Logo, company name

Description automatically generated

VNCERT   
Công việc của nhóm thực hành trong 5/1/2023 đến 12/1/2023

**MỤC LỤC**

[I. TÓM TẮT VIỆC ĐÃ LÀM 2](#_Toc127060193)

[II. MÔ HÌNH XÂY DỰNG HẠ TẦNG 3](#_Toc127060194)

[III. PHẦN MỀM SPLUNK 4](#_Toc127060195)

[1.1. Tìm hiểu về Splunk 4](#_Toc127060196)

[1.1.1. Splunk là gì? 4](#_Toc127060197)

[1.1.2. Các thành phần chính của Splunk? 4](#_Toc127060198)

[1.2. Cài đặt công cụ 4](#_Toc127060199)

[1.2.1. Cài đặt Docker 4](#_Toc127060200)

[1.2.2. Cài đặt Splunk bằng Docker 5](#_Toc127060201)

[IV. LỖ HỔNG LOG4J 8](#_Toc127060202)

[3.1. Tìm hiểu về Log4j 8](#_Toc127060203)

[3.2. Mức Độ Nguy Hiểm 9](#_Toc127060204)

[3.3. Triễn Khai Và Khai Thác Log4j 9](#_Toc127060205)

[V. LỔ HỖNG ACTIVE DIRECTORY 10](#_Toc127060206)

[4.1. Cài Đặt AD 10](#_Toc127060207)

# TÓM TẮT VIỆC ĐÃ LÀM

Dựng thành công windows server 2016 với lỗ hổng AD

Cài đặt thành công splunk trên ubuntu 18 và dự kiến thay thành ubuntu 20

Cấu hình lỗ hổng log4j trên ubuntu

Về mặt hạn chế: vẫn chỉ đang cài đặt theo các đường dẫn như github, google mà vẫn chưa đọc code sâu về những lỗ hổng trên

Nhiệm vụ dự kiến trong tuần tiếp theo:

* Đọc phân tích code và triễn khai lỗ hổng log4j
* Phân tích đoạn code tạo ra AD dễ bị tổn thương
* Tìm hiểu về Security Operations Center (SOC)

# MÔ HÌNH XÂY DỰNG HẠ TẦNG

Diagram

Description automatically generated

Ubuntu cài phần mềm giám sát spunk

Ubuntu triển khai lỗ hổng Log4j

Windows Server triển khai lỗ hổng Active Directory

# PHẦN MỀM SPLUNK

## Tìm hiểu về Splunk

### Splunk là gì?

* Splunk là một phần mềm giám sát mạng dựa trên sức mạnh của việc phân tích Log. Splunk thực hiện các công việc tìm kiếm, giám sát và phân tích các dữ liệu lớn được sinh ra từ các ứng dụng, các hệ thống và các thiết bị hạ tầng mạng.
* Splunk là một trong những giải pháp SIEM hàng đầu trên thị trường cung cấp khả năng thu thập, phân tích và tương quan giữa nhật ký mạng và máy trong thời gian thực.

### Các thành phần chính của Splunk?

Splunk có 3 thành phần chính: Forwarder, Indexer và Search Head.

* Splunk Forwarder là một agent được cài đặt trên endpoint nhằm mục đích giám sát và nhiệm vụ chính của nó là thu thập dữ liệu và gửi dữ liệu đến máy chủ Splunk. Splunk Forwarder cần rất ít tài nguyên để xử lý nên không ảnh hưởng đến hiệu suất của endpoint.
* Splunk Indexer đóng vai trò chính trong việc xử lý dữ liệu mà nó nhận được từ các forwarders. Splunk Indexer lấy dữ liệu, chuẩn hóa dữ liệu thành các cặp trường-giá trị, xác định kiểu dữ liệu và lưu trữ chúng dưới dạng sự kiện => Dữ liệu đã qua xử lý dễ tìm kiếm và phân tích.
* Splunk Search Head là nơi trong Ứng dụng Tìm kiếm & Báo cáo nơi người dùng có thể tìm kiếm nhật ký được lập chỉ thư mục như hình bên dưới. Khi người dùng tìm kiếm một cụm từ hoặc sử dụng ngôn ngữ Tìm kiếm được gọi là Ngôn ngữ xử lý tìm kiếm Splunk, yêu cầu sẽ được gửi đến bộ lập chỉ mục và các sự kiện có liên quan được trả về dưới dạng các cặp trường-giá trị.

## Cài đặt công cụ

### Cài đặt Docker

* Cài đặt docker ***sudo apt install docker.io***

Text

Description automatically generated

* Kiểm tra phiên bản của docker ***docker --version***



* Chạy docker container với tên “hello world” bằng dòng lệnh ***sudo docker run hello-world***

Docker sẽ tìm kiếm images “hello-world” trên hệ thống của bạn, nếu images “hello-world” chưa tồn tại thì sẽ tải về từ DockerHub. Sau đó, Docker sẽ tạo một images đó và chạy.

Text

Description automatically generated

* Xem danh sách các image Docker đang có trong hệ thống: ***sudo docker images.*** Kết quả hình bên dưới là có một image “hello-world” với phiên bản “latest”.

Text

Description automatically generated

### Cài đặt Splunk bằng Docker

* Tải xuống một image Docker của Splunk từ Docker Hub và cài đặt bằng dòng lệnh **sudo docker pull splunk/splunk:lastest.**
* "docker pull" là lệnh để tải xuống một image Docker từ Docker Hub
* "splunk/splunk:lastest" là tên của image Docker mà bạn muốn tải xuống và phiên bản "lastest".

Text

Description automatically generated

* Xem danh sách các image Docker đang có trên hệ thống và kiểm tra xem image Docker của Splunk đã được cài đặt chưa bằng dòng lệnh ***sudo docker images***

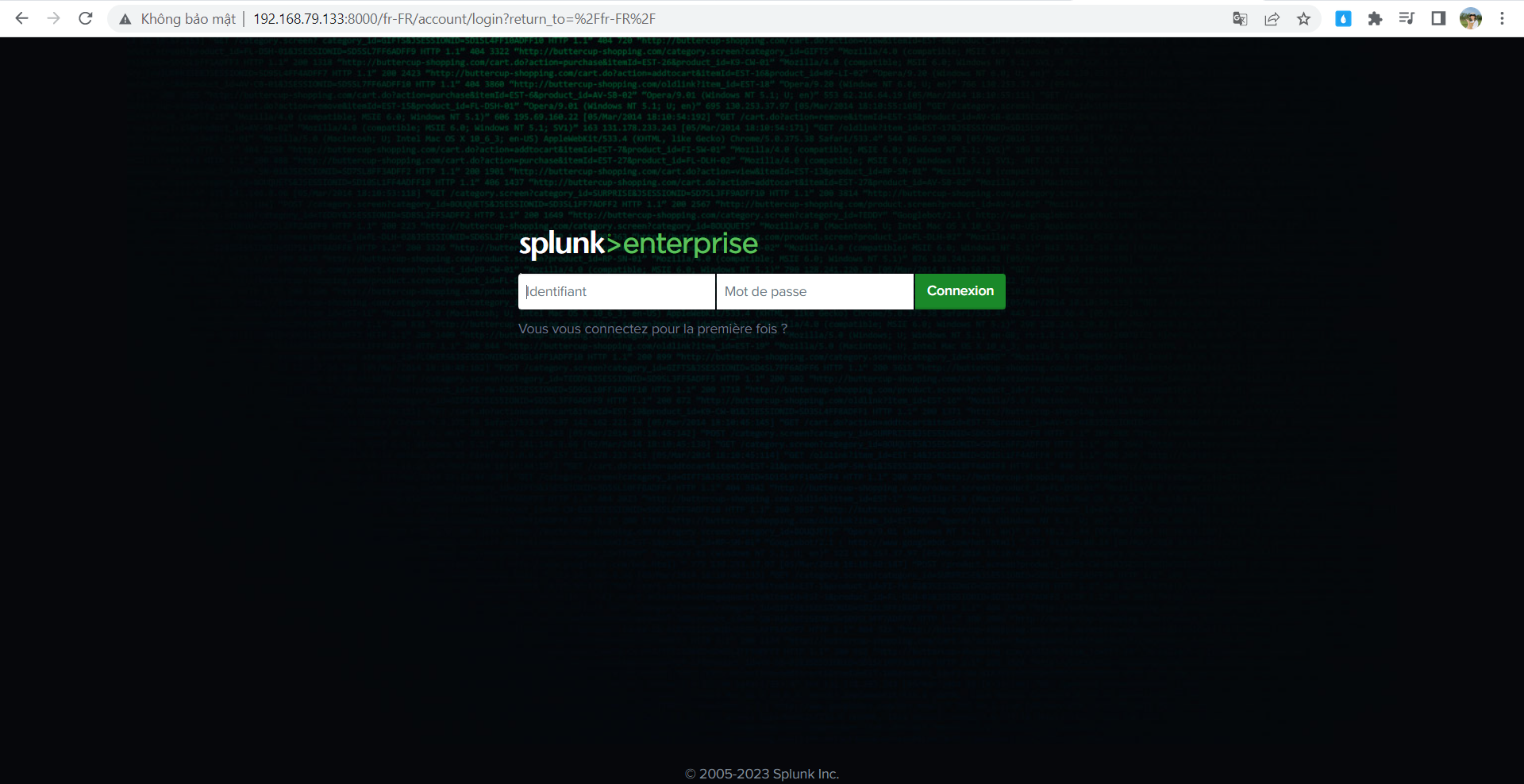
Text

Description automatically generated

* Để chạy một instance của Splunk trong Docker bằng dòng lệnh docker run -d -p 8000:8000 -e SPLUNK\_START\_ARGS='--accept-license' -e SPLUNK\_PASSWORD='<12345678>' splunk/splunk:latest
* "-d" chỉ định rằng Docker container sẽ chạy dưới dạng background process.
* "-p 8000:8000" chỉ định rằng giao diện người dùng của Splunk sẽ được map với cổng 8000 trên host và cổng 8000 trong container.
* "-e SPLUNK\_START\_ARGS='--accept-license'" chỉ định rằng bạn đồng ý với các điều khoản của license của Splunk.
* "-e SPLUNK\_PASSWORD='<12345678>'" chỉ định mật khẩu cho tài khoản admin của Splunk.
* "splunk/splunk:latest" chỉ định tên và phiên bản của Docker image mà bạn muốn chạy.



* Sau đó, truy cập SplunkWeb tại <http://192.168.79.133:8000> với user: admin; pass: <12345678>.



Graphical user interface, application

Description automatically generated

# LỖ HỔNG LOG4J

## Tìm hiểu về Log4j

Log4j2 là một thư viện mã nguồn mở dựa trên Java và thường được tích hợp trên các máy chủ web Apache với chức năng ghi lại nhật ký. Theo các nguồn tin, nhà nghiên cứu Chen Zhaojun của Alibaba đã gửi báo cáo lỗ hổng thực thi mã từ xa Log4j2 (RCE) cho Apache vào ngày 24 tháng 11 năm 2021. Lỗ hổng nghiêm trọng này sau đó đã được gán mã định danh CVE-2021-44228, hay còn được gọi là “Log4Shell”, tác động đến tất cả các phiên bản Log4j2 từ 2.0-beta9 đến 2.14.1.

Lỗ hổng CVE-2021-44228 cho phép kẻ tấn công bên ngoài hệ thống, không cần xác thực, có thể khai thác bằng cách gửi yêu cầu chứa mã khai thác (payload) đến máy chủ đang chạy phiên bản Log4j tồn tại lỗi. Yêu cầu được gửi đi sử dụng JNDI thông qua nhiều dịch vụ bao gồm:

* Lightweight Directory Access Protocol (LDAP)
* Remote Method Invocation (RMI)
* Domain Name System (DNS)

Lỗ hổng Log4j được kích hoạt bởi payload, phía máy chủ sẽ tạo yêu cầu trên JNDI thông qua một trong các dịch vụ do kẻ tấn công kiểm soát. Khi nhận được yêu cầu này, kẻ tấn công sẽ trả về một đường dẫn đến tệp Java class được lưu trữ từ xa, tệp này sau đó sẽ được phía máy chủ chèn vào luồng xử lý và cho phép kẻ tấn công có thể thực thi mã tuỳ ý.

Graphical user interface, text, application, email

Description automatically generated

## Mức Độ Nguy Hiểm

Do tính phổ biến của thư viện Log4j2, rất nhiều hệ thống đã và đang chịu ảnh hưởng từ lỗ hổng CVE-2021-44228 Log4Shell, bao gồm cả những hệ thống, dịch vụ đám mây của Steam, Cloudflare, Twitter, Tesla… Kèm theo rất nhiều mã khai thác công khai được cập nhật trên Github. Hiện tại, lỗ hổng này đang được hacker khai thác rất tích cực.

## Triễn Khai Và Khai Thác Log4j

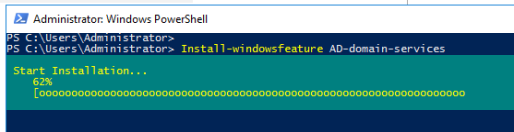
# LỔ HỖNG ACTIVE DIRECTORY

## Cài Đặt AD

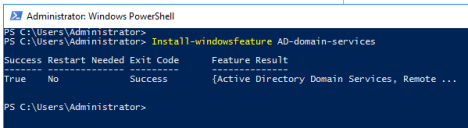
Active Directory là cơ sở dữ liệu tập trung lưu trữ thông tin về các đối tượng trong mạng, chẳng hạn như người dùng, máy tính và máy in. Nó được giới thiệu với Windows 2000 Server và là một thành phần quan trọng của Windows Server kể từ đó. Active directory được sử dụng để quản lý và tổ chức các tài nguyên trong mạng và cung cấp một vị trí tập trung để xác thực và ủy quyền người dùng. Điều này cho phép quản trị viên quản lý quyền truy cập vào tài nguyên mạng và thực thi các chính sách bảo mật một cách nhất quán và hiệu quả.

*# if you didn't install Active Directory yet , you can try*

* *Install-windowsfeature AD-domain-services*

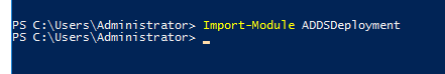


Sau khi quá trình cài AD-domain-services hoàn thành, nếu thành công bạn sẽ thấy như sau.



import thành phần câu lệnh của AD.

* *Import-Module ADDSDeployment*



Sau khi import thành phần triển khai AD, bạn có thể cấu hình và kết thúc quá trình cài đặt hệ thống AD.

Câu lệnh PS một dòng dưới đây sẽ cài đặt AD làm domain controller đầu tiêu trong một forest mới (có nghĩa đây là cài đặt AD đầu tiên trong hệ thống).

Nó sẽ đặt tên cho domain của bạn là **cs.org** (bạn có thể đặt tên domain là bất cứ thứ gì cũng được)

Và nó sẽ đặt tên cho máy chủ là **cs**, đặt tất cả các log và NTDS (mỏ vàng lưu trữ các mật khẩu nội bộ dưới dạng các mã băm) vào trong thư mục **C:\Windows\** .

* *Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\\Windows\\NTDS" -DomainMode "7" -DomainName "cs.org" -DomainNetbiosName "cs" -ForestMode "7" -InstallDns:$true -LogPath "C:\\Windows\\NTDS" -NoRebootOnCompletion:$false -SysvolPath "C:\\Windows\\SYSVOL" -Force:$true*

*# if you already installed Active Directory, just run the script !*

* *IEX((new-object net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1"));*
* *Invoke-VulnAD -UsersLimit 100 -DomainName "cs.org"*

