|  |
| --- |
| **TÊN CÔNG TY**  Công ty TNHH phần mềm nhân hòa |
|  |

**BÁO CÁO KẾT QUẢ CÔNG VIỆC NGÀY**

**Họ và tên:Lê Anh Tú Chức vụ:Thực tập sinh Bộ phận công tác:IT Support**

Thời gian thực hiện:8h-5h30 *Ngày:10 Tháng:04 Năm: 2023*

|  |  |  |
| --- | --- | --- |
| **TT** | **Nội dung công việc** | **Chi tiết công việc** |
| **1** | **Overview Selinux** | 1. **What is Selinux ?**  * SeLinux ( Security-Enhanced Linux ) là một cơ chế bảo mật của hệ thống linux * Selinux cung cấp một cơ chế bảo mật có khả năng kiểm soát chặt chẽ quyền truy cập vào hệ thống cho từng tiến trình và tài nguyên, tăng cường đáng kể tính bảo mật của hệ thống linux * Selinux hoạt động gần giống với Windows defender Firewall trên windows là đều liên quan đến việc kiểm soát truy cập và bảo vệ hệ thống bởi các cuộc tấn công * Được phát triển bởi Cục An ninh quốc gia Hoa Kỳ (NSA) và được tích hợp sẵn vào nhiều bản phân phối Linux như (CentOs, Fedora )  1. **Các trạng thái của Selinux**   **Selinux có 3 chế độ khác nhau gồm : Enforcing, Permissive và Disabled**  **+ Enforcing :** đây là chế độ mặc định sẽ cho phép và thực thi các chính sách bảo mật của Selinux trên hệ thống, ghi log yêu cầu truy cập tại /var/log/audit/audit.log, Sau đó kiểm tra chính sách, nếu ứng dụng không có quyền truy cập thì sẽ bị từ chối và chặn luôn  + **Permissive** : Selinux cho phép truy cập nhưng vẫn ghi log tại /var/log/audit/audit.log  **+ Disabled:** Selinux bị tắt hoàn toàn và không ghi log   1. **Cơ chế hoạt động của Selinux**  * Khi trạng thái Selinux đang ở chế độ bật( cụ thể là enforcing ), khi bạn cài bất kỳ ứng dụng gì lên server, hệ thống sẽ ghi lại các truy cập của ứng dụng vào file nào, thư mục nào, cổng nào trên hệ thống, và khi một ứng dụng được cài đặt nó chỉ được truy cập đến file, thư mục hay cổng được áp dụng trong chính sách bảo mật của Selinux, nếu truy cập của ứng dụng ngoài chính sách bảo mật của Selinux thì ứng dụng đó sẽ bị chặn cài đặt * **Để kiểm tra chính sách mà Selinux đang áp dụng : truy cập vào file /etc/selinux/config**      1. **Cho biết Selinux đang được bật chế độ Enforcing trên hệ thống** 2. **Cho biết đang sử dụng chính sách bảo mật mặc định được cung cấp bởi Selinux và được gọi là chính sách “targeted”. Chính sách này cho phép SELinux áp dụng các quy tắc bảo mật trên 1 số ứng dụng cụ thể hoặc 1 nhóm ứng dụng, chứ không phải trên toàn hệ thống( Lưu ý: các chính sách Selinux dành cho ứng dụng do các lập trình viên đưa vào ứng dụng, không phải bạn )** 3. **Ưu nhược điểm của SELinux**  * **Ưu điểm** * Là cơ chế điều khiển truy xuất có tính bảo mật cao trong việc ngăn chặn truy cập dữ liệu hoặc các chưng trình trái phép * Bảo vệ máy chủ chống lại việc khai thác. Tránh tình trạng leo thang đặc quyền * **Nhược điểm** * Tuy nhiên có những trường hợp SELinux lại gây ra sự phiền phức khi bạn muốn cài một phần mềm mà phần mềm đó lại cần can thiệp sâu vào hệ thống Linux. Do đó bạn cần phải vô hiệu hóa tính năng của SELinux |
| **2** |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |

*Khó khăn, vướng mắc, góp ý:*