HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI THỰC HÀNH

Kiểm thử xâm nhập

Quét mạng và dịch vụ nâng cao

Giảng viên: Đinh Trường Duy

Nhóm lớp: 01

Sinh viên: Hoàng Trung Kiên

Mã sinh viên: B20DCAT098

Hà Nội – 2024

Mục lục

1. Mục đích.

Bài thực hành này sử dụng nmap và các kỹ năng đã thực hiện trong các bài lab trước để xác định và khai thác điểm yếu trong hệ thống.

Thực hiện kiểm tra bảo mật đặc biệt cho một khách hàng, họ tin rằng máy chủ SSH nội bộ của họ tương đối an toàn, nhưng lại muốn xác nhận tính hợp lệ của việc này. Mục tiêu là cố gắng truy cập từ xa vào máy chủ SSH đó và xem nội dung của một tệp đã chọn.

2. Yêu cầu.

a, Nmap, viết tắt của Network Mapper, là một công cụ mã nguồn mở miễn phí dùng để quét mạng và phát hiện lỗ hổng bảo mật. Nó hoạt động bằng cách gửi các gói tin đến các máy tính trên mạng và phân tích phản hồi để xác định các dịch vụ đang chạy, hệ điều hành và các lỗ hổng bảo mật tiềm ẩn.

Nmap có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm:

- Khám phá mạng: Nmap có thể được sử dụng để xác định tất cả các thiết bị trên mạng của bạn, bao gồm cả máy tính, máy chủ, thiết bị mạng và các thiết bị IoT.
- Quét cổng: Nmap có thể được sử dụng để xác định các cổng TCP và UDP đang mở trên một máy tính cụ thể. Điều này có thể hữu ích để xác định các dịch vụ đang chạy trên máy tính và các lỗ hổng bảo mật tiềm ẩn.
- Phát hiện hệ điều hành: Nmap có thể được sử dụng để xác định hệ điều hành đang chạy trên một máy tính cụ thể.
- Kiểm tra bảo mật: Nmap có thể được sử dụng để kiểm tra các lỗ hổng bảo mật trên mạng của bạn. Nmap có thể phát hiện các lỗ hổng phổ biến như Heartbleed, Shellshock và WannaCry.
- Lập bản đồ mạng: Nmap có thể được sử dụng để tạo bản đồ mạng của bạn, hiển thị tất cả các thiết bị và kết nối trên mạng.

b, Tshark là phiên bản dòng lệnh của Wireshark, một phần mềm phân tích giao thức mạng phổ biến. Nó cho phép bạn thực hiện nhiều tác vụ tương tự như Wireshark, nhưng với giao diện đơn giản hơn dựa trên văn bản.

Tshark là phiên bản dòng lệnh của Wireshark, một phần mềm phân tích giao thức mạng phổ biến. Nó cho phép bạn thực hiện nhiều tác vụ tương tự như Wireshark, nhưng với giao diện đơn giản hơn dựa trên văn bản.

Dưới đây là một số tính năng chính của Tshark:

- Bắt gói tin: Tshark có thể được sử dụng để bắt các gói tin mạng đang truyền qua giao diện mạng của bạn.
- Lọc gói tin: Tshark có thể lọ c các gói tin dựa trên nhiều tiêu chí khác nhau, chẳng hạn như địa chỉ IP, cổng TCP/UDP, giao thức và nội dung gói tin.
- Phân tích gói tin: Tshark có thể hiển thị thông tin chi tiết về các gói tin được bắt, bao gồm tiêu đề gói tin, dữ liệu payload và phân tích giao thức.
- Lưu và xuất dữ liệu: Tshark có thể lưu dữ liệu gói tin vào tệp để phân tích sau này hoặc xuất dữ liệu sang các định dạng khác nhau.

c, Tcpdump là một công cụ mã nguồn mở miễn phí dùng để bắt gói tin và phân tích lưu lượng mạng. Nó hoạt động bằng cách ghi lại các gói tin mạng đang truyền qua giao diện mạng của bạn và hiển thị chúng cho bạn theo thời gian thực.

Tcpdump có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm:

- Khắc phục sự cố mạng: Tcpdump có thể được sử dụng để xác định nguyên nhân của các vấn đề về mạng, chẳng hạn như mất gói tin hoặc hiệu suất mạng kém.
- Phân tích bảo mật: Tcpdump có thể được sử dụng để phân tích lưu lượng mạng để tìm kiếm các hoạt động độc hại, chẳng hạn như tấn công mạng hoặc phần mềm độc hại.

- Bắt gói tin: Tcpdump có thể bắt các gói tin mạng đang truyền qua giao diện mạng của bạn.
- Lọc gói tin: Tcpdump có thể lọc các gói tin dựa trên nhiều tiêu chí khác nhau, chẳng hạn như địa chỉ IP, cổng TCP/UDP, giao thức và nội dung gói tin.
- Phân tích gói tin: Tcpdump có thể hiển thị thông tin chi tiết về các gói tin được bắt, bao gồm tiêu đề gói tin, dữ liệu payload và phân tích giao thức.
- Lưu và xuất dữ liệu: Tcpdump có thể lưu dữ liệu gói tin vào tệp để phân tích sau này hoặc xuất dữ liệu sang các định dạng khác nhau.

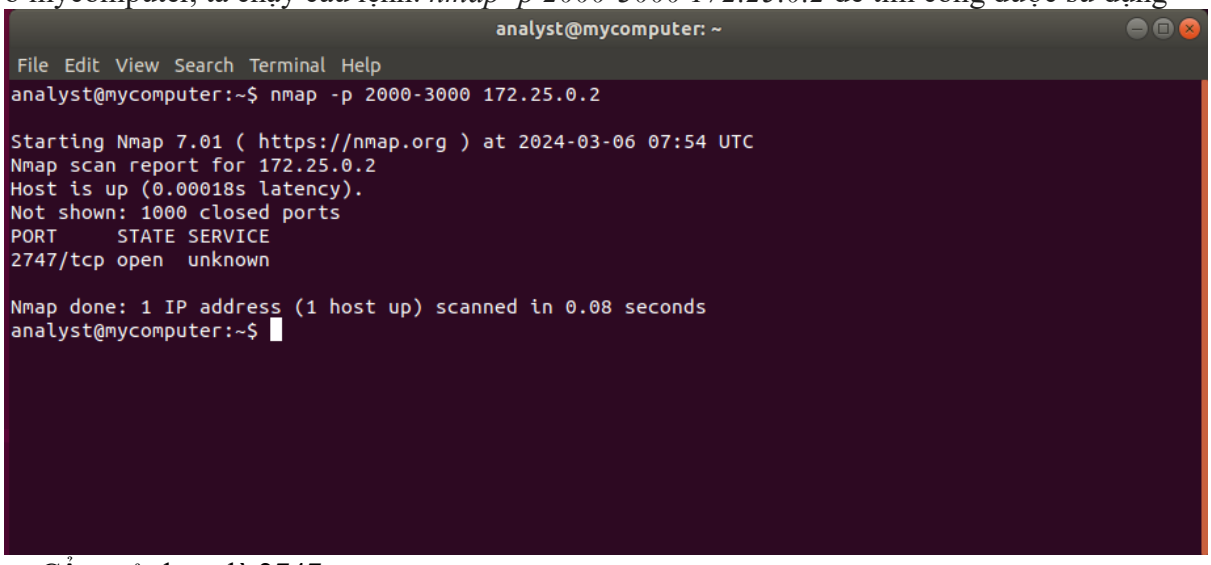
3. Nội dung thực hành.

Khởi động lab

Chạy lệnh: labtainer -r nmap-ssh trong terminal của Labtainer

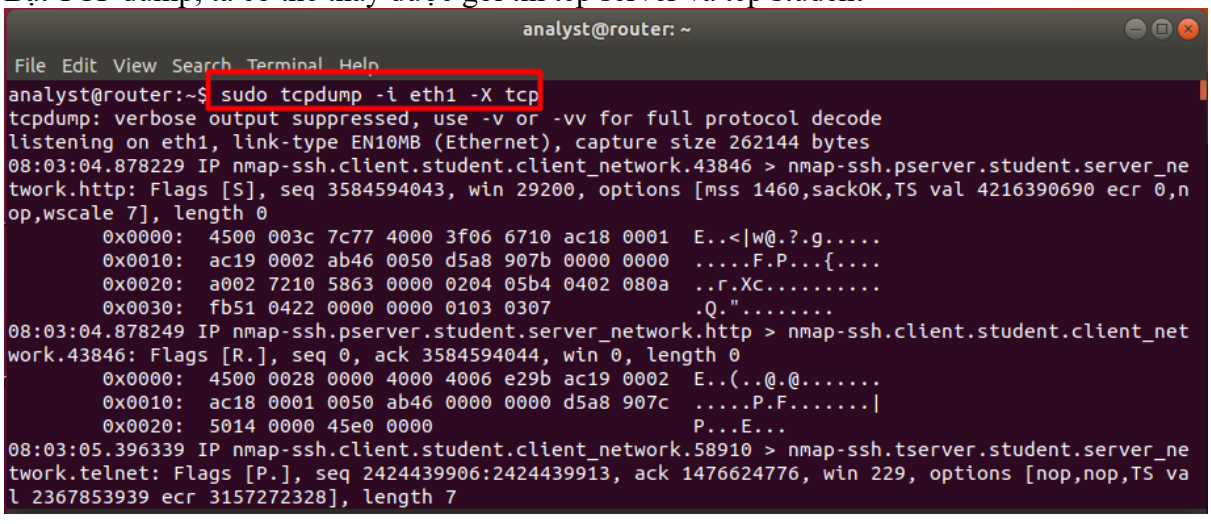
Biết địa chỉ IP máy chủ SSH mục tiêu là 172.25.0.2 và số cổng SSH thường xuyên thay đổi trong phạm vi 2000-3000.

ở mycomputer, ta chạy câu lệnh: *nmap -p 2000-3000 172.25.0.2* để tìm cổng được sử dụng



=>Cổng sử dụng là 2747

Bật TCP dump, ta có thể thấy được gói tin tcp server và tcp student



Sau đó ssh đến người dùng ubuntu trên máy chủ ssh bằng lệnh:

ssh ubuntu@172.25.0.2 -p 2747

```
analyst@mycomputer:~$ ssh ubuntu@172.25.0.2 -p 2747
The authenticity of host '[172.25.0.2]:2747 ([172.25.0.2]:2747)' can't be established.
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '[172.25.0.2]:2747' (ECDSA) to the list of known hosts.
ubuntu@172.25.0.2's password:
```

Ta sử dụng tshark để bắt gói tin và lấy mật khẩu, gõ lệnh:
sudo tshark -T -fields -e telnet.data -i eth1

```
analyst@router: ~
File  Edit  View  Search  Terminal  Help
                packets, or a multi-line view of the details of each of the
                packets, depending on whether the -V flag was specified.
                This is the default.
analyst@router:~$ sudo tshark -T fields -e telnet.data -i eth1
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as s
uperuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshar
k as an unprivileged user.
Capturing on 'eth1'
```

Server bắt được 1 gói tin chứa mật khẩu

```
analyst@router: ~
File  Edit  View  Search  Terminal  Help

ubuntu

ubuntu


Password:


894ea1



Last login: Wed Mar  6 08:12:02 UTC 2024 from 172.24.0.1 on pts/1


Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.18.0-15-generic x86_64)
```

Đã kết nối tới server

```
analyst@mycomputer:~$ ssh ubuntu@172.25.0.2 -p 2747
ubuntu@172.25.0.2's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ubuntu@pserver:~$
```

Đọc secretfile.txt

```
ubuntu@pserver:~$ ls
secretfile.txt
ubuntu@pserver:~$ cat secretfile.txt
# Filename: secretfile.txt
#
# Description: This is a pre-created file for each student (nmaplab) container

My string is: This is a secret file on the server.
ubuntu@pserver:~$
```

4. Checkwork

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nmap-ssh
Labname nmap-ssh

Student              |      nmap_count |    tshark_count |   tcpdump_count |         sshview |
==================== | =============== | =============== | =============== | =============== |
B20DCAT098           |               1 |               2 |               1 |               Y |
What is automatically assessed for this lab:

       nmap_count, tshark_count, tcpdump_count: quantity of tool invocations
       sshview: viewed the secret file using ssh
```