Challenge 10

Challenge 10 - Linux Administration 201: 101 + Network Integration - 5/21 | Mike Morris

Linux Administration 201: 101 + Network Integration [NG]

Author: Jeff Echlin
Framework Category: Operate and Maintain
Specialty Area: Network Services
Work Role: Network Operations Specialist
Task Description: Integrate new systems into existing network architecture. (T0129)
Scenario

Dedeker Randolph, a new temporary security consultant, requires a workstation. Ms. Randolph started today and does not have access to her Kali Linux workstation, nor is that workstation setup to access the network properly. Company network policy dictates that all devices on the network must have the IP address, gateway, and DNS server statically assigned in it by our IT staff (i.e. you). Company policy also dictates that all systems have a up to date DNS entry in the DNS server. This system will be integrated into the overall network but will not be managed by Active Directory. This is due to the nature of Dedeker's work which is highly sensitive. Thus, her system will be on the network and she will need a local account on her workstation, not our single sign-on solution

Additional Information

More details and objectives about this challenge will be introduced during the challenge meeting, which will start once you begin deploying the challenge.
You will be able to check your progress during this challenge using the check panel within the workspace once the challenge is deployed. The checks within the check panel report on the state of some or all of the required tasks within the challenge.
Once you have completed the requested tasks, you will need to document the methodology you used with as much detail and professionalism as necessary. This should be done on the documentation tab within the workspace once the challenge is deployed. Below the main documentation section be sure to include a tagged list of applications you used to complete the challenge.

NICE Framework KSAA0055.

Ability to operate common network tools (e.g., ping, traceroute, nslookup).A0058.

Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).A0059.

Ability to operate the organization's LAN/WAN pathways.K0011.

Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.K0029.

Knowledge of organization's Local and Wide Area Network connections.K0050.

Knowledge of local area and wide area networking principles and concepts including bandwidth management.K0061.

Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).K0076.

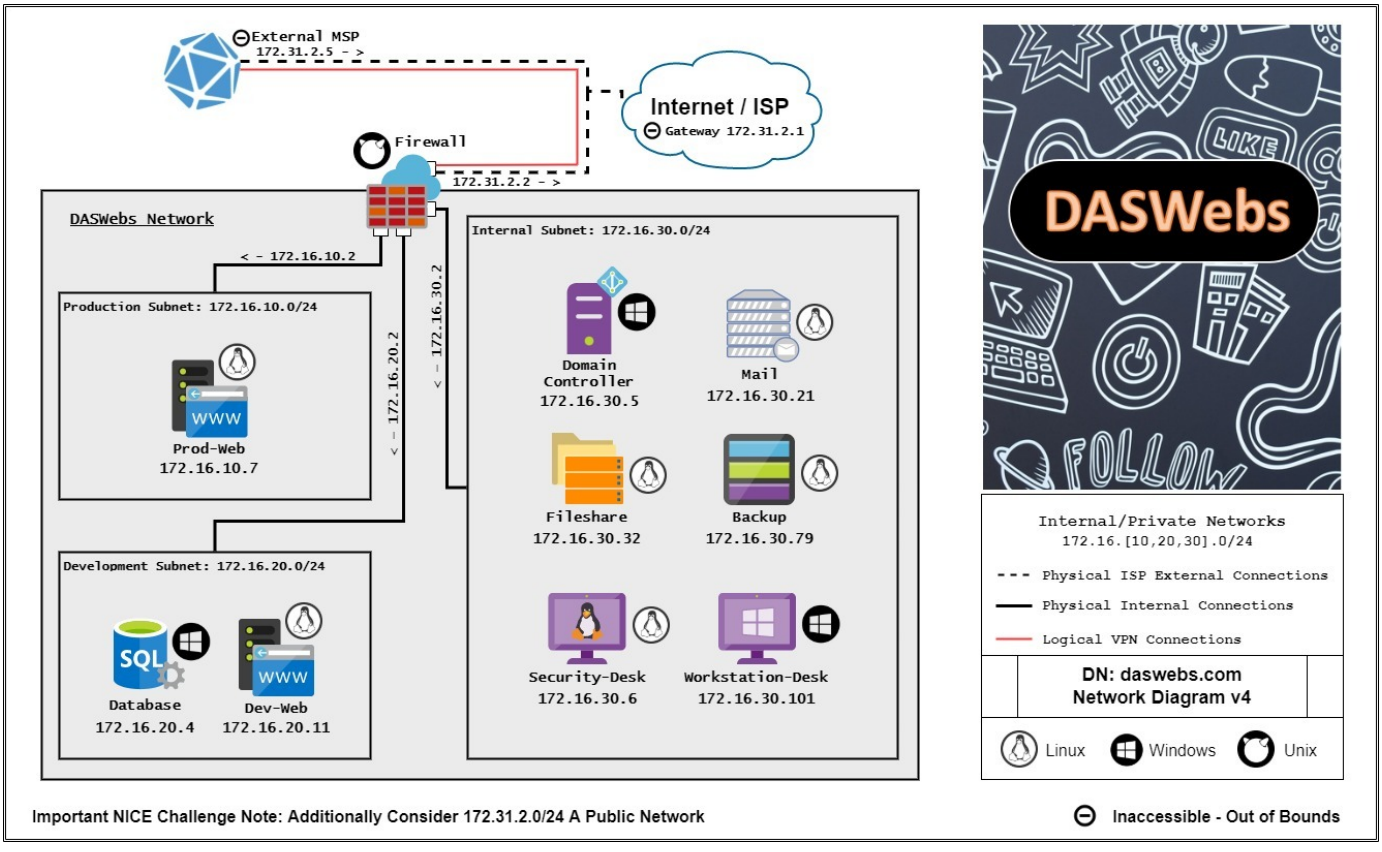
Knowledge of server administration and systems engineering theories, concepts, and methods.K0111.

Knowledge of network tools (e.g., ping, traceroute, nslookup)K0332.

Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.S0162.

Skill in applying various subnet techniques (e.g., CIDR)CAE Knowledge UnitsBasic NetworkingNetwork Technology and ProtocolsOperating Systems Administration

Network Map



Meeting Notes

(@Playerone = myself)

Dedeker Randolph

Hello, I was scheduled to begin work today but I seem to have no access to my workstation. The workstation at my desk does not really seem to be setup at all! Please help!

 Richard LeGrand

Richard LeGrand

I JUST GOT THIS EMAIL FROM THE NEW TEMPORARY SECURITY CONSULTANT. MS. RANDOLPH DOES NOT YET HAVE AN ACCOUNT OR CONNECTED SYSTEM THIS SHOULD HAVE BEEN DONE LONG AGO AND I DON'T HAVE TIME FOR THIS, FIX IT.

 Gary Thatcher

Gary Thatcher

Hello @playerone as you can see things are a bit stressful lately and I have not had time to work on some of these more trivial matters, many other things have taken my attention so I leave the task in your capable hands. @gbates will tell you more.

 Gilly Bates

Gilly Bates

Hi @playerone, I have been assigned to help you along with adding Ms. Randolph, our new temporary security consultant, to our network. There are certain considerations that must be taken into account. Her workstation should be assigned 172.16.30.6 for the IP address; make sure to set the right subnet mask as well. We are a /24 network if you didn't know. Based on the IP address that would mean her workstation is in the Internal subnet and the gateway you set should reflect as such.
The DNS server address also needs to be manually set on her workstation so it can resolve internal and external names. Since our DNS server also happens to be our Domain-Controller, you can find it's IP address on the network map.
Oh! Almost forgot, you will need to add a DNS entry for her workstation in the DNS server on the Domain-Controller. Her workstation FQDN should be SecConsultantKali.daswebs.com and to make it all match up the workstation hostname needs to be set to SecConsultantKali.

 Gilly Bates

Gilly Bates

So.. that takes care of all the network stuff I think. Once you are done with that you need to make sure she has sufficient local machine access so she can get her sensitive work done. Our naming guidelines are always first initial plus last name (all lowercase) for usernames so we will just do that here for Ms. Randolph. Not sure how you usually create users but just make sure her user account also gets a home directory in the usual /home/herusername/ way. Also, since I'm not sure what she is doing, or if we should ask, just give her full sudo access on her workstation. Anything else @drandolph?

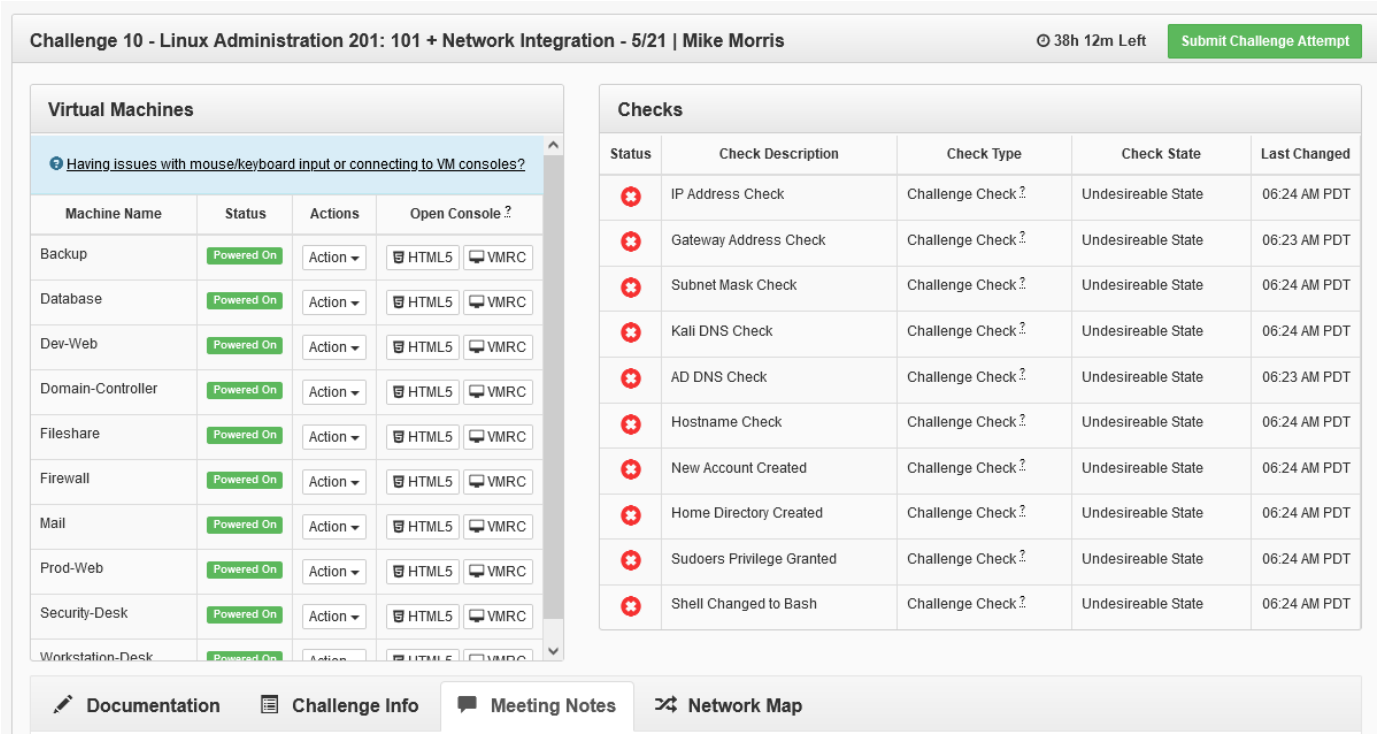
Dedeker Randolph

All that sounds fine to me. As one other thing I'd like @playerone, make sure my default shell is bash. Other than that we are good! Thanks!

(personal notes)

adding Ms. Randolph, our new temporary security consultant, to our network.

- Her workstation should be assigned 172.16.30.6 for the IP address;
- make sure to set the right subnet mask as well. We are a /24 network if you didn't know. (*Based on the IP address that would mean her workstation is in the Internal subnet and the gateway you set should reflect as such.)*
- The DNS server address also needs to be manually set on her workstation so it can resolve internal and external names. *(Since our DNS server also happens to be our Domain-Controller, you can find it's IP address on the network map.)*
  DNS ip= 172.16.30.5
- add a DNS entry for her workstation in the DNS server on the Domain-Controller. Her workstation FQDN should be SecConsultantKali.daswebs.com and to make it all match up the workstation hostname needs to be set to SecConsultantKali.
- make sure she has sufficient local machine access so she can get her sensitive work done.
- *Our naming guidelines are always first initial plus last name (all lowercase) for usernames so we will just do that here for Ms. Randolph. Not sure how you usually create users but just make sure her user account also gets a home directory in the usual /home/herusername/ way*.
- just give her full sudo access on her workstation. Anything else @drandolph?
- Dedeker Randolph
  make sure my default shell is bash. Other than that we are good! Thanks!



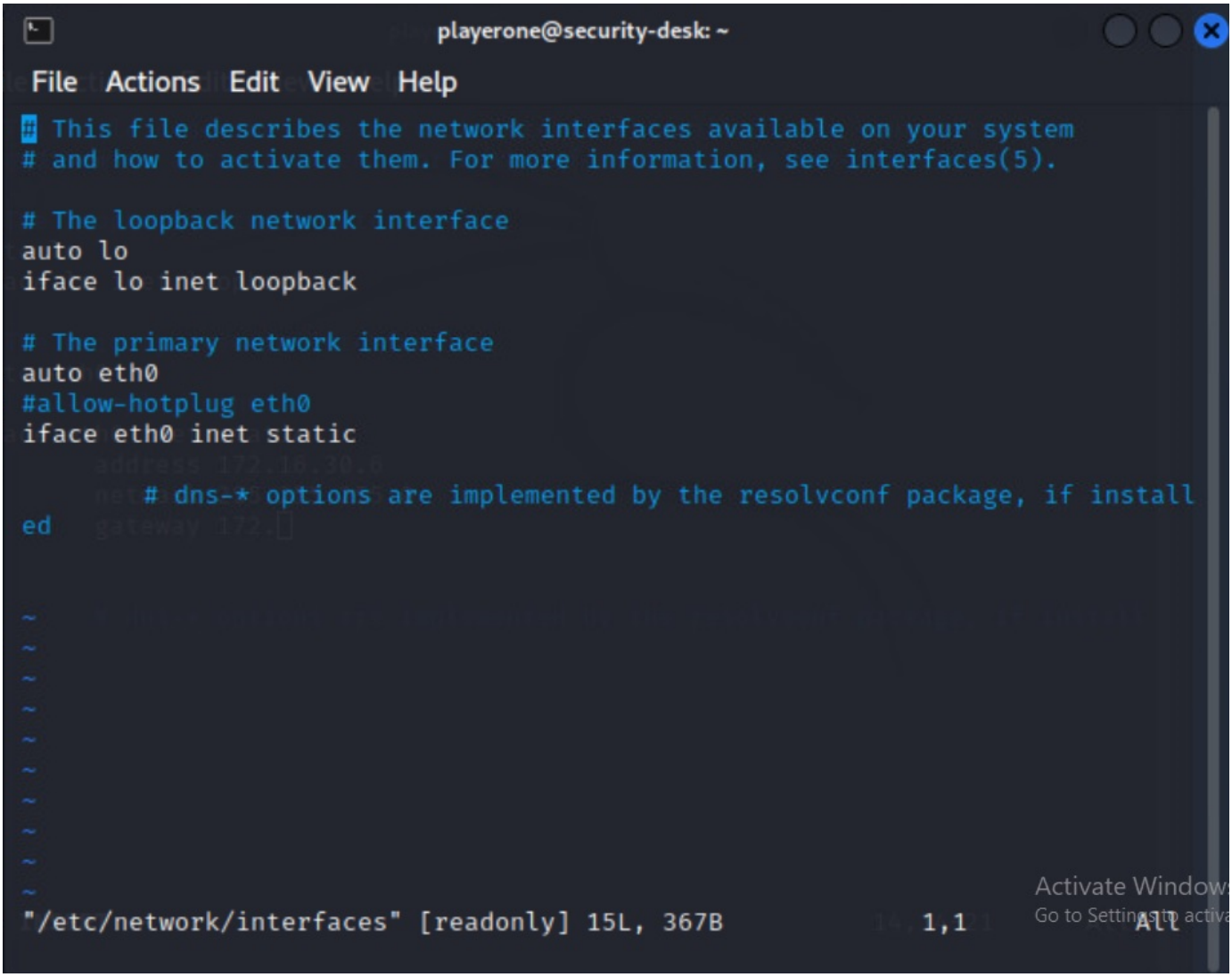
Documentation

Stated that she" NEW TEMPORARY SECURITY CONSULTANT. MS. RANDOLPH DOES NOT YET HAVE AN ACCOUNT OR CONNECTED SYSTEM THIS SHOULD HAVE BEEN DONE LONG AGO AND I DON'T HAVE TIME FOR THIS, FIX IT"

To obtain these checks I:

- [x] ## IP Address Check
- [x] ## Gateway Check
- [x] ## Subnet Mask Check

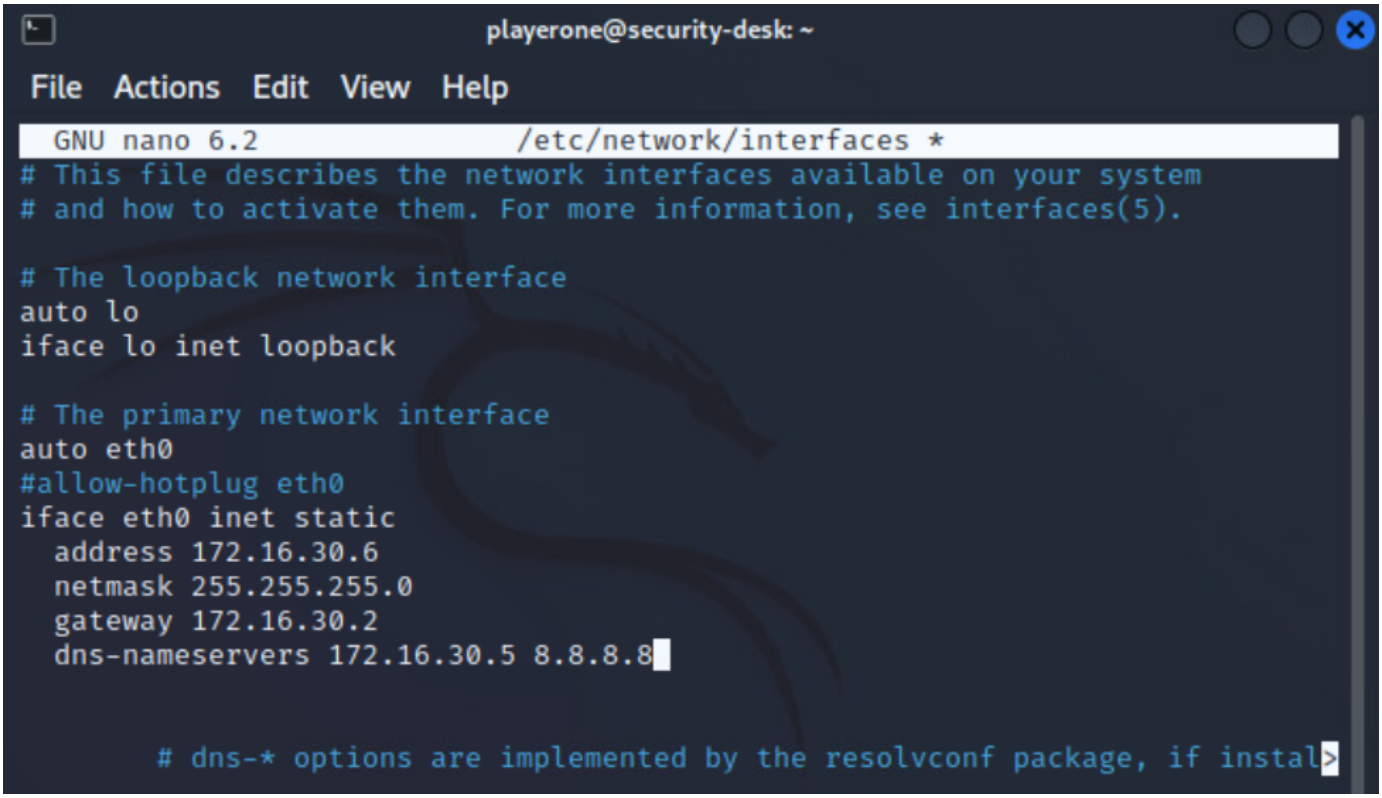
used command `sudo vim /etc/network/interfaces`



I used the Network Map to manual add IP address, netmask, gateway, and DNS servers

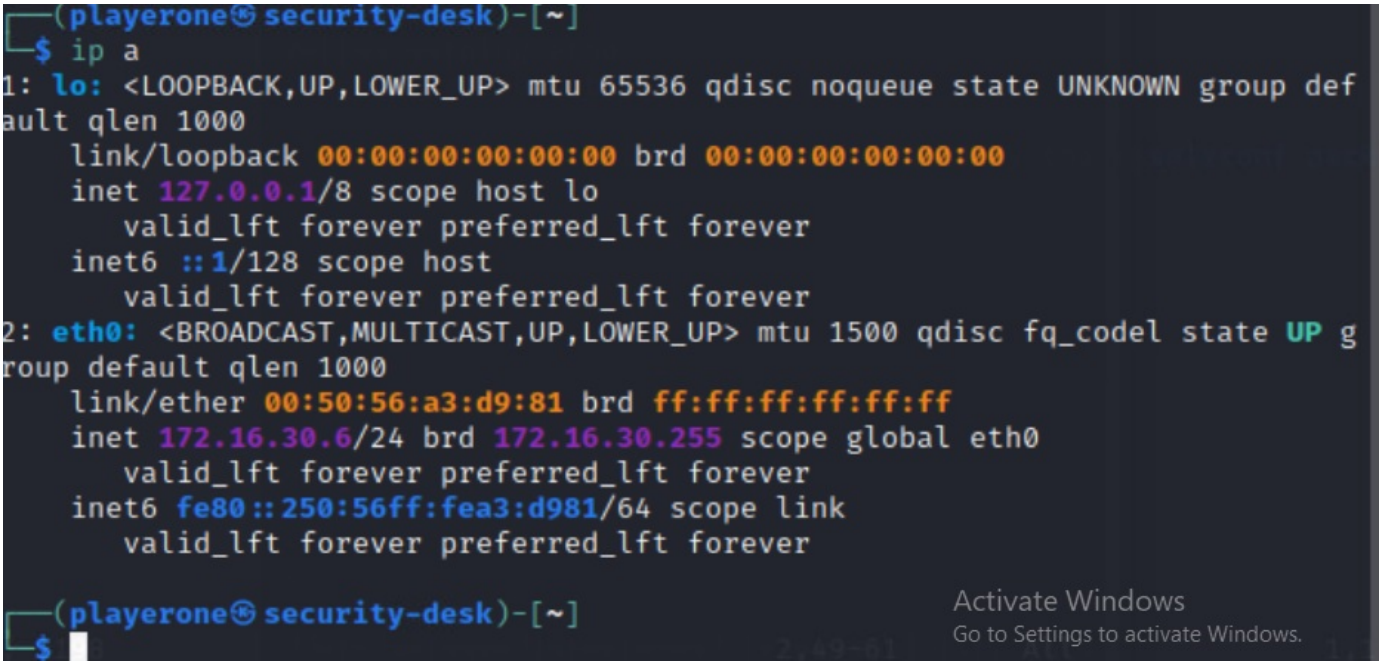
use `i` to enter edit mode

Press esc and command `:wq!` save and quit



To verify I used

`vim /etc/networks/interfaces` everything is correct. Then `ip a` to further verify that it is up.



To restart ip

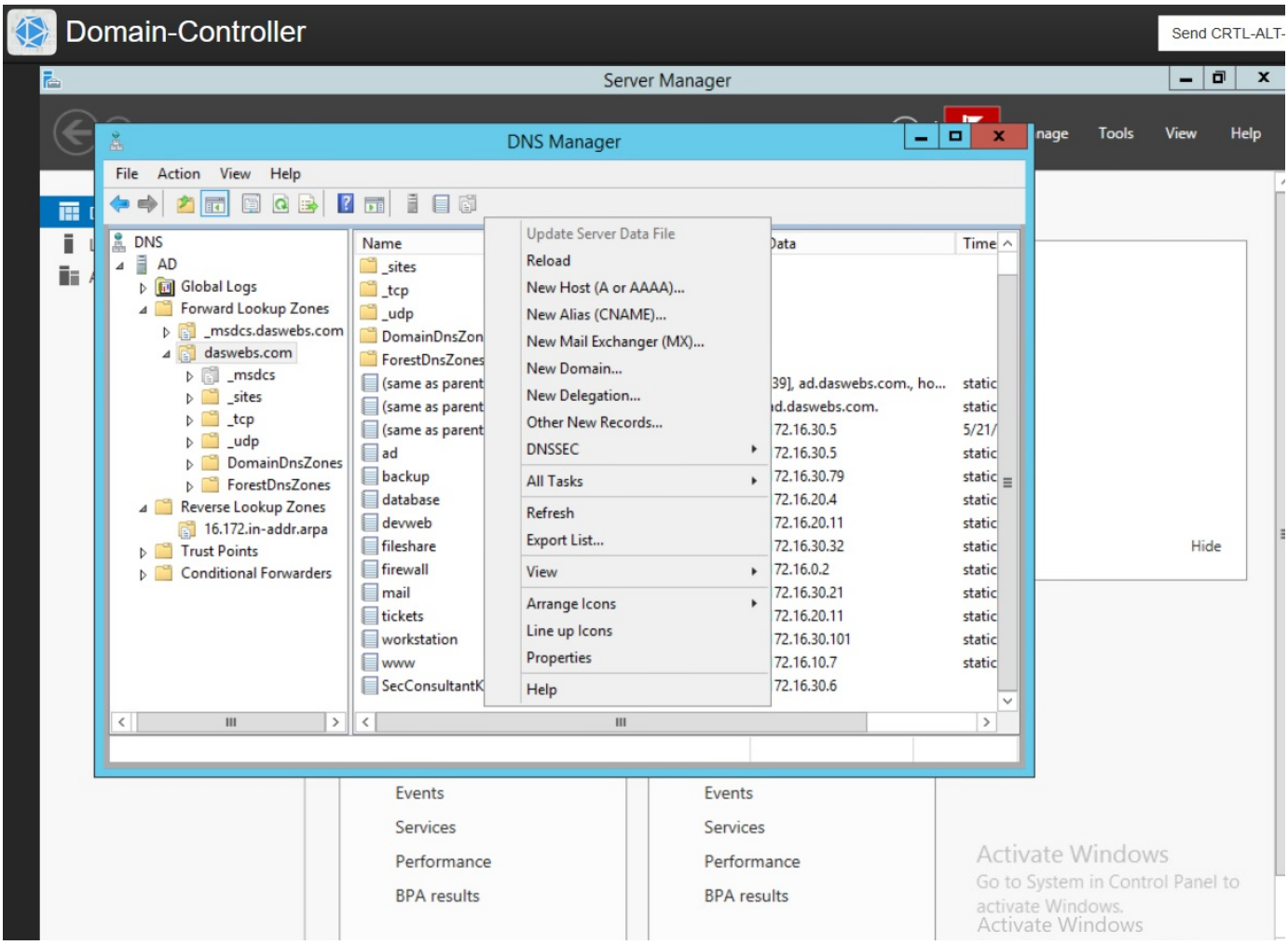
used `sudo up addr flush dev eth0`

`sudo ifup eth0`

- [x] ## AD DNS Check

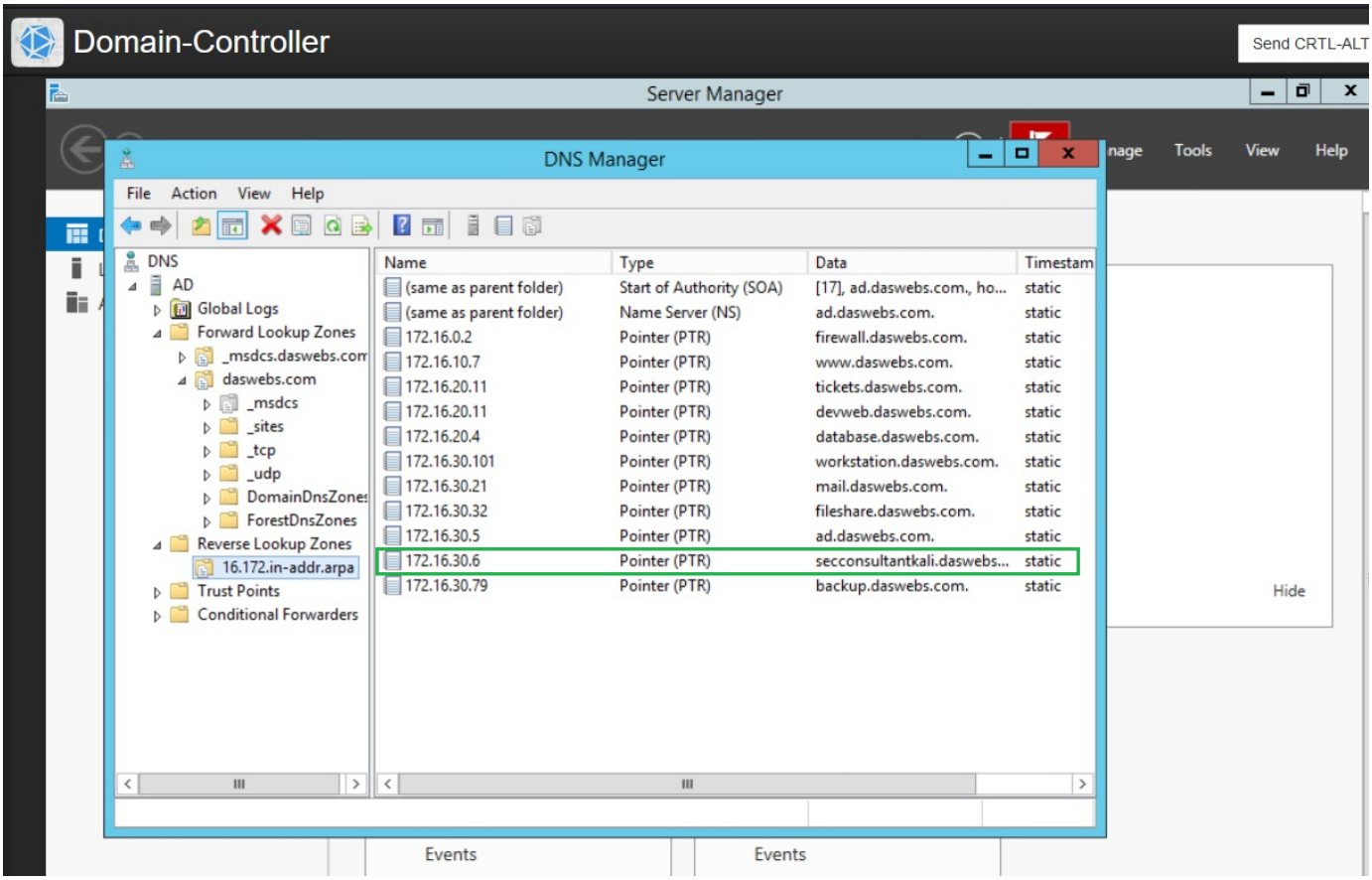
Logged into Domain-Controller and went into Server Manager>Tools>DNS>DNS Manager> Forward LooupZones>daswebs.com

Right clicked on the side in the directory>New Host and filled in the needed information.



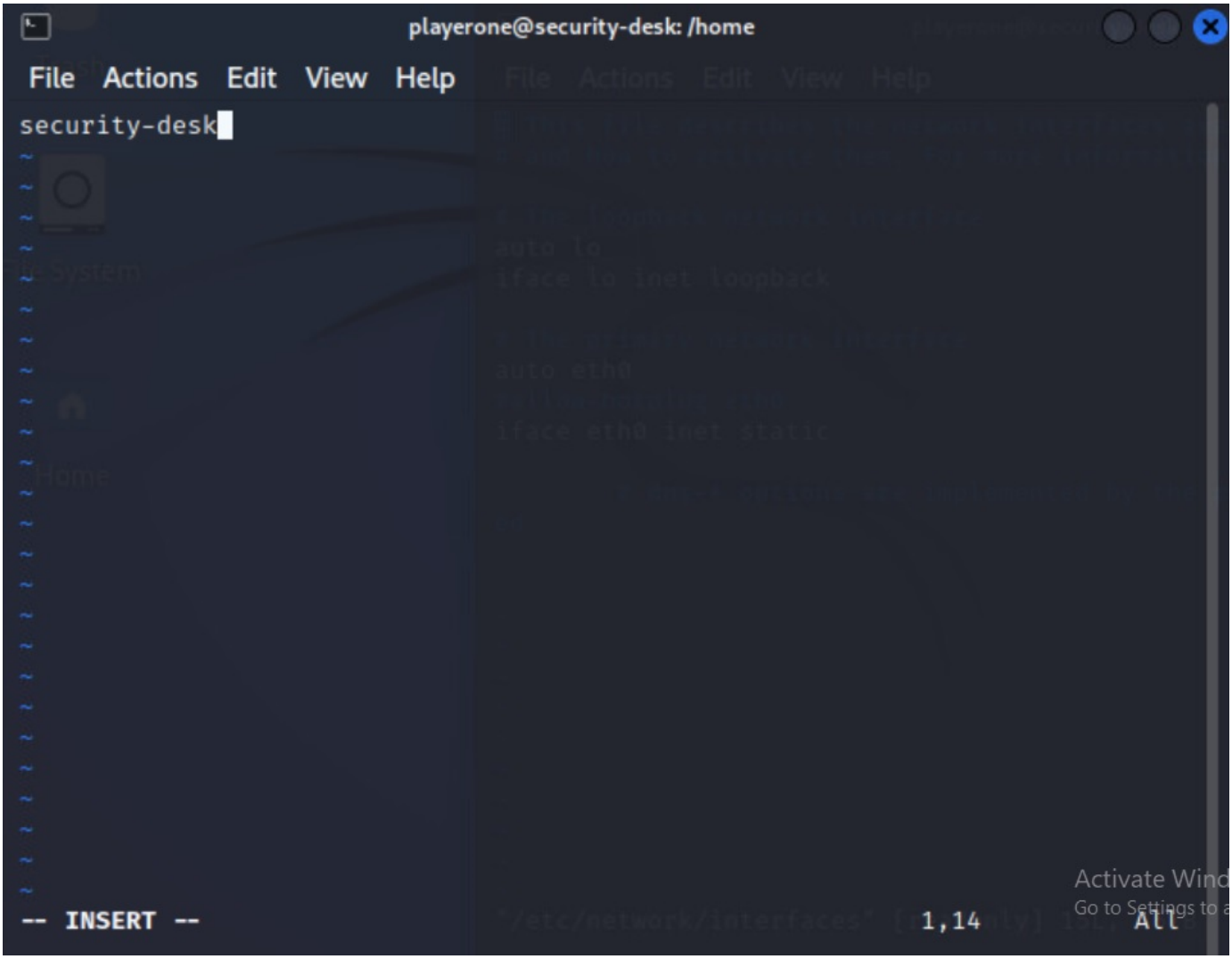
After that I went into Reverse LookupZone>

and added the IP and secconsultantkali.daswebs.com



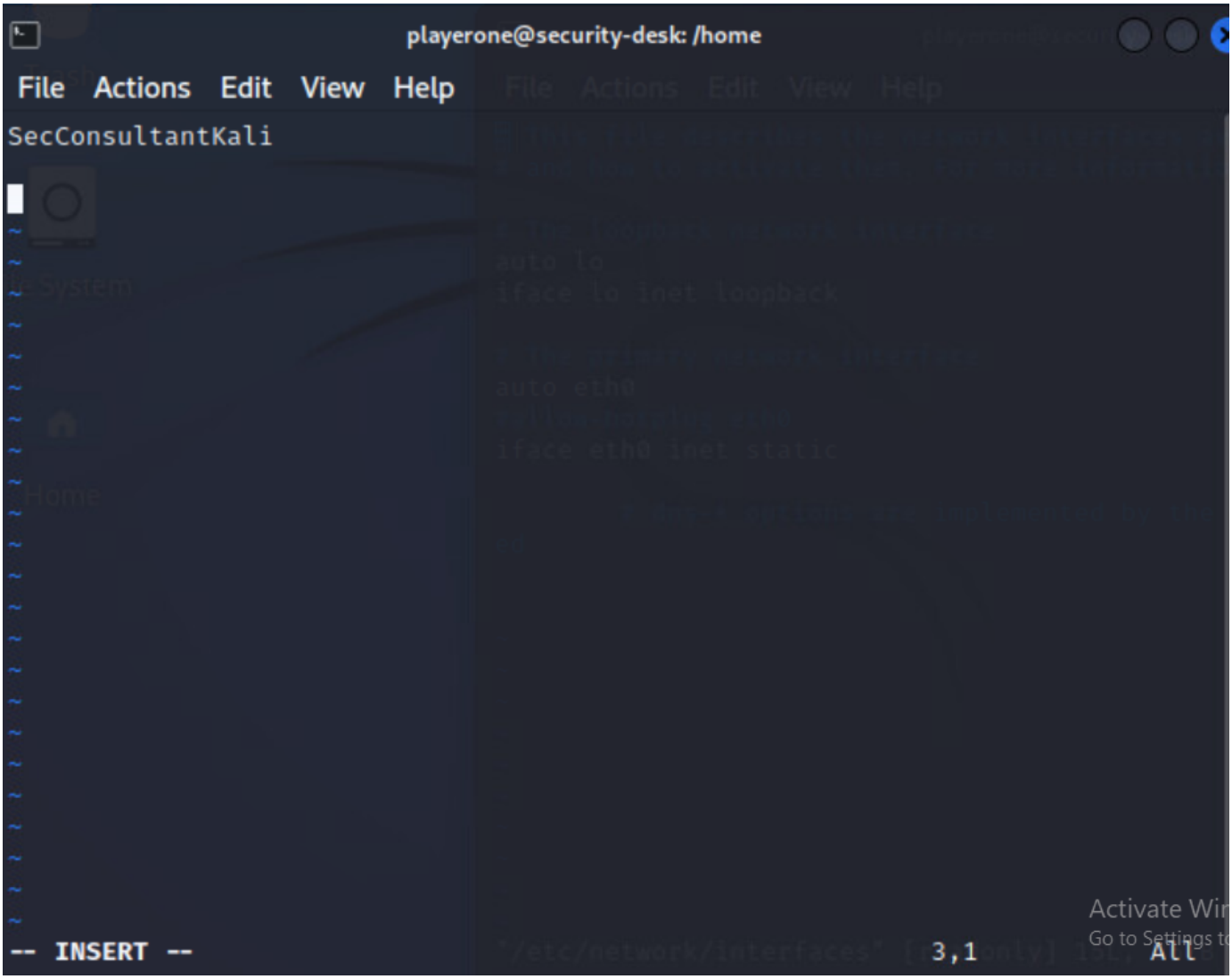
- [x] ## Hostname Check

Using Security-Desk VM, went into the terminal and used `sudo  vim edit /etc/hostname` and /etc/hosts on security-desk and change the name to SecConsultantKali



`i` in vim to edit

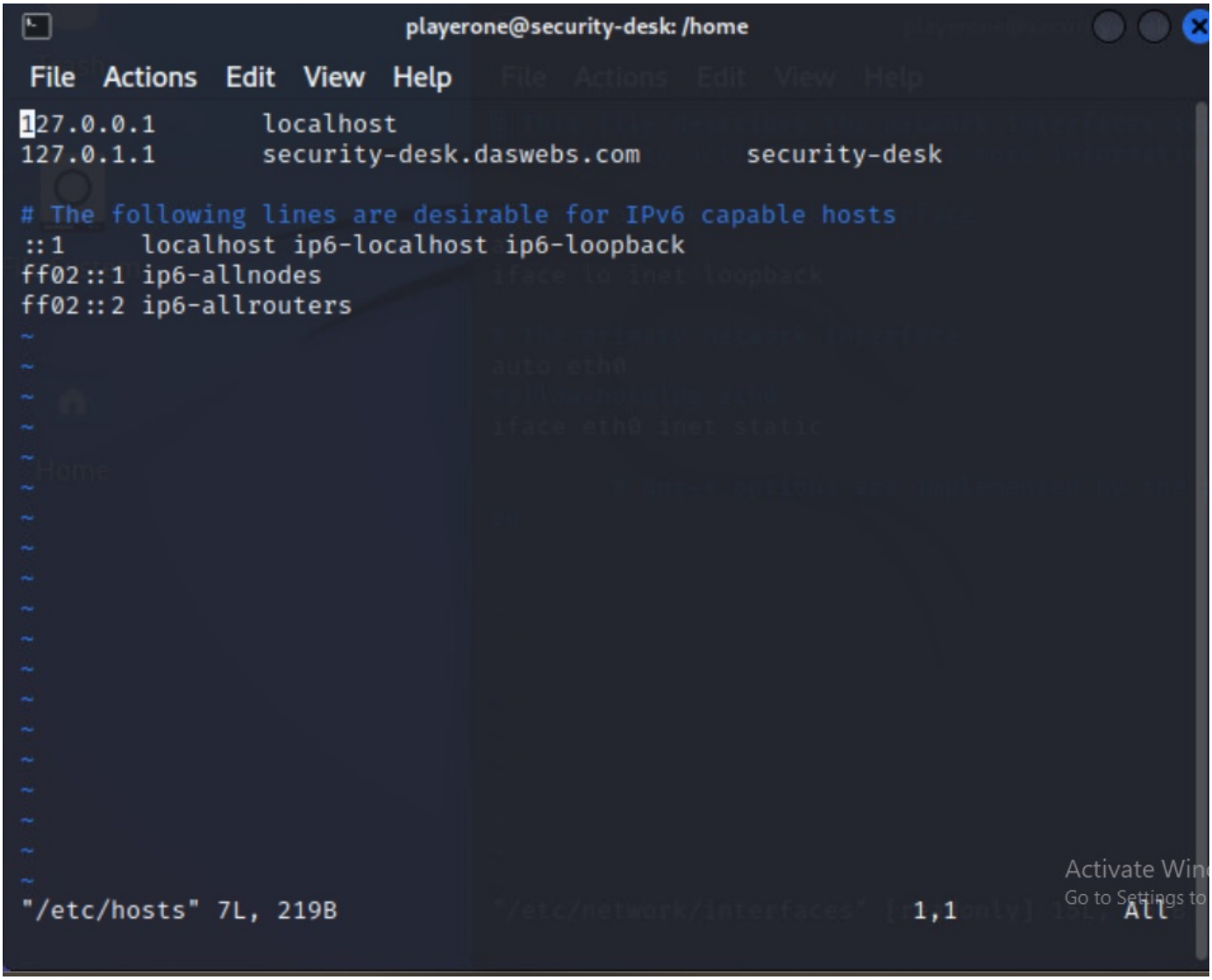
and changed the name, pressed esc then `:wq!` save, quit exit.



Below is /etc/hosts on security-desk and change the name to SecConsultantKali and secuirty-desk.daswebs.com to SecConsultantKali.daswebs.com

(`sudo vim /etc/hosts`)

then CTRL+X exit and save vim

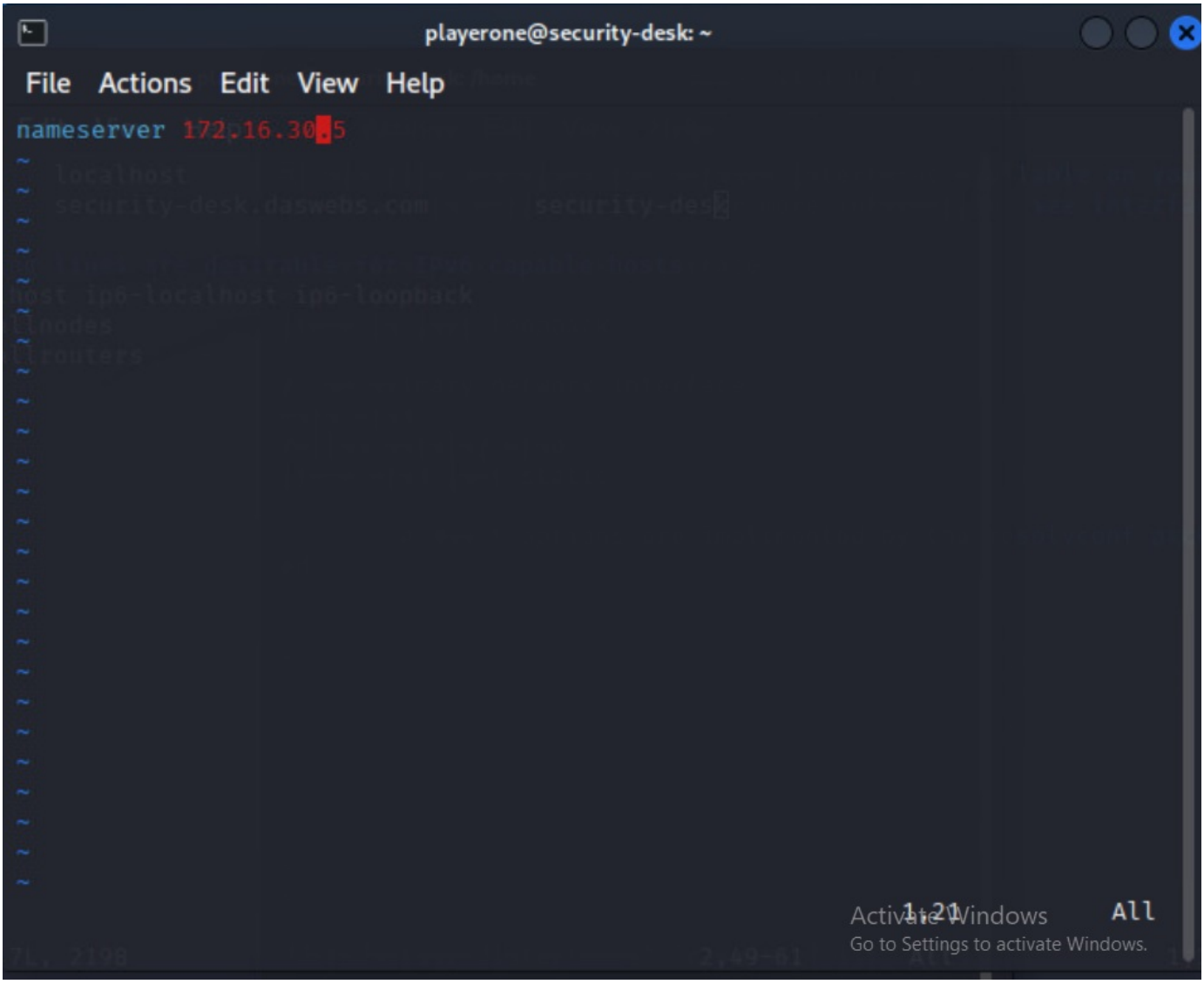


To verify: `ip` `ifup` - if ethernet is up

Reference: how to setup DHCP static syntax

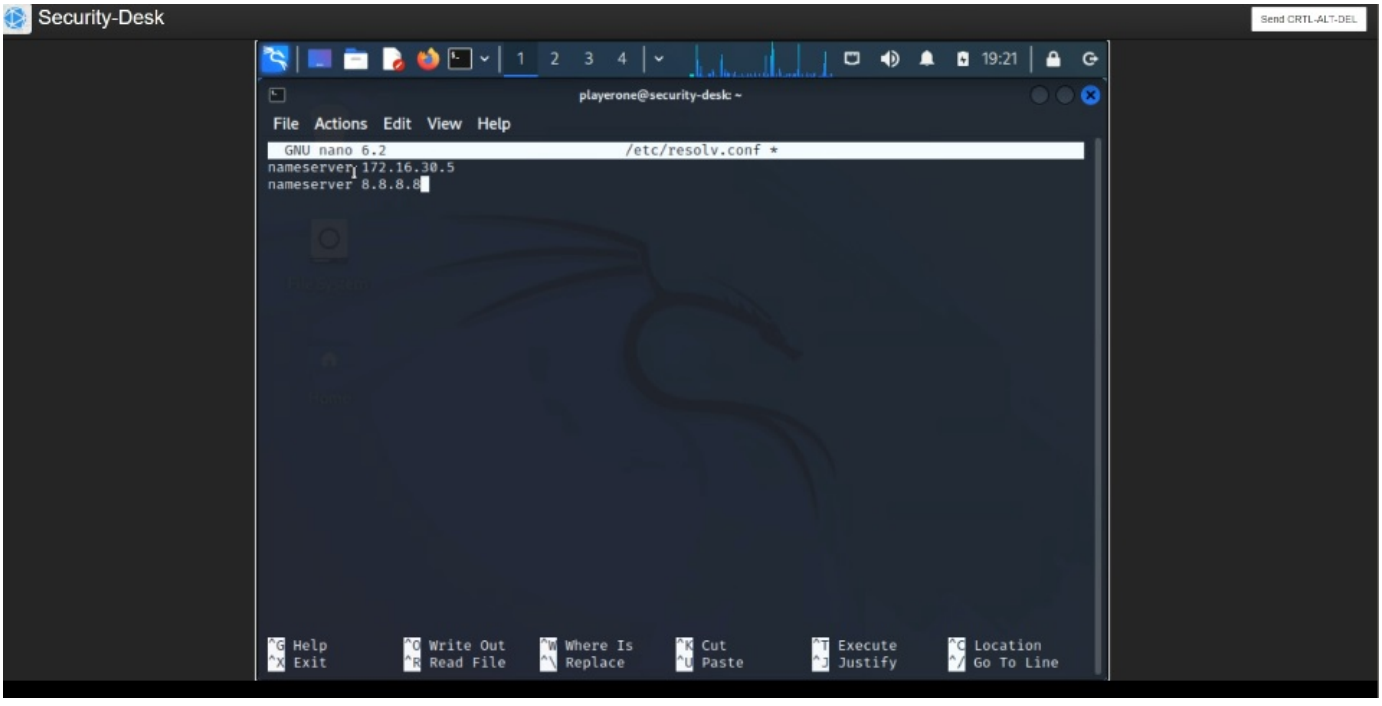
- [x] ## Kali DNS Check

Changed this from



To this and use `chattr -i vim /etc/resolv.conf` then edit your changes and then `chattr +i /etc/resolv.conf` to make it so it can not be edited again

press esc then `:wq!` to save and quit.



- [x] ## New Account Created
- [x] ## Home Directory Created
- [x] ## Sudoers Privilege's Granted
- [x] ## Shell Changed to Bash

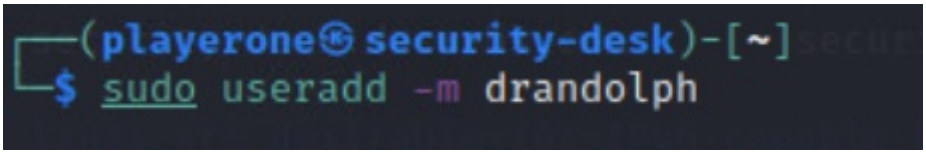
Logged into Security Desk

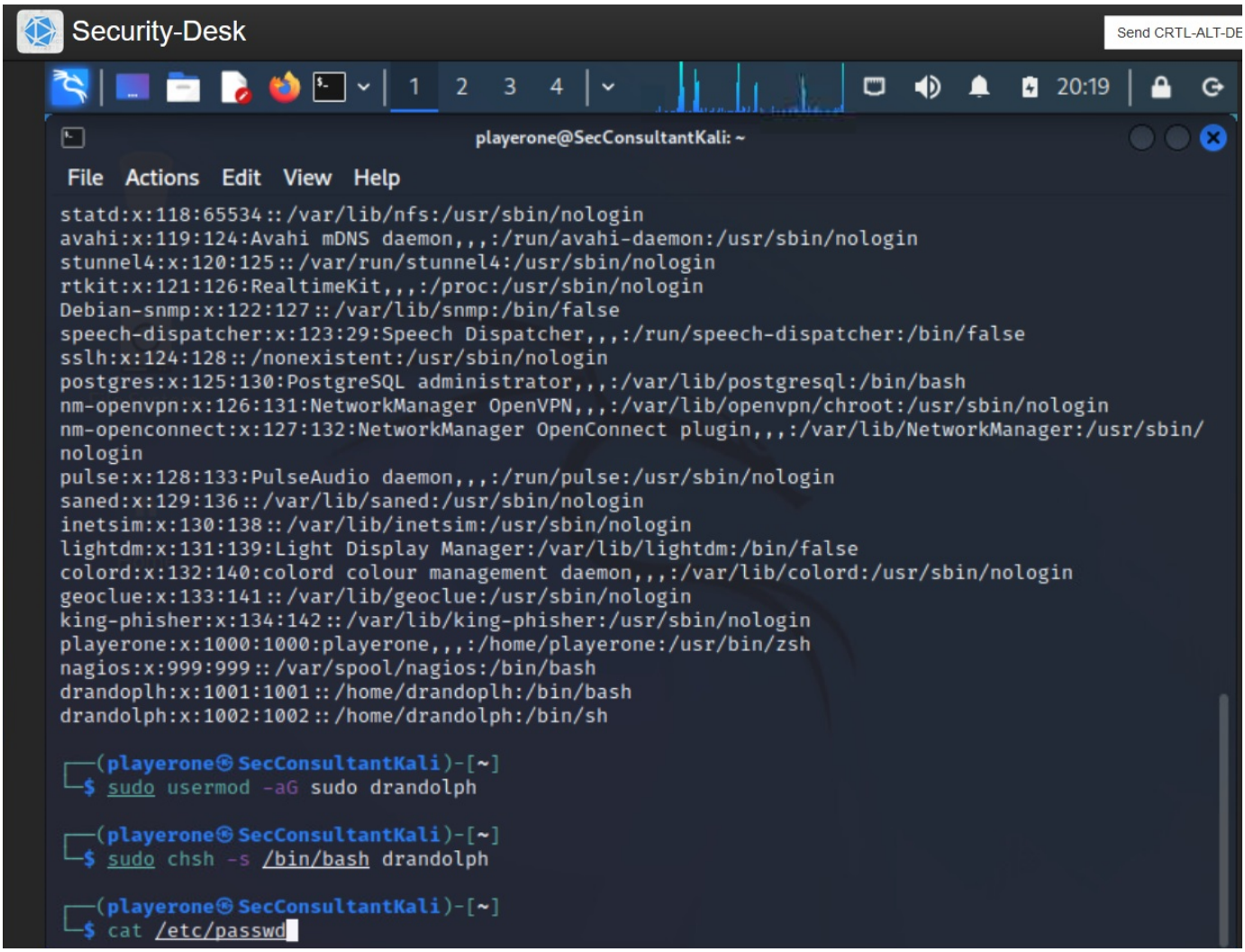
Googled/Watched video on how to manually add new user in Linux.

Added user by using `sudo useradd -m drandolph` (-m= default directory.)

then `sudo usermod -aG sudo dradolph` (-aG = Add to group) sudoers

Lastly `sudo chsh -s /bin/bash drandolph` chsh= change shell,



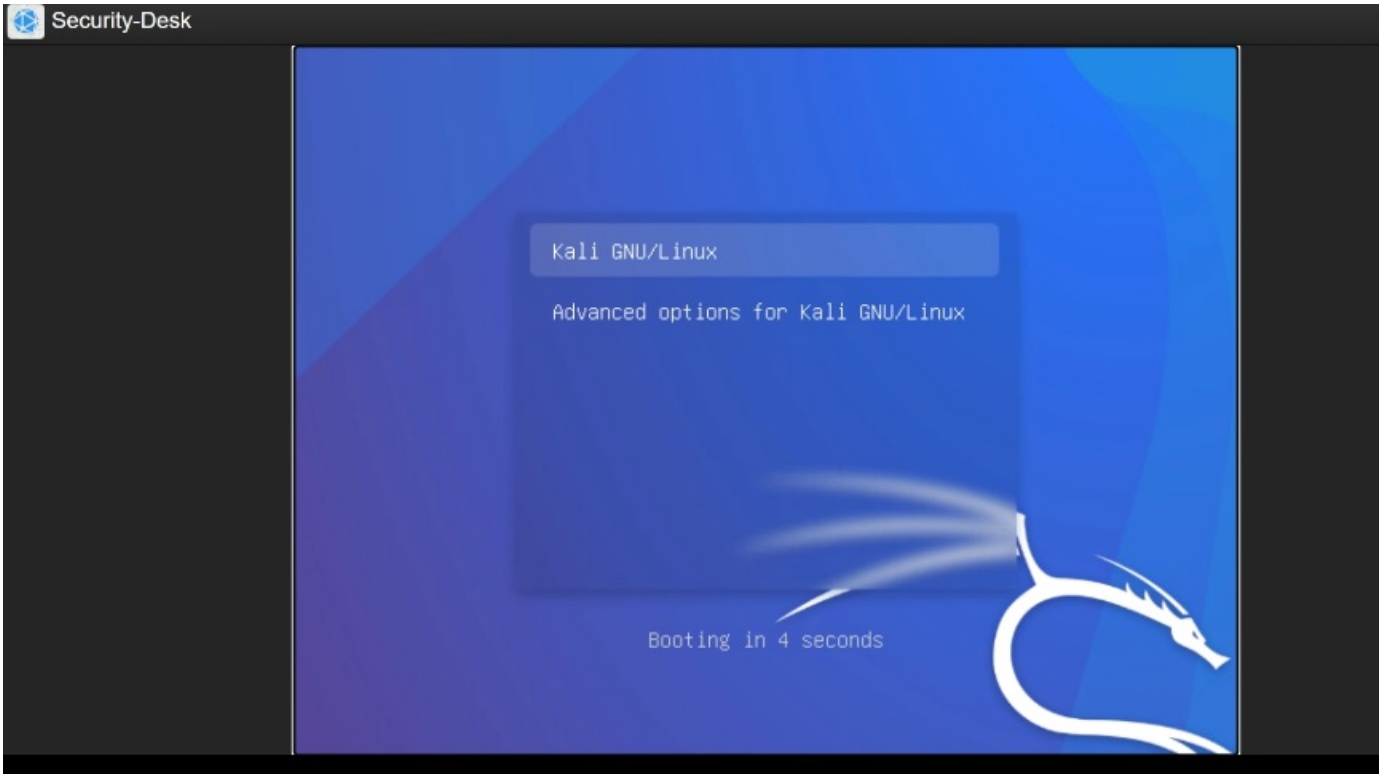


To verify :

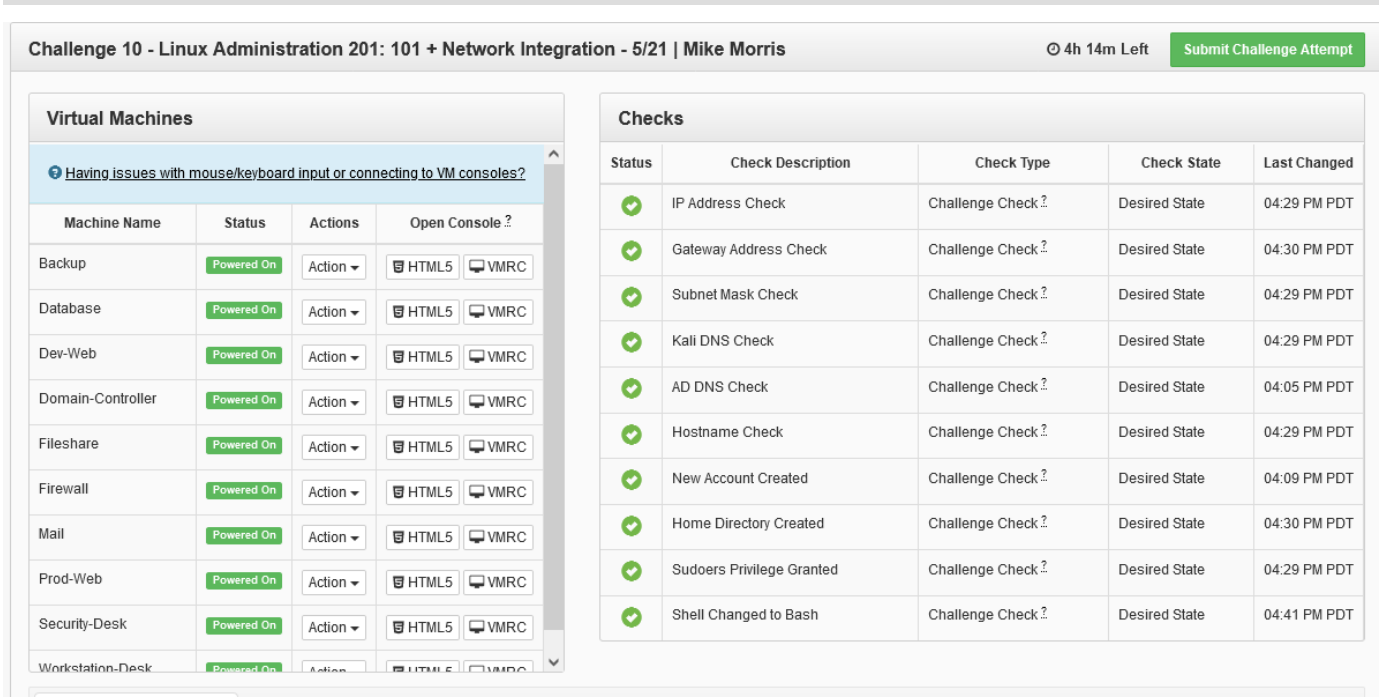
`cat /etc/passwd` -To show usernames inlcuding directories as stated with the picture above ^.

Finally,

Restart Kali



Finished!



Challenge 10 - Linux Administration 201: 101 + Network Integration - 5/21 | Mike Morris

4h 14m Left | Submit Challenge Attempt

Virtual Machines

Having issues with mouse/keyboard input or connecting to VM consoles?

Machine Name	Status	Actions	Open Console
Backup	Powered On	Action	HTML5 VMRC
Database	Powered On	Action	HTML5 VMRC
Dev-Web	Powered On	Action	HTML5 VMRC
Domain-Controller	Powered On	Action	HTML5 VMRC
Fileshare	Powered On	Action	HTML5 VMRC
Firewall	Powered On	Action	HTML5 VMRC
Mail	Powered On	Action	HTML5 VMRC
Prod-Web	Powered On	Action	HTML5 VMRC
Security-Desk	Powered On	Action	HTML5 VMRC
Workstation-Desk	Powered On	Action	HTML5 VMRC

Checks

Status	Check Description	Check Type	Check State	Last Changed
✓	IP Address Check	Challenge Check	Desired State	04:29 PM PDT
✓	Gateway Address Check	Challenge Check	Desired State	04:30 PM PDT
✓	Subnet Mask Check	Challenge Check	Desired State	04:29 PM PDT
✓	Kali DNS Check	Challenge Check	Desired State	04:29 PM PDT
✓	AD DNS Check	Challenge Check	Desired State	04:05 PM PDT
✓	Hostname Check	Challenge Check	Desired State	04:29 PM PDT
✓	New Account Created	Challenge Check	Desired State	04:09 PM PDT
✓	Home Directory Created	Challenge Check	Desired State	04:30 PM PDT
✓	Sudoers Privilege Granted	Challenge Check	Desired State	04:29 PM PDT
✓	Shell Changed to Bash	Challenge Check	Desired State	04:41 PM PDT