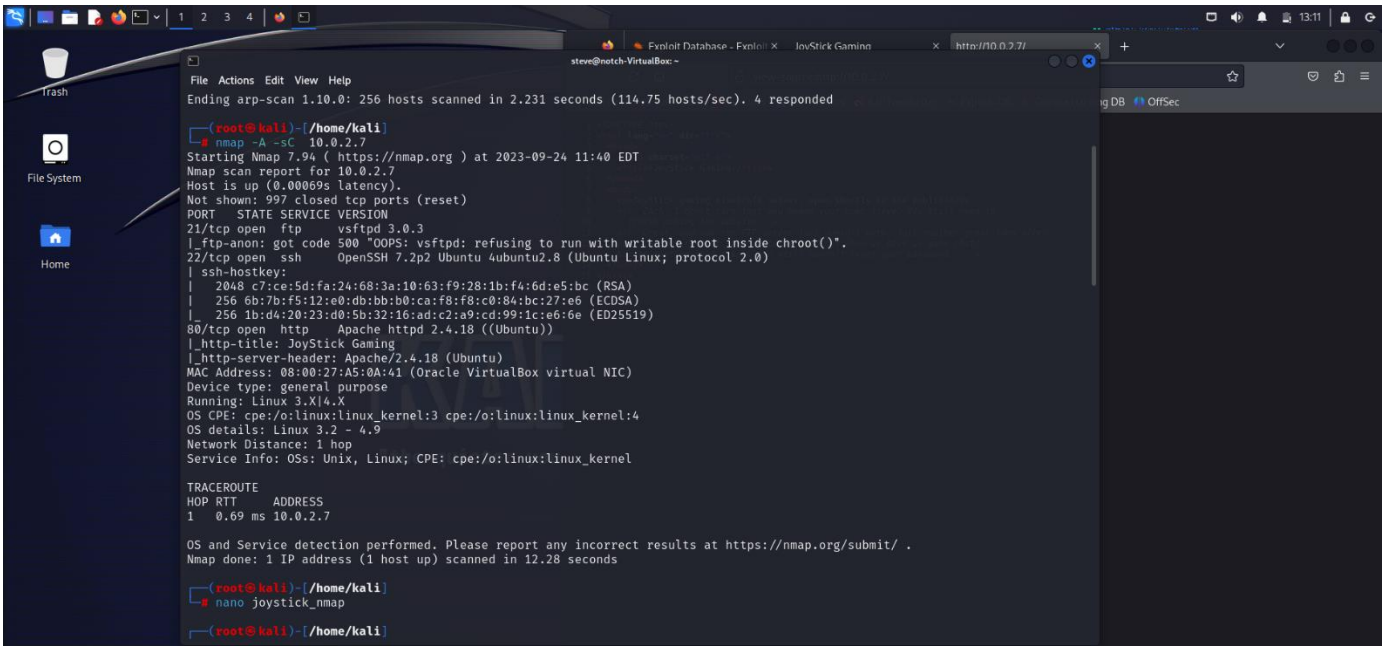

Figure 1 – Information gathering to reveals active name ports

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”

Open port 80

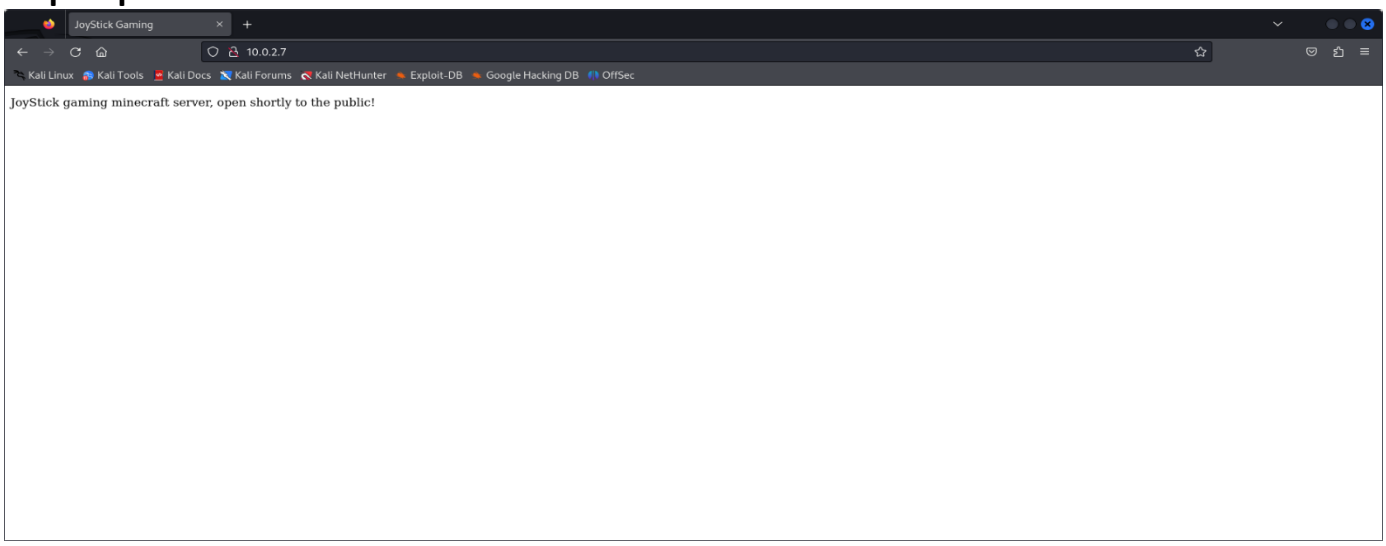

Figure 2 – Open port 80 web page

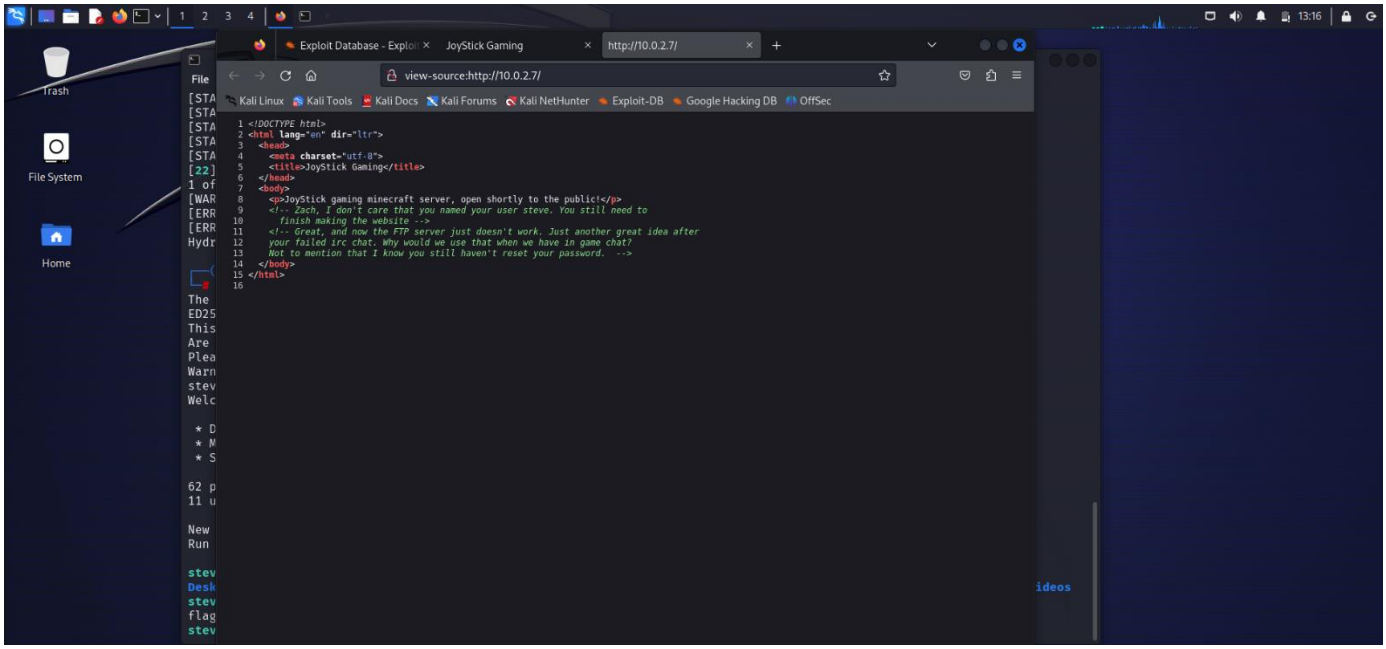

Figure 3 – Open port 80 web page sourcecode

From figure 3 , we can 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

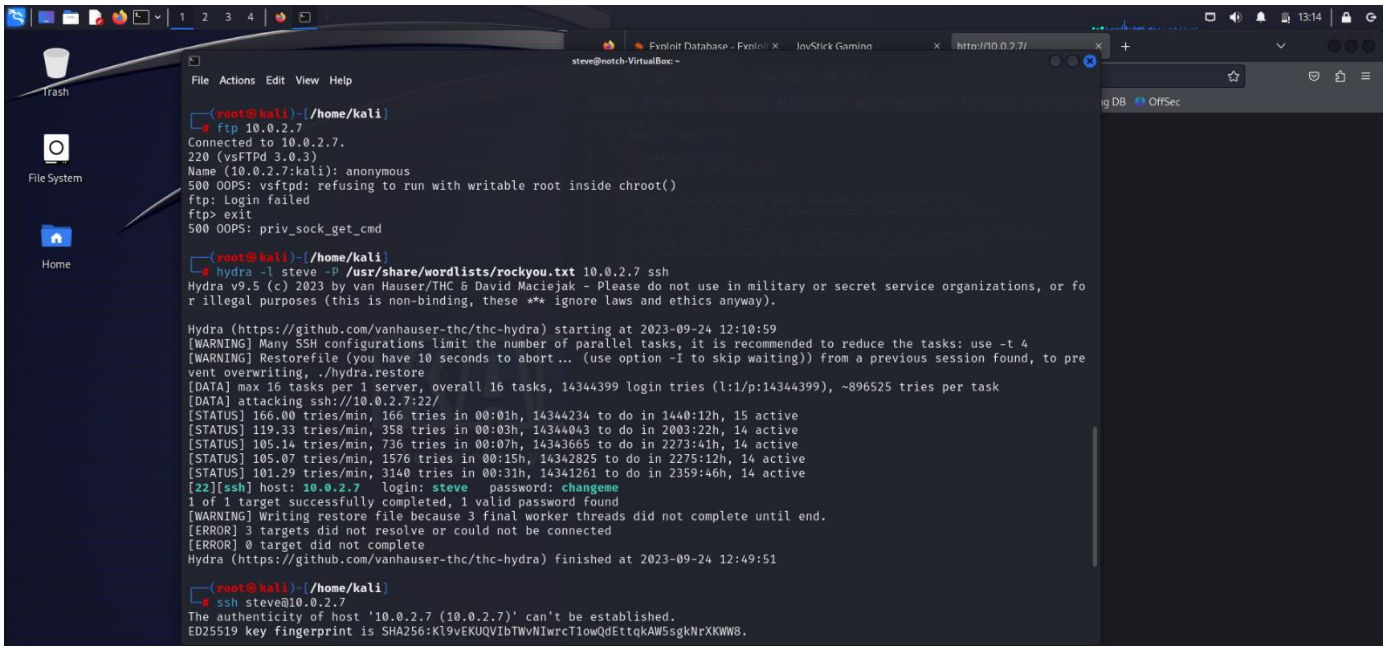

Figure 4 – hydra bruteforce

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

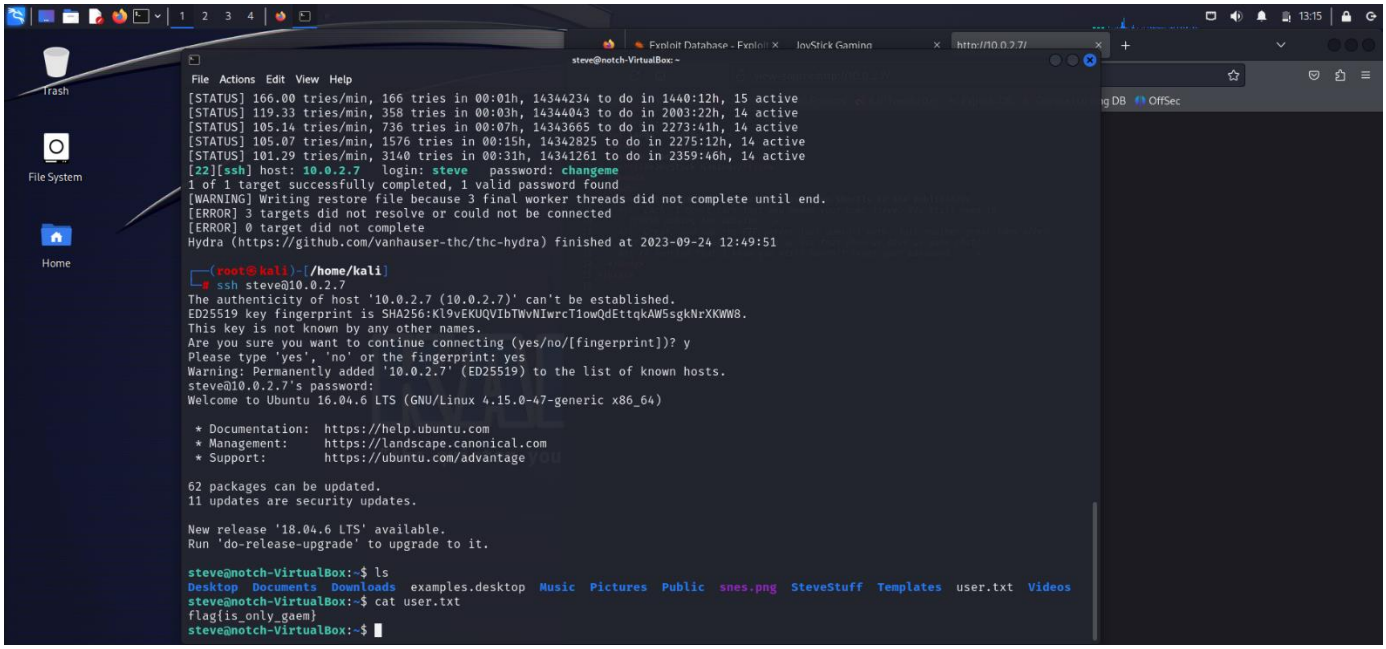

Figure -5 SSH login

I successfully logined 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 kernal has overlayfs vulnerability.

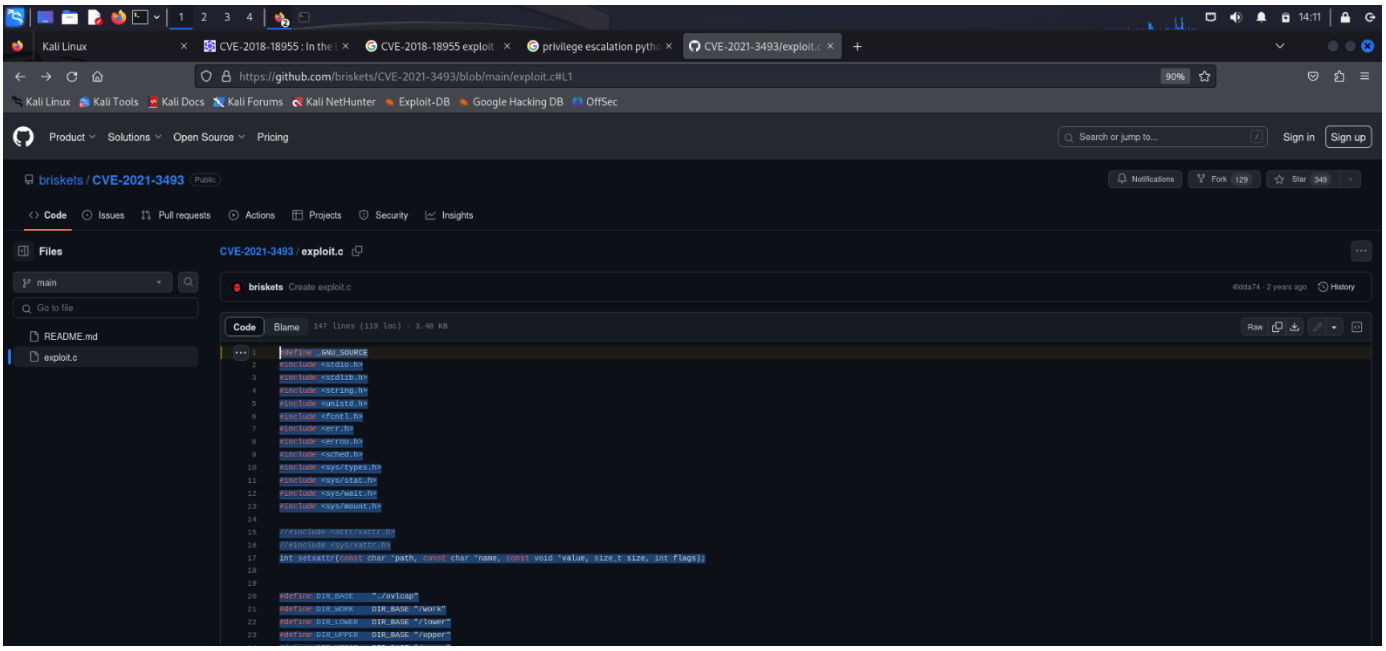

Figure –6 exploit from github

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

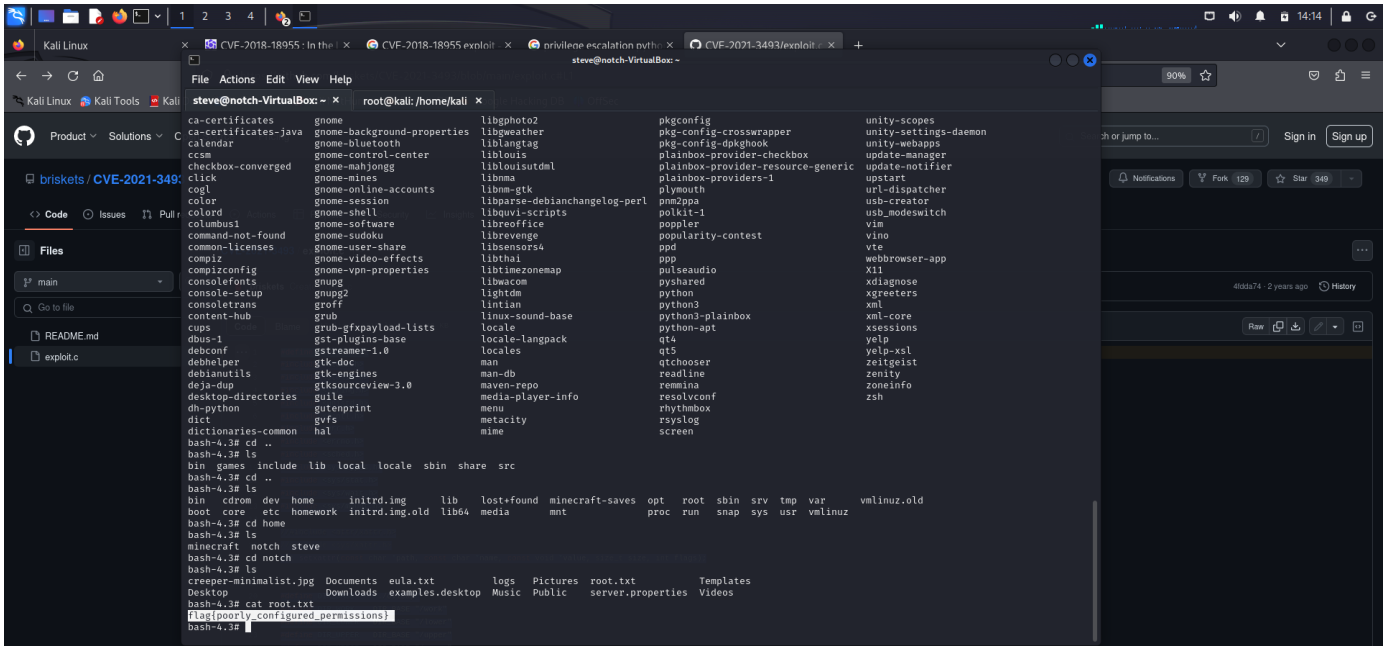

Figure 8 –root flag captured

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 monst 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 o be one and only choice for end-to-end cybersecurity training among security aspirants and organizations and contribute towards minimizing cyber theats and crimes .