LAB 1

QUÉT LỖ HỔNG BẢO MẬT BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Kỳ báo cáo: Buổi 03 (Session 03)**

**Tên chủ đề: Information Gathering**

*GVHD: Nghi Hoàng Khoa*

**Nhóm: 06 (ghi số thứ tự nhóm)**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT101.M11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Trần Hoàng Khang | 19521671 | 19521671@gm.uit.edu.vn |
| 2 | Nguyễn Đoàn Xuân Bình | 19521265 | 19521265@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 01 | 100% |
| 2 | Kịch bản 02 | 100% |
| 3 | Kịch bản 03 | 100% |
| 4 | Kịch bản 04 | 100% |
| 5 | Kịch bản 05 | 100% |

BÁO CÁO CHI TIẾT

***2. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.***

Chart, table

Description automatically generated

*Như ta thấy ở trên, việc scan là do máy scanner liên tục gửi các gói tin SYN đến máy đối phương và nhận lại các gói [RST,ACK] và thực hiện lấy payload để phân tích(còn phân tích sao thì không rõ ~~). Điều này tương tự với cờ -sS trong lệnh “nmap”.*

***3. Quét lại nhưng quét thêm port UDP.***

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

***5. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.***

Dùng tài khoản chứng thực để quét sẽ phát hiện được nhiều lỗ hổng hơn, đồng thời cũng xuất hiện nhiều lỗi nghiêm trọng hơn, can thiệp vào mức đặc quyền và bên trong lõi hệ thống.

***6. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực***

*Sử dụng tài khoản chứng thực:*

*Ưu điểm:*

*+ Ít bị lỗi*

*+ Phát hiện được nhiều lỗi nghiêm trọng hơn và đa dạng hơn*

*Khuyết điểm:*

*+ Đôi khi quá trình scan ảnh hưởng tới hiệu suất hoạt động của máy patient, nghẽn mạng, gây quá tải và tăng payload và traffic cho các port được quét.*

*=> Sử dụng tài khoản không chứng thực sẽ có những đặc điểm ngược với bên trên*

***8. Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111?  
Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?***

Table

Description automatically generated with medium confidence

1 số port khác 111: 81, 8009, ….

Nhìn vào kết quả, ta thấy có một số gói tin [SYN,ACK], [RST] thì chắc có thể đoán được là Nessus cần scan hết để xác định được state của port  
***9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?***

*Tích vào ô bên dưới*

Graphical user interface, text, application, email, website

Description automatically generated

*Mọi thứ đã khá OK:*

A screenshot of a computer

Description automatically generated with medium confidence

***10. Thực hiện quét lại sử dụng 2 plugin khác.***

Graphical user interface, text, application

Description automatically generated

***11. Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây, và viết báo cáo kết quả theo như các phần đã chia ở bài tập 1***

Sn1per (<https://github.com/1N3/Sn1per>)

Sni1per cung cấp nhiều công cụ để scan, về mặt nhận xét cá nhân, đây là công cụ được tích hợp scan theo nhiều loại công cụ khác nhau, và cung cấp nhiều tùy chọn để scan.

Text

Description automatically generated

Thử scan dưới NORMAL MODE, công cụ sẽ thực hiện theo trình tự dưới đây:

- Load và Check các file config

- Ping để kiểm tra host còn active không

Text

Description automatically generated

Chạy công cụ nmap với TCP portscan option:

Text

Description automatically generated

Chạy các script để detect các lỗ hổng :

Text

Description automatically generated

và cuối cùng là tìm shell và mở nó để thực hiện remote command. Cái này khá bá đạo

Text

Description automatically generated