國立成功大學 111 學年度 第二學期 計算機系統管理
National Cheng Kung University
Computer System Administration 2023 Spring

Final Exam - Setup, Fix and Found

# Description

1. Date: 2023-06-15 (Thu.) 13:00~16:00 (UTC+8)
2. Operating system: FreeBSD 13.1-RELEASE
3. Open book exam. Online search and ChatGPT is allowed but the **DISCUSSION IS NOT ALLOWED.**
4. Online Judge: https://sa.imslab.org
5. TA's email: nasa@imslab.org
6. Total: 100 points.

# Goals

1. Configure the SSH service.
2. Create a shell script to generate users with specific rules.
3. Repair the ZFS disks and locate a specific file within them.
4. Identify a malicious process and terminate it.
5. Resolve the hostname (Do not require to setup any DNS server).
6. Construct the web server and perform the necessary configuration.
7. Establish firewall rules for enhanced security.
8. Setup the NFS server & client.

# Before you start...

- **DO NOT ATTACK JUDGE SYSTEM OTHERWISE YOU WILL FAIL THIS COURSE!!!**
- Make sure everything is fine after reboot.
- While TAs can assist with VM rollback, please note that each instance of this action will incur a **3-POINT DEDUCTION** from your final exam score.
- The username and the password for the VM are the same as those used for your online judge.
- Please **AVOID connecting WireGuard to your VM** as it may disrupt the judge's functionality.
- The `<username>` represents your judge's username.
- All instructions below must be done in the VM we provided.

# Tasks & Requirements

General

- Modify the timezone to UTC+8 (a.k.a. CST Central Standard Time).
    - Make sure you update your time by `sudo ntpdate clock.stdtime.gov.tw` after changing the timezone.
- Update the hostname to `<username>`.
- Generate a user account called `judge` that fulfills the specified criteria.
    - Set the user password to `m30owme0w`.
    - Configure the default shell to be Bash.
    - Enable password-less use of the `sudo` command for the user.
    - Ensure the user can login using the SSH keys we provided. You can obtain the SSH key from https://sa.imslab.org/pubkey.
- You are tasked with modifying the SSH configuration file(s) on your machine to comply with the following rules.
    - Only allow user login with private keys, prohibiting password-based authentication.
    - Restrict SSH access by disallowing root login.
    - Modify the SSH port to use port `2222`.

Shell Scripts

- You are asked to create 50 users in your machine with the following rules.
    - Usernames follow the pattern `sa_xx` where `xx` ranges from 00 to 49.
    - Passwords follow the pattern `sa_xx` where `xx` ranges from 49 to 00.
    - Check username. For even-numbered users, set the default shell to `/bin/sh`; for odd-numbered users, set the default shell to `/bin/tcsh`.
    - For example the `sa_00` user has the password `sa_49` the it's shell will be `/bin/sh` since the `00` is an even number.
- To create 50 users in batches, you have flexibility in choosing the method that best suits your needs, including but not limited to using shell scripting, manual creation, programming languages, or any other suitable approach.

ZFS

- On your machine, there is a ZFS partition named `sa_pool/sa_final` with a RAID1 array. But it has been corrupted using the command `dd if=/dev/urandom of=/dev/da1 bs=512M` by a hacker. Please use the appropriate ZFS command to **import the partition and repair it** until the sa_pool state is back to `ONLINE`.
- Fortunately, the ZFS is so powerful in the RAID1 that a single disk corruption will not prevent the ZFS contents from being accessed.
  - Use the ZFS or BSD built-in commands to locate a file named `zfsflag.txt` in the `sa_pool/sa_final` ZFS partition. This file should have the text prefix `douwant2buildasn0wman`. Upon discovery, please copy the file to the judge's home directory and rename it as `zfsflag.txt`. Please note that the partition contains `ONLY ONE CORRECT` flag file. If either the file name or prefix is incorrect, the flag itself will be considered incorrect.

Web Client

- To simplify access to the web service provided at IP address `10.187.10.1`, please configure your machine to associate the hostname `sa-judge.meow` with this IP address.

Web Server

- You are assuming the use of Nginx for this task. However, feel free to explore other web servers as long as they can effectively accomplish tasks.
- Set up a load balancing server to distribute traffic for the provided sites (`http://facebook.sa` and `http://google.sa`).
  - Create a host configuration specifically for the `<username>.ncku` domain.
  - Implement the round-robin strategy to distribute incoming traffic evenly between the two specified sites.
  - Assuming your configuration is correct, refreshing the page for `<username>.ncku` should display different content each time.
- Enable SSL compatibility.
  - Download `finalsacertbot` from Judge to acquire your CA certificate and key.
  - Sign your web certificate using the provided CA certificate and key.
- Establish a 301 redirection rule to automatically redirect all incoming HTTP traffic to HTTPS.

Malicious Processes

- Your machine is being burdened by malicious processes that are utilizing CPU resources. Please take steps to identify and eradicate these processes.
  - However, please note that the malware reappears upon rebooting the BSD. Therefore, if you can completely remove the malicious processes, you will earn extra points. To ensure complete removal, you can verify by rebooting your FreeBSD system and confirming that the malicious process no longer reappears.
- Hint: 🌽tab

Firewall

- Allow all loopback and outgoing traffic.
- Restrict incoming traffic access to ICMP, SSH, NFS, and Web only.
- You should create a whitelist dedicated to your SSH and NFS services.
  - Allow `10.187.0.0/23` and `10.187.112.0/20` to access your SSH service.
  - Allow `10.187.0.0/23` to access your NFS service.
  - Deny other IPs traffic when they try to connect those two services.
- You should create a blacklist dedicated to your Nginx services.
  - Apply IP blocking to prevent access from IPs `10.187.10.5` and `10.187.0.253` to all of your web hosts.

NFS Server

- Connect the NFS we provided in `nfs.sa:/flagplace` and copy the script `getflag.sh` to your machine.
  - use `./getflag.sh <username>` to generate a file name `flag`.
- Setup a NFS server with following requirements.
  - Create and share the `/data/shared/` directory.
  - Allow the read/write permission to `10.187.1.0/24` only.
  - Allow the read to all IPs.
  - Copy the `flag` file generated by the script into the `/data/shared` folder.

# Grading

Tasks	Dependency	Testing Commands	Score
General (25%)			
1-a. SSH port is correct and the judge user allows login with the provided key.			5
1-b. Set the judge user to use the sudo command password-less.	1-a		5
1-c. Set judge user's password.	1-b		5
1-d. Change the hostname.	1-a	hostname	2
1-e. Set the correct time zone.	1-a	date	2
1-f. Set judge user's default shell to bash.	1-a	getent passwd	2
1-g. SSH key authentication only.	1-c	sshpass -p m30owme0w ssh -o PubkeyAuthentication=no -o PreferredAuthentications=keyboard-interactive,password -p 2222 judge@<vm ip> whoami	2
1-h. Deny root login from SSH.	1-b	ssh -p 2222 root@<vm ip> whoami	2
Shell Scripts (10%)			
2-a. All users' usernames are correct.	1-a	getent passwd	4
2-b. All users' passwords are correct.	1-b, 2-a		2
2-c. All users' shells are correct.	1-a, 2-a	getent passwd	4
ZFS (10%)			

3-a. Health check.	1-a	`sudo zpool list -Ho name,health sa_pool`
		`# sa_pool ONLINE`
			5

3-b. Check the flag file is correct.	1-a.	cat /home/judge/zfsflag.txt	5
Web Client (5%)			
4-a. Access the website with sa-judge.meow.	1-a	curl sa-judge.meow	5
Web Server (20%)			
5-a. Web server is configured without errors.		`curl --connect-timeout 1 -s -k -L http://<username>.ncku`	8
5-b. Setup HTTPS redirection rules.		`curl --connect-timeout 1 -s -w "%{redirect_url}" -o /dev/null http://<username>.ncku`	2

5-c. Check HTTPS is valid and the Intermediate certificate’s CN is your username.		`python3 -c "import requests; print(requests.get('https://<username>.ncku').text)"`
		`echo | openssl s_client -connect <username>.ncku:443 2>&1 1>/dev/null`
			5

5-d. Setup the load balance server.		`curl --connect-timeout 1 -s -k -L http://<username>.ncku`	5
Malicious Processes (5%)			
6-a. Malicious processes are killed.	1-a		3
6-b. Malicious processes wont start on boot.	1-b		2
Firewall (15%)			

7-a. Allow all loopback and outgoing traffic.	1-a	`ping <some ip>`
		`curl <some url>`
			3

7-b. Only allow incoming traffic access to the ICMP, SSH, NFS and Web.	1-b		3
7-c. Allow 10.187.0.0/23 and 10.187.112.0/20 to access your SSH service.	1-a	ssh -p 2222 judge@<vm ip> whoami	3
7-d. Allow 10.187.0.0/23 to access your NFS service.	8-a	mount_nfs <username>.ncku:/data/shared /mnt	3
7-e. Prevent access from IPs 10.187.10.5 and 10.187.0.253 to all of your web hosts.	5-a	curl --connect-timeout 1 -s -k -L http://<username>.ncku	3
NFS Server (10%)			
8-a. Check the flag is correct.	1-b	mount_nfs <username>.ncku:/data/shared /mnt cat /mnt/flag	6
8-b. Allow read/write permissions to 10.187.1.0/24.	8-a	mount_nfs <username>.ncku:/data/shared /mnt echo aaa > /mnt/<some file>	2
8-c. Allow read permission to all IPs.	8-a	mount_nfs <username>.ncku:/data/shared /mnt cat /mnt/flag echo aaa > /mnt/<some file>	2
Total			**100**

# Recommended Steps

We suggest that you can follow the steps below to complete tasks, as it will make it easier for the exam.

1. General
2. Shell Scripts
3. Web Client
4. ZFS
5. Web Server or NFS
6. Malicious Processes
7. Firewall

# Useful Resources

- CatGPT (cat-gpt.com)
- TCP/IP addressing and subnetting - Windows Client | Microsoft Learn
- FreeBSD Handbook | FreeBSD Documentation Portal
- HTTP Load Balancing | NGINX Documentation
- Network File System (NFS) | Ubuntu
- Resolving ZFS File System Problems
- OpenBSD PF: User's Guide
- SSH config file syntax and how-tos for configuring the OpenSSH client
- OpenVPN/easy-rsa: easy-rsa - Simple shell based CA utility (github.com)