Franklin Wang

Task 1: Firewall

```
franklin-wang@franklin-wang-VMware20-1: ~
franklin-wang@franklin-wang-VMware20-1:~$ sudo ufw allow https
Rule added
Rule added (v6)
franklin-wang@franklin-wang-VMware20-1:~$ sudo ufw allow from 192.168.0.0/24
Rule added
franklin-wang@franklin-wang-VMware20-1:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
franklin-wang@franklin-wang-VMware20-1:~$ sudo ufw enable
Firewall is active and enabled on system startup
franklin-wang@franklin-wang-VMware20-1:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
443                        ALLOW       Anywhere
Anywhere                   ALLOW       192.168.0.0/24
22/tcp                     ALLOW       Anywhere
443 (v6)                   ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)

franklin-wang@franklin-wang-VMware20-1:~$
```

Task 2: SSH Host Access

```
franklin-wang@franklin-wang-VMware20-1: /etc/ssh
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo vi /etc/hosts.allow
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo cat /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
ALL: 192.168.1.101
ALL: 192.168.1.102
ALL: 192.168.1.103
```

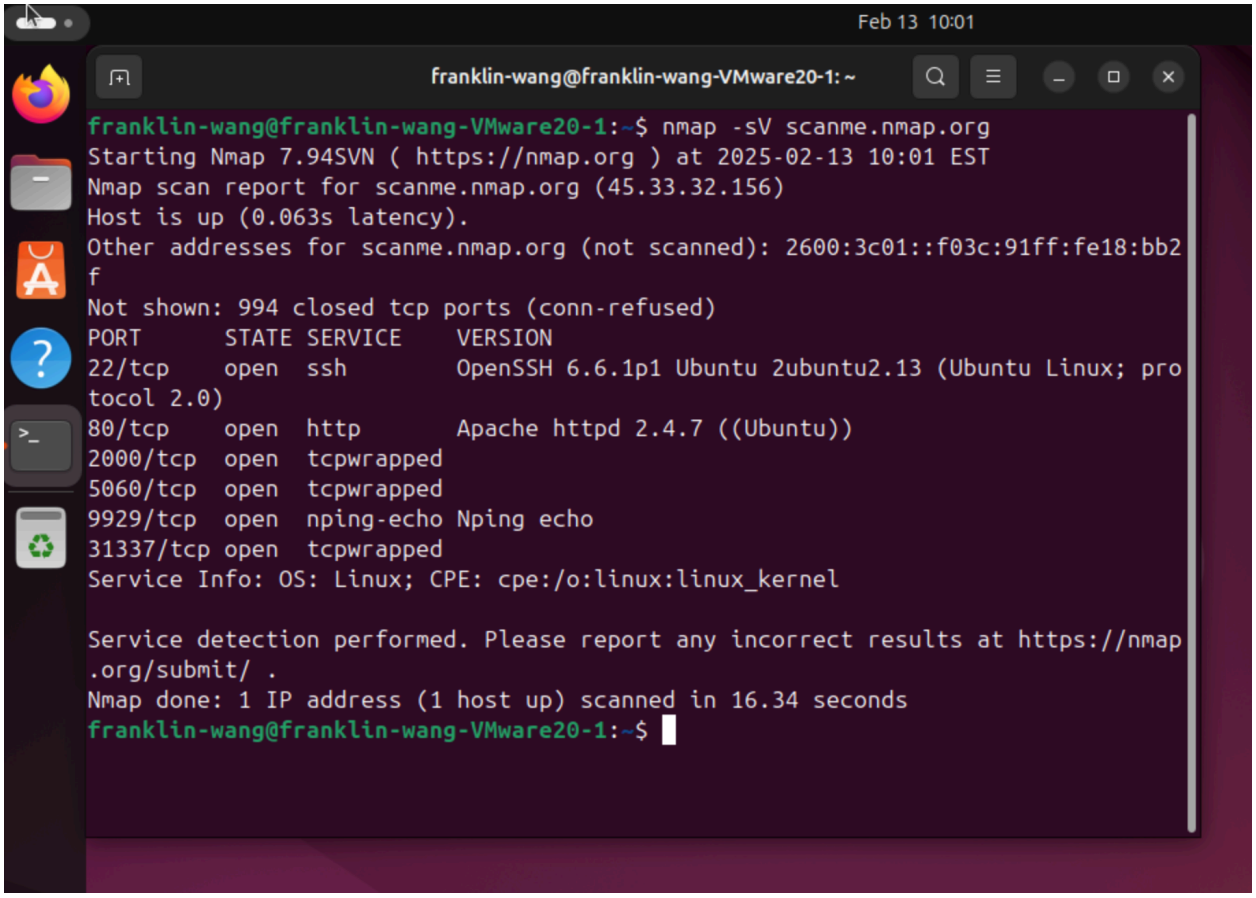
```
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo vi /etc/hosts.deny
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo cat /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID

ALL:ALL
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$
```

Task 3: Server Username Access

```
# PAM configuration for the Secure Shell service

# Standard Un*x authentication.
@include common-auth

# Disallow non-root logins when /etc/nologin exists.
account    required     pam_nologin.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
 account  required     pam_access.so
```

```
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo tail /etc/security/access.
conf
#
# User "john" should get access from ipv6 net/mask
#+:john:2001:4ca0:0:101::/64
#
# All other users should be denied to get access from all sources.
#-:ALL:ALL

+ : franklin-wang : ALL
+ : compsecprof : ALL
- : ALL : ALL
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$
```

Task 4: Nmap scan



Running Apache version 2.4.7

Task 5: SSHD Config

```
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo vi sshd_config
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$ sudo systemctl restart ssh
franklin-wang@franklin-wang-VMware20-1:/etc/ssh$
```

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 2
MaxSessions 2
```

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