SWE3009: Internet Service and Computer Security

Exploit Writing Tutorial Series: Automation

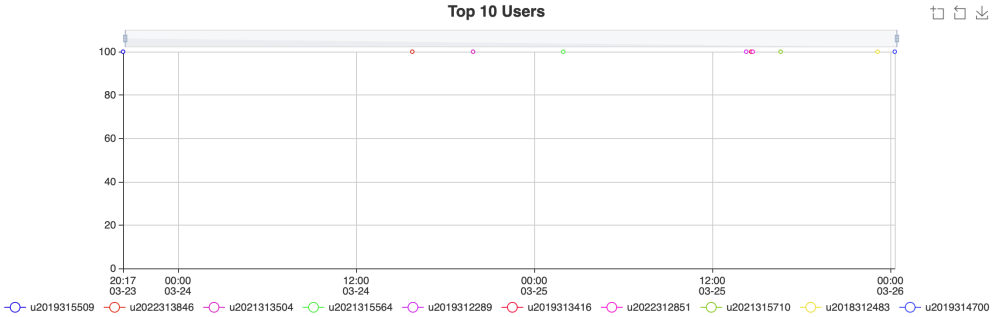
Hojoon Lee

Systems Security Lab @ SKKU

Systems Security Lab

SUNGKYUNKWAN UNIVERSITY 1398 성균관대학교

The Scoreboard



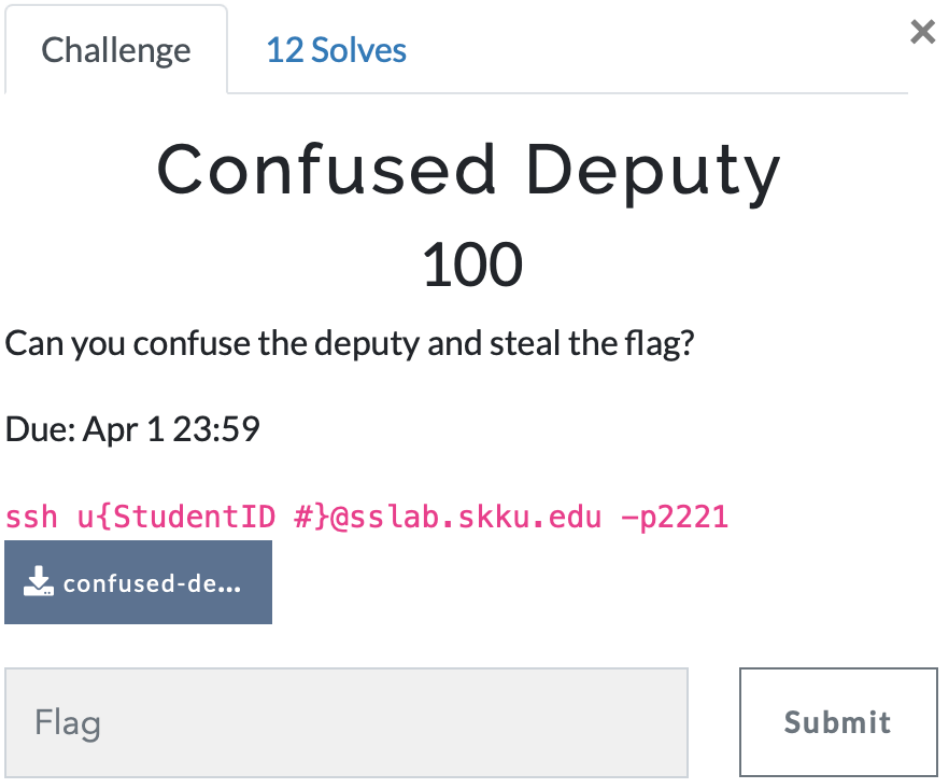
Place	User	Score
1	u2019315509	100
2	u2022313846	100
3	u2021313504	100
4	u2021315564	100
5	u2019312289	100
6	u2019313416	100
7	u2022312851	100
8	u2021315710	100
9	u2018312483	100
10	u2019314700	100
11	u2019312755	100
12	u2020312576	100

Systems Security Lab

SUNGKYUNKWAN UNIVERSITY 1398 성균관대학교

Q: I want to analyze the binary locally:

A:



Q: I cannot log in to the server

A:

- Password is the same as ID
  - E.g., 202312345 / 202312345
- ctf.skku.edu password is not the same as server ssh password

Getting VPN/Proxy

2.3 Getting around university's firewall

As of 2023, the university has tightened up the firewall policy, and you *cannot* directly connect to our servers. There are two known ways to get a connection to the university network. 1. You can request a VPN account and then install the VPN software (https://vpninfo.skku.edu). 2. If you can get an account at https://skkuoverflow.com/ko/posts/school/inuiyeji/, you can use that account as a proxy to our CTF server.

You can set the ProxyJump server as an argument to the `ssh` command as the following:

```
$ ssh -J ¡jump server¿ ¡remote server¿
```

Or more conveniently, you can edit your ssh config your (`~/.ssh/config`)

```
Host sslab-ctf
  HostName sslab.skku.edu
  User u202312345
  Port 2221
  # Your Proxy Server
  ProxyJump user@¡jumpserver¿
```

Systems Security Lab

SUNGKYUNKWAN UNIVERSITY 1398 성균관대학교

Workflows (e.g., SCP)

- Read SSLab-CTF-Guide

Confused Deputy: Hints

- Hint 1: How are passwords stored?
  - Hash algorithms are known, you can compute them
    - $ echo “Hello” | sha256sum
    - 5891b5b522d5df086d0ff0b110fbd9d21bb4fc7163af34d08286a2e846f6be03
- Hint 2: Weakness of ACLs + SETUID
- Hint 3: Reverse engineering is not really necessary

SSLab CTF Framework

SSLAB 취약점 보고 : Arbitrary Code Execute

[redacted]

- A student whose name shall remain anonymous (I haven't got his/her consent yet)
- Reported a few possibly abusable security loopholes in our CTF framework
- We will not reveal the loopholes at this point to prevent abusing
- But the student gets +10 points in his lab1 assignment (but not above 100)

SSLab CTF Framework

- Open Design Principle
  - Hiding your security mechanism does not help you
  - Security mechanism should still be secure when its design is fully open
- Kerckhoff's principle of cryptography
  - A cryptosystem should be secure if everything about the system (except the key) is public knowledge

SSLab CTF Framework