Configuration Manual

MSc Research Project
Cloud Computing

Niharika Vashishtha
Student ID: x21153213

School of Computing
National College of Ireland

Supervisor: Aqeel Kazmi

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Niharika Vashishtha
Student ID:	x21153213
Programme:	Cloud Computing
Year:	2022
Module:	MSc Research Project
Supervisor:	Aqeel Kazmi
Submission Due Date:	01/02/2023
Project Title:	Configuration Manual
Word Count:	1712
Page Count:	12

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Niharika Vashishtha
Date:	29th January 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Niharika Vashishtha
x21153213

1 Software and Services requirement for this Research

This section give a preview of all the system requirement that will be required to perform the research. And those are given here.

- It is requires to have an AWS account to avail the EC2 services.
- EC2 Ubuntu instance with server spec 18.04 LTS as hosting environment for ubuntu antivirus.
- EC2 Windows instance with server spec Windows2016 as hosting environment for Windows antivirus.
- Ubuntu Antivirus
  - ClamAV
  - COMODO
  - F-PROT
  - Roothkit Hunter
  - Sophos

  In table 1 all the configuration requirements are mentioned for Ubuntu Antivirus.

Table 1: Ubuntu's Antivirus software configuration requirement

AntiVirus	Server Version	AMI	RAM	CPU	Version
ClamAV	Ubuntu 18.04 or higher	64-bit x-86 or 32 bit	3 GiB	1 CPU	0.103.6 /26734
COMODO	Ubuntu 16.04.2 or higher	64-bit x-86 or higher	284 MB	1 CPU	1
F-Prot	Ubuntu 16.04.2 or higher	64-bit x-86 or 32 bit	1GB	1 CPU	4.6.5.141
RootkitHunter	Ubuntu 18 LTS or higher	64-bit x-86 or 32 bit	1 GB	1 CPU	1.4.6
Sophos	Ubuntu 18 LTS or higher	64-bit x-86 or 32 bit	2 GB	1 CPU	9.12.1 /2600654

- Windows Server Antivirus
  - ClamWin

  - ScanGuard
  - TotalAV
  - VIRUSfighter
  - Windows Defender

  In table 2 all the configuration requirements are mentioned for Window's Server Antivirus.

Table 2: Window's Antivirus software configuration requirement

AntiVirus	Server Version	AMI	RAM	HardDisk	File Size	Version
ClamWin	Window Server 2003 or higher	64-bit x-86 or 32 bit	512 MB	512 MB	231MB	0.103.2.1
ScanGuard	Windows7 or higher	64-bit x-86	2 GB	800 MB or higher	55.6 MB	5.19.15.0
TotalAV	Windows7 or higher	64-bit x-86	2 GB	800 MB or higher	55.6 MB	5.19.15.0
VIRUSfighter	Window Server 2008 or higher	64-bit x-86 or 32 bit	128 MB	15 MB	2.30 MB	7.5.174
Windows Defender	Window Server 2008 or higher	64-bit x-86 or 32 bit	1GB	1 GB	115MB	1.379. 1039.0

- Cloud Watch to monitor

2 Setting Ubuntu EC2 Instance

Starting from taking EC2 instance details of configuring the Ubuntu EC2 instance are as below Services (2022a)

- Go to AWS and from side menu where services are given select new instance from intstance tab, instance window will open and then select launch instance button available in the right end corner a new launch instance window will appear there name and give tag to the instance

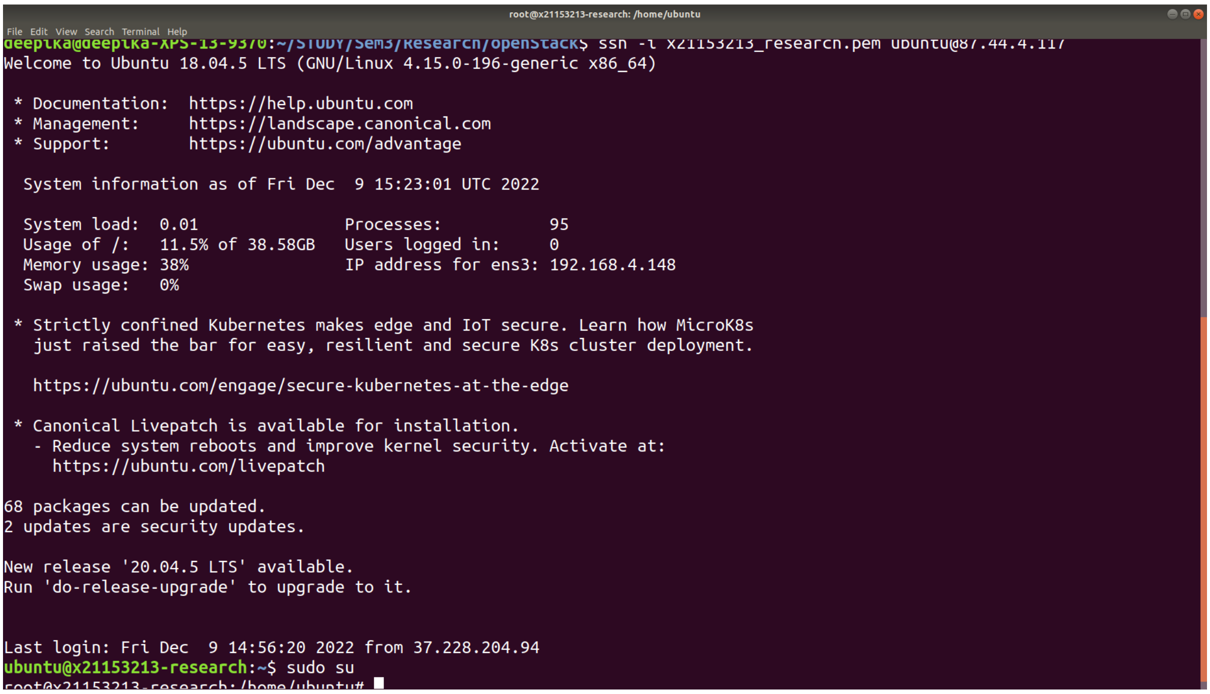
- Select OS images from available option, type the image name in this case type ubuntu the AMI for ubuntu will appear, and then select your choice, Ubuntu Server 18.04 LTS (HVM), SSD Volume Type ami-07cd20392675b2b83 (64-bit (x86)) was selected for this research.

  - Generate a key pair if do not have already or provide a name if have already

  - Create a security group with network settings

  - Configure storage and launch instance, after sometime launch started running.

- Connect to the instance using the with generated keypair using ssh. the exact command will appear in connect window when connect button is pressed in instance window, there select SSH Client and command will appear to connect through SSH Figure1 is showing the connecting process using command prompt. Go to the directory path through command prompt where pem file is located and type
  ssh -i "keypairFileName.pem" ec2-user@public-ip.compute.amazonaws.com



root@x21153213-research: /home/ubuntu
File Edit View Search Terminal Help

```
deepika@deepika-XPS-13-9370:~/STUDY/Sem3/Research/openstack$ ssh -i x21153213_research.pem ubuntu@87.44.4.117
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-196-generic x86_64)

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

  System information as of Fri Dec  9 15:23:01 UTC 2022

  System load:  0.01               Processes:           95
  Usage of /:   11.5% of 38.58GB   Users logged in:     0
  Memory usage: 38%                IP address for ens3: 192.168.4.148
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

68 packages can be updated.
2 updates are security updates.

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Fri Dec  9 14:56:20 2022 from 37.228.204.94
ubuntu@x21153213-research:~$ sudo su
root@x21153213-research:/home/ubuntu#
```

Figure 1: Connecting EC2 Ubuntu instance using Command prompt

- Take a privilged by using sudo su and start by installing antivirus.
- Copy sample virus data from local to the directory into the EC2 using below command in the local machine.

```
$ scp -i "pemfile.pem" VirusSmaples/Samples.zip
    ubuntu@87.44.4.117:/tmp
```

- After copy from local system to temporary folder of EC2 named tmp, move it from there to any other location in the EC2. using below command.

```
/tmp# mv Samples.zip /home/ubuntu/virus
```

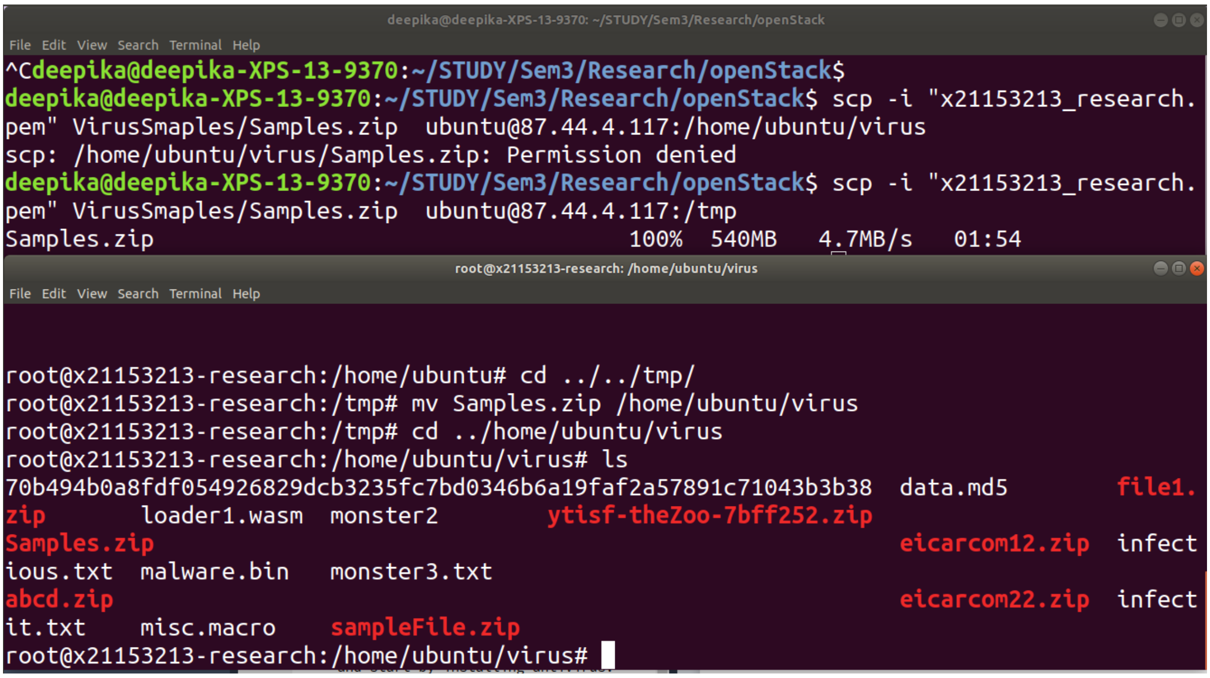
In the below Figure 2 is showing a view of transfer of files.

3 Installing and testing using ClamAV

To install ClamAv in EC2 ubuntu instance follow below given commands. The clamav official website provided documentation for installation and other help.Clamav (1988)

- Update the server using

```
$ sudo apt update
```


deepika@deepika-XPS-13-9370: ~/STUDY/Sem3/Research/openStack
File Edit View Search Terminal Help

```
^Cdeepika@deepika-XPS-13-9370:~/STUDY/Sem3/Research/openStack$
deepika@deepika-XPS-13-9370:~/STUDY/Sem3/Research/openStack$ scp -i "x21153213_research.
pem" VirusSmaples/Samples.zip  ubuntu@87.44.4.117:/home/ubuntu/virus
scp: /home/ubuntu/virus/Samples.zip: Permission denied
deepika@deepika-XPS-13-9370:~/STUDY/Sem3/Research/openStack$ scp -i "x21153213_research.
pem" VirusSmaples/Samples.zip  ubuntu@87.44.4.117:/tmp
Samples.zip                                   100%   540MB    4.7MB/s    01:54
```

root@x21153213-research: /home/ubuntu/virus
File Edit View Search Terminal Help

```
root@x21153213-research:/home/ubuntu# cd ../../tmp/
root@x21153213-research:/tmp# mv Samples.zip /home/ubuntu/virus
root@x21153213-research:/tmp# cd ../home/ubuntu/virus
root@x21153213-research:/home/ubuntu/virus# ls
70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38  data.md5       file1.
zip       loader1.wasm  monster2       ytisf-theZoo-7bff252.zip
Samples.zip                                                       eicarcom12.zip  infect
ious.txt  malware.bin   monster3.txt
abcd.zip                                                          eicarcom22.zip  infect
it.txt    misc.macro    sampleFile.zip
root@x21153213-research:/home/ubuntu/virus# 
```

Figure 2: Copying Virus file from local to EC2

- Install clamav using

```
$ sudo apt-get install clamav clamav-daemon -y
```

- To check version

```
$ clamscan -v
```

- More command can be checked using

```
$ clamscan -h
```

- After installation first need to update the clamAV Virus signature database, to do so, first stop ClamAV

```
$ sudo systemctl stop clamav-freshclam
```

- Now update signature databse manually running the command

```
$ sudo freshclam
```

- Restart the calmav process and then start scanning

```
$sudo systemctl start clamav-freshclam
```

- To scan and move infected files from scanned directory to quarantine directory

  ```
  $ clamscan -r --move=/home/ubuntu/Virus /home/qurantine
  ```

  -r is used to scan recursively all the directories and subdirectories will be scanned.

- To remove infected files

  ```
  $ clamscan -r --remove /home/ubuntu/Virus
  ```

  all the infected files found in the scan will be removed.

4 Sophos

Download the free Sophos antivirus from Sophos Official Website [1] and save it to a directory.

- Open ubuntu terminal in local and copy the downloaded zip folder to temporary forlder in the ec2 using. Maurya (2019)

  ```
  /STUDY/Sem3/Research/openStack/VirusSmaples$ scp -i "keypair_ec2.pem"
      SophosInstall.zip ubuntu@ip:/tmp/SophosInstall.zip
  ```

- Move this zip file from tmp folder to any other directory in ec2 terminal using below command.

  ```
  $ mv /tmp/SophosInstall.zip /home/ubuntu/antivirus/
  ```

  Unzip the file using unzip command (if unzip not installed then use sudo yum install unzip).

  ```
  $ unzip /home/ubuntu/antivirus//SophosInstall.zip
  ```

- Now change the directory and go to the Sophos using cd command.

  ```
  $ cd sophos-av
  ```

  Run installer using.

[1] https://www.sophos.com/en-us/free-tools

```
$ sudo sh ./install.sh
```

the License and Agreement has shown, go through it by using space bar and press Y when ask for the permission to install

Choose the location as /opt/sophps-av when asked for location and enter.

- On-access scanning should not be chosen as it will activate background scanning.
- The installation will ask to select for auto upadate of software, select s if want to update from sophos, o if want to update by your own and n if want no update. o was selected for this project.
- It will ask for free version installation or supported version, press f for free version enter and then press N to not access sohpos update.
- This will complete the installation. To check if installed successfully or not use command

  ```
  $ sudo /opt/sophos-av/bin/savdstatus
  ```

  Now scan can be start by using

  ```
  $ savscan /filepath
  ```

- To find more sophos commands use

  ```
  $ sudo /opt/sophos-av/bin/commands
  ```

5 Rootkit Hunter

Given command will be used to install check using RootkitHunter Jethva (2021).

- Start with updating ubuntu with latest available package

  ```
  $ apt-get update -y
  ```

- Install Rootkit Hunter using following command

  ```
  $ apt-get install rkhunter -y
  ```

- A postfix configuration box will come select local only and ok button. This will finish the installation. Now check the version using this command

  ```
  $ rkhunter --version
  ```

- To configure rkhunter to scan the system edit rkhunter.conf file

```
$ nano /etc/rkhunter.conf
```

in the configuration file change

```
UPDATE_MIRRORS=1
MIRRORS_MODE=0
WEB_CMD=""
```

save and close the config file

- To update the virus database

```
$ rkhunter --update
```

and to update the data files

```
$ rkhunter --propupd
```

- Finally the scan will start using

```
$ rkhunter --check
```

6 COMODO

To install Comodo on EC2 use below instructions.Kumar (2022)

/item First need to download the antivirus Package directly into the EC2

```
$ wget
    https://cdn.download.comodo.com/cis/download/installs/linux/cav-linux_x64.deb
```

- The antivirus program will need libssl that need to be installed

```
$ sudo apt install libssl1.1 -y
```

- Change directory using cd command to the downloaded directory where the antivirus is and run the following command

```
$ sudo dpkg -i cav-linux_x64.deb
```

- Run post installation script using this command

```
$ sudo /opt/COMODO/post_setup.sh
```

- To Scan the system first change directory to /opt/comodo and then scan using following command

```
$ /opt/COMODO/cmdscan -s /the/directory/needto/scan
```

7 F-Prot

- To install F-PROT antivirus follow below steps.Timme (2022)

  First copy the F-prot antivirus link location from F-prot official website[2], from the website choose linux version and copy the link location.

- Connect to the ec2 as super user and use command wget with the link location just copied.

```
$ wget https://files.f-prot.com/files/linux-x86/fp-linux-ws.deb
```

- Install package using

```
$ dpkg -i fp-linux-ws.deb
```

- Installed software can be used to scan the system or particular folder using these command.

```
$ fpscan -a /home/ubuntu/virus

 or

$ fpscan -a
```

8 Getting results

Performance Results of each antivirus can be get by following way.

- **Scanning Result stored in the log** The scanning results can be stored in a file and can be copied from EC2 to local to analyze later. Using command

```
$ scp -i "x21153213_research.pem"
    ubuntu@public/ip:/home/ubuntu/clamavlog.txt
    /home/deepika/STUDY/Sem3/Research/resultLog
```

- **Copying process log** To check the process log during the scanning use command in following way

  - Run this command in one terminal

```
       $while true; do ps -all --forest |tail -n 8 >>
           /home/ubuntu/ps.txt; date >> /home/ubuntu/ps.txt; sleep
           10; done
```

[2] http://www.f-prot.com/download/home_user/:

- in another terminal run process to scan like

```
        $ clamscan -r /home/ubuntu/virus
```

- copy the ps.txt saved in to /home/ubuntu to local using below command.

```
$ scp -i "x21153213_research.pem"
    ubuntu@public/ip:/home/ubuntu/ps.txt
    /home/deepika/STUDY/Sem3/Research/processLog
```

Do the same for each antivirus.

- **Installation Space** to check the installed packge size these commands are used Command for checking how much space is taking running into ec2
  - Installed package in machine

```
$ sudo dpkg-query -Wf '${Installed-size}\t${Package}\n' | column
    -t > spaceopt.txt
```

  - Space in one directory sudo du -sh /home/f-prot

9 Setting Window EC2 using AWS instances

To set up Windows EC2 instance need to follow following steps. Services (2022b)

- Go to AWS and from side menu where services are given select new instance from intstance tab, instance window will open and then select launch instance button available in the right end corner a new launch instance window will appear there name and give tag to the instance
- Select OS images from available option, type the image name, in this case type window the AMI for Windows will appear, and then select your choice, Window Server 2016 server, (64-bit (x86)), t2 micro with 1GiB memory and 1 vCPU was selected.

  - Generate a key pair if do not have already or provide a name if have already

  - Create a security group with network settings

  - Configure storage and launch instance, after sometime launch started running.
- Go to the running instances window, select your windows instance and press connect button and a connection window appear to connect, choose RDP client tab and there public DNS and User name is given, click on Get Password button, a separate window appear and ask for the private key file that generated or used when creating the instance. Upload that file and generate the password and saved it with care to use in next step.

- As I am using ubuntu system as a local machine the steps to connect the windows server with ubuntu machine as follow. I install Remmina tool to make connection with Windows EC2 instance.*How to install Remmina* (n.d.) To install use following steps.
  - first install a package flatpak

    ```
    $ flatpak run --filesystem=$SSH_AUTH_SOCK
        --env=SSH_AUTH_SOCK=$SSH_AUTH_SOCK org.remmina.Remmina
    ```

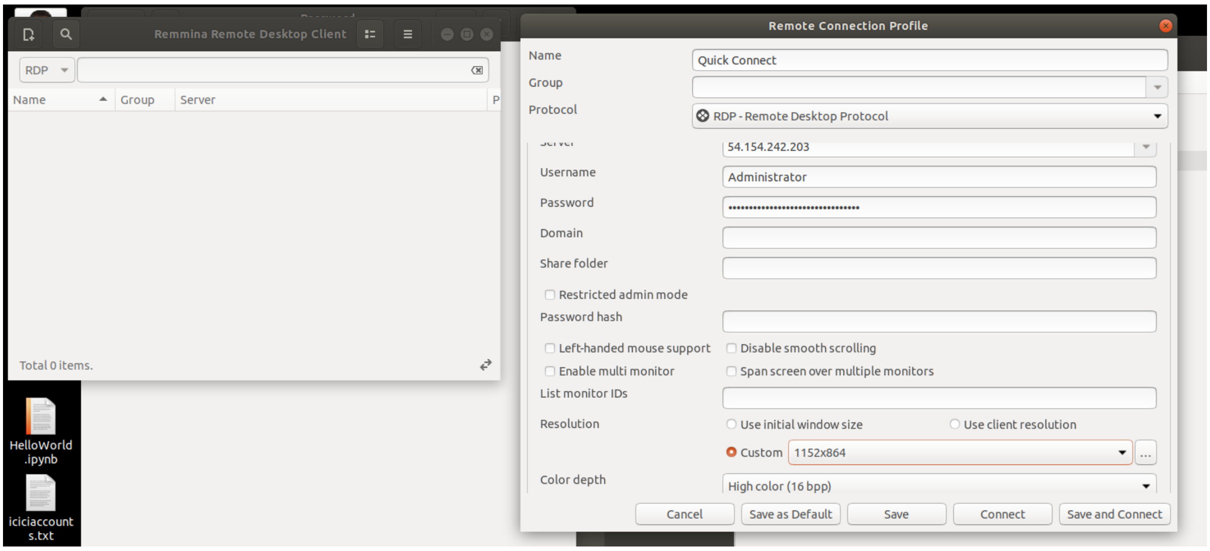
  - Now install remmina

    ```
    $ sudo snap install remmina --edge

    $ sudo snap refresh remmina --channel=edge # use --channel=stable
        otherwise

    $ sudo apt-add-repository ppa:remmina-ppa-team/remmina-next
    $ sudo apt update
    $ sudo apt install remmina remmina-plugin-rdp
        remmina-plugin-secret
    ```

  - After completing installation, open Remmina the GUI is available and select RDP and to connect press the + icon on top left corner a connection window will appear as shown in the Figure3



Name: Quick Connect
Group:
Protocol: RDP - Remote Desktop Protocol
Server: 54.154.242.203
Username: Administrator
Password: ••••••••••••••••••••••••••••••
Domain:
Share folder:
□ Restricted admin mode
Password hash:
□ Left-handed mouse support □ Disable smooth scrolling
□ Enable multi monitor □ Span screen over multiple monitors
List monitor IDs:
Resolution: ○ Use initial window size ○ Use client resolution
● Custom 1152x864
Color depth: High color (16 bpp)

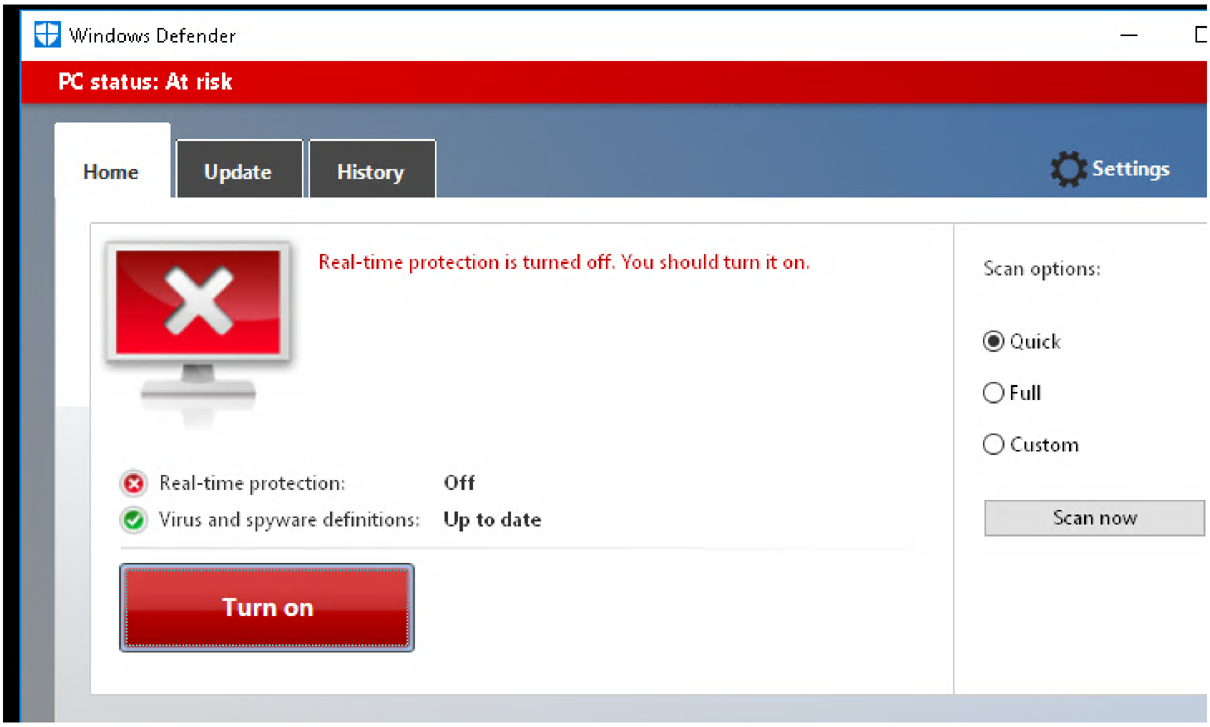
Figure 3: Connecting EC2 Window instance using Remmina

- In the Remote Connection Profile window give protocol name as RDP- Remote Desktop Protocol, in Server text box give public DNS, Username given in the EC2 instance connection window and give password that you generated in above stpes.

- Down in the Resolution field select custom and from drop down menu select 1152*864 and in Color depth choose High Color(16bpp).
- Click Save and Connect button the remote desktop window will appear which shows ec2 connection.

10 Installation of Antivirus

- After getting into the EC2 first deactivate window defender by searching in the start menu and select window defender and switch off every button like real time protection and web browser protection and cloud based protection.
- And started downloading the virus file and make a folder in the directory.
- Download each antivirus one by one.
- Start installing them one at a time. Figure 4 shows Window Defender screen after installation.



PC status: At risk

Real-time protection is turned off. You should turn it on.

Real-time protection: Off

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

Figure 4: Showing the Window Defender after starting the services

- Do the custom and full scan one by one.
- Take reading by going to task manager.
- Stop the scan and take the cloud watch log from AWS.

11 Collecting Cloud Watch Log

- To collect cloud watch log go to the instance created first in the drop-down menu there is some information about the instance.
- Select the monitoring tab.
- Select the CPU Usage log and go to view in metric.
- In metric window select the for the time period, like for each 5 mins or for each hour.
- aggregator functions can also be selected and label also.
- from the top tab, select the drop down menu and select download as csv.Services (2022c)

References

Clamav (1988). Clamav configuration, https://docs.clamav.net/. Accessed on 2022-10-20.

How to install Remmina (n.d.). https://remmina.org/how-to-install-remmina/. Accessed on 2022-11-1.

Jethva, H. (2021). Detect linux security holes and rootkits with rkhunter on ubuntu 20.04, https://www.atlantic.net/dedicated-server-hosting/detect-linux-security-holes-and-rootkits-with-rkhunter-on-ubuntu-20-04/. Accessed on 2022-10-25.

Kumar, L. (2022). How to install comodo antivirus on ubuntu linux, https://explorelinux.com/how-to-install-comodo-antivirus-on-ubuntu-linux/. Accessed on 2022-10-25.

Maurya, R. (2019). How to install sophos antivirus for linux (ubuntu/debian), https://www.how2shout.com/how-to/how-to-install-sophos-antivirus-for-linux.html. Accessed on 2022-10-25.

Services, A. W. (2022a). Amazon elastic compute cloud - user guide for linux instances, https://docs.aws.amazon.com/pdfs/AWSEC2/latest/UserGuide/ec2-ug.pdf#get-set-up-for-amazon-ec2. Accessed on 2022-10-18.

Services, A. W. (2022b). Aws codedeploy - user guide - launch a window server, https://docs.aws.amazon.com/codedeploy/latest/userguide/tutorials-windows-launch-instance.html. Accessed on 2022-11-01.

Services, A. W. (2022c). Cloudwatch tutorials, https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-tutorials.html. Accessed on 2022-10-22.

Timme, F. (2022). Virus protection with f-prot, https://www.howtoforge.com/f_prot_antivirus_ubuntu_feisty. Accessed on 2022-11-1.