Travaux pratiques – Renforcer un système Linux

Objectifs

Montrer comment utiliser un outil d'audit de sécurité pour renforcer un système Linux.

Contexte/Scénario

L'audit d'un système pour détecter des erreurs de configuration ou des services non protégés est un élément primordial du renforcement de ce système. Lynis est un outil open source d'audit de sécurité disposant d'un jeu de scripts automatisés conçus pour tester un système Linux.

Ressources requises

- Ordinateur équipé d'Ubuntu 16.04 Desktop LTS dans une machine virtuelle VirtualBox or VMware

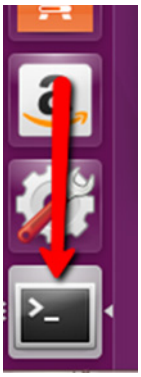
Étape 1 : Ouvrez une fenêtre de terminal dans Ubuntu.

a. Connectez-vous à Ubuntu à l'aide des informations d'identification suivantes :

Utilisateur : **cisco**

Mot de passe : **password**

b. Cliquez sur l'icône du terminal pour ouvrir une fenêtre de terminal.



Étape 2 : L'outil Lynis

a. À l'invite de commandes, saisissez la commande suivante pour accéder au répertoire de Lynis :

```
cisco@ubuntu:~$ cd Downloads/lynis/
```

```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

b. À l'invite de commandes, saisissez la commande suivante, puis le mot de passe **password** lorsque vous y êtes invité :

```
cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
```

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info

[ Lynis 2.2.0 ]

################################################################################
  comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profile file (./default.prf)...
  - Program update status...                                  [ NO UPDATE ]

[+] Helper: update
------------------------------------
```

Cette commande permet de vérifier que vous disposez de la version la plus récente et d'effectuer une mise à jour de l'outil à la date de réalisation de ces travaux pratiques.

Étape 3 : Lancez l'outil.

a. Saisissez la commande suivante dans le terminal, puis appuyez sur **Entrée** :

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco

[ Lynis 2.2.0 ]

################################################################################
  comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]

  -------------------------------------------------------
  Program version:           2.2.0
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  16.04
  Kernel version:            4.4.0
  Hardware platform:         x86_64
  Hostname:                  ubuntu
  Auditor:                   cisco
  Profile:                   ./default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
```

Comme dans l'illustration ci-dessus, l'outil lancera l'audit an assignant le rôle d'auditeur à l'utilisateur **cisco**.

Remarque : vous recevrez des **avertissements**.

b. Pour passer à l'étape suivante de l'audit, appuyez sur **Entrée**. Vous recevrez des avertissements analogues à ceux illustrés ci-dessous.

```
[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ WARNING ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 23 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 37 enabled services
  - Check startup files (permissions)                         [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

c. Vous recevrez des suggestions analogues à celles illustrées ci-dessous.

```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts                              [ OK ]
  - Checking for non-unique UIDs                               [ OK ]
  - Checking consistency of group files (grpck)                [ OK ]
  - Checking non unique group ID's                             [ OK ]
  - Checking non unique group names                            [ OK ]
  - Checking password file consistency                         [ OK ]
  - Query system users (non daemons)                           [ DONE ]
  - Checking NIS+ authentication support                       [ NOT ENABLED ]
  - Checking NIS authentication support                        [ NOT ENABLED ]
  - Checking sudoers file                                      [ FOUND ]
    - Check sudoers file permissions                           [ OK ]
  - Checking PAM password strength tools                       [ SUGGESTION ]
  - Checking PAM configuration files (pam.conf)                [ FOUND ]
  - Checking PAM configuration files (pam.d)                   [ FOUND ]
  - Checking PAM modules                                       [ FOUND ]
  - Checking LDAP module in PAM                                [ NOT FOUND ]
  - Checking accounts without expire date                      [ OK ]
  - Checking accounts without password                         [ OK ]
  - Checking user password aging (minimum)                     [ DISABLED ]
  - Checking user password aging (maximum)                     [ DISABLED ]
  - Checking expired passwords                                 [ OK ]
```

d. Vous recevrez une notification pour chaque partie configurée qui présente une faiblesse (WEAK), comme illustré ci-dessous.

```
[+] Banners and identification
------------------------------------
  - /etc/motd                                                  [ NOT FOUND ]
  - /etc/issue                                                 [ FOUND ]
    - /etc/issue contents                                      [ WEAK ]
  - /etc/issue.net                                             [ FOUND ]
    - /etc/issue.net contents                                  [ WEAK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

e. Vous recevrez des suggestions détaillées en vue d'améliorer votre sécurité, ainsi qu'une synthèse finale précisant l'emplacement du fichier journal.

```
  Lynis security scan details:

  Hardening index : 56 [###########         ]
  Tests performed : 188
  Plugins enabled : 0

  Quick overview:
  - Firewall [X] - Malware scanner [X]

  Lynis Modules:
  - Compliance Status    [NA]
  - Security Audit       [V]
  - Vulnerability Scan   [V]

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

Étape 4 : Analyse des résultats

a. Faites défiler l'écran vers le haut pour atteindre la section des résultats lorsque l'outil a terminé son analyse.

   Combien d'avertissements avez-vous reçus ?

   Combien de suggestions avez-vous reçues ?

b. Faites défiler les suggestions et sélectionnez-en une. Recherchez une suggestion que vous pouvez appliquer pour résoudre le problème.

   Quel problème choisissez-vous de résoudre ?

   Quelle est la solution qui vous est suggérée ?

Références

Lynis : https://cisofy.com/lynis/