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.

2. **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.

3. **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.

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%20/flag.txt

curl -v "http://172.70.10.200/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.

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