# 检查SSH端口是否被攻击 // 检查失败登录

> SSH端口暴露在公网上很可能被黑客扫描，并尝试登入系统。这种攻击基本每天都在发生。

## 一、检查攻击来源

`btmp`文件会记录`SSH`端口登录失败的信息，包括尝试的用户名、`IP`地址和时间等信息。

`btmp`为二进制文件，文件路径为`/var/log/btmp`。

### 1. 查看文件btmp

使用命令`lastb`可以查看文件`btmp`的信息，参数`-n`可以指定显示数量。

```
lastb -n 10 | tac
```

### 2. 查看攻击者IP及攻击次数

```
lastb | awk '{ print $3}' | sort | uniq -c | sort -n
```

### 3. 查看攻击者尝试的用户名

```
lastb | awk '{ print $1}' | sort | uniq -c | sort -n
```

### 4. 分析攻击者

对攻击次数第一的`IP`进行分析。

- 查看攻击开始时间

  ```
  lastb | grep 137.184.155.125
  ```

- 查看攻击终止时间

  ```
  lastb | grep 137.184.155.125 | tac
  ```

- 查看`IP`地理位置

```
curl ipinfo.io/137.184.155.125
```

# 二、防范措施

## 1. 修改SSH端口

修改`SSH`端口可以避免广撒网式的端口扫描及后续的攻击。

- 打开文件`sshd_config`

  ```
  vim /etc/ssh/sshd_config
  ```

- 修改参数`Port`

  修改前：

  ```
  #port 22
  ```

  修改后：

  ```
  port 8500
  ```

- 重启`SSH`守护程序

  ```
  systemctl restart sshd
  ```

## 2. 设置复杂密码

设置密码为`字母+数字+符号`组合，提升暴力破解难度。