BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của mã độc**

**Kỳ báo cáo: Buổi 3 (Session 03)**

**Tên chủ đề: Simple Botnet**

*GVHD: Nghi Hoàng Khoa*

**Nhóm: 09**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT230.O21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |
| 2 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

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

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Yêu cầu 1: Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.**

* Đầu tiên, chạy ứng dụng mIRC client trên windows 10.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Tại máy server, khởi động chương trình Wireshark để theo dõi quá trình kết nối của botmaster với irc.swiftirc.net
* Chạy lệnh:

Python2 boss.py -c Allnitecafe -n hien -s irc.swiftirc.net -p 6667

A screenshot of a computer program

Description automatically generated

* Bắt đầu phân tích các gói tin
* 2 gói tin thứ 19 20 protocol DNS là thực hiện phân giải tên miền.
* Gói 21 22 23 là quá trình bắt tay 3 bước.
* Gói 24 đến 36 là thực hiện quá trình kết nối đến server là gửi các request tạo các thông tin được nhập ở console.
* Gói 37 đến 44 là thực hiện việc join boss vào server và tạo channel như người dùng đã nhập ở console.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Yêu cầu 2: Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.**

* Trên máy 2, thực hiện chỉnh sửa code: Tạo một bản copy của worker.py đặt tên là myworker.py
* Tắt các dòng lệnh:

#from gevent import DNSError

#Except DNSError:

#pass

* Sau đó thực hiện chạy bằng lệnh python myworker.py -b hien

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Thực hiện phân tích gói tin.
* Gói tin 1 và 2 thực hiện phân giải tên miền.
* Gói 3 4 5 là quá trình bắt tay 3 bước.
* Các gói còn lại là quá trình thực hiện kết nối đến channel. Ta thấy được sẽ có những gói join như boss vì không thực hiện việc tạo channel mà join vào channel sẵn có.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Yêu cầu 3: Báo cáo kết quả chạy command IRC client.**

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Yêu cầu 4: Tiếp tục những gì đang thực hiện tại C.1, bạn hãy mở rộng mạng Botnet với 2 bots.**

* Ở máy 2 mở 2 terminal và chạy lệnh python của worker:

A screenshot of a computer

Description automatically generated

* Kiểm tra trên windows 10 thì thấy đã kết nối được với 2 worker.

A screenshot of a computer

Description automatically generated

* Màn hình console hiển thị tương tự:

A screenshot of a computer program

Description automatically generated

1. **Yêu cầu 5: Với những kiến thức về Simple Worm đã làm và Botnet vừa làm. Bạn hãy tích hợp Simple Worm vào Bot để ngoài việc thực hiện command từ xa còn có thể khai thác được lỗ hổng của máy từ xa.**

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [*NT101.K11.ATCL*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)