

REMOTE SERVER

Command execution (Screenshots)

#To find missing apps & download missing apps

#Part 1 – Apps: whois, curl, ssh, sshpass, nmap

```
xmnrproject2.sh x xmnrproject.sh x xmnrproject3.sh x removeapp.sh x
1  #!/bin/bash
2
3  function inst () {
4      sudo apt-get install -y $1
5  }
6
7  function inst2 () {
8      git clone https://github.com/htrgouvea/nipe && cd nipe
9      sudo cpan install Try::Tiny Config::Simple JSON
10     sudo perl nipe.pl install
11 }
12
13 #find apps - "whois" "curl" "ssh" "sshpass" "nmap"
14
15 declare -a arr=("whois" "curl" "ssh" "sshpass" "nmap")
16
17 for app in "${arr[@]}"
18 do
19     if ! command -v $app &> /dev/null
20     then
21         echo "$app could not be found"
22         inst $app
23     fi
24 done
25
```

```
$ sudo bash xmnrproject.sh
[sudo] password for kali:
whois could not be found
inst geoip-bin
fi
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblinear4 libnetaddr-ip-perl lua-lpeg nmap-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  whois
0 upgraded, 1 newly installed, 0 to remove and 889 not upgraded.
Need to get 0 B/81.1 kB of archives.
After this operation, 373 kB of additional disk space will be used.
Selecting previously unselected package whois.
(Reading database ... 233240 files and directories currently installed.)
Preparing to unpack .../whois_5.5.10_amd64.deb ...
Unpacking whois (5.5.10) ...
Setting up whois (5.5.10) ...
Processing triggers for kali-menu (2021.2.3) ...and directories currently installed.)
Processing triggers for man-db (2.9.4-2) ...
```

```

curl could not be found
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblinear4 libnetaddr-ip-perl lua-lpeg nmap-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 889 not upgraded.
Need to get 0 B/267 kB of archives.
After this operation, 437 kB of additional disk space will be used.
Selecting previously unselected package curl.
(Reading database ... 233263 files and directories currently installed.)
Preparing to unpack .../curl_7.74.0-1.3+b1_amd64.deb ...
Unpacking curl (7.74.0-1.3+b1) ...
Setting up curl (7.74.0-1.3+b1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...

```

```

sshpass could not be found
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblinear4 libnetaddr-ip-perl lua-lpeg nmap-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sshpass
0 upgraded, 1 newly installed, 0 to remove and 889 not upgraded.
Need to get 0 B/13.0 kB of archives.
After this operation, 38.9 kB of additional disk space will be used.
Selecting previously unselected package sshpass.
(Reading database ... 233272 files and directories currently installed.)
Preparing to unpack .../sshpass_1.09-1+b1_amd64.deb ...
Unpacking sshpass (1.09-1+b1) ...
Setting up sshpass (1.09-1+b1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...

```

```

nmap could not be found
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libnetaddr-ip-perl
Use 'sudo apt autoremove' to remove it.
Suggested packages:
  ncat ndiff zenmap
The following NEW packages will be installed:
  nmap
0 upgraded, 1 newly installed, 0 to remove and 889 not upgraded.
Need to get 0 B/2,007 kB of archives.
After this operation, 5,052 kB of additional disk space will be used.
Selecting previously unselected package nmap.
(Reading database ... 233279 files and directories currently installed.)
Preparing to unpack .../nmap_7.91+dfsg1-1kali1_amd64.deb ...
Unpacking nmap (7.91+dfsg1-1kali1) ...
Setting up nmap (7.91+dfsg1-1kali1) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...

```

#Part 2 – Apps: geoiplookup

Name of app and installation name is different, therefore cannot be categorized with Part 1

```
25
26 #find apps - "geoiplookup"
27
28 declare -a arr=("geoiplookup")
29
30 for app in "${arr[@]}"
31 do
32     if ! command -v $app &> /dev/null
33     then
34         echo "$app could not be found"
35         inst geoip-bin
36     fi
37 done
```

```
geoiplookup could not be found
Reading package lists... Done
Building dependency tree... Done 233307 files and directories currently i
Reading state information... Done 1.3+b1) ...
The following NEW packages will be installed:
  geoip-bin
0 upgraded, 1 newly installed, 0 to remove and 889 not upgraded.
Need to get 0 B/84.7 kB of archives.
After this operation, 309 kB of additional disk space will be used.
Selecting previously unselected package geoip-bin.
(Reading database ... 233307 files and directories currently installed.)
Preparing to unpack .../geoip-bin_1.6.12-7_amd64.deb ...
Unpacking geoip-bin (1.6.12-7) ...
Setting up geoip-bin (1.6.12-7) ...
Processing triggers for kali-menu (2021.2.3) ...
Processing triggers for man-db (2.9.4-2) ...
```

#Part 3 – Apps: nipe

Nipe is a github repository that is not the common apps that can be downloaded with apt-get installed. Therefore a separate checker and download script is required.

```
39 #find apps - "nipe.pl"
40
41 declare -a arr=("nipe.pl")
42
43 for app in "${arr[@]}"
44 do
45     if $(find ./ -name nipe.pl | awk -F/ '{print $NF}') && /dev/null
46     then
47         echo "$app could not be found"
48         inst2
49     fi
50 done
```

```
nipe.pl could not be found
Cloning into 'nipe' ...
remote: Enumerating objects: 1558, done.
remote: Counting objects: 100% (29/29), done.
remote: Compressing objects: 100% (21/21), done.
remote: Total 1558 (delta 9), reused 22 (delta 6), pack-reused 1529
Receiving objects: 100% (1558/1558), 240.19 KiB | 10.44 MiB/s, done.
Resolving deltas: 100% (822/822), done.
Loading internal logger. Log::Log4perl recommended for better logging
Reading '/root/.cpan/Metadata'
  Database was generated on Wed, 13 Oct 2021 15:17:03 GMT
Fetching with LWP:
http://www.cpan.org/authors/01mailrc.txt.gz
Reading '/root/.cpan/sources/authors/01mailrc.txt.gz'
.....DONE
Fetching with LWP:
http://www.cpan.org/modules/02packages.details.txt.gz
Reading '/root/.cpan/sources/modules/02packages.details.txt.gz'
  Database was generated on Sun, 24 Oct 2021 10:41:03 GMT
.....
New CPAN.pm version (v2.28) available.
[Currently running version is v2.27]
You might want to try
  install CPAN
  reload cpan
to both upgrade CPAN.pm and run the new version without leaving
the current session.
.....DONE
Fetching with LWP:
http://www.cpan.org/modules/03modlist.data.gz
Reading '/root/.cpan/sources/modules/03modlist.data.gz'
DONE
Writing /root/.cpan/Metadata
Try::Tiny is up to date (0.30).
Config::Simple is up to date (4.58).
JSON is up to date (4.03).
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.7-1).
tor is already the newest version (0.4.5.10-1+b1).
0 upgraded, 0 newly installed, 0 to remove and 889 not upgraded.
```

#To check if connection is anonymous

Note: 'restart' is used instead of 'start' to ensure that nipe runs even if not stopped properly.

```
52 function anon() {
53     cd "nipe"
54
55     sudo perl nipe.pl restart
56     (curl ifconfig.me; echo) | tee >> ip.lst
57
58     for x in $(cat ip.lst | tail -n 1)
59     do
60         geotracklookup $x | awk '{print $4}' | cut -c 1-2 >> cty
61     done
62
63     for x in $(cat cty | tail -n 1)
64     do
65         if [ $x = SG ]
66         then
67             echo "Connection from SG, origin country"
68         else
69             echo "Connection from $x, not origin country"
70         fi
71     done
72 }
73
74 anon
```

```
(kali㉿kali)-[~/Desktop/XM]
$ sudo bash xmnproject.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload   Total   Spent    Left     Speed
100    15  100    15    0     0    10      0  0:00:01  0:00:01 --:--:--   10
Connection from SE, not origin country
```

#Connect to a vps + scans

To set up a VPS using Digital Ocean and connecting to it via SSH

We start by setting up a root user with ssh keys, followed by adding users with sudo privileges that can access our server with password authentications

#step 1: set up a public key

ssh-keygen -t ed25519 -C "email@address.com"

```
(kali㉿kali)-[~/Desktop/XM]
$ ssh-keygen -t ed25519 -C " "
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/kali/.ssh/id_ed25519): y
Enter passphrase (empty for no passphrase): remote ip
Enter same passphrase again: #1
Your identification has been saved in y
Your public key has been saved in y.pub
The key fingerprint is:
SHA256:
The key's randomart image is:
+--[ED25519 256]--+
|+=B0.+Eo. .      |
|=.B=++= =        |
|O+.O= =. =       |
|. *..=.+ ++      |
|+.+ .O So        |
|o.               |
|o                |
+---[SHA256]-----+
(kali㉿kali)-[~/Desktop/XM]
$ ls
y
y.pub
(kali㉿kali)-[~/Desktop/XM]
$ cat y.pub
ssh-ed25519
```

#step 2: add ssh public key to server

cloud.digitalocean.com/droplets/new?fleetU[REDACTED] Incognito (3)

does this mean?

Select additional options ?

☐ IPv6 ☐ User data ☐ Monitoring

Authentication ?

☒ **SSH keys**
A more secure authentication method

☐ **Password**
Create a root password to access your Droplet



Choose your SSH keys


ssh-ed25519


[REDACTED]

☐ Select all ☐ user ☐ kali ☒ y ☐ ROG_XM_

New SSH Key

 **Ubuntu-xm**
In  XM / 1 GB Memory / 1 Intel vCPU / 25 GB Disk / SGPI - Ubuntu 20.04 (LTS) x64



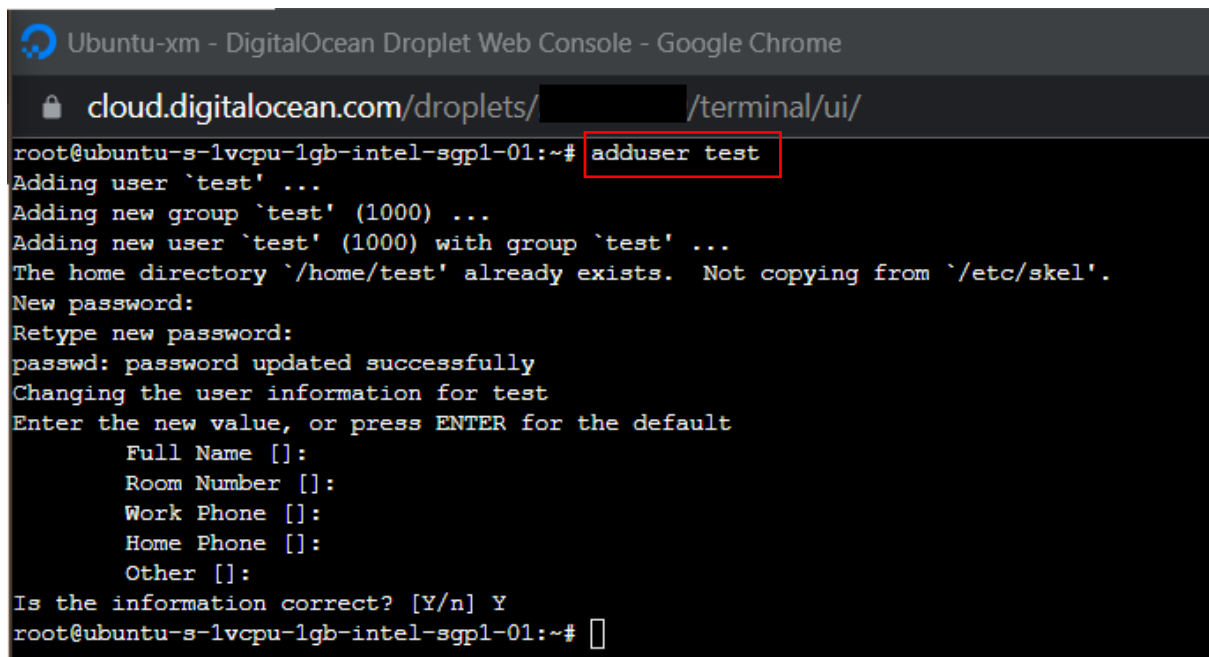
ipv4: 139.59.229.99 ipv6: Enable now Private IP: 10.104.0.3 Floating IP: Enable now Console:  ?

Graphs
Access
Power
Volumes
Resize
Networking
Backups
Snapshots

Droplet Console

Use the Droplet Console for native-like terminal access to your Droplet from your browser. Here is [the list of supported OSes](#) for the new console.

#step 3: access server using root, create new user



The screenshot shows a web browser window with the address bar displaying 'cloud.digitalocean.com/droplets/[redacted]/terminal/ui/'. The browser tab is titled 'Ubuntu-xm - DigitalOcean Droplet Web Console - Google Chrome'. The terminal window shows a root user at the prompt 'root@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~#'. The command 'adduser test' has been entered and is highlighted with a red box. The terminal output shows the process of adding a new user 'test' with a group 'test' (1000). It indicates that the home directory '/home/test' already exists and that the password has been successfully updated. It then prompts for user information (Full Name, Room Number, Work Phone, Home Phone, Other) and asks if the information is correct. The user has responded with 'Y'.

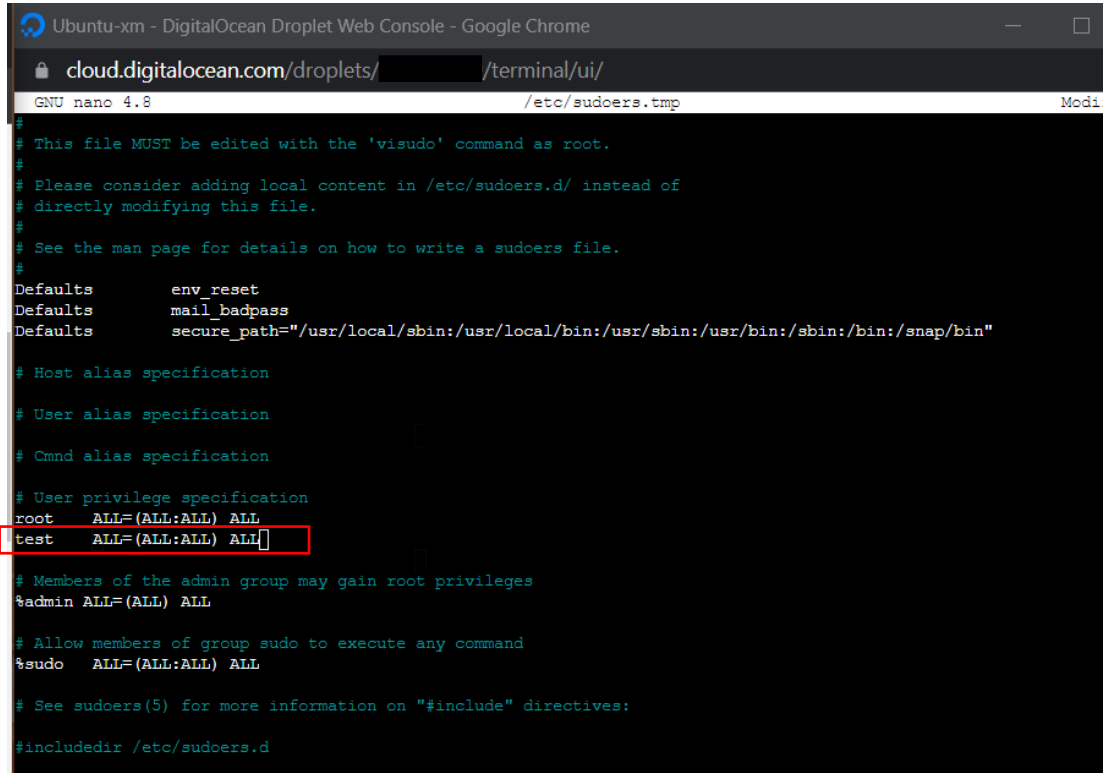
```
root@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~# adduser test
Adding user `test' ...
Adding new group `test' (1000) ...
Adding new user `test' (1000) with group `test' ...
The home directory `/home/test' already exists. Not copying from `/etc/skel'.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
root@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~#
```

Username: test

Password: 1

#step 4: give new user “test” sudo privileges

```
root@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~# usermod -aG sudo test
root@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~# visudo
```



The screenshot shows a web browser window titled "Ubuntu-xm - DigitalOcean Droplet Web Console - Google Chrome" displaying a terminal session. The terminal shows the command `visudo` being executed, which opens the `/etc/sudoers.tmp` file in the `nano` editor. The file content includes default settings, host and user alias specifications, and user privilege specifications. The line `test ALL=(ALL:ALL) ALL` is highlighted with a red box, indicating the new user 'test' is granted full sudo privileges. Other lines include `root ALL=(ALL:ALL) ALL`, `%admin ALL=(ALL) ALL`, and `%sudo ALL=(ALL:ALL) ALL`. The terminal also shows instructions on how to edit the file and where to add local content.

```
GNU nano 4.8 /etc/sudoers.tmp Modif
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
test    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include_dir /etc/sudoers.d
```

#step 5: login to SSH server with new user “test” to configure password access

The screenshot shows the DigitalOcean Droplet console for an Ubuntu-xm droplet. The console is open, showing a terminal window with the following output:

```
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Oct 31 08:06:08 UTC 2021

System load: 0.0          Users logged in: 1
Usage of /: 10.0% of 24.0GB IPv4 address for eth0: 139.59.229.99
Memory usage: 24%        IPv4 address for eth0: 10.15.0.6
Swap usage: 0%           IPv4 address for eth1: 10.104.0.3
Processes: 109

72 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

*** System restart required ***
To run a command as administrator (user "root"), use "sudo -i" command.
See "man sudo_root" for details.

test@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~$
```

```
test@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~$ sudo vim /etc/ssh/sshd_config
[sudo] password for test:
```

The screenshot shows the contents of the `/etc/ssh/sshd_config` file in a terminal window. The file is being edited with `vim`, and the current line is `PasswordAuthentication yes`, which is highlighted with a red box. The terminal output shows the following configuration:

```
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

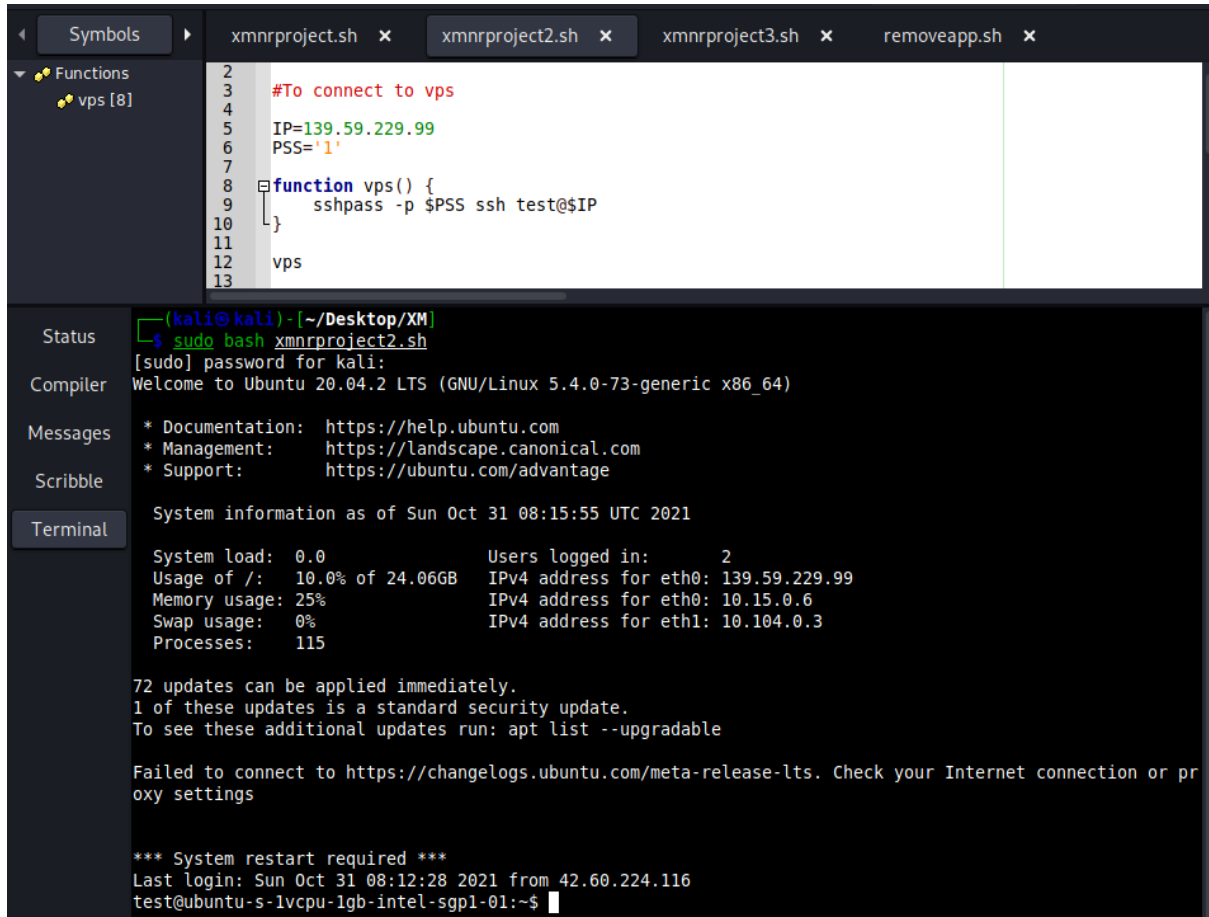
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
```

```
test@ubuntu-s-1vcpu-1gb-intel-sgpl-01:~$ sudo systemctl restart ssh
```

Test if script allows us to connect with user 'test' to SSH using password



The screenshot shows a code editor with four tabs: `xmnrproject.sh`, `xmnrproject2.sh`, `xmnrproject3.sh`, and `removeapp.sh`. The `xmnrproject2.sh` tab is active, displaying a script with the following content:

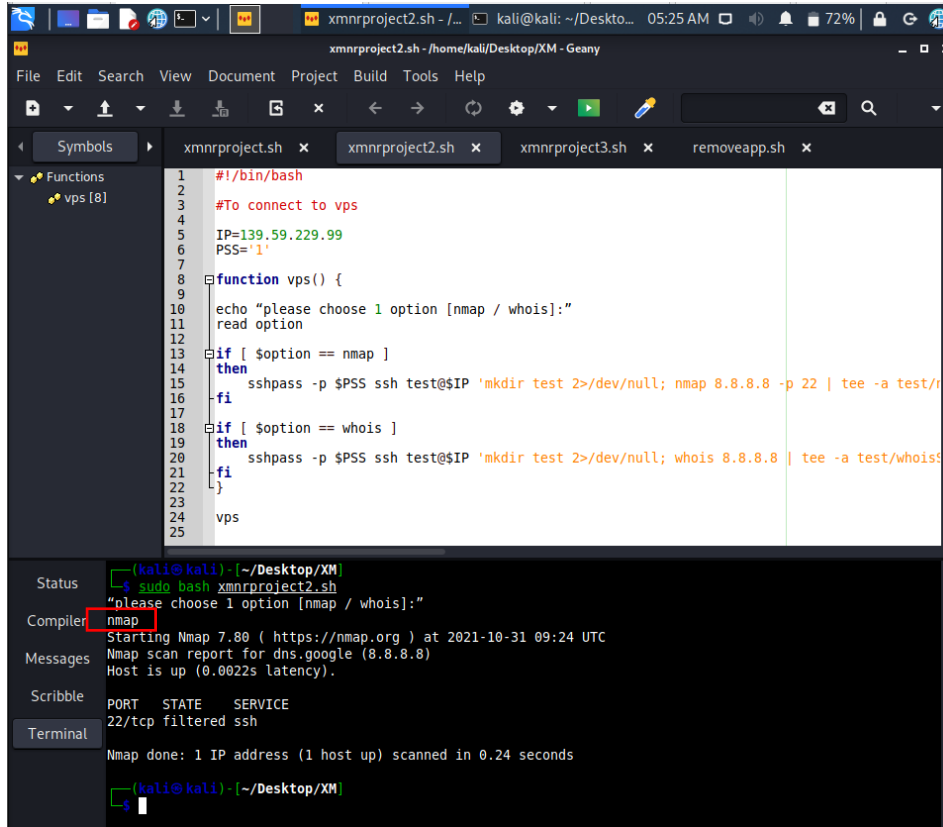
```
2  
3 #To connect to vps  
4  
5 IP=139.59.229.99  
6 PSS='1'  
7  
8 function vps() {  
9     sshpass -p $PSS ssh test@$IP  
10 }  
11  
12 vps  
13
```

Below the code editor is a terminal window. The terminal shows the command `sudo bash xmnrproject2.sh` being executed. The output includes the Ubuntu login prompt, system information, and a message about updates.

```
(kali@kali)-[~/Desktop/XM]  
$ sudo bash xmnrproject2.sh  
[sudo] password for kali:  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-73-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Sun Oct 31 08:15:55 UTC 2021  
  
System load:  0.0           Users logged in:      2  
Usage of /:   10.0% of 24.06GB  IPv4 address for eth0: 139.59.229.99  
Memory usage: 25%           IPv4 address for eth0: 10.15.0.6  
Swap usage:   0%            IPv4 address for eth1: 10.104.0.3  
Processes:    115  
  
72 updates can be applied immediately.  
1 of these updates is a standard security update.  
To see these additional updates run: apt list --upgradable  
  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
*** System restart required ***  
Last login: Sun Oct 31 08:12:28 2021 from 42.60.224.116  
test@ubuntu-s-1vcpu-1gb-intel-sgp1-01:~$
```

Note: Make sure that nmap and whois is installed onto VPS

#run nmap/whois scans on VPS



```
1 #!/bin/bash
2
3 #To connect to vps
4 IP=139.59.229.99
5 PSS='1'
6
7 function vps() {
8
9     echo "please choose 1 option [nmap / whois]:"
10    read option
11
12    if [ $option == nmap ]
13    then
14        sshpass -p $PSS ssh test@$IP 'mkdir test 2>/dev/null; nmap 8.8.8.8 -p 22 | tee -a test/nmap.txt'
15    fi
16
17    if [ $option == whois ]
18    then
19        sshpass -p $PSS ssh test@$IP 'mkdir test 2>/dev/null; whois 8.8.8.8 | tee -a test/whois.txt'
20    fi
21
22 }
23
24 vps
25
```

Status (kali@kali) - [~/Desktop/XM]
\$ sudo bash xmnrproject2.sh
"please choose 1 option [nmap / whois]:"

Compiler nmap
Starting Nmap 7.80 (https://nmap.org) at 2021-10-31 09:24 UTC

Messages Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0022s latency).

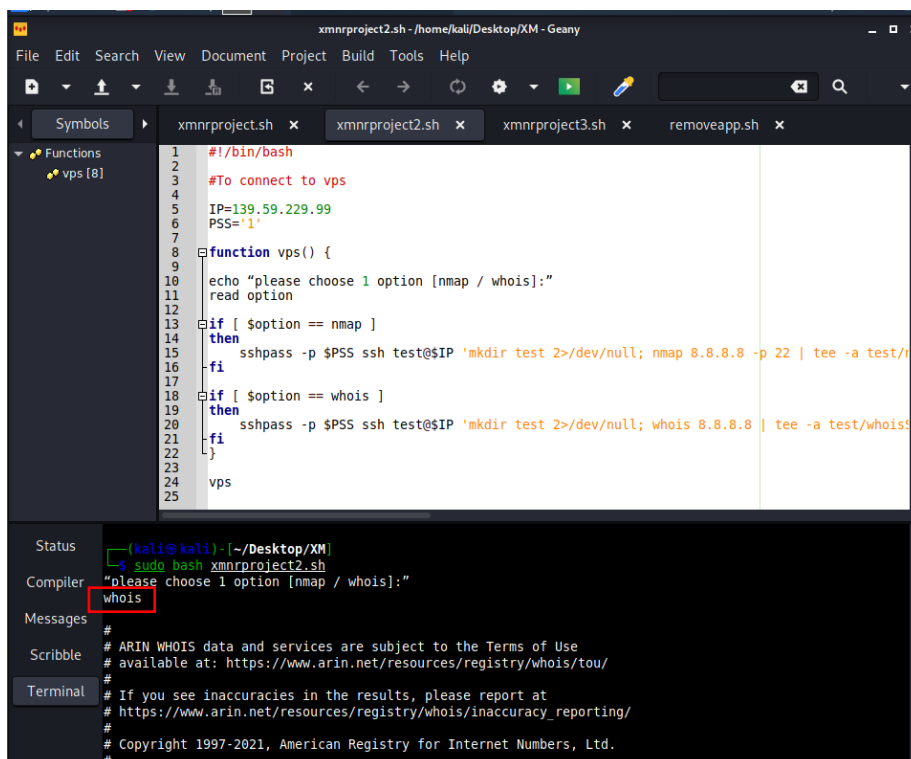
Scribble

Terminal

PORT	STATE	SERVICE
22/tcp	filtered	ssh

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

(kali@kali) - [~/Desktop/XM]
\$



```
1 #!/bin/bash
2
3 #To connect to vps
4 IP=139.59.229.99
5 PSS='1'
6
7 function vps() {
8
9     echo "please choose 1 option [nmap / whois]:"
10    read option
11
12    if [ $option == nmap ]
13    then
14        sshpass -p $PSS ssh test@$IP 'mkdir test 2>/dev/null; nmap 8.8.8.8 -p 22 | tee -a test/nmap.txt'
15    fi
16
17    if [ $option == whois ]
18    then
19        sshpass -p $PSS ssh test@$IP 'mkdir test 2>/dev/null; whois 8.8.8.8 | tee -a test/whois.txt'
20    fi
21
22 }
23
24 vps
25
```

Status (kali@kali) - [~/Desktop/XM]
\$ sudo bash xmnrproject2.sh
"please choose 1 option [nmap / whois]:"

Compiler whois

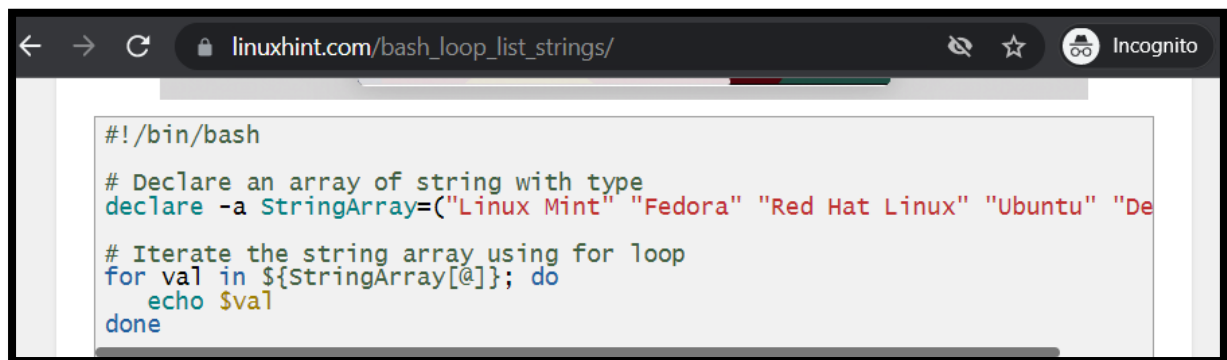
Messages

Scribble

Terminal

```
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#
```

Credits

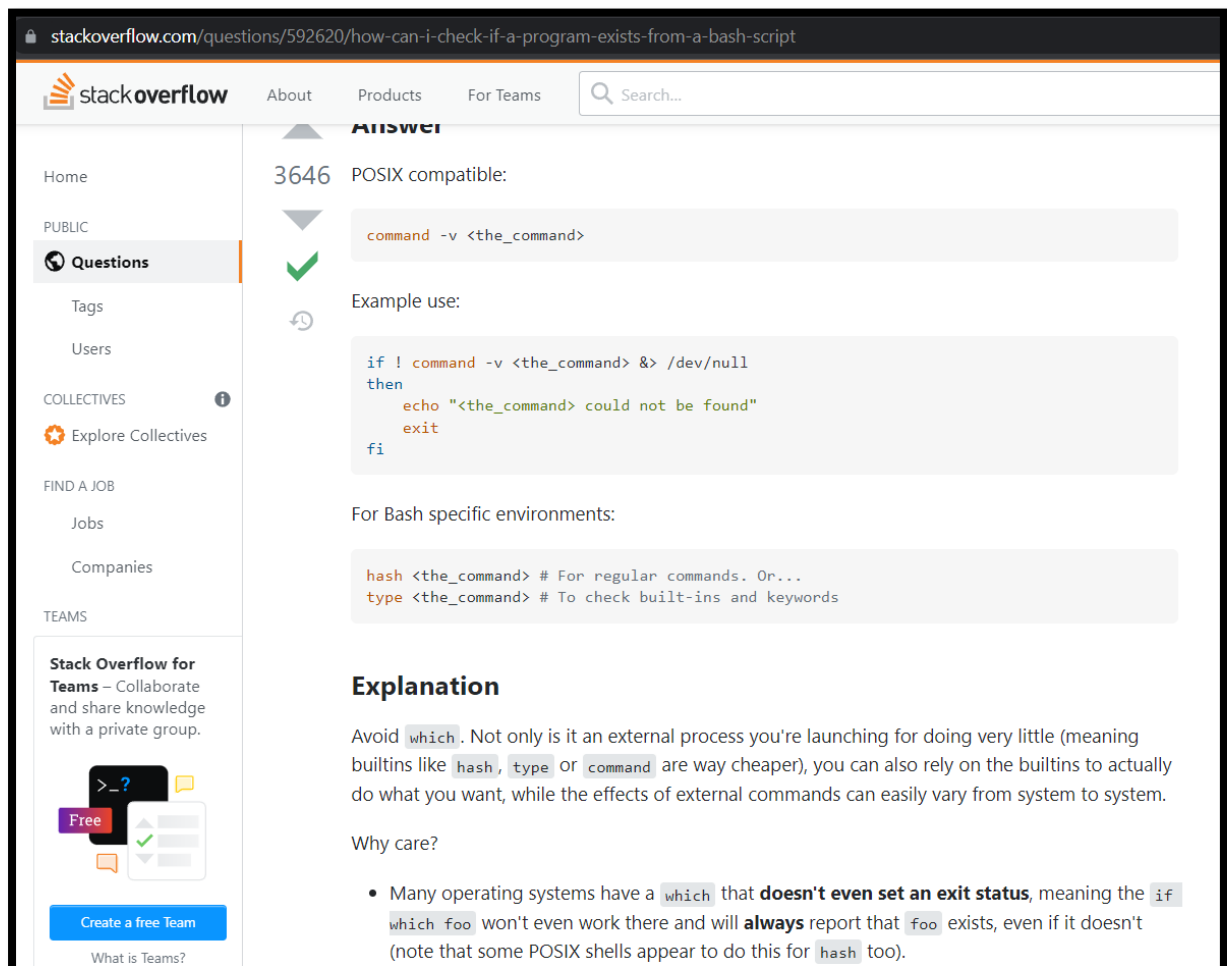


A screenshot of a web browser window showing a bash script on the website linuxhint.com. The browser's address bar displays the URL 'linuxhint.com/bash_loop_list_strings/'. The script is as follows:

```
#!/bin/bash

# Declare an array of string with type
declare -a StringArray=("Linux Mint" "Fedora" "Red Hat Linux" "Ubuntu" "Debian")

# Iterate the string array using for loop
for val in ${StringArray[@]}; do
    echo $val
done
```



A screenshot of a Stack Overflow page. The URL in the address bar is 'stackoverflow.com/questions/592620/how-can-i-check-if-a-program-exists-from-a-bash-script'. The page shows a question with 3646 votes and an answer marked with a green checkmark. The answer provides the following information:

Answer

3646 POSIX compatible:

```
command -v <the_command>
```

Example use:

```
if ! command -v <the_command> && /dev/null
then
    echo "<the_command> could not be found"
    exit
fi
```

For Bash specific environments:

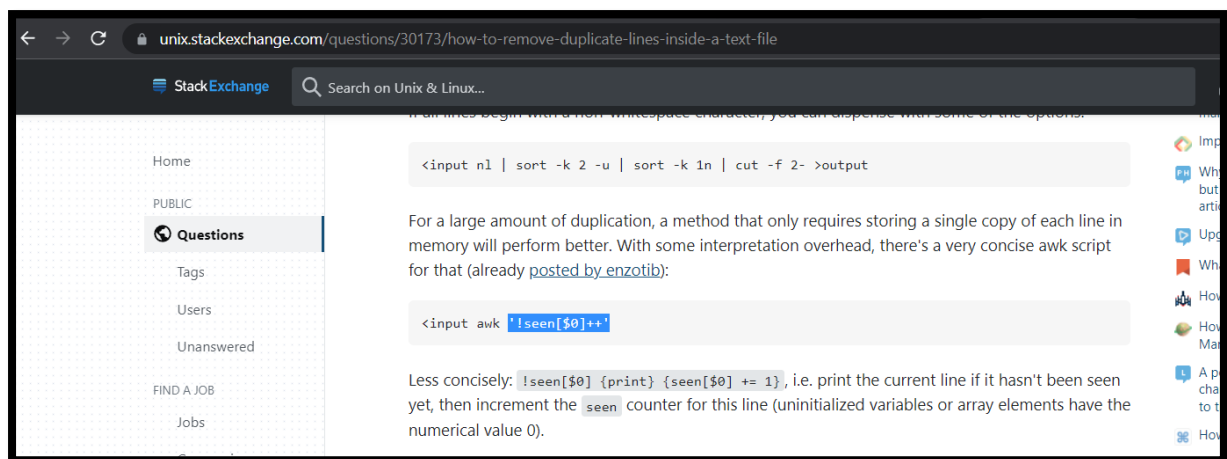
```
hash <the_command> # For regular commands. Or...
type <the_command> # To check built-ins and keywords
```

Explanation

Avoid `which`. Not only is it an external process you're launching for doing very little (meaning builtins like `hash`, `type` or `command` are way cheaper), you can also rely on the builtins to actually do what you want, while the effects of external commands can easily vary from system to system.

Why care?

- Many operating systems have a `which` that **doesn't even set an exit status**, meaning the `if which foo` won't even work there and will **always** report that `foo` exists, even if it doesn't (note that some POSIX shells appear to do this for `hash` too).



stackoverflow.com/questions/12849584/automatically-add-newline-at-end-of-curl-response-body

stackoverflow About Products For Teams Search...

Home
PUBLIC
Questions
Tags
Users
COLLECTIVES
Explore Collectives
FIND A JOB
Jobs

120

Use this:

```
curl jsonip.com; echo
```

If you need *grouping* to feed a *pipe* :

```
{ curl jsonip.com; echo; } | tee new_file_with_newline
```

OUTPUT

```
{"ip":"x.x.x.x","about":"/about"}
```

← → ↻ digitalocean.com/community/tutorials/how-to-add-and-... 🔍 🗑️ ☆ Incognito

Adding a User

If you are signed in as the **root** user, you can create a new user at any time by typing:

```
# adduser newuser
```

If you are signed in as a non-root user who has been given **sudo** privileges, you can add a new user by typing:

```
$ sudo adduser newuser
```


← → ↻ digitalocean.com/community/tutorials/how-to-add-and-... 🔍 🗑️ ☆ Incognito (3)

Granting a User Sudo Privileges

If your new user should have the ability to execute commands with root (administrative) privileges, you will need to give the new user access to `sudo`. Let's examine two approaches to this problem: adding the user to a pre-defined **sudo user group**, and specifying privileges on a per-user basis in `sudo`'s configuration.

Adding the New User to the Sudo Group

By default, `sudo` on Ubuntu 18.04 systems is configured to extend full privileges to any user in the **sudo** group.

You can see what groups your new user is in with the `groups` command:

```
$ groups newuser
```

Output

```
newuser : newuser
```

By default, a new user is only in their own group which `adduser` creates along with the user profile. A user and its own group share the same name. In order to add the user to a new group, we can use the `usermod` command:

```
$ usermod -aG sudo newuser
```

The `-aG` option here tells `usermod` to add the user to the listed groups.

← → ↻ digitalocean.com/community/tutorials/how-to-add-and-... 🔍 🗑️ ☆ Incognito (3) ⋮

overwriting the file. This helps to prevent a situation where you misconfigure `sudo` and are prevented from fixing the problem because you have lost `sudo` privileges.

If you are currently signed in as **root**, type:

```
# visudo
```

If you are signed in as a non-root user with `sudo` privileges, type:


```
$ sudo visudo
```


Traditionally, `visudo` opened `/etc/sudoers` in the `vi` editor, which can be confusing for inexperienced users. By default on new Ubuntu installations, `visudo` will instead use `nano`, which provides a more convenient and accessible text editing experience. Use the arrow keys to move the cursor, and search for the line that looks like this:

```
/etc/sudoers
root    ALL=(ALL:ALL) ALL
```

Below this line, add the following highlighted line. Be sure to change `newuser` to the name of the user profile that you would like to grant `sudo` privileges:

```
/etc/sudoers
root    ALL=(ALL:ALL) ALL
newuser ALL=(ALL:ALL) ALL
```

 [sylapaliyev](#) July 12, 2018
0 Same here. Doesn't fallback to password mode for me either.
[Reply](#) [Report](#)

 [toughskin](#) December 14, 2018
3 What you have to do is edit the `/etc/ssh/sshd_config` file and provide **PasswordAuthentication** with a value of **Yes**.

```
$ sudo vim /etc/ssh/sshd_config
```

Find:

```
PasswordAuthentication no
```

```
press i for insert mode
```

Change to:

```
PasswordAuthentication yes
```

Save and Close

```
[escape] :wq
```

Restart Your SSH

```
$ sudo systemctl restart ssh
Some systems make require
$ sudo systemctl restart sshd
```