KUMASI TECHNICAL UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE

GitHub Repo: https://github.com/Neting1/automated-security-audit-GROUP_9

NAME	INDEX	ROLE
Oduro Thompson	052441360132	Research and work on the sysadmin and audit to our local cloud (week week 4 and 5)
Johnson Asante	052443070030	Research and work on the scripting (week 6)
Akunah Benjamin	052441360307	Research and work on the sync report to our local cloud (week 7)
Hededzi Dovene Nancy	052441360185	Work on the screenshot from all the works and combine it on Microsoft word. Our group administrator.

PROJECT WORK

SUBJECT: Build a script to perform a daily security audit, logs results, and run as a system service.

Step-by-Step Instructions

Project Setup

Create a project directory:

- mkdir -p ~/myproject/{scripts,docs}
- cd ~/myproject

Write the Audit Script (`security_audit.sh`)

Navigate to the `scripts` folder and create the script:

- cd ~/myproject/scripts
- nano security_audit.sh

Paste the following code (customize as needed):

```
#!/bin/bash
 # Define output file
 REPORT=~/myproject/docs/audit_report.txt
 echo "Daily Security Audit Report - $(date)" > $REPORT

 # Check open ports
 echo -e "\n==== OPEN PORTS ====" >> $REPORT
 ss -tuln >> $REPORT

 # Analyze failed logins
 echo -e "\n==== FAILED LOGINS ====" >> $REPORT
 grep "Failed password" /var/log/auth.log | tail -n 10 >> $REPORT

 # Review user permissions (non-system users)
 echo -e "\n==== USER PERMISSIONS ====" >> $REPORT
 awk -F: '($3 >= 1000) {print $1}' /etc/passwd | xargs -I {} ls -ld /home/{} >> $REPORT
```

echo "Audit completed. Report saved to $REPORT."

Make the script executable:

- chmod +x security_audit.sh

Create a Systemd Service

Create a service file:

- sudo nano /etc/systemd/system/security-audit.service

Add this configuration:

[Unit]

Description=Daily Security Audit

After=network.target

[Service]

Type=oneshot

ExecStart=/home/$USER/myproject/scripts/security_audit.sh

User=$USER

Create a timer to run daily:

- sudo nano /etc/systemd/system/security-audit.timer

[Unit]

Description=Run security audit daily

[Timer]

OnCalendar=daily

Persistent=true

[Install]

WantedBy=timers.target

Enable and start the timer:

- sudo systemctl daemon-reload
- sudo systemctl enable security-audit.timer
- sudo systemctl start security-audit.timer

Test the Setup

Manually run the script to verify:

- ./security_audit.sh
- cat ~/myproject/docs/audit_report.txt

Check the service status:

- sudo systemctl status security-audit

Documentation (`project_readme.md`)

Create a README in the `docs` folder:

- cd ~/myproject/docs
- nano project_readme.md

Include:

Markdown

Automated Security Audit Tool

Purpose: Daily checks for open ports, failed logins, and user permissions.

Usage

Script: ./security_audit.sh

Service: Runs daily via systemd timer.

Output

Reports saved to `audit_report.txt`.

Sync Reports to Cloud

Use `rsync` to upload reports to a droplet (replace placeholders):

rsync -az ~/myproject/docs/ user@your-droplet-ip:/path/to/remote/folder

Submission

Take screenshots of:

i. sudo systemctl status security-audit`
ii. cat ~/myproject/docs/audit_report.txt`

Push to GitHub (if required):

- git init
- git add .
- git commit -m "Automated Security Audit Tool"
- git remote add origin https://github.com/your-username/repo-name.git
- git push -u origin main

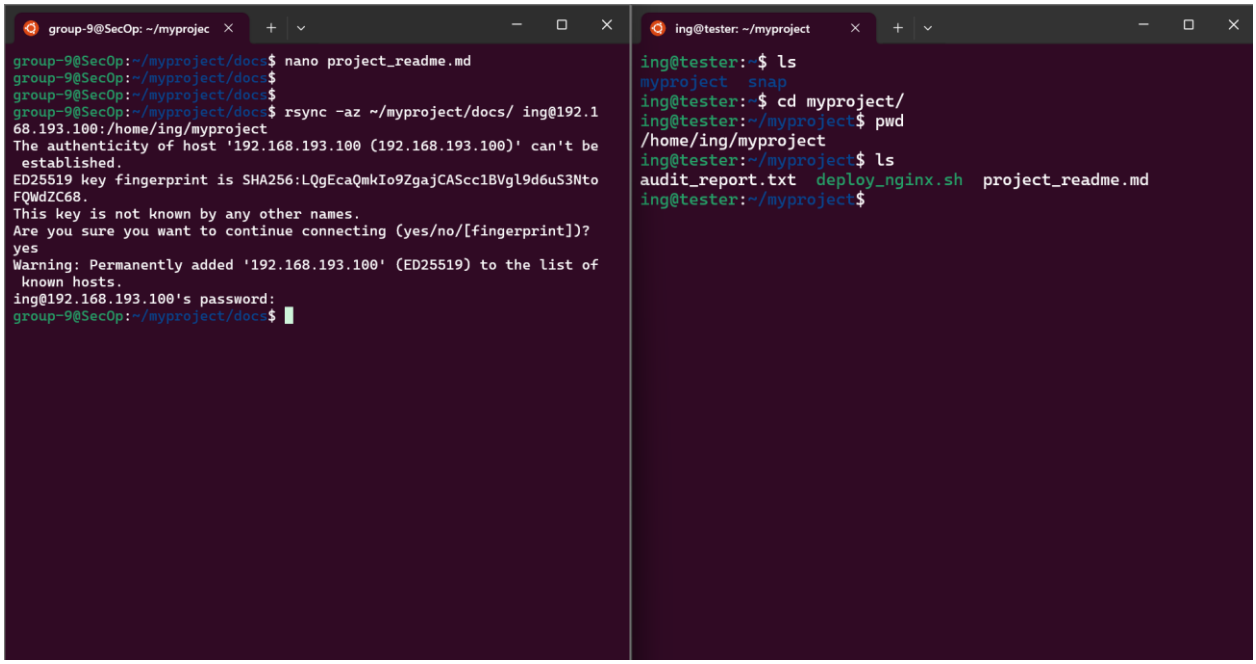
Group Tasks:

I. Split roles (scripting, systemd setup, documentation).
II. Test on multiple systems (Ubuntu/Ubuntu Server).
III. Present findings in class.

```
group-9@SecOp:~$ cat ~/myproject/docs/audit_report.txt
Daily Security Audit Report - Thu Aug 14 09:44:24 UTC 2025

==== OPEN PORTS ====
Netid State  Recv-Q Send-Q      Local Address:Port  Peer Address:PortProcess
udp   UNCONN 0      3584   172.17.0.1%docker0:27962      0.0.0.0:*
udp   UNCONN 0      0      192.168.93.26%eth0:27962      0.0.0.0:*
udp   UNCONN 0      0            127.0.0.54:53           0.0.0.0:*
udp   UNCONN 0      0         127.0.0.53%lo:53           0.0.0.0:*
udp   UNCONN 0      0         10.255.255.254:53          0.0.0.0:*
udp   UNCONN 0      0             127.0.0.1:323          0.0.0.0:*
udp   UNCONN 0      3584   172.17.0.1%docker0:25767      0.0.0.0:*
udp   UNCONN 0      0      192.168.93.26%eth0:25767      0.0.0.0:*
udp   UNCONN 0      3584   172.17.0.1%docker0:9993       0.0.0.0:*
udp   UNCONN 0      0      192.168.93.26%eth0:9993       0.0.0.0:*
udp   UNCONN 0      0                 [::1]:323             [::]:*
tcp   LISTEN 0      4096          127.0.0.54:53           0.0.0.0:*
tcp   LISTEN 0      4096           127.0.0.1:39451        0.0.0.0:*
tcp   LISTEN 0      5              0.0.0.0:9993           0.0.0.0:*
tcp   LISTEN 0      4096       127.0.0.53%lo:53           0.0.0.0:*
tcp   LISTEN 0      4096           0.0.0.0:22             0.0.0.0:*
tcp   LISTEN 0      100            127.0.0.1:25           0.0.0.0:*
tcp   LISTEN 0      1000      10.255.255.254:53           0.0.0.0:*
tcp   LISTEN 0      5                    *:9993                 *:*
tcp   LISTEN 0      4096              [::]:22                [::]:*
tcp   LISTEN 0      100              [::1]:25                [::]:*

==== FAILED LOGINS ====

==== USER PERMISSIONS ====
drwxr-x--- 11 oduro oduro 4096 Aug 13 12:59 /home/oduro
drwxr-x--- 9 okocha okocha 4096 Aug 12 18:40 /home/okocha
drwxr-x--- 2 protecteduser protecteduser 4096 Aug 13 12:11 /home/protecteduser
drwxr-x--- 5 group-9 group-9 4096 Aug 14 09:42 /home/group-9
group-9@SecOp:~$
```

```
group-9@SecOp:~$ sudo systemctl status security-audit
○ security-audit.service - Daily Security Audit
     Loaded: loaded (/etc/systemd/system/security-audit.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: ● security-audit.timer
group-9@SecOp:~$
```

```
group-9@SecOp: ~/myprojec
  GNU nano 7.2                                  project_readme.md *
# Automated Security Audit Tool
**Purpose**: Daily checks for open ports, failed logins, and user permissions.

## Usage
1. Script: `./security_audit.sh`
2. Service: Runs daily via systemd timer.

## Output
Reports saved to `audit_report.txt`.

## Group Members Name
Group 9 Project Assignment Members

1.Oduro Thompson - 052441360132
2.Johnson Asante - 052443070030
3.Akunah Benjamin _052441360307
4.Hededzi Dovene Nancy -052441360185

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was
```


group-9@SecOp: ~/myprojec
group-9@SecOp:~/myproject/docs$ nano project_readme.md
group-9@SecOp:~/myproject/docs$
group-9@SecOp:~/myproject/docs$
group-9@SecOp:~/myproject/docs$ rsync -az ~/myproject/docs/ ing@192.168.193.100:/home/ing/myproject
The authenticity of host '192.168.193.100 (192.168.193.100)' can't be established.
ED25519 key fingerprint is SHA256:LQgEcaQmkIo9ZgajCAScc1BVgl9d6uS3NtoFQWdZC68.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added '192.168.193.100' (ED25519) to the list of known hosts.
ing@192.168.193.100's password:
group-9@SecOp:~/myproject/docs$
ing@tester: ~/myproject
ing@tester:~$ ls
myproject snap
ing@tester:~$ cd myproject/
ing@tester:~/myproject$ pwd
/home/ing/myproject
ing@tester:~/myproject$ ls
audit_report.txt deploy_nginx.sh project_readme.md
ing@tester:~/myproject$