

Uma breve introdução à gerência de contas de  
usuário em sistemas GNU/Linux  
(aka crash course on Linux User Account  
Management :))  
Prof. Rossano Pablo Pinto  
03/2019 - v0.7  
(em construção)

# Agenda

- Introdução
- Usuários locais
- Criação/Modificação/Deleção de contas de usuário
- Senhas criptografadas em `/etc/shadow`
- Prática

# Introdução

- Sistemas multiusuário precisam conhecer seus usuários
  - Precisam de base de usuários
  - Usuários podem representar pessoas
  - Usuários podem representar sistemas/serviços
  - Usuários podem possuir papéis distintos
    - Usuários administrativos (root, bin, etc...)
    - Usuários não-administrativos
    - Usuários “serviços” (apache, postgres, avahi, sshd, etc...)

# Introdução

- Sistemas com vários usuários são mais fáceis de administrar pensando em grupo
  - Usuários são organizados em grupos
  - Precisam de base de grupos
- Mecanismos de Autenticação
  - Exemplos:
    - PAM: Pluggable Authentication Modules
    - Kerberos: third-party cryptographic authentication

# Introdução

- Isso nos leva ao **CONTROLE DE ACESSO**
  - Controle de acesso tradicional no UNIX (DAC - Discretionary Access Control)
    - Objetos (ex.: arquivos e processos) possuem dono
    - Você é dono de objetos criados por você
    - A conta especial “root” pode atuar como “dona” de qualquer objeto
    - Apenas root pode executar certas operações administrativas

# Introdução

- ...Isso nos leva ao **CONTROLE DE ACESSO**
- Controle de acesso moderno (DAC + MAC)
  - **DAC** - Discretionary Access Control
    - Role Based Access Control (RBAC)\*
    - **ACLs (Access Control Lists)**
  - **MAC** - Mandatory Access Control
    - LSM (Linux Security Module Framework). Exemplos:
      - SELinux: Security-Enhanced linux
      - AppArmor
    - POSIX capabilities\*
      - At linux: `/usr/include/linux/capability.h`
      - `man 7 capabilities`; `man setcap`; `man getcap`

# Introdução

- ...Isso nos leva ao **CONTROLE DE ACESSO**
  - O que é utilizado na **MAIORIA** dos sistemas? **DAC**
    - conta de root com uma senha **MUITO BEM GUARDADA**
    - políticas de troca de senha constante
    - senhas robustas
    - su, sudo (arquivo /etc/sudoers)
    - ACLs no sistema de arquivos
  - **O que deveria ser usado? DAC + MAC**
    - Observe sempre: conveniência X segurança

# Usuários locais

- Arquivos:
  - /etc/passwd - base de usuários
  - /etc/group - base de grupos
  - /etc/shadow - senhas + controles diversos de conta
- Arquivos de configuração
  - /etc/login.defs
  - /etc/default/useradd



# Usuários locais

- `/etc/passwd`
  - login name
  - optional encrypted password
  - numerical User ID (UID)
  - numerical Group ID (GID)
  - User Name or Comment field (GECOS)
  - user home directory
  - optional user command interpreter
- Exemplo de entrada
  - `root:x:0:0:root:/root:/bin/bash`

# Usuários locais

- `/etc/group`
  - group name
  - password
  - GID
  - User list
- Exemplo de entrada
  - `scanner:x:117:saned,rossano`

# Criação de contas

- Comandos

- useradd - não interativo
- adduser - interativo
- passwd
- usermod

- Exemplo

```
useradd -m -g users -G audio,video,scanner,storage \  
-s /bin/bash -c "usuario teste - tel 3333-4444" \  
teste
```

# Criação de contas

- Flags do useradd
  - m -> cria diretório home
  - g -> grupo primário
  - G -> grupos secundários
  - s -> shell
  - c -> GECOS
  - p -> senha criptografada
  - d -> diretório home
  - e -> expiração YYYY-MM-DD
  - k -> skeleton directory
  - r -> create system account
  - u -> User ID

# Criação de contas

- Flags do usermod (mesmas do useradd)
  - Use -a para append
  - Deixe de usar -a para reconstruir lista de grupos

# Criação de contas

- Outros comandos
  - groupmems - permite o usuário administrar seu próprio grupo primário (grupo c/ mesmo nome do login)
  - chsh - muda shell
  - chfn - muda Full Name (campo GECOS)
  - pwck - check integrity of password file
  - grpck - check integrity of group file
  - chage - change user account expiration data
  - id - displays user and group IDs

# Deleção de contas

- `userdel <username>`
- example:
  - `userdel teste`
  - `userdel -r teste`

# Senhas criptografadas

- `/etc/shadow`
  - loginname
  - senha criptografada
  - data da última troca de senha
  - Número mínimo de dias entre troca de senhas
  - Número máximo de dias entre troca de senhas
  - Número de dias antes que um usuário deve ser avisado sobre expiração da senha
  - Número de dias após a expiração de senha que a conta será desabilitada
  - Data da expiração da conta
  - Campo reservado



# Prática

- Adicionar usuário teste
  - `useradd -g users teste`
    - `cat /etc/passwd`
    - `cat /etc/group`
    - `cat /etc/shadow`
- Quais as características do usuário teste?
  - Leve em consideração: grupos, senha, diretório home, conta ativa/inativa

# Prática

- Atribuir senha ao usuário teste
  - `passwd teste`
    - Tente logar
- Desabilitar conta (lock)
  - `passwd -l teste`
- Habilitar conta (unlock)
  - `passwd -u teste`

# Prática

- Modificando grupos com `usermod`
  - `usermod -a -G video, audio, scanner teste`
    - a flag “-a” faz um append dos novos grupos
    - `cat /etc/group | grep teste`
    - `groups teste`
  - `usermod -G audio, video teste`
    - observe a omissão da flag “-a”
    - sem o “-a” o usu'ario teste permanecerá apenas nos grupos audio e video

# Prática

- **Modificando grupos** `gpasswd`
  - `gpasswd -a teste video`
  - `gpasswd -a teste audio`
  - `gpasswd -a teste scanner`
    - `cat /etc/group | grep teste`
    - `groups teste`
  - `gpasswd -d teste scanner`

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no `/etc/shadow`

```
teste$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksfgjjgflkdjgflkd
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksfgjjgflkdjgflkd
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: **\$1\$iuywherfeilksfgjjgflkdjgflkd**
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksfgjjgflkdjgflkd
- Última troca de senha: **15614**
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO



# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksgjjgflkdjgflkd
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksfgjjgflkdjgflkd
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksfgjjgflkdjgflkd
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: VAZIO
- Data de desabilitação de conta: VAZIO
- Campo reservado: VAZIO

# Prática: Modificar expiração de senha e conta

- Observe a linha para o usuário teste no /etc/shadow

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Username: teste
- senha: \$1\$iuywherfeilksfgjjgflkdjgflkd
- Última troca de senha: 15614
- Nro. mín. dias p/ troca de senhas: 0
- Nro. máx. dias p/ troca de senhas: 99999
- Aviso expiração de senha: 7
- Desabilitar conta XX dias após expiração de senha: **VAZIO**
- Data de desabilitação de conta: **VAZIO**
- Campo reservado: **VAZIO**

# Prática: Modificar expiração de senha e conta

- Obrigar o usuário a trocar de senha no primeiro/próximo login
  - Modificar arquivo `/etc/pam.d/other` (apenas para archlinux a partir de 2019):

– Alterar de

```
password    required    pam_deny.so
```

```
password    required    pam_warn.so
```

– Para

```
#password   required    pam_deny.so
```

```
#password   required    pam_warn.so
```

```
password    required    pam_unix.so
```

# Prática: Modificar expiração de senha e conta

- Obrigar o usuário a trocar de senha no primeiro/próximo login

- Trocar o 3o campo para 0 (zero). Era assim:

```
teste:$1$iuywherfeilksgfjjgflkdjgflkd:15614:0:99999:7:::
```

- Fica assim:

```
teste:$1$iuywherfeilksgfjjgflkdjgflkd:0:0:99999:7:::
```

- Tente logar como teste. Vai pedir para trocar a senha!
- Comando similar: `chage -d 0 teste`

# Prática: Modificar expiração de senha e conta

- Obrigar o usuário a trocar de senha em 1 dia
  - Trocar o 5o campo para 1. Era assim:

```
teste:$1$iuywherfeilksgfjjgflkdjgflkd:15614:0:99999:7:::
```

- Fica assim:

```
teste:$1$iuywherfeilksgfjjgflkdjgflkd:15614:0:1:7:::
```

- Verifique as informações de expiração: `chage -l teste`
  - Comando p/ atribuir valor ao 5o campo:

```
chage -M 1 teste
```

# Prática: Modificar expiração de senha e conta

- Expirar a conta do usuário teste amanhã

- Trocar o 8o campo para 15615. Era assim (VAZIO):

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::
```

- Fica assim:

```
teste:$1$iuywherfeilksfgjjgflkdjgflkd:15614:0:99999:7:::15615:
```

- Verifique as informações de expiração: `chage -l teste`

- A alteração poderia ser feita assim:

- `usermod -e 2012-10-02 teste`



# Prática

- Verificar datas de último login e falhas de login
  - `lastlog`
  - `lastlog -b 20`
  - Archlinux pré 2019: `faillog`
  - Archlinux 2019 em diante: `pam_tally2 -u USER`

## Exemplo:

```
for USER in $(cut -d: -f1 /etc/passwd); do
    pam_tally2 -u ${USER};
done
```

# Prática

- Desabilitar TODOS os logins (menos o de root)
  - Criar arquivo `/etc/nologin` com alguma mensagem
  - `echo 'Maquina em manutencao - logins desabilitados. Volte em 30 minutos.'`  
`> /etc/nologin`
  - Tente logar como teste
- Remova o arquivo `/etc/nologin` para reabilitar os logins

# Prática

- Site:

`rossano.pro.br/fatec/cursos/  
admsorede/exercicios-contas-usuario-  
archlinux.txt`

# Prática - Restrição de login com base em horário (PAM)

- Verificar se a linha a seguir existe no arquivo `/etc/pam.d/system-auth`

.....

```
account required pam_time.so
```

....

- Editar arquivo `/etc/security/time.conf` com a sintaxe:

```
services; ttys; users; times
```

# Prática - Restrição de login com base em horário (PAM)

- Exemplo:

```
login ; * ; teste ; Wk0800-1730
```

```
login ; * ; games ; Wk1700-0900 | SaSu0000-2400
```

- Sintaxe:

- 1o campo indica o **serviço**:
- 2o campo indica **lista de terminais**:
- 3o campo indica **lista de usuários**:
- 4o campo indica **horários permitidos**:
  - **Wk** - segunda à sexta; **Su, Mo, Tu, We, Th, Fr, Sa** (Dom, Seg, Ter, Qua, Qui, Sex, Sab); **Al** - todo dia

# Prática - Impondo limites (PAM)

- Verificar se a linha a seguir existe no arquivo `/etc/pam.d/system-auth`

```
... .  
session required pam_limits.so
```

```
... .
```

- Editar arquivo `/etc/security/limits.conf` com a sintaxe:

```
<domain> <type> <item> <value>
```

# Prática - Impondo limites (PAM)

- Exemplo:

```
teste hard maxlogins 2
```

```
teste hard nproc 10
```

- Outros domínios - próximo slide

# Prática - Impondo limites (PAM)

- Outros domínios:
  - core
  - fsize
  - data
  - nofile
  - cpu
  - stack
  - nproc
  - as
  - maxlogins
  - rss