Análise prática de segurança

Autor: Alexandre Aparecido Scrocaro Junior
email: alescrocaro@gmail.com

Professor: Luiz Arthur Feitosa dos Santos
Universidade Tecnológica Federal do Paraná (UTFPR)

Especificação do trabalho

Introdução a respeito dos procedimentos realizados

Os procedimentos realizados nesta atividade foram baseados em conhecimentos adquiridos durante as aulas sobre práticas de segurança. Tais aulas mostraram passos para realizar uma análise do sistema em busca de evidências de que ele foi comprometido quanto à sua segurança. Os passos realizados foram: verificação de usuários não autorizados ou suspeitos, verificação de processos suspeitos e/ou maliciosos, verificação de alterações ou possíveis alterações no sistema de arquivos e, por fim, análise nos arquivos de log do sistema que podem apontar atividades maliciosas ou suspeitas. Todos os comando apresentados foram utilizados durante as aulas.

Descrição dos passos realizados Tal descrição deve apresentar comandos utilizados, resultados obtidos e

conclusão parcial de cada resultado

Usuários não autorizados ou suspeitos

Primeiramente, fiz a conexão com a máquina via ssh, e então utilizei o comando w para verificar se havia mais algum usuário conectado a máquina. Como pode ser visto abaixo, apenas a minha instância estava sendo processada.

```
aluno@seg2022:~$ w
 14:05:07 up  1:04,  1 user,  load average: 0.00, 0.01, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
aluno    pts/0    192.168.56.1     14:04    0.00s  0.03s  0.00s w
```

Então utilizei o comando last para visualizar as últimas ações de logon, tentando visualizar usuários não autorizados. Como visto abaixo, há um usuário proxy e outro usuário reboot que são suspeitos.

```
aluno@seg2022:/var/log/apache2$ last
aluno    pts/0        192.168.56.1     Sun Oct 30 14:04   still logged in
aluno    tty1                          Sun Oct 30 13:48 - 14:05  (00:16)
reboot   system boot  5.4.0-66-generic Sun Oct 30 13:00   still running
reboot   system boot  5.4.0-66-generic Sat Sep 24 03:17   still running
aluno    pts/0        192.168.56.1     Thu Sep 15 17:50 - 17:50  (00:00)
reboot   system boot  5.4.0-66-generic Thu Sep 15 17:49 - 17:50  (00:00)
aluno    pts/0        192.168.56.1     Thu Sep 15 17:49 - 17:49  (00:00)
reboot   system boot  5.4.0-66-generic Thu Sep 15 17:47 - 17:49  (00:02)
aluno    pts/0        192.168.56.1     Thu Sep 15 17:45 - 17:47  (00:01)
reboot   system boot  5.4.0-66-generic Thu Sep 15 17:45 - 17:47  (00:02)
aluno    pts/0        192.168.56.1     Thu Sep 15 17:44 - 17:45  (00:00)
aluno    pts/0        192.168.56.1     Thu Sep 15 17:39 - 17:44  (00:04)
aluno    tty1                          Thu Sep 15 17:36 - down   (00:08)
reboot   system boot  5.4.0-66-generic Thu Sep 15 17:36 - 17:45  (00:08)
aluno    pts/1        192.168.56.1     Wed Mar  3 23:38 - 00:17  (00:38)
```

Ao utilizar o comando "cat ~/etc/passwd" consigo visualizar todos os usuários do sistema. Assim é possível visualizar que além do usuário root, o usuário uucp possui o UID = 0, sendo uma duplicata do root, isso é uma possível ameaça que deve ser verificada.

```
root@seg2022:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:0:0:uucp:/var/spool/uucp:/bin/bash
proxy:x:13:13:proxy:/bin:/bin/bash
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
dacom:x:1000:1000:aluno:/home/dacom:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
aluno:x:1001:1001:,,,:/home/aluno:/bin/bash
professor:x:1002:1002:,,,:/home/professor:/bin/bash
telnetd:x:112:118::/nonexistent:/usr/sbin/nologin
ftp:x:113:119:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
_rpc:x:114:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin
estagiario:x:1003:1003:,,,:/home/estagiario:/bin/bash
vendas:x:1004:1004:,,,:/home/vendas:/bin/bash
oficina:x:1005:1005:,,,:/home/oficina:/bin/bash
mysql:x:116:120:MySQL Server,,,:/nonexistent:/bin/false
```

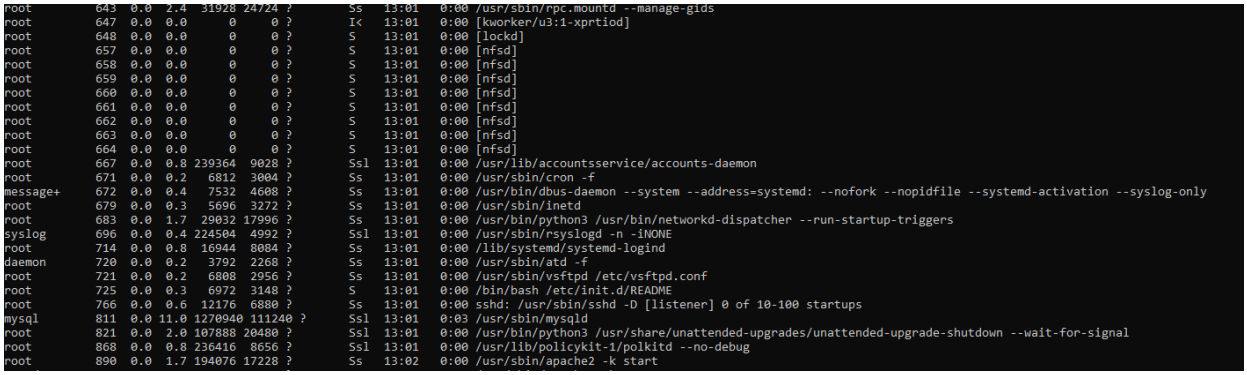
Agora, utilizei o comando "cat ~/etc/shadow", para visualizar o arquivo de senhas. Como pode ser visto abaixo, há usuários estranhos, como o "nobody" e "proxy" que devem ser verificados.

```
root@seg2022:/etc# cat shadow
root:*:18659:0:99999:7:::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:$6$CaadO9BzrYGRC/Q1$r.IzadVEC9UFxNL64sPZ3w5j6mDOKhbWw7D2WvvugXhMQ7cq3MH1HQdO8FD6tey2SsT9xpIuQuV8L8ZFSP4jF0:18689:0:99999:7:::
proxy:$6$zy/nWn33FMvccb/Q$3HAuu97dwBDpw7gF9FSaXOwPwgvX.GQ2hhgwfp7WPJ0HAfnwSJVTVPtFzWOolb2bD3GHQYe5H56N4XzMkia/U0:18689:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
sshd:*:18678:0:99999:7:::
systemd-coredump:!!:18678::::::
dacom:$6$4bl9h7JkM1pXnx0z$JTT/NHUwvM2Ee9oBYy1b3ubzUCV2K3J3H1L.4vGkiJl93eZo/vo6s9pvsg05PwHqeIWbkGeUw6h/dAiz2I7xX0:18678:0:99999:7:::
lxd:!:18678::::::
aluno:$6$15J6puqsdyztnX53$Q9YABVlJRKpq.TudQZAoLJZNmlbiNkVus115DvJsfxLWjf.jJ0RI5dVFuAJeBnxcDuWlir6ooNa9qL7G2KQwe/:19250:0:99999:7:::
professor:$6$564HLQ.uP0TpcQkr$VSVCCb9KuLJc5SLKwCCzG86HUO8KF9FTDbHzRhO/Xj5VcokPa3qEbOBvgSwJ/tsZZHqi7Gat4pQ06TGGPbhUr.:18678:0:99999:7:::
telnetd:*:18678:0:99999:7:::
ftp:*:18678:0:99999:7:::
_rpc:*:18678:0:99999:7:::
statd:*:18678:0:99999:7:::
estagiario:$6$uW4y2M2KWnvgUbkU$vn0Utu6lgUHes7Qeh5wGsHwC8/fnvv5NERTT0bn2tjnxlhyUFKYTBTi9a32qRgRZbLLRapOsksEYPc8z6YYnb0:18678:0:99999:7:::
vendas:$6$w5lESfpztymTUoOA$s8aIVVNLdh/qanBwPpx8UYytNsTOSOKiU33jdgK1AYn2RsoeOmCr/0S37oirvU8TLrCeYM.9g/fjmepmIK6lN.:18678:0:99999:7:::
oficina:$6$EY8OLmHGPsceVDHV$uT21dU20P5tsK4mqVho1x/VdsHP3ElSTEj2ulPEN81siiuWTBbsa2Ln2enVOA0w3RUv9KGL0wxWssKsxjECLI1:18678:0:99999:7:::
mysql:!:18678:0:99999:7:::
```

Processos suspeitos e/ou maliciosos

Tais processos podem servir para o atacante explorar uma falha na máquina e devem ser fechados, outra forma de recuperar o sistema contra tais processos é reinstalar uma versão mais atualizada do mesmo.\

Para visualizar todos processos em execução na máquina (de todos usuários, devido a opção 'a') utilizei o comando "ps aux", além do "pstree" para relacionar os processos. Como pode ser observado abaixo, há processos que provavelmente não deveriam estar em execução, como o caso do mysql e do nfs, é necessário, no mínimo, matar esses processos.



```
root         643  0.0  2.4  31928 24724 ?        Ss   13:01   0:00 /usr/sbin/rpc.mountd --manage-gids
root         647  0.0  0.0      0     0 ?        I<   13:01   0:00 [kworker/u3:1-xprtiod]
root         648  0.0  0.0      0     0 ?        S    13:01   0:00 [lockd]
root         657  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         658  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         659  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         660  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         661  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         662  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         663  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         664  0.0  0.0      0     0 ?        S    13:01   0:00 [nfsd]
root         667  0.0  0.8 239364  9028 ?        Ssl  13:01   0:00 /usr/lib/accountsservice/accounts-daemon
root         671  0.0  0.2   6812  3004 ?        Ss   13:01   0:00 /usr/sbin/cron -f
message+     672  0.0  0.4   7532  4608 ?        Ss   13:01   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root         679  0.0  0.3   5696  3272 ?        Ss   13:01   0:00 /usr/sbin/inetd
root         683  0.0  1.7  29032 17996 ?        Ss   13:01   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
syslog       696  0.0  0.4 224504  4992 ?        Ssl  13:01   0:00 /usr/sbin/rsyslogd -n -iNONE
root         714  0.0  0.8  16944  8084 ?        Ss   13:01   0:00 /lib/systemd/systemd-logind
daemon       720  0.0  0.2   3792  2268 ?        Ss   13:01   0:00 /usr/sbin/atd -f
root         721  0.0  0.2   6808  2956 ?        Ss   13:01   0:00 /usr/sbin/vsftpd /etc/vsftpd.conf
root         725  0.0  0.3   6972  3148 ?        S    13:01   0:00 /bin/bash /etc/init.d/README
root         766  0.0  0.6  12176  6880 ?        Ss   13:01   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
mysql        811  0.0 11.0 1270940 111240 ?      Ssl  13:01   0:03 /usr/sbin/mysqld
root         821  0.0  2.0 107888 20480 ?        Ssl  13:01   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
root         868  0.0  0.8 236416  8656 ?        Ssl  13:01   0:00 /usr/lib/policykit-1/polkitd --no-debug
root         890  0.0  1.7 194076 17228 ?        Ss   13:02   0:00 /usr/sbin/apache2 -k start
```

```
root@seg2022:/# pstree
systemd─┬─README───sleep
        ├─accounts-daemon───2*[{accounts-daemon}]
        ├─2*[agetty]
        ├─apache2───5*[apache2]
        ├─atd
        ├─blkmapd
        ├─cron
        ├─dbus-daemon
        ├─fwupd───4*[{fwupd}]
        ├─inetd
        ├─multipathd───6*[{multipathd}]
        ├─mysqld───29*[{mysqld}]
        ├─networkd-dispat
        ├─polkitd───2*[{polkitd}]
        ├─rpc.idmapd
        ├─rpc.mountd
        ├─rpcbind
        ├─rsyslogd───3*[{rsyslogd}]
        ├─snapd───8*[{snapd}]
        ├─sshd───sshd───sshd───bash───sudo───su───bash───pstree
        ├─systemd───(sd-pam)
        ├─systemd-journal
        ├─systemd-logind
        ├─systemd-network
        ├─systemd-resolve
        ├─systemd-timesyn───{systemd-timesyn}
        ├─systemd-udevd
        ├─unattended-upgr───{unattended-upgr}
        └─vsftpd
```

Além disso, é possível observar os processos visualizando kernel diretamente com o comando "cat /proc/*/stat | awk '{print $1, $2}'". Dessa forma podemos visualizar processos que possivelmente foram escondidos por um invasor. Com isso descobri o processo rpc.mountd, que é um risco à segurança e pode ser usado (ou ter sido usado) por um invasor.

```
540 (multipathd)
550 (loop0)
551 (loop1)
553 (loop2)
555 (loop3)
558 (loop4)
559 (loop5)
560 (jbd2/sda2-8)
561 (ext4-rsv-conver)
574 (rpcbind)
575 (systemd-timesyn)
586 (rpc.idmapd)
630 (systemd-network)
638 (systemd-resolve)
643 (rpc.mountd)
647 (kworker/u3:1-xprtiod)
648 (lockd)
```

Para matar um processo (utilizarei o mysql como exemplo), utilizei o comando "kill -811 pid". Ao utilizar o comando "ps aux" novamente pode ser observado que tal comando sumiu.

Alterações ou possíveis alterações no sistema de arquivos

Para buscar por alterações, fiz a instalação do rpm, que fará tal verificação. Para tanto, utilizei o comando "rpm -Va > /tmp/rpmVA.log"; entretanto nenhuma saída foi gerada, então imagino que esteja tudo correto.

Análise nos arquivos de log do sistema que podem apontar atividades maliciosas ou suspeitas

Os arquivos de log são locais onde se pode obter informações preciosas à respeito da segurança da máquina, então deve-se realizar consultas neles periodicamente.

Utilizei o comando "grep fail auth.log" e "grep repeat auth.log"; o segundo não retornou nada, já o primeiro retorno as duas mensagens vistas abaixo que não aparentam representar perigos à segurança.

```
root@seg2022:/var/log# grep fail auth.log
Oct 30 14:00:21 seg2022 sudo: pam_unix(sudo:auth): authentication failure; logname=aluno uid=1001 euid=0 tty=/dev/tty1 ruser=aluno rhost=  user=aluno
Oct 30 14:04:15 seg2022 sshd[2046]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
```

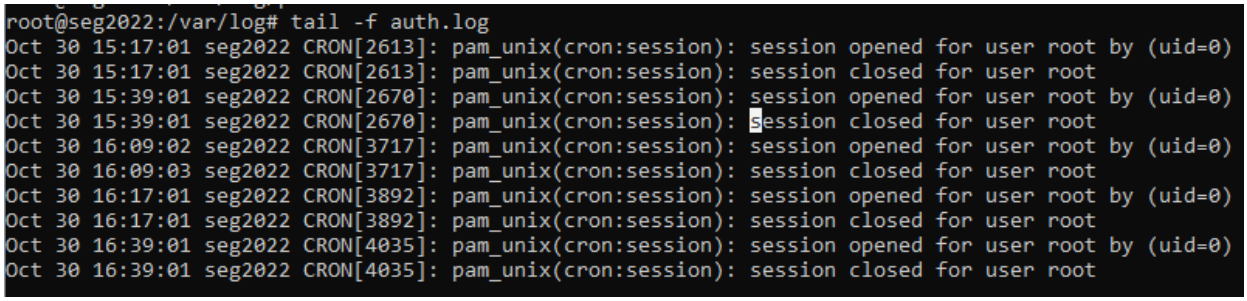
Além disso, utilizei os comandos "zgrep fail auth.log*" e "zgrep repeat auth.log*". Como mostrado nas capturas abaixo.

```
root@seg2022:/var/log# grep fail auth.log
Oct 30 14:00:21 seg2022 sudo: pam_unix(sudo:auth): authentication failure; logname=aluno uid=1001 euid=0 tty=/dev/tty1 ruser=aluno rhost=  user=aluno
Oct 30 14:04:15 seg2022 sshd[2046]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
root@seg2022:/var/log# grep repeat auth.log
root@seg2022:/var/log# zgrep auth.log*
root@seg2022:/var/log# zgrep fail auth.log*
auth.log:Oct 30 14:00:21 seg2022 sudo: pam_unix(sudo:auth): authentication failure; logname=aluno uid=1001 euid=0 tty=/dev/tty1 ruser=aluno rhost=  user=aluno
auth.log:Oct 30 14:04:15 seg2022 sshd[2046]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
auth.log.2.gz:Sep 15 17:39:22 redes2 sshd[2616]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
auth.log.2.gz:Sep 15 17:50:10 seg2022 login[706]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=aluno
auth.log.2.gz:Sep 15 17:50:12 seg2022 login[706]: FAILED LOGIN (1) on '/dev/tty1' FOR 'aluno', Authentication failure
auth.log.3.gz:Mar  3 21:30:00 redes2 sshd[2301]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
auth.log.3.gz:Mar  3 21:30:20 redes2 sshd[2301]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
auth.log.3.gz:Mar  3 21:30:32 redes2 sshd[2304]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=oficina
auth.log.3.gz:Mar  3 21:30:46 redes2 sshd[2304]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=oficina
auth.log.3.gz:Mar  3 21:30:57 redes2 sshd[2315]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=mysql
auth.log.3.gz:Mar  3 21:31:07 redes2 sshd[2315]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=mysql
auth.log.3.gz:Mar  3 21:43:40 redes2 sshd[1115]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=estagiario
auth.log.3.gz:Mar  3 22:00:42 redes2 sshd[1747]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=uucp
auth.log.3.gz:Mar  3 22:00:58 redes2 sshd[1747]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=uucp
auth.log.3.gz:Mar  3 22:02:03 redes2 sudo: pam_unix(sudo:auth): authentication failure; logname=estagiario uid=1003 euid=0 tty=/dev/pts/0 ruser=estagiario rhost=  user=estagiario
auth.log.3.gz:Mar  3 22:02:35 redes2 sshd[1905]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=proxy
auth.log.3.gz:Mar  3 22:02:48 redes2 sshd[1905]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=proxy
auth.log.3.gz:Mar  3 22:03:16 redes2 sshd[1919]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=proxy
auth.log.3.gz:Mar  3 22:03:31 redes2 sshd[1919]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=proxy
auth.log.3.gz:Mar  3 23:38:22 redes2 sshd[3097]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
auth.log.4.gz:Feb 20 18:43:27 redes2 login[1465]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
auth.log.4.gz:Feb 20 18:43:30 redes2 login[1465]: FAILED LOGIN (1) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure
auth.log.4.gz:Feb 20 18:43:38 redes2 login[1465]: FAILED LOGIN (2) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure
auth.log.4.gz:Feb 20 18:43:47 redes2 login[1465]: FAILED LOGIN (3) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure
auth.log.4.gz:Feb 20 18:50:15 redes2 sudo: pam_unix(sudo:auth): authentication failure; logname=dacom uid=1001 euid=0 tty=/dev/tty1 ruser=aluno rhost=  user=aluno
auth.log.4.gz:Feb 20 18:50:44 redes2 su: pam_unix(su-l:auth): authentication failure; logname=dacom uid=1000 euid=0 tty=tty1 ruser=dacom rhost=  user=root
auth.log.4.gz:Feb 20 18:53:20 redes2 login[684]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost=  user=aluno
auth.log.4.gz:Feb 20 18:53:23 redes2 login[684]: FAILED LOGIN (1) on '/dev/tty1' FOR 'aluno', Authentication failure
auth.log.4.gz:Feb 20 18:54:04 redes2 sudo: pam_unix(sudo:auth): authentication failure; logname=aluno uid=1001 euid=0 tty=/dev/tty1 ruser=aluno rhost=  user=aluno
auth.log.4.gz:Feb 20 18:56:31 redes2 sudo: pam_unix(sudo:auth): authentication failure; logname=aluno uid=1001 euid=0 tty=/dev/pts/0 ruser=aluno rhost=  user=aluno
auth.log.4.gz:Feb 20 19:02:01 redes2 sshd[1683]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
auth.log.4.gz:Feb 23 09:00:23 redes2 sshd[11462]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
auth.log.4.gz:Feb 23 09:12:32 redes2 login[795]: Authentication failure
auth.log.4.gz:Feb 23 09:12:32 redes2 login[955]: Authentication failure
auth.log.4.gz:Feb 23 09:12:32 redes2 login[963]: Authentication failure
auth.log.4.gz:Feb 23 09:12:32 redes2 login[966]: Authentication failure
auth.log.4.gz:Feb 23 09:12:32 redes2 login[967]: Authentication failure
auth.log.4.gz:Feb 23 09:13:01 redes2 sshd[970]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
auth.log.4.gz:Feb 23 09:17:37 redes2 login[1193]: Authentication failure
auth.log.4.gz:Feb 23 09:17:37 redes2 login[1202]: Authentication failure
auth.log.4.gz:Feb 23 09:17:37 redes2 login[1204]: Authentication failure
auth.log.4.gz:Feb 23 09:17:37 redes2 login[1205]: Authentication failure
auth.log.4.gz:Feb 23 09:17:37 redes2 login[1206]: Authentication failure
auth.log.4.gz:Feb 23 18:39:31 redes2 sudo: pam_unix(sudo:auth): authentication failure; logname=aluno uid=1001 euid=0 tty=/dev/tty1 ruser=aluno rhost=  user=aluno
auth.log.4.gz:Feb 23 18:45:11 redes2 sshd[1285]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1  user=aluno
```

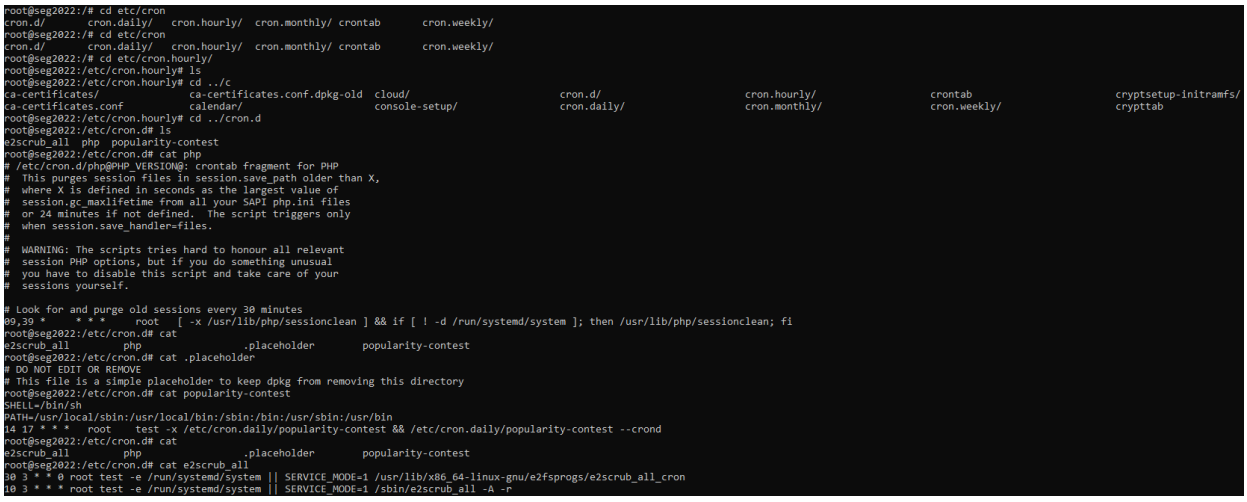
```
root@seg2022:/var/log# zgrep repeat auth.log*
auth.log.3.gz:Mar  3 21:30:45 redes2 sshd[2304]: message repeated 2 times: [ Failed password for oficina from 192.168.56.1 port 38720 ssh2]
auth.log.3.gz:Mar  3 21:31:06 redes2 sshd[2315]: message repeated 2 times: [ Failed password for mysql from 192.168.56.1 port 38730 ssh2]
auth.log.3.gz:Mar  3 22:00:57 redes2 sshd[1747]: message repeated 2 times: [ Failed password for invalid user uucp from 192.168.56.1 port 41822 ssh2]
auth.log.3.gz:Mar  3 22:02:12 redes2 sudo: message repeated 2 times: [ pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory]
auth.log.3.gz:Mar  3 22:02:48 redes2 sshd[1905]: message repeated 2 times: [ Failed password for invalid user proxy from 192.168.56.1 port 41842 ssh2]
auth.log.4.gz:Feb 20 18:50:25 redes2 sudo: message repeated 3 times: [ pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory]
```

Analizando as capturas acima, percebe-se que há algo estranho no arquivo 'auth.log.4.gz', com várias falhas de autenticação seguidas, isso pode ser um problema, então iremos utilizar o comando "zcat auth.log.4.gz" para analisar.
A saída desse comando não gerou nenhuma ameaça aparente acerca do que eu estava procurando, porém encontrei outra ameaça (que pode ser vista no printscreen abaixo). Essa adição do usuário 'dacom' aos grupos é suspeita e deve ser analisada, principalmente por ele ter sido adicionado ao grupo 'adm'.

Para verificar últimas tentativas de logon, utilizei o comando "tail -f auth.log" (no diretorio /var/log), e analisando a saída, vista abaixo, há indícios de que está sendo executado um script (devido à várias e repetidas sessões criadas e fechadas).



Fiz uma breve análise e pesquisas do que isso poderia ser, mas não encontrei muitos resultados.



Análise/resumo geral a respeito do resultado obtido na análise realizada, tentando correlacionar os dados obtidos em cada um dos passos da prática de segurança. Se foram encontrados problemas, aponte esses problemas, comente como esses podem afetar

ou já afetaram a segurança do sistema e se você conseguir apresente possíveis soluções

Como pôde ser visto, foram encontrados usuários, processos e informações em log suspeitas. Esses três itens são extremamente interligados, pois quando um cracker vai realizar um ataque, ele geralmente vai tentar explorar processos em execução na máquina, ao conseguir realizar essa exploração, provavelmente vai querer manter seu acesso ao sistema, e então vai manipular ou criar um usuário e tentar mudar sua permissão para de administrador; e, se ele não excluir ou modificar arquivos de log, toda sua ação ficará registrada neles. Ao acontecer esse ataque, tal como há indícios de que houve na máquina estudada, pode ser que ele seja devastador, ou seja, o cracker tem completo acesso ao sistema, podendo vigiar ou roubar dados tranquilamente.
Para resolver o problema de usuários suspeitos, se utilizaria o comando "passwd -l user", dessa forma é possível bloquear o acesso de um usuário. Acerca do problema dos processos, já foi exemplificado acima como seria feito com o comando "kill".

Conclusão a respeito dos passos realizados e de possíveis facilidades/dificuldades encontradas durante a realização desses passos

Como pôde ser observado, os passos para realização da análise são bem sistemáticos, claros e efetivos. Há passos que necessitam de menos esforço, como o primeiro, e outros mais difíceis como a verificação do sistema de arquivos, que necessitaria de uma configuração de um programa como o AIDE para ser mais efetivo e evitar esforços desnecessários (verificação manual de todo o sistema).

Comparar PenTeste com as Práticas de segurança, principalmente em relação aos resultados obtidos

Ambos estão diretamente interligados, a verificação de usuários poderia encontrar um usuário criado na fase 'mantendo acesso', já a verificação de processos poderia encontrar rastros criados na fase 'escaneamento' ou 'ganhando acesso', e as fases de verificação de sistema de arquivos e verificação dos logs podem encontrar pistas de tudo que um possível invasor observou, alterou ou excluiu no sistema.