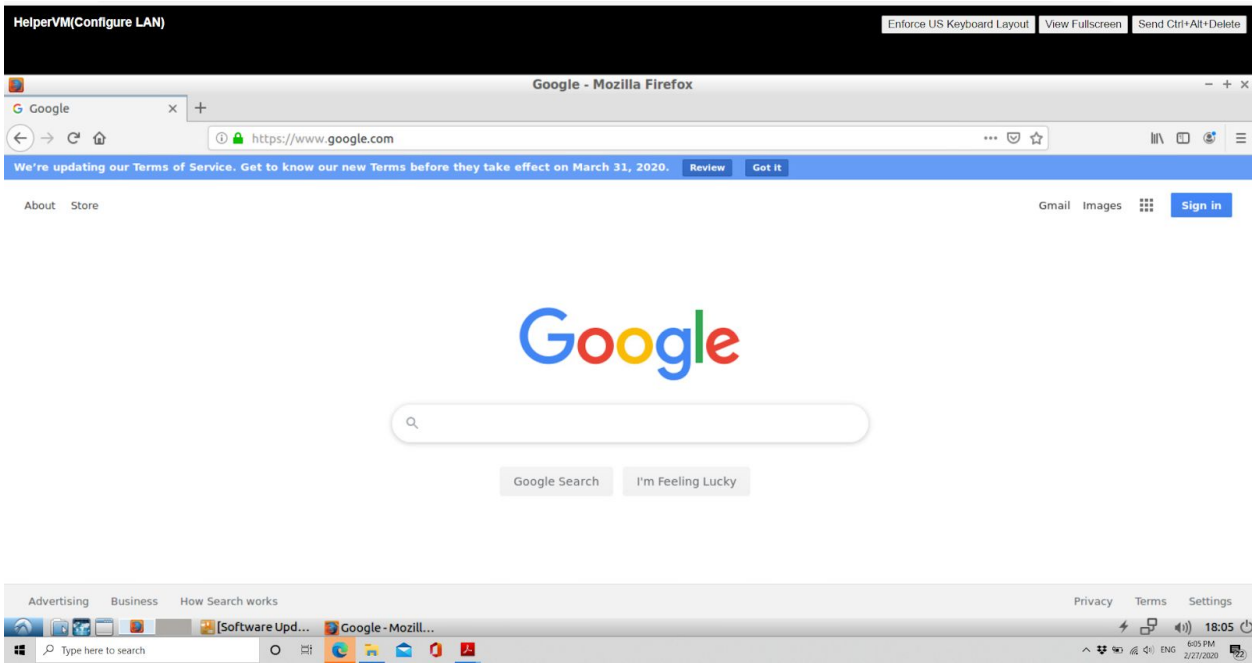
Linux Homework

Contents

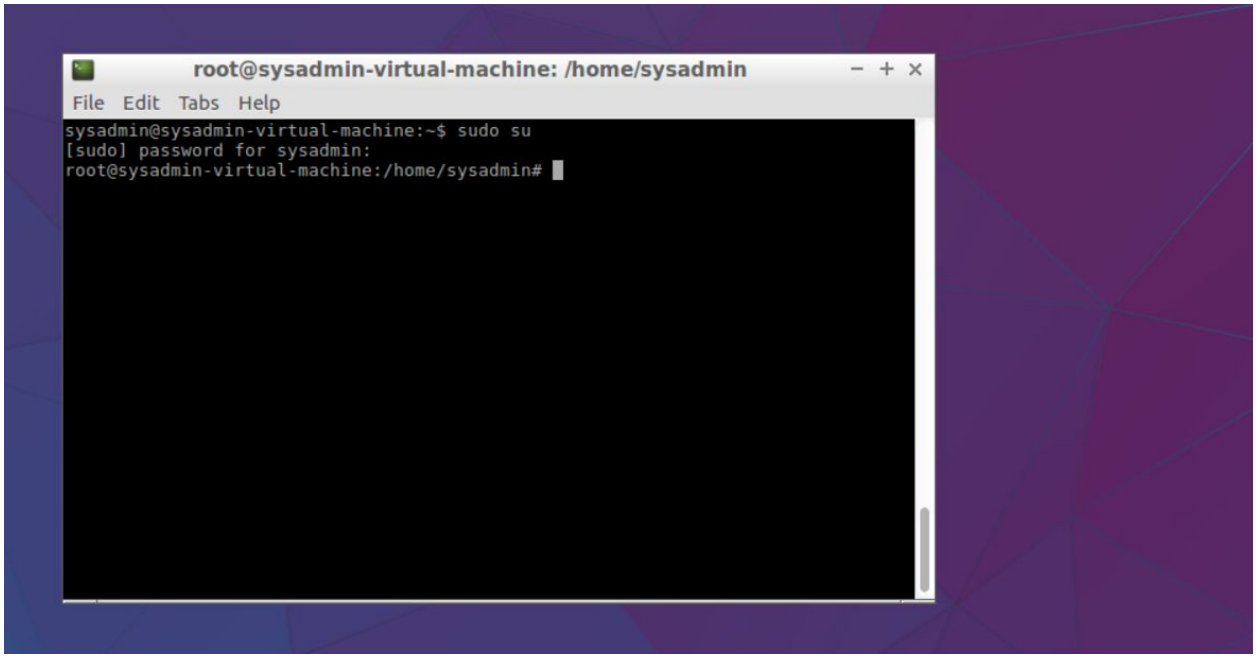
Linux Setup

1. After signing into the HelperVM, check the network connectivity by going to the browser and searching google.com as shown below or pinging 8.8.8.8. If ping is working but you can't connect to the internet check you DNS server in the Network Settings.



Creating Users and Groups

1. Now open up the terminal*(Ctrl + Alt + T or use GUI)* and type *sudo su* to get the root(aka superuser) access to the machine.



2. Now to add user using useradd command just type *useradd* <*username*>(gursimr2 in my case). The *-m* is for creating a home directory for the user(it's optional, but I like it better this way).

```
root@sysadmin-virtual-machine:/etc# useradd gursimr2 -m
```

3. The *useradd* by default doesn't do anything except creating a user. If you want to set a password for the user you can type *passwd* <*username*> and change the password as shown below.

```
root@sysadmin-virtual-machine:/home# passwd gursimr2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

4. Now to add user sdileto using adduser which is more interactive, just follow the screenshot.

```
root@sysadmin-virtual-machine:/home/sysadmin# adduser sdileto
Adding user `sdileto' ...
Adding new group `sdileto' (1002) ...
Adding new user `sdileto' (1002) with group `sdileto' ...
Creating home directory `/home/sdileto' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sdileto
Enter the new value, or press ENTER for the default
        Full Name []: Shanelle lleto
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@sysadmin-virtual-machine:/home/sysadmin#
```

5. Repeat the previous step for user djmurray (as assigned) and you can use any command but I am using adduser here.

```
root@sysadmin-virtual-machine: /home/sysadmin
File  Edit  Tabs  Help
root@sysadmin-virtual-machine:/home/sysadmin# adduser djmurray
Adding user `djmurray' ...
Adding new group `djmurray' (1003) ...
Adding new user `djmurray' (1003) with group `djmurray' ...
Creating home directory `/home/djmurray' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for djmurray
Enter the new value, or press ENTER for the default
        Full Name []: Dave Murray
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@sysadmin-virtual-machine:/home/sysadmin#
```

6. You can check the user directories by going to home directory and using the *ls* command. You can even go to */etc/passwd* file to check if the user is created.

```
root@sysadmin-virtual-machine:/home# ls
djmurray  gursimr2  sdileto  sysadmin
```

7. Now for creating a group, just type *groupadd* <*groupname*> (UBNetDef in our case)as shown below.

```
root@sysadmin-virtual-machine:/home# groupadd UBNetDef
```

8. Create two more groups (SysSec and SecDev) or as many as you like with the same command as shown below.

```
root@sysadmin-virtual-machine:/home# groupadd SysSec
root@sysadmin-virtual-machine:/home# groupadd SecDev
```

9. Now since we want all our users to be part of UBNetDef, we will set the primary group for all users as UBNetDef by using the command - *usermod -g* <*group*> <*user*>. You can check the user id and group id along with the number of groups user is in using the command - *id* <*user*> as shown below.

```
root@sysadmin-virtual-machine: /h
File  Edit  Tabs  Help
root@sysadmin-virtual-machine:/home# usermod -g UBNetDef gursimr2
root@sysadmin-virtual-machine:/home# id gursimr2
uid=1004(gursimr2) gid=1005(UBNetDef) groups=1005(UBNetDef)
root@sysadmin-virtual-machine:/home# usermod -g UBNetDef sdileto
root@sysadmin-virtual-machine:/home# id sdileto
uid=1002(sdileto) gid=1005(UBNetDef) groups=1005(UBNetDef)
root@sysadmin-virtual-machine:/home# usermod -g UBNetDef djmurray
root@sysadmin-virtual-machine:/home# id djmurray
uid=1003(djmurray) gid=1005(UBNetDef) groups=1005(UBNetDef)
```

10. Now add the users djmurray and sdileto to the group SecDev as their secondary group using the command - *usermod -G* <*group*> <*user*>. You can check the group using the id command mentioned in the previous step. Similarly, add user gursimr2 to the group SysSec as their secondary group as shown in the following screenshots.

```
root@s
File  Edit  Tabs  Help
root@sysadmin-virtual-machine:/home# usermod -G SecDev djmurray
root@sysadmin-virtual-machine:/home# usermod -G SecDev sdileto
root@sysadmin-virtual-machine:/home# id djmurray
uid=1003(djmurray) gid=1005(UBNetDef) groups=1005(UBNetDef),1007(SecDev)
root@sysadmin-virtual-machine:/home# id sdileto
uid=1002(sdileto) gid=1005(UBNetDef) groups=1005(UBNetDef),1007(SecDev)
```

```
root@sysadmin-virtual-machine:/home# usermod -G SysSec gursimr2
root@sysadmin-virtual-machine:/home# id gursimr2
uid=1004(gursimr2) gid=1005(UBNetDef) groups=1005(UBNetDef),1006(SysSec)
```

File and Owner Permissions

1. Now go to home directory(can use *cd*) and then *cd djmurray* directory and create a file using the command - *touch <filename>* which will be *students_grades.txt* in our case and *ls* to view the created file in the directory.

```
root@sysadmin-virtual-machine:/home# cd djmurray
root@sysadmin-virtual-machine:/home/djmurray# touch students_grades.txt
root@sysadmin-virtual-machine:/home/djmurray# ls
students_grades.txt
```

2. You can write into the file as shown below using the *cat* command or you can just leave it empty(Yes, you can always use *nano*).

```
root@sysadmin-virtual-machi
File  Edit  Tabs  Help
root@sysadmin-virtual-machine:/home/djmurray# cat >> students_grades.txt
I would tell you a UDP joke, but you might not get it.
root@sysadmin-virtual-machine:/home/djmurray# cat students_grades.txt
I would tell you a UDP joke, but you might not get it.
root@sysadmin-virtual-machine:/home/djmurray#
```

3. Now make djmurray the owner of the file using the command *chown* as shown below. After that, to make the file accessible to a group use command *chgrp* as shown below.

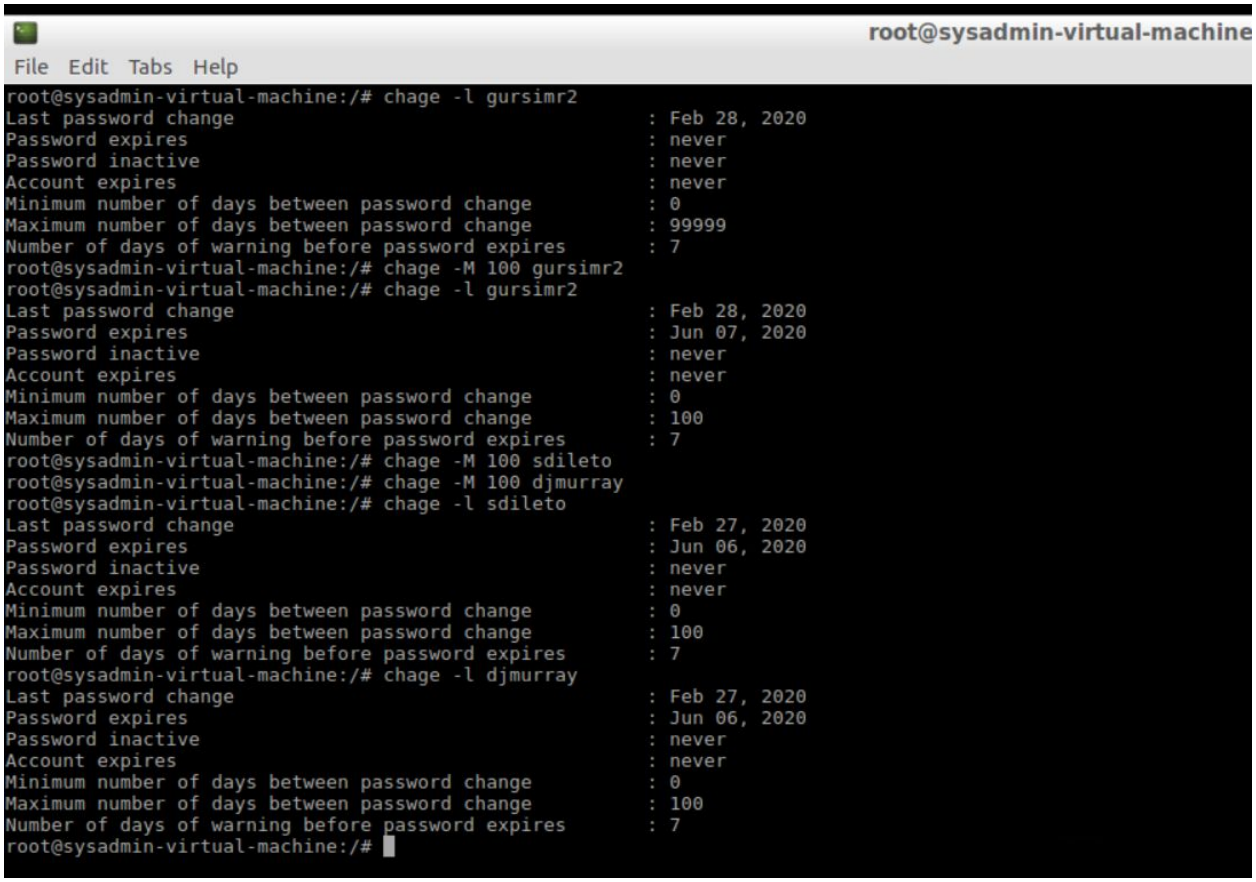
```
root@sysadmin-virtual-machine: /hor
File  Edit  Tabs  Help
root@sysadmin-virtual-machine:/home/djmurray# chown djmurray students_grades.txt
root@sysadmin-virtual-machine:/home/djmurray# chgrp SecDev students_grades.txt
```

4. Now in order to change the file permissions using command *chmod* as shown below. The following command allows the owner to read, write and execute the file, whereas it restricts the group to only read the file and doesn't allow anyone else access to the file(If you are *root*, you don't have to worry).

```
root@sysadmin-virtual-machine:/home/djmurray# chmod 740 students_grades.txt
root@sysadmin-virtual-machine:/home/djmurray# ls -l
total 4
-rwxr----- 1 djmurray SecDev 55 Feb 28 11:31 students_grades.txt
```

Linux Hardening

1. Use the command *chage* as shown below with the argument *-l* to list any password restrictions and to restrict the user to change password every 100 days type command - *chage -M 100 <user>* as shown below. Do it for all the users to force them to change their passwords regularly, which is a good habit.



```
root@sysadmin-virtual-machine
File  Edit  Tabs  Help
root@sysadmin-virtual-machine:/# chage -l gursimr2
Last password change                                    : Feb 28, 2020
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
root@sysadmin-virtual-machine:/# chage -M 100 gursimr2
root@sysadmin-virtual-machine:/# chage -l gursimr2
Last password change                                    : Feb 28, 2020
Password expires                                        : Jun 07, 2020
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 100
Number of days of warning before password expires       : 7
root@sysadmin-virtual-machine:/# chage -M 100 sdileto
root@sysadmin-virtual-machine:/# chage -M 100 djmurray
root@sysadmin-virtual-machine:/# chage -l sdileto
Last password change                                    : Feb 27, 2020
Password expires                                        : Jun 06, 2020
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 100
Number of days of warning before password expires       : 7
root@sysadmin-virtual-machine:/# chage -l djmurray
Last password change                                    : Feb 27, 2020
Password expires                                        : Jun 06, 2020
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 100
Number of days of warning before password expires       : 7
root@sysadmin-virtual-machine:/#
```

2. To apply security updates only, first you can just use *apt-get update* to update the machine before applying changes(it's optional and depends on the machine). You need to first download the package *unattended-upgrades* as shown below and then run it by typing *unattended-upgrades -d* or you can do it without if you don't want to see anything interactive.

```
root@sysadmin-virtual-machine:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Hit:2 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [831 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [1,110 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [643 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [902 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [316 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [486 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [424 kB]
Get:12 http://security.ubuntu.com/ubuntu xenial-security/universe i386 Packages [420 kB]
Get:13 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [791 kB]
Get:14 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [199 kB]
Get:15 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [717 kB]
Get:16 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [330 kB]
Fetched 7,495 kB in 2s (2,701 kB/s)
Reading package lists... Done
```

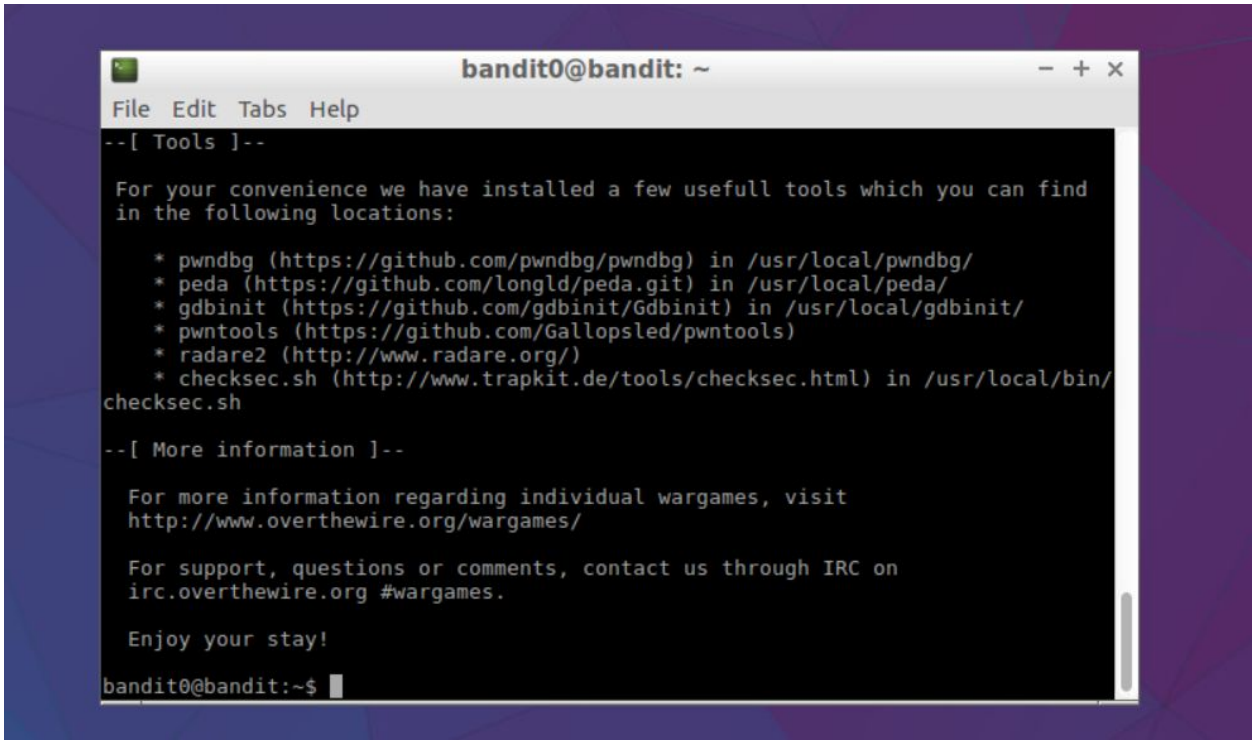
```
root@sysadmin-virtual-machine:/# apt-get install unattended-upgrades
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  bsd-mailx default-mta | mail-transport-agent needrestart
The following NEW packages will be installed:
  unattended-upgrades
0 upgraded, 1 newly installed, 0 to remove and 192 not upgraded.
Need to get 0 B/42.1 kB of archives.
After this operation, 418 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously unselected package unattended-upgrades.
(Reading database ... 155736 files and directories currently installed.)
Preparing to unpack .../unattended-upgrades_1.1ubuntu1.18.04.7~16.04.6_all.deb ...
Unpacking unattended-upgrades (1.1ubuntu1.18.04.7~16.04.6) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.21) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up unattended-upgrades (1.1ubuntu1.18.04.7~16.04.6) ...

Creating config file /etc/apt/apt.conf.d/20auto-upgrades with new version

Creating config file /etc/apt/apt.conf.d/50unattended-upgrades with new version
Synchronizing state of unattended-upgrades.service with SysV init with /lib/systemd/systemd-sysv-install...
Executing /lib/systemd/systemd-sysv-install enable unattended-upgrades
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.21) ...
root@sysadmin-virtual-machine:/#
```

```
root@sysadmin-virtual-machine:/# unattended-upgrade -d
Initial blacklisted packages:
Initial whitelisted packages:
Starting unattended upgrades script
Allowed origins are: o=Ubuntu,a=xenial, o=Ubuntu,a=xenial-security, o=UbuntuESMApps,a=xenial-apps-security, o=UbuntuESM,a=xenial-infra-security
Using (^linux-image-[0-9]+\.[0-9\.]+-.*|^linux-headers-[0-9]+\.[0-9\.]+-.*|^linux-image-extra-[0-9]+\.[0-9\.]+-.*|^linux-modules-[0-9]+\.[0-9\.]+-.*|^linux-modules-extra-[0-9]+\.[0-9\.]+-.*
|^linux-signed-image-[0-9]+\.[0-9\.]+-.*|^kfreebsd-image-[0-9]+\.[0-9\.]+-.*|^kfreebsd-headers-[0-9]+\.[0-9\.]+-.*|^gnumach-image-[0-9]+\.[0-9\.]+-.*|^.*-modules-[0-9]+\.[0-9\.]+-.*|^.*-ker
nel-[0-9]+\.[0-9\.]+-.*|^linux-backports-modules-.*-[0-9]+\.[0-9\.]+-.*|^linux-modules-.*-[0-9]+\.[0-9\.]+-.*|^linux-tools-[0-9]+\.[0-9\.]+-.*|^linux-cloud-tools-[0-9]+\.[0-9\.]+-.*|^linux-
image-[0-9]+\.[0-9\.]+-.*|^linux-headers-[0-9]+\.[0-9\.]+-.*|^linux-image-extra-[0-9]+\.[0-9\.]+-.*|^linux-modules-[0-9]+\.[0-9\.]+-.*|^linux-modules-extra-[0-9]+\.[0-9\.]+-.*|^linux-signed
-image-[0-9]+\.[0-9\.]+-.*|^kfreebsd-image-[0-9]+\.[0-9\.]+-.*|^kfreebsd-headers-[0-9]+\.[0-9\.]+-.*|^gnumach-image-[0-9]+\.[0-9\.]+-.*|^.*-modules-[0-9]+\.[0-9\.]+-.*|^.*-kernel-[0-9]+\.[0
-9\.]+-.*|^linux-backports-modules-.*-[0-9]+\.[0-9\.]+-.*|^linux-modules-.*-[0-9]+\.[0-9\.]+-.*|^linux-tools-[0-9]+\.[0-9\.]+-.*|^linux-cloud-tools-[0-9]+\.[0-9\.]+-.*) regexp to find kerne
l packages
Using (^linux-image-4\.15\.0\-50\-generic$|^linux-headers-4\.15\.0\-50\-generic$|^linux-image-extra-4\.15\.0\-50\-generic$|^linux-modules-4\.15\.0\-50\-generic$|^linux-modules-extra-4\.15\.
0\-50\-generic$|^linux-signed-image-4\.15\.0\-50\-generic$|^kfreebsd-image-4\.15\.0\-50\-generic$|^kfreebsd-headers-4\.15\.0\-50\-generic$|^gnumach-image-4\.15\.0\-50\-generic$|^.*-modules-
4\.15\.0\-50\-generic$|^.*-kernel-4\.15\.0\-50\-generic$|^linux-backports-modules-.*-4\.15\.0\-50\-generic$|^linux-modules-.*-4\.15\.0\-50\-generic$|^linux-tools-4\.15\.0\-50\-generic$|^lin
ux-cloud-tools-4\.15\.0\-50\-generic$|^linux-image-4\.15\.0\-50\-generic$|^linux-headers-4\.15\.0\-50\-generic$|^linux-image-extra-4\.15\.0\-50\-generic$|^linux-modules-4\.15\.0\-50\-generi
c$|^linux-modules-extra-4\.15\.0\-50\-generic$|^linux-signed-image-4\.15\.0\-50\-generic$|^kfreebsd-image-4\.15\.0\-50\-generic$|^kfreebsd-headers-4\.15\.0\-50\-generic$|^gnumach-image-4\.1
5\.0\-50\-generic$|^.*-modules-4\.15\.0\-50\-generic$|^.*-kernel-4\.15\.0\-50\-generic$|^linux-backports-modules-.*-4\.15\.0\-50\-generic$|^linux-modules-.*-4\.15\.0\-50\-generic$|^linux-to
ols-4\.15\.0\-50\-generic$|^linux-cloud-tools-4\.15\.0\-50\-generic$) regexp to find running kernel packages
Checking: amd64-microcode ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'
xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubuntu.com' isTrusted:True>])
Checking: apparmor ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenial-
security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubuntu.com' isTrusted:True>])
Checking: apport ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenial-up
dates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubuntu.c
om' isTrusted:True>, <Origin component:'main' archive:'xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubuntu.com' isTrusted:True>])
Checking: apport-gtk ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenia
l-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubun
tu.com' isTrusted:True>, <Origin component:'main' archive:'xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubuntu.com' isTrusted:True>])
Checking: apt ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>])
adjusting candidate version: apt=1.2.29ubuntu0.1
Checking: apt-transport-https ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>])
adjusting candidate version: apt-transport-https=1.2.29ubuntu0.1
Checking: apt-utils ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>])
adjusting candidate version: apt-utils=1.2.29ubuntu0.1
Checking: aptdaemon ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenial
-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubunt
u.com' isTrusted:True>, <Origin component:'main' archive:'xenial-security' origin:'Ubuntu' label:'Ubuntu' site:'security.ubuntu.com' isTrusted:True>])
Checking: aptdaemon-data ([<Origin component:'main' archive:'xenial-updates' origin:'Ubuntu' label:'Ubuntu' site:'us.archive.ubuntu.com' isTrusted:True>, <Origin component:'main' archive:'x
```

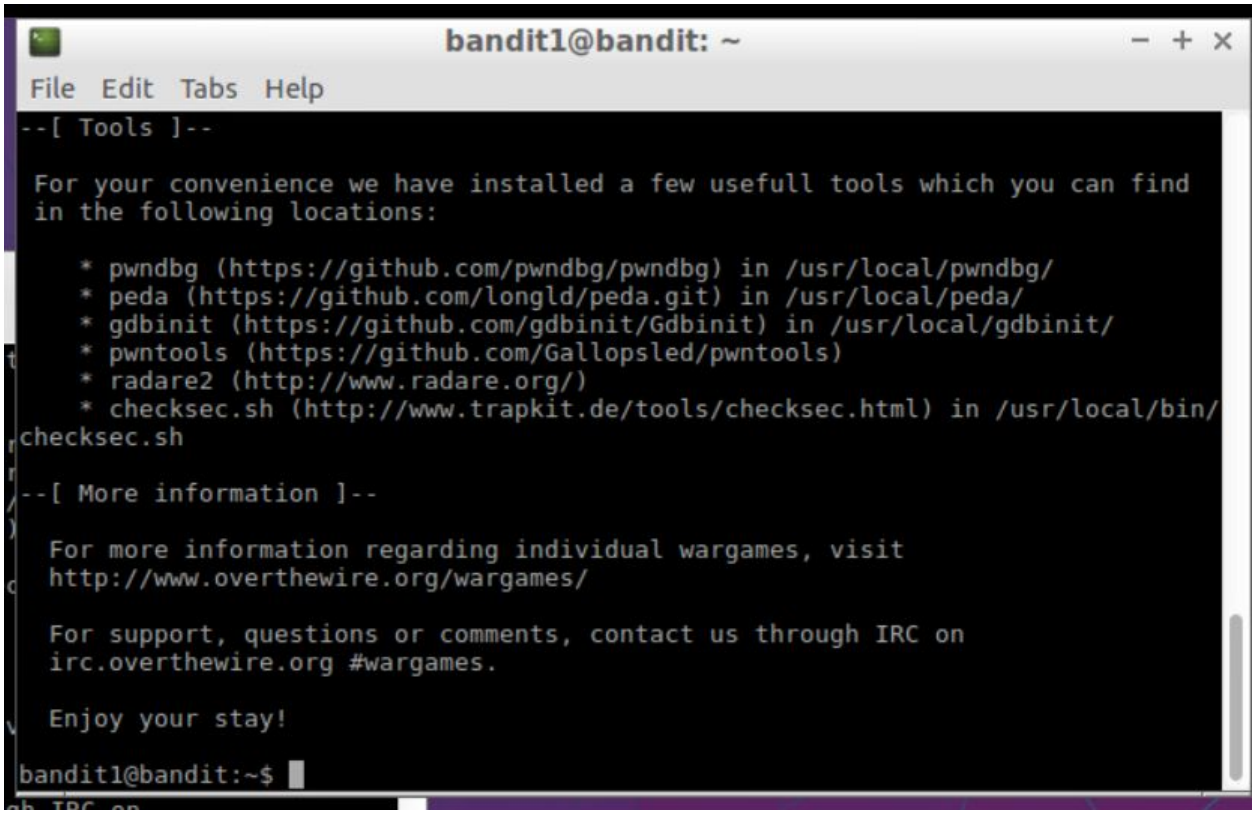
```
/etc/kernel/postinst.d/zz-update-grub:
Generating grub configuration file ...
Warning: Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_TIMEOUT is set is no longer supported.
Found linux image: /boot/vmlinuz-4.15.0-88-generic
Found initrd image: /boot/initrd.img-4.15.0-88-generic
Found linux image: /boot/vmlinuz-4.15.0-50-generic
Found initrd image: /boot/initrd.img-4.15.0-50-generic
Found linux image: /boot/vmlinuz-4.15.0-29-generic
Found initrd image: /boot/initrd.img-4.15.0-29-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
left to upgrade set()
All upgrades installed
InstCount=0 DelCount=0 BrokenCount=0
Extracting content from /var/log/unattended-upgrades/unattended-upgrades-dpkg.log since 2020-02-28 11:53:42
root@sysadmin-virtual-machine:/#
```

OverTheWire

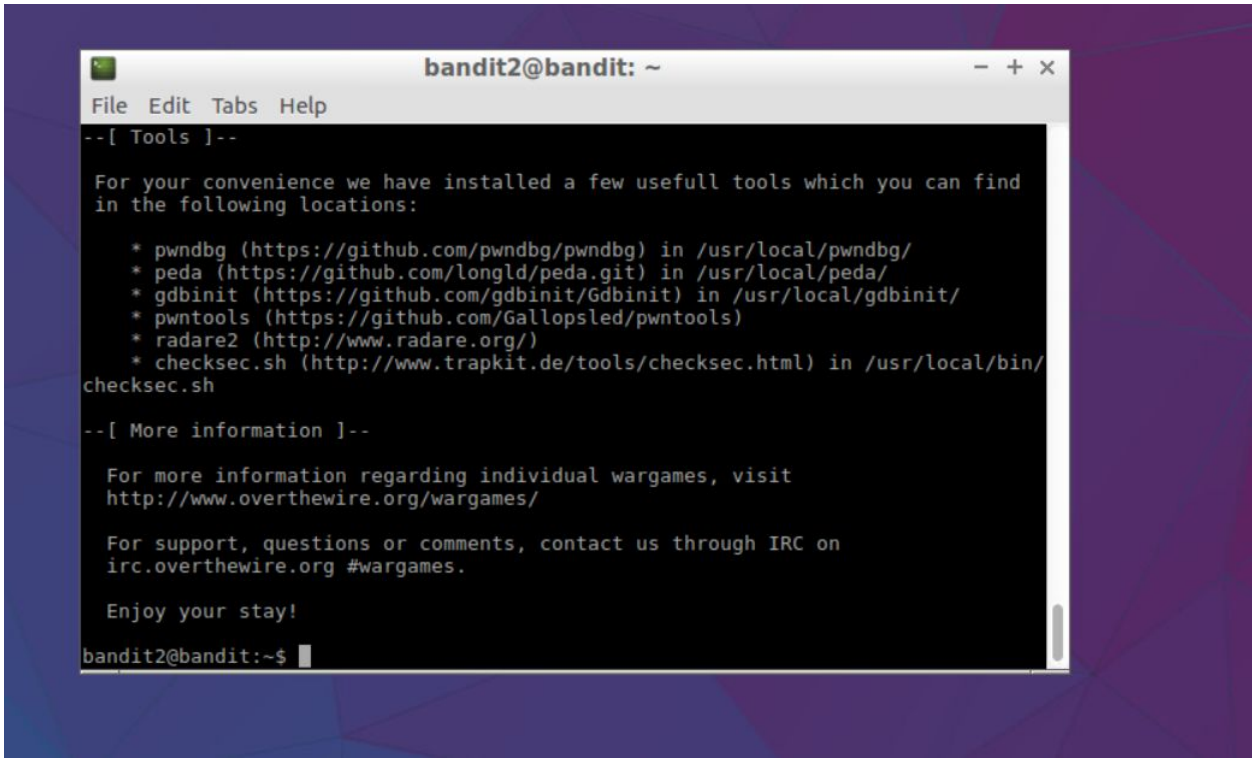
1. Bandit0-shell



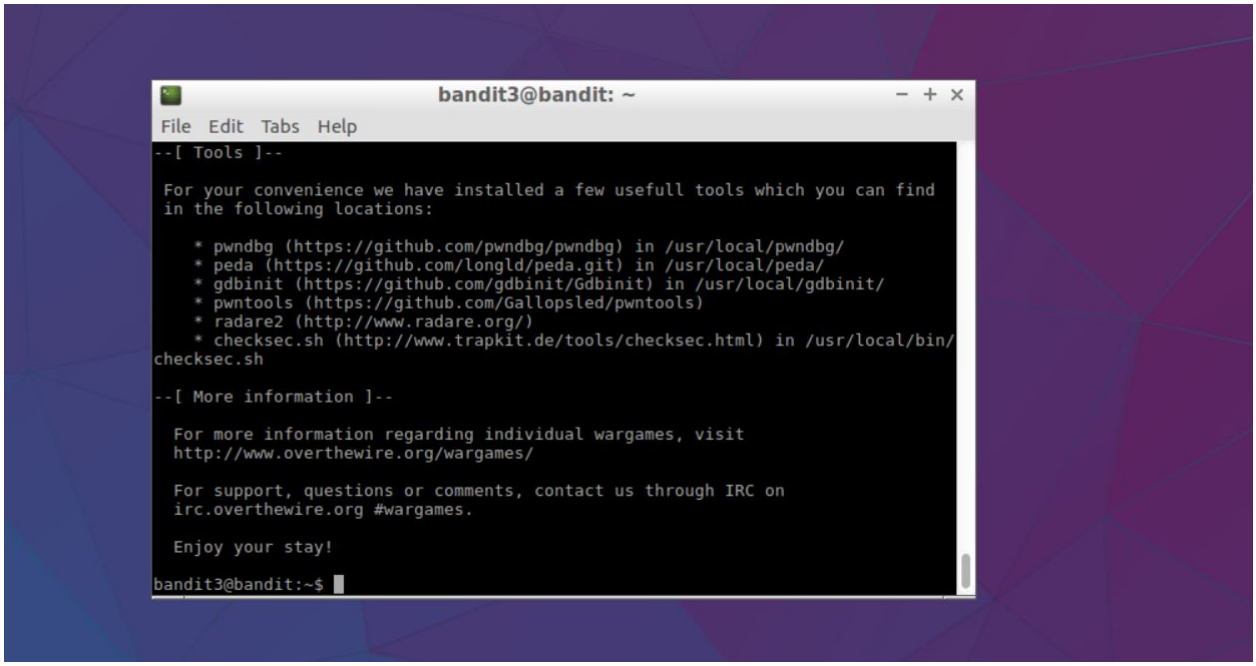
2. Bandit1-shell



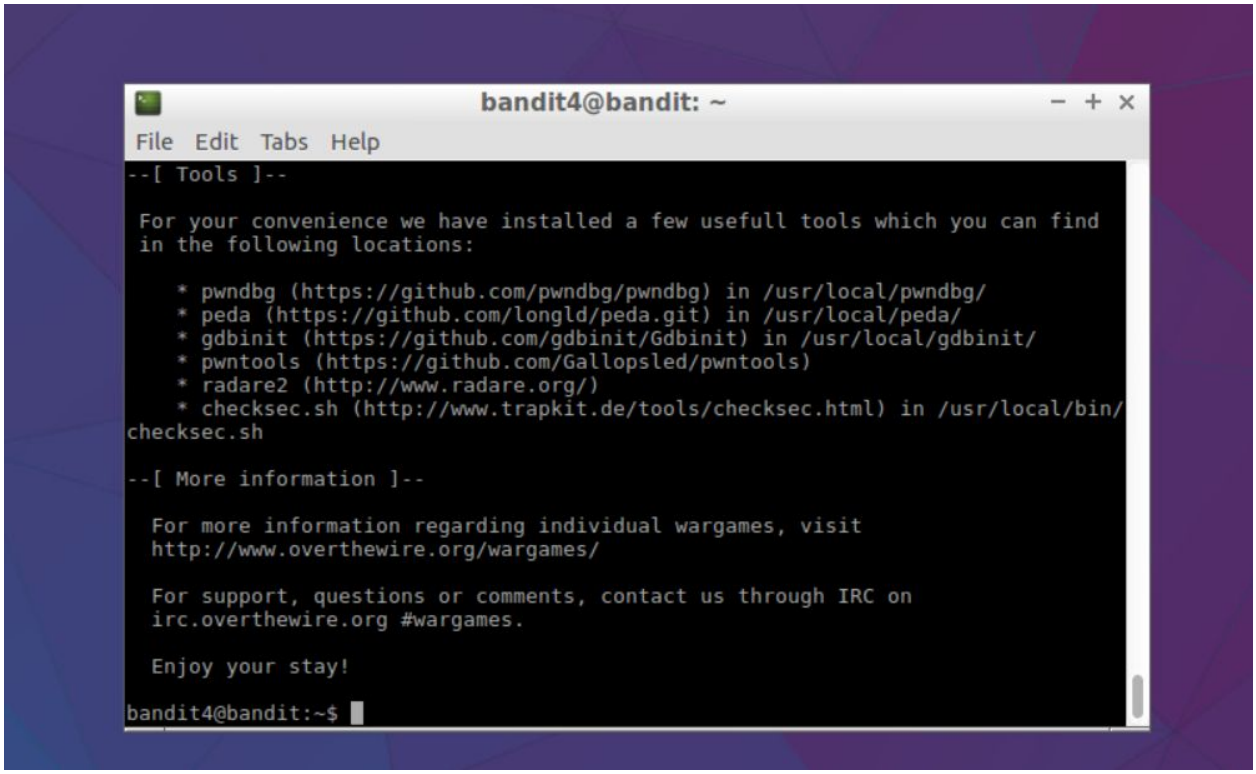
3. Bandit2-shell



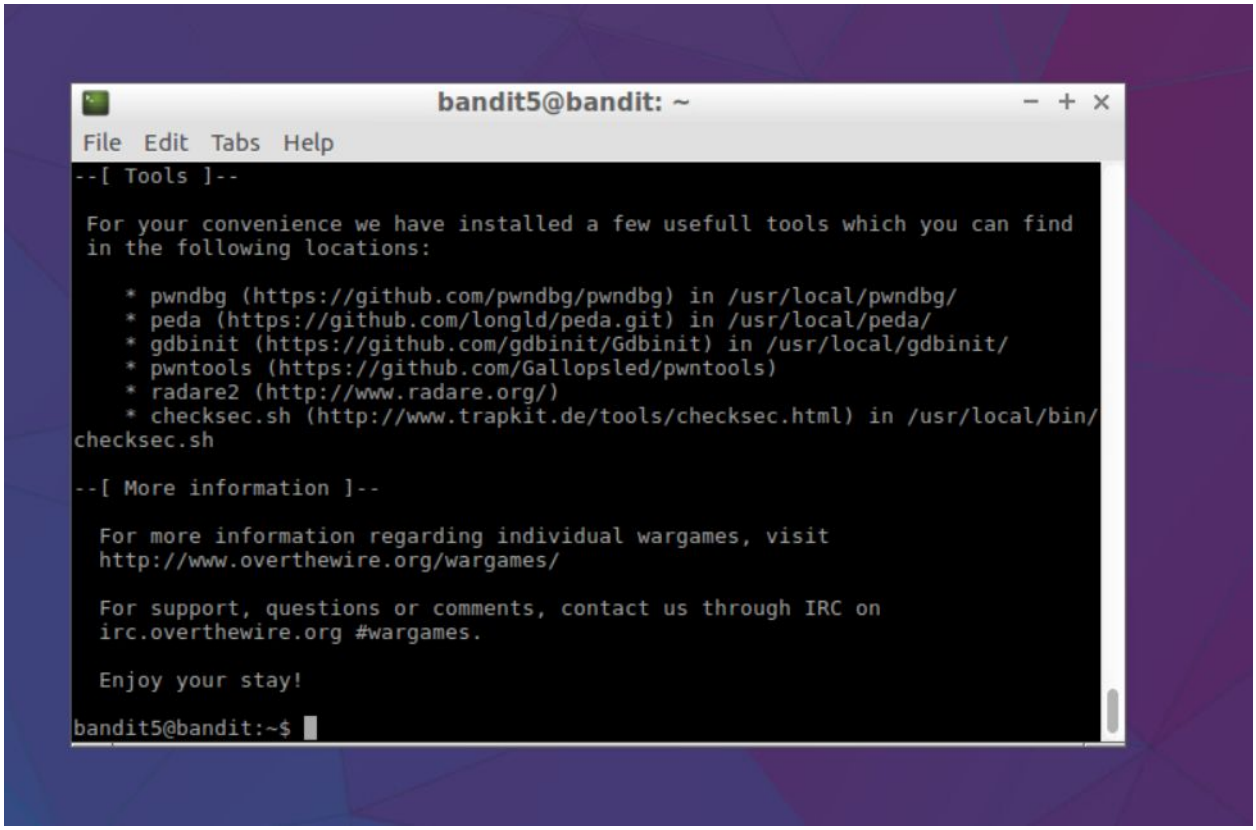
4. Bandit3-shell



5. Bandit4-shell



6. Bandit5-shell



THE END