EDGAR ALVARADO

DEVOPS BOOTCAMP

DESAFIO 17

OBJETIVO

Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) para una organización que aloja aplicaciones en la nube.

Desplegar un conjunto de controles de seguridad que incluyan medidas técnicas, organizativas y de gestión para reducir los riesgos asociados con el alojamiento de aplicaciones en la nube.

Incorporar un plan de continuidad del negocio, que permita recuperar los servicios en caso de desastres naturales o fallas en la infraestructura.

El SGSI será diseñado para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para cumplir con las normativas y estándares de seguridad aplicables.

LINUX

Objeto de estudio: Sistema operativo + web server + base de datos.

1. Implementar un programa completo del ciclo PDCA que contenga al menos dos aspectos de seguridad y desarrollar, un objetivo o más, en cada aspecto de seguridad seleccionado (en total, 2 objetivos a desarrollar):

a. Identificación y autentificación.

b. Autorización.

c. Integridad.

d. Auditoría.

CONSIDERACIONES

• Planificar: Elaborar un "plan estandarizado" para aplicar a futuros despliegues. Esto incluye la identificación de un problema, una oportunidad de mejora o la creación de un plan de acción para abordarlo.

• Do (Hacer): Implementar y documentar las tareas a realizar según lo planificado. Realizar un paso a paso que incluya ficheros de configuraciones, instalación de paquetes, capturas de pantallas, y otros.

• Check: Realizar una verificación de las tareas realizadas en la etapa "Do". Indicar, al menos, 2 puntos a mejorar incluyendo aspectos que no se hayan tenido en cuenta en la etapa de "planificar".

• Actuar: Elaborar un checklist para futuros despliegues de la imagen seleccionada, que incluya aspectos resultantes de la etapa "check".

Implementación del ciclo PDCA:

a) Planificar:

Objetivo 1 (Identificación y autenticación): Implementar autenticación de dos factores (2FA) para todos los usuarios que acceden al sistema.

Objetivo 2 (Auditoría): Establecer un sistema de registro y monitoreo de eventos de seguridad críticos en todos los componentes del sistema.

Plan estandarizado:

Evaluar los sistemas actuales de autenticación y auditoría.

Identificar las herramientas necesarias para implementar 2FA y el sistema de registro.

Definir políticas de seguridad para el uso de 2FA y la gestión de logs.

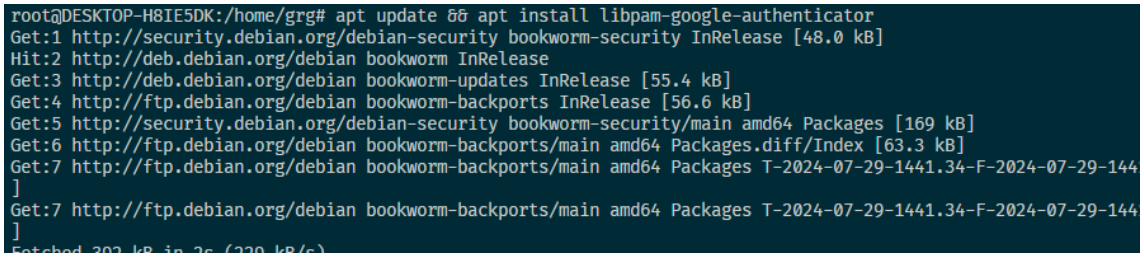
Establecer un cronograma para la implementación y pruebas.

Asignar recursos y responsabilidades.

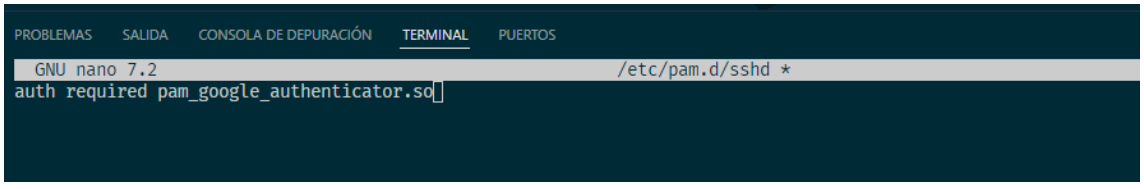
b) Hacer:

Objetivo 1: Implementación de 2FA

Instalar y configurar Google Authenticator en el servidor Linux



Configurar PAM para utilizar Google Authenticator



Configurar SSH para permitir 2FA

```
 GNU nano 7.2                                    /etc/ssh/sshd_config *
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

ChallengeResponseAuthentication yes
UsePAM yes
```

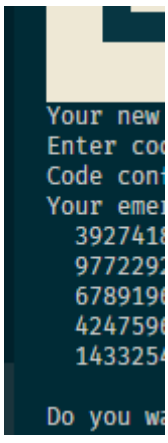
Reiniciar el servicio SSH

```
root@DESKTOP-H8IE5DK:/home/grg# service ssh restart
Restarting OpenBSD Secure Shell server: sshd.
root@DESKTOP-H8IE5DK:/home/grg#
```

Configurar Google Authenticator para cada usuario

```
root@DESKTOP-H8IE5DK:/home/grg# google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/root@DESKTOP-H8
6issuer%3DDESKTOP-H8IE5DK
```



Objetivo 2: Implementación del sistema de auditoría

Instalar y configurar auditd

```
root@DESKTOP-H8IE5DK:/home/grg# apt install auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
```

Configurar reglas de auditoría

```
 GNU nano 7.2                                                    /etc/audit/audit.rules *
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
--backlog_wait_time 60000
-w /etc/passwd -p wa -k identity
-w /etc/group -p wa -k identity
-w /var/log/auth.log -p wa -k auth_logs
-w /etc/ssh/sshd_config -p wa -k sshd_config
```

Configurar la retención de logs

```
 GNU nano 7.2                                                    /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
transport = TCP
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
q_depth = 2000
overflow_action = SYSLOG
```

c) Verificar:

Pruebas de 2FA:

Intentar iniciar sesión SSH sin 2FA (debería fallar).

Iniciar sesión SSH con 2FA (debería tener éxito).

Verificar que todos los usuarios tienen 2FA configurado.

Pruebas de auditoría:

Realizar cambios en los archivos monitoreados.

Verificar que los eventos se registran correctamente en /var/log/audit/audit.log.

Puntos a mejorar:

Implementar una solución de backup para los logs de auditoría.

Establecer un proceso de revisión periódica de los logs.

d) Actuar:

Checklist para futuros despliegues:

Verificar la compatibilidad del sistema con Google Authenticator.

Asegurar que todos los usuarios están capacitados en el uso de 2FA.

Confirmar que las reglas de auditoría cubren todos los eventos críticos.

Implementar un sistema de backup y rotación de logs.

Establecer un proceso de revisión mensual de logs y eventos de seguridad.

Documentar y actualizar las políticas de seguridad relacionadas con 2FA y auditoría.

Realizar pruebas de penetración para validar la efectividad de las medidas implementadas.

Programar revisiones trimestrales del SGSI para mantenerlo actualizado.