**VIETNAM NATIONAL UNIVERSITY HCMC**

**UNIVERSITY OF INFORMATION TECHNOLOGY**

**FACULTY OF COMPUTER NETWORKS AND COMMUNICATIONS**

A blue logo with a planet and text

Description automatically generated

**BÁO CÁO ĐỒ ÁN**

Môn học: Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

**Đề tài:**

Triển khai hệ thống IDPS bằng Zeek (Bro)

**Giảng viên hướng dẫn:** Đỗ Hoàng Hiển

**Lớp:** NT204.O21.ATCL

**Nhóm 5:**

|  |  |
| --- | --- |
| Lương Hồ Trọng Nghĩa | 21522375 |
| Phạm Công Lập | 21522281 |
| Trần Tấn Hải | 21522036 |
| Nguyễn Tấn Phát | 21522447 |

**MỤC LỤC**

1. **Giới thiệu 3**
   1. **Giới thiệu vấn đề 3**
   2. **Mục tiêu của đồ án 3**
   3. **Phương pháp nghiên cứu 3**
2. **Cơ sở lý thuyết 4**
   1. **Giới thiệu 4**
   2. **Tính năng 4**
3. **Phân tích thiết kế hệ thống 5**
   1. **Mô hình tổng quan 5**
   2. **Phương pháp 5**
   3. **Kiến trúc từng thành phần 6**
   4. **Luồng hoạt động 6**
4. **Hiện thực hệ thống 7**
5. **Cài đặt và cấu hình cho máy Zeek 7**
6. **Cài đặt và cấu hình cho máy Ubuntu Client 9**
7. **Thực nghiệm và đánh giá 10**
8. **Các kịch bản thực nghiệm 10**
9. **Đánh giá kết quả thực nghiệm 22**
10. **So sánh với các công cụ liên quan 22**
11. **Kết luận 23**

**Chương 1: Giới thiệu chung**

* 1. **Giới thiệu vấn đề**

Trong không gian mạng ngày nay, việc bảo vệ mạng và hệ thống thông tin trở thành một bài toán nan giải với các tổ chức. Mạng nội bộ của các tổ chức thường đối mặt với nhiều mối đe dọa bảo mật, từ các cuộc tấn công đơn giản đến phức tạp như từ chối dịch vụ (DoS) hay tinh vi hơn như tấn công mã độc tống tiền (ransomware).

* 1. **Mục tiêu của đồ án**

Mục tiêu của đồ án là xây dựng một hệ thống Network-based Intrusion Detection System (NDIS) sử dụng công cụ mã nguồn mở Zeek, nhằm giám sát và phát hiện các mối đe dọa tìm tàng trong mạng nội bộ của tổ chức như:

* Phát hiện sớm các cuộc tấn công mạng và hành vi đáng ngờ trong mạng nội bộ
* Cảnh báo về các sự kiện mạng có thể gây nguy hiểm cho hệ thống
* Cung cấp thông tin chi tiết và phân tích về các traffic trong mạng thông qua logs
  1. **Phương pháp nghiên cứu**

Để thực hiện được mục tiêu đề ra, đồ án sẽ thực hiện theo các bước sau:

1. Nghiên cứu, tìm hiểu về cách hoạt động của Zeek trong môi trường mạng nội bộ
2. Cấu hình Zeek để phát hiện các mối đe dọa phổ biến
3. Phát triển và triển khai để phát hiện các mối đe dọa tinh vi hơn, cũng như theo nhu cầu
4. Thử nghiệm, đánh giá và tối ưu hệ thống

**Chương 2: Cơ sở lý thuyết**

**2.1. Giới thiệu**

Zeek IDS (trước đây được biết đến với tên Bro IDS) là một công cụ mạnh mẽ và linh hoạt được sử dụng cho việc phát hiện và phản ứng lại các mối đe dọa mạng trong mạng nội bộ. Zeek không chỉ giúp người quản trị mạng phát hiện các cuộc tấn công mạng, mà còn cung cấp thông tin chi tiết và phân tích về các mẫu tấn công mạng và hành vi không mong muốn.

**2.2 Tính năng**

Zeek IDS có các tính năng chính sau:

* Phát hiện tấn công mạng: Zeek có khả năng phát hiện các mẫu tấn công mạng thông qua việc phân tích lưu lượng mạng.
* Phân tích lưu lượng mạng: Zeek phân tích lưu lượng mạng và tạo ra các sự kiện (events) với thông tin chi tiết về các kết nối mạng, gói tin mạng, và các hoạt động khác trên mạng.
* Thiết lập quy tắc phát hiện tùy chỉnh: Zeek cho phép người dùng tạo ra các quy tắc phát hiện tùy chỉnh dựa trên nhu cầu cụ thể của tổ chức.
* Tích hợp dữ liệu: Zeek có khả năng tích hợp với các công cụ và hệ thống khác như SIEM (Security Information and Event Management) và các công cụ phân tích bảo mật khác.
* Hỗ trợ đa nền tảng: Zeek có thể chạy trên nhiều nền tảng hệ điều hành khác nhau như Linux, macOS và FreeBSD.

**Chương 3: Phân tích thiết kế hệ thống**

**3.1 Mô hình tổng quan**

A diagram of a computer security system

Description automatically generated

**Hình 1**. Mô hình tổng quan

**3.2 Phương pháp**

**-** Sử dụng Zeek làm công cụ chính cho hệ thống NIDS

- Thiết kế môi trường mạng ảo hóa sử dụng VMware để triển khai hệ thống

- Xây dựng môi trường bao gồm các máy ảo: Attacker, LinuxClient, WindowsClient, Zeek

**3.3 Kiến trúc từng thành phần**

**3.3.1 Zeek**

**-** Zeek được cài đặt trên máy này để giám sát và phân tích lưu lượng mạng

- Sử dụng iptables rule để cấu hình cho máy làm router

**3.3.2 Attacker**

**-** Máy Attacker sử dụng Kali Linux để tạo các cuộc tấn công mạng

- Kết nối với máy Zeek thông qua card host-only

**3.3.3 LinuxClient**

**-** Máy sử dụng Ubuntu là một máy trong mạng nội bộ

- Kết nối với máy Zeek thông qua card host-only

**3.3.4 WindowsClient**

**-** Máy sử dụng Windows là một máy trong mạng nội bộ

- Kết nối với máy Zeek thông qua card host-only

**3.4 Luồng hoạt động**

**-** Máy Attacker tạo các cuộc tấn công mạng

- Máy Zeek giám sát và phát hiện các cuộc tấn công trên mạng nội bộ

- Khi phát hiện có tấn công Zeek tạo ra các cảnh báo cho người quản trị

**Chương 4: Hiện thực hệ thống**

* 1. **Cài đặt và cấu hình cho máy Zeek**

A screenshot of a computer screen

Description automatically generated

**Hình 2.** Cài đặt thư viện và update hệ thống chuẩn bị cài đặt Zeek

A screenshot of a computer

Description automatically generated

**Hình 3.** Cài đặt Zeek

A screenshot of a computer

Description automatically generated

**Hình 4**. Kiểm tra các card mạng đã cấu hình và điều chỉnh interface cho Zeek

**A screenshot of a computer

Description automatically generated**

**Hình 5**. Cấu hình cho máy Zeek thành router

* 1. **Cài đặt và cấu hình cho máy Ubuntu Client**

**A screenshot of a computer

Description automatically generated**

**Hình 6**. Cài đặt DVWA cho client để attacker tấn công

**Chương 5: Thực nghiệm và đánh giá**

**5.1 Các kịch bản thực nghiệm**

**5.1.1 DOS**

- Mô tả: Tấn công DNS Amplification được thực hiện bằng cách gửi các yêu cầu DNS giả mạo với địa chỉ IP của nạn nhân đến các server DNS công cộng, nhằm làm quá tải hệ thống DNS và gây ra tình trạng từ chối dịch vụ (DoS)

- Thực hiện kịch bản: sử dụng công cụ dnsblast để tạo ra lưu lương giả truy cập dns

A screenshot of a computer

Description automatically generated

**Hình 7.** Sử dụng công cụ dnsblast để tấn công dos

A screenshot of a computer program

Description automatically generated

**Hình 8**.Dùng trace-summary để đọc tổng lưu lượng, xem giao thức để phát hiện

A screenshot of a computer

Description automatically generated

**Hình 9.** Dùng script để kiểm tra thông qua uid

A screenshot of a computer

Description automatically generated

**Hình 10**. Dùng uid tìm thấy để kiểm tra trong log

**5.1.2 Vulnerability Scan**

**-** Mô tả: Sử dụng công cụ Burp Suite để thực hiện quét lỗ hổng bảo mật trên ứng dụng web

- Thực hiện kịch bản: Dựng DVWA ở máy client để cho attacker dùng Burp Suite quét lỗ hổng

A screenshot of a computer

Description automatically generated

**Hình 11**. Chuẩn bị cho Burp Suite để scan

A screenshot of a computer

Description automatically generated

**Hình 12**. Burp Suite scan ra được 1 số lỗi

A screenshot of a computer

Description automatically generated

**Hình 13**. Zeek detect thành công

**5.1.3 Data Exfiltration Through Command Injection**

**-** Mô tả: Sử dụng lỗ hổng command injection trong ứng dụng web của tổ chức để thực hiện truy cập không được ủy quyền vào hệ thống và truyền dữ liệu bí mật ra ngoài.

- Thực hiện kịch bản: tấn công command injection trên web DVWA để gửi dữ liệu ra webhook

A screenshot of a computer

Description automatically generated

**Hình 14**. Setup để bắt đầu khai thác

A screenshot of a computer

Description automatically generated

**Hình 15.** Khai thác thành công thông tin database của DVWA

A screenshot of a computer

Description automatically generated

**Hình 16.** Đọc thông tin của file /etc/passwd

A screenshot of a computer

Description automatically generated

**Hình 17**. Phát hiện được 1 số bất thường

A screenshot of a computer

Description automatically generated

**Hình 18.** Kiểm tra logs thì phát hiện ra payload

**5.1.4 Malware through EternalBlue**

**-** Mô tả: Tấn công sử dụng lỗ hổng EternalBlue trên hệ điều hành Windows để lan truyền malware và thực hiện kiểm soát từ xa (RCE) trên các máy chạy Windows trong mạng nội bộ.

- Thực hiện kịch bản: Sử dụng công cụ Metasploit để thực hiện tấn công sử dụng lỗ hổng EternalBlue.

A screenshot of a computer

Description automatically generated

**Hình 19.** Setup tấn công

**A screenshot of a computer

Description automatically generated**

**Hình 20**. Tấn công thành công

A screenshot of a computer

Description automatically generated

**Hình 21**. Zeek đã phát hiện thành công

**5.1.5 Anomaly Detection**

**-** Mô tả: Phát hiện thông lượng bất thường trong mạng nội bộ

- Kịch bản: sử dụng công cụ trace-summary trong Zeek để tạo profile và tìm kiếm bất thường từ profile đó

A screenshot of a computer

Description automatically generated

Hình 22. Dùng Burp Suite để tạo ra sự bất thường trong mạng

A screenshot of a computer

Description automatically generated

**Hình 23**. Phát hiện ra bất thường

A screenshot of a computer

Description automatically generated

**Hình 24.** Kiểm tra lại bằng trace-summary

**5.2 Đánh giá kết quả thực nghiệm**

**5.2.1 Tiêu chí đánh giá**

**-** Độ chính xác: Tính hiệu quả của Zeek IDS trong việc phát hiện và ngăn chặn các cuộc tấn công mạng.

- Thời gian phản ứng: Thời gian phản ứng của Zeek IDS khi phát hiện các mối đe dọa mạng.

- Tính linh hoạt: Khả năng tùy chỉnh và cấu hình Zeek IDS để phát hiện các cuộc tấn công mạng theo nhu cầu cụ thể của tổ chức.

**5.2.2 Thước đo**

**-** Số lượng các cuộc tấn công phát hiện được

- Thời gian phản ứng

**5.3 So sánh với các công cụ liên quan**

**Snort:**

* So với Snort, Zeek IDS có khả năng phân tích chi tiết hơn về lưu lượng mạng và cung cấp thông tin chi tiết về các kết nối mạng và gói tin mạng.

**Suricata:**

* Zeek cho phép người dùng tùy chỉnh và thiết lập các quy tắc phát hiện một cách linh hoạt hơn so với Suricata.

**Chương 6: Kết luận**

Dự án này đã minh chứng khả năng của Zeek IDS trong việc bảo vệ mạng nội bộ trước các mối đe dọa và tấn công mạng. Với những kết quả đạt được và hướng phát triển rõ ràng, Zeek IDS sẽ tiếp tục là một công cụ mạnh mẽ trong việc đảm bảo an ninh mạng cho các tổ chức và doanh nghiệp.