AIX et CIS benchmark

duo gagnant pour améliorer la sécurité

Marie-Lorraine Bontron | IT Specialist, Unix on Power
Genève | 14 juin 2018

IBM **Services**

IBM

Agenda

Une étude du cabinet d'audit et de conseil KPMG sur 60 entreprises révèle…

Tribune deGenève 30 mai 2017

Genève Suisse Monde **Économie** Sports Culture Auto High-Tech People Savoir Vivre Plus

Entreprises Argent & finances Emploi & formation Bourse Chroniques Images

88% des entreprises victimes de cyberattaques

Suisse Au cours des douze derniers mois, près de 9 entreprises suisses sur 10 ont été victimes de cyberattaques, contre 54% l'année précédente, selon une enquête de KPMG.

Elles sont 27%

à s'être fait dérober des données confidentielles de clients ou de partenaires

(contre 16% un an auparavant)

Chez plus de la moitié (56%) l'assaut a provoqué une interruption de l'activité commerciale.

Même phénomène dans le monde virtuel que dans le monde réel, les petites et moyennes entreprises (PME), plus vulnérables, deviennent des cibles privilégiées.

Tribune de Genève

Prise de conscience du probléme

- Besoin d’améliorer la sécurité de tous les systèmes
- Les serveurs AIX, traditionnellement “protégés” dans l’intranet de l’entreprise sont aussi concernés
- Discussion ”cordiale” nécessaire entre les responsables systèmes et les responsables securité

Presentation du CIS

Centre for Internet Security

The CIS:

CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities

Formed in October 2000, by a group of IT Security leaders from large governement agencies, large end-user companies and IT Security Service and software companies

The CIS Vision:

Leading the global community to secure our connected world

CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks

The CIS Mission:

Identify, develop, validate, promote, and sustain best practice solutions for cyber defense

Build and lead communities to enable an environment of trust in cyberspace

https://www.cisecurity.org/

CIS … quelques membres des premiers jours

Aujourd'hui

Gouvernement

- NIST - National Institute of Standards and Technology
- Federal Reserve System
- State of Maryland
- NASA
- US Dept of Justice
- Communications Security Establishment (Canada)
- Royal Canadian Mounted Police
- Australian Nat'l Audit Ofc
- Infocomm Development Authority of Singapore
- NSA …

Secteur privé

- Deutsche Telekom T-Com
- Bank of Montreal
- Caterpillar
- Swiss Reinsurance Company
- Agilent Technologies
- Shell Info. Tech. Int'l
- PeopleSoft ...

Universités

- Virginia Tech
- Monash University (Australia)
- Blenkinge Inst. of Technology (Sweden)
- University of California, SF
- New York University …

Consulting / Services

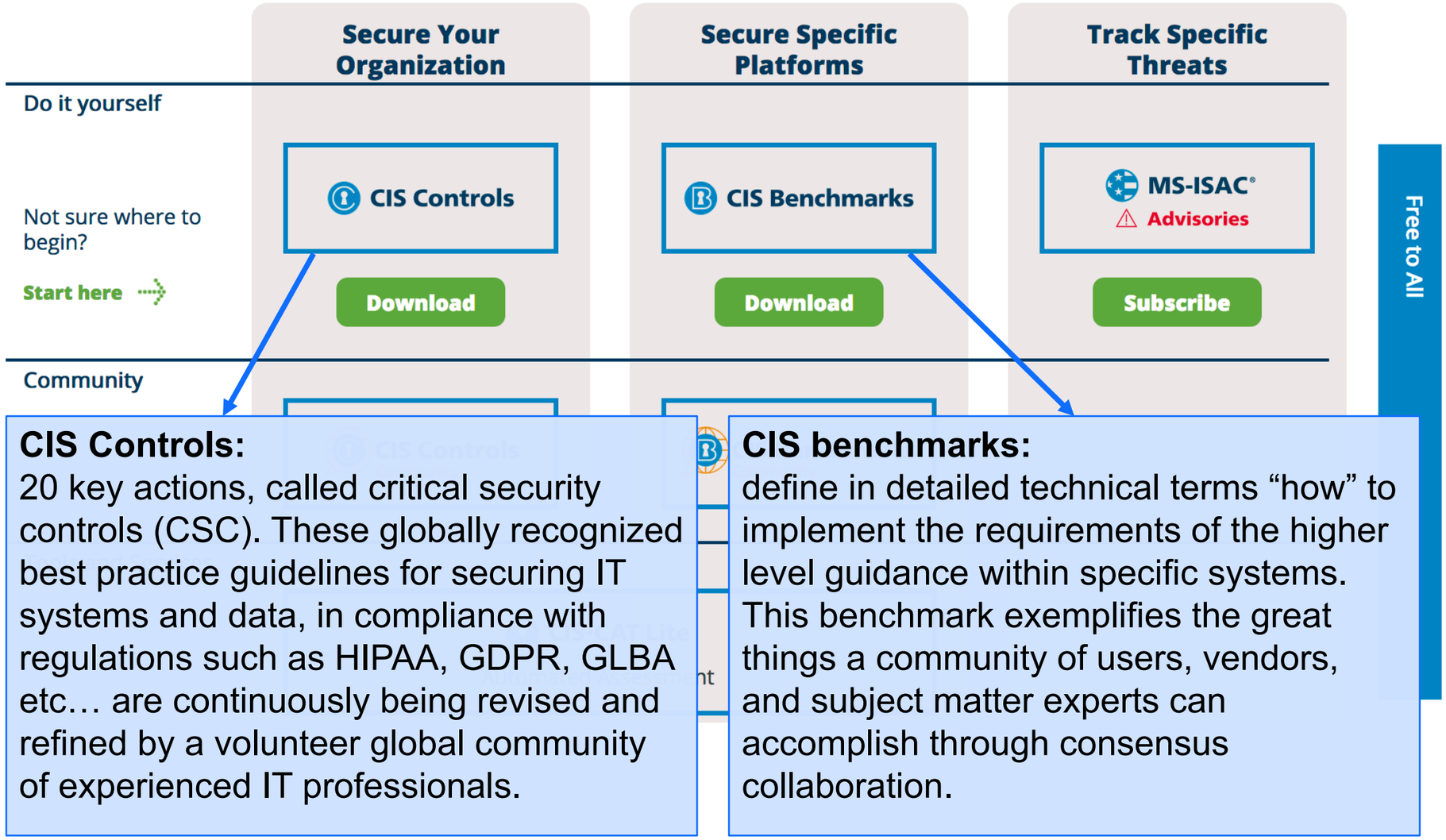
- IBM Consulting
- Configuresoft
- ISS
- Symantec
- BindView
- NetIQ …

Vendeurs de logiciels

- Microsoft
- Sun
- HP
- Cisco
- Oracle
- AOL ...

https://www.cisecurity.org/

Cybersecurity tools proposées par le CIS



CIS Controls:
20 key actions, called critical security controls (CSC). These globally recognized best practice guidelines for securing IT systems and data, in compliance with regulations such as HIPAA, GDPR, GLBA etc… are continuously being revised and refined by a volunteer global community of experienced IT professionals.

CIS benchmarks:
define in detailed technical terms “how” to implement the requirements of the higher level guidance within specific systems. This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration.

https://www.cisecurity.org/

CIS benchmarks

Why?

Pourquoi adopter les recommendations du CIS ?

- Organisme indépendant
- Mondialement reconnu
- Multi-plateformes : Linux, Apple, AIX, Windows, mais aussi Apache, TomCat, DB2, Oracle, Cisco switches…
- Mise à jour régulière par une communauté d'expert

IBM propose PowerSC, framework disponible sur Power pour AIX et Linux on Power
https://www.ibm.com/us-en/marketplace/powersc

CIS Benchmark
Implementation sur AIX

version

download

Existe pour

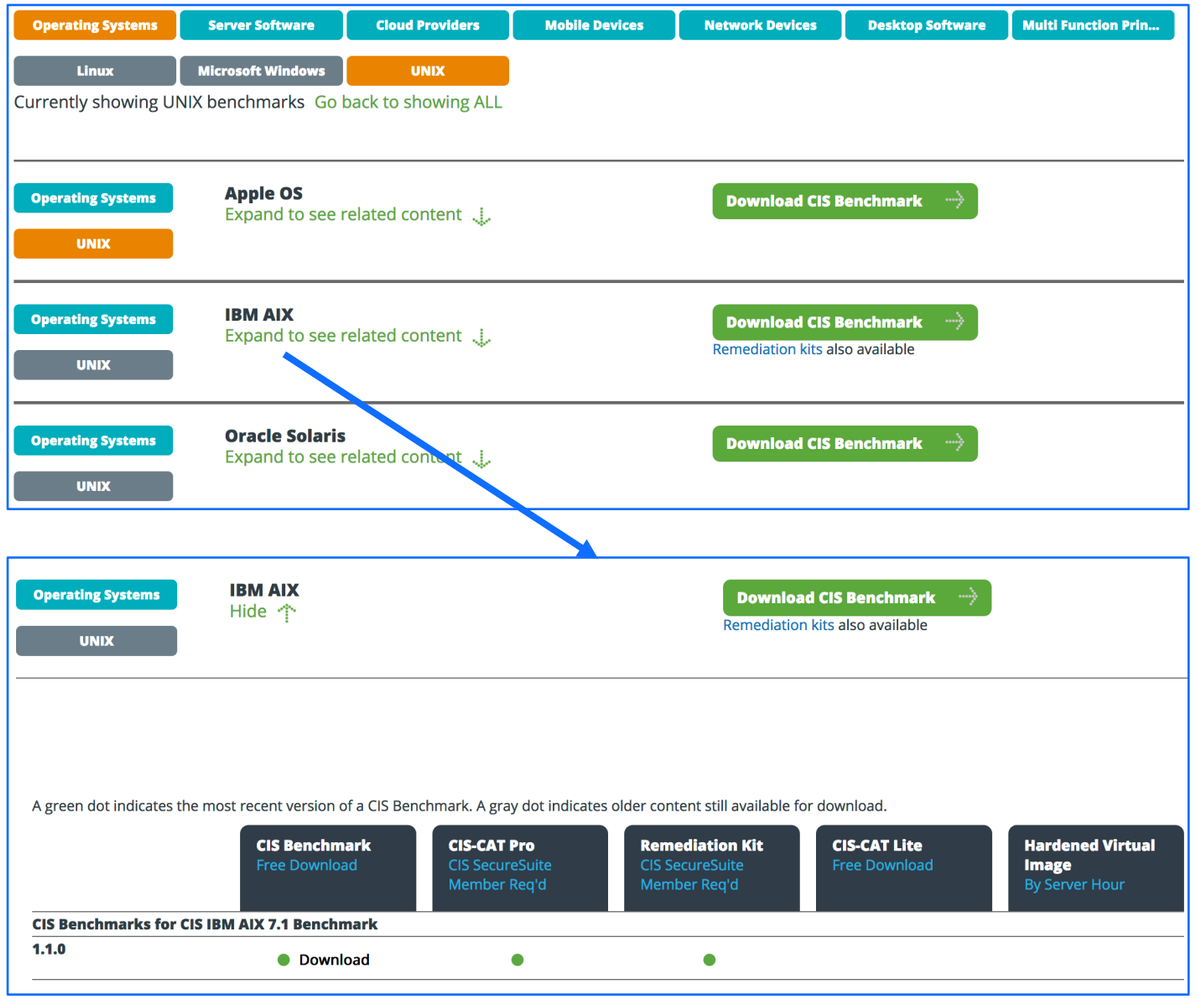
- AIX 5.3 / 6.1
- AIX 7.1

Version pour 7.2 en demande dans la communauté (dernière en date 28.5.18)

=> Version 7.1 applicable

Plusieurs IBMers ont participé à la rédaction

https://www.cisecurity.org/benchmark/ibm_aix/



Que trouve t'on dans le pdf...

Plus de 200 recommendations

Section 3

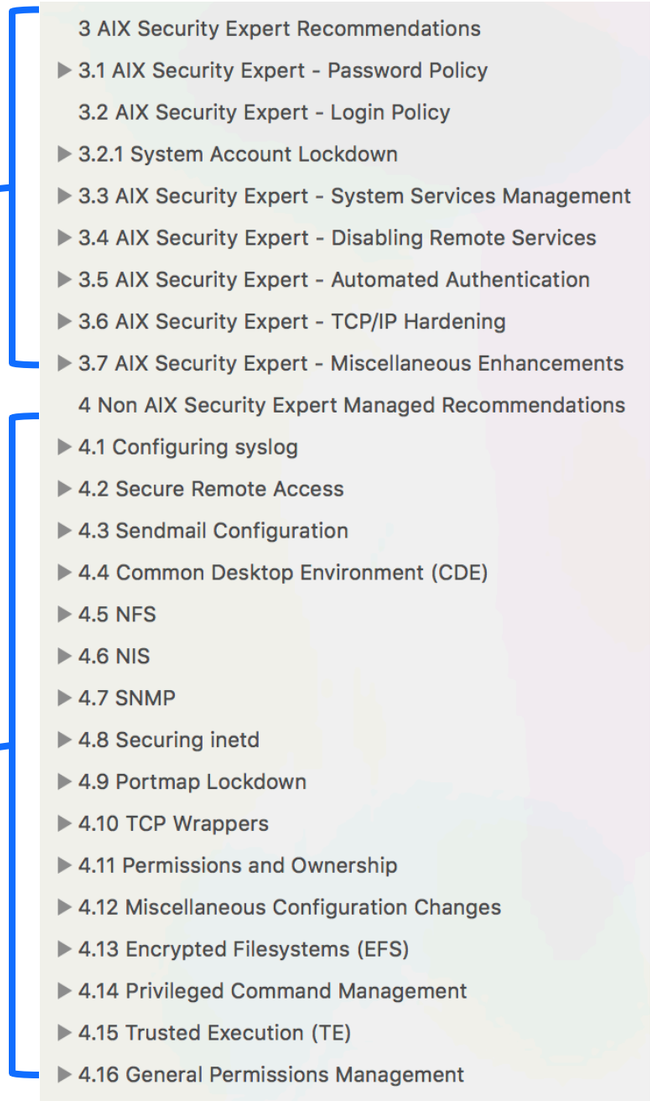
~ 110 recommendations applicables avec AIXPERT

- Se base sur une commande intégrée dans AIX
- Utilise la fonction "custom" de aixpert
- Fichier XML modifiable

Section 4

~ 110 recommendations qui ne peuvent être gérées par aixpert

- Nécessite du scripting



Recommendations par sujet

Section 3: applicable avec aixpert

- Password Policy
- Login Policy
- System Account Lockdown
- System Services Management
- Disabling Remote Services
- Automated Authentication
- TCP/IP Hardening
- Miscellanous: crontab, at, ftp, umask…

aixpert -f /etc/security/aixpert/core/custom.xml

Section 4: applicable par script

- Configuring syslog
- Secure remote access
- Configuring sendmail
- Configuring CDE
- Configuring NFS
- Configuring SNMP
- TCP Wrappers
- File and directory permissions and ownership
- Privileged command management - Enhanced RBAC and sudo
- Encrypted Filesystem (EFS)
- Trusted Execution
- General Permissions Management

aixpert

exemple de stanza

Fichier custom.xml

…

<AIXPertEntry name="hls_minlen" function="minlen">

<AIXPertRuleType type="HLS"/>

<AIXPertDescription>Minimum length for password: Specifies the minimum length of a password to 8</AIXPertDescription>
<AIXPertPrereqList>bos.rte.date,bos.rte.commands,bos.rte.security,bos.rte.shell,bos.rte.ILS</AIXPertPrereqList>
<AIXPertCommand>/etc/security/aixpert/bin/chusrattr</AIXPertCommand>

<AIXPertArgs>minlen=8 ALL hls_minlen</AIXPertArgs>

<AIXPertGroup>Password policy rules</AIXPertGroup>

</AIXPertEntry>

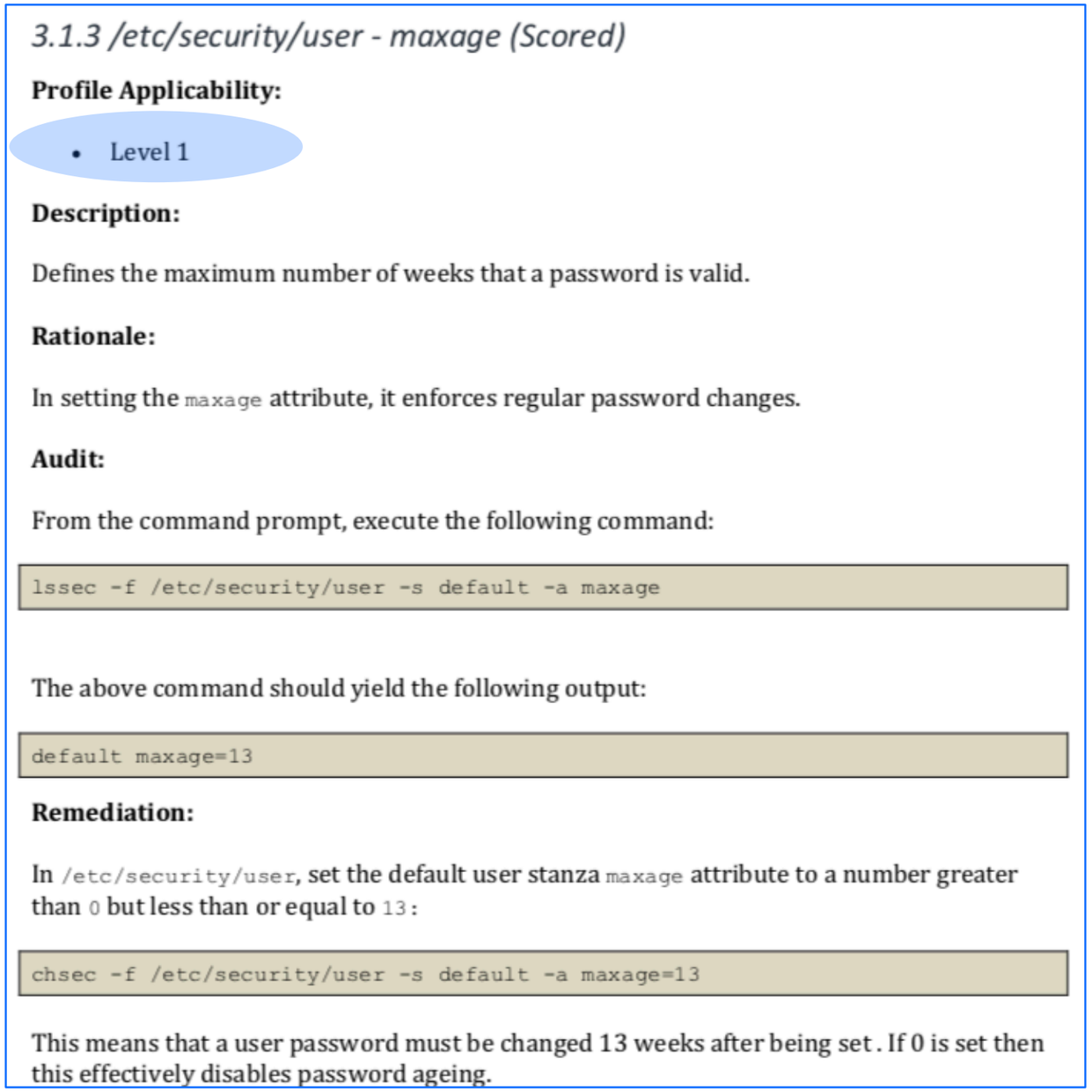
…

Possible de modifier les valeurs ou d'enlever des stanzas…

aixpert -f /etc/security/aixpert/core/custom.xml

En détail, une recommendation

Le benchmark pour AIX 7.1 comprend environ 100 recommendations Level 1 et 120 recommendations Level 2



3.1.3 /etc/security/user - maxage (Scored)

Profile Applicability:

- Level 1

Description:

Defines the maximum number of weeks that a password is valid.

Rationale:

In setting the `maxage` attribute, it enforces regular password changes.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxage
```

The above command should yield the following output:

```
default maxage=13
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxage` attribute to a number greater than `0` but less than or equal to `13`:

```
chsec -f /etc/security/user -s default -a maxage=13
```

This means that a user password must be changed 13 weeks after being set . If 0 is set then this effectively disables password ageing.

2 profils d'application :

- **Level 1**

Ces recommendations sont sensées

- être pratique et prudente
- apporter un bénéfice clair à la sécurité
- ne pas inhiber l'utilisation de la technoligie plus que de manière acceptable

- **Level 2**

Le benchmark level 2 a au moins l'une de ces caractéristiques

- Il est destiné à des environnements ou des cas d'utilisation où la sécurité est primordiale
- Il agit en tant que mesure de défense en profondeur
- Il peut inhiber négativement l'utilité ou la performance de la technologie

En détail, une recommendation

3.1.3 /etc/security/user - maxage (Scored)

Profile Applicability:

- Level 1

Description:

Defines the maximum number of weeks that a password is valid.

Rationale:

In setting the `maxage` attribute, it enforces regular password changes.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxage
```

The above command should yield the following output:

```
default maxage=13
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxage` attribute to a number greater than `0` but less than or equal to `13`:

```
chsec -f /etc/security/user -s default -a maxage=13
```

This means that a user password must be changed 13 weeks after being set . If 0 is set then this effectively disables password ageing.

Une description du point

Une explication de la raison

La commande pour auditer

La commande pour appliquer

Déroulement d'un projet de hardening

Détection

Comparaison de l'état du système par rapport aux préconisations

⇒ Liste de points "Failed"

https://www.cisecurity.org/

Adaptation

Collaboration avec les équipes de sécurité pour décider des points qui peuvent être "bypassés"

⇒ Document de décision

Déploiement

- Outils d'automatisation

Ansible, Puppet, CHEF …

- Remediation Kit

Fichier custom.xml pour AIXPERT et script pour la section 4

⇒ Disponible pour les membres du CIS seulement

Auditing

Production de rapport de "compliance"

- Intégration dans Nessus
- CIS-CAT Pro

⇒ Requires CIS membership

- Script de check

Auditing: rapport de “compliance”

Nessus

Table Of Contents

4.12.1 Miscellaneous Config - serial port restriction

Info

The recommendation is to disable the login capability of all connected tty devices.
It is recommended that the login capability for all serial ports is disabled, so that unauthorized users cannot attach modems or remote access devices to these ports and bypass any network access control.If the environment utilizes tty devices to facilitate user connections. This recommendation may be ignored.

Solution

Create a list of active tty ports-
lsitab -a legrep 'respawn:/usr/sbin/gettylon:/usr/sbin/getty'
If any tty devices are returned from the previous output, lock down each any unrequired devices via-
chitab 'tty2:2:off:/usr/sbin/getty /dev/tty2'
NOTE- Replace tty2 with the relevant port.

See Also

https://benchmarks.cisecurity.org/tools2/aix/CIS_IBM_AIX_7.1_Benchmark_v1.1.0.pdf

References

800-53	CM-7
800-171	3.4.6
800-171	3.4.7
CSF	PR.IP-1
CSF	PR.PT-3
ITSG-33	CM-7
SWIFT-CSCV1	2.3
LEVEL	2S
PCI-DSS	2.2.4

Audit File

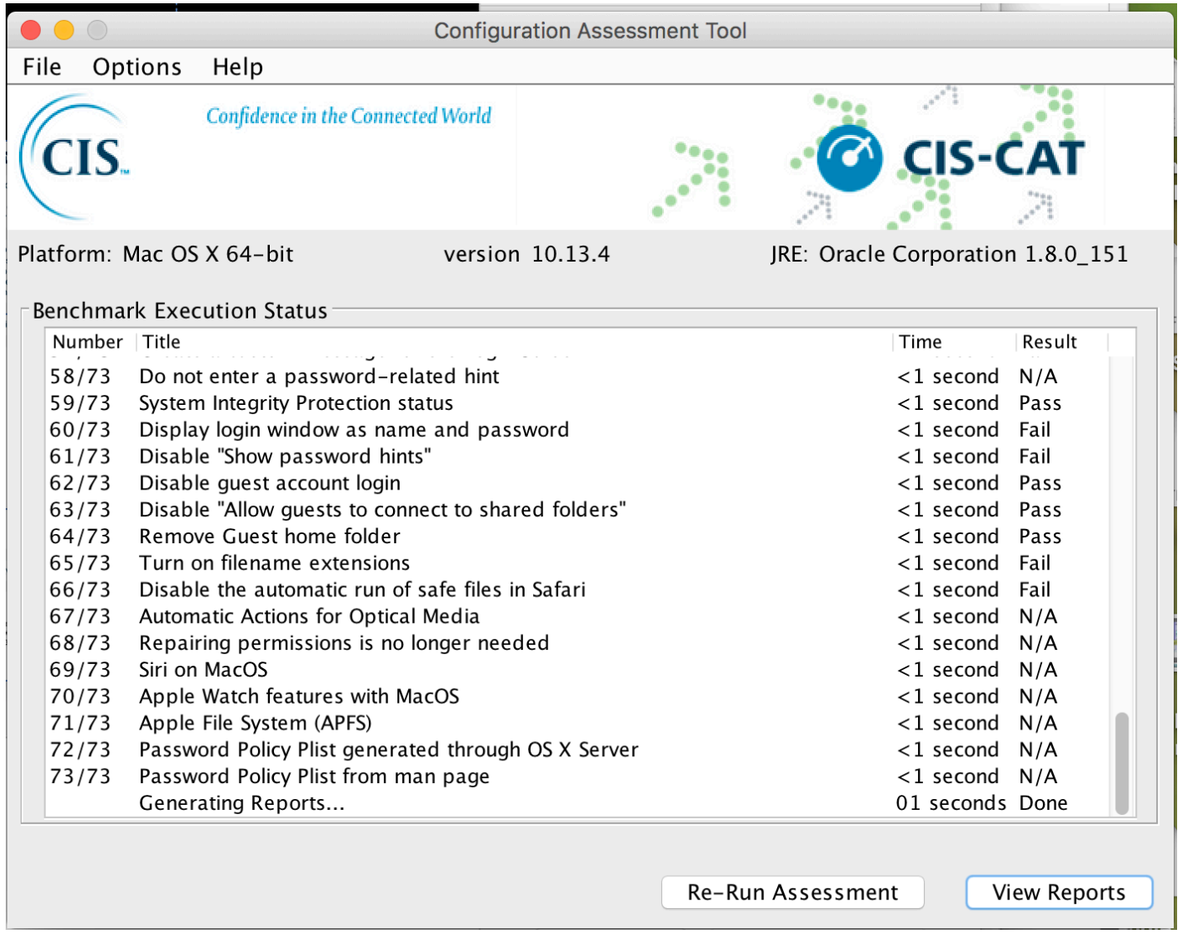
CIS_AIX_7.1_Benchmark_v1.1.0_Level_2.audit

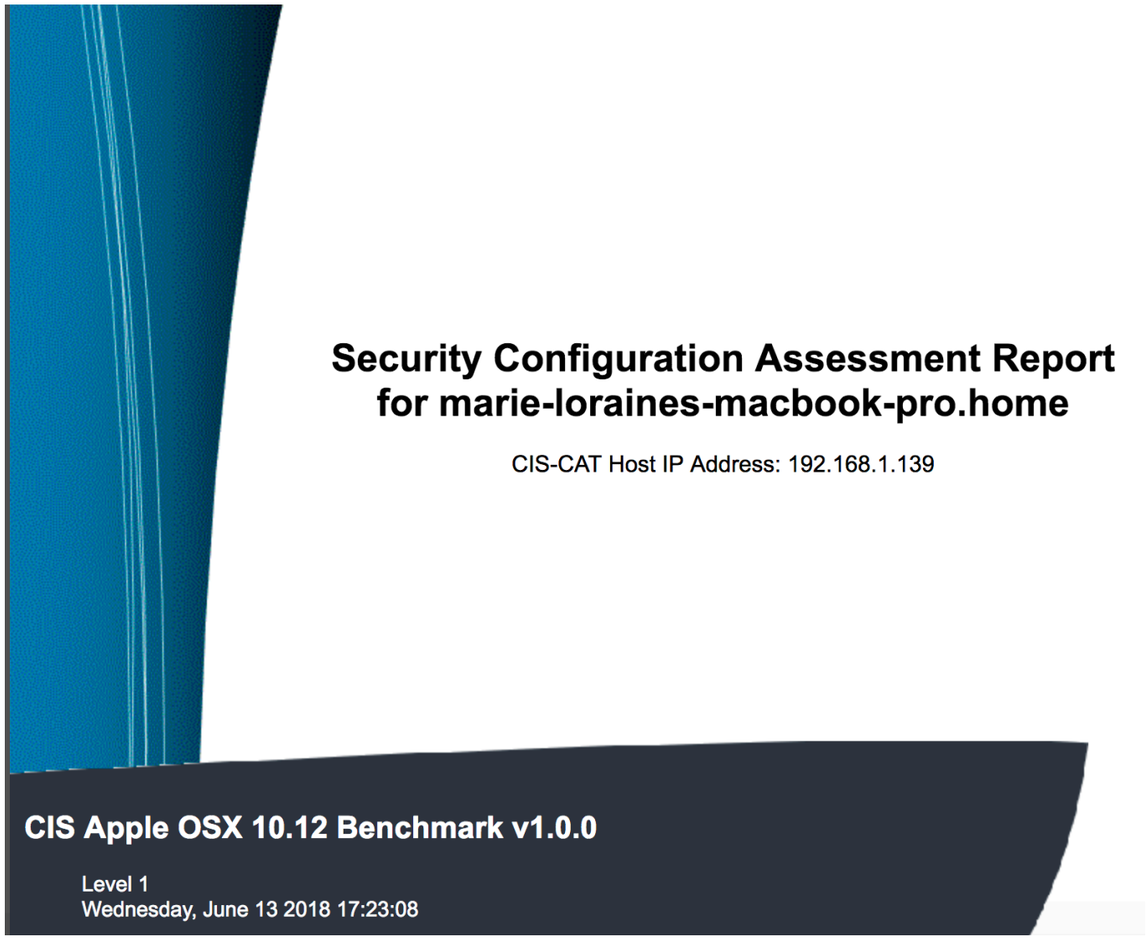
Hosts

```
Non-compliant file(s):
      /etc/inittab - regex '^[A-Za-z0-9_]+:[0-9]+:(respawn|on):/usr/sbin/getty' found - expect
 '^[A-Za-z0-9_]+:[0-9]+:(respawn|on):/usr/sbin/getty' found in the following lines:
         49: cons:0123456789:respawn:/usr/sbin/getty /dev/console
```


Auditing: rapport de “compliance”

CIS-CAT Pro





Backup slides

6 reasons to become a member

Save time with automated system reviews

CIS-CAT Pro Assessor saves you hours of configuration review by scanning against a target system's configuration settings and reporting the system's compliance to the corresponding CIS Benchmark.

Track compliance automatically

CIS-CAT Pro Dashboard consumes assessment reports and shows system(s) compliance to the CIS Benchmarks over a period of time.

Customize benchmarks to your needs

With CIS Workbench, you can easily tailor benchmark recommendations to fit organizational or compliance policies. Export selected CIS Benchmarks in various formats (Microsoft Word, Microsoft Excel, XCCDF, OVAL, XML)

Quickly and easily configure systems

Remediation content (GPOs, Linux scripts and more) allows you to rapidly implement CIS Benchmark recommendations.

Enjoy enhanced technical support

Take advantage of email and discussion forum support services from our expert cybersecurity staff and CIS-CAT Pro developers.

Join Our Cybersecurity Community

Network and collaborate with cybersecurity professionals around the world and discuss best practices for securing a wide range of technologies.

PriceList

Différentes catégories de membres:

- End User
- Academic
- Non-profit 501(c)(3)
- SLTT (State, Local, Tribal, Territorial) Governments
- Services - Consulting
- Services - Hosting, Cloud, and Managed
- Product Vendor

Employee Range	1-Year Total	2-Year Total (20% off 2nd year)	3-Year Total (20% off 2nd year,
250,000+	$14,180	$25,524	$35,450
100,000 - 249,999	$13,130	$23,634	$32,825
50,000 - 99,999	$12,080	$21,744	$30,200
25,000 - 49,999	$11,030	$19,854	$27,575
10,000 - 24,999	$10,500	$18,900	$26,250
5,000 - 9,999	$9,980	$17,964	$24,950
1,000 - 4,999	$9,450	$17,010	$23,625
500 - 999	$6,830	$12,294	$17,075
250 - 499	$4,730	$8,514	$11,825
100 - 249	$3,420	$6,156	$8,550
50 - 99	$2,100	$3,780	$5,250
up to 49	$1,320	$2,376	$3,300

**Pricing in USD. Subject to change.*

Update your Unix on Power environment to the latest industry standards with "IBM Services" team

Some examples of mission we've recently performed

UNIX hardening to meet CIS standards

(Center for Internet Security)

Customize CIS benchmark for your Aix or Linux environment

- Validate on a test environment and deploy on production
- Provide compliance report for IT security team
- Provide scripts to harden and check compliance

Unix users integration with Directory Services

Integrate Aix & Linux user's authentication in your enterprise solution

- Analyse and define requirements in Directory server
- Install and validate on a test environment
- Deploy on production servers

HealthCheck on IBM Power

Including HW, virtualization layer and Operating System

- Capture data on your environment
- Analyze HA and performance tuning parameters and compare to best practices
- Report with enhancement proposal

Contact: IBM Services

Marie-Lorraine Bontron
mbon@ch.ibm.com 079/3671385

Nimal Abhaya
nima@ch.ibm.com 079/4755616

May you have any concerns regarding the evolution of your IBM Power Systems environment, powerVM, powerHA, PowerVC, AIX, Linux on Power, Hana on Power and so on, do not hesitate to contact us. It will be a pleasure for us to discuss solutions with you.