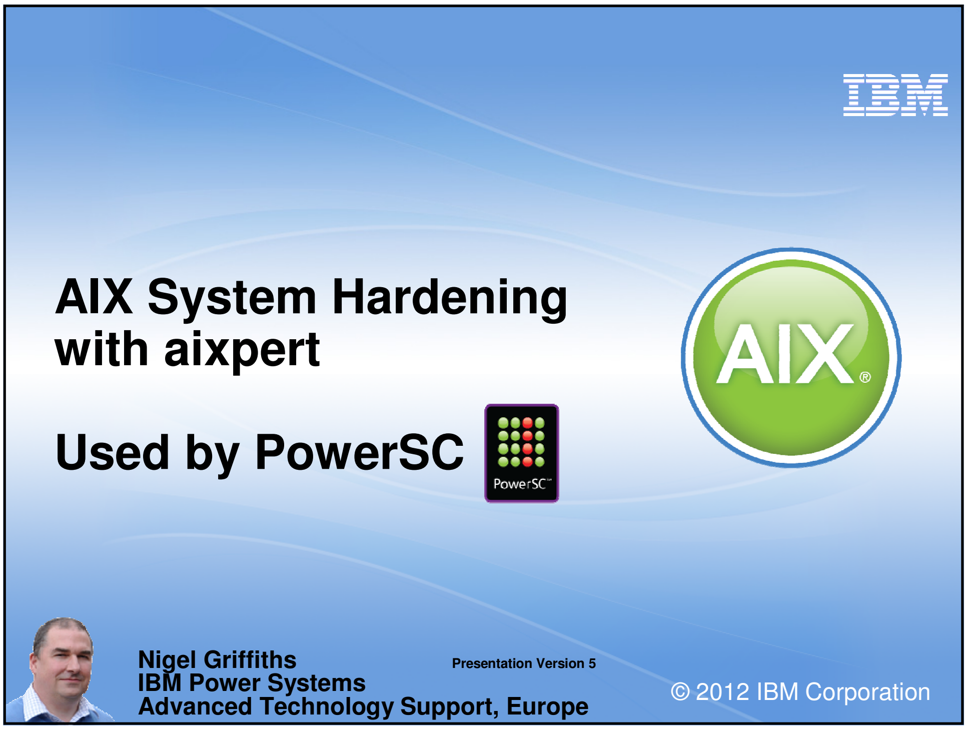
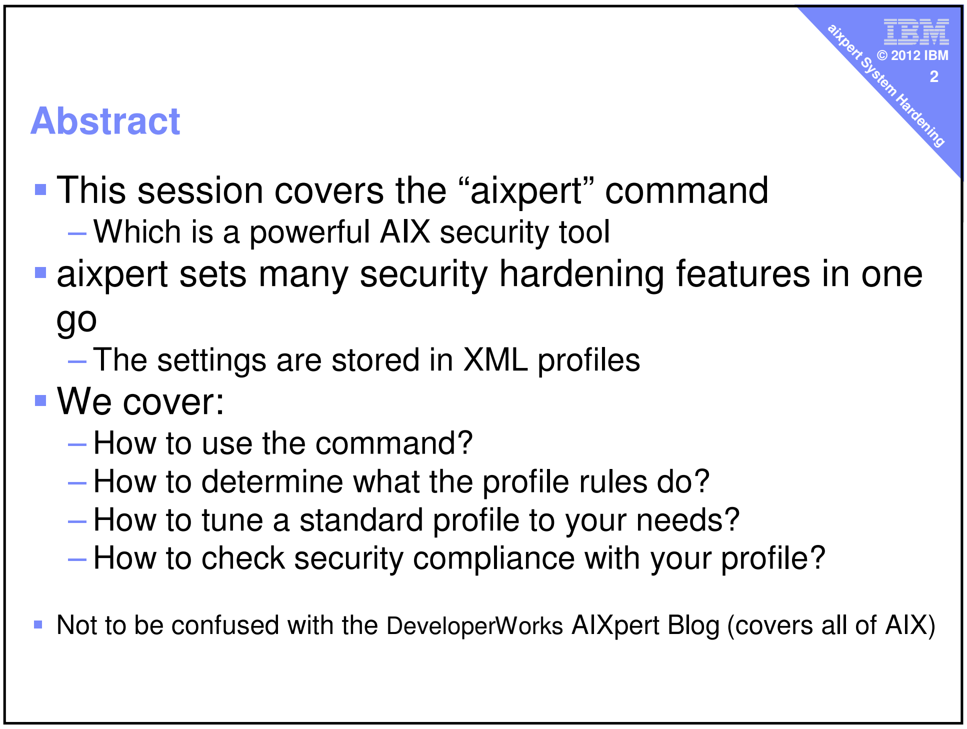


AIX System Hardening with aixpert

Used by PowerSC

Nigel Griffiths
IBM Power Systems
Advanced Technology Support, Europe

Presentation Version 5



Abstract

- This session covers the “aixpert” command
  - Which is a powerful AIX security tool
- aixpert sets many security hardening features in one go
  - The settings are stored in XML profiles
- We cover:
  - How to use the command?
  - How to determine what the profile rules do?
  - How to tune a standard profile to your needs?
  - How to check security compliance with your profile?
- Not to be confused with the DeveloperWorks AIXpert Blog (covers all of AIX)

"aixpert" Overview

- aixpert = single command for AIX system hardening
  - Introduced ~ 2006 in AIX 5.3 TL5 with ~300 settings
  - A very powerful tool in its own right
  - Replaces 100's of home grown handmade rules and scripts
  - Gets you to higher security than you can by yourself
- IBM developed the initial profiles & newer ones
  - We worked with Banking customers to get these right
  - Designed to meet various industry security standards
  - Much better for IBM to get it right once → then all benefit

Information sources

- AIX Manuals for aixpert command
  - http://tinyurl.com/aixpert-cmd
- DeveloperWorks AIX Wiki PowerSC page
  - http://tinyurl.com/PowerSC
- Older DeveloperWorks aixpert Hints and Tips article
  - http://www.ibm.com/developerworks/wikis/display/WikiPtype/aixpert
- Older DeveloperWorks Using AIX Security Expert article
  - http://www.ibm.com/developerworks/aix/library/au-aixsecurity/

- Aixpert – The Movie →
  - 23 minutes
  - By a genius ☺
  - http://tinyurl.com/AIXmovies

AIX 5.3 & AIX 6

IBM

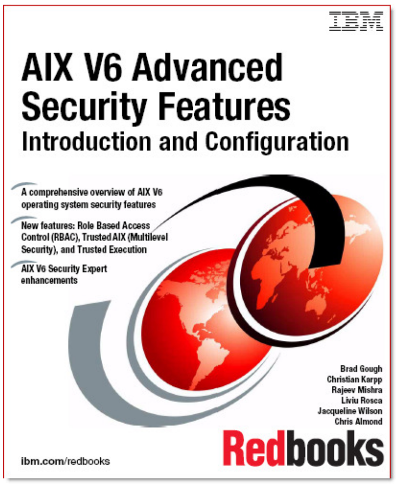
System Hardening the Easy Way
AIX Security Expert → aixpert

Nigel Griffiths
Advanced Technology Centre, UK
pSeries & System p, IBM Europe

© 2008 IBM Corporation

AIX Security Expert - aixpert

Want More? **http://www.redbooks.ibm.com/**



IBM

AIX V6 Advanced Security Features

Introduction and Configuration

A comprehensive overview of AIX V6 operating system security features

New features: Role Based Access Control (RBAC), Trusted AIX (Multilevel Security), and Trusted Execution

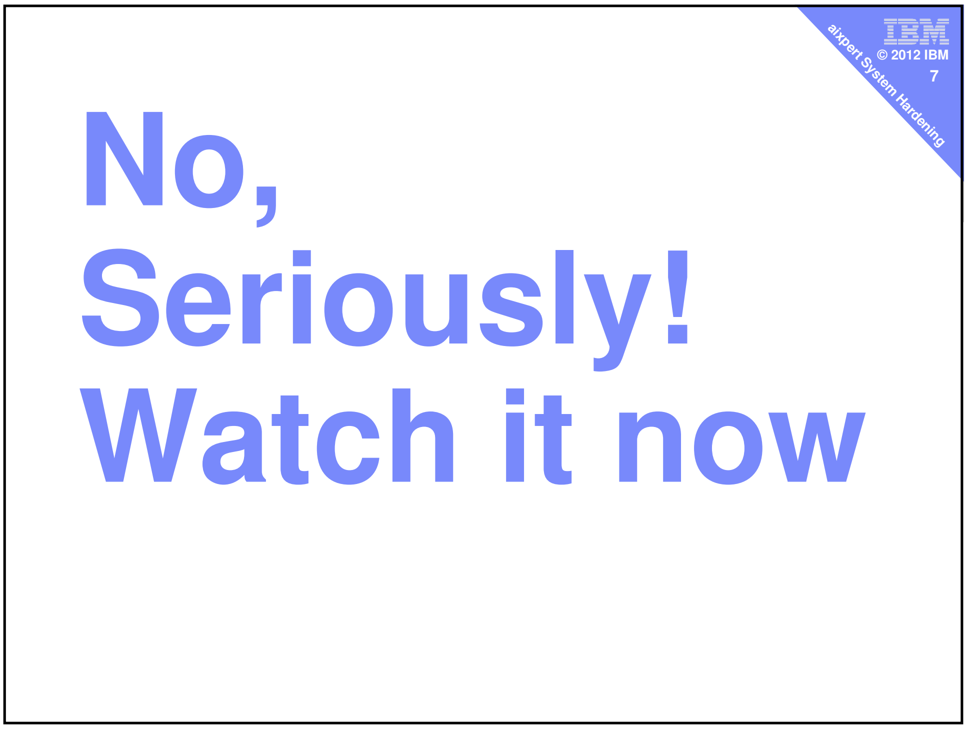
AIX V6 Security Expert enhancements

Brad Gough
Christian Karpp
Rajeev Mishra
Liviu Rosca
Jacqueline Wilson
Chris Almond

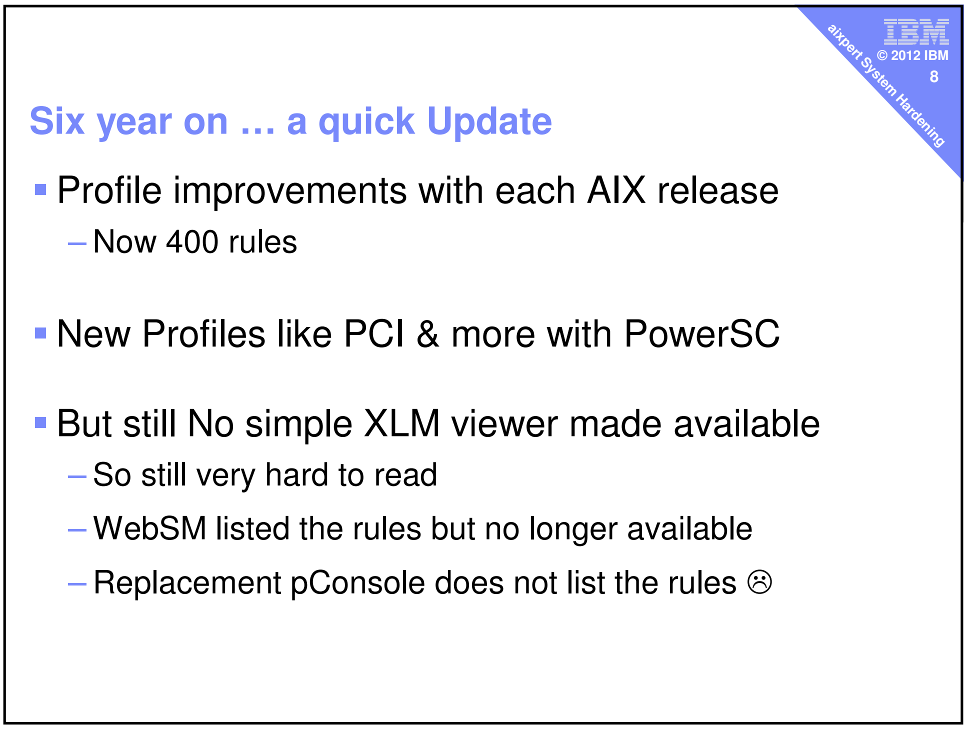
Redbooks

ibm.com/redbooks

Go no further until you have watch the movie



No,
Seriously!
Watch it now



Six year on … a quick Update

- Profile improvements with each AIX release
  - Now 400 rules
- New Profiles like PCI & more with PowerSC
- But still No simple XLM viewer made available
  - So still very hard to read
  - WebSM listed the rules but no longer available
  - Replacement pConsole does not list the rules ☹

Warning don’t casually dabble

- I applied Default settings to regular AIX install
- It is a low-ish setting, so no harm right!

- NFS processes shutdown – it was my NFS server!

- I ran undo but it does not restart NFS
  - It just relaxes the no NFS server rule
  - I quick “smitty nfs” and all is well

- You have been warned!

The Devil is in the Detail & Testing

Mandatory:

1. Read & Understand profiles rules
2. Test your profiles in a sandbox

Or your vital system get so secure it can’t used
& may you never login again!

So how to understand the profile rules?

- Where are they

- What do they look like?
  - Naked
- Via Tools
  - XML Editor ☹
  - XML Viewer 😐
  - Nigel's secret website ☺

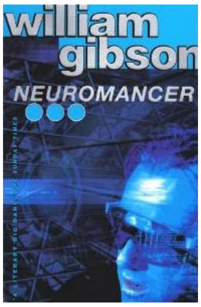
Where are the XML profiles?

- Assuming a recent AIX version (here AIX 6 TL7)
- /etc/security/
- Root only access

```
# ls
.idlck                   ice                      privcmds.backup
.ids                     ipsec_filter             privdevs
.kst                     ipsec_filter.vc          privfiles
.profile                 ipsec_tunnel_IBM         pwdalg.cfg
.rbac_ids                ipsec_tunnel_IBM.vc      pwdhist.dir
acl                      ipsec_tunnel_manual      pwdhist.pag
aixpert                  ipsec_tunnel_manual.vc   roles
artex                    lastlog                  services
audit                    ldap                     smitacl.group
authorizations           limits                   smitacl.user
certificates             login.cfg                sysck.cfg
domains                  mkuser.default           tsd
domobjs                  mkuser.sys               tss
environ                  passwd                   user
failedlogin              portlog                  user.roles
fpm                      priv
group                    privcmds
```

ICE ???

- ICE → Intrusion Countermeasure Electronics
- I first came across this in **Neuromancer** in 1984
- Term attributed to Tom Maddox



Where are the XML profiles?   AIX 6 TL7

- /etc/security/aixpert
- Root only access
  - **bin** 52 scripts to set, unset, check = these names are in rules
  - **core** Master profiles – Do not change these
    - All the supported Languages have a directory
    - aixpertall.xml ← ALL the rules in one file
    - appliedaixpert.bak
    - appliedaixpert.xml
  - **custom** For your customised profiles (not mandatory)
  - **dictionary** No idea – a large file of English words!
  - **ldap** empty
  - **log** FAILEDRULES.log PASSESRULES.log aixpert.log
  - **tmp** applied.tmp
  - **undo** files used to undo last operation

/etc/security/aixpert/core/aixpertall.xml

- This has ALL rules for ALL security levels
  - Low, medium, high, default and special ones

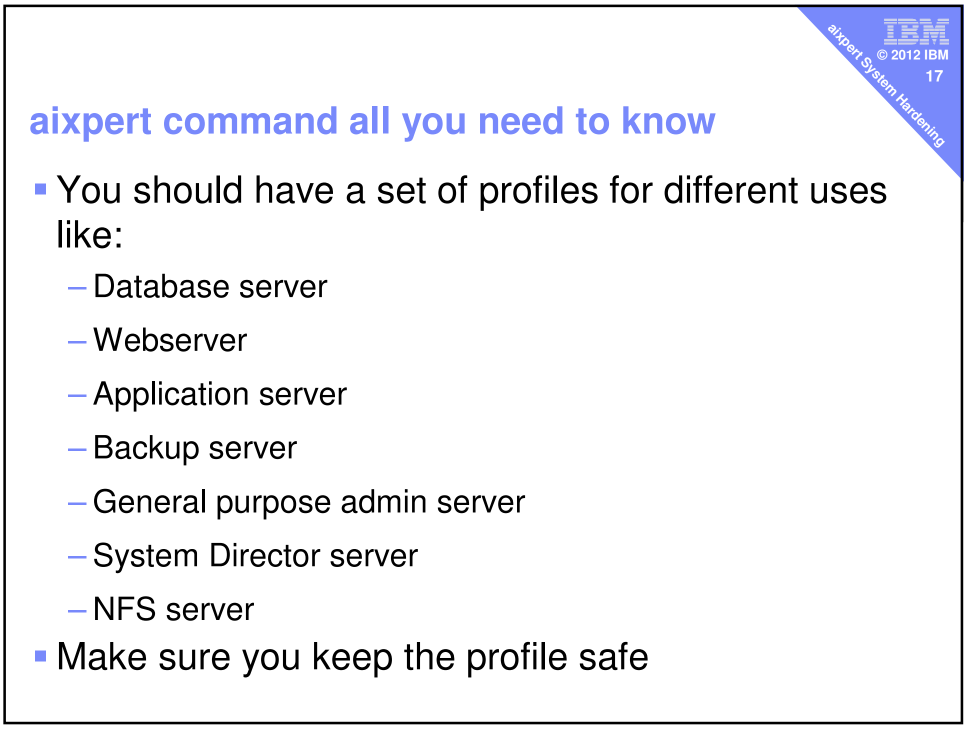
- AIX 6 TL7 has 3222 lines
- It is the Master set
- Never use this Profile

- You need to extract a subset
- Save your profiles in a safe place
  - /etc/security/aixpert/custom/xxxxxxx.xml

aixpert command all you need to know

- You can extract one level using
  - aixpert -l high -n -o my_high_settings.xml
  - Modify you profile → next few slides
  - I recommend commenting out
- Apply your profile
  - aixpert -f my_high_settings.xml
- If problem undo:
  - aixpert –u -p

- Check you are Compliance later
  - aixpert -c -p



IBM

© 2012 IBM

17

aixpert System Hardening

aixpert command all you need to know

- You should have a set of profiles for different uses like:
  - Database server
  - Webserver
  - Application server
  - Backup server
  - General purpose admin server
  - System Director server
  - NFS server
- Make sure you keep the profile safe

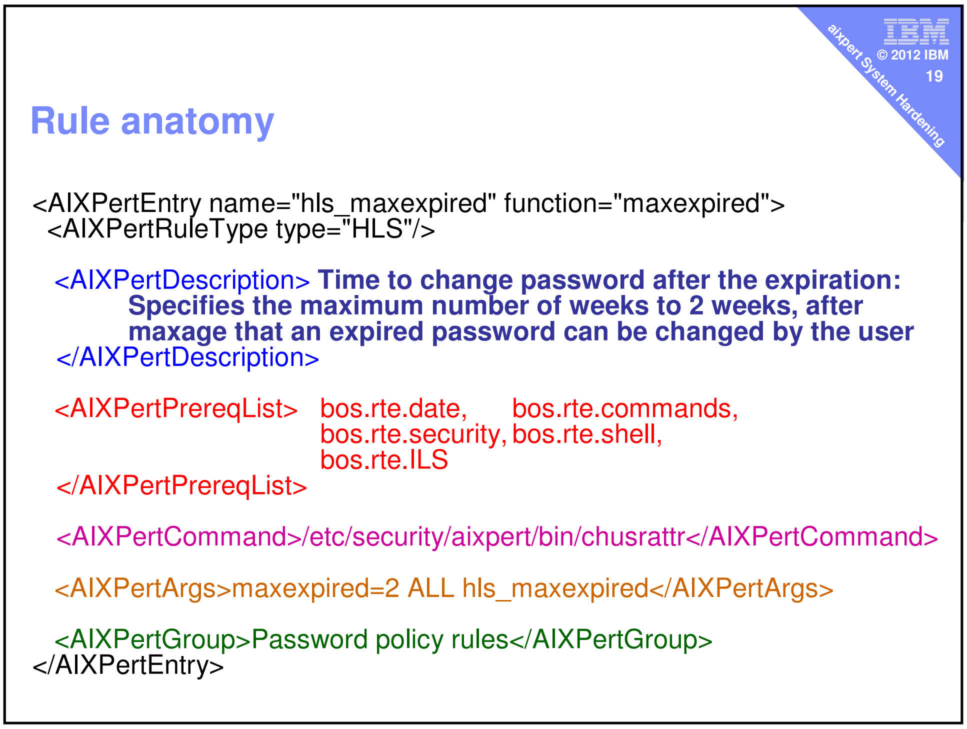
IBM

© 2012 IBM

18

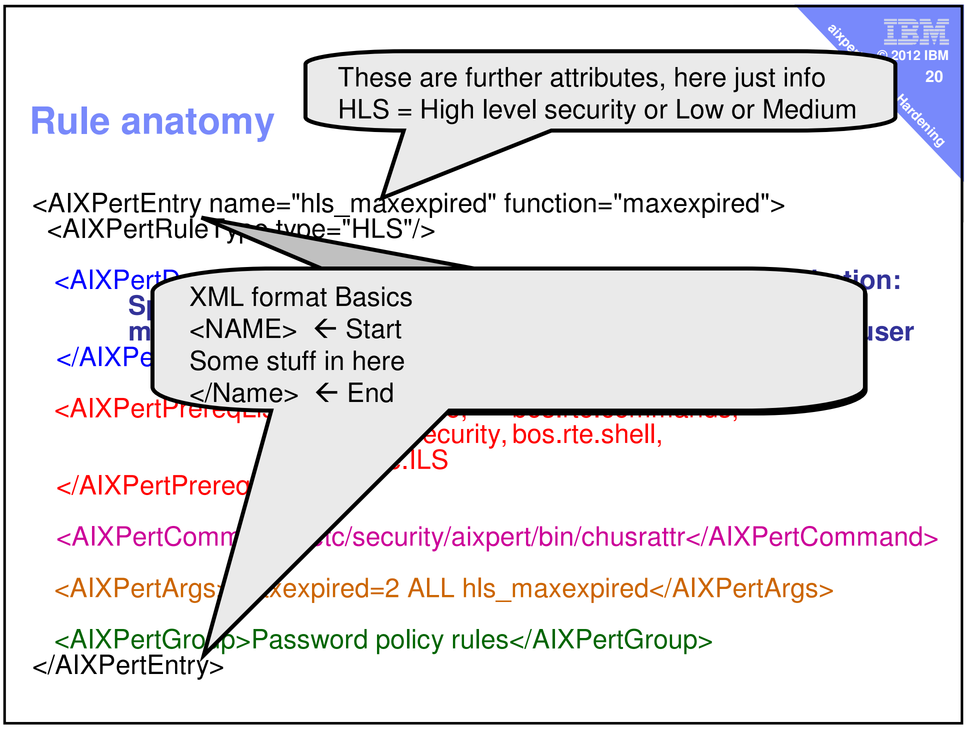
aixpert System Hardening

Now lets look are the rule profiles



Rule anatomy

```
<AIXPertEntry name="hls_maxexpired" function="maxexpired">
  <AIXPertRuleType type="HLS"/>

  <AIXPertDescription> Time to change password after the expiration:
         Specifies the maximum number of weeks to 2 weeks, after
         maxage that an expired password can be changed by the user
  </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>maxexpired=2 ALL hls_maxexpired</AIXPertArgs>

  <AIXPertGroup>Password policy rules</AIXPertGroup>
</AIXPertEntry>
```

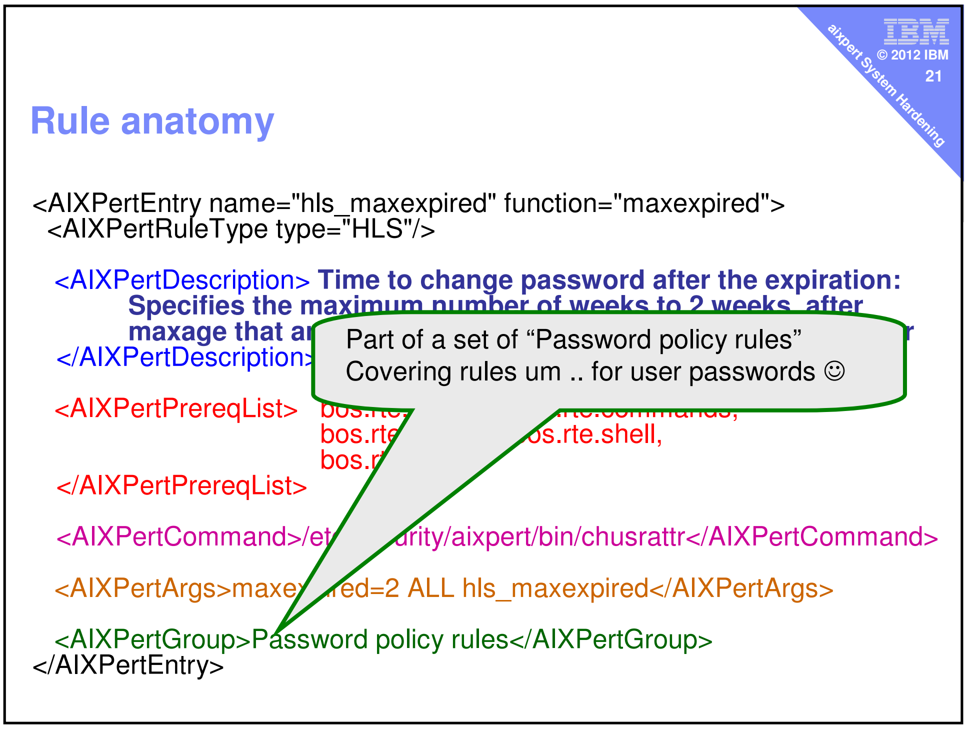


Rule anatomy

These are further attributes, here just info
HLS = High level security or Low or Medium

XML format Basics
<NAME> ← Start
Some stuff in here
</Name> ← End

```
<AIXPertEntry name="hls_maxexpired" function="maxexpired">
  <AIXPertRuleType type="HLS"/>

  <AIXPertD                                                    tion:
         Sp
         m                                                     user
  </AIXPe

  <AIXPertPrereqLi
                       ecurity, bos.rte.shell,
                       .ILS
  </AIXPertPrereq

  <AIXPertComm      tc/security/aixpert/bin/chusrattr</AIXPertCommand>

  <AIXPertArgs      xexpired=2 ALL hls_maxexpired</AIXPertArgs>

  <AIXPertGroup>Password policy rules</AIXPertGroup>
</AIXPertEntry>
```



aixpert System Hardening

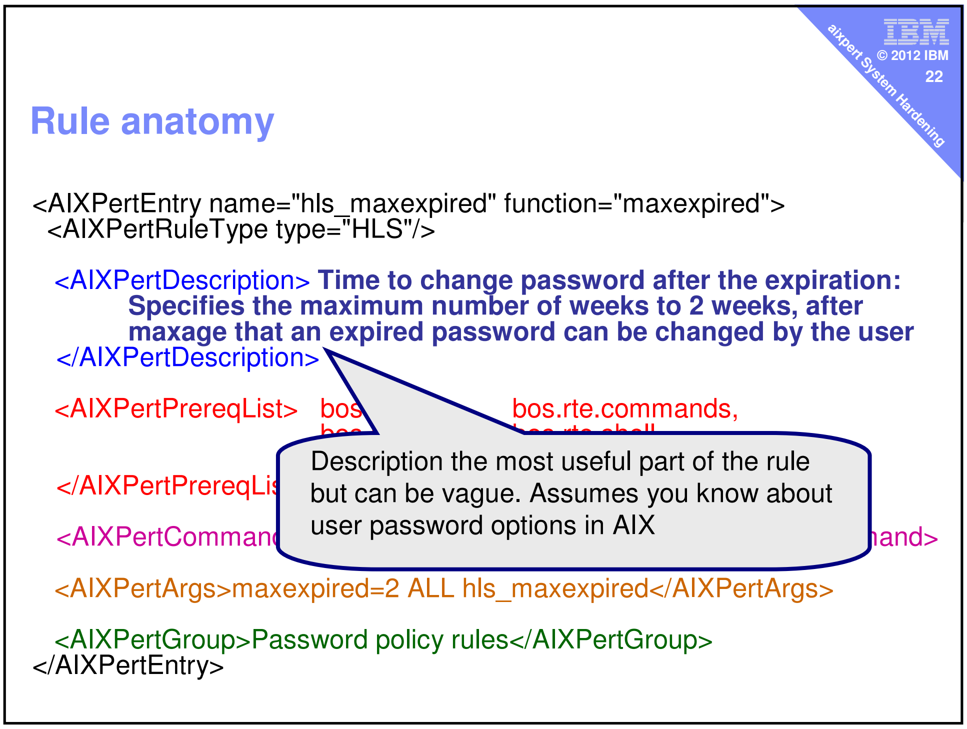
© 2012 IBM

21

Rule anatomy

```
<AIXPertEntry name="hls_maxexpired" function="maxexpired">
  <AIXPertRuleType type="HLS"/>

   <AIXPertDescription> Time to change password after the expiration:
         Specifies the maximum number of weeks to 2 weeks, after
         maxage that ar                                        r
   </AIXPertDescription>

   <AIXPertPrereqList>  bos.rte            rte.commands,
                        bos.rte          os.rte.shell,
                        bos.r
   </AIXPertPrereqList>

   <AIXPertCommand>/et       urity/aixpert/bin/chusrattr</AIXPertCommand>

   <AIXPertArgs>maxe    red=2 ALL hls_maxexpired</AIXPertArgs>

   <AIXPertGroup>Password policy rules</AIXPertGroup>
</AIXPertEntry>
```

Part of a set of “Password policy rules”
Covering rules um .. for user passwords ☺



aixpert System Hardening

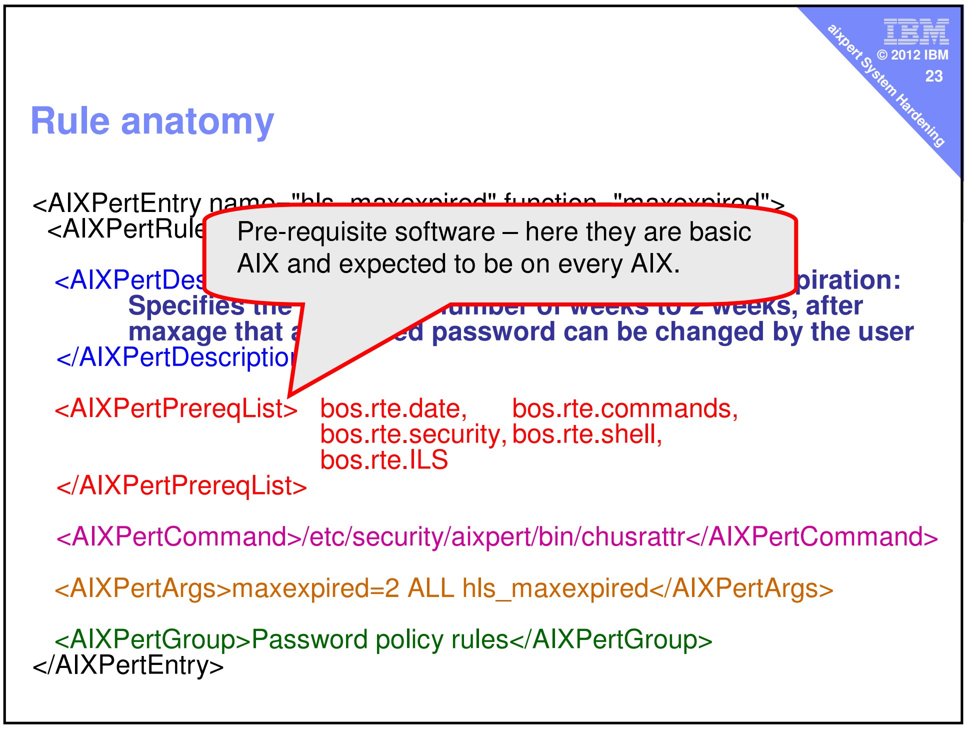
© 2012 IBM

22

Rule anatomy

```
<AIXPertEntry name="hls_maxexpired" function="maxexpired">
  <AIXPertRuleType type="HLS"/>

   <AIXPertDescription> Time to change password after the expiration:
         Specifies the maximum number of weeks to 2 weeks, after
         maxage that an expired password can be changed by the user
   </AIXPertDescription>

   <AIXPertPrereqList>  bos             bos.rte.commands,

   </AIXPertPrereqLis

   <AIXPertComman                                                    and>

   <AIXPertArgs>maxexpired=2 ALL hls_maxexpired</AIXPertArgs>

   <AIXPertGroup>Password policy rules</AIXPertGroup>
</AIXPertEntry>
```

Description the most useful part of the rule
but can be vague. Assumes you know about
user password options in AIX



aixpert System Hardening

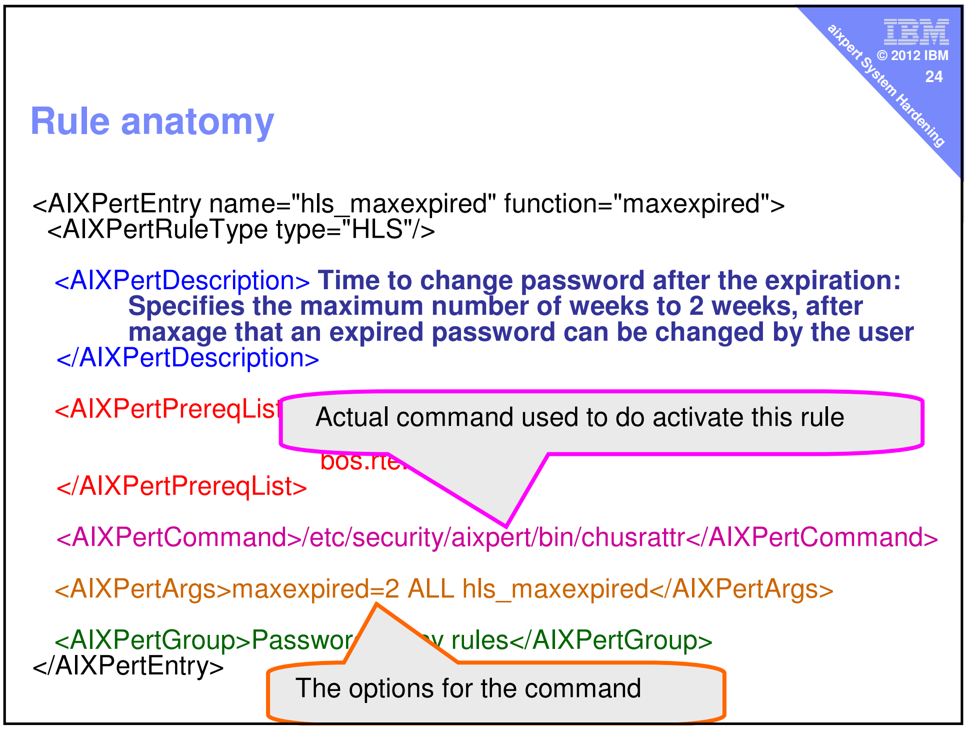
© 2012 IBM

23

Rule anatomy

```
<AIXPertEntry name="hls_maxexpired" function="maxexpired">
  <AIXPertRule
   <AIXPertDes                                              piration:
          Specifies the           umber of weeks to 2 weeks, after
          maxage that a         ed password can be changed by the user
   </AIXPertDescriptio

   <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>maxexpired=2 ALL hls_maxexpired</AIXPertArgs>

   <AIXPertGroup>Password policy rules</AIXPertGroup>
</AIXPertEntry>
```

Pre-requisite software – here they are basic AIX and expected to be on every AIX.



aixpert System Hardening

© 2012 IBM

24

Rule anatomy

```
<AIXPertEntry name="hls_maxexpired" function="maxexpired">
  <AIXPertRuleType type="HLS"/>

   <AIXPertDescription> Time to change password after the expiration:
          Specifies the maximum number of weeks to 2 weeks, after
          maxage that an expired password can be changed by the user
   </AIXPertDescription>

   <AIXPertPrereqList

                         bos.rte.
   </AIXPertPrereqList>

   <AIXPertCommand>/etc/security/aixpert/bin/chusrattr</AIXPertCommand>

   <AIXPertArgs>maxexpired=2 ALL hls_maxexpired</AIXPertArgs>

   <AIXPertGroup>Passwor          y rules</AIXPertGroup>
</AIXPertEntry>
```

Actual command used to do activate this rule

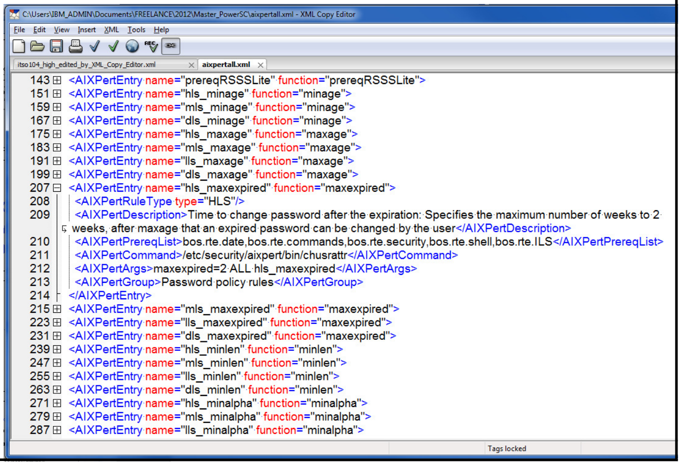
The options for the command

First 13 rules out of 400 = tricky

```
<AIXPertEntry name="lls_maxexpired" function="maxexpired">
    <AIXPertRuleType type="LLS"/>
    <AIXPertDescription>Time to change password after the expiration: Specifies the maximum number of weeks to 8 weeeks, after maxag
e that an expired password can be changed by the user</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>maxexpired=8 ALL lls_maxexpired</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="dls_maxexpired" function="maxexpired">
    <AIXPertRuleType type="DLS"/>
    <AIXPertDescription>Time to change password after the expiration: Removes any minimum number of weeks requirements, after maxage
 that an expired password can be changed by the user</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>maxexpired=-1 ALL dls_maxexpired</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <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>
  <AIXPertEntry name="mls_minlen" function="minlen">
    <AIXPertRuleType type="MLS"/>
    <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 mls_minlen</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="lls_minlen" function="minlen">
    <AIXPertRuleType type="LLS"/>
    <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 lls_minlen</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="dls_minlen" function="minlen">
    <AIXPertRuleType type="DLS"/>
    <AIXPertDescription>Minimum length for password: Removes the minimum length constraint on password</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=0 ALL dls_minlen</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="hls_minalpha" function="minalpha">
    <AIXPertRuleType type="HLS"/>
    <AIXPertDescription>Minimum number of alphabetic chars: Specifies the minimum number of alphabetic characters in a password to 2
</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>minalpha=2 ALL hls_minalpha</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
 <AIXPertEntry name="mls_minalpha" function="minalpha">
    <AIXPertRuleType type="MLS"/>
    <AIXPertDescription>Minimum number of alphabetic chars: Specifies the minimum number of alphabetic characters in a password to 2
</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>minalpha=2 ALL mls_minalpha</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="lls_minalpha" function="minalpha">
    <AIXPertRuleType type="LLS"/>
    <AIXPertDescription>Minimum number of alphabetic chars: Specifies the minimum number of alphabetic characters in a password to 2
</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>minalpha=2 ALL lls_minalpha</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="dls_minalpha" function="minalpha">
    <AIXPertRuleType type="DLS"/>
    <AIXPertDescription>Minimum number of alphabetic chars: Removes the minimum number of alphabetic characters constraint, in a pas
sword</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>minalpha=0 ALL dls_minalpha</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="hls_minother" function="minother">
    <AIXPertRuleType type="HLS"/>
    <AIXPertDescription>Minimum number of non-alphabetic chars: Specifies the minimum number of non-alphabetic characters in a passw
ord to 2</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>minother=2 ALL hls_minother</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="mls_minother" function="minother">
    <AIXPertRuleType type="MLS"/>
    <AIXPertDescription>Minimum number of non-alphabetic chars: Specifies the minimum number of non-alphabetic characters in a passw
ord to 2</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>minother=2 ALL mls_minother</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
  <AIXPertEntry name="lls_minother" function="minother">
    <AIXPertRuleType type="LLS"/>
    <AIXPertDescription>Minimum number of non-alphabetic chars: Specifies the minimum number of non-alphabetic characters in a passw
ord to 2</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>minother=2 ALL lls_minother</AIXPertArgs>
```

Tried XMV Copy Editor 1.2.0.7

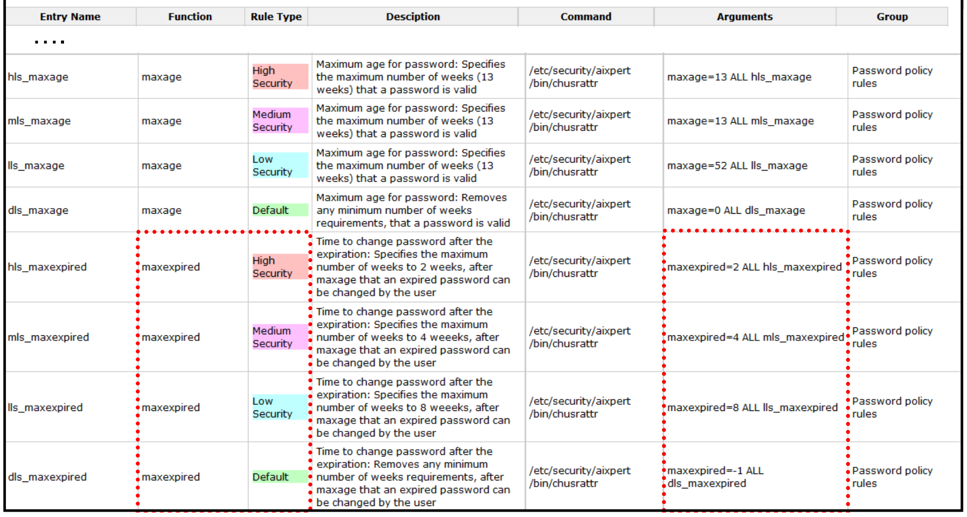
- Open Source – http://xml-editor.sourceforge.net
- Browse & expand rules
- Colour coding helps
- Still rather hard to read


C:\Users\IBM_ADMIN\Documents\FREELANCE\2012\Master_PowerSC\aixpertall.xml - XML Copy Editor
File Edit View Insert XML Tools Help
itso104_high_edited_by_XML_Copy_Editor.xml
aixpertall.xml
Tags locked

```
⊞ <AIXPertEntry name="prereqRSSSLite" function="prereqRSSSLite">
⊞ <AIXPertEntry name="hls_minage" function="minage">
⊞ <AIXPertEntry name="mls_minage" function="minage">
⊞ <AIXPertEntry name="dls_minage" function="minage">
⊞ <AIXPertEntry name="hls_maxage" function="maxage">
⊞ <AIXPertEntry name="mls_maxage" function="maxage">
⊞ <AIXPertEntry name="lls_maxage" function="maxage">
⊞ <AIXPertEntry name="dls_maxage" function="maxage">
⊟ <AIXPertEntry name="hls_maxexpired" function="maxexpired">
    <AIXPertRuleType type="HLS"/>
    <AIXPertDescription>Time to change password after the expiration: Specifies the maximum number of weeks to 2
  weeks, after maxage that an expired password can be changed by the user</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>maxexpired=2 ALL hls_maxexpired</AIXPertArgs>
    <AIXPertGroup>Password policy rules</AIXPertGroup>
  </AIXPertEntry>
⊞ <AIXPertEntry name="mls_maxexpired" function="maxexpired">
⊞ <AIXPertEntry name="lls_maxexpired" function="maxexpired">
⊞ <AIXPertEntry name="dls_maxexpired" function="maxexpired">
⊞ <AIXPertEntry name="hls_minlen" function="minlen">
⊞ <AIXPertEntry name="mls_minlen" function="minlen">
⊞ <AIXPertEntry name="lls_minlen" function="minlen">
⊞ <AIXPertEntry name="dls_minlen" function="minlen">
⊞ <AIXPertEntry name="hls_minalpha" function="minalpha">
⊞ <AIXPertEntry name="mls_minalpha" function="minalpha">
⊞ <AIXPertEntry name="lls_minalpha" function="minalpha">
```

http://tinyurl.com/PowerSC

- List of PowerSC "aixpert" Rules from AIX 7 TL1



Entry Name	Function	Rule Type	Desciption	Command	Arguments	Group
....						
hls_maxage	maxage	High Security	Maximum age for password: Specifies the maximum number of weeks (13 weeks) that a password is valid	/etc/security/aixpert /bin/chusrattr	maxage=13 ALL hls_maxage	Password policy rules
mls_maxage	maxage	Medium Security	Maximum age for password: Specifies the maximum number of weeks (13 weeks) that a password is valid	/etc/security/aixpert /bin/chusrattr	maxage=13 ALL mls_maxage	Password policy rules
lls_maxage	maxage	Low Security	Maximum age for password: Specifies the maximum number of weeks (13 weeks) that a password is valid	/etc/security/aixpert /bin/chusrattr	maxage=52 ALL lls_maxage	Password policy rules
dls_maxage	maxage	Default	Maximum age for password: Removes any minimum number of weeks requirements, that a password is valid	/etc/security/aixpert /bin/chusrattr	maxage=0 ALL dls_maxage	Password policy rules
hls_maxexpired	maxexpired	High Security	Time to change password after the expiration: Specifies the maximum number of weeks to 2 weeks, after maxage that an expired password can be changed by the user	/etc/security/aixpert /bin/chusrattr	maxexpired=2 ALL hls_maxexpired	Password policy rules
mls_maxexpired	maxexpired	Medium Security	Time to change password after the expiration: Specifies the maximum number of weeks to 4 weeeks, after maxage that an expired password can be changed by the user	/etc/security/aixpert /bin/chusrattr	maxexpired=4 ALL mls_maxexpired	Password policy rules
lls_maxexpired	maxexpired	Low Security	Time to change password after the expiration: Specifies the maximum number of weeks to 8 weeeks, after maxage that an expired password can be changed by the user	/etc/security/aixpert /bin/chusrattr	maxexpired=8 ALL lls_maxexpired	Password policy rules
dls_maxexpired	maxexpired	Default	Time to change password after the expiration: Removes any minimum number of weeks requirements, after maxage that an expired password can be changed by the user	/etc/security/aixpert /bin/chusrattr	maxexpired=-1 ALL dls_maxexpired	Password policy rules

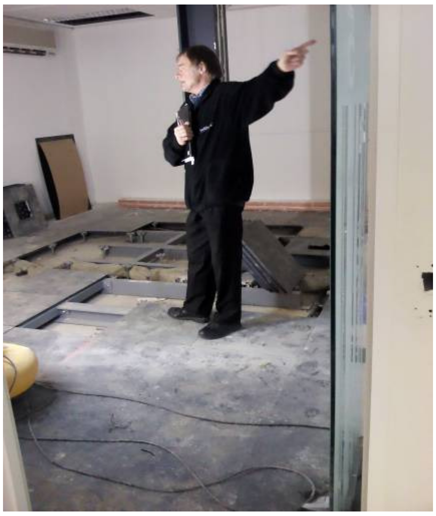
Supplied basic profiles - differences are small

- AIX 6 TL6 basic set
- AIX 6 TL 7 added
  - Port Scan undo IPSec shun host & shun port
- AIX 7 TL1 adds
  - CDE & LFT pre-req checks
  - Proactive kill of telnetd

Let me tell you a story

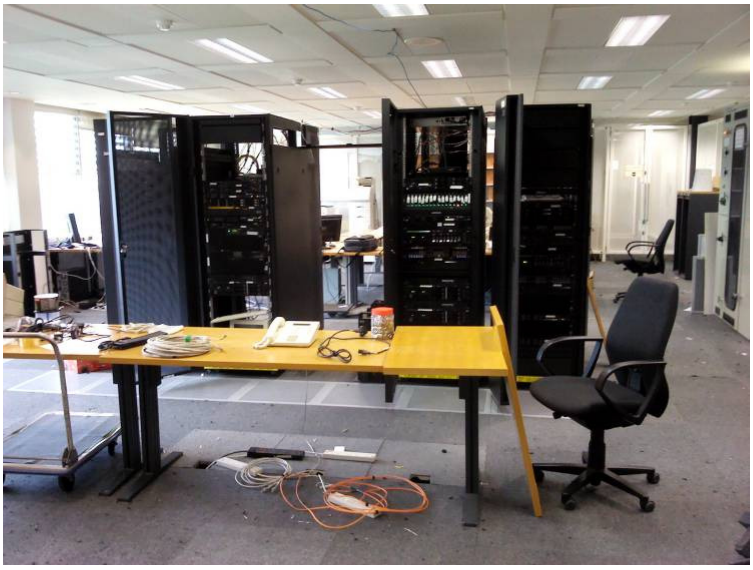
- The Power EMEA ATS move building

New Computer room Bedfont Lakes Building 3
The floor needed strengthening and air conditioning



Building 2
Old massive computer room when empty
Some machines went to other IBM sites

ATS Consolidate down to 3 racks plus HPC rack



aixpert System Hardening

© 2012 IBM

33

All moved but now behind the IBM firewall and have to obey the IBM network security rules

aixpert System Hardening

© 2012 IBM

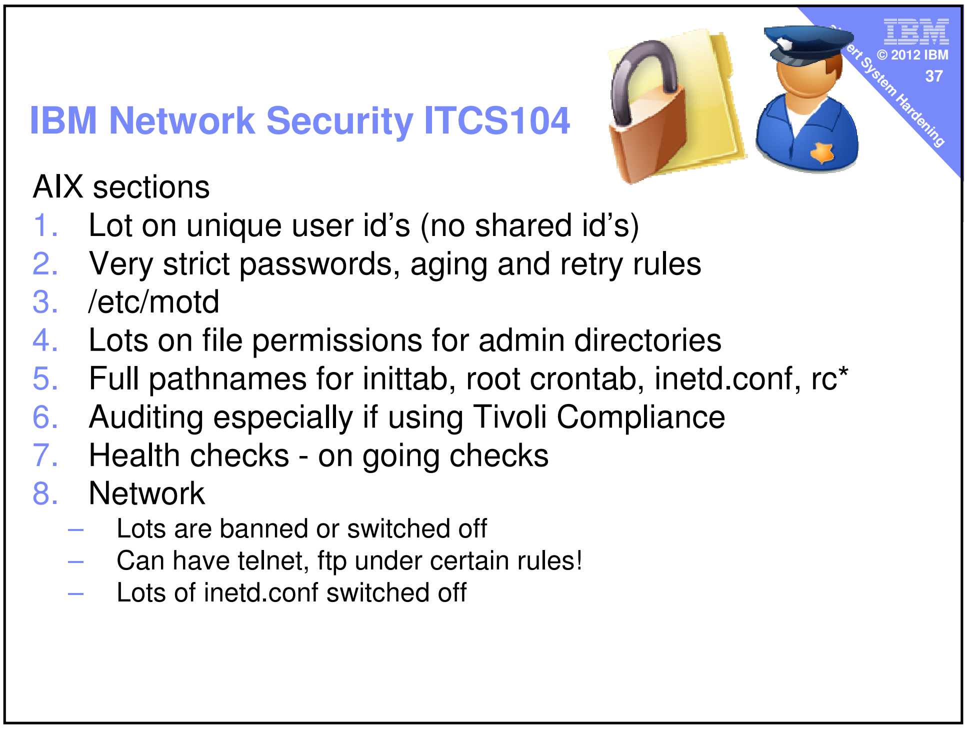
34

The Team – note: all four have IBM badges

So now visible to the IBM "Thought Police"
[We are joking they do a good job]
- Now behind a Bedfont lakes Firewall
- Had to obey the IBM network security standards
- The "dreaded" IBM Network Security ITCS104
[Actually not as bad as we thought]
ITSC 104 - Only using this as an example of an internal security standard = we give no details away here

IBM Network Security ITCS104

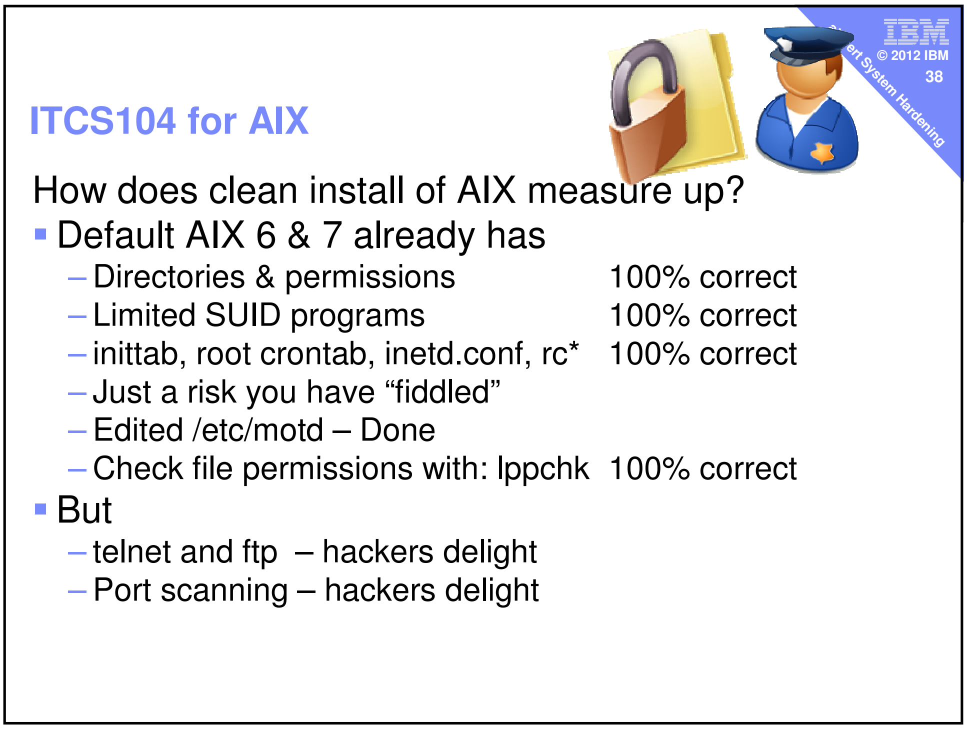
- Machine Class:
  - 1=core ← core to IBM business
  - 2=workstation + laptop
  - 3=dept server
  - 4=demo, education, test ← us, phew!
- Lot of dull bland wordy general statements
  → Unimplementable
- Then sub-docs for AIX and Apache



IBM Network Security ITCS104

AIX sections

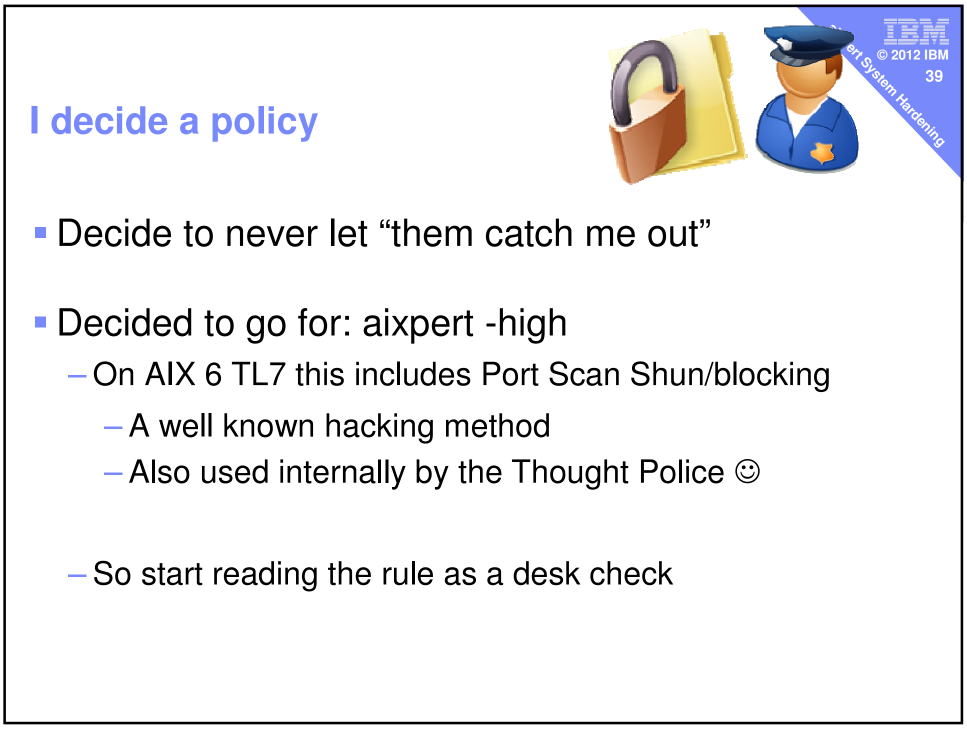
1. Lot on unique user id’s (no shared id’s)
2. Very strict passwords, aging and retry rules
3. /etc/motd
4. Lots on file permissions for admin directories
5. Full pathnames for inittab, root crontab, inetd.conf, rc*
6. Auditing especially if using Tivoli Compliance
7. Health checks - on going checks
8. Network
   - Lots are banned or switched off
   - Can have telnet, ftp under certain rules!
   - Lots of inetd.conf switched off



ITCS104 for AIX

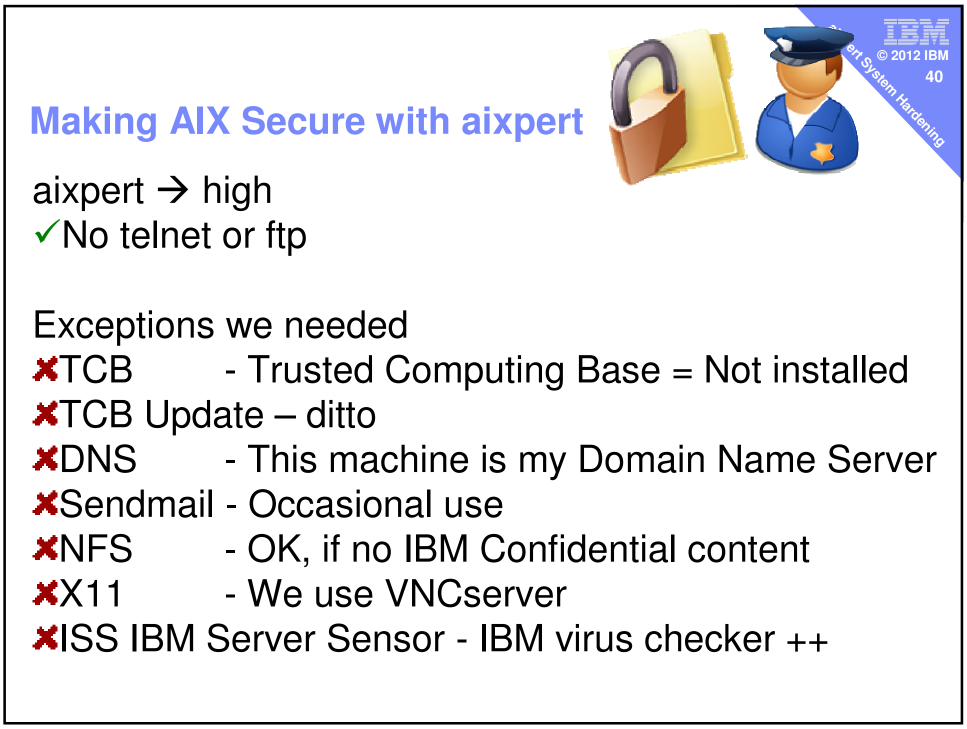
How does clean install of AIX measure up?

- Default AIX 6 & 7 already has
  - Directories & permissions 100% correct
  - Limited SUID programs 100% correct
  - inittab, root crontab, inetd.conf, rc* 100% correct
  - Just a risk you have “fiddled”
  - Edited /etc/motd – Done
  - Check file permissions with: lppchk 100% correct
- But
  - telnet and ftp – hackers delight
  - Port scanning – hackers delight



I decide a policy

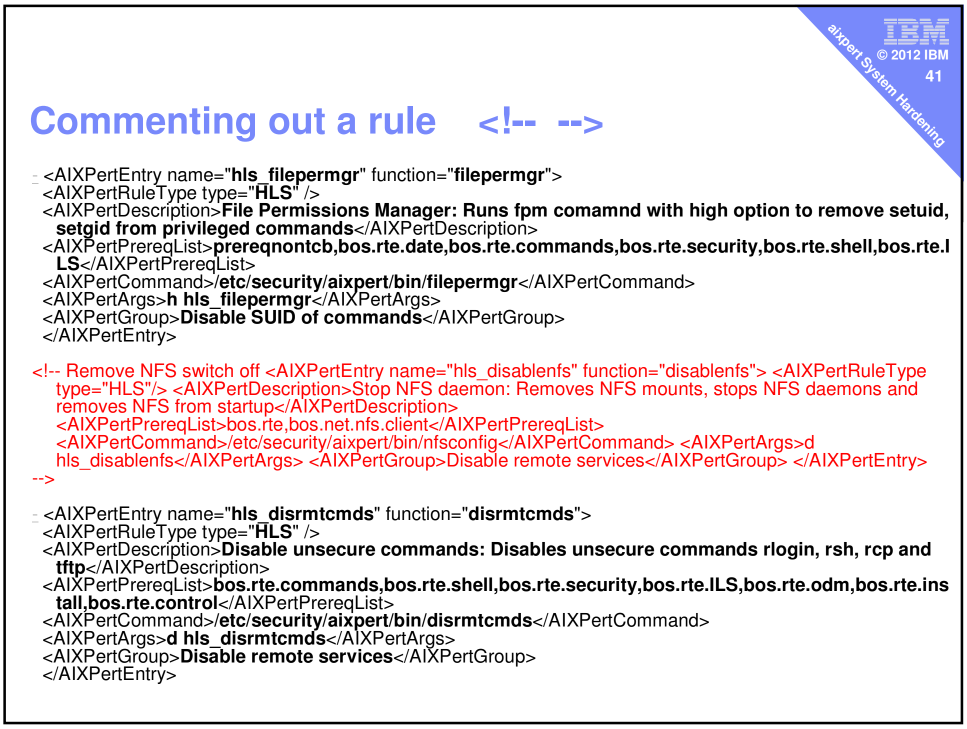
- Decide to never let “them catch me out”
- Decided to go for: aixpert -high
  - On AIX 6 TL7 this includes Port Scan Shun/blocking
    - A well known hacking method
    - Also used internally by the Thought Police ☺
  - So start reading the rule as a desk check



Making AIX Secure with aixpert

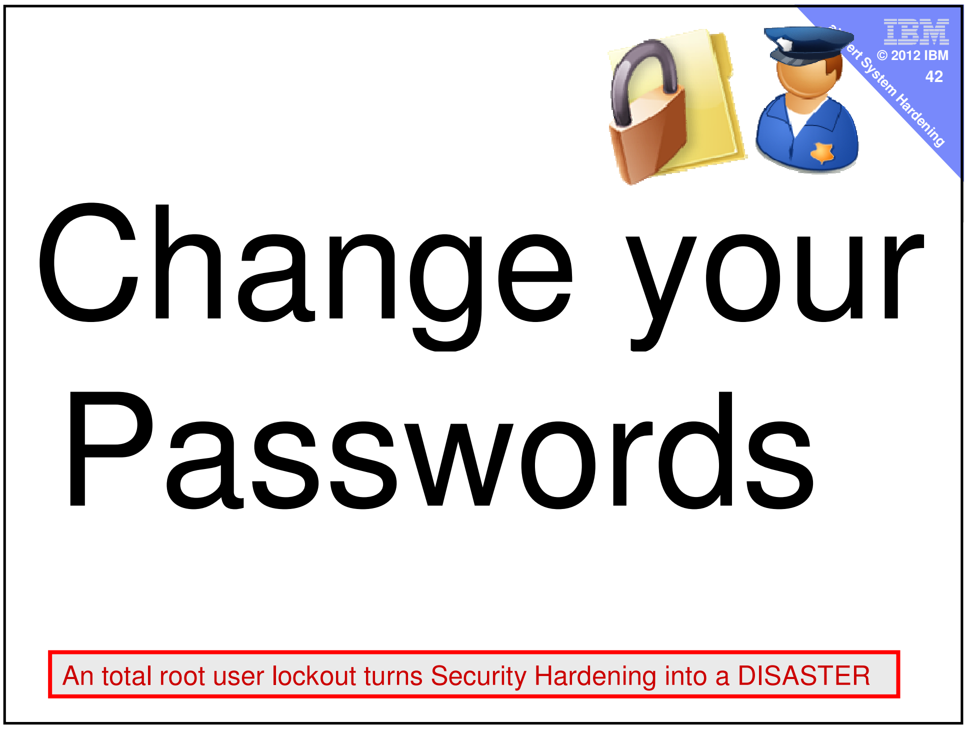
aixpert → high
✓No telnet or ftp

Exceptions we needed
✗TCB - Trusted Computing Base = Not installed
✗TCB Update – ditto
✗DNS - This machine is my Domain Name Server
✗Sendmail - Occasional use
✗NFS - OK, if no IBM Confidential content
✗X11 - We use VNCserver
✗ISS IBM Server Sensor - IBM virus checker ++



Commenting out a rule <!-- -->

```
- <AIXPertEntry name="hls_filepermgr" function="filepermgr">
  <AIXPertRuleType type="HLS" />
  <AIXPertDescription>File Permissions Manager: Runs fpm comamnd with high option to remove setuid,
    setgid from privileged commands</AIXPertDescription>
  <AIXPertPrereqList>prereqnontcb,bos.rte.date,bos.rte.commands,bos.rte.security,bos.rte.shell,bos.rte.I
    LS</AIXPertPrereqList>
  <AIXPertCommand>/etc/security/aixpert/bin/filepermgr</AIXPertCommand>
  <AIXPertArgs>h hls_filepermgr</AIXPertArgs>
  <AIXPertGroup>Disable SUID of commands</AIXPertGroup>
  </AIXPertEntry>

<!-- Remove NFS switch off <AIXPertEntry name="hls_disablenfs" function="disablenfs"> <AIXPertRuleType
    type="HLS"/> <AIXPertDescription>Stop NFS daemon: Removes NFS mounts, stops NFS daemons and
    removes NFS from startup</AIXPertDescription>
    <AIXPertPrereqList>bos.rte,bos.net.nfs.client</AIXPertPrereqList>
    <AIXPertCommand>/etc/security/aixpert/bin/nfsconfig</AIXPertCommand> <AIXPertArgs>d
    hls_disablenfs</AIXPertArgs> <AIXPertGroup>Disable remote services</AIXPertGroup> </AIXPertEntry>
-->

- <AIXPertEntry name="hls_disrmtcmds" function="disrmtcmds">
  <AIXPertRuleType type="HLS" />
  <AIXPertDescription>Disable unsecure commands: Disables unsecure commands rlogin, rsh, rcp and
    tftp</AIXPertDescription>
  <AIXPertPrereqList>bos.rte.commands,bos.rte.shell,bos.rte.security,bos.rte.ILS,bos.rte.odm,bos.rte.ins
    tall,bos.rte.control</AIXPertPrereqList>
  <AIXPertCommand>/etc/security/aixpert/bin/disrmtcmds</AIXPertCommand>
  <AIXPertArgs>d hls_disrmtcmds</AIXPertArgs>
  <AIXPertGroup>Disable remote services</AIXPertGroup>
  </AIXPertEntry>
```

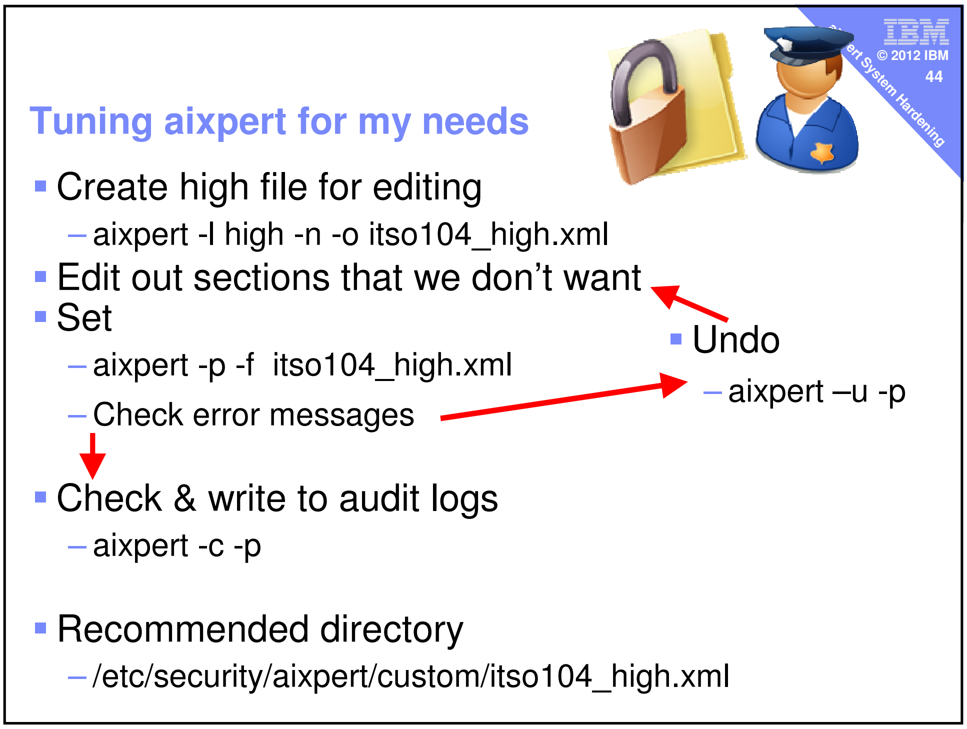


Change your Passwords

An total root user lockout turns Security Hardening into a DISASTER

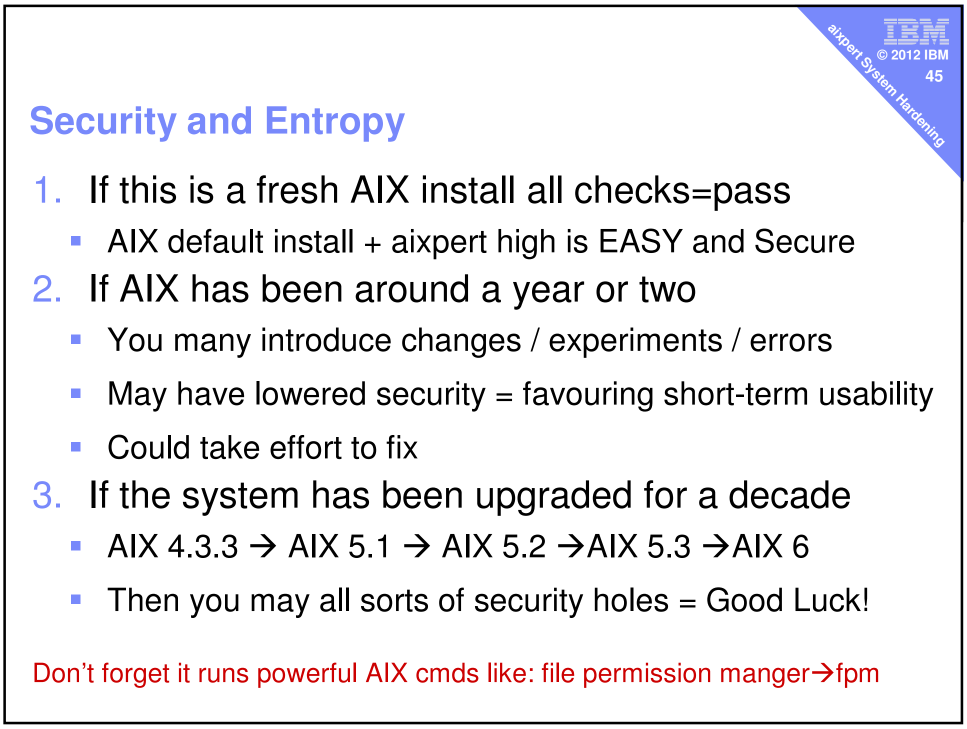
WARNING !!!

- High Level Security can mean too secure!
- Can lock the root user due to password aging
- So set your root password **before** using aixpert



Tuning aixpert for my needs

- Create high file for editing
  - aixpert -l high -n -o itso104_high.xml
- Edit out sections that we don't want
- Set
  - aixpert -p -f itso104_high.xml
  - Check error messages
- Undo
  - aixpert –u -p
- Check & write to audit logs
  - aixpert -c -p
- Recommended directory
  - /etc/security/aixpert/custom/itso104_high.xml



aixpert System Hardening

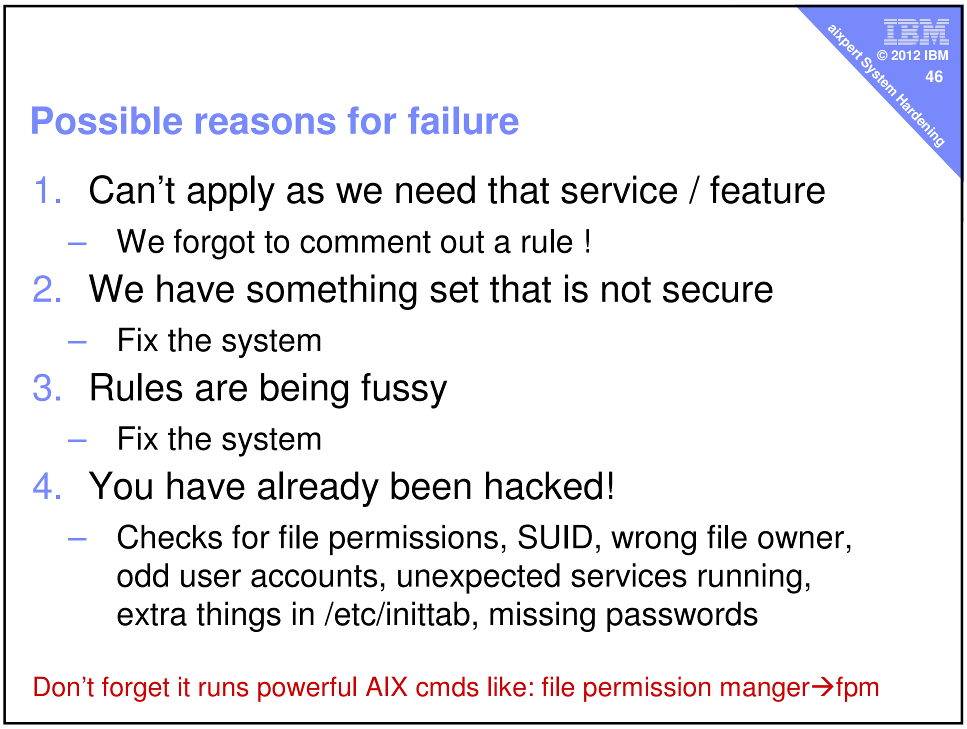
© 2012 IBM

45

Security and Entropy

1. If this is a fresh AIX install all checks=pass
   - AIX default install + aixpert high is EASY and Secure
2. If AIX has been around a year or two
   - You many introduce changes / experiments / errors
   - May have lowered security = favouring short-term usability
   - Could take effort to fix
3. If the system has been upgraded for a decade
   - AIX 4.3.3 → AIX 5.1 → AIX 5.2 →AIX 5.3 →AIX 6
   - Then you may all sorts of security holes = Good Luck!

Don’t forget it runs powerful AIX cmds like: file permission manger→fpm



aixpert System Hardening

© 2012 IBM

46

Possible reasons for failure

1. Can’t apply as we need that service / feature
   - We forgot to comment out a rule !
2. We have something set that is not secure
   - Fix the system
3. Rules are being fussy
   - Fix the system
4. You have already been hacked!
   - Checks for file permissions, SUID, wrong file owner, odd user accounts, unexpected services running, extra things in /etc/inittab, missing passwords

Don’t forget it runs powerful AIX cmds like: file permission manger→fpm

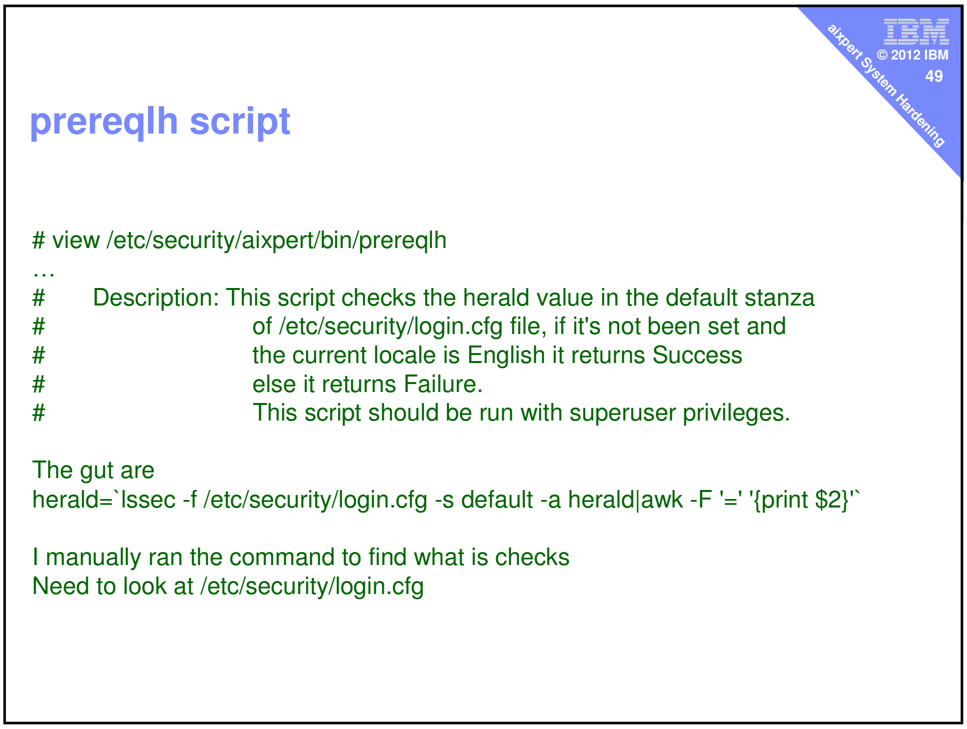
Worked example:

```
# aixpert -p -f itso104_high.xml
Processing prereqbinaudit :cached
Processing prereqcde :cached
Processing prereqgated :cached
Processing prereqipsec :cached
Processing prereqlft :cached
Processing prereqlh :cached
Processing prereqnosyn :cached
Processing prereqrl :cached
Processing prereqrrl :cached
Processing prereqsed :cached
Processing prereqnontcb :cached
Processing prereqRSSSFull :cached
Processing prereqRSSSLite :cached
Processing hls_minage .....:done.
Processing hls_maxage .....:done.
Processing hls_maxexpired .....:done.
Processing hls_minlen .....:done.
Processing hls_minalpha .....:done.
Processing hls_minother .....:done.
Processing hls_maxrepeats .....:done.
Processing hls_mindiff .....:done.
Processing hls_histexpire .....:done.
```

```
… 100+ of lines removed here
Processing hls_rfc1323 ......:done.
Processing hls_tcp_mssdflt ......:done.
Processing hls_sb_max ......:done.
Processing hls_tcp_tcpsecure ......:done.
Processing hls_sockthresh ......:done.
Processing hls_ipsecshunhost .......:done.
Processing hls_ipsecshunports ........:done.
Processing hls_umask .....:done.
Processing hls_core .....:done.
Processing hls_limitsysacc ....:done.
Processing hls_crontabperm ....:done.
Processing hls_loginherald ....: warning.
do_action(): Warning: Prereq failed for
   prereqlh
Processing hls_rmdotfrmpathroot .....:done.
Processing hls_rmdotfrmpathnroot ....:done.
Processing hls_chetcftpusers ....:done.
Processing hls_removeguest ....:done.
Processing hls_sedconfig ....:done.
Processing hls_rootpwdintchk .....:done.
Processing hls_tcptr .:done.
Processedrules=121      Passedrules=120
   Failedrules=1   Level=AllRules
       Input file=itso104_high.xml
```

Prereqlh → Login Herald

```
 # view itso104_high.xml

<AIXPertEntry name="prereqlh" function="prereqlh">
           <AIXPertRuleType type="Prereq"/>
           <AIXPertDescription>
          Prereq rule for loginherald: Checks the herald value is set or not
          </AIXPertDescription>
           <AIXPertPrereqList></AIXPertPrereqList>
           <AIXPertCommand>/etc/security/aixpert/bin/prereqlh</AIXPertCommand>
           <AIXPertArgs></AIXPertArgs>
           <AIXPertGroup></AIXPertGroup>
      </AIXPertEntry>

# Next to /etc/security/aixpert/bin/prereqlh
```



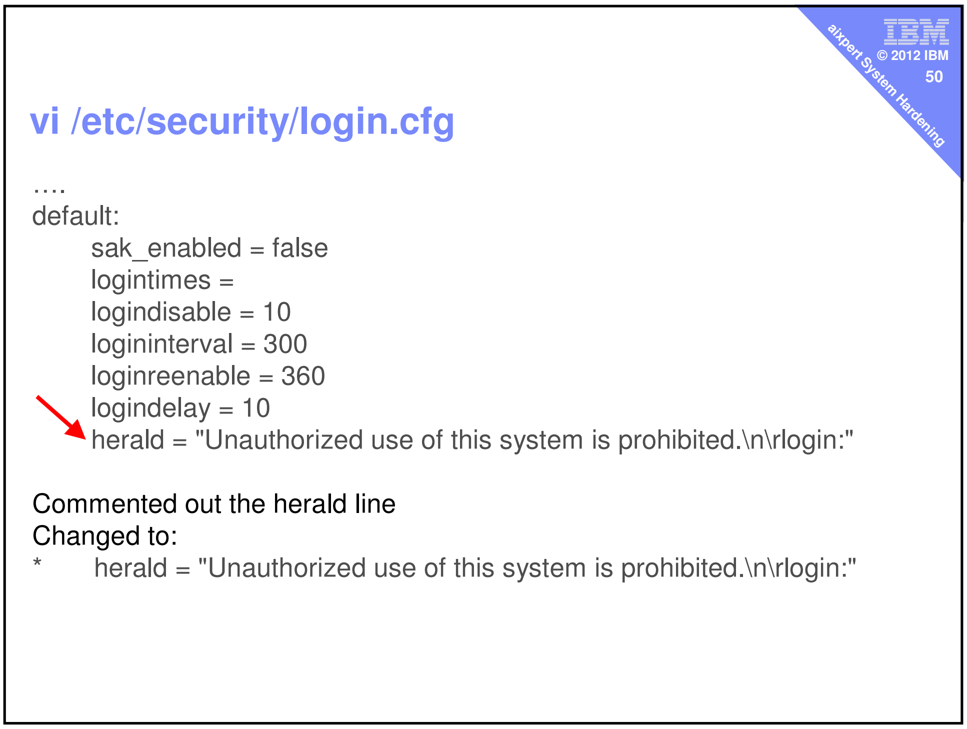
prereqlh script

```
# view /etc/security/aixpert/bin/prereqlh
…
#       Description: This script checks the herald value in the default stanza
#                           of /etc/security/login.cfg file, if it's not been set and
#                           the current locale is English it returns Success
#                           else it returns Failure.
#                           This script should be run with superuser privileges.
```

The gut are

```
herald=`lssec -f /etc/security/login.cfg -s default -a herald|awk -F '=' '{print $2}'`
```

I manually ran the command to find what is checks
Need to look at /etc/security/login.cfg

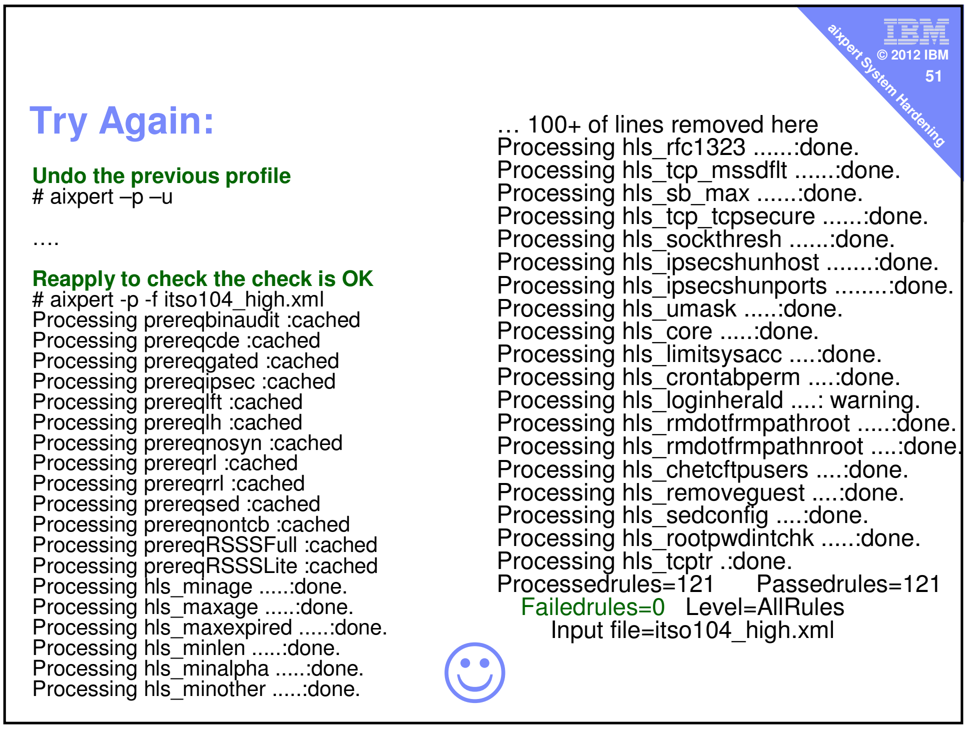


vi /etc/security/login.cfg

```
….
default:
        sak_enabled = false
        logintimes =
        logindisable = 10
        logininterval = 300
        loginreenable = 360
        logindelay = 10
        herald = "Unauthorized use of this system is prohibited.\n\rlogin:"
```

Commented out the herald line
Changed to:

```
*       herald = "Unauthorized use of this system is prohibited.\n\rlogin:"
```



Try Again:

Undo the previous profile

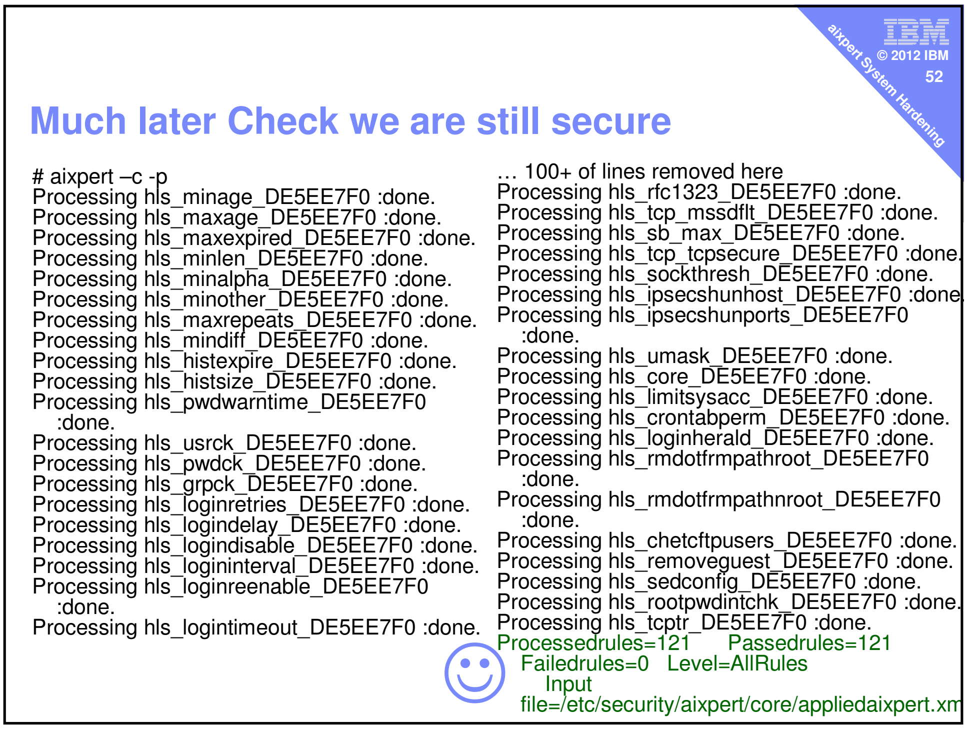
```
# aixpert –p –u

….
```

Reapply to check the check is OK

```
# aixpert -p -f itso104_high.xml
Processing prereqbinaudit :cached
Processing prereqcde :cached
Processing prereqgated :cached
Processing prereqipsec :cached
Processing prereqlft :cached
Processing prereqlh :cached
Processing prereqnosyn :cached
Processing prereqrl :cached
Processing prereqrrl :cached
Processing prereqsed :cached
Processing prereqnontcb :cached
Processing prereqRSSSFull :cached
Processing prereqRSSSLite :cached
Processing hls_minage .....:done.
Processing hls_maxage .....:done.
Processing hls_maxexpired .....:done.
Processing hls_minlen .....:done.
Processing hls_minalpha .....:done.
Processing hls_minother .....:done.
```

```
… 100+ of lines removed here
Processing hls_rfc1323 ......:done.
Processing hls_tcp_mssdflt ......:done.
Processing hls_sb_max ......:done.
Processing hls_tcp_tcpsecure ......:done.
Processing hls_sockthresh ......:done.
Processing hls_ipsecshunhost .......:done.
Processing hls_ipsecshunports ........:done.
Processing hls_umask .....:done.
Processing hls_core .....:done.
Processing hls_limitsysacc ....:done.
Processing hls_crontabperm ....:done.
Processing hls_loginherald ....: warning.
Processing hls_rmdotfrmpathroot .....:done.
Processing hls_rmdotfrmpathnroot ....:done.
Processing hls_chetcftpusers ....:done.
Processing hls_removeguest ....:done.
Processing hls_sedconfig ....:done.
Processing hls_rootpwdintchk .....:done.
Processing hls_tcptr .:done.
Processedrules=121      Passedrules=121
    Failedrules=0   Level=AllRules
       Input file=itso104_high.xml
```

☺



Much later Check we are still secure

```
# aixpert –c -p
Processing hls_minage_DE5EE7F0 :done.
Processing hls_maxage_DE5EE7F0 :done.
Processing hls_maxexpired_DE5EE7F0 :done.
Processing hls_minlen_DE5EE7F0 :done.
Processing hls_minalpha_DE5EE7F0 :done.
Processing hls_minother_DE5EE7F0 :done.
Processing hls_maxrepeats_DE5EE7F0 :done.
Processing hls_mindiff_DE5EE7F0 :done.
Processing hls_histexpire_DE5EE7F0 :done.
Processing hls_histsize_DE5EE7F0 :done.
Processing hls_pwdwarntime_DE5EE7F0
    :done.
Processing hls_usrck_DE5EE7F0 :done.
Processing hls_pwdck_DE5EE7F0 :done.
Processing hls_grpck_DE5EE7F0 :done.
Processing hls_loginretries_DE5EE7F0 :done.
Processing hls_logindelay_DE5EE7F0 :done.
Processing hls_logindisable_DE5EE7F0 :done.
Processing hls_logininterval_DE5EE7F0 :done.
Processing hls_loginreenable_DE5EE7F0
    :done.
Processing hls_logintimeout_DE5EE7F0 :done.
```

```
… 100+ of lines removed here
Processing hls_rfc1323_DE5EE7F0 :done.
Processing hls_tcp_mssdflt_DE5EE7F0 :done.
Processing hls_sb_max_DE5EE7F0 :done.
Processing hls_tcp_tcpsecure_DE5EE7F0 :done.
Processing hls_sockthresh_DE5EE7F0 :done.
Processing hls_ipsecshunhost_DE5EE7F0 :done.
Processing hls_ipsecshunports_DE5EE7F0
    :done.
Processing hls_umask_DE5EE7F0 :done.
Processing hls_core_DE5EE7F0 :done.
Processing hls_limitsysacc_DE5EE7F0 :done.
Processing hls_crontabperm_DE5EE7F0 :done.
Processing hls_loginherald_DE5EE7F0 :done.
Processing hls_rmdotfrmpathroot_DE5EE7F0
    :done.
Processing hls_rmdotfrmpathnroot_DE5EE7F0
    :done.
Processing hls_chetcftpusers_DE5EE7F0 :done.
Processing hls_removeguest_DE5EE7F0 :done.
Processing hls_sedconfig_DE5EE7F0 :done.
Processing hls_rootpwdintchk_DE5EE7F0 :done.
Processing hls_tcptr_DE5EE7F0 :done.
Processedrules=121      Passedrules=121
    Failedrules=0   Level=AllRules
        Input
    file=/etc/security/aixpert/core/appliedaixpert.xm
```

☺

Check writes to /etc/security/aixpert/check_report.txt

```
…
***** blue.aixncc.uk.ibm.com : Aug 21 11:20:59 ******

comntrows.sh: Daemon/Script/String:lpd: should have status disabled, however its entry is not
   found in file /etc/inittab
comntrows.sh: Daemon/Script/String:dt: should have status disabled, however its entry is not
   found in file /etc/inittab
cominetdconf.sh: Service dtspc should have status d, however its entry is missing from
   /etc/inetd.conf
cominetdconf.sh: Service ttdbserver should have status d, however its entry is missing from
   /etc/inetd.conf
cominetdconf.sh: Service cmsd should have status d, however its entry is missing from
   /etc/inetd.conf
```

I prefer a missing /etc/inittab entries than a commented out ones ☺

Check writes to /etc/security/aixpert/log/*

```
…
***** blue.aixncc.uk.ibm.com : Aug 21 11:20:59 ******

comntrows.sh: Daemon/Script/String:lpd: should have status disabled, however its entry is not found in file /etc/inittab
comntrows.sh: Daemon/Script/String:dt: should have status disabled, however its entry is not found in file /etc/inittab
cominetdconf.sh: Service dtspc should have status d, however its entry is missing from /etc/inetd.conf
cominetdconf.sh: Service ttdbserver should have status d, however its entry is missing from /etc/inetd.conf
cominetdconf.sh: Service cmsd should have status d, however its entry is missing from /etc/inetd.conf
```

I prefer missing /etc/inittab entries than a commented out ones ☺

aixpert & PowerSC

“aixpert” and PowerSC Standard Edition

- PowerSC Security Hardening & Compliance
  - Relies on the AIX “aixpert” command & XML profiles
  - Includes extra profiles too
  - You then create a mixture of tuned profiles for you specific needs & server workloads
  - These profiles are loaded in to the IBM Systems Director (ISD) plus Profile Manager plug-in
- ISD then used to
  - rolled out profiles across 1000’s of AIX Virtual Machines
  - check compliance with the profile & report

PowerSC Express

- Security Hardening & Compliance
- Includes all these files
- Difficult to find out the contents
- New aixpert security checker commands
- New XML profiles

```
# lslpp -f  powerscExp.ice.cmds
powerscExp.ice.cmds 1.1.0.0
/etc/security/aixpert/ICEEXP0102.SYS2
/etc/security/aixpert/README.ICEexpress
/etc/security/aixpert/bin/SSHfordataxchg
/etc/security/aixpert/bin/aha
/etc/security/aixpert/bin/autologoff
/etc/security/aixpert/bin/chcronfiles
/etc/security/aixpert/bin/chdodftpusers
/etc/security/aixpert/bin/chetchostsfiles
/etc/security/aixpert/bin/chowndodfiles
/etc/security/aixpert/bin/chsshd_config
/etc/security/aixpert/bin/chsyslog
/etc/security/aixpert/bin/chusrattrdod
/etc/security/aixpert/bin/ckextcompliance
/etc/security/aixpert/bin/comntrowsdod
/etc/security/aixpert/bin/configrepomgmt
/etc/security/aixpert/bin/disableacct
/etc/security/aixpert/bin/dodaudit
/etc/security/aixpert/bin/efsKSonLDAP
/etc/security/aixpert/bin/erroreporting
/etc/security/aixpert/bin/fpmdodfiles
/etc/security/aixpert/bin/logindodherald
/etc/security/aixpert/bin/manageITsecurity
/etc/security/aixpert/bin/managephyaccess
/etc/security/aixpert/bin/manageprtrsrvc
/etc/security/aixpert/bin/mvhostsfiles
/etc/security/aixpert/bin/pciaudit
/etc/security/aixpert/bin/prereqTE
/etc/security/aixpert/bin/prereqahafs
/etc/security/aixpert/bin/prereqcefs
/etc/security/aixpert/bin/prereqda
/etc/security/aixpert/bin/protsectech
/etc/security/aixpert/bin/rmdotfrmpathvar
/etc/security/aixpert/bin/securitymonitor
/etc/security/aixpert/bin/update_tcb
/etc/security/aixpert/bin/updateshells
/etc/security/aixpert/custom/DoD.xml
/etc/security/aixpert/custom/DoD_to_AIXDefault.xml
/etc/security/aixpert/custom/PCI.xml
/etc/security/aixpert/custom/PCI_to_AIXDefault.xml
/etc/security/aixpert/custom/SOX-COBIT.xml
//etc/security/aixpert/undo/data/aix_default
/etc/security/aixpert/undo/data/dod_high
/etc/security/aixpert/undo/data/sox-cobit.inp
```

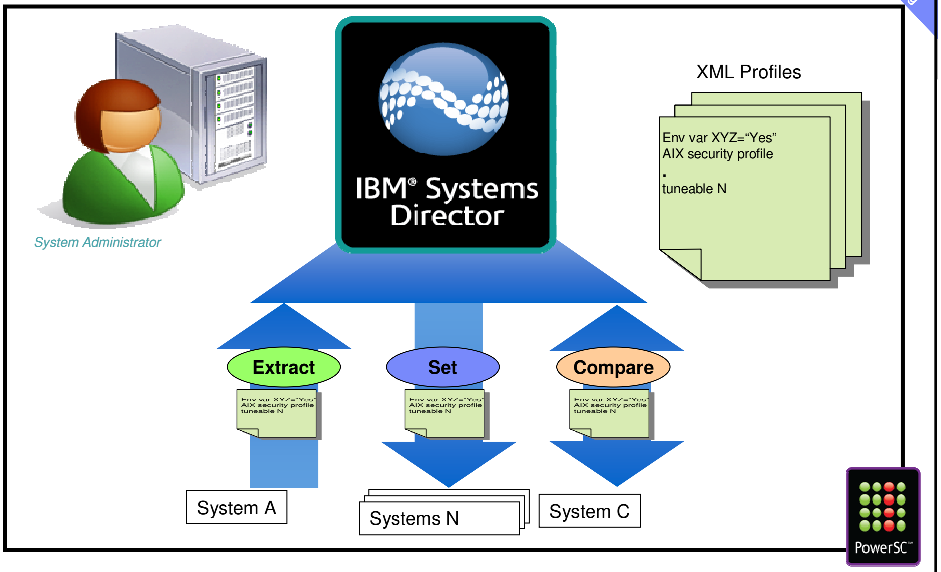
PowerSC™

Install PowerSC Express - powerscExp.ice

- Extra XML Profiles
  - USA Department of Defence - DoD
  - Payment Card Industry security standard -PCI
  - SOX-Cobit Banking standard
- All get put in /etc/security/aixpert/custom
  - 42 rules DoD.xml
  - 41 rules DoD_to_AIXDefault.xml
  - 90 rules PCI.xml
  - 83 rules PCI_to_AIXDefault.xml
  - 24 rules SOX-COBIT.xml
- In total 280 rules

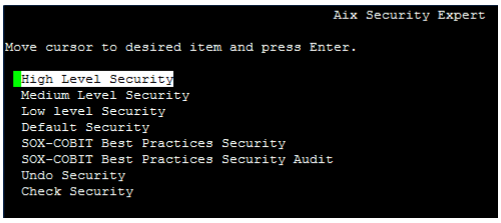
PowerSC™

aixpert Profiles & System Director + PowerSC Profile Manager plug-in to roll out across the estate

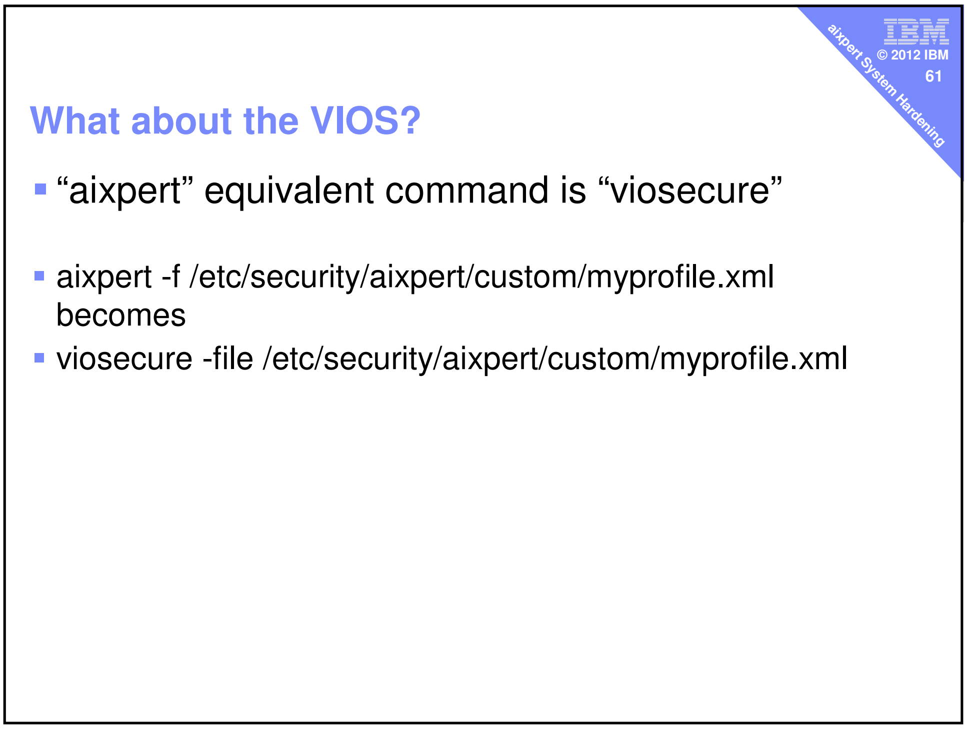


smitty = problematic

- smitty aixpert
- Only allows supplied profiles
- WARNING: don't play in here:
  You may "accidentally" apply security which kills telnet, blocks remote root & times out your passwords
- Does selecting High Level immediately apply it?



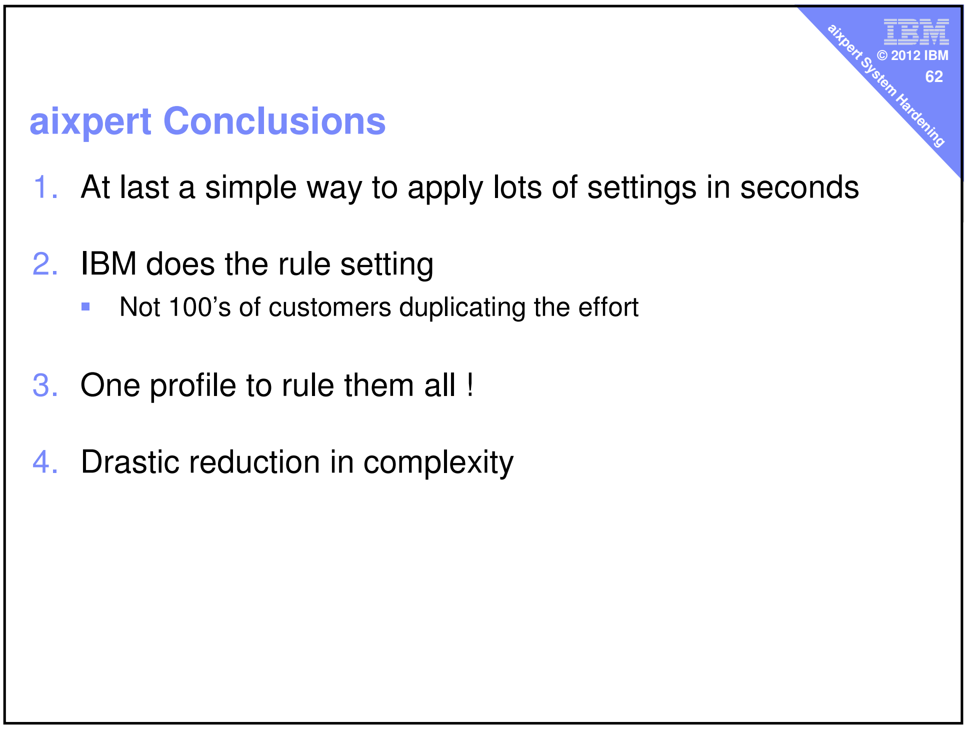
```
                                        Aix Security Expert

Move cursor to desired item and press Enter.

  High Level Security
  Medium Level Security
  Low level Security
  Default Security
  SOX-COBIT Best Practices Security
  SOX-COBIT Best Practices Security Audit
  Undo Security
  Check Security
```



What about the VIOS?

- “aixpert” equivalent command is “viosecure”

- aixpert -f /etc/security/aixpert/custom/myprofile.xml becomes
- viosecure -file /etc/security/aixpert/custom/myprofile.xml



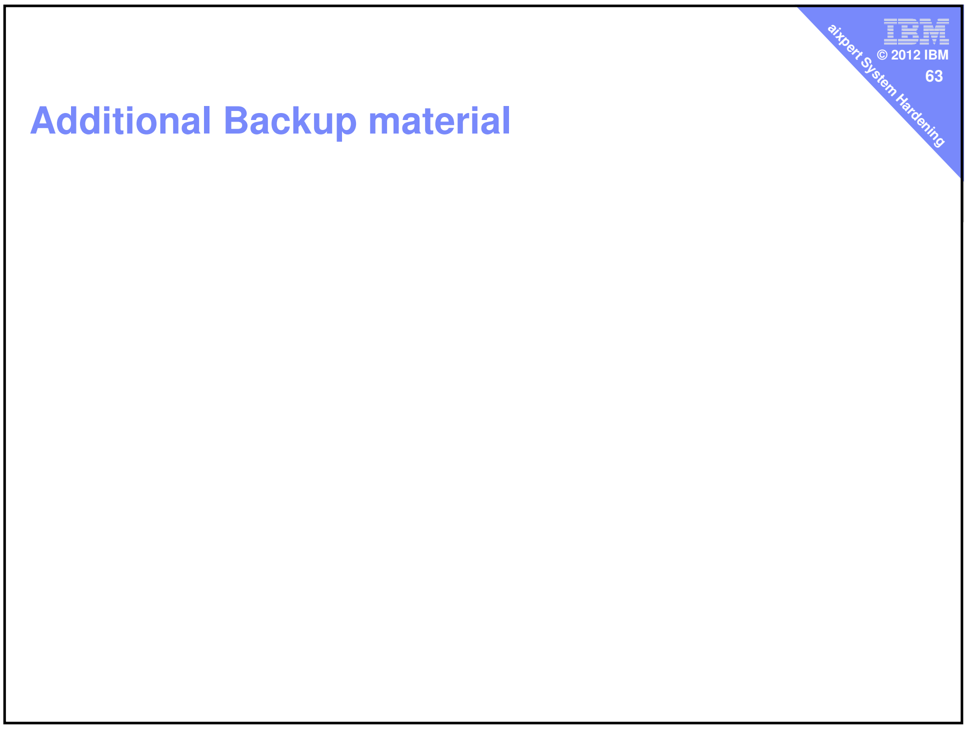
aixpert Conclusions

1. At last a simple way to apply lots of settings in seconds

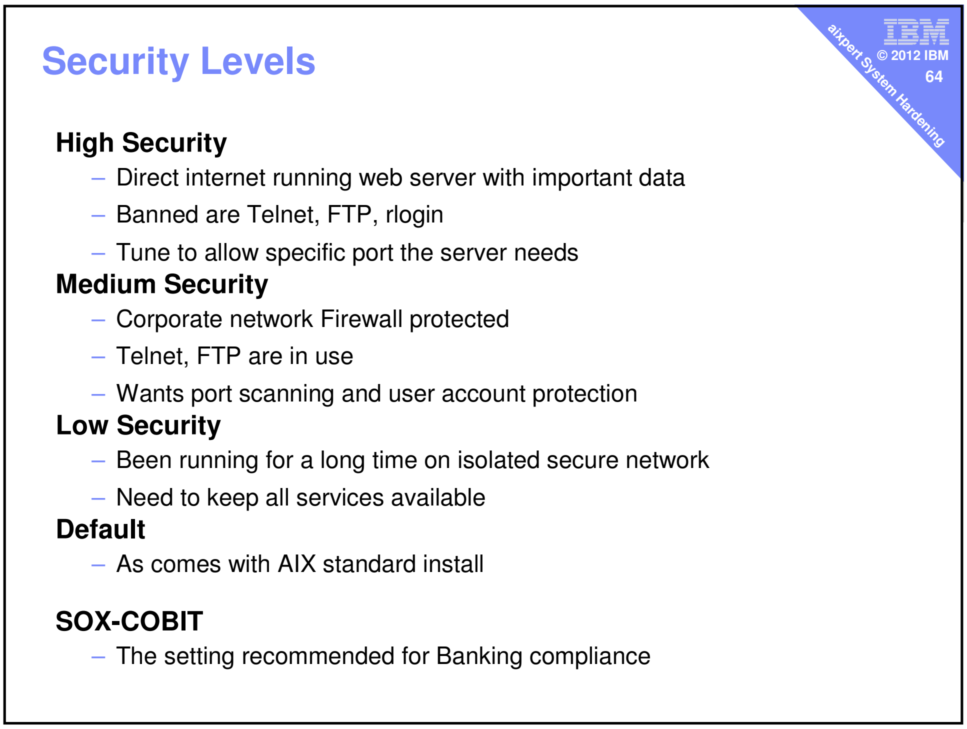
2. IBM does the rule setting
   - Not 100’s of customers duplicating the effort

3. One profile to rule them all !

4. Drastic reduction in complexity



Additional Backup material



Security Levels

High Security
- Direct internet running web server with important data
- Banned are Telnet, FTP, rlogin
- Tune to allow specific port the server needs

Medium Security
- Corporate network Firewall protected
- Telnet, FTP are in use
- Wants port scanning and user account protection

Low Security
- Been running for a long time on isolated secure network
- Need to keep all services available

Default
- As comes with AIX standard install

SOX-COBIT
- The setting recommended for Banking compliance

Underlying aixpert Files

- **/etc/security/aixpert/core/aixpertall.xml**
  XML file of all possible settings
- **/etc/security/aixpert/core/appliedaixpert.xml**
  XML file of applied security
- **/etc/security/aixpert/log/aixpert.log**
  Trace log of applied settings
  Does not use syslog, aixpert writes directly to this file
- **/etc/security/aixpert/core/undo.xml**
  XLM file of settings, which can be undone

Further example

- Morten Vagmo IBM Norway
- Looks at the new PCI profile

Example 2: Applying PCI.xml with a failure

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85 Passedrules=84 Failedrules=1
  Level=AllRules
```

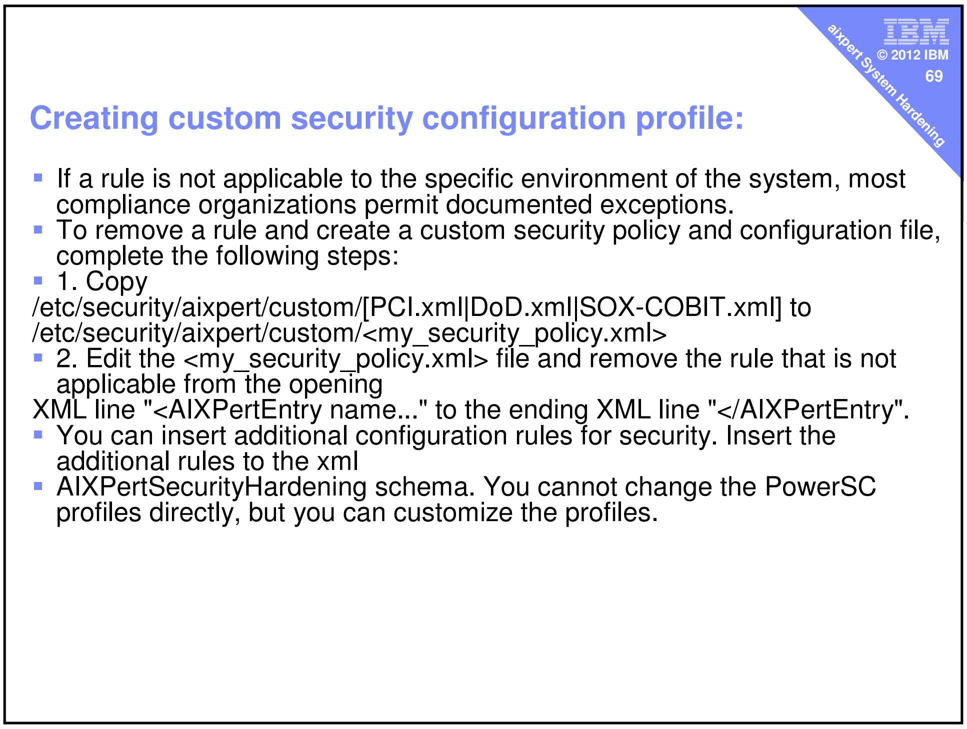
- Input file=/etc/security/aixpert/custom/PCI.xml
- The failure of pci_grpck rule must be resolved. The possible causes for failure include the following
- reason:
  - The rule does not apply to the environment and must be removed.
  - There is an issue on the system that must be fixed.

Investigating a failed rule

- View the /etc/security/aixpert/custom/PCI.xml file and locate the failing rule. In this example the rule is pci_grpck. Run the **fgrep** command, search the pci_grpck failing rule, and see the associated XML rule.

```
#fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml

    <AIXPertEntry name="pci_grpck" function="grpck"
    <AIXPertRuleType type="DLS"/
    <AIXPertDescription&gt;Implements portions of PCI Section 8.2,
    Check group definitions: Verifies the correctness of group definitions and fixes the errors
    </AIXPertDescription
    <AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
    <AIXPertCommand
    /etc/security/aixpert/bin/execmds</AIXPertCommand
    <AIXPertArgs
    "/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
    <AIXPertGroup
    User Group System and Password Definitions</AIXPertGroup
    </AIXPertEntry
```

- From the pci_grpck rule, the /usr/sbin/grpck command can be seen.



Creating custom security configuration profile:

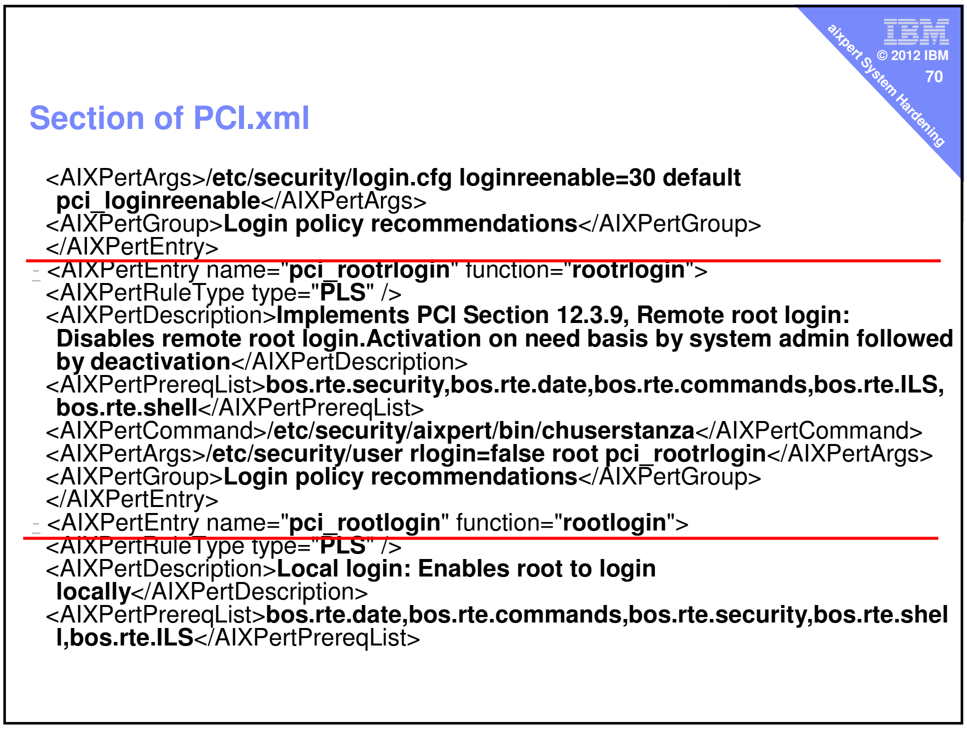
- If a rule is not applicable to the specific environment of the system, most compliance organizations permit documented exceptions.
- To remove a rule and create a custom security policy and configuration file, complete the following steps:
- 1. Copy

/etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml] to
/etc/security/aixpert/custom/<my_security_policy.xml>

- 2. Edit the <my_security_policy.xml> file and remove the rule that is not applicable from the opening

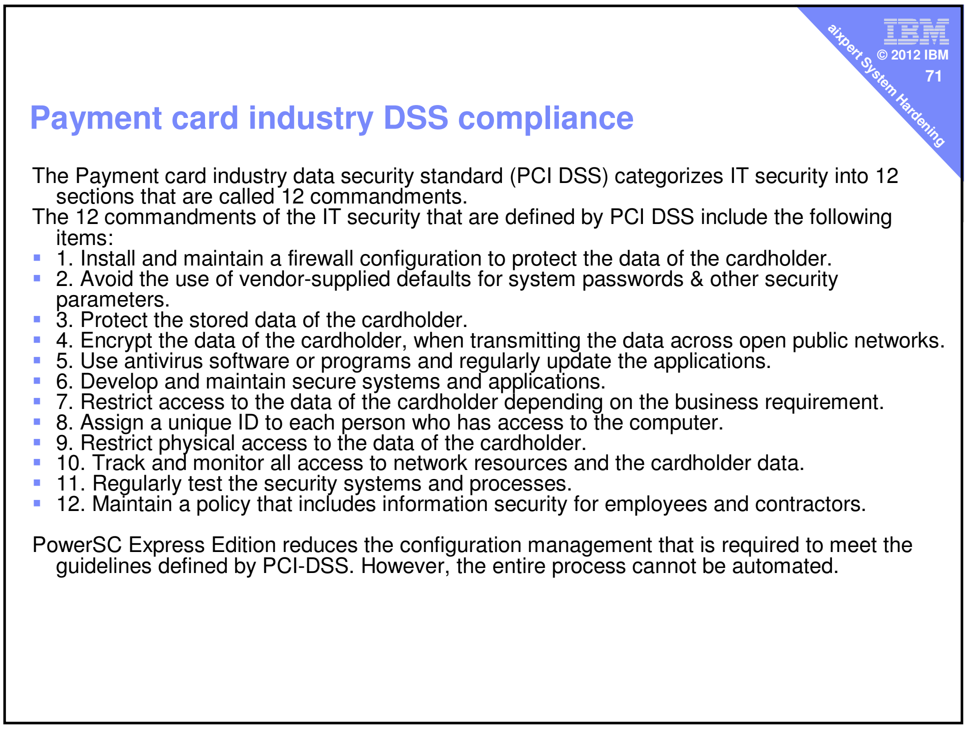
XML line "<AIXPertEntry name..." to the ending XML line "</AIXPertEntry".

- You can insert additional configuration rules for security. Insert the additional rules to the xml
- AIXPertSecurityHardening schema. You cannot change the PowerSC profiles directly, but you can customize the profiles.



Section of PCI.xml

```
<AIXPertArgs>/etc/security/login.cfg loginreenable=30 default
 pci_loginreenable</AIXPertArgs>
<AIXPertGroup>Login policy recommendations</AIXPertGroup>
</AIXPertEntry>
- <AIXPertEntry name="pci_rootrlogin" function="rootrlogin">
<AIXPertRuleType type="PLS" />
<AIXPertDescription>Implements PCI Section 12.3.9, Remote root login:
 Disables remote root login.Activation on need basis by system admin followed
 by deactivation</AIXPertDescription>
<AIXPertPrereqList>bos.rte.security,bos.rte.date,bos.rte.commands,bos.rte.ILS,
 bos.rte.shell</AIXPertPrereqList>
<AIXPertCommand>/etc/security/aixpert/bin/chuserstanza</AIXPertCommand>
<AIXPertArgs>/etc/security/user rlogin=false root pci_rootrlogin</AIXPertArgs>
<AIXPertGroup>Login policy recommendations</AIXPertGroup>
</AIXPertEntry>
- <AIXPertEntry name="pci_rootlogin" function="rootlogin">
<AIXPertRuleType type="PLS" />
<AIXPertDescription>Local login: Enables root to login
 locally</AIXPertDescription>
<AIXPertPrereqList>bos.rte.date,bos.rte.commands,bos.rte.security,bos.rte.shel
 l,bos.rte.ILS</AIXPertPrereqList>
```



Payment card industry DSS compliance

The Payment card industry data security standard (PCI DSS) categorizes IT security into 12 sections that are called 12 commandments.

The 12 commandments of the IT security that are defined by PCI DSS include the following items:

- 1. Install and maintain a firewall configuration to protect the data of the cardholder.
- 2. Avoid the use of vendor-supplied defaults for system passwords & other security parameters.
- 3. Protect the stored data of the cardholder.
- 4. Encrypt the data of the cardholder, when transmitting the data across open public networks.
- 5. Use antivirus software or programs and regularly update the applications.
- 6. Develop and maintain secure systems and applications.
- 7. Restrict access to the data of the cardholder depending on the business requirement.
- 8. Assign a unique ID to each person who has access to the computer.
- 9. Restrict physical access to the data of the cardholder.
- 10. Track and monitor all access to network resources and the cardholder data.
- 11. Regularly test the security systems and processes.
- 12. Maintain a policy that includes information security for employees and contractors.

PowerSC Express Edition reduces the configuration management that is required to meet the guidelines defined by PCI-DSS. However, the entire process cannot be automated.