Auditoría sistemas operativos GNU/Linux e UNIX: lynis

ESCENARIO

Máquina virtual ou física:
RAM ≥ 4096MB CPU ≥ 2 PAE/NX habilitado
ISO/CD/DVD/USB: kali-linux amd64
REDE: DHCP (NAT)
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **[1] Lynis**
- **[2] Práctica SI Apache WAF-ModSecurity**
- **[3] Servidor Web Apache**

Máquina virtual Kali amd64

1. ## lynis (Auditar o sistema operativo)

   Na contorna gráfica abrir un terminal e executar:

   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

   root@kali:~# apt update || apt-get update #Actualizar repositorios declarados no ficheiro */etc/apt/souces.list* e nos ficheiros existentes no directorio */etc/apt/sources.list.d*
   Así, unha vez realizada a consulta dos ficheiros existentes nas rutas anteriores, descárganse uns ficheiros coas listas de paquetes posibles a instalar. Estes ficheiros son gardados en */var/lib/apt/lists*
   root@kali:~# apt search lynis || apt-cache search lynis #Buscar nas anteriores listas descargadas en */var/lib/apt/lists* paquetes que coincidan co patrón de búsqueda *lynis*. A saída do/s comando/s amosan o nome do/s paquete/s e unha pequena descrición do/s mesmo/s.
   root@kali:~# apt show lynis || apt-cache show lynis #Amosa información sobre o paquete lynis, incluídas as súas dependencias, instalación e tamaño de descarga, fontes nas que está dispoñible o paquete, descrición do contido dos paquetes e moito máis.

   > Lynis é unha ferramenta de auditoría para reforzar os sistemas baseados en GNU/Linux e Unix. Analiza a configuración do sistema e crea unha visión xeral da información do sistema e cuestións de seguridade empregadas por auditores profesionais. Pode axudar nas auditorías automatizadas.

   root@kali:~# apt -y install lynis || apt-get -y install lynis #Instalar o paquete de nome *lynis*. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
   root@kali:~# lynis audit system #Execución para auditar o sistema operativo. Ao final da execución amosa un resumo (-[Lynis 3.0.8 Results]-) onde podemos conseguir suxerencias para mellorar a seguridade (bastionado/hardening) do sistema operativo.

   ```
   * Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
     https://cisofy.com/lynis/controls/HTTP-6640/

   * Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
     https://cisofy.com/lynis/controls/HTTP-6643/

   * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
     https://cisofy.com/lynis/controls/LOGG-2154/
   ```

   Tamén amosa un número en porcentaxe indicando o nivel do hardening do sistema operativo (Lynis security scan details):

   ```
   ================================================================================

   Lynis security scan details:

   Hardening index : 61 [############        ]
   Tests performed : 261
   Plugins enabled : 1

   Components:
   - Firewall               [V]
   - Malware scanner        [X]

   Scan mode:
   Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

   Lynis modules:
   - Compliance status      [?]
   - Security audit         [V]
   - Vulnerability scan     [V]

   Files:
   - Test and debug information      : /var/log/lynis.log
   - Report data                     : /var/log/lynis-report.dat

   ================================================================================

   Lynis 3.0.8

   Auditing, system hardening, and compliance for UNIX-based systems
   (Linux, macOS, BSD, and others)

   2007-2021, CISOfy - https://cisofy.com/lynis/
   Enterprise support available (compliance, plugins, interface and tools)
   ```

2. **Solucionar Suxerencia auditada: Instalar ModSecurity [2]**

root@kali:~# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
root@kali:~# apt search modsecurity #Buscar calquera paquete que coincida co patrón de búsqueda modsecurity
root@kali:~# apt -y install libapache2-mod-security2 #Instalar o paquete libapache2-mod-security2, é dicir, instalar o WAF modsecurity intregrado como módulo para o servidor web apache2. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
root@kali:~# cat /etc/apache2/mods-available/security2.conf #Ver o contido do ficheiro security2.conf, o cal cargarase ao activar o módulo security2 (modsecurity)

```
    <IfModule security2_module>
          # Default Debian dir for modsecurity's persistent data
          SecDataDir /var/cache/modsecurity

          # Include all the *.conf files in /etc/modsecurity.
          # Keeping your local configuration in that directory
          # will allow for an easy upgrade of THIS file and
          # make your life easier
          IncludeOptional /etc/modsecurity/*.conf

          # Include OWASP ModSecurity CRS rules if installed
          IncludeOptional /usr/share/modsecurity-crs/*.load
    </IfModule>
```

root@kali:~# mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf #Renomear o ficheiro necesario para cargar a configuración do módulo security2 (modsecurity).
root@kali:~# sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/' /etc/modsecurity/modsecurity.conf #Modificar a directiva **SecRuleEngine**. Por defecto configúrase modsecurity en modo detección **(DetectionOnly)**, polo cal soamente detecta ataques pero non actúa sobre o detectado.

root@kali:~# sed -i 's/SecAuditLogParts ABDEFHIJZ/SecAuditLogParts ABEFHIJKZ/' /etc/modsecurity/modsecurity.conf #Modificar a directiva **SecAuditLogParts**.

Por defecto configúrase modsecurity coa opción D que non está implementada e sen a opción K, a cal permite ver nos logs unha lista completa de todas as regras que coincidían (unha por liña) na orde en que foron coincidentes. As regras están totalmente cualificadas e, polo tanto, mostrarán accións herdadas e operadores predeterminados. Compatible a partir da versión 2.5.0.

root@kali:~# a2enmod security2 #Habilitar o módulo security2 que permite activar a configuración do WAF ModSecurity
root@kali:~# /etc/init.d/apache2 restart #Reiniciar o servidor web Apache.
root@kali:~# tail -f /var/log/apache2/modsec_audit.log #Deixar aberto o ficheiro /var/log/apache2/modsec_audit.log para lectura, comenzando a ver polas 10 últimas liñas.

Comprobar que a suxerencia auditada non aparece executando, nunha nova consola de *root*, unha nova auditoría do sistema operativo co comando *lynis audit system*

Ricardo Feijoo Costa