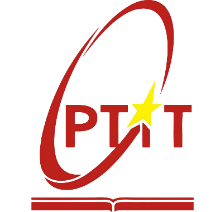
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

-------🙞🙜🕮🙞🙜-------



**BÁO CÁO BÀI THỰC HÀNH**

**Tìm hiểu về kỹ thuật T1100 trong Mitre Att&CK Web Shell**

Sinh viên: Đỗ Mạnh Cường

Mã sinh viên: B20DCAT021

Giảng viên hướng dẫn: T.S Nguyễn Ngọc Điệp

**Hà Nội - 2025**

MỤC LỤC

[MỤC LỤC 1](#_Toc186064753)

[DANH MỤC CÁC HÌNH VẼ 2](#_Toc186064754)

[DANH MỤC CÁC BẢNG BIỂU 2](#_Toc186064755)

[DANH MỤC CÁC TỪ VIẾT TẮT 3](#_Toc186064756)

[1.1 Giới thiệu chung về bài thực hành 4](#_Toc186064757)

[1.2 Nội dung và hướng dẫn bài thực hành 4](#_Toc186064758)

[1.2.1 Mục đích 4](#_Toc186064759)

[1.2.2 Yêu cầu đối với sinh viên 4](#_Toc186064760)

[1.2.3 Nội dung thực hành 4](#_Toc186064761)

[1.3 Phân tích yêu cầu bài thực hành 5](#_Toc186064762)

[1.4 Thiết kế bài thực hành 6](#_Toc186064763)

[1.5 Cài đặt và cấu hình các máy ảo 7](#_Toc186064764)

[1.6 Tích hợp và triển khai 10](#_Toc186064765)

[1.6.1 Docker Hub 10](#_Toc186064766)

[1.6.2 Github 12](#_Toc186064767)

[1.7 Thử nghiệm và đánh giá 13](#_Toc186064768)

[TÀI LIỆU THAM KHẢO 15](#_Toc186064769)

DANH MỤC CÁC HÌNH VẼ

[Hình 1 Giao diện Labedit của bài lab 8](#_Toc186064786)

[Hình 2 Cài đặt phần Result 8](#_Toc186064787)

[Hình 3 Dockerfiles của máy client 9](#_Toc186064788)

[Hình 4 Dockerfiles của máy chủ server 10](#_Toc186064789)

[Hình 5 Add và commit bài lab 11](#_Toc186064790)

[Hình 6 Đẩy các vùng chứa lên dockerhub 11](#_Toc186064791)

[Hình 7 Tạo imodule.tar chứa bài thực hành 12](#_Toc186064792)

[Hình 8 Các vùng chứa được đẩy lên dockerhub 12](#_Toc186064793)

[Hình 9 Tạo file Imodule.tar 13](#_Toc186064794)

[Hình 10 Đẩy file imodule.tar lên github 13](#_Toc186064795)

[Hình 11 SSH tới server bằng thông tin được cung cấp 14](#_Toc186064796)

[Hình 12 Đọc file getflag 14](#_Toc186064797)

[Hình 13 Thêm web shell 14](#_Toc186064798)

[Hình 14 Xóa file getflag -> SSH session bị xóa 15](#_Toc186064799)

[Hình 15 Minh chứng web shell hoạt động. 15](#_Toc186064800)

[Hình 16 Checkwork 15](#_Toc186064801)

DANH MỤC CÁC BẢNG BIỂU

[Bảng 1. Bảng Result 7](#_Toc186064284)

DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **Từ  viết tắt** | **Thuật ngữ tiếng Anh/Giải thích** | **Thuật ngữ tiếng Việt/Giải thích** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Giới thiệu chung về bài thực hành

Bài thực hành "Tìm hiểu về kỹ thuật WebShell T1100 trong Mitre ATT&CK Framework" được thiết kế nhằm giúp sinh viên hiểu rõ cách thức kẻ tấn công duy trì quyền truy cập và điều khiển hệ thống mục tiêu thông qua việc cài đặt mã độc trên máy chủ Web. Theo khung Mitre ATT&CK, kỹ thuật WebShell (T1100) thường được sử dụng để tạo “cổng hậu” (backdoor) trên các máy chủ Web công khai, cho phép kẻ tấn công khai thác lỗ hổng và mở rộng phạm vi xâm nhập vào hệ thống.

Trong bài thực hành này, sinh viên sẽ được tiếp cận tình huống khi mà có thể truy cập đến mục tiêu nhưng để có thể duy trì quyền kiểm soát ngay cả khi thông tin đăng nhập bị thay đổi hay lỗ hổng ứng dụng đã được vá, kẻ tấn công phải cài các mã độc, shell, backdoor, …trên máy chủ mục tiêu. Ở đây sinh viên sẽ học cách triển khai WebShell, hiểu các phương thức mà kẻ tấn công có thể khai thác để ẩn giấu và duy trì kết nối, cũng như áp dụng các biện pháp bảo vệ và phát hiện hoạt động WebShell trong môi trường thực tế.

Quá trình tìm hiểu và thực hành kỹ thuật WebShell T1100 không chỉ giúp sinh viên nắm vững khái niệm và cách thức tấn công, mà còn cung cấp kiến thức cần thiết để triển khai các biện pháp phòng thủ hiệu quả. Từ đó, sinh viên sẽ phát triển kỹ năng phân tích, điều tra, và bảo vệ hệ thống mạng, góp phần nâng cao nhận thức về an ninh thông tin trong môi trường công nghệ ngày nay.

* 1. Nội dung và hướng dẫn bài thực hành
     1. Mục đích

Giúp sinh viên hiểu rõ cách mà kẻ tấn công có thể duy trì quyền truy cập và điều khiển hệ thống mục tiêu thông qua việc cài đặt WebShell, từ đó nâng cao khả năng nhận diện và đánh giá các hoạt động bất thường trên hệ thống. Thông qua việc triển khai và phân tích WebShell, sinh viên sẽ nắm bắt được quy trình tấn công, cách thức ẩn giấu, cũng như xây dựng kỹ năng bảo mật, phòng thủ vững chắc trước các mối đe dọa tương tự trong tương lai.

* + 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, biết viết shell php, hiểu cơ chế hoạt động của web server, giao thức ssh.

* + 1. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

*labtainer -r web\_attack\_adv\_webshell*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi động xong một terminal ảo sẽ xuất hiện, đại diện cho máy tấn công: ***client***.

Sinh viên sẽ được cung cấp một tài khoản của user trên server.

SSH tới server tới account được cung cấp, VD:

*ssh student@172.70.10.200*

Liệt kê các file trên thư mục home của user nhận thấy có file getflag. Đọc nó.

Nếu xóa file getflag, kết thúc phiên ssh hiện tại, đổi mật khẩu của user hiện tại và 1 file flag.txt được tạo trên thư mục gốc.

Để đọc được flag thì ta phải triển khai web shell để duy trì xâm nhập dù thông tin xâm nhập ban đầu đã được vá.

Viết một PHP web shell trên directory root với các func như ***system,* *exec****,* …

Từ máy client truy cập tới endpoint web shell truyền các command vào các tham số đã được định nghĩa trước. VD:

*curl -v [ip-addr]/shell.php?cmd=cat /flag.txt*

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab web\_attack\_adv\_webshell*

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer –r web\_attack\_adv\_webshell*

* 1. Phân tích yêu cầu bài thực hành

Bài thực hành gồm 2 máy tính nằm trên 1 dải mạng. Trong đó một máy là client và một máy là server đang chạy một web service. Để hoàn thành bài thực hành sinh viên cần truy cập vào máy chủ web từ thông tin có được, sau đó tạo shell nhằm duy trì quyền kiểm soát để dù máy chủ có vá hay xóa kết nối thì ta vẫn có backdoor để xâm nhập lại.

* 1. Thiết kế bài thực hành

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 2 container: 1 container mang tên “client” đóng vai trò máy khách, 1 container mang tên “server” đóng vai trò máy chủ.

Tạo 1 dải mạng có cấu hình: 172.70.10.0/24 và gateway: 172.70.10.1.

Cấu hình docker gồm có:

Client: lưu cấu hình cho máy khách, trong đó gồm có:

Tên máy: client

Địa chỉ trong mạng: 172.70.10.100

Server: lưu cấu hình cho máy chủ, trong đó gồm có:

Tên máy: web\_server

Địa chỉ trong mạng: 172.70.10.200

config: lưu cấu hình hoạt động của hệ thống

dockerfiles: mô tả cấu hình của container trong đó:

Server chạy apache service triển khai dịch vụ web server và một dịch vụ ssh.

Client chạy như một người dùng bình thường khi truy cập web server.

Các nhiệm vụ cần phải thực hiện để thực hành thành công:

Sinh viên được cung cấp thông tin ssh của một user trên server.

Attacker sử dụng thông tin đó để truy cập vào máy chủ.

Đọc file getflag.

Tạo một shell trên directory root của server nhằm duy trì quyền truy cập.

Xóa file getflag -> đồng thời lúc đó password ssh của user được cung cấp cũng sẽ thay đổi.

Chứng minh từ shell vẫn có thể duy trì truy cập.

Kết thúc bài lab và đóng gói kết quả.

Thiết lập hệ thống mạng sao cho máy client và máy server cùng một mạng LAN.

Để đánh giá được sinh viên đã hoàn thành bài thực hành hay chưa, cần chia bài thực hành thành các nhiệm vụ nhỏ, mỗi nhiệm vụ cần phải chỉ rõ kết quả để có thể dựa vào đó đánh giá, chấm điểm. Do vậy, trong bài thực hành này hệ thống cần ghi nhận các thao tác, sự kiện được mô tả và cấu hình như bảng 1:

1. Bảng Result

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Result Tag | Container | File | Field Type | Field ID | Timestamp Type | LINE ID |
| password\_prompt | client | ssh.stdout | CONTAINS | 172.70.10.200's password | FILE |  |
| correct\_password | client | ssh.stdout | CONTAINS | Welcome to Ubuntu | FILE |  |
| poc\_rce\_ifconfig\_input | client | curl.stdout | CONTAINS | Ifconfig | FILE |  |
| poc\_rce\_ifconfig\_input | client | curl.stdout | CONTAINS | Init 172.70.10.200 | FILE |  |

- password\_prompt: Yêu cầu nhập password khi ssh.

- correct\_password: Nhập đúng password cho user

- poc\_rce\_ifconfig\_input: Chạy câu lệnh để chứng minh web shell hoạt động

- poc\_rce\_ifconfig\_output: Output mong đợi từ việc chạy command trên.

* 1. Cài đặt và cấu hình các máy ảo

A screenshot of a computer

Description automatically generated

1. Giao diện Labedit của bài lab

A screenshot of a computer

Description automatically generated

1. Cài đặt phần Result

A screenshot of a computer

Description automatically generated

1. Dockerfiles của máy client

A screenshot of a computer

Description automatically generated

1. Dockerfiles của máy chủ server
   1. Tích hợp và triển khai

Bài thực hành đã được triển khai như sau:

Docker Hub

https://hub.docker.com/u/domanhcuong2502

A computer screen shot of a program

Description automatically generated

1. Add và commit bài lab

A screenshot of a computer

Description automatically generated

1. Đẩy các vùng chứa lên dockerhub

A screenshot of a computer

Description automatically generated

1. Tạo imodule.tar chứa bài thực hành

A screenshot of a computer

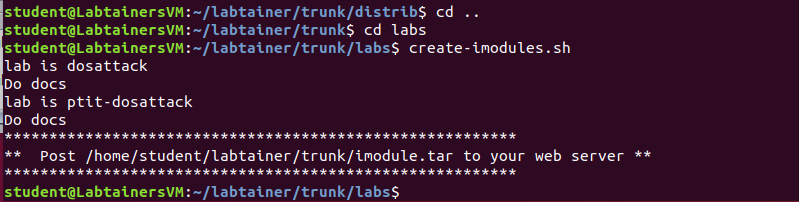
Description automatically generated

1. Các vùng chứa được đẩy lên dockerhub

Github

https://github.com/oceanmancuonh/web\_attack\_adv\_webshell

Nhập lệnh create-imodules.sh



1. Tạo file Imodule.tar

Tạo repo mới để đẩy imodule.tar lên và tạo phần release mới

A screenshot of a computer

Description automatically generated

1. Đẩy file imodule.tar lên github
   1. Thử nghiệm và đánh giá

Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:

A computer screen shot of a computer program

Description automatically generated

1. SSH tới server bằng thông tin được cung cấp

A black background with white text

Description automatically generated

1. Đọc file getflag

A computer screen shot of a program

Description automatically generated

1. Thêm web shell

A computer screen shot of a program

Description automatically generated

1. Xóa file getflag -> SSH session bị xóa

A computer screen shot of a program

Description automatically generated

1. Minh chứng web shell hoạt động.

A computer screen shot of a program

Description automatically generated

1. Checkwork

TÀI LIỆU THAM KHẢO

[1] ATT&CK, M. (n.d.). *Server Software Component: Web Shell.* Retrieved from https://attack.mitre.org/techniques/T1505/003/

[2] attackdefense.pentesteracademy.com. (n.d.). Retrieved from T1100: Web Shell : https://www.attackdefense.pentesteracademy.com/challengedetails?cid=1555