Module 6: Introduction to Linux

Review of Kali Linux
-metasploit: pen test
-burpsuite: webapp pen
-zenmap: network scan

Phases of Ethical Hacking:
1.Information gathering
2.Vulnerability analysis
3.Web Application Analysis
4.Database Assessment
5.Password Attacks
6.Wireless Attacks
7.Reverse Engineering
8.Exploitation
9.Sniffing and Spoofing
10.Post Exploitation
11.Forensics
12.Reporting
13.Social Engineering

Navigating the Filesystem
pwd - Printworking directory
cd - change directory
ls - lists everything in the folder

double tab can be used to ls

mkdir - make directory
rmdir - remove directory
'ls -la' - searches for hidden folders

cp - copy a file or folder
mv - move a file or folder
locate - finds everything with a keyword
updatedb - updates database of information w/update
passwd - changes password
man - instructions for any command that you are using. ex. 'man ls'

Users and Privleges

Privleges

'-' is a file
'd' is a directory
'r' means read

'w' means write
'x' means execute

chmod - change access to a file
adduser - allows you to add a user
/etc/passwd - file that shows you all the users (does not show the actual password)
cat /etc/shadow - will help you see password information
su 'user' - change the usersudo

Network Commands
ifconfig (shows network information.)

iwconfig (used to show wirelsess network information.)

ping 'address we are trying to talk to' (cntrl c stops the ping)

arp -a (shows ip address it talks to and the mac address associated.)

netstat -ano (shows active connections running on your machine.)

route (prints your routing table) tells you where your traffic is exiting.

pivoting (switching a network from one to another using a machine)

Viewing, Creating, Editing files

'echo' can be used to write to a file
ex. echo "hey" > hey.txt

append this txt with:
echo "hey again" >> hey.txt

nano is a terminal text editor
ex.nano newfile.txt

Starting and Stopping Kali Services

Apache2 is a web server (If want to run a webpage we need to run apache2)

'service apache2 start'

computer /var/www/html to change address but an easy way is by

echo "hello" > hello.txt
ls
python -m SimpleHTTPServer 80

HOW TO SPIN UP FTP SERVER WITH PYTHON:

1.apt-get install vsftpd

Need to learn about FTP (File transfer protocol) networks (this will touched on when learning metasploit I think.)

Examples:
-pureFTPd

-Metasploits FTP server module
-Python pyftpdlib
-Kali's atftpd Trivial FTP Server

PERMENANT SERVICE

systemctl enable (or disable) ssh

ssh - is a Secure Shell. It is a method of secure remote login from on computer to another.

Ex. systemctl enable postgresql

Installing and Updating Tools

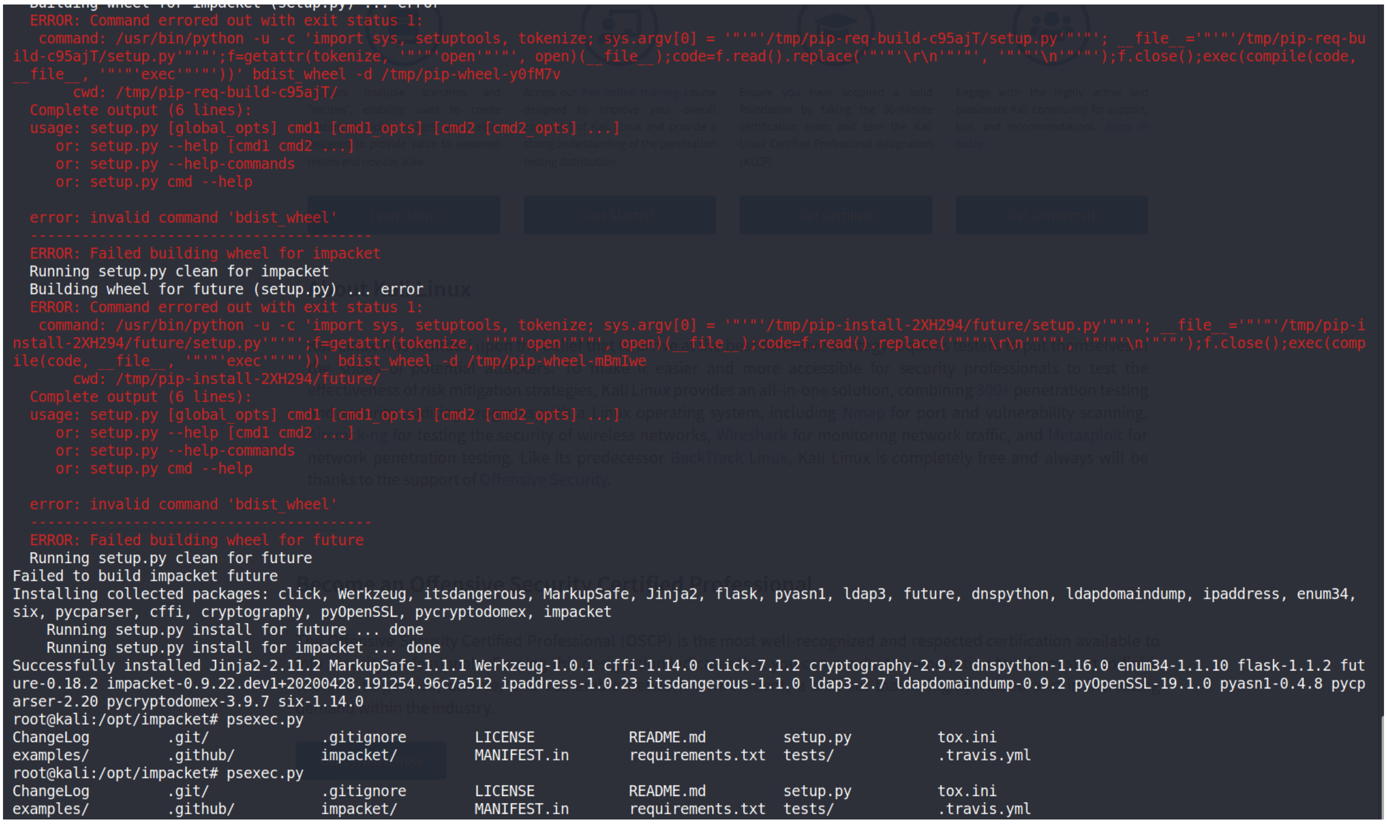
```
-apt update && apt upgrade
*this will update and then upgrade*
```

apt python3-pip to install python 3

go to github to install impacket.

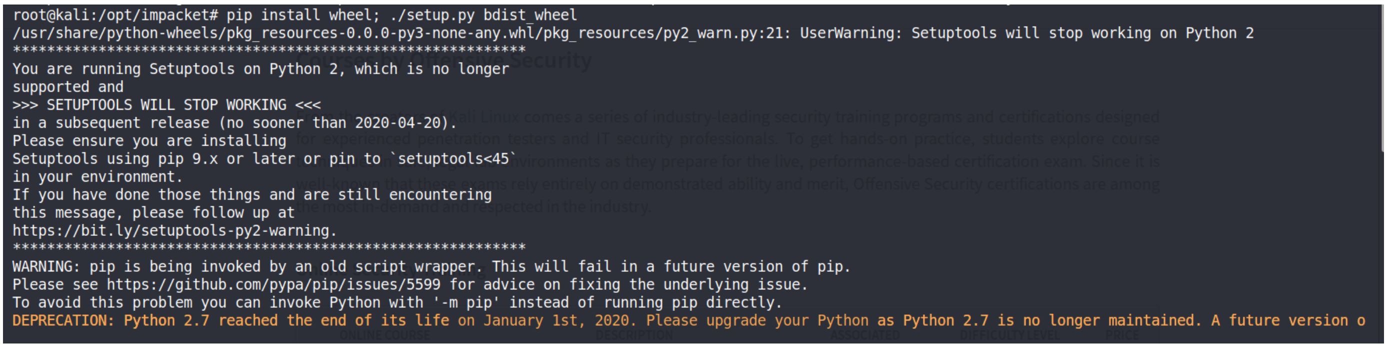
'git clone https://github.com/SecureAuthCorp/impacket.git'

while in /opt/impacket run 'pip install .'
ran into issue installing impacket using python3-pip error bdist wheel:



```
  Building wheel for impacket (setup.py) ... error
  ERROR: Command errored out with exit status 1:
   command: /usr/bin/python -u -c 'import sys, setuptools, tokenize; sys.argv[0] = '"'"'/tmp/pip-req-build-c95ajT/setup.py'"'"'; __file__='"'"'/tmp/pip-req-bu
ild-c95ajT/setup.py'"'"';f=getattr(tokenize, '"'"'open'"'"', open)(__file__);code=f.read().replace('"'"'\r\n'"'"', '"'"'\n'"'"');f.close();exec(compile(code,
__file__, '"'"'exec'"'"'))' bdist_wheel -d /tmp/pip-wheel-y0fM7v
       cwd: /tmp/pip-req-build-c95ajT/
  Complete output (6 lines):
  usage: setup.py [global_opts] cmd1 [cmd1_opts] [cmd2 [cmd2_opts] ...]
     or: setup.py --help [cmd1 cmd2 ...]
     or: setup.py --help-commands
     or: setup.py cmd --help

  error: invalid command 'bdist_wheel'
  ----------------------------------------
  ERROR: Failed building wheel for impacket
  Running setup.py clean for impacket
  Building wheel for future (setup.py) ... error
  ERROR: Command errored out with exit status 1:
   command: /usr/bin/python -u -c 'import sys, setuptools, tokenize; sys.argv[0] = '"'"'/tmp/pip-install-2XH294/future/setup.py'"'"'; __file__='"'"'/tmp/pip-i
nstall-2XH294/future/setup.py'"'"';f=getattr(tokenize, '"'"'open'"'"', open)(__file__);code=f.read().replace('"'"'\r\n'"'"', '"'"'\n'"'"');f.close();exec(comp
ile(code, __file__, '"'"'exec'"'"'))' bdist_wheel -d /tmp/pip-wheel-mBmIwe
       cwd: /tmp/pip-install-2XH294/future/
  Complete output (6 lines):
  usage: setup.py [global_opts] cmd1 [cmd1_opts] [cmd2 [cmd2_opts] ...]
     or: setup.py --help [cmd1 cmd2 ...]
     or: setup.py --help-commands
     or: setup.py cmd --help

  error: invalid command 'bdist_wheel'
  ----------------------------------------
  ERROR: Failed building wheel for future
  Running setup.py clean for future
Failed to build impacket future
Installing collected packages: click, Werkzeug, itsdangerous, MarkupSafe, Jinja2, flask, pyasn1, ldap3, future, dnspython, ldapdomaindump, ipaddress, enum34,
six, pycparser, cffi, cryptography, pyOpenSSL, pycryptodomex, impacket
    Running setup.py install for future ... done
    Running setup.py install for impacket ... done
Successfully installed Jinja2-2.11.2 MarkupSafe-1.1.1 Werkzeug-1.0.1 cffi-1.14.0 click-7.1.2 cryptography-2.9.2 dnspython-1.16.0 enum34-1.1.10 flask-1.1.2 fut
ure-0.18.2 impacket-0.9.22.dev1+20200428.191254.96c7a512 ipaddress-1.0.23 itsdangerous-1.1.0 ldap3-2.7 ldapdomaindump-0.9.2 pyOpenSSL-19.1.0 pyasn1-0.4.8 pycp
arser-2.20 pycryptodomex-3.9.7 six-1.14.0
root@kali:/opt/impacket# psexec.py
ChangeLog         .git/             .gitignore        LICENSE           README.md         setup.py          tox.ini
examples/         .github/          impacket/         MANIFEST.in       requirements.txt  tests/            .travis.yml
root@kali:/opt/impacket# psexec.py
ChangeLog         .git/             .gitignore        LICENSE           README.md         setup.py          tox.ini
examples/         .github/          impacket/         MANIFEST.in       requirements.txt  tests/            .travis.yml
```

solution was to install wheel and reinstall impacket by command 'pip install .' in /opt/impacket#



```
root@kali:/opt/impacket# pip install wheel; ./setup.py bdist_wheel
/usr/share/python-wheels/pkg_resources-0.0.0-py3-none-any.whl/pkg_resources/py2_warn.py:21: UserWarning: Setuptools will stop working on Python 2
************************************************************
You are running Setuptools on Python 2, which is no longer
supported and
>>> SETUPTOOLS WILL STOP WORKING <<<
in a subsequent release (no sooner than 2020-04-20).
Please ensure you are installing
Setuptools using pip 9.x or later or pin to `setuptools<45`
in your environment.
If you have done those things and are still encountering
this message, please follow up at
https://bit.ly/setuptools-py2-warning.
************************************************************
WARNING: pip is being invoked by an old script wrapper. This will fail in a future version of pip.
Please see https://github.com/pypa/pip/issues/5599 for advice on fixing the underlying issue.
To avoid this problem you can invoke Python with '-m pip' instead of running pip directly.
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. A future version o
```

Bash Scripting (ex. Building a ping sweeper script.)

COMMANDS THAT WILL BE USED:

-grep (allows us to narrow results)

-cut (narrow results)

-tr (narrow results)

-script writing

-for loops

NARROWING RESULTS

Narrowing down a ping result

if we only want to send on ping packet. ping 172.16.4.128 -c 1

save to text file 'ping 172.16.4.128 -c 1 > ip.txt'

cat ip.txt

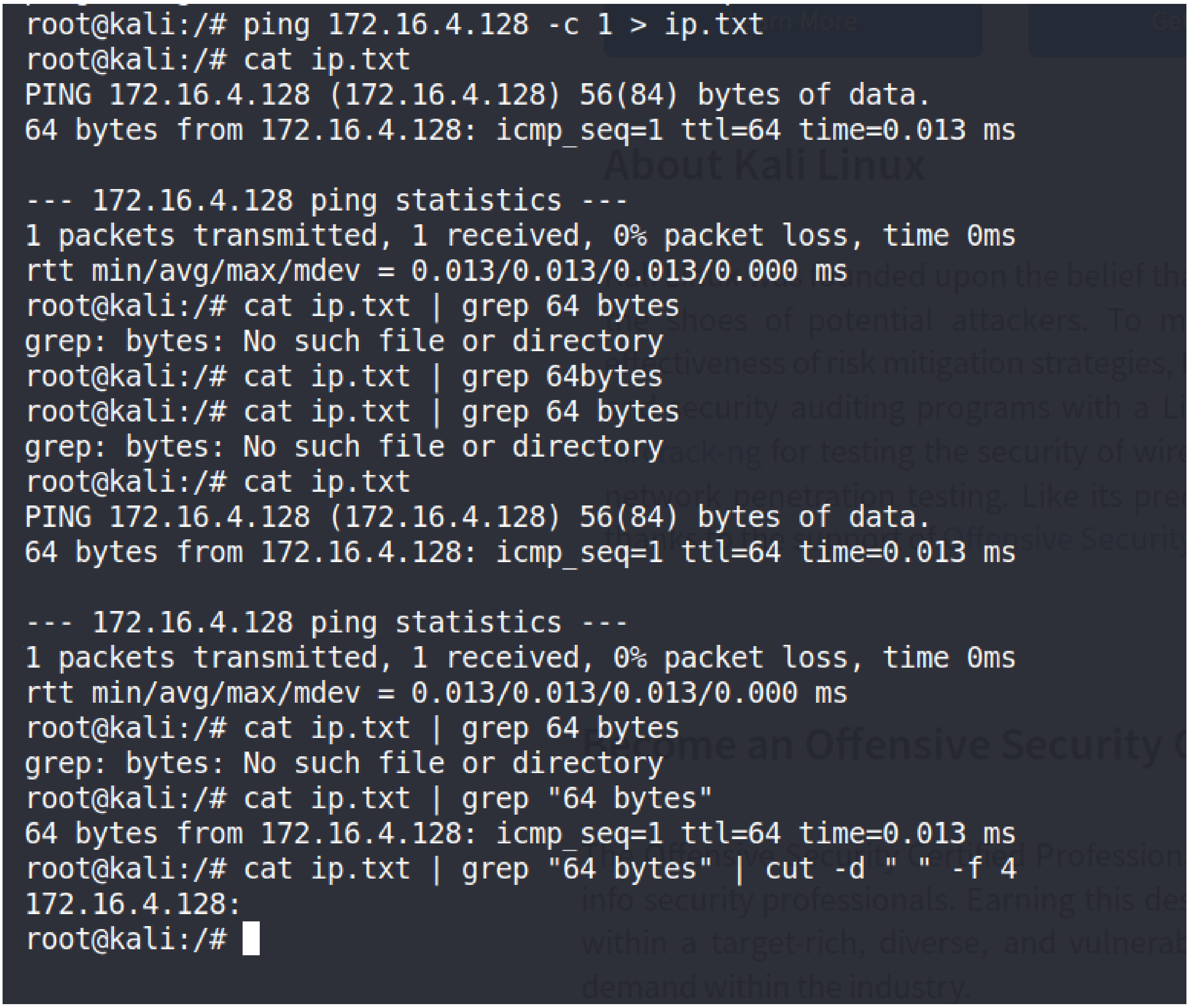
*goal is to extract ip address from large list of information from pinging a range of ip addresses.

*tool called cut gives us the ability to narrow down beyond using grep pipe.

-d = delimiter (gives us a delimeter to cut on)

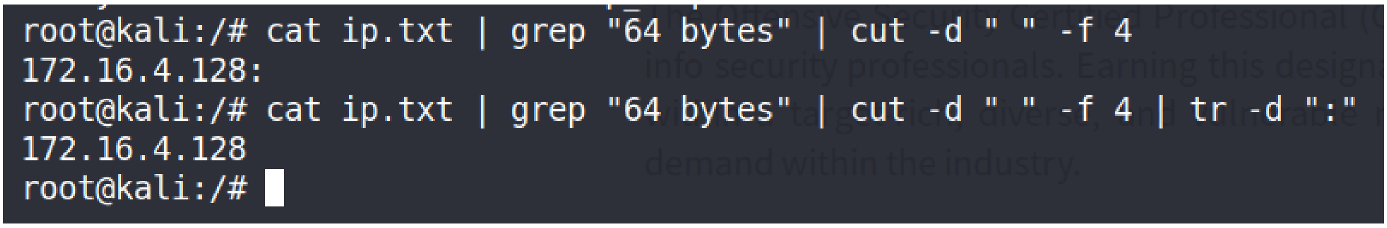
-f = field (cuts by a space to give us what we want)

See below:



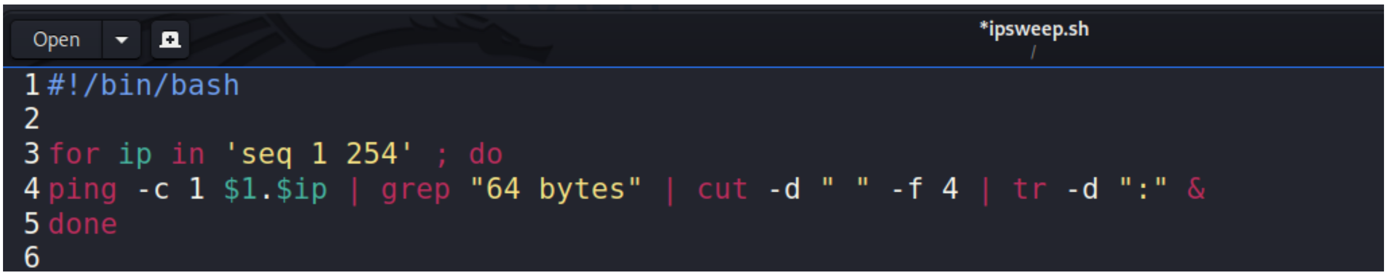
```
root@kali:/# ping 172.16.4.128 -c 1 > ip.txt
root@kali:/# cat ip.txt
PING 172.16.4.128 (172.16.4.128) 56(84) bytes of data.
64 bytes from 172.16.4.128: icmp_seq=1 ttl=64 time=0.013 ms

--- 172.16.4.128 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.013/0.013/0.013/0.000 ms
root@kali:/# cat ip.txt | grep 64 bytes
grep: bytes: No such file or directory
root@kali:/# cat ip.txt | grep 64bytes
root@kali:/# cat ip.txt | grep 64 bytes
grep: bytes: No such file or directory
root@kali:/# cat ip.txt
PING 172.16.4.128 (172.16.4.128) 56(84) bytes of data.
64 bytes from 172.16.4.128: icmp_seq=1 ttl=64 time=0.013 ms

--- 172.16.4.128 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.013/0.013/0.013/0.000 ms
root@kali:/# cat ip.txt | grep 64 bytes
grep: bytes: No such file or directory
root@kali:/# cat ip.txt | grep "64 bytes"
64 bytes from 172.16.4.128: icmp_seq=1 ttl=64 time=0.013 ms
root@kali:/# cat ip.txt | grep "64 bytes" | cut -d " " -f 4
172.16.4.128:
root@kali:/#
```

If the IP address we would still have the IP address with a colon on the end. Pipe and use another delimiter of -d ":" " to remove:



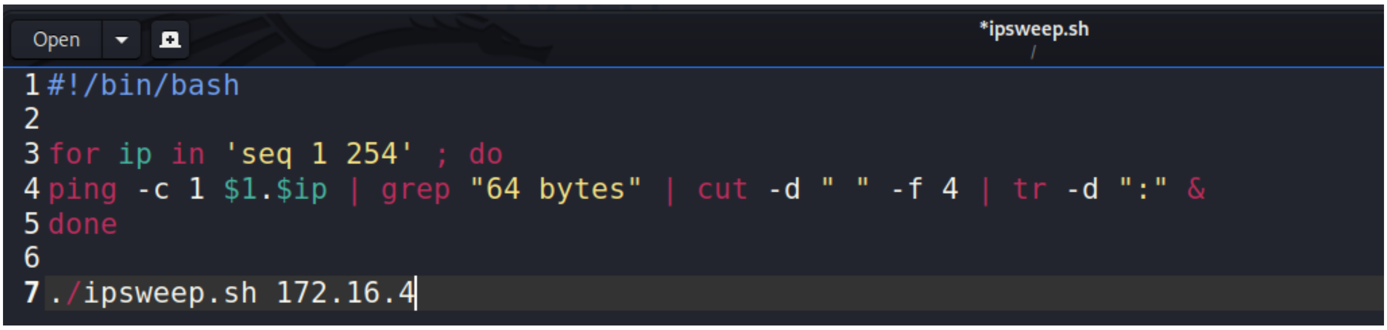
```
root@kali:/# cat ip.txt | grep "64 bytes" | cut -d " " -f 4
172.16.4.128:
root@kali:/# cat ip.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"
172.16.4.128
root@kali:/#
```

writing a ping sweep with bash
$1= user input



```
#!/bin/bash

for ip in 'seq 1 254' ; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done

```

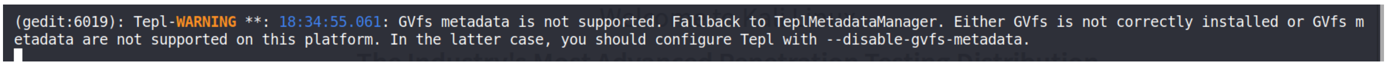
so we need to specify User input (Could also be hard coded directly where the $1 is. as '172.16.4.ip')



```
#!/bin/bash

for ip in 'seq 1 254' ; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done

./ipsweep.sh 172.16.4
```

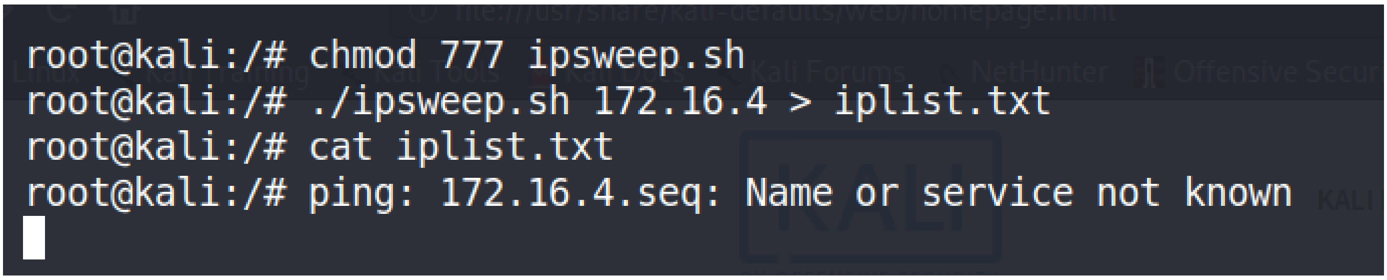
Save and run this. We will need to chmod 777 (x privledges to UserGroupOthers "UGO") and then run. We will have to enter an ip for the user input and save to our txt file. like such: (note: I cannot figure out why i keep getting service unknown. Issue with GVfs metadata not supported but I don't know how to turn it off. Tried search but feeling frustrated. I suppose it is an issue with the GNOME/gedit installation but I'm unsure why this would be happening. The installation appeared to go well. I am going to try hard coding the ip.)

Issue:



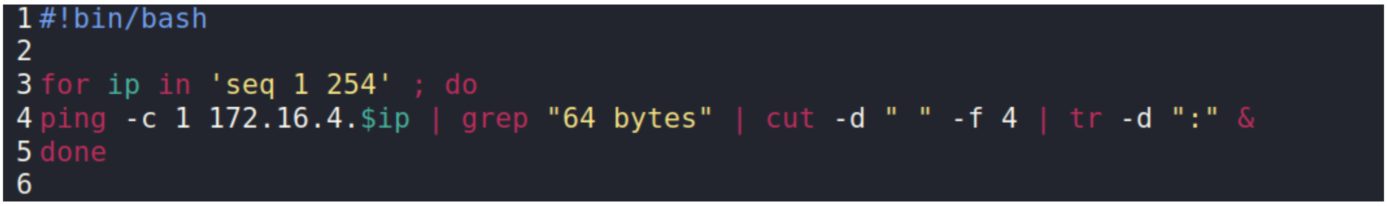
```
(gedit:6019): Tepl-WARNING **: 18:34:55.061: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs m
etadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
```

Before Hard coding:

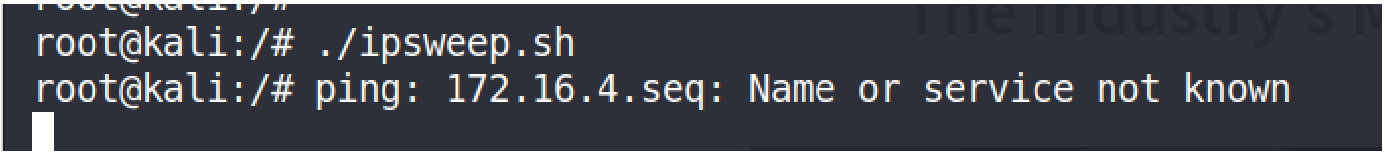


```
root@kali:/# chmod 777 ipsweep.sh
root@kali:/# ./ipsweep.sh 172.16.4 > iplist.txt
root@kali:/# cat iplist.txt
root@kali:/# ping: 172.16.4.seq: Name or service not known
```

After Hard coding:

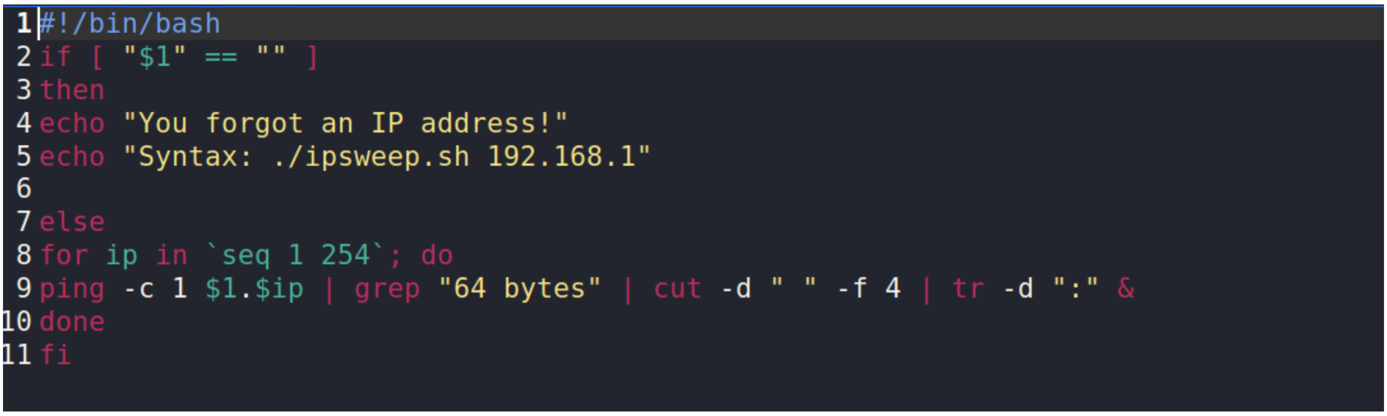


```
#!bin/bash

for ip in 'seq 1 254' ; do
ping -c 1 172.16.4.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done

```



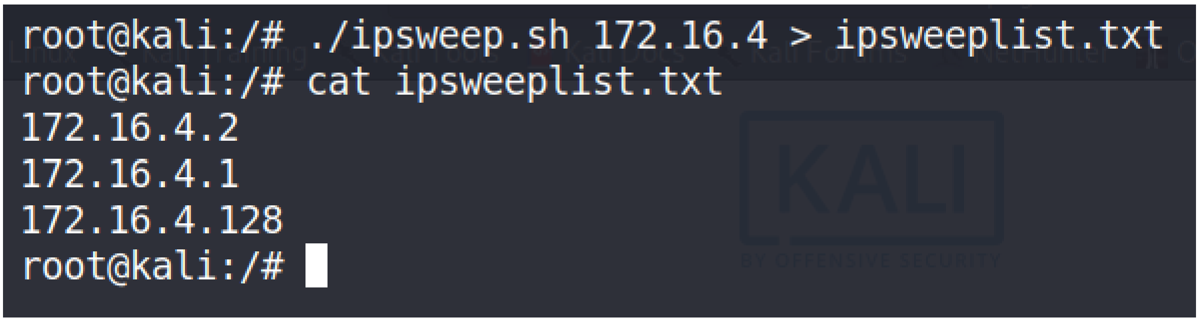
```
root@kali:/# ./ipsweep.sh
root@kali:/# ping: 172.16.4.seq: Name or service not known
```

(I think this is likely an issue with the sequence which i've entered for the ping. Looking now...) (okay, turns out that it was a syntax error but I dont know where. I used the course resource to copy/paste into my gedit ipsweep.sh file and here is what it looks like. *compared it with above but I still can't find the issue. Its may be because i've been staring at it too long.) see below: (Note: at the end we need to write if backwards as fi)



```
#!/bin/bash
if [ "$1" == "" ]
then
echo "You forgot an IP address!"
echo "Syntax: ./ipsweep.sh 192.168.1"

else
for ip in `seq 1 254`; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done
fi
```

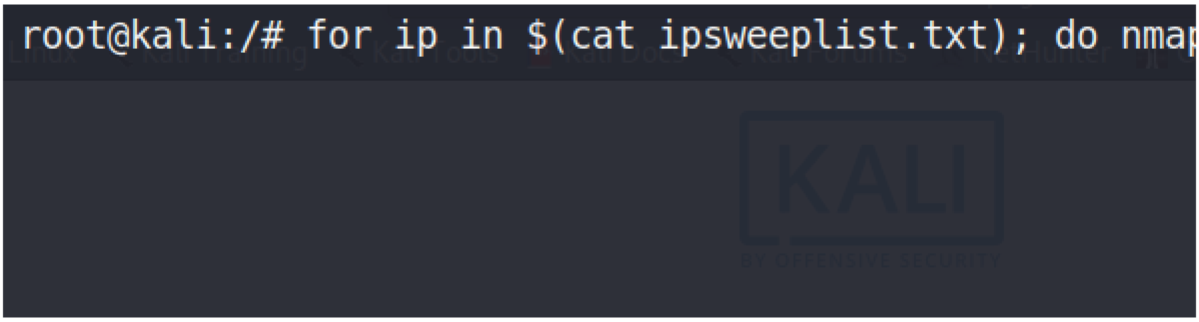
Now i'm going to copy this into a .txt file I create called ipsweeplist.txt



```
root@kali:/# ./ipsweep.sh 172.16.4 > ipsweeplist.txt
root@kali:/# cat ipsweeplist.txt
172.16.4.2
172.16.4.1
172.16.4.128
root@kali:/# 
```

Looping on liners

Example:



```
root@kali:/# for ip in $(cat ipsweeplist.txt); do nmap
```

Example Explanation:
For ip's in the list we will loop. when we loop we will nmap stealth scan port 80, T4 (speed), $declare ip, & to let it run multiples.

Need more studies on nmap