Pieter Meulemeester

PAM

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

Vraagjes:

1. Waar bevinden zich de PAM-modules?

default bevinden de modules zich in /lib/security

2. Waar bevinden zich de configuratiebestanden?

in /etc/pam.d directory (meerdere configuratie-

bestanden) of /etc/pam.conf (bestand)

3. Welke PAM-module wordt gebruikt voor het controleren van

de login-gegevens aan de hand van de /etc/passwd-file?

pam\_unix🡺auth

4. Welke PAM-module kan je gebruiken om de sterkte van

wachtwoorden te checken?

pam\_pwcheck

5. Bekijk de inhoud van deze file (system-auth.txt) en

beschrijf het authenticatieproces.

eerst worden omgevingsvariabelen geset door de module pam\_env

vervolgens wordt het paswoord gecontroleerd (pam\_unix module)

ten slotte wordt de uid gecontroleerd, als die >= 500 is,

dan is het ok, anders wordt de gebruiker niet toegelaten (pam\_deny)

voorbereiding: 2 gebruikers aanmaken

------------------------------------

specificatie:

- gebruiker1: uid>500 en gid>500

- gebruiker2: uid<500 en gid<500

- beide gebuikers hebben een wachtwoord.

su (inloggen als root)

(eerst controleren als de gebruikte id's al niet bestaan)

groupadd -g 520 groep1

groupadd -g 420 groep2

useradd -u 520 -g 520 gebruiker1

useradd -u 420 -g 420 gebruiker2

passwd gebruiker1

passwd gebruiker2

controle: bekijken /etc/passwd & /etc/group

-> users en groepen zitten er in, ID's kloppen

backup van /etc/pam.d/system-auth-ac

cp system-auth-ac system-auth-ac\_backup

controle: ls -al /etc/pam.d -> bestanden zijn even groot

1. Configureer PAM zodat de meeste modules debug-informatie

wegschrijven.

Vraag: In welk(e) bestand(en) komt deze informatie terecht?

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

debug-informatie:

bij de modules de parameter 'debug' plaatsen

testen:

auth requisite pam\_succeed\_if.so uid < 500 debug

auth required pam\_env.so debug

auth sufficient pam\_fprintd.so debug

-> als gebruiker: su gebruiker2

'\*\* Message: debug on' wordt getoond op scherm

bekijken in /var/log/messages -> actie wordt geregistreerd

in dit log

bij de configuratiebestanden debug parameter ingeven

Vraag: in de syslog, standaard: /var/log/messages

2. Pas de configuratie aan zodat een gebruiker 5 kansen

krijgt om een aanvaardbaar nieuw wachtwoord in te geven bij

het wijzigen van zijn wachtwoord.

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

password required pam\_cracklib.so try\_first\_pass retry=5

type=

test:

passwoord veranders als gebruiker1:

passwd commando

-> huidig wachtwoord ingeven

-> 5 keer een te kort wachtwoord ingeven, bvb: 1 letter

-> test geslaagd

test voor gebruiker2:

passwd comamndo

-> huidig wachtwoord ingeven

-> 5 keer een te kort wachtwoord ingeven, bvb: 1 letter

-> test geslaagd

probleem:

de test met de pamtester bleef paswoorden vragen

opgelost: inloggen in een terminal en zelf met behulp van

het passwd commando 5 keer een te kort wachtwoord ingeven.

Dit lukte.

3. Pas het systeem aan zodat gebruikers met uid>500 niet

kunnen inloggen en die met een uid<500 wel. Test uit met

de nieuw aangemaakte gebruikers.

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

nano /etc/pam.d/system-auth

-> deze regel aanpassen: auth requisite pam\_succeed\_if.so

uid >= 500 quiet

veranderen naar: auth requisite pam\_succeed\_if.so uid

< 500

met pamtester:

[root@huygens ~]# pamtester login gebruiker1 authenticate

pamtester: Authentication failure

[root@huygens ~]# pamtester login gebruiker2 authenticate

\*\* Message: debug on

Password: <-- paswoord hier

pamtester: successfully authenticated

4. Bij systeemonderhoud is het wenselijk dat niet-root-

gebruikers zich voor een bepaalde tijd niet kunnen

aanmelden; pas dit toe voor ssh en niet voor login. Zorg

hiervoor en maak dat gebruikers die dit toch proberen een

passende boodschap te zien krijgen.

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

/etc/nologin bestand aanmaken met de gepaste boodschap

echo "inloggen is nu niet mogelijk, onderhoudswerken zijn

bezig" > /etc/nologin

in /etc/pam.d/sshd het volgende aanbrengen:

auth required pam\_nologin.so

test: met ssh vanop ising.groep14.iii.hogent.be proberen

connecteren naar huygens.groep14.iii.hogent.be

commando: ssh tiwi1@huygens.groep14.iii.hogent.be

resultaat: "inloggen is nu niet mogelijk, onderhoudswerken

zijn bezig"

connection closed by 192.168.64.1

5. Configureer PAM zodat gebruiker1 enkel kan inloggen

vanop één van de buurcomputers.

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

in het bestand /etc/security/access.conf

+:gebruiker1:192.168.64.0/24

-:ALL:ALL

in system-auth:

auth requisite pam\_access.so

6. Configureer PAM zodanig dat root uitsluitend nog kan

inloggen vanop tty4. Vergeet niet om root nog steeds

ingelogd te houden op 1 andere console!

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

het bestand /etc/securetty aanpassen. dit bestand

specifieert vanop welke tty's de root kan inloggen.

-> alle regels in commentaar zetten (# ervoor)

behalve de regel die tty4 bevat, en opslaan

test: ttyX openen:

ctrl+alt+fX tegelijkertijd indrukken

test op tty3

vraagt login -> root ingeven

vraagt paswoord -> paswoord ingeven

tty zegt boodschap: login incorect

-> test geslaagd

test op tty4

vraagt login -> root ingeven

vraagt paswoord -> paswoord ingeven

inloggen gelukt

-> test geslaagd

test op tty5

vraagt login -> root ingeven

vraagt paswoord -> paswoord ingeven

tty zegt boodschap: login incorect

-> test geslaagd

problemen die ik had:

bij het inloggen vanop tty4 kreeg ik bij het

ingeven van een correct wachtwoord hetzelfde effect als

bij tty3 en tty5

oorzaak: ik had bij het ingeven van het wachtwoord

(e=mc\*\*2) voor de laatste 3 tekens gebruik gemaakt van het

keypad, blijkbaar wordt dit niet ondersteund bij

consolelogins

oplossing: shift + andere\_toets combinatie gebruiken om het

zelfde effect te krijgen, en volledige test herhalen.

Toen kreeg ik het gewenste effect

7. Zorg ervoor dat lokaal inloggen en inloggen via ssh

enkel mogelijk is op donderdagen van 10 tot 12. Uiteraard

pas je deze tijden aan om de kunnen testen.

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

/etc/pam.d/sshd en /etc/pam.d/login aanpassen:

nano /etc/pam.d/sshd

nano /etc/pam.d/login

volgende regel toevoegen aan de bestanden (indien nog niet

aanwezig)

account required pam\_time.so

vervolgens /etc/security/time.conf aanpassen:

login;\*;\*;Th1000-1200

sshd;\*;\*;Th1000-1200

gewoon voor de zekerheid de service herstarten

service sshd restart

test:

via ssh vanop ising onloggen op huygens op een ongeldig

tijdstip:

-> ssh tiwi1@huygens.groep14.iii.hogent.be

--> melding: 'Connection has been closed by 192.168.64.1'

via ssh vanop ising inloggen op huygens op een geldig

tijdstip

-> ssh tiwi1@huygens.groep14.iii.hogent.be

-> inloggen geslaagd

Pamtester lukt niet thuis

-> getest met inloggen op tty2

tijdens een ongeldig tijdstip:

gegevens ingeven

toont op scherm:

permission denied

--> inloggen lukt niet -> test geslaagd

tijdens een geldig tijdstip:

gegevens ingeven

--> inloggen lukt -> test geslaagd

8. Zorg ervoor dat lokaal inloggen en inloggen via ssh

enkel mogelijk is op maandagen en vrijdagen voor gebruiker1

en gebruiker2.

Uiteraard pas je deze tijden aan om de kunnen testen.

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

de instellingen van /etc/pam.d/sshd behouden (na de vorige

vraag)

/etc/pam.d/login idem

/etc/security/time.conf aanpassen:

sshd ; \* ; gebruiker1 | gebruiker2 ; MoFr0000-2400

login; \* ; gebruiker1 | gebruiker2 ; MoFr0000-2400

test inloggen op tty2 op een ongeldig tijdstip:

correcte inloggegevens ingeven

-> 'permission denied' komt op het scherm

--> test geslaagd

test inloggen op tty2 op een geldig tijdstip:

correcte inloggegevens ingeven

-> inloggen lukt

--> test geslaagd

inloggen met ssh

vanop ising met ssh inloggen op huygens tijdens een

ongeldig tijdstip:

ssh gebruiker1@huygens.groep14.iii.hogent.be

'connection closed by 192.168.64.1' wordt weergegeven op het

scherm

-> inloggen is mislukt

--> test geslaagd

vanop ising met ssh inloggen op huygens tijdens een geldig

tijdstip:

ssh gebruiker1@huygens.groep14.iii.hogent.be

-> inloggen lukt

--> test geslaagd

9. Wat gebeurt er indien iemand zich aanmeldt via een

service die niet voorkomt in de directory /etc/pam.d?

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

Dan wordt de configuratie van /etc/pam.d/other gebruikt