Linux & Cyber Security

Scenari e soluzioni in contesti professionali

Palermo, 28/10/2023

Comprensione del concetto di sicurezza su Linux

Si da sempre per scontato che i sistemi con kernel Linux siano sempre in ogni caso più sicuri «di default», e sembra essere uno di quei pre-concetti rimasto praticamente immutato da sempre.

Facendo la premessa fondamentale dove non esiste un concetto assoluto di sicurezza, alcune statistiche dovrebbero far comprendere all'intera audience informatica qual è lo scenario che si presenta.

I dati che seguiranno sono stati raccolti con la massima trasparenza, cercando di evidenziare solo dei dati quantitativi.

Che cosa dicono i numeri

Dati riferiti all'anno 2022, dal 01/01 al 31/12

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	1222
2	Fedora	Fedoraproject	OS	947
3	Debian Linux	Debian	OS	931
4	Windows Server 2019	Microsoft	OS	552
5	Windows 10	Microsoft	OS	521
6	Windows Server 2016	Microsoft	OS	514
7	Windows 11	Microsoft	OS	498
8	Windows Server 2022	Microsoft	OS	422
9	Windows Server 2012	Microsoft	OS	413
10	Macos	Apple	OS	379

C’è da preoccuparsi..?

Salta fuori che il sistema operativo con più vulnerabilità di tutti è Android, distribuzione che non ha bisogno certo di presentazioni, seguito a ruota da Fedora e Debian.
Ovviamente, non è il solo numero di vulnerabilità ad essere puramente indicativo su un ipotetico indice di insicurezza di un sistema, infatti ci sono altre variabili quali:

- Indice di gravità delle singole vulnerabilità.
- Rapidità con la quale queste vengono risolte o mitigate, fattore importante soprattutto nelle community Open, le quali sono molto reattive nell’erogare soluzioni tempestive.
- A quali tipologie di codice o genericamente di software è associata una specifica vulnerabilità.

Come trovare delle soluzioni per la realtà operativa

In ambito aziendale vengono attuate delle contromisure e usati degli strumenti che vanno a prevenire e mitigare quelli che possono essere quei problemi dovuti ad una cattiva gestione delle risorse, mancanza di policy di security o misconfiguration.

Ragionevolmente, ogni qualvolta di va ad integrare una soluzione di sicurezza si devono valutare attentamente gli impatti e l'effort necessario affinchè tutte le soluzioni possano funzionare senza avere troppi vincoli o lati negativi

Strumenti

Il focus sarà su tre componenti interessanti sotto il profilo della sicurezza:

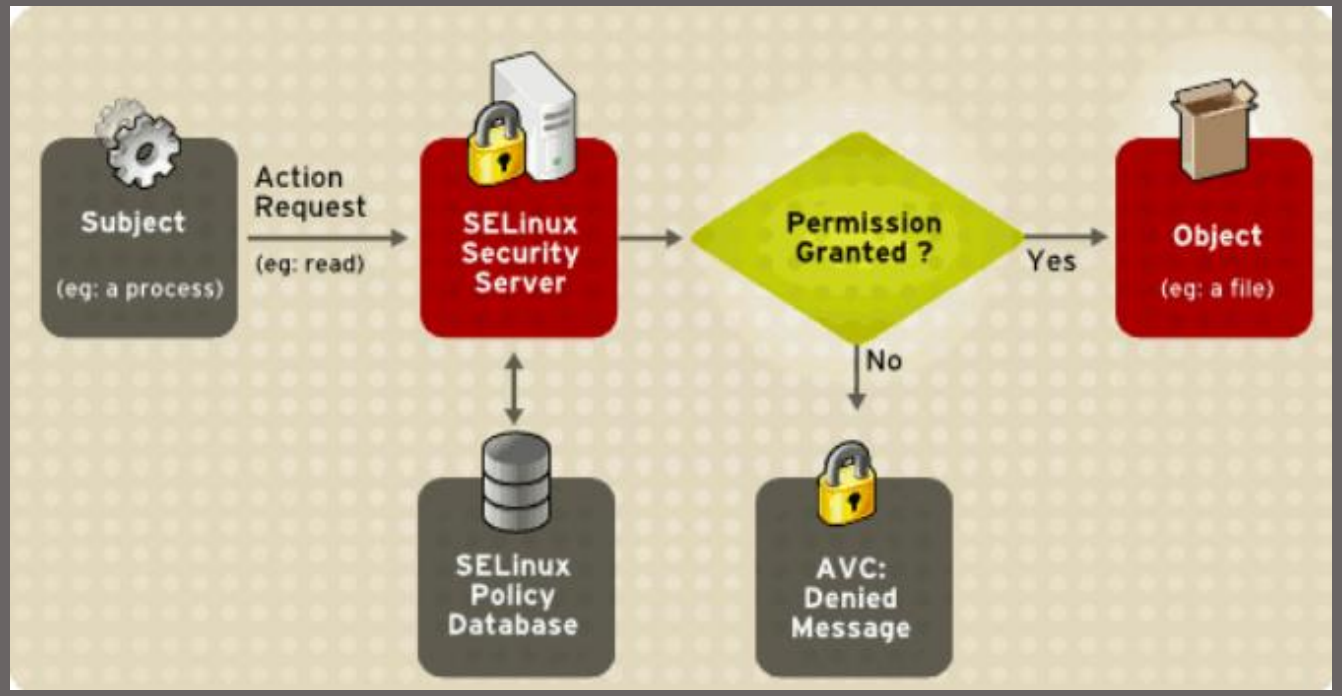
- SELinux – Securiry Enhanced Linux
- PAM – Pluggable Authentication Module
- ClamAV – Clam Antivirus tool

SELinux

Sviluppato dall'NSA come serie di patch per il kernel Linux, SELinux fornisce un’architettura flessibile per il controllo degli accessi obbligatori MAC – Mandatory Access Control - integrato nel kernel Linux.
Nel DAC - Discretionary Access Control - standard di Linux, un'applicazione o un processo in esecuzione come utente dispone delle autorizzazioni dell'utente per oggetti come file, socket e altri processi, mentre con SELinux si va a definire l'accesso di ciascun processo, utente, file e applicazione sul sistema. L'esecuzione di un kernel attraverso MAC protegge il sistema da applicazioni potenzialmente dannose o con problemi che possono danneggiare o peggio compromettere irreparabilmente l’intero sistema.

Come per praticamente tutti i metodi MAC, anche SELinux lavora con l'assegnazione delle label e proprio l'applicazione del tipo specifico di label è uno dei concetti cardine in SELinux associandone una a ciascun file, processo e porta di un sistema; queste costituiscono un metodo logico per raggruppare gli oggetti e vengono gestite dal kernel durante la fase di avvio.

SELinux



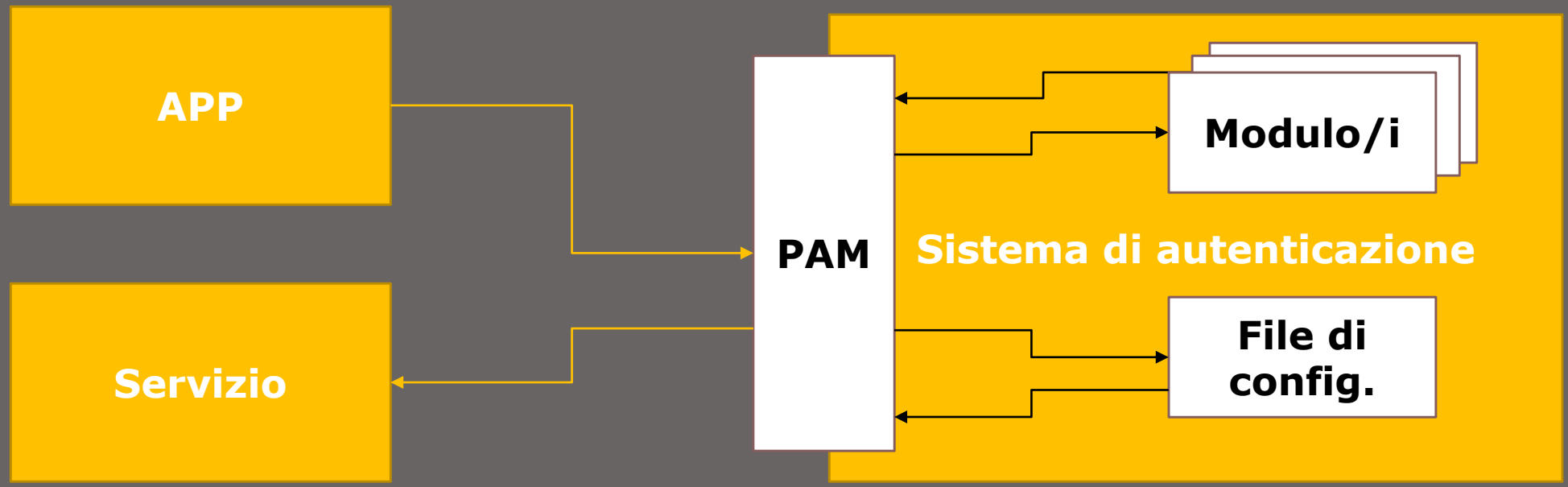
Quando un'applicazione o un processo effettua una richiesta d'accesso a un oggetto, SELinux consulta la cache dei vettori d'accesso (AVC) dove sono memorizzate le autorizzazioni per soggetti e oggetti. Se non è possibile determinarne l'accesso, SELinux invia la richiesta al server di sicurezza che verifica il contesto di sicurezza dell'app o del processo e quello del file. Il contesto di sicurezza applicato è quello disponibile nel database dei criteri di SELinux e su quei criteri l'autorizzazione viene concessa / negata.

PAM: Pluggable Authentication Module

PAM è un meccanismo per integrare più metodi di autenticazione a basso livello portandone la gestione ad alto livello anche tramite API, permettendo ai programmi che necessitino di una forma di autenticazione, di essere creati in modo indipendentemente dallo schema di autenticazione richiesto, il che lo rende molto flessibile. Divide i compiti di autenticazione in quattro gruppi di gestione indipendenti:

- Password management
- Session management
- Account management
- Authentication management

PAM: Pluggable Authentication Module



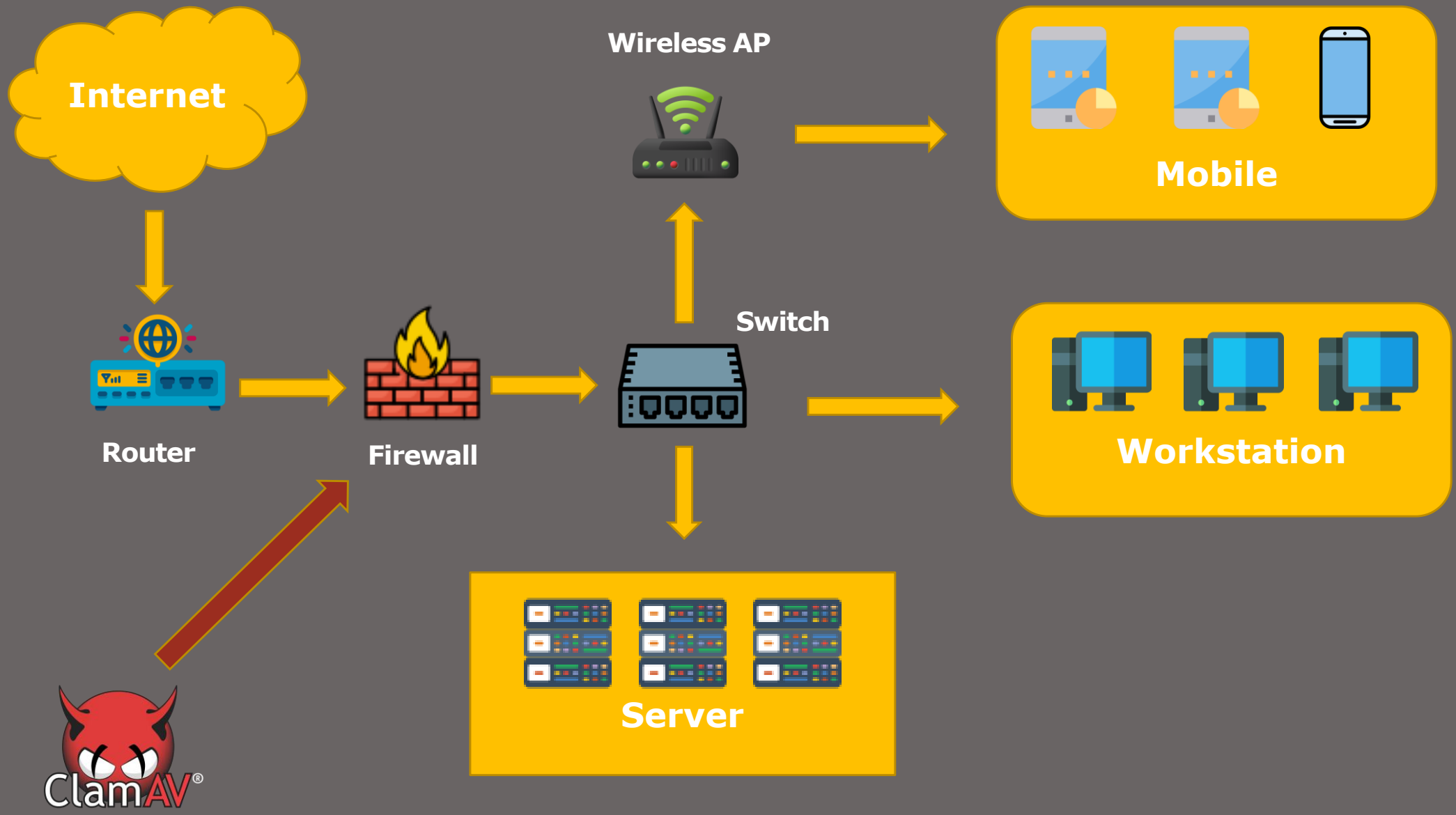
L'app si interfaccia con la libreria PAM, che consulta il contenuto del file di configurazione relativo e va a caricare i moduli, che mettono in funzione il meccanismo di autenticazione.
Il dati richiesti all'utente e le relative risposte, sono scambiati tra l'applicazione ed i moduli attraverso un opportuno meccanismo di dialogo fornito dalla libreria PAM.

Clam AV

Per chi già conosce il mondo Linux, probabilmente la parola «*antivirus*» potrebbe suonare strana: negli anni, sebbene in numero minore rispetto ai sistemi Windows le minacce informatiche sono comunque cresciute e avere uno strumento di controllo aggiuntivo può rivelarsi fondamentale in molti contesti.

ClamAV è un antivirus open source multipiattaforma per rilevare trojan,virus, malware in genere; nasce inizialmente come scanner antimalware dedicato ai server di posta, ma allarga presto la sua platea integrandosi sia come plug-in su varie piattaforme che come software standalone.

Consideriamo qui di seguito una delle eventuali implementazioni in una semplice architettura di rete in un contesto di produzione:


Internet
Wireless AP
Mobile
Router
Firewall
Switch
Workstation
Server
ClamAV®

Clam AV

Perché dunque si dovrebbe installare una componente antivirus su un dispositivo di rete?
Principalmente mettiamo due motivi cardine:

- avere la necessità di filtrare il traffico di rete indirizzato anche ad altri sistemi non Linux, che possono essere infettati o comunque essere compromessi.
- in alcune condizioni di reti miste (specialmente Linux / Windows) impedire che l'ambiente Linux, pur rimanendo intaccato da eventuali infezioni, possa fare da «portatore sano» che dunque faciliti l'ingresso di eventuali malware che hanno in target gli ambienti Windows, al netto delle misure singole prese per la protezioni di questi ultimi.

Domande?

Grazie per l’attenzione!