Team -1 Project Report

Problem Statement

The project involves creating scripts to automate the installation of specific security tools and running scans on a target IP address. The main tasks are:

1. **Installation Script (install_main.sh)**:
    - **Purpose**: To install necessary security tools (like figlet, postfix, nikto, rustscan, and feroxbuster) if they are not already installed on the system.
    - **Process**:
        - Checks if each tool is installed.
        - If not, installs the tool.
        - Sets the correct permissions for the tools.
        - Prints confirmation messages to indicate the progress and completion of the installation.
2. **Scan Script (script_scan.sh)**:
    - **Purpose**: To perform a security scan on a given IP address, detect open ports, and send an email with the scan results.
    - **Process**:
        - Takes an IP address as input.
        - Runs RustScan on the IP address to find open ports.
        - If port 80 (HTTP) is open, runs Feroxbuster to discover directories.
        - Saves the results in a file called results.txt.
        - Prompts the user for an email address and sends the results to this email.

Summary

We are automating the setup and use of security tools to scan a target IP address and report the findings. One script installs the tools, while the other runs the scans and sends the results via email. The scripts ensure that tools are installed if needed, perform scans, and alert the user with the results.

Tools Integrated and Their Functionalities

1. **Figlet**
   - **Function**: Generates stylized text banners in the terminal.
   - **Usage in Script**: Used to display the project title and completion messages in a visually appealing way.
2. **Postfix**
   - **Function**: Mail transfer agent used for sending emails.
   - **Usage in Script**: Essential for sending the scan results to the specified email address.
3. **Rustscan**
   - **Function**: Fast port scanner designed to quickly identify open ports on a target.
   - **Usage in Script**: Scans the target IP address to find open ports, specifically checks if port 80 is open.
4. **Feroxbuster**
   - **Function**: Directory brute-forcing tool that scans for hidden directories and files on a web server.
   - **Usage in Script**: If port 80 is found open by Rustscan, Feroxbuster is used to find directories and files on the target web server.
5. **sendemail**
   - **Function**: Lightweight command-line email client.
   - **Usage in Script**: Sends the scan results via email to the user-provided email address.

Description

- **Figlet**: Makes text look cool in the terminal.
- **Postfix**: Sends emails.
- **Rustscan**: Quickly finds open doors (ports) on a computer.
- **Feroxbuster**: Looks for hidden folders on websites.
- **sendemail**: Sends emails from the command line.

These tools are used to set up and perform security scans on an IP address, find vulnerabilities, and send the results to your email.

REPORT

Summary: Our goal was to thoroughly evaluate the security of the Cloudfront server (server-108-139-182-67.gru3.r.cloudfront.net) to identify and mitigate potential vulnerabilities. This report provides a detailed overview of our findings, recommendations, and steps for enhancing the server's overall security.

Objective: The objective of this assessment is to conduct a comprehensive analysis of the server's security vulnerabilities, evaluate its current security posture, and provide actionable recommendations to enhance its security. Our aim is to ensure the server's protection against potential cyber threats.

Scope: Our assessment primarily focused on analyzing open ports and potential vulnerabilities that could pose security risks to the server. We also reviewed the server's WHOIS information and conducted a vulnerability scan to identify any potential security weaknesses.

Key Findings: We identified several critical findings during our assessment, including the presence of open ports FTP (21/tcp), RTSP (554/tcp), and PPTP (1723/tcp). These open ports represent significant security risks and could potentially be exploited by malicious actors to gain unauthorized access to the server.

Overall Security Posture: Based on our findings, the overall security posture of the server is considered to be at risk. The presence of open ports and potential vulnerabilities could compromise the confidentiality, integrity, and availability of the server's data and services.

Methodology: Our audit approach utilized a combination of automated tools and manual analysis. We utilized Nmap for port scanning and vulnerability scanning, supplemented by manual analysis for detailed findings. The process included scanning the server, analyzing the results, and documenting the findings.

Target: DNS records for server-108-139-182-67.gru3.r.cloudfront.net

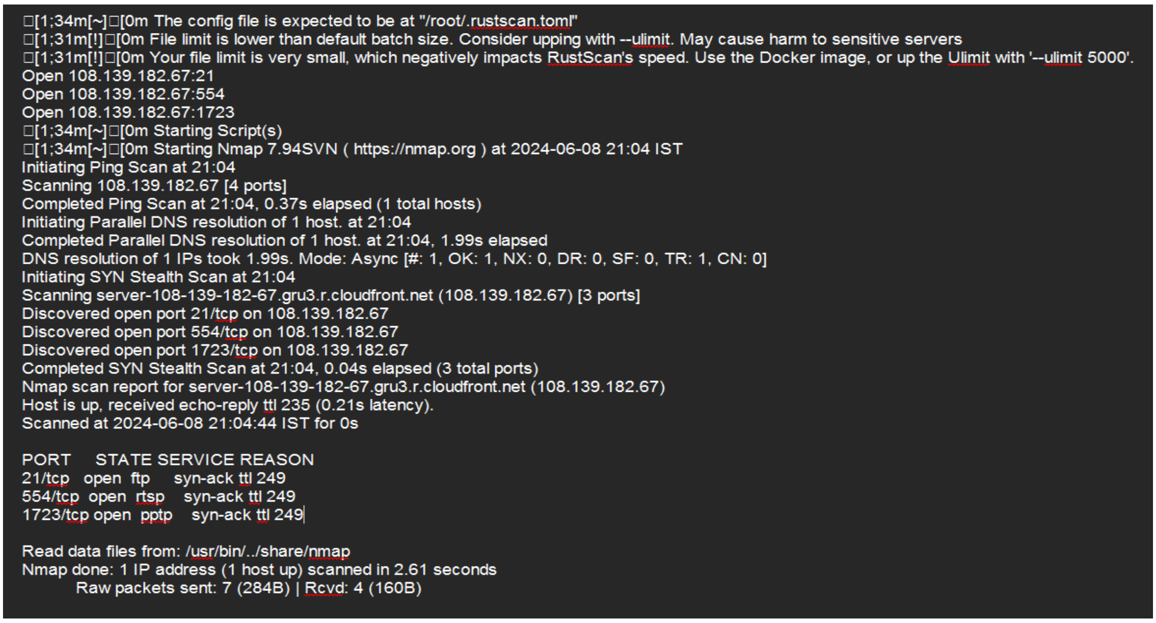
Testing Findings:

Description	Location	Impact	Evidence	Severity Rating
Open FTP Port (21/tcp)	server-108-139-182-67.gru3.r.cloudfront.net	Potential unauthorized file access	Nmap scan results	High
Open RTSP Port (554/tcp)	server-108-139-182-67.gru3.r.cloudfront.net	Potential unauthorized media access	Nmap scan results	High
Open PPTP Port (1723/tcp)	server-108-139-182-67.gru3.r.cloudfront.net	Potential VPN protocol vulnerability	Nmap scan results	High

Technical Details:

- **Subdomains Analysis:** No subdomains were identified during the assessment.
- **Port Scanning:** Nmap scan results revealed open ports FTP (21/tcp), RTSP (554/tcp), and PPTP (1723/tcp).
- **Vulnerability Scanning:** Vulnerability scanning revealed potential vulnerabilities associated with the open ports.

Screenshots:



```
□[1;34m[~]□[0m The config file is expected to be at "/root/.rustscan.toml"
□[1;31m[!]□[0m File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
□[1;31m[!]□[0m Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 108.139.182.67:21
Open 108.139.182.67:554
Open 108.139.182.67:1723
□[1;34m[~]□[0m Starting Script(s)
□[1;34m[~]□[0m Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-08 21:04 IST
Initiating Ping Scan at 21:04
Scanning 108.139.182.67 [4 ports]
Completed Ping Scan at 21:04, 0.37s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:04
Completed Parallel DNS resolution of 1 host. at 21:04, 1.99s elapsed
DNS resolution of 1 IPs took 1.99s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 21:04
Scanning server-108-139-182-67.gru3.r.cloudfront.net (108.139.182.67) [3 ports]
Discovered open port 21/tcp on 108.139.182.67
Discovered open port 554/tcp on 108.139.182.67
Discovered open port 1723/tcp on 108.139.182.67
Completed SYN Stealth Scan at 21:04, 0.04s elapsed (3 total ports)
Nmap scan report for server-108-139-182-67.gru3.r.cloudfront.net (108.139.182.67)
Host is up, received echo-reply ttl 235 (0.21s latency).
Scanned at 2024-06-08 21:04:44 IST for 0s

PORT     STATE SERVICE REASON
21/tcp   open  ftp     syn-ack ttl 249
554/tcp  open  rtsp    syn-ack ttl 249
1723/tcp open  pptp    syn-ack ttl 249

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds
           Raw packets sent: 7 (284B) | Rcvd: 4 (160B)
```

Recommendations:

- **Close Unused Ports:** Close all unused ports to reduce the attack surface.
- **Implement Access Control:** Implement strict access controls and authentication mechanisms.
- **Enable Encryption:** Use encryption protocols such as SSL/TLS to secure data in transit.
- **Regular Security Updates:** Keep the server's software and applications up to date.
- **Monitor and Log Activities:** Implement monitoring and logging mechanisms to detect and respond to suspicious activities.

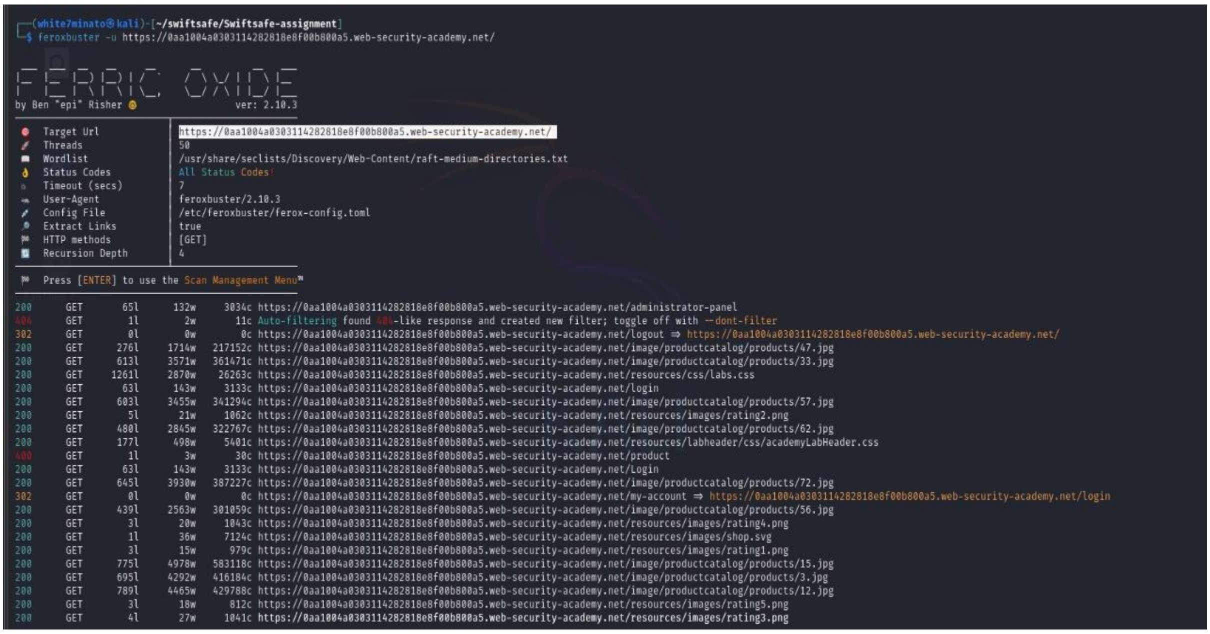
Conclusion: In conclusion, the vulnerability assessment of the Cloudfront server identified significant security vulnerabilities that require immediate attention. By implementing the recommended measures, the server's security posture can be significantly enhanced, protecting it against potential cyber threats.

Note: It is crucial to address these vulnerabilities promptly to ensure the security and integrity of your server. We recommend implementing the recommended measures as soon as possible to mitigate the risks identified in this assessment.

Feroxbuster Scan Results:

Target: https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/

Screenshots:



```
┌──(white7minato㉿kali)-[~/swiftsafe/Swiftsafe-assignment]
└─$ feroxbuster -u https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.10.3
───────────────────────────┬──────────────────────
     Target Url            │ https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/
     Threads               │ 50
     Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
     Status Codes          │ All Status Codes!
     Timeout (secs)        │ 7
     User-Agent            │ feroxbuster/2.10.3
     Config File           │ /etc/feroxbuster/ferox-config.toml
     Extract Links         │ true
     HTTP methods          │ [GET]
     Recursion Depth       │ 4
───────────────────────────┴──────────────────────
     Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET       65l      132w     3034c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/administrator-panel
404      GET        1l        2w       11c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
302      GET        0l        0w        0c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/logout ⇒ https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/
200      GET      276l     1714w   217152c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/47.jpg
200      GET      613l     3571w   361471c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/33.jpg
200      GET     1261l     2870w    26263c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/css/labs.css
200      GET       63l      143w     3133c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/login
200      GET      603l     3455w   341294c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/57.jpg
200      GET        5l       21w     1062c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/images/rating2.png
200      GET      480l     2845w   322767c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/62.jpg
200      GET      177l      498w     5401c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/labheader/css/academyLabHeader.css
400      GET        1l        3w       30c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/product
200      GET       63l      143w     3133c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/Login
200      GET      645l     3930w   387227c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/72.jpg
302      GET        0l        0w        0c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/my-account ⇒ https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/login
200      GET      439l     2563w   301059c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/56.jpg
200      GET        3l       20w     1043c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/images/rating4.png
200      GET        1l       36w     7124c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/images/shop.svg
200      GET        3l       15w      979c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/images/rating1.png
200      GET      775l     4978w   583118c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/15.jpg
200      GET      695l     4292w   416184c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/3.jpg
200      GET      789l     4465w   429788c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/image/productcatalog/products/12.jpg
200      GET        3l       18w      812c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/images/rating5.png
200      GET        4l       27w     1041c https://0aa1004a0303114282818e8f00b800a5.web-security-academy.net/resources/images/rating3.png
```

Scan Findings: A vulnerability has been identified during the website scan, indicating that it's possible to delete users from the users database.

Technical Details:

- **Scan Method:** Feroxbuster was used to scan the URLs.
- **Status Codes:** Various status codes were encountered, including 200 (OK), 301 (Moved Permanently), 403 (Forbidden), and 404 (Not Found).

Recommendations:

- **Regular Monitoring:** Continue regular monitoring and update practices to maintain security.
- **Patch Management:** Apply patches promptly to address any newly discovered vulnerabilities.

Conclusion: The website scan has revealed a vulnerability, suggesting that the deletion of users from the database is feasible.

Note: This report is based on the scan results at the time of assessment and may not reflect the current security status of the URLs.