BÀI TẬP 2 LÝ THUYẾT

THỰC HÀNH AN TOÀN BẢO MẬT MẠNG MÁY TÍNH

Lab 2: Làm quen với Wireshark

Họ tên: Phạm Hồ Bình An

Lớp: 10DH\_CNPM2

Mã số sinh viên: 1050080127

• Bước 1: Tải và cài đặt RFK trên Windows.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Khởi động RFK.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

• Bước 2: Dùng trình duyệt web, đăng nhập thành công vào một tài khoản Gmail

tại <https://gmail.com>

• Bước 3: Truy cập vào Youtube.com và chọn xem một video bất kỳ.

• Bước 4: Truy cập Google.com và tìm kiếm với từ khóa là tên sinh viên, chọn xem

một kết quả bất kỳ.

• Bước 5: Mở RFK và xem kết quả thu thập được.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Nội dung do AI tạo ra có thể không chính xác.

Hình 3. Xem các kết quả thu thập được từ RFK

2. Thử nghiệm Keylogger gửi kết quả qua email, FTP server

BlazingTools Perfect Keylogger (BPK) là một trong những keylogger chuyên nghiệp

với nhiều tính năng nâng cao so với các Keylogger miễn phí. Tham khảo các tính

năng của BPK tại http://www.blazingtools.com/bpk.html

BPK cũng cho phép gửi kết quả thu thập được từ máy tính mục tiêu qua email hoặc

FTP server của attacker, do đó có thể thu thập được thông tin máy mục tiêu từ xa.

Phần mềm này cung cấp dưới dạng trả phí tại http://www.blazingtools.com, tuy

nhiên, với điều kiện thực hành, sinh viên có thể tìm bản đầy đủ được chia sẻ tại

Internet để thử nghiệm.

Sinh viên cũng có thể dùng Keylogger khác có chức năng tương đương để thực hiện

các yêu cầu sau.

Lưu ý: Tắt các phần mềm Antivirus trước khi cài đặt.

Lab 2: Keylogger trên PC và điện thoại

5

• Bước 1: Cài đặt BPK, thay đổi các tùy chọn mặc định để tránh bị phát hiện.

Hình 4. Cài đặt BPK 1.68.2

Hình 5. Kích hoạt bản Full của Perfect Keylogger (chỉ dùng cho mục đích thử nghiệm)

• Bước 2: Bật các chức năng chụp ảnh màn hình, theo dõi gõ bàn phím

Hình 6. Thiết lập theo dõi bàn phím

Hình 7. Thiết lập chụp ảnh màn hình

• Bước 3: Cấu hình email để gửi kết quả thu thập được.

Hình 8. Cấu hình email

Cấu hình email nhận ở tab Delivery. Sinh viên tự cấu hình (Có thể xem hướng dẫn

của BPK bằng cách chọn More Details) và giải thích quá trình cấu hình của mình.

• Bước 4: Đăng ký một free hosting có chức năng FTP dùng username/password

để upload file hoặc tự xây dựng 1 FTP server.

• Bước 5: Cấu hình FTP trên BPK để gửi kết quả thu thập được

Hình 9. Cấu hình FTP để gửi kết quả về FTP server

Cấu hình các thông số của FTP server tại tab FTP server: Sinh viên tự cấu hình (Có

thể xem hướng dẫn của BPK bằng cách chọn More Details) và giải thích quá trình cấu

hình của mình.

• Bước 6: Thực hiện một số thao tác trên máy tính như:

- Mở trình duyệt web: Nghe nhạc, xem phim, đọc báo, ...

- Đăng nhập vào một website hoặc một công cụ bất kỳ có sử dụng mật khẩu.

- Truy cập vào một số thư mục trên website và mở, chỉnh sửa một số file.

• Bước 7: Kiểm tra kết quả thu thập được bằng giao diện chính của BPK.

Hình 10. Kiểm tra Keystrokes, Chats, Screenshot, Websites từ BPK

• Bước 8: Kiểm tra kết quả thu thập được qua email đã cấu hình.

• Bước 9: Kiểm tra kết quả thu thập được qua FTP server đã cấu hình.

3. Thử nghiệm Keylogger trên smartphone Andoid/iOS

Sinh viên tìm hiểu và tự chọn 1 trình keylogger/theo dõi hoạt động trên Android

hoặc iOS và thử nghiệm các chức năng và minh họa. Ví dụ: Spytic, Hoverwatch, ...

Có thể thử nghiệm trên máy ảo Android như Bluestack, Genymotion, ... hoặc thiết bị thật.

C. CÂU HỎI

Sau quá trình thực hành, sinh viên trả lời các câu hỏi sau:

1. Nêu biện pháp phòng tránh; các cách phát hiện Keylogger trên máy tính - điện

thoại và minh họa nếu có thể.

Cài các phần mềm Anti Keylogger, Bật chế độ Anti Viruss

2. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính và điện thoại khác.

**Free Keylogger**

**DanuSoft Free Keylogger**

**Real Free Keylogger**

D. YÊU CẦU

 Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện theo nhóm hoặc

cá nhân như đã đăng ký từ buổi 1.

 Sinh viên báo cáo kết quả thực hiện và nộp bài gồm:

- Báo cáo:

+ Trình bày trong file Word (.doc, .docx) hoặc .PDF theo mẫu có sẵn tại courses.

+ Đặt tên theo định dạng: [Mã lớp]-LabX\_MSSV1-Tên SV1\_MSSV2 –Tên SV2

Ví dụ: [NT101.H11.1]-Lab1\_14520000-Viet\_14520999-Nam.

- Video:

+ Quay lại quá trình thực hiện Lab của sinh viên.

+ Upload lên Youtube.com và chèn link vào đầu báo cáo theo mẫu.

Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

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.

 Video trình bày trực quan, dễ hiểu.

 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.