
گزارش تمرین لینوکس

سناریو:

راه اندازی + SSH اجازه به چند یوزر از یک آدرس مشخص.

مراحل کلی (خلاصه):

۱. نصب و فعال سازی OpenSSH server
۲. ایجاد کاربران و تنظیم (password-based) auth
۳. محدود کردن دسترسی SSH برای کاربران مشخص و/یا از IP خاص با sshd_config
۴. (اختیاری/تکمیلی) اعمال قاعده فایروال برای اجازه فقط به IP خاص

مراحل انجام شده

نصب OpenSSH و ایجاد کاربران

ابتدا سرویس openssh-server بر روی اوبونتو نصب و فعال سازی گردید. سپس، دو کاربر مورد نیاز سناریو با نام های samin-sh و sina-sh با موفقیت ایجاد و برای آن ها رمز عبور تعیین شد.

```
sudo adduser samin-sh
```

```
sudo adduser sina-sh
```

پیکربندی فایروال (UFW)

برای افزایش امنیت و پیاده‌سازی بخش اختیاری سناریو، فایروال UFW فعال‌سازی شد. قانونی وضع گردید که به موجب آن، تنها ترافیک ورودی به پورت 22 (پورت ssh) از آدرس IP عمومی کاربر مجاز باشد. آدرس IP عمومی با ابزارهای آنلاین شناسایی و در قانون زیر استفاده شد.

```
sudo ufw allow from 5.74.234.124 to any port 22
```

```
sudo ufw enable
```

پیکربندی نهایی سرویس SSH

فایل اصلی پیکربندی سرویس SSH در مسیر `/etc/ssh/sshd_config` به منظور اعمال محدودیت‌های دسترسی ویرایش شد. تنظیمات زیر برای فعال‌سازی ورود با رمز عبور و محدود کردن کاربران و آدرس‌های IP مجاز، اعمال گردید. این پیکربندی به گونه‌ای تنظیم شد که اتصال هم از آدرس IP عمومی (5.74.234.124) و هم از آدرس IP داخلی میزبان (192.168.112.1) WSL امکان‌پذیر باشد.

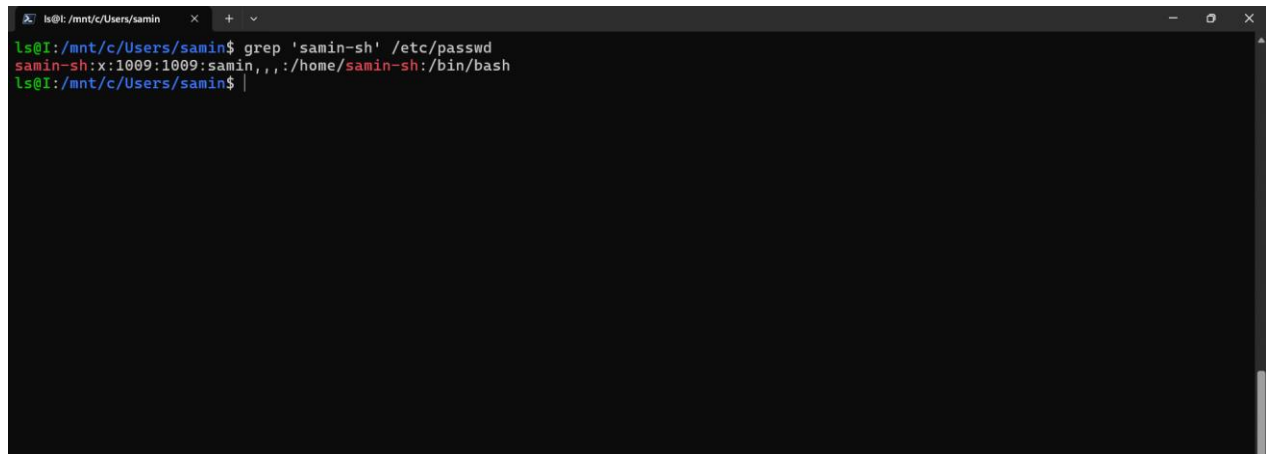
```
PasswordAuthentication yes
```

```
ChallengeResponseAuthentication no
```

```
AllowUsers samin-sh@5.74.234.124 sina-sh@5.74.234.124 samin-  
sh@192.168.112.1 sina-sh@192.168.112.1
```

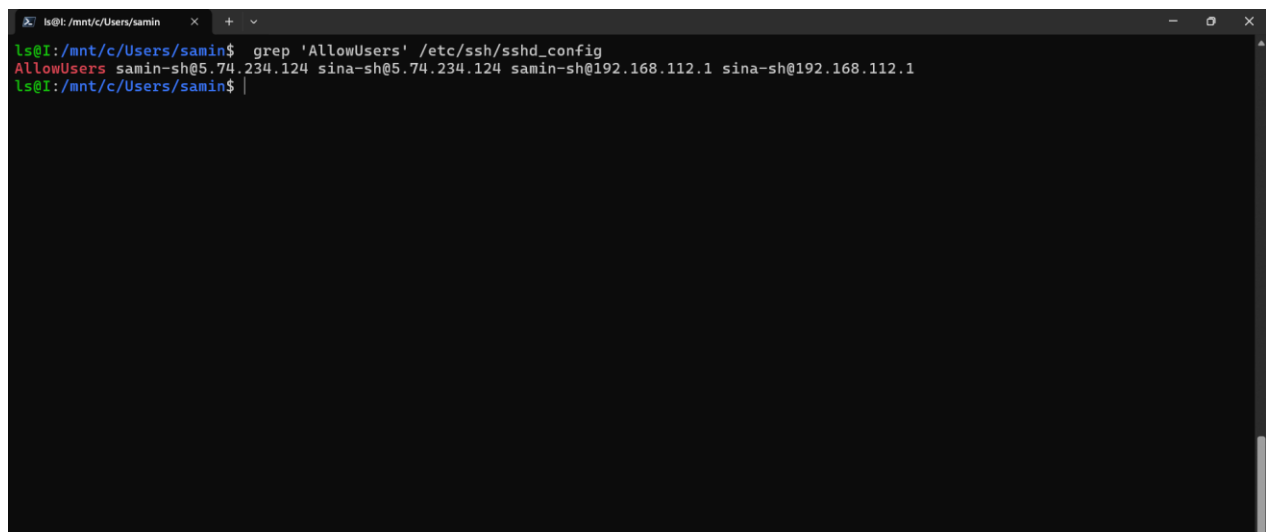
پس از ذخیره تغییرات، سرویس SSH با دستور `sudo systemctl restart ssh` مجدداً راه‌اندازی شد.

نتیجه نهایی و اثبات عملکرد



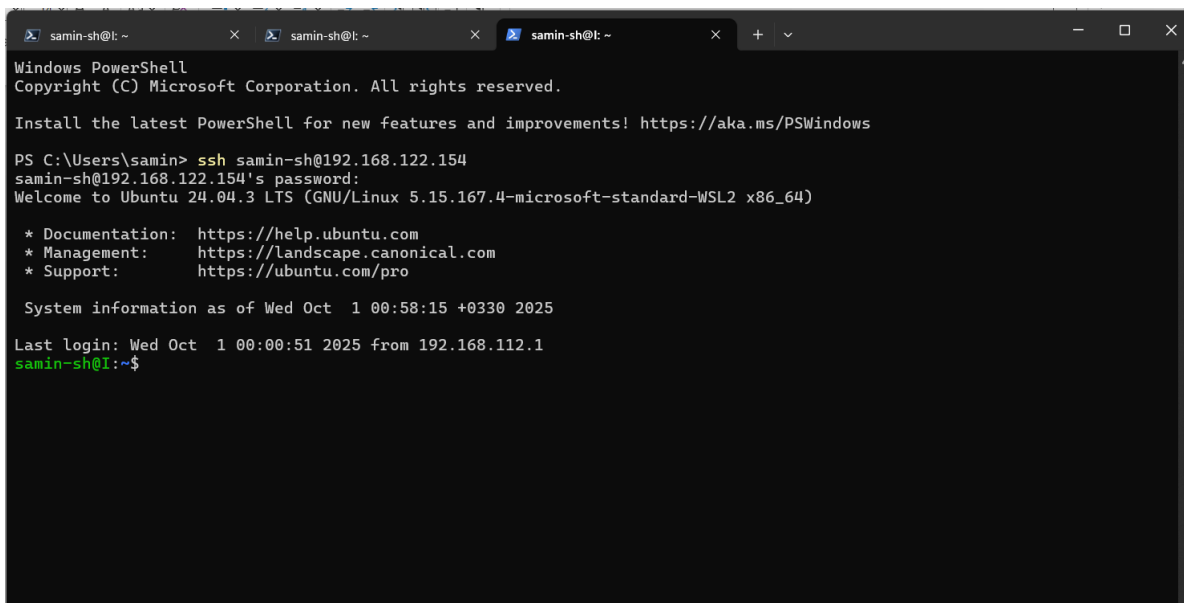
```
ls@I: /mnt/c/Users/samin$ grep 'samin-sh' /etc/passwd
samin-sh:x:1009:1009:samin,,,:/home/samin-sh:/bin/bash
ls@I: /mnt/c/Users/samin$
```

شکل ۱: تأیید ایجاد موفقیت‌آمیز کاربر samin-sh با نمایش اطلاعات آن در فایل `/etc/passwd` سیستم.



```
ls@I: /mnt/c/Users/samin$ grep 'AllowUsers' /etc/ssh/sshd_config
AllowUsers samin-sh@5.74.234.124 sina-sh@5.74.234.124 samin-sh@192.168.112.1 sina-sh@192.168.112.1
ls@I: /mnt/c/Users/samin$
```

شکل ۲: نمایش قانون کلیدی `AllowUsers` در فایل `sshd_config` که دسترسی SSH را به کاربران و IP های تعریف شده در سناریو محدود می‌کند.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

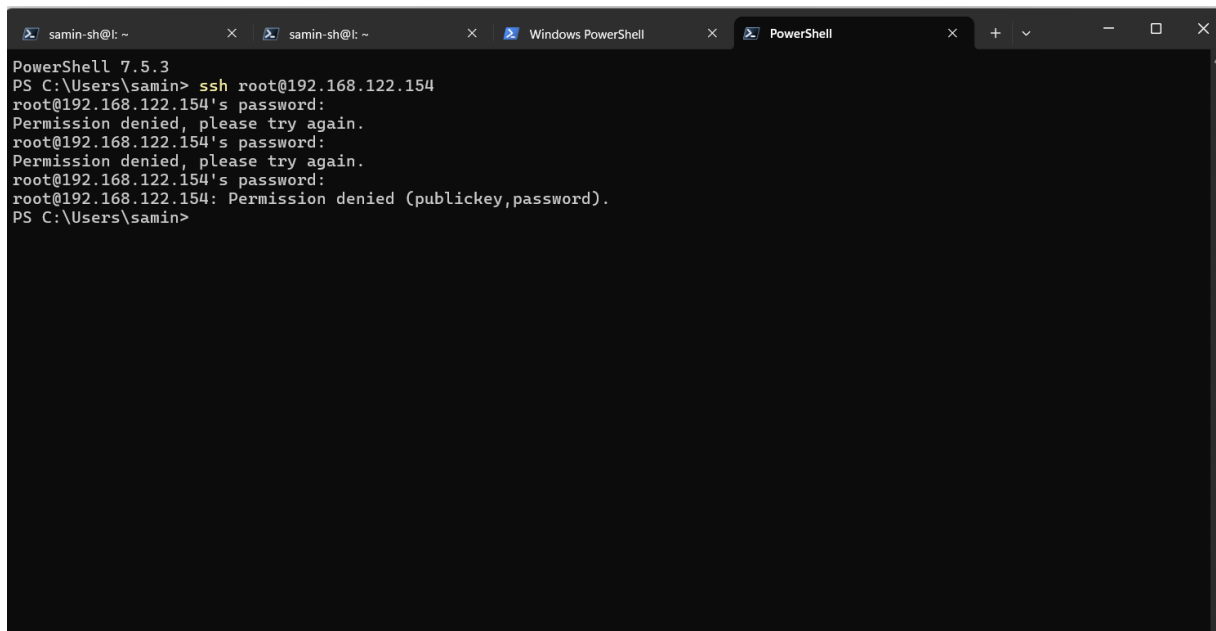
PS C:\Users\samin> ssh samin-sh@192.168.122.154
samin-sh@192.168.122.154's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 5.15.167.4-microsoft-standard-WSL2 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Oct  1 00:58:15 +0330 2025

Last login: Wed Oct  1 00:00:51 2025 from 192.168.112.1
samin-sh@i:~$
```

شکل ۳: اثبات نهایی عملکرد صحیح سناریو ورود موفقیت‌آمیز کاربر samin-sh به سرور از طریق SSH.



```
PowerShell 7.5.3
PS C:\Users\samin> ssh root@192.168.122.154
root@192.168.122.154's password:
Permission denied, please try again.
root@192.168.122.154's password:
Permission denied, please try again.
root@192.168.122.154's password:
root@192.168.122.154: Permission denied (publickey,password).
PS C:\Users\samin>
```

شکل ۴: تست امنیتی؛ تلاش ناموفق برای ورود با کاربر غیرمجاز (root) که نشان‌دهنده عملکرد صحیح محدودیت‌های اعمال شده است.

جمع‌بندی

سناریوی امن‌سازی سرور SSH با موفقیت کامل پیاده‌سازی شد و تمام اهداف اولیه، شامل محدودسازی کاربران و آدرس‌های IP، محقق گردید.