CVES

What they are?

How can you find out about them ? (https://cve.mitre.org/)

Selinux

turning it on and off

how to change manipulate selinux

Firewalld

How to open and close ports on your box

Netstat and lsof

what services are running on what ports

Wireshark

Looking at traffic coming into your box

Nmap

Scanning of boxes and network

Including diagram mapping

tcpdump (goes with wireshark)

Logfiles

Audit files (audit.d)

Messages

systctl

Hardening your box

Nist standards and Hardening your linux box from scratch

what is it and why

Ansible (automation)

introduction to automation tool. You may want to deploy multiple vms

Aide

Checking to see what has changed (atime, ctime)

stat on file

Encryption

create a directory and encrypted it

mount it on boot

Securing grub

Spin up instances in google from command line

Need to setup your ssh keys

Here is the link for reference:

<https://cloud.google.com/sdk/gcloud/reference/compute/instances/create>

There should be two instances one for centos 7.2 and redhat 7.2

* Name can be something you can remember
* Disksize should 20 gigs
* Boot-disk-type
* Place on vm in us-west-1b and the other us-east-1b
* Can-ip-foward = yes

Example commands

somecomputer$ gcloud compute zones list

NAME REGION STATUS NEXT\_MAINTENANCE TURNDOWN\_DATE

asia-east1-c asia-east1 UP

asia-east1-a asia-east1 UP

asia-east1-b asia-east1 UP

europe-west1-b europe-west1 UP

europe-west1-c europe-west1 UP

europe-west1-d europe-west1 UP

us-central1-b us-central1 UP

us-central1-a us-central1 UP

us-central1-c us-central1 UP

us-central1-f us-central1 UP

us-east1-b us-east1 UP

us-east1-c us-east1 UP

us-east1-d us-east1 UP

us-west1-b us-west1 UP

us-west1-a us-west1 UP

somecomputer$ gcloud compute disk-types list

NAME ZONE VALID\_DISK\_SIZES

local-ssd asia-east1-c 375GB-375GB

pd-ssd asia-east1-c 10GB-65536GB

pd-standard asia-east1-c 10GB-65536GB

local-ssd europe-west1-d 375GB-375GB

pd-ssd europe-west1-d 10GB-65536GB

pd-standard europe-west1-d 10GB-65536GB

local-ssd asia-east1-a 375GB-375GB

pd-ssd asia-east1-a 10GB-65536GB

pd-standard asia-east1-a 10GB-65536GB

somecomputer:~ tameikareed$ gcloud compute machine-types list| awk '{print $1,$4}'

NAME MEMORY\_GB

f1-micro 0.60

g1-small 1.70

n1-highcpu-16 14.40

n1-highcpu-2 1.80

n1-highcpu-32 28.80

n1-highcpu-4 3.60

n1-highcpu-8 7.20

n1-highmem-16 104.00

n1-highmem-2 13.00

n1-highmem-32 208.00

n1-highmem-4 26.00

n1-highmem-8 52.00

Selinux

Firewalls

Troubleshooting

* Nmap
* Ss
* Using the ip command
* What services are running on each other box
  + Network scans
* Tcpdump
* Turning firewall on and off
* Using

https://cloud.google.com/security/