

Relatório de ASIST

Sprint 1

Turma 3DG – Grupo 038

1190718 – João Beires

1190782 – José Soares

1190811 – Lourenço Melo

1191419 – José Maia

Data: 03/11/2022

User Story 1:

A: Login via consola

Para realizarmos esta parte da “User Story”, fizemos uma breve pesquisa pelo manual do comando “getty”. Verificamos que antes do login é apresentado o conteúdo do ficheiro “/etc/issue”.

Assim, procedemos a alterar o conteúdo do mesmo para o que tinha sido pedido, que neste caso era a data e o número de “active users”.

Resultado:

```
Debian GNU/Linux 11 uvm038 tty1
Date: 01/11/2022
Active Users: 0
uvm038 login: _
```

B: Login via SSH

Antes de começarmos a resolução da User Storie 1 a mensagem do ssh ao user asist na máquina uvm038 mostra esta mensagem:

```
kali)-[~]
$ ssh asist@10.9.10.38
asist@10.9.10.38's password:
Linux uvm038 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 31 17:19:25 2022 from 10.8.32.59
asist@uvm038:~$ logout
Connection to 10.9.10.38 closed.
```

É possível verificar que não existe qualquer mensagem previa à autentificação. Como a imagem acima pode demonstrar.

Para conseguirmos completar esta US pensamos em criar um ficheiro de texto chamado “banner.txt” capaz de satisfazer as necessidades pedidas. Estas sendo, mostrar a data e a quantidade de “active users”, ou seja, os “users” que estão “logged in”.

Banner.txt

```
root@uvm038:/etc/ssh# cat banner.txt
=====
DATE:
01/11/2022
ACTIVE USERS:
1
=====
```

Este ficheiro deve estar no diretório:/etc/ssh

Para este ficheiro poder ser visualizado antes de autenticação do SSH é necessário definir a banner no ficheiro “sshd_config” como definido na imagem seguinte.

```
# no default banner path
Banner /etc/ssh/banner.txt

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server
```

Para atualizar esta informação ao SSH é preciso correr este comando: `systemctl restart sshd`

Para testar esta US é necessário tentar um login via SSH.

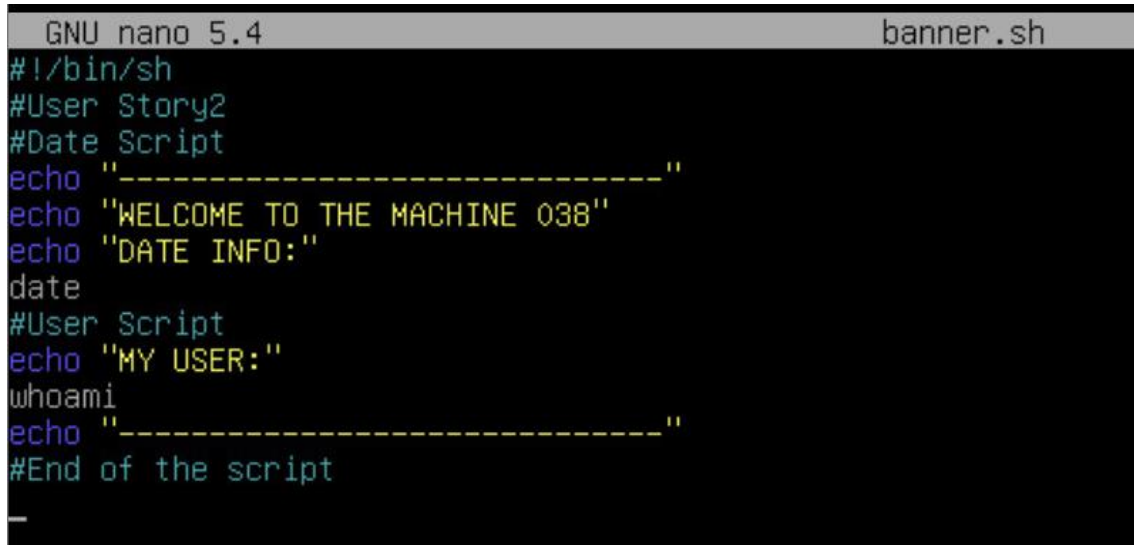
```
kali)-[~]
$ ssh asist@10.9.10.38
=====
DATE:
01/11/2022
ACTIVE USERS:
1
=====
asist@10.9.10.38's password: █
```

USER STORY 2:

Para conseguir resolver esta “User Story”, utilizamos o diretório “/etc/profile.d”. Este “folder” executa todos os comandos presentes nos ficheiros existentes ao “users” que tenha acesso à “shell”, após a sua autenticação.

Sabendo isso criamos um script capaz de satisfazer as particularidades pedidas.

Script:



```
GNU nano 5.4 banner.sh
#!/bin/sh
#User Story2
#Date Script
echo "-----"
echo "WELCOME TO THE MACHINE 038"
echo "DATE INFO:"
date
#User Script
echo "MY USER:"
whoami
echo "-----"
#End of the script
```

Mostramos que o utilizador conseguiu se autenticar com sucesso na máquina “038”. Em seguida mostramos a data atual em que foi efetuado o login, com o comando “date” que disponibiliza a data e a hora. De seguida, usamos o comando “whoami” que retorna o utilizador que está a ser usado de momento.

Para poder verificar o sucesso a mensagem deste script, na situação pedida, recorreremos ao comando “systemctl restart ssh”. De seguida, experimentamos ligar por SSH à máquina com o utilizador “asist”.

Resultado:

```
(kali)~[~]
$ ssh asist@10.9.10.38
asist@10.9.10.38's password:
Linux uvm038 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 31 18:15:57 2022 from 10.8.32.59

WELCOME TO THE MACHINE 038
DATE INFO:
seg 31 out 2022 18:16:44 WET
MY USER:
asist
```

User Story 3

Para resolver esta “UserStory”, é necessário alterar o ficheiro “/etc/pam.d/sshd”. Neste ficheiro vamos introduzir um comando para apenas permitir o acesso à máquina Linux aos utilizadores com um “user ID” inferior a 7000 e que pertençam ao grupo “lasistgrupo”.

Primeiramente vamos visualizar no ficheiro “/etc/passwd” para ver os utilizadores com os seus respectivos “users ID’s” e os seus respectivos “group ID’s”.

```

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:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
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:/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
Lapt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
asist:x:1000:6005:asist,,:/home/asist:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
luser1:x:6000:6005:/home/luser1:/bin/sh
luser2:x:6001:6005:/home/luser2:/bin/sh
luser3:x:6002:6005:/home/luser3:/bin/sh
luser4:x:7000:6005:/home/luser4:/bin/sh
luser5:x:7001:6005:/home/luser5:/bin/sh
luser6:x:7002:6005:/home/luser6:/bin/sh
nslcd:x:106:112:nslcd name service LDAP connection daemon,,:/var/run/nslcd:/usr/sbin/nologin
luser7:x:6003:6006:/home/luser7:/bin/sh

```

Assim sabemos que os utilizadores que vão ser bloqueados ao acesso por “SSH” à máquina, devido ao seu “User ID” que neste caso serão: luser4, luser5 e luser6.

Vamos agora ver que utilizadores fazem parte do grupo “lasistgrupo”.

```
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:asist
sasl:x:45:
plugdev:x:46:asist
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-timesync:x:101:
systemd-journal:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
input:x:105:
kvm:x:106:
render:x:107:
crontab:x:108:
netdev:x:109:asist
messagebus:x:110:
ssh:x:111:
asist:x:1000:
systemd-coredump:x:999:
luser1:x:6000:
luser2:x:6001:
luser3:x:6002:
lgrupo1:x:6003:
lgrupo2:x:6004:luser1,luser2,luser3,luser4,luser5,luser6
lasistgrupo:x:6005:root,luser1
root:x:998:
nslcd:x:112:
luser7:x:6006:
```

Ao comparar as duas imagens conseguimos perceber que os únicos utilizadores que vão ser capazes de se conectar por ssh serão o “root” e o “luser1” e “asist”. Pois são os únicos que são validados nas regras pedidas.

Adicionamos ao ficheiro “/etc/pam.d/sshd” estes dois comandos.

```
#US3 restrict uid<7000 and only of lasistgrupo
auth    required      pam_succeed_if.so quiet uid < 7000
auth    required      pam_succeed_if.so quiet gid eq 6005
```

O “auth” demonstra que é referente ao modulo de autenticação e “required” pois o modulo apenas pode ser bem-sucedido se a “flag” for bem-sucedida. O “quiet” para não mostrar a falha.

Em seguida, estão apresentadas as condições pedidas nesta user story. O “eq” referece em ingles “equals”. O “ui” e o “gid” respectivamente reference-se a “User ID” e “Group ID”.

Após a esta alteração corremos o comando para dar restart ao protocolo sshd: “systemctl restart sshd”.

Por exemplo, tentamos nos conectar com o user “asist” que está dentro destes parâmetros tanto de “User ID” e “Group ID” e o resultado foi bem-sucedido.

```
kali)-[~]
$ ssh asist@10.9.10.38
=====
DATE:
01/11/2022
ACTIVE USERS:
1
=====
asist@10.9.10.38's password:
Linux uvm038 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov  3 14:41:22 2022 from 10.8.36.199
=====
WELCOME TO THE MACHINE 038
DATE INFO:
qui 03 nov 2022 15:03:37 WET
MY USER:
asist
```

Se tentarmos conectarmos por “SSH” com o user “luser5” não nos é permitido.

```
kali)-[~]
$ ssh luser5@10.9.10.38
=====
DATE:
01/11/2022
ACTIVE USERS:
1
=====
luser5@10.9.10.38's password:
Permission denied, please try again.
```


User Story 5

Para realizar esta “User Story” é necessário criar um ficheiro “/etc/bad-guys”. Neste ficheiro devemos introduzir os “users” que queremos que não tenham a capacidade de se conectar por “SSH”.

Assim neste ficheiro introduzimos o “user” “asist”.

```
root@uvm038:~# cat /etc/bad-guys
asist
```

De seguida fomos ao ficheiro “/etc/pam.d/sshd” e introduzimos este comando, tal como, referido no manual do “pam_listfile”.

```
#US5 restrict users on file
auth    required      pam_listfile.so \
        onerr==succeed item=user sense=deny file=/etc/bad-guys

root@uvm038:~# systemctl restart sshd
```

De seguida demos “restart” ao “sshd” com o comando: “systemctl restart sshd”.

```
(kali)-[~]
$ ssh asist@10.9.10.38
=====
DATE:
01/11/2022
ACTIVE USERS:
1
=====
asist@10.9.10.38's password:
Permission denied, please try again.
asist@10.9.10.38's password:
```

Tentamo-nos conectar por “SSH” com o “user” “asist” e mesmo introduzindo os parâmetros corretos foi nos negada o acesso à máquina.