Setup

Since I am using cloud vm, there have been multiple instances of my vm becoming unresponsive due to blocking of ssh, and I had to delete my VM instance, this is the reason why my IP address keeps changing

```
import cv2
from matplotlib import pyplot as plt

# This is a bit of magic to make matplotlib figures appear inline in
the notebook
# rather than in a new window.
%matplotlib inline
plt.rcParams['figure.figsize'] = (100.0, 80.0) # set default size of
plots
plt.rcParams['image.interpolation'] = 'nearest'
plt.rcParams['image.cmap'] = 'gray'


def show_img(img):
    img = cv2.imread(img,-1)
    plt.subplot(131),plt.imshow(img),
    plt.title('Color'),plt.xticks([]), plt.yticks([])
    plt.show()
```

Task 1: Using Firewall

- Prevent A from doing telnet to Machine B

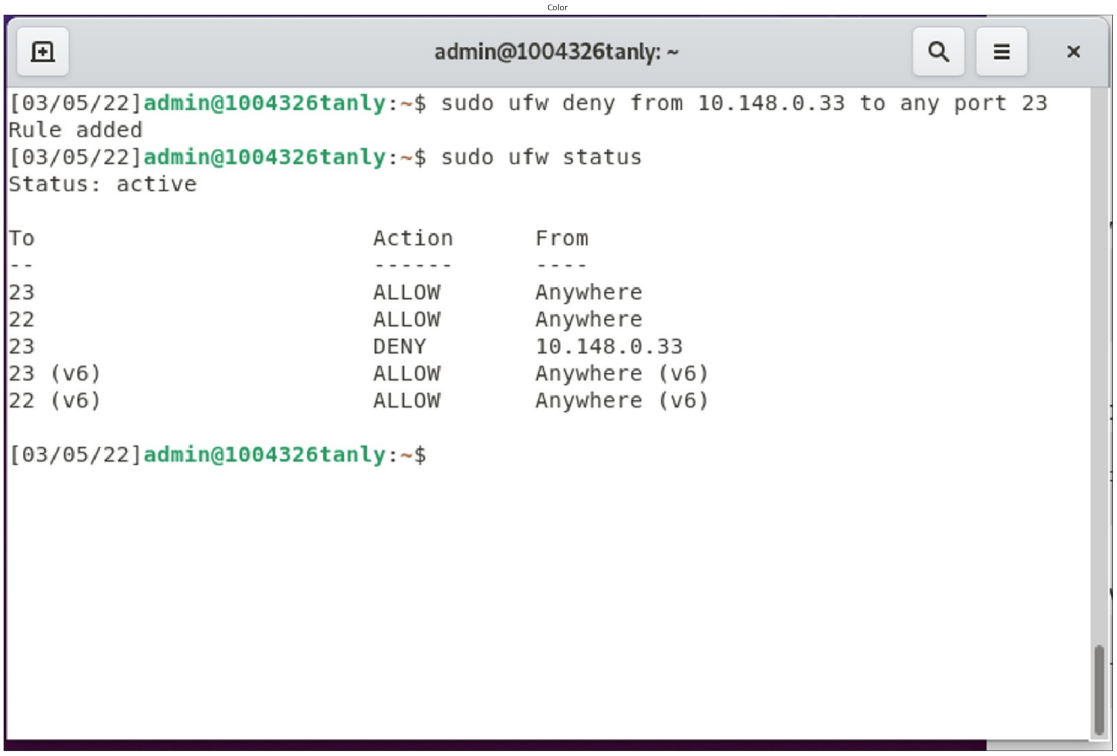
  ufw

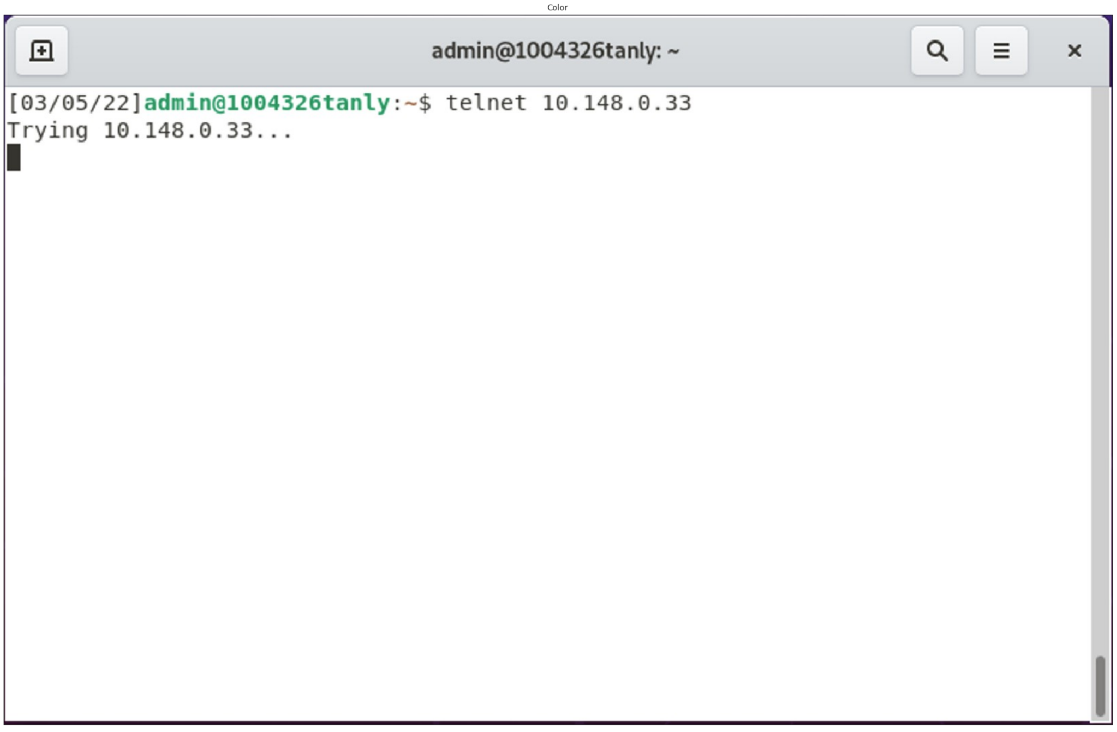
Using ufw to deny any incoming connection from 10.148.0.33 (A) to port 23 (telnet), results in telnet connection being blocked at B.

```
show_img('Task 1/ufw/check_telnet_A.png')
show_img('Task 1/ufw/deny_telnet_A.png')
show_img('Task 1/ufw/telnet_blocked_A.png')
```

Color

```
[03/05/22]admin@1004326tanly:~$ telnet 10.148.0.33
Trying 10.148.0.33...
Connected to 10.148.0.33.
Escape character is '^]'.
Ubuntu 20.04.3 LTS
1004326tanly login: admin
Password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1029-gcp x86_64)

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

  System information as of Sat Mar  5 13:07:17 UTC 2022

  System load:                      0.54
  Usage of /:                       13.4% of 57.98GB
  Memory usage:                     30%
  Swap usage:                       0%
  Processes:                        212
  Users logged in:                  0
  IPv4 address for br-3e5f42528ad9: 10.9.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for ens4:            10.148.0.33

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

88 updates can be applied immediately.
53 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

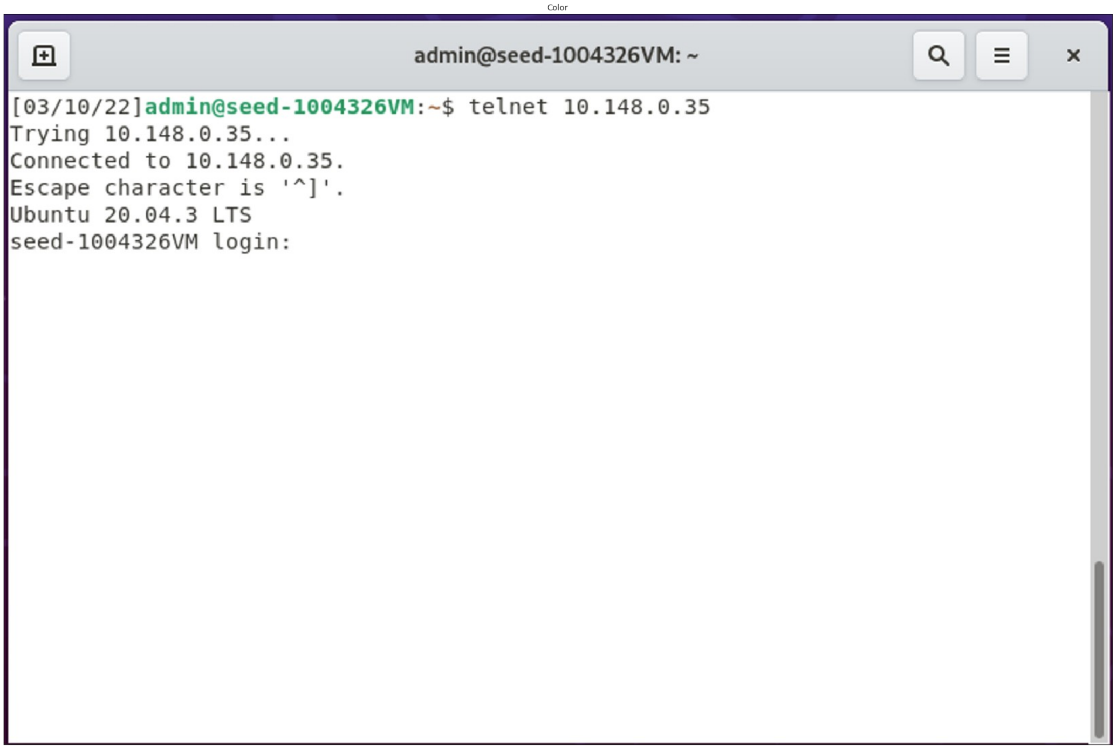


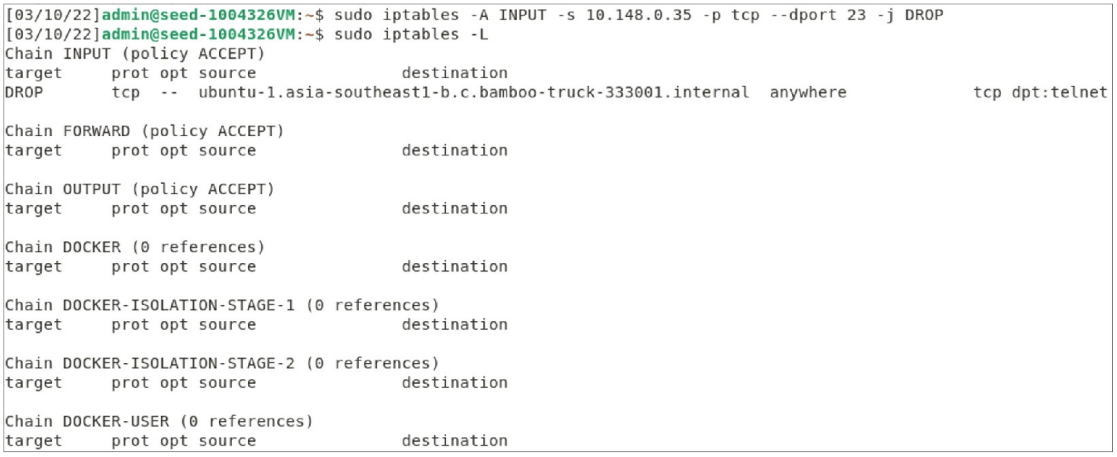


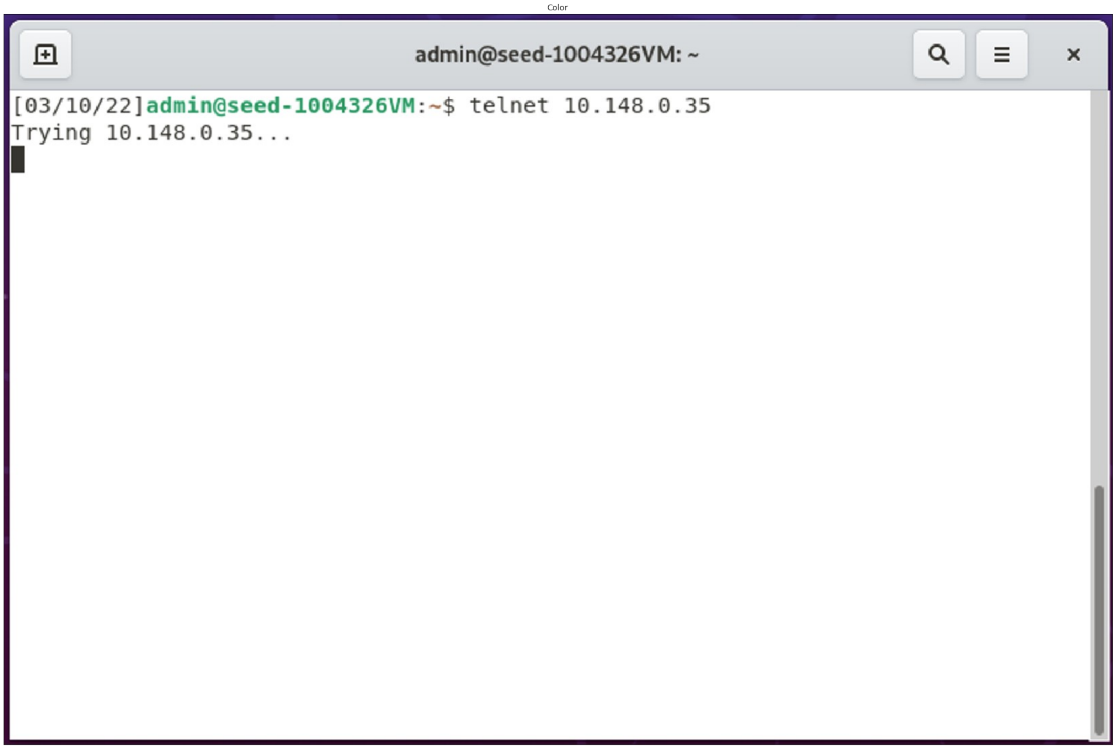
iptables

At the INPUT chain, we can append a rule to drop packet 10.148.0.35 (A) at destination port 23. This results in telnet connection being blocked at B.

```
show_img('Task 1/iptables/check_telnet_A.png')
show_img('Task 1/iptables/drop_telnet_A.png')
show_img('Task 1/iptables/telnet_blocked_A.png')
```







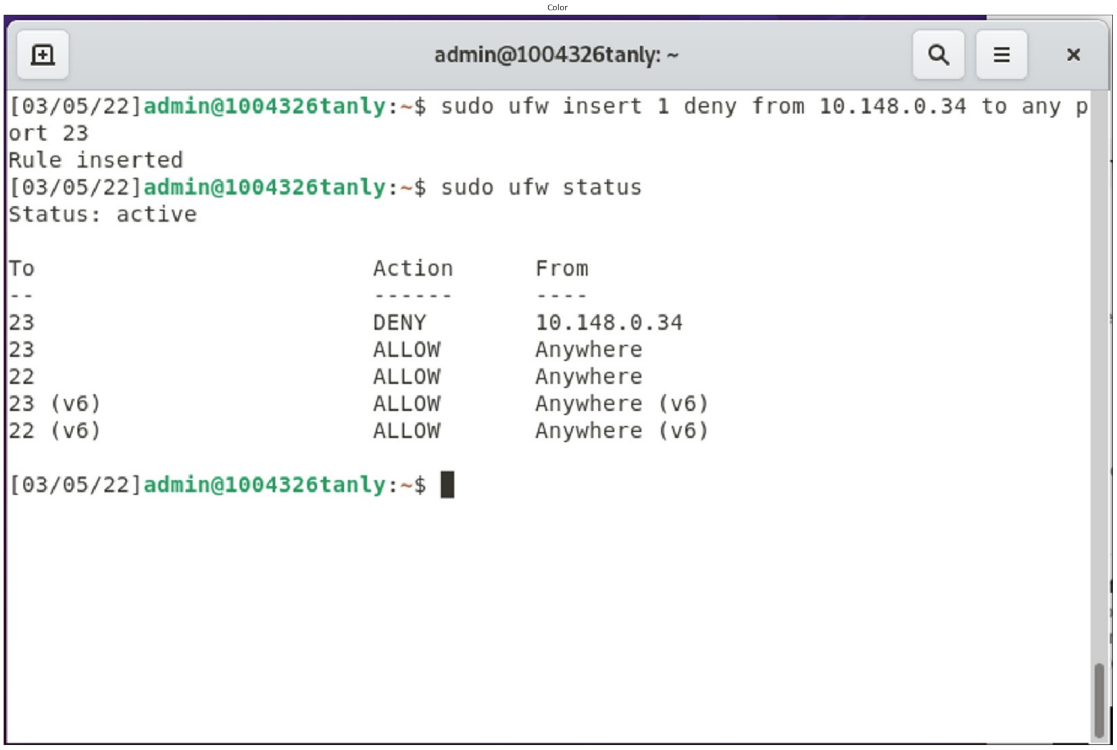
- Prevent B from doing telnet to Machine A

  ufw

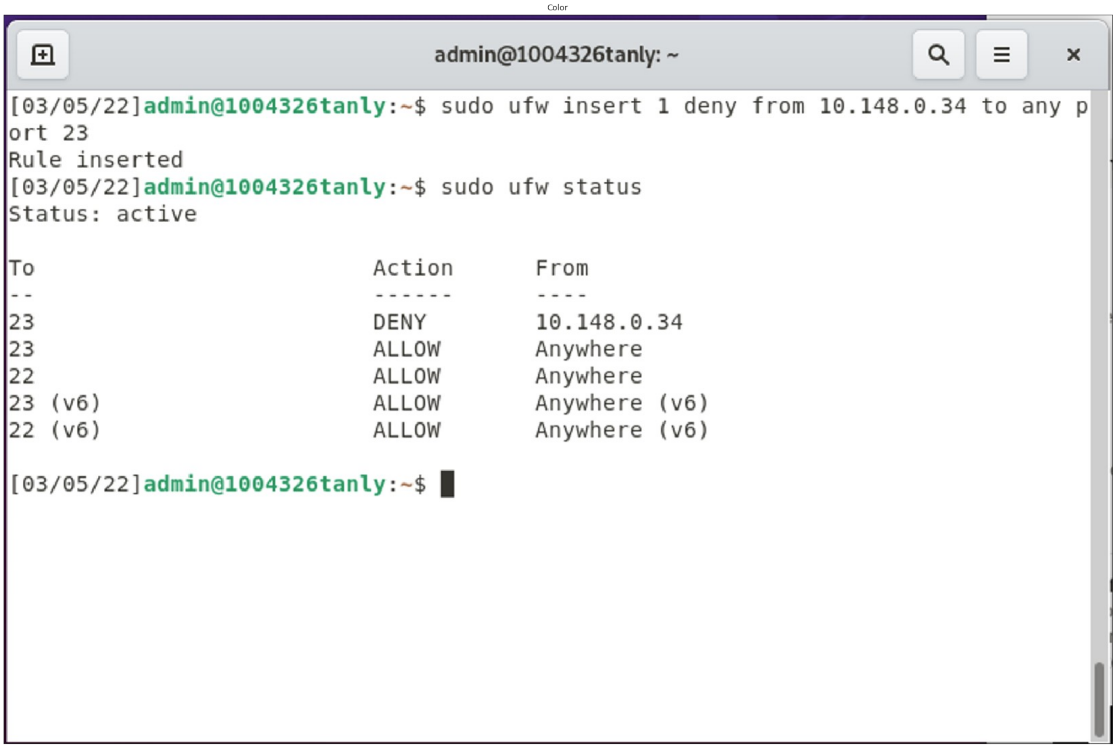
Using ufw to deny any incoming connection from 10.148.0.34 (B) to port 23 (telnet), results in telnet connection being blocked at A.

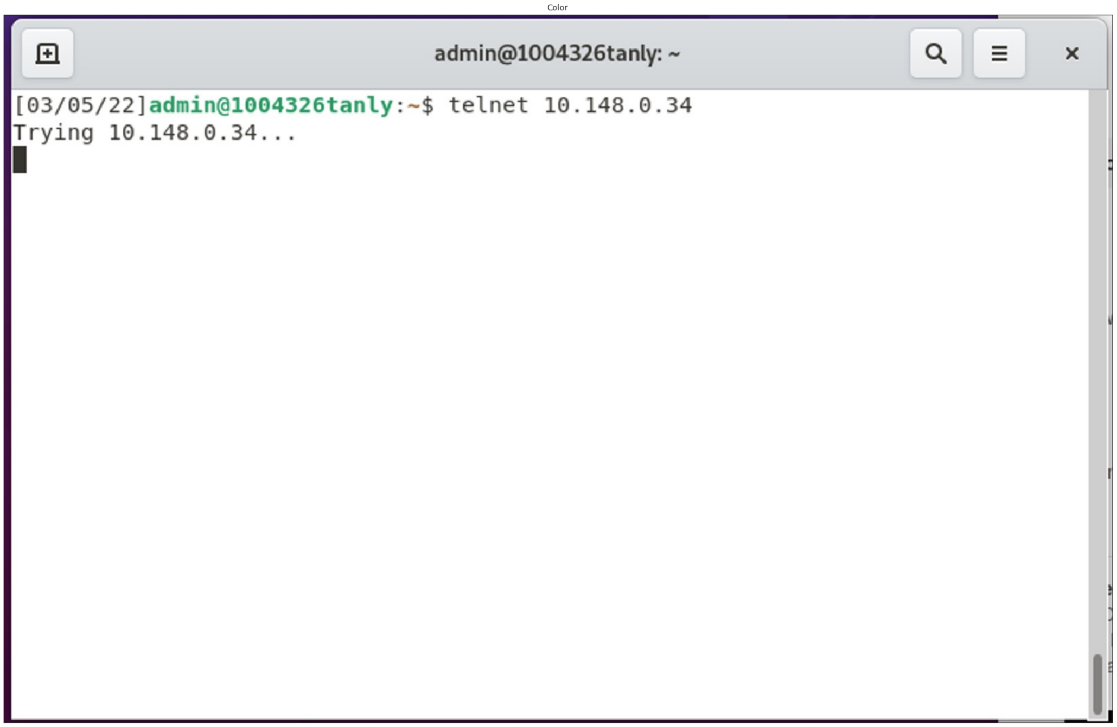
```
show_img('Task 1/ufw/deny_telnet_B.png')
show_img('Task 1/ufw/deny_telnet_B.png')
show_img('Task 1/ufw/telnet_blocked_B.png')
```

Color


admin@1004326tanly: ~
[03/05/22]admin@1004326tanly:~$ sudo ufw insert 1 deny from 10.148.0.34 to any p
ort 23
Rule inserted
[03/05/22]admin@1004326tanly:~$ sudo ufw status
Status: active
To Action From
-- ------ ----
23 DENY 10.148.0.34
23 ALLOW Anywhere
22 ALLOW Anywhere
23 (v6) ALLOW Anywhere (v6)
22 (v6) ALLOW Anywhere (v6)
[03/05/22]admin@1004326tanly:~$

Color

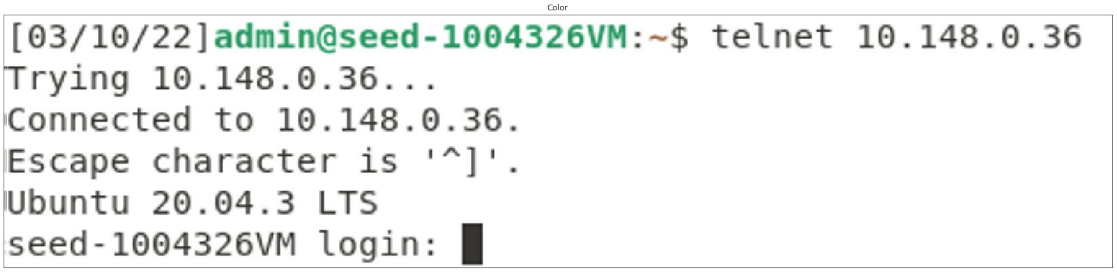

admin@1004326tanly: ~
[03/05/22]admin@1004326tanly:~$ sudo ufw insert 1 deny from 10.148.0.34 to any p
ort 23
Rule inserted
[03/05/22]admin@1004326tanly:~$ sudo ufw status
Status: active
To Action From
-- ------ ----
23 DENY 10.148.0.34
23 ALLOW Anywhere
22 ALLOW Anywhere
23 (v6) ALLOW Anywhere (v6)
22 (v6) ALLOW Anywhere (v6)
[03/05/22]admin@1004326tanly:~$



iptables

At the INPUT chain, we can append a rule to drop packet 10.148.0.36 (A) at destination port 23. This results in telnet connection being blocked at A.

```
show_img('Task 1/iptables/check_telnet_B.png')
show_img('Task 1/iptables/drop_telnet_B.png')
show_img('Task 1/iptables/telnet_blocked_B.png')
```



```
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -A INPUT -s 10.148.0.36 -p tcp --dport 23 -j DROP
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  ubuntu-2.asia-southeast1-b.c.bamboo-truck-333001.internal  anywhere             tcp dpt:telnet

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain DOCKER (0 references)
num  target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
num  target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
num  target     prot opt source               destination

Chain DOCKER-USER (0 references)
num  target     prot opt source               destination
```

```
[03/10/22]admin@seed-1004326VM:~$ telnet 10.148.0.36
Trying 10.148.0.36...
```

- Prevent A from visiting an external web site find webserver

Using wget, we can find the IP addresses of the facebook webserver

```
show_img('Task 1/find_webserver.png')
show_img('Task 1/find_webserver_2.png')
```

```
[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-10 06:03:21--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.7.35, 2a03:2880:f10c:83:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.7.35|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.facebook.com/ [following]
--2022-03-10 06:03:21--  https://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.13.35, 2a03:2880:f10c:83:face:b00c:0:25de
Connecting to www.facebook.com (www.facebook.com)|157.240.13.35|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.facebook.com/unsupportedbrowser [following]
--2022-03-10 06:03:22--  https://www.facebook.com/unsupportedbrowser
Reusing existing connection to www.facebook.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html              [ <=>                ]  54.72K  --.-KB/s    in 0.02s

2022-03-10 06:03:22 (2.85 MB/s) - 'index.html' saved [56031]
```

```
[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-10 06:17:07--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:283:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.facebook.com/ [following]
--2022-03-10 06:17:07--  https://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.13.35, 2a03:2880:f10c:181:face:b00c:0:25de
Connecting to www.facebook.com (www.facebook.com)|157.240.13.35|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.facebook.com/unsupportedbrowser [following]
--2022-03-10 06:17:08--  https://www.facebook.com/unsupportedbrowser
Reusing existing connection to www.facebook.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html                          [ <=>                                                ]  54.71K  --.-KB/s    in 0.09s

2022-03-10 06:17:08 (616 KB/s) - 'index.html' saved [56018]

[03/10/22]admin@seed-1004326VM:~$ rm index.html
```

ufw

Using ufw, we deny all connections from facebook webserver 157.240.13.35. In this case, there are multiple webservers, so we deny the connection to the subsequent webserver.

```
show_img('Task 1/ufw/deny_webserver.png')
show_img('Task 1/ufw/deny_webserver_2.png')
```

Color

```
[03/10/22]admin@seed-1004326VM:~$ sudo ufw deny from 157.240.13.35
Rule added
[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-10 06:17:28--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:283:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.facebook.com/ [following]
--2022-03-10 06:17:28--  https://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.13.35, 2a03:2880:f10c:181:face:b00c:0:25de
Connecting to www.facebook.com (www.facebook.com)|157.240.13.35|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.facebook.com/unsupportedbrowser [following]
--2022-03-10 06:17:28--  https://www.facebook.com/unsupportedbrowser
Reusing existing connection to www.facebook.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html                              [ <=>                                                                ]  54.70K  --.-KB/s    in 0.03s

2022-03-10 06:17:29 (2.01 MB/s) - 'index.html' saved [56013]

[03/10/22]admin@seed-1004326VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        157.240.13.35
```

Color

```
[03/10/22]admin@seed-1004326VM:~$ sudo ufw deny out to 157.240.13.35
Rule added
[03/10/22]admin@seed-1004326VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        157.240.13.35

157.240.13.35              DENY OUT    Anywhere

[03/10/22]admin@seed-1004326VM:~$ sudo ufw delete 1
Deleting:
 deny from 157.240.13.35
Proceed with operation (y|n)? y
Rule deleted
[03/10/22]admin@seed-1004326VM:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
157.240.13.35              DENY OUT    Anywhere

[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-10 11:01:32--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:83:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... ^C
```

iptables

At the output chain, we create a firewall rule to prevent local traffic from communicating the facebook webserver 157.240.13.35 by dropping all packets to the specifc IP address

```
show_img('Task 1/iptables/drop_webserver.png')
```

```
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -A OUTPUT -d 157.240.13.35 -j DROP
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             edge-star-mini-shv-02-sin6.facebook.com

Chain DOCKER (0 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
target     prot opt source               destination

Chain DOCKER-USER (0 references)
target     prot opt source               destination
[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-10 06:09:44--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:283:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443...
```

Task 2: Implementing a Simple Firewall

In the init_module, we set the handler function to be hook_pre_routing_func.

From the ip header, we retrieve the tcp header.

To prevent A from doing telnet to Machine B, we filter packets running TCP protocol, with destination of 23 and IP destination of 10.148.0.41 and drop them. To prevent A from visiting the facebook webserver, we filter packets running TCP protocol and IP destination of 157.240.7.35 and drop them. To prevent A from doing ssh to Machine B (correction from screenshot), we filter packets running TCP protocol, with destination of 22 and IP destination of 10.148.0.41 and drop them.

```
show_img('Task 2/netfilter_1.png')
show_img('Task 2/netfilter_2.png')
show_img('Task 2/insmod.png')
show_img('Task 2/telnet_blocked.png')
show_img('Task 2/webserver_blocked.png')
```

Color

Activities Terminal Mar 14 17:05

admin@seed-1004326VM: ~/Lab/FW

admin@seed-1004326VM: ~/Lab/FW | admin@seed-1004326VM: ~ | admin@seed-1004326VM: ~

```
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/netfilter.h>
#include <linux/netfilter_ipv4.h>
#include <linux/inet.h>
#include <linux/ip.h>
#include <linux/tcp.h>

static struct nf_hook_ops nfho;

unsigned int hook_pre_routing_func(void *priv, struct sk_buff *skb,
                                   const struct nf_hook_state *state)
{
    struct iphdr *iph;
    struct tcphdr *tcph;

    iph = ip_hdr(skb);
    tcph = (void *)iph + iph->ihl * 4;

    // Prevent A from doing telnet to Machine B
    if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && iph->daddr == in_aton("10.148.0.41"))
    {
        return NF_DROP;
    }

    // Prevent A from visiting a website
    if (iph->protocol == IPPROTO_TCP && iph->daddr == in_aton("157.240.7.35"))
    {
        return NF_DROP;
    }

    // Prevent A from doing telnet to Machine B
    if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22) && iph->daddr == in_aton("10.148.0.41"))
    {
        return NF_DROP;
    }



    return NF_ACCEPT; /* Accept other packets */
}
```

"netfilter.c" 61L, 1585C 1,1 Top

Color

Activities Terminal Mar 14 17:06

admin@seed-1004326VM: ~/Lab/FW

admin@seed-1004326VM: ~/Lab/FW | admin@seed-1004326VM: ~ | admin@seed-1004326VM: ~

```
    // Prevent A from doing telnet to Machine B
    if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(23) && iph->daddr == in_aton("10.148.0.41"))
    {
        return NF_DROP;
    }

    // Prevent A from visiting a website
    if (iph->protocol == IPPROTO_TCP && iph->daddr == in_aton("157.240.7.35"))
    {
        return NF_DROP;
    }

    // Prevent A from doing telnet to Machine B
    if (iph->protocol == IPPROTO_TCP && tcph->dest == htons(22) && iph->daddr == in_aton("10.148.0.41"))
    {
        return NF_DROP;
    }



    return NF_ACCEPT; /* Accept other packets */
}

/* Initialization routine */
int init_module()
{
    MODULE_LICENSE("GPL");
    /* Fill in our hook structure */
    nfho.hook = hook_pre_routing_func;  /* Handler function */
    nfho.hooknum = NF_INET_PRE_ROUTING; /* First hook for IPv4 */
    nfho.pf = PF_INET;
    nfho.priority = NF_IP_PRI_FIRST; /* Make our function first */
    nf_register_net_hook(&init_net, &nfho);

    return 0;
}

/* Cleanup routine */
void cleanup_module()
{
    nf_unregister_net_hook(&init_net, &nfho);
}
```

"netfilter.c" 61L, 1585C 61,1 Bot

Color

```
[03/12/22]admin@seed-1004326VM:~/Lab/FW$ make
make -C /lib/modules/5.11.0-1029-gcp/build M=/home/admin/Lab/FW modules
make[1]: Entering directory '/usr/src/linux-headers-5.11.0-1029-gcp'
  CC [M]  /home/admin/Lab/FW/netfilter.o
  MODPOST /home/admin/Lab/FW/Module.symvers
  LD [M]  /home/admin/Lab/FW/netfilter.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.11.0-1029-gcp'
[03/12/22]admin@seed-1004326VM:~/Lab/FW$ sudo insmod netfilter.ko
```

Task 3: Evading Egress Filtering

- Block all the outgoing traffic to external telnet servers

At the output chain, we create a firewall rule to prevent local traffic to drop all packets to destination port 23, thereby disabling telnet connections.

```
show_img('Task 3/deny_telnet.png')
show_img('Task 3/telnet_blocked.png')
```

```
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -A OUTPUT -p tcp --dport 23 -j DROP
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
ufw-after-logging-output  all  --  anywhere             anywhere
ufw-reject-output  all  --  anywhere             anywhere
ufw-track-output  all  --  anywhere             anywhere
DROP       tcp  --  anywhere             anywhere             tcp dpt:telnet
```

```
[03/10/22]admin@seed-1004326VM:~$ telnet 10.148.0.38
Trying 10.148.0.38...
```

- Block all the outgoing traffic to www.facebook.com

Similar to the explanation of denying the website, we find the webserver IP address, and drop the packets that are sent to 157.240.15.35. The firewall command is added to the output chain.

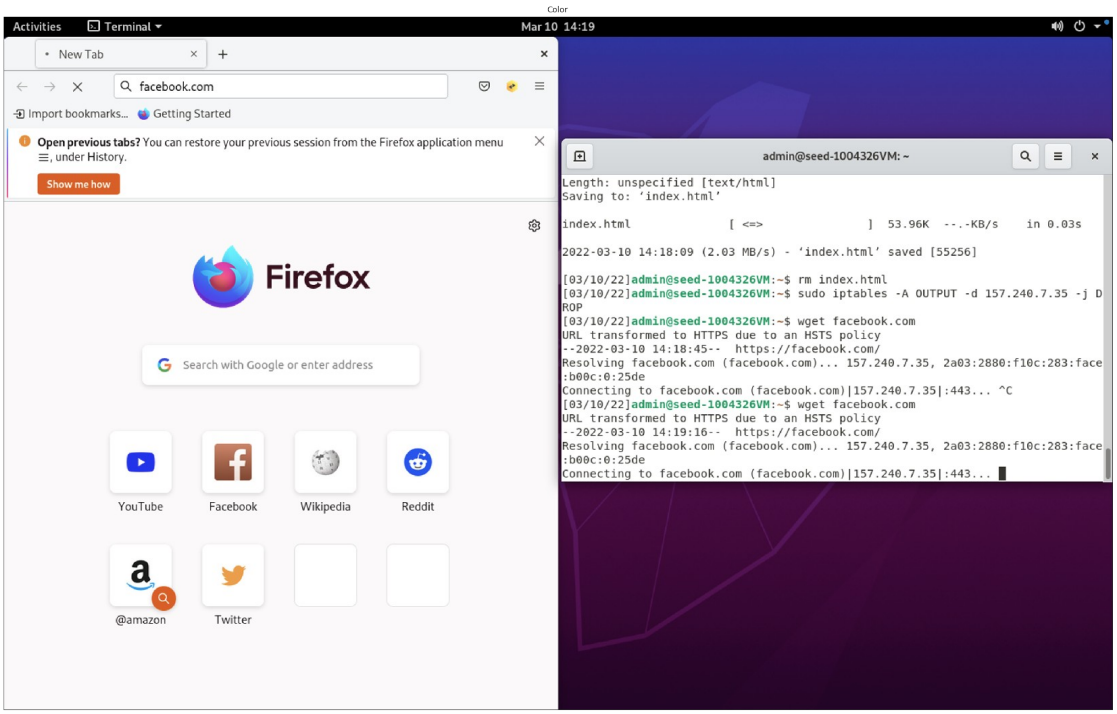
```
show_img('Task 3/find_facebook.png')
show_img('Task 3/find_facebook_2.png')
show_img('Task 3/facebook_blocked.png')
```

Color

```
[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
--2022-03-10 14:08:38--  http://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.15.35, 2a03:2880:f10c:283:face:b00
Connecting to facebook.com (facebook.com)|157.240.15.35|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://facebook.com/ [following]
--2022-03-10 14:08:38--  https://facebook.com/
Connecting to facebook.com (facebook.com)|157.240.15.35|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.facebook.com/ [following]
--2022-03-10 14:08:39--  https://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.7.35, 2a03:2880:f10c:283:f
Connecting to www.facebook.com (www.facebook.com)|157.240.7.35|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.facebook.com/unsupportedbrowser [following]
--2022-03-10 14:08:39--  https://www.facebook.com/unsupportedbrowser
Reusing existing connection to www.facebook.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html                                  [ <=>

2022-03-10 14:08:39 (3.47 MB/s) - 'index.html' saved [55260]

[03/10/22]admin@seed-1004326VM:~$ rm index.html
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -A OUTPUT -d 157.240.15.35 -j DROP
```

Color

```
[03/10/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-10 14:18:09--  https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.7.35, 2a03:2880:f10c:283:face:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.7.35|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.facebook.com/ [following]
--2022-03-10 14:18:09--  https://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.7.35, 2a03:2880:f10c:283:face:b00c:0:25de
Connecting to www.facebook.com (www.facebook.com)|157.240.7.35|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.facebook.com/unsupportedbrowser [following]
--2022-03-10 14:18:09--  https://www.facebook.com/unsupportedbrowser
Reusing existing connection to www.facebook.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html              [ <=>               ]  53.96K  --.-KB/s    in 0.03s

2022-03-10 14:18:09 (2.03 MB/s) - 'index.html' saved [55256]

[03/10/22]admin@seed-1004326VM:~$ rm index.html
[03/10/22]admin@seed-1004326VM:~$ sudo iptables -A OUTPUT -d 157.240.7.35 -j DROP
```



Task 3a: Telnet to Machine B through the firewall

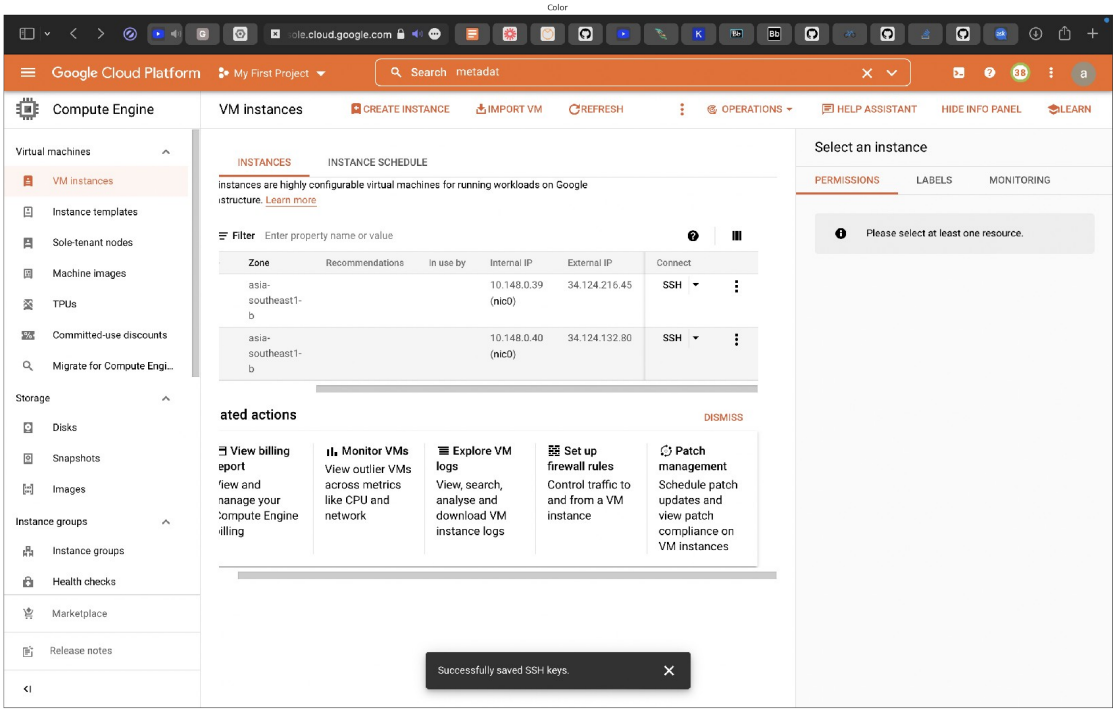
Unfortunately, this was extremely difficult to do on the cloud VM, I had to do quite a bit of workaround by editing on the GCP cloud VM interface and on the VMs to get ssh to work. GCP is a pain to work with!

Steps:

Edit ssh_config to allow PasswordAuthentication and Challenge

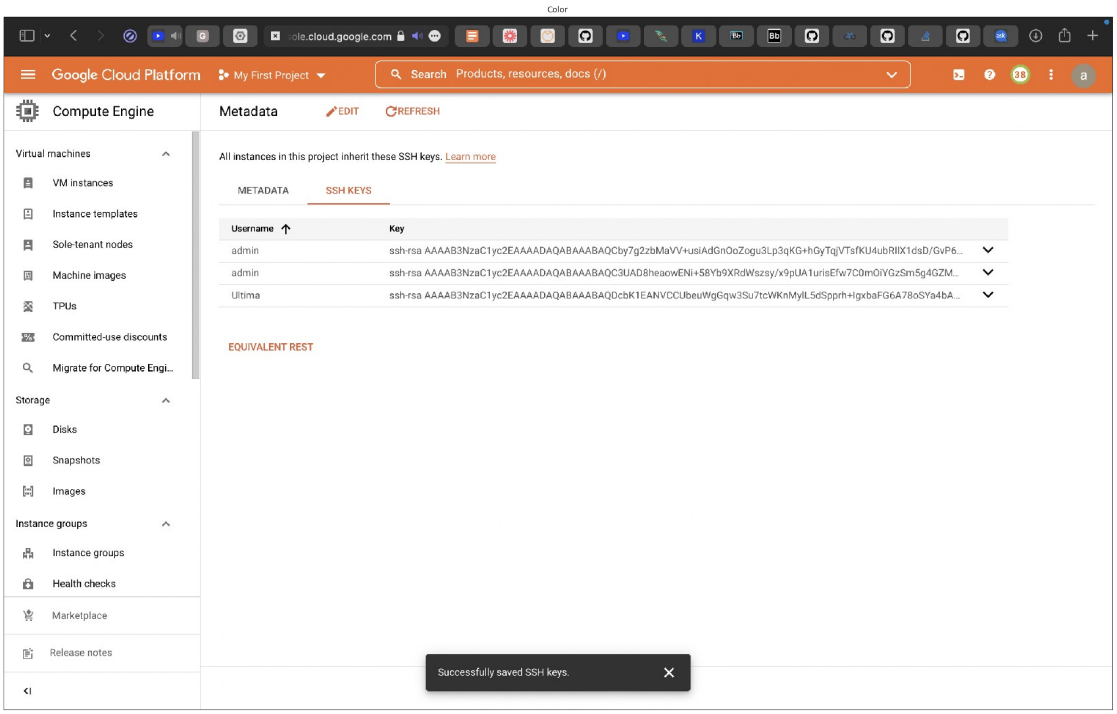
```
show_img('Task 3a/setup/awesome_vms.png')
show_img('Task 3a/setup/ssh_config.png')
show_img('Task 3a/setup/sshkey_setup.png')
```

Color

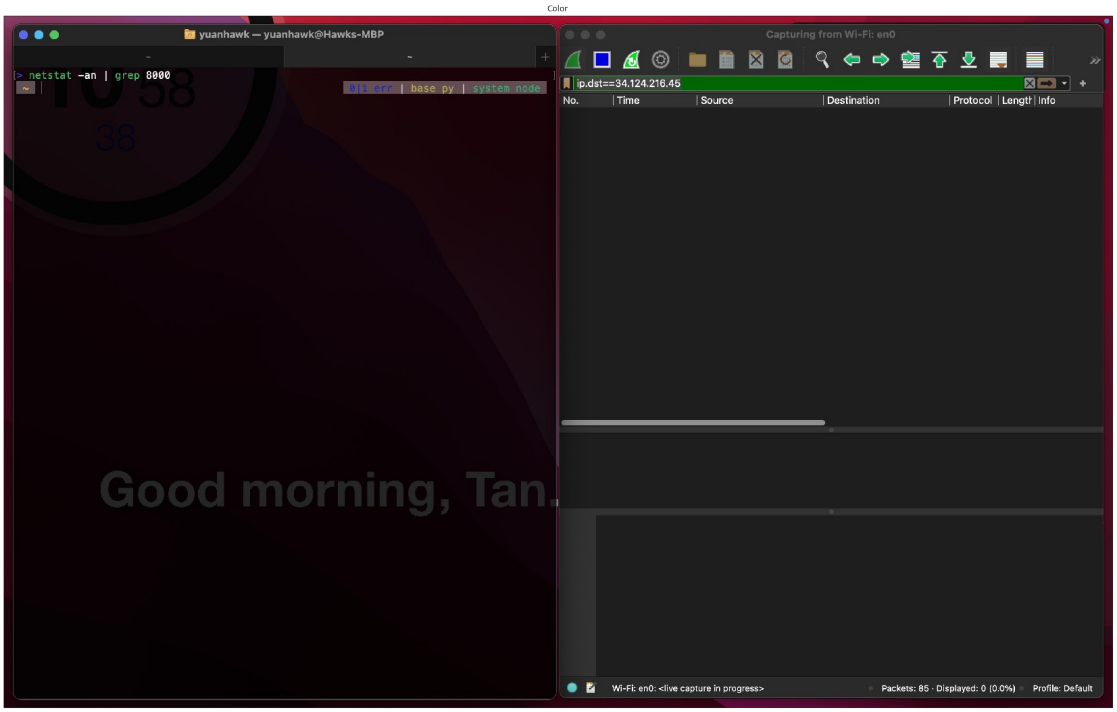

Google Cloud Platform
My First Project
Search metadat
Compute Engine
VM instances
CREATE INSTANCE
IMPORT VM
REFRESH
OPERATIONS
HELP ASSISTANT
HIDE INFO PANEL
LEARN
Virtual machines
VM instances
Instance templates
Sole-tenant nodes
Machine images
TPUs
Committed-use discounts
Migrate for Compute Engi...
Storage
Disks
Snapshots
Images
Instance groups
Instance groups
Health checks
Marketplace
Release notes
INSTANCES
INSTANCE SCHEDULE
Instances are highly configurable virtual machines for running workloads on Google
nfrastructure. Learn more
Filter Enter property name or value
Zone
Recommendations
In use by
Internal IP
External IP
Connect
asia-southeast1-b
10.148.0.39 (nic0)
34.124.216.45
SSH
asia-southeast1-b
10.148.0.40 (nic0)
34.124.132.80
SSH
ated actions
DISMISS
View billing eport
iew and anage your ompute Engine illing
Monitor VMs
View outlier VMs across metrics like CPU and network
Explore VM logs
View, search, analyse and download VM instance logs
Set up firewall rules
Control traffic to and from a VM instance
Patch management
Schedule patch updates and view patch compliance on VM instances
Select an instance
PERMISSIONS
LABELS
MONITORING
Please select at least one resource.
Successfully saved SSH keys.

Color

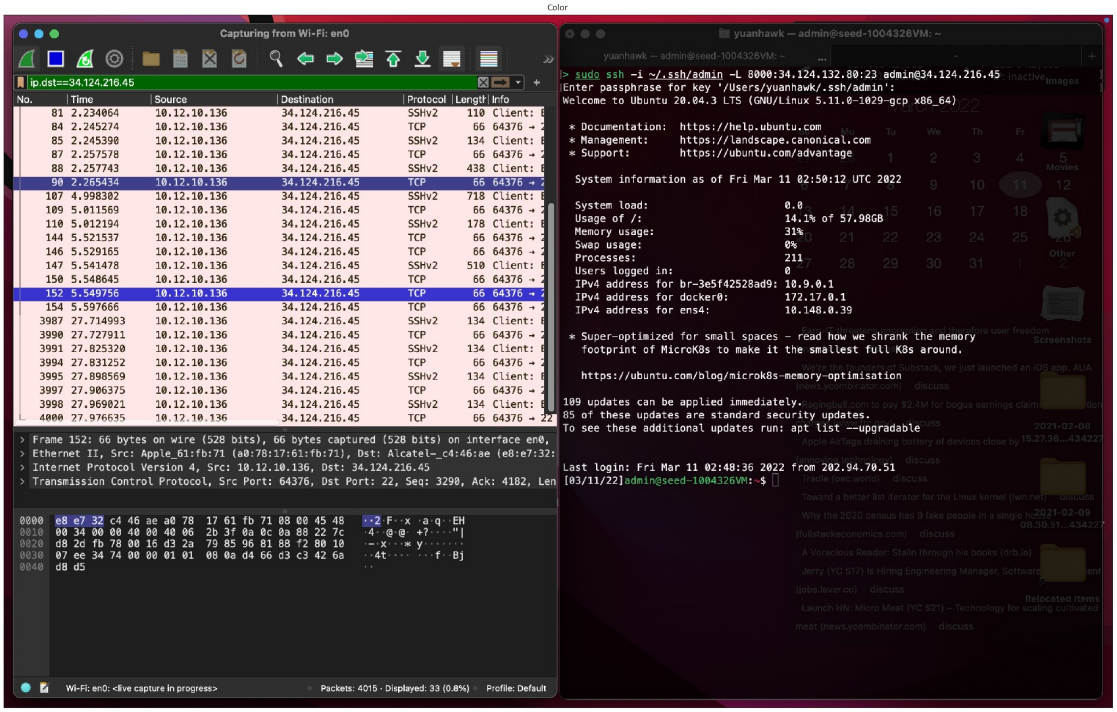

Activities
Terminal
Mar 11 01:26
admin@seed-1004326VM: ~
GNU nano 4.8
/etc/ssh/ssh_config
Site-wide defaults for some commonly used options. For a comprehensive
list of available options, their meanings and defaults, please see the
ssh_config(5) man page.
Include /etc/ssh/ssh_config.d/*.conf
Host *
ForwardAgent no
ForwardX11 no
ForwardX11Trusted yes
PasswordAuthentication yes
HostbasedAuthentication no
GSSAPIAuthentication no
GSSAPIDelegateCredentials no
GSSAPIKeyExchange no
GSSAPITrustDNS no
BatchMode no
CheckHostIP yes
AddressFamily any
ConnectTimeout 0
StrictHostKeyChecking ask
IdentityFile ~/.ssh/id_rsa
IdentityFile ~/.ssh/id_dsa
IdentityFile ~/.ssh/id_ecdsa
IdentityFile ~/.ssh/id_ed25519
Port 22
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
MACs hmac-md5,hmac-sha1,umac-64@openssh.com
EscapeChar ~
Tunnel no
TunnelDevice any:any
PermitLocalCommand no
VisualHostKey no
ProxyCommand ssh -q -W %h:%p gateway.example.com
RekeyLimit 1G 1h
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
ChallengeResponseAuthentication no
[Wrote 53 lines]
^G Get Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut Text
^U Paste Text
^J Justify
^T To Spell
^C Cur Pos
^_ Go To Line
M-U Undo
M-E Redo
M-A Mark Text
M-6 Copy Text
M-] To Bracket
^Q Where Was



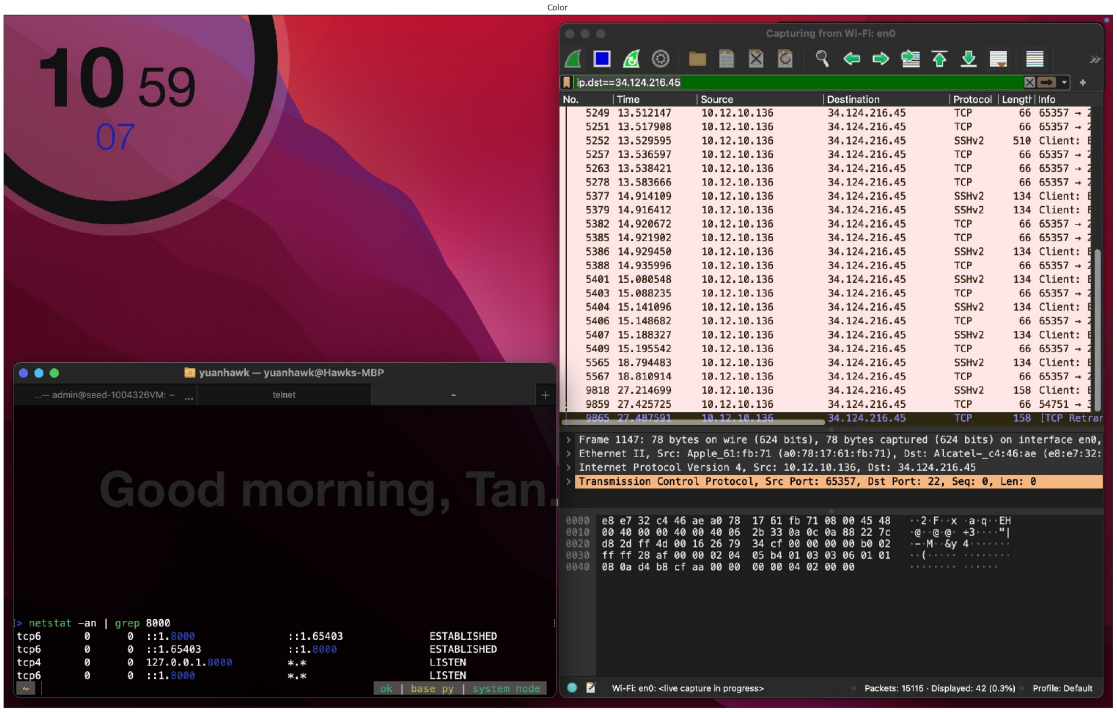

```
show_img('Task 3a/check_8000_is_empty.png')
show_img('Task 3a/ssh_tunnel.png')
show_img('Task 3a/check_8000.png')
show_img('Task 3a/wireshark_8000.png')
```

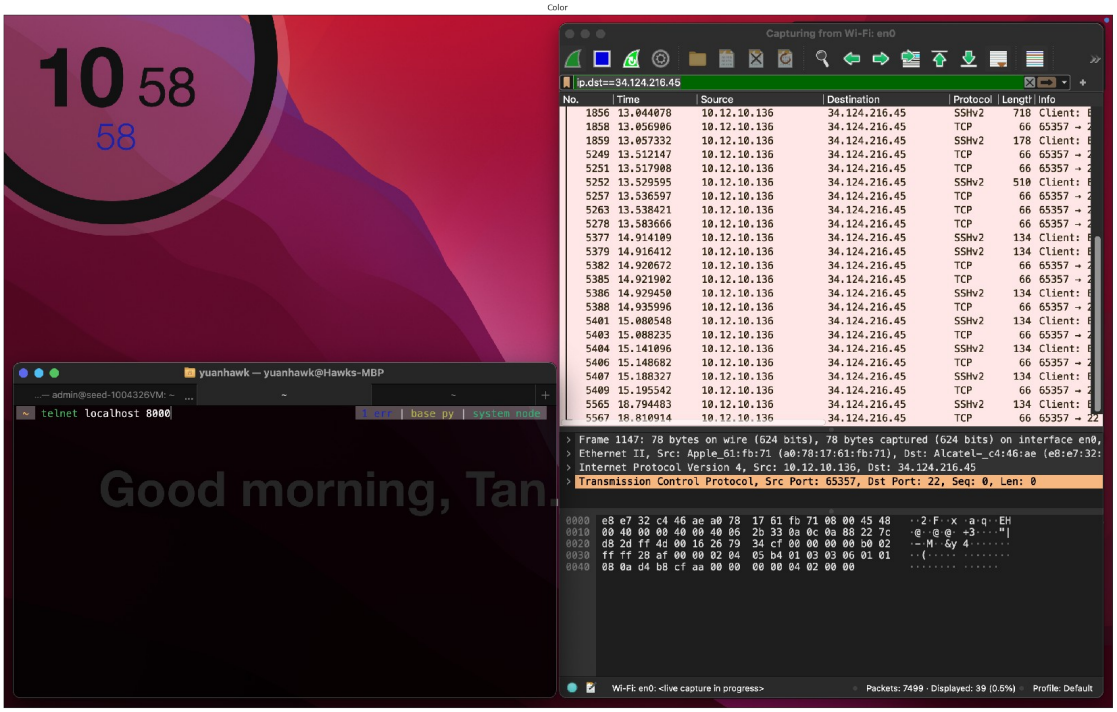


Color


Capturing from Wi-Fi: en0
ip.dst==34.124.216.45
No. Time Source Destination Protocol Length Info
81 2.234064 10.12.10.136 34.124.216.45 SSHv2 110 Client: E
84 2.245274 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
85 2.245398 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
87 2.257578 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
88 2.257743 10.12.10.136 34.124.216.45 SSHv2 438 Client: E
90 2.265434 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
107 4.998302 10.12.10.136 34.124.216.45 SSHv2 718 Client: E
109 5.011569 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
110 5.012194 10.12.10.136 34.124.216.45 SSHv2 178 Client: E
144 5.521537 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
146 5.529165 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
147 5.541478 10.12.10.136 34.124.216.45 SSHv2 510 Client: E
150 5.548645 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
152 5.549756 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
154 5.597666 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
3987 27.714993 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
3990 27.727911 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
3991 27.825320 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
3994 27.831252 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
3995 27.898569 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
3997 27.906375 10.12.10.136 34.124.216.45 TCP 66 64376 → 2
3998 27.969021 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
4000 27.976635 10.12.10.136 34.124.216.45 TCP 66 64376 → 22
Frame 152: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0,
Ethernet II, Src: Apple_61:fb:71 (a0:78:17:61:fb:71), Dst: Alcatel-_c4:46:ae (e8:e7:32:
Internet Protocol Version 4, Src: 10.12.10.136, Dst: 34.124.216.45
Transmission Control Protocol, Src Port: 64376, Dst Port: 22, Seq: 3290, Ack: 4182, Len
0000 e8 e7 32 c4 46 ae a0 78 17 61 fb 71 08 00 45 48
0010 00 34 00 00 40 00 40 06 2b 3f 0a 0c 0a 88 22 7c
0020 d8 2d fb 78 00 16 d3 2a 79 85 96 81 88 f2 80 10
0030 07 ee 34 74 00 00 01 01 08 0a d4 66 d3 c3 42 6a
0040 d8 d5
Wi-Fi: en0: <live capture in progress>
Packets: 4015 · Displayed: 33 (0.8%)
Profile: Default
yuanhawk — admin@seed-1004326VM: ~
sudo ssh -i ~/.ssh/admin -L 8000:34.124.132.80:23 admin@34.124.216.45
Enter passphrase for key '/Users/yuanhawk/.ssh/admin':
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1029-gcp x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Fri Mar 11 02:50:12 UTC 2022
System load: 0.0
Usage of /: 14.1% of 57.98GB
Memory usage: 31%
Swap usage: 0%
Processes: 211
Users logged in: 0
IPv4 address for br-3e5f42528ad9: 10.9.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for ens4: 10.148.0.39
* Super-optimized for small spaces - read how we shrank the memory
footprint of MicroK8s to make it the smallest full K8s around.
https://ubuntu.com/blog/microk8s-memory-optimisation
109 updates can be applied immediately.
85 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Last login: Fri Mar 11 02:48:36 2022 from 202.94.70.51
[03/11/22]admin@seed-1004326VM:~$

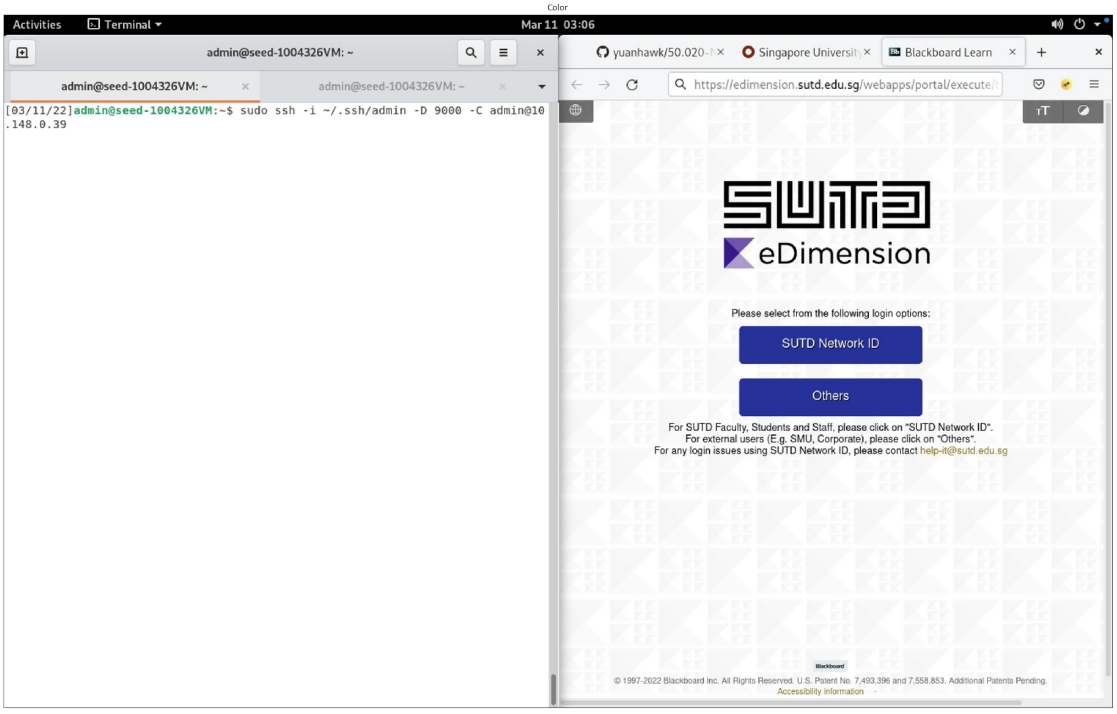
Color

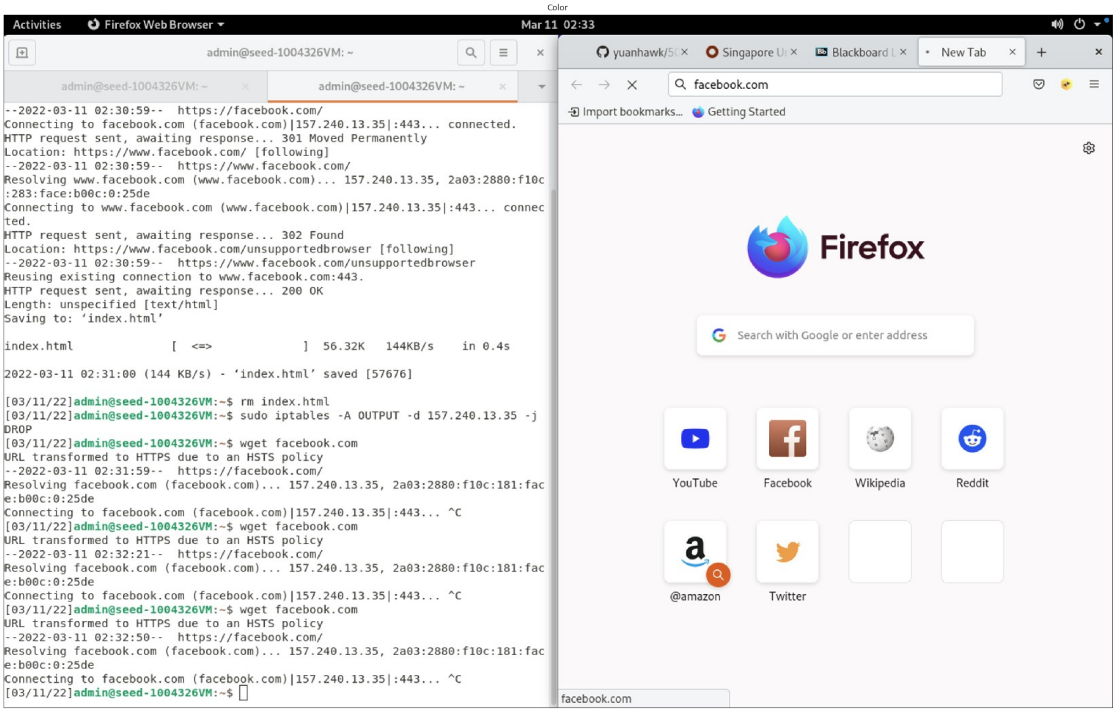

10 59
07
yuanhawk — yuanhawk@Hawks-MBP
admin@seed-1004326VM: ~
telnet
Good morning, Tan
netstat -an | grep 8000
tcp6 0 0 ::1.8000 ::1.65403 ESTABLISHED
tcp6 0 0 ::1.65403 ::1.8000 ESTABLISHED
tcp4 0 0 127.0.0.1.8000 *.* LISTEN
tcp6 0 0 ::1.8000 *.* LISTEN
ok | base py | system node
Capturing from Wi-Fi: en0
ip.dst==34.124.216.45
No. Time Source Destination Protocol Length Info
5249 13.512147 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5251 13.517908 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5252 13.529595 10.12.10.136 34.124.216.45 SSHv2 510 Client: E
5257 13.536597 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5263 13.538421 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5278 13.583666 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5377 14.914109 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5379 14.916412 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5382 14.920672 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5385 14.921902 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5386 14.929450 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5388 14.935996 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5401 15.080548 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5403 15.088235 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5404 15.141096 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5406 15.148682 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5407 15.188327 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5409 15.195542 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
5565 18.794483 10.12.10.136 34.124.216.45 SSHv2 134 Client: E
5567 18.810914 10.12.10.136 34.124.216.45 TCP 66 65357 → 2
9818 27.214699 10.12.10.136 34.124.216.45 SSHv2 158 Client: E
9859 27.425725 10.12.10.136 34.124.216.45 TCP 66 54751 → 3
9865 27.487591 10.12.10.136 34.124.216.45 TCP 158 [TCP Retrar
Frame 1147: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0,
Ethernet II, Src: Apple_61:fb:71 (a0:78:17:61:fb:71), Dst: Alcatel-_c4:46:ae (e8:e7:32:
Internet Protocol Version 4, Src: 10.12.10.136, Dst: 34.124.216.45
Transmission Control Protocol, Src Port: 65357, Dst Port: 22, Seq: 0, Len: 0
0000 e8 e7 32 c4 46 ae a0 78 17 61 fb 71 08 00 45 48
0010 00 40 00 00 40 00 40 06 2b 33 0a 0c 0a 88 22 7c
0020 d8 2d ff 4d 00 16 26 79 34 cf 00 00 00 00 b0 02
0030 ff ff 28 af 00 00 02 04 05 b4 01 03 03 06 01 01
0040 08 0a d4 b8 cf aa 00 00 00 00 04 02 00 00
Wi-Fi: en0: <live capture in progress>
Packets: 15115 · Displayed: 42 (0.3%)
Profile: Default

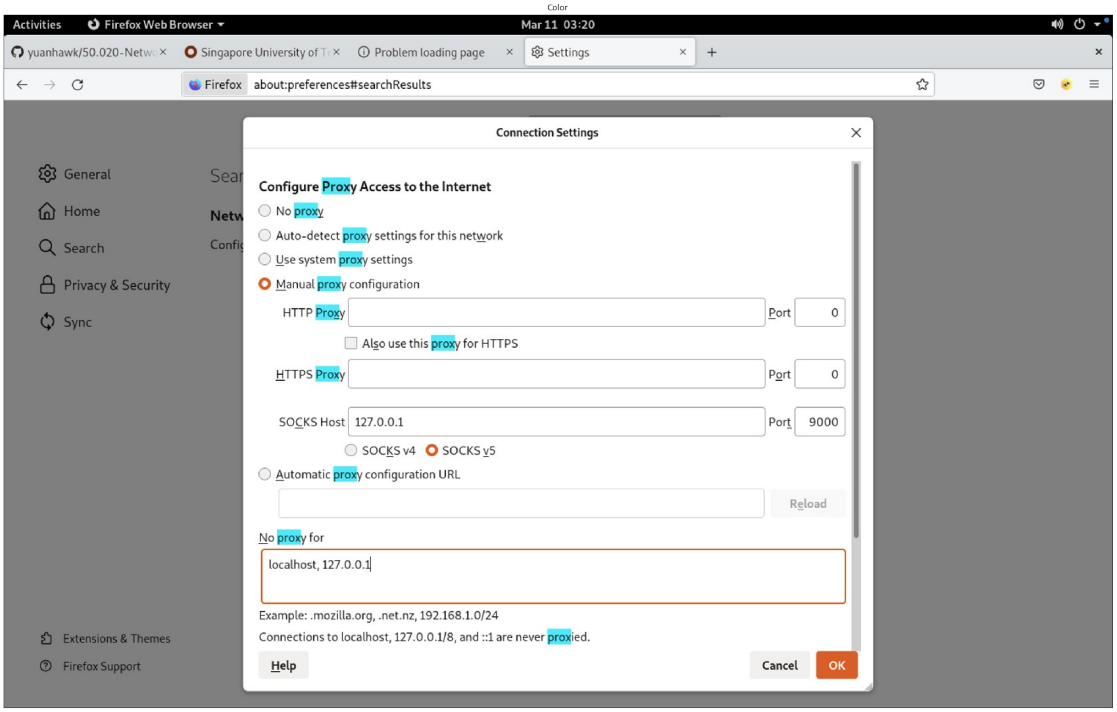


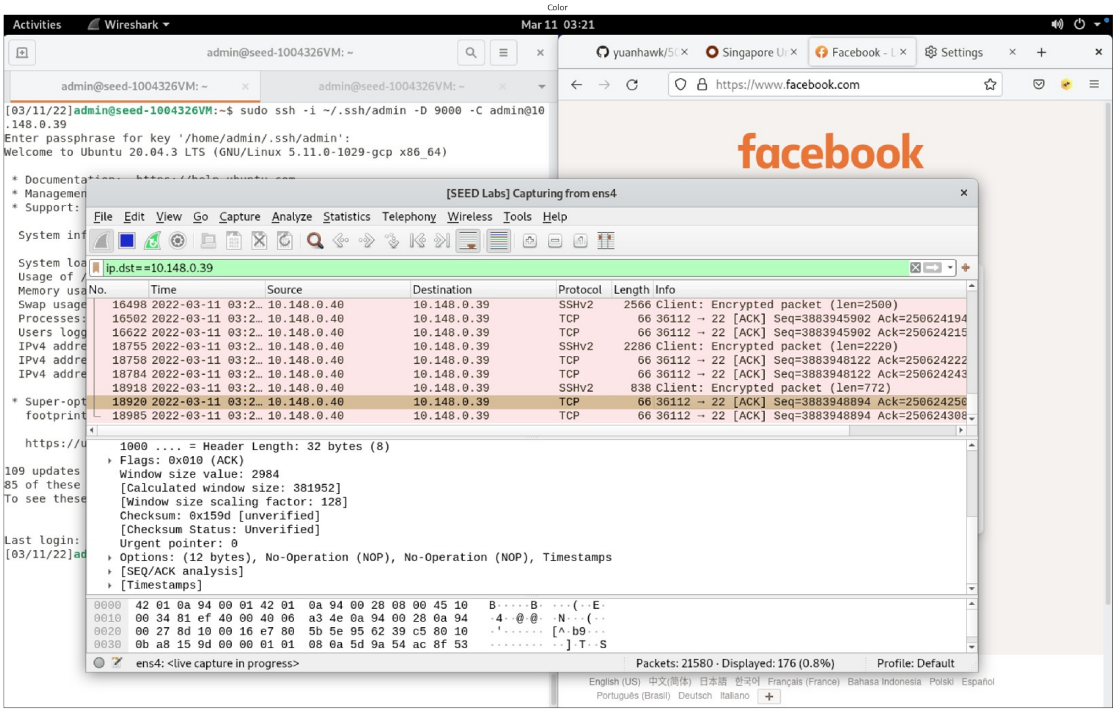
Task 3b: Connect to Facebook using SSH Tunnel

```
show_img('Task 3b/ssh_tunnel.png')
show_img('Task 3b/facebook_blocked.png')
show_img('Task 3b/config_socks.png')
show_img('Task 3b/wireshark_facebook.png')
```




Color
Activities
Firefox Web Browser
Mar 11 02:33
admin@seed-1004326VM: ~
admin@seed-1004326VM: ~
admin@seed-1004326VM: ~
--2022-03-11 02:30:59-- https://facebook.com/
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.facebook.com/ [following]
--2022-03-11 02:30:59-- https://www.facebook.com/
Resolving www.facebook.com (www.facebook.com)... 157.240.13.35, 2a03:2880:f10c
:283:face:b00c:0:25de
Connecting to www.facebook.com (www.facebook.com)|157.240.13.35|:443... connec
ted.
HTTP request sent, awaiting response... 302 Found
Location: https://www.facebook.com/unsupportedbrowser [following]
--2022-03-11 02:30:59-- https://www.facebook.com/unsupportedbrowser
Reusing existing connection to www.facebook.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'
index.html [<=>] 56.32K 144KB/s in 0.4s
2022-03-11 02:31:00 (144 KB/s) - 'index.html' saved [57676]
[03/11/22]admin@seed-1004326VM:~$ rm index.html
[03/11/22]admin@seed-1004326VM:~$ sudo iptables -A OUTPUT -d 157.240.13.35 -j
DROP
[03/11/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-11 02:31:59-- https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:181:fac
e:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... ^C
[03/11/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-11 02:32:21-- https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:181:fac
e:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... ^C
[03/11/22]admin@seed-1004326VM:~$ wget facebook.com
URL transformed to HTTPS due to an HSTS policy
--2022-03-11 02:32:50-- https://facebook.com/
Resolving facebook.com (facebook.com)... 157.240.13.35, 2a03:2880:f10c:181:fac
e:b00c:0:25de
Connecting to facebook.com (facebook.com)|157.240.13.35|:443... ^C
[03/11/22]admin@seed-1004326VM:~$
New Tab
facebook.com
Import bookmarks...
Getting Started
Firefox
Search with Google or enter address
YouTube
Facebook
Wikipedia
Reddit
@amazon
Twitter
facebook.com


Color
Activities
Firefox Web Browser
Mar 11 03:20
Problem loading page
Settings
Firefox
about:preferences#searchResults
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
Port
0
Also use this proxy for HTTPS
HTTPS Proxy
Port
0
SOCKS Host
127.0.0.1
Port
9000
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Help
Cancel
OK



Task 4: Evading Ingress Filtering

This was the output, but I could not get it work fully unfortunately...

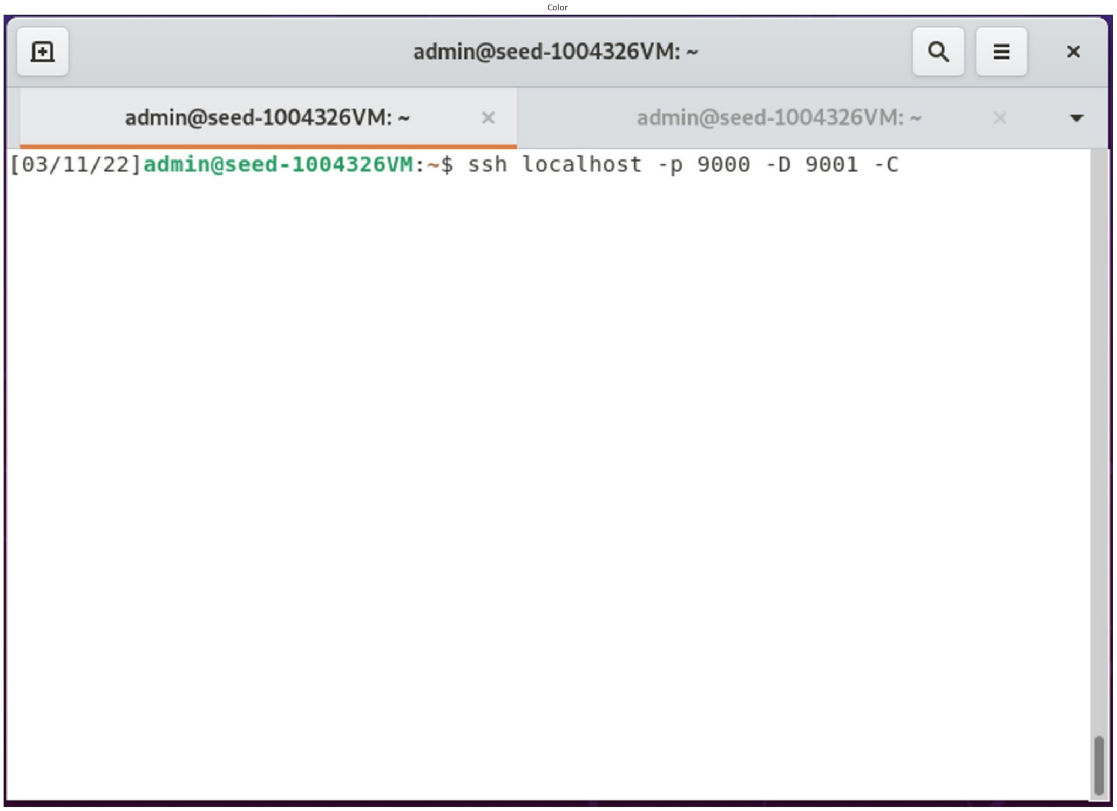
```
show_img('Task 4/drop_80_22.png')
show_img('Task 4/reverse_ssh_tunnel.png')
show_img('Task 4/connect_localhost.png')
show_img('Task 4/check_port_connect.png')
show_img('Task 4/connect_9001.png')
```

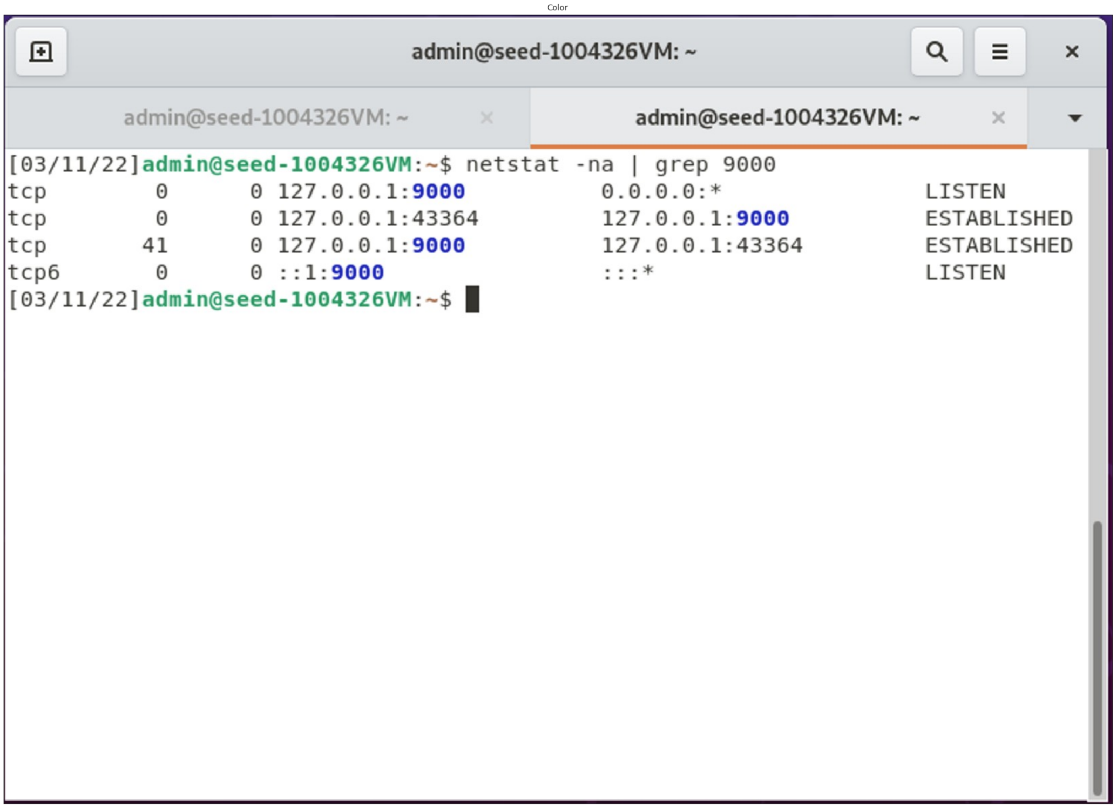
```
[03/11/22]admin@seed-1004326VM:~$ sudo iptables -A INPUT -p tcp --dport 80 -j
DROP
[03/11/22]admin@seed-1004326VM:~$ sudo iptables -A INPUT -p tcp --dport 22 -j
DROP
[03/11/22]admin@seed-1004326VM:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             edge-star-mini-shv-02-sin6.facebook.c
om
DROP       all  --  anywhere             edge-star-mini-shv-03-sin6.facebook.c
om

Chain DOCKER (0 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (0 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
target     prot opt source               destination

Chain DOCKER-USER (0 references)
target     prot opt source               destination
```

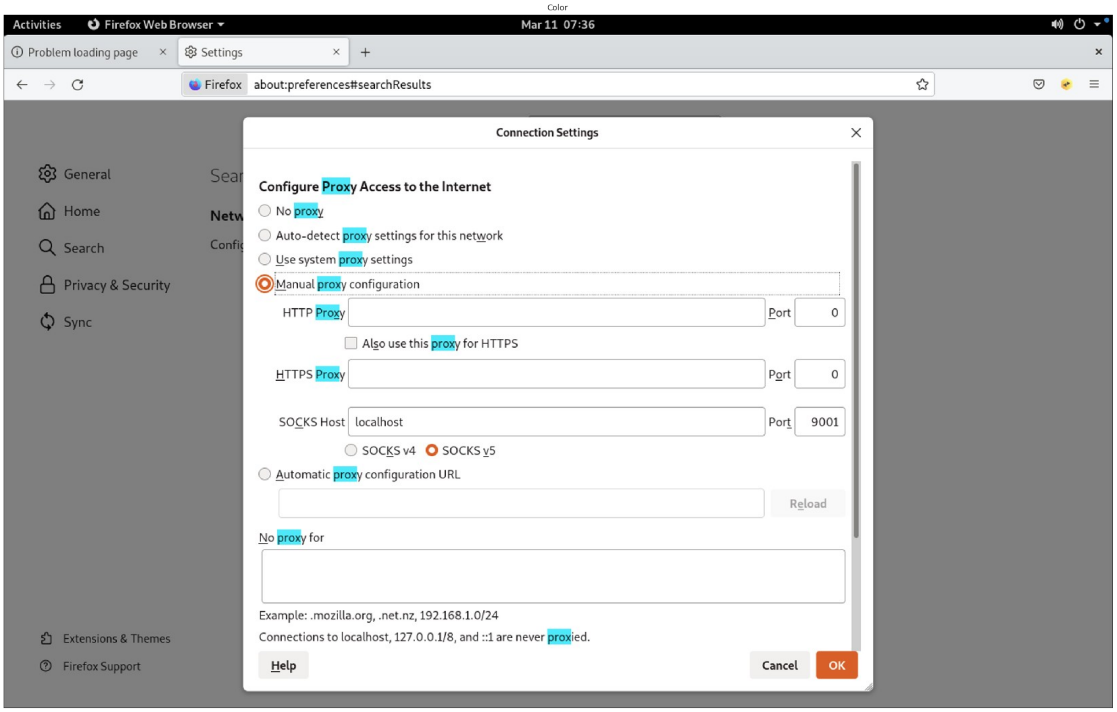
admin@seed-1004326VM: ~

admin@seed-1004326VM: ~ | admin@seed-1004326VM: ~

```
[03/11/22]admin@seed-1004326VM:~$ sudo ssh -i ~/.ssh/admin -R 9000:localhost:22
 admin@10.148.0.41 -N
Enter passphrase for key '/home/admin/.ssh/admin':
```


admin@seed-1004326VM: ~
admin@seed-1004326VM: ~
admin@seed-1004326VM: ~
[03/11/22]admin@seed-1004326VM:~$ ssh localhost -p 9000 -D 9001 -C


admin@seed-1004326VM: ~
admin@seed-1004326VM: ~
admin@seed-1004326VM: ~
[03/11/22]admin@seed-1004326VM:~$ netstat -na | grep 9000
tcp 0 0 127.0.0.1:9000 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:43364 127.0.0.1:9000 ESTABLISHED
tcp 41 0 127.0.0.1:9000 127.0.0.1:43364 ESTABLISHED
tcp6 0 0 ::1:9000 :::* LISTEN
[03/11/22]admin@seed-1004326VM:~$


Color
Activities
Firefox Web Browser
Mar 11 07:36
Problem loading page
Settings
Firefox
about:preferences#searchResults
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
Port
0
Also use this proxy for HTTPS
HTTPS Proxy
Port
0
SOCKS Host
localhost
Port
9001
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Help
Cancel
OK