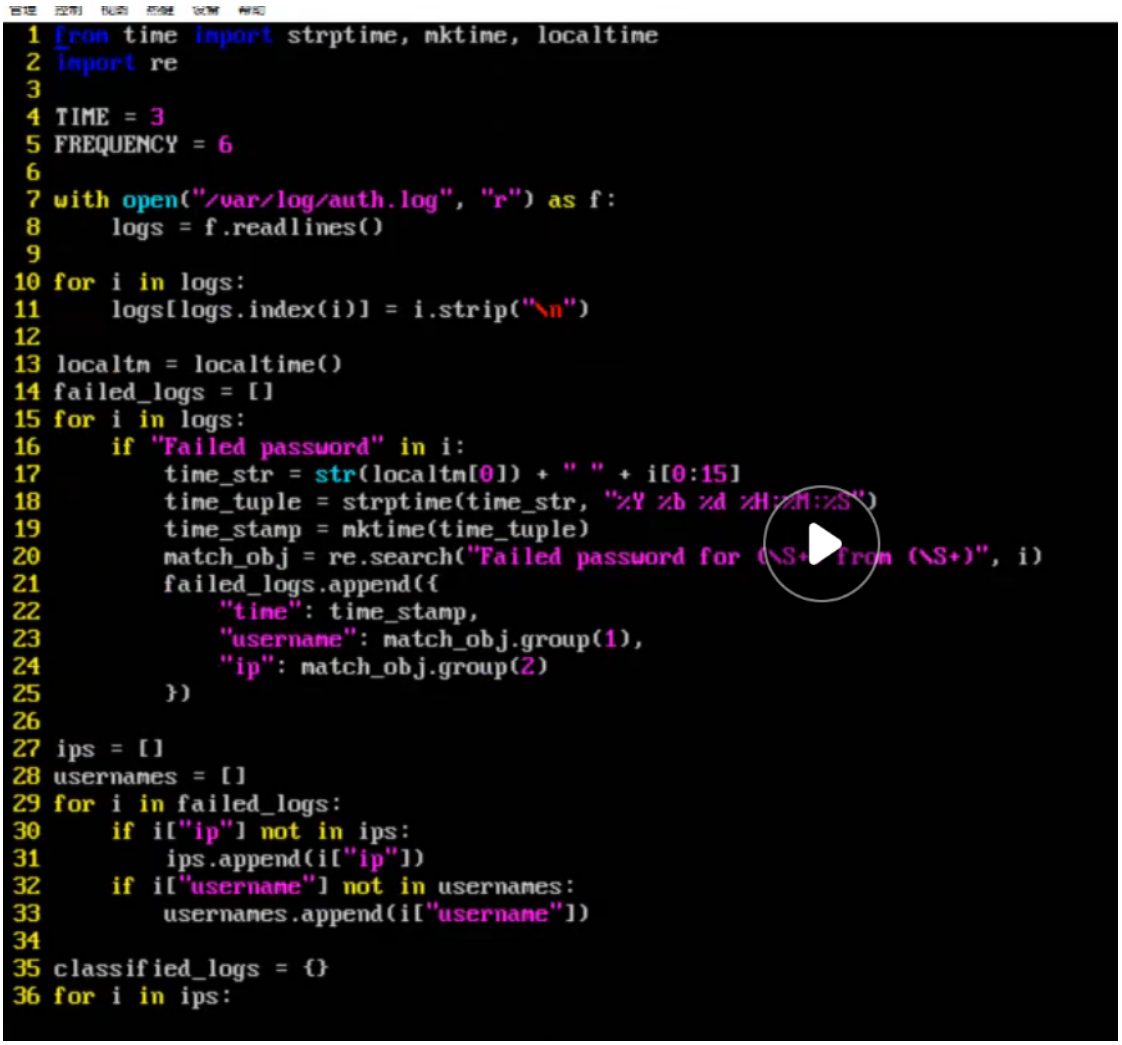
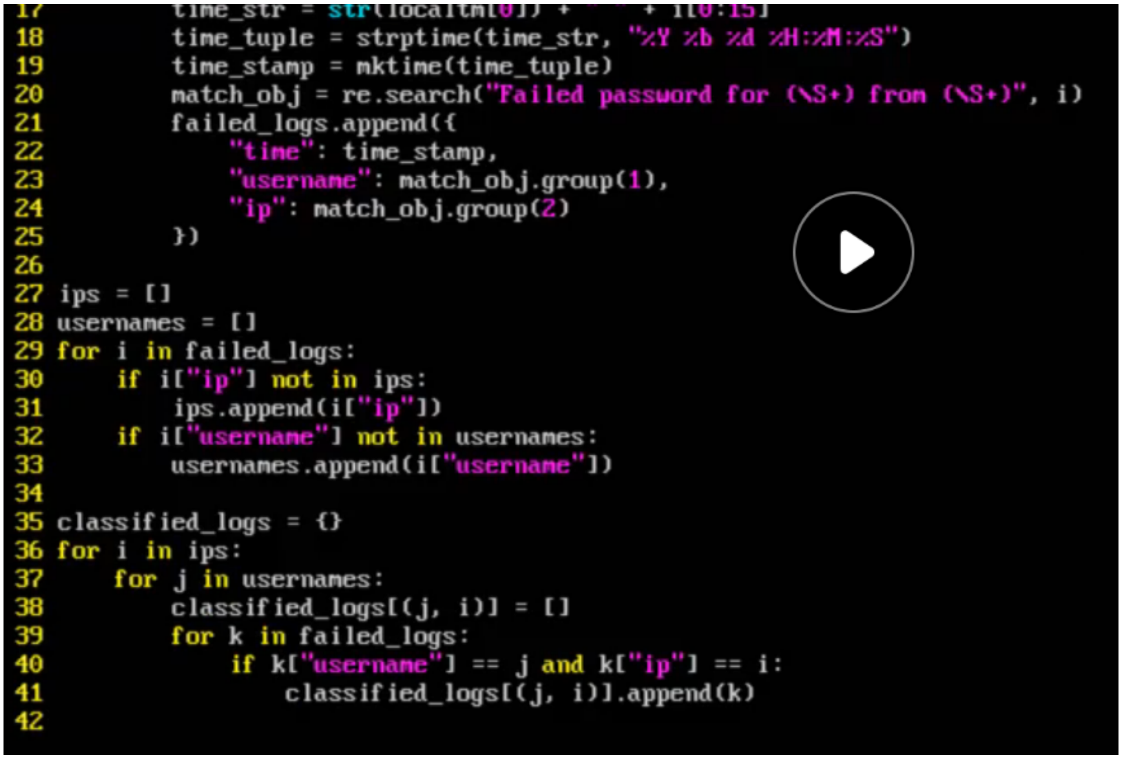
20200819信息安全实训

笔记本：	我的第一个笔记本		
创建时间：	2020/8/19 21:33	**更新时间：**	2020/8/19 21:36
作者：	820410740@qq.com		

python基础
列表 元组 for循环
生成字典 与hydra



```
from time import strptime, mktime, localtime
import re

TIME = 3
FREQUENCY = 6

with open("/var/log/auth.log", "r") as f:
    logs = f.readlines()

for i in logs:
    logs[logs.index(i)] = i.strip("\n")

localtm = localtime()
failed_logs = []
for i in logs:
    if "Failed password" in i:
        time_str = str(localtm[0]) + " " + i[0:15]
        time_tuple = strptime(time_str, "%Y %b %d %H:%M:%S")
        time_stamp = mktime(time_tuple)
        match_obj = re.search("Failed password for (\S+) from (\S+)", i)
        failed_logs.append({
            "time": time_stamp,
            "username": match_obj.group(1),
            "ip": match_obj.group(2)
        })

ips = []
usernames = []
for i in failed_logs:
    if i["ip"] not in ips:
        ips.append(i["ip"])
    if i["username"] not in usernames:
        usernames.append(i["username"])

classified_logs = {}
for i in ips:
```



```python
        time_str = str(localtm[0]) + " " + i[0:15]
        time_tuple = strptime(time_str, "%Y %b %d %H:%M:%S")
        time_stamp = mktime(time_tuple)
        match_obj = re.search("Failed password for (\S+) from (\S+)", i)
        failed_logs.append({
            "time": time_stamp,
            "username": match_obj.group(1),
            "ip": match_obj.group(2)
        })

ips = []
usernames = []
for i in failed_logs:
    if i["ip"] not in ips:
        ips.append(i["ip"])
    if i["username"] not in usernames:
        usernames.append(i["username"])

classified_logs = {}
for i in ips:
    for j in usernames:
        classified_logs[(j, i)] = []
        for k in failed_logs:
            if k["username"] == j and k["ip"] == i:
                classified_logs[(j, i)].append(k)

```