BÁO CÁO BÀI TẬP

**Môn học: Pháp chứng kỹ thuật số**

**Kỳ báo cáo: Buổi**

**Tên chủ đề: Email Forensics**

*GVHD: Nguyễn Tấn Cầm*

*Ngày báo cáo: 31/5/2023*

**Nhóm:**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT334.N21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |
| 2 |  |  |  |
| 3 |  |  |  |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Công việc** | **Thực hiện** | **Thành viên thực hiện** | **Kết quả tự đánh giá** |
| 1 | Email Forensics | Tìm flag | 100% |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

BÁO CÁO CHI TIẾT

Đầu tiên ta tải file về và mở bằng FTK imager

A screenshot of a computer

Description automatically generated

Thực hiện export directory listing

A screenshot of a computer

Description automatically generated with medium confidence

Mở file được xuất ra xem thì ta thấy thông tin của các custom images thunderbird

A screenshot of a computer

Description automatically generated

Tiếp tục xem mail trong inbox

A screenshot of a computer

Description automatically generated

Ta có được password khi kéo xuống phía dưới

A screenshot of a computer

Description automatically generated

Thực hiện copy thông tin dạng base64 vào file bên linux

A screenshot of a computer

Description automatically generated

Thực hiện decode base64 và lưu thành file zip

A screen shot of a computer

Description automatically generated with medium confidence

Thực hiện giải nén với password: Passw0rd!23

A computer screen shot of a file

Description automatically generated with low confidence

Cài đặt tool olevtool

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Thực hiện giải mã file policy.xlsm

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Kiểm tra các hàm thì thấy đây là những hàm liên quan đến malware dùng để đọc, mã hoá dữ liệu, thay đổi địa chỉ

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Nhưng ta thấy đây có một đoạn code lạ:

Dim kzujiavquwjkahbl As Variant

kzujiavquwjkahbl = Array(223, 195, 213, 236, 246, 226, 227, 167, 231, 228, 238, 200, 167, 241, 200, 163, 249, 200, 166, 249, 245, 167, 239, 200, 229, 164, 225)

Dim wwiqwvyhemghupdahkj As Integer

wwiqwvyhemghupdahkj = 0

For i = 0 To 26

wwiqwvyhemghupdahkj = wwiqwvyhemghupdahkj + kzujiavquwjkahbl(i) Xor 151

Next

Ta sẽ thực hiện code python và giải mã:

A screenshot of a computer

Description automatically generated

Ta có được flag đầu là: HTB{aut0psy\_0f\_4n\_1nb0x\_r3v

Thực hiện tải file về và thực hiện dịch ngược update.exe

A screenshot of a computer

Description automatically generated

Ta có được code trong phần PSEmpire\_Stage1.Program

byte[] array2 = Convert.FromBase64String("Ki11akYtd0YqdGkoa3xGLW1Gbilrcjg4ZA==");

for (int j = 0; j < array2.Length; j++)

{

array2[j] = (byte)(array2[j] ^ Convert.ToByte(25));

}

Thực hiện sử dụng cyberchef để giải mã

A screenshot of a computer

Description automatically generated

Ta có nữa sau của flag 34ls\_4n\_3mp1re\_4t\_w0rk!!}

Flag: HTB{aut0psy\_0f\_4n\_1nb0x\_r3v34ls\_4n\_3mp1re\_4t\_w0rk!!}

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

*(Xem trang kế tiếp)*

---

*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.H11.1]-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 và đóng góp tích cực tại lớp.
* 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-2)