

QRadar

<https://www.youtube.com/watch?v=tPCdBwoNgcM>

- **(Part-1)**

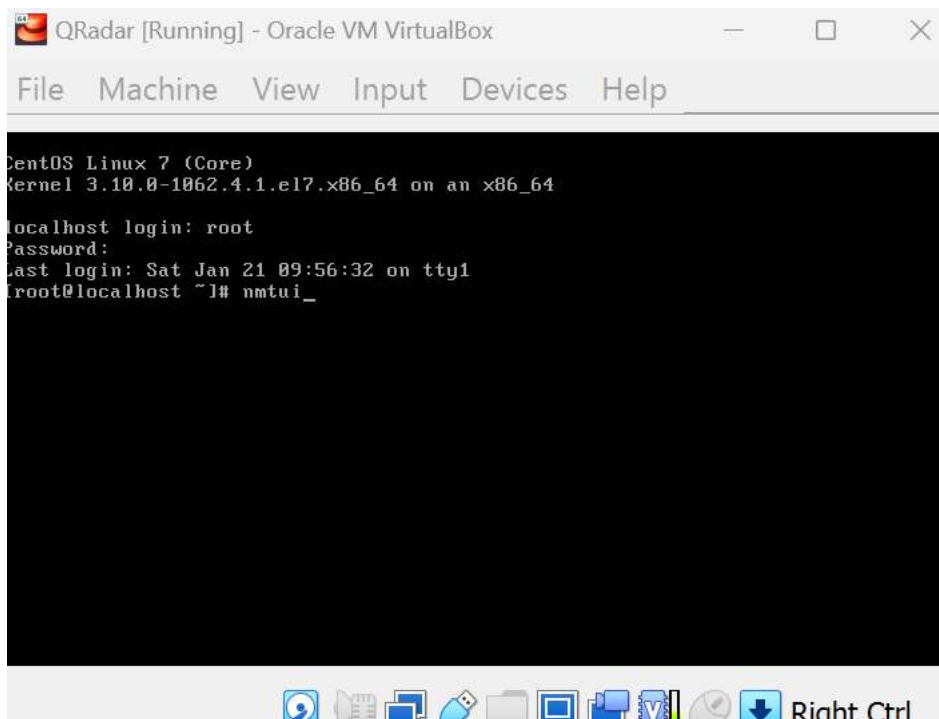
- 3,478 views Apr 5, 2022
 - This is the first video in a series of four videos. In this video, i have explained how you can download and install qradar community edition v7.3.3 on VM in Vmware Workstation and Oracle VM Virtual Box. Whether you are using Vmware Workstation or Oracle VM VirtualBox, other than importing the .ova file during installation that I have shown in the video all other steps remain the same. Download Qradar community Edition V7.3.3
<https://www.ibm.com/community/qradar/ce/>
-

- **Google qradar-**

<https://www.ibm.com/community/qradar/ce/>

-
- **Fill up given detail then Download**
QRadarCE733GA_v1_0.OVA – open virtual box - file – import appliance –in file add QRadarCE733GA_v1_0.OVA – next - give qradar name &10 gb ram –finish
-
- **Select qradr- settings – check in network–bridge adaptor-ok**
-
- **Start qradar- in local host login: root- set new pswd-**

-
- **root@localhost~1#-**
-
- **win cmd – ipconfig- wirelesslan adapter wi fi – ipv add, defaultgatewayip note down**
-
- **went to qradarvm root@localhost~1#- nmtui**



- **Edit a connection- enter**



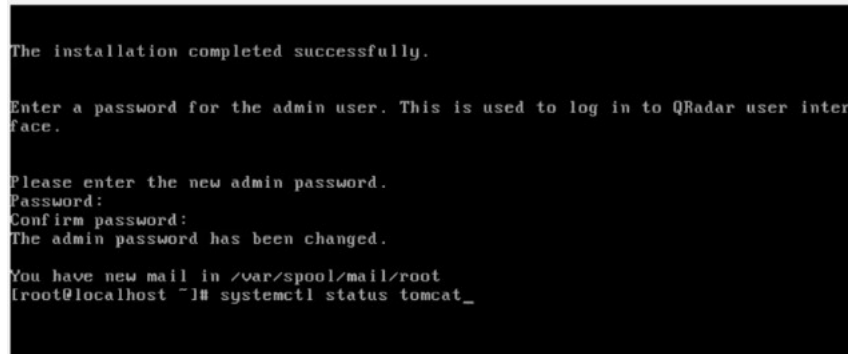
- **Network manager TUI**
- **Wired connection 1- edit**
- **Edit Profile name –enp0s17-**
- **Ipv configuration – manual- show-**
- **Address – write win pv4- host octet will change–**
- **gateway – write here gateway ip- same**
- **dns server- 8.8.8.8 - this is googleip/dns server**
- **ip v6 configuration – ignore - ok**
- **go back to c - set system hostname- qradar.tabby.com(fully qualified Doman name)-ok-ok**
- **network manager tui –activate connection- enp0s17- deactivate – activate -deactivate– back- quit**

- clear- root@localhost~1# ipaddr | less – output-q

Restart qradar

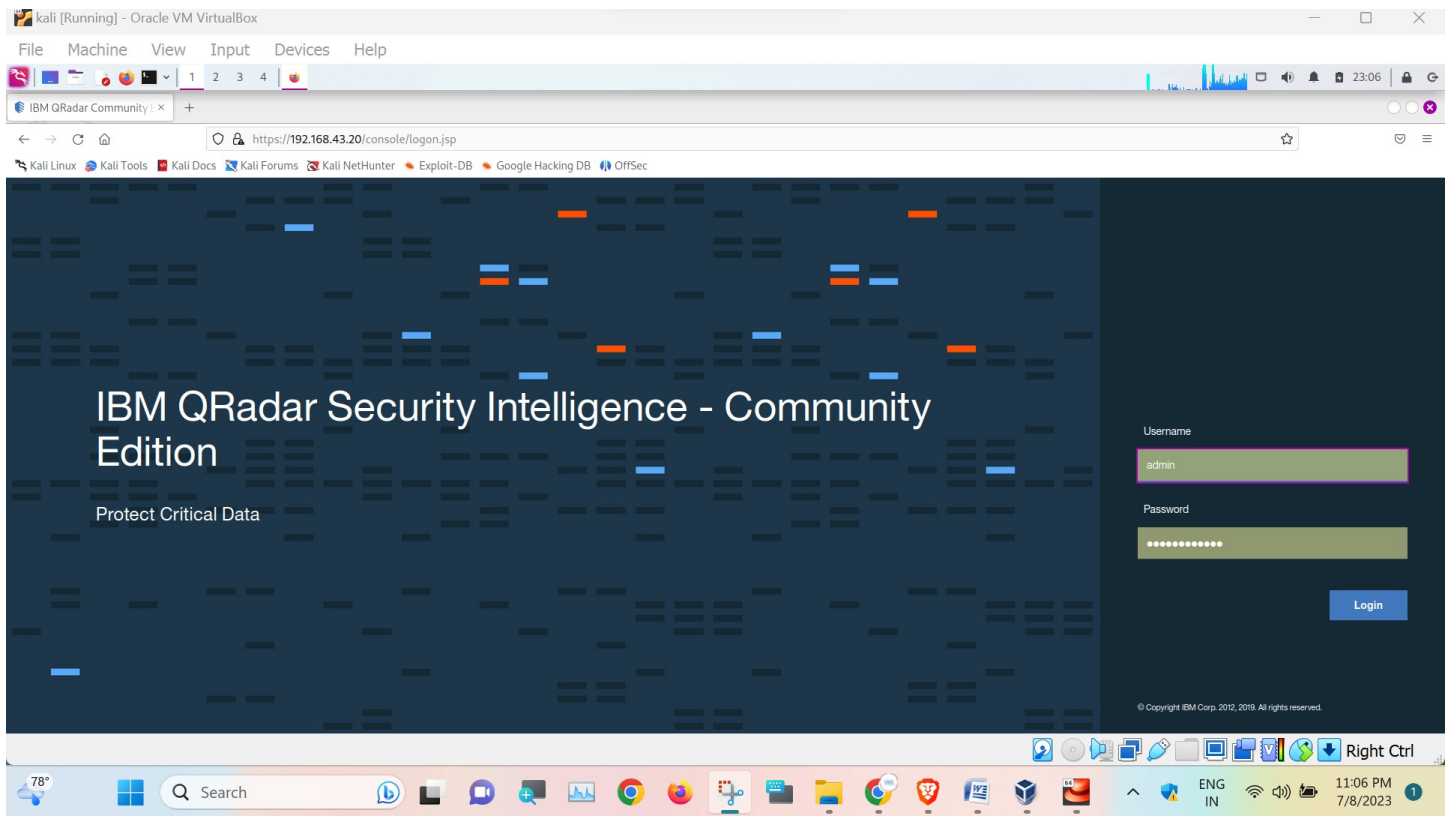
- root@localhost~1# ping 8.8.8.8 – output- ctrl Z
- root@localhost~1# ls – setup-
- root@localhost~1#- ./setup
- continue quite-enter
- space batten—again....
- (end) –press q – enter
- Continue y / n- y – enter- it will take time
- Installation started – take time-
- Installation completed successful
- Enter new admin password.
- Password (to access qradar interface)

- **Conform password- admin password change-**

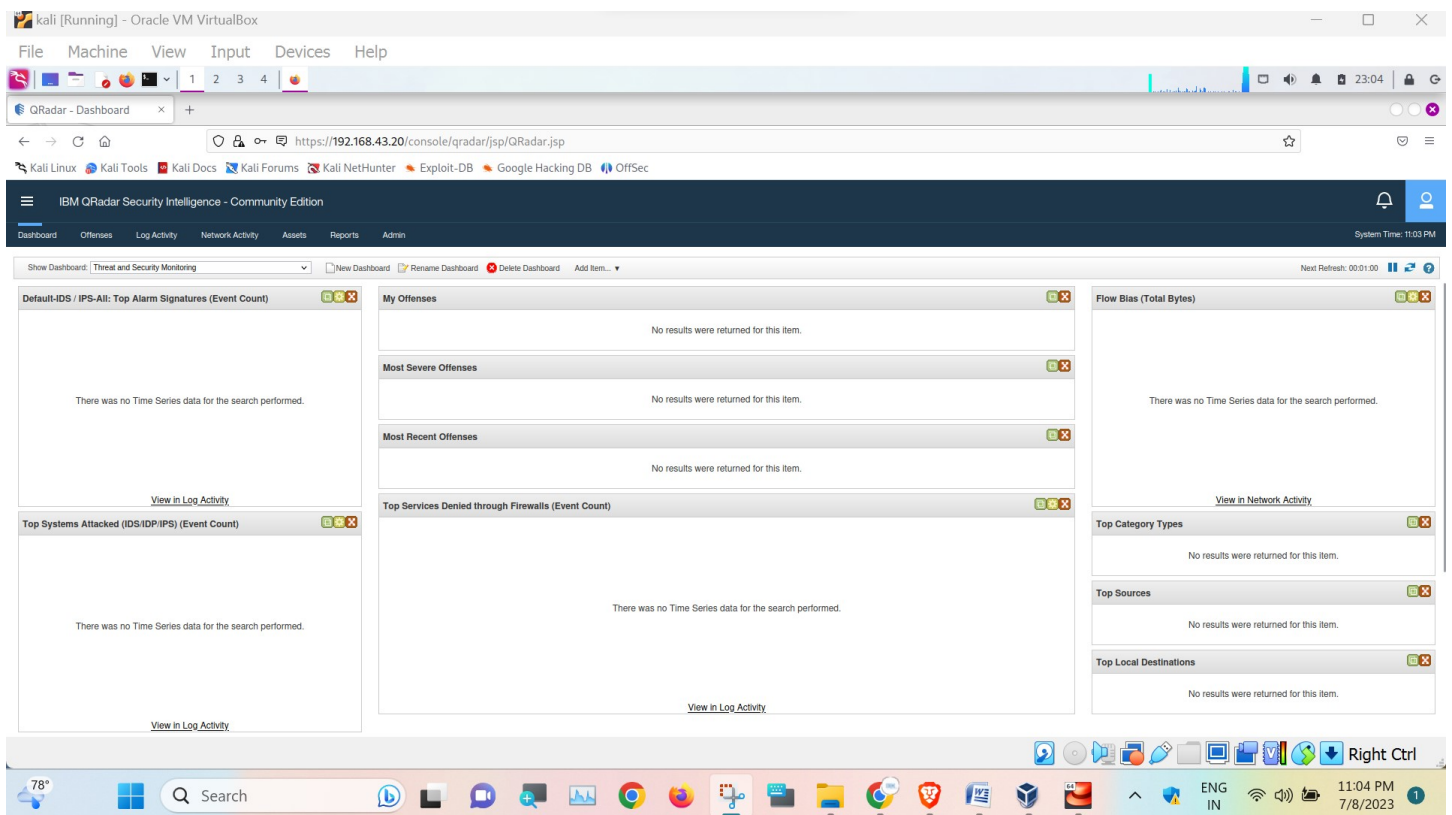


```
The installation completed successfully.  
  
Enter a password for the admin user. This is used to log in to QRadar user interface.  
  
Please enter the new admin password.  
Password:  
Confirm password:  
The admin password has been changed.  
  
You have new mail in /var/spool/mail/root  
[root@localhost ~]# systemctl status tomcat_
```

- **root@localhost~1# systemctl status tomcat- enter- running**
- **root@localhost~1# ipaddr | less –output given ip in nmtui -q**
- **root@localhost~1# ping with win ipv4 add**
- **open kali / ubuntu**
- **went to win browser- https//192.168.100.200- advance- proceed to 192.168.100.200 (unsafe)-accept security risk and proceed**
-
- **qradar interface appear- username- password**
- **accept licence**



- all empty need system configuration



-

<https://www.ibm.com/community/qradar/ce/>

- Admin- data source –
- Win search – winscp (use copy file win to linuxqradar)-
install winscp if not in win – host name – insert qradar,s
enp0s17 ip – user name root- password root pwd–login –
yes

- --- Search – win collect agent -[QRadar® 7.3 RPMs contained in the WinCollect SFS installer](#)

-

<https://www.youtube.com/watch?v=IwkEm772EZI>

- (Part-2)
- After installing the Qradar community edition, there is an issue with events not showing in the log activity tab. In this video, explained how you can resolve this issue. <https://youtu.be/tPCdBwoNgcM> (Qrdar CE installation || VMware Workstation || VirtualBox || Getting started with Qradar (Part 1)) <https://putty.org/> (Download putty) <https://www.ibm.com/community/qradar/ce/> Or use the link to access the document <https://www.ibm.com/support/pages/nod...>

This is in window

-open browser- [putty.org](https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html) – download putty-

- <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

- setup download then install-
- goqradar- type cmd- if config| (pai) less
- ip address note down of enp0s17 -
- open putty configuration -
- insert ip in [host name for ipaddr]
- port 22 – connection type SSH – OPEN
- in root @qradar - login: root, ipassword:
- right click on min.max.close bar- change setting-appearance-
- 16-color- foreground- red.0-green.255-blue.0
- Search in browser- ibmqradar community edition-re page
- click on red notice appear on screen –
- scroll down – procedure –

qradar console

(the all server command allow console appliance to update)[<https://www.ibm.com/community/qradar/ce/>] - [<https://www.ibm.com/support/pages/node/6395080>] -

```
[
1. if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "QRadar:Q1 Labs
2. Inc.:0007634bdale2:WnT9X7BDFOGBlWaXwokODc:12/31/20"> /opt/qradar/ecs/license.txt ; fi ;
1. if [ -f /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ] ; then echo
-n "QRadar:Q1 Labs Inc.:0007634bdale2:WnT9X7BDFOGBlWaXwokODc:12/31/20">
/opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/license.txt ; fi ; if [ -f
/opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1
Labs Inc.:0007634bdale2:WnT9X7BDFOGBlWaXwokODc:12/31/20"> /opt/ibm/si/services/ecs-
ep/current/eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bdale2:WnT9X7BDFOGBlWaXwokODc:12/31/20"> /opt/ibm/si/services/ecs-
ec/current/eventgnosis/license.txt ; fi ; if [ -f /usr/eventgnosis/ecs/license.txt ] ;
then echo -n "QRadar:Q1 Labs Inc.:0007634bdale2:WnT9X7BDFOGBlWaXwokODc:12/31/20">
/usr/eventgnosis/ecs/license.txt ; fi ; if [ -f
/opt/qradar/conf/templates/ecs_license.txt ] ; then echo -n "QRadar:Q1 Labs
Inc.:0007634bdale2:WnT9X7BDFOGBlWaXwokODc:12/31/20">
/opt/qradar/conf/templates/ecs_license.txt ; fi
]
```

- for QRadar community edition:- copy that- paste in putty
right mouse click hold shift + insert key or (category –
selection - in auto copy - ctrl+shift+c.v. - select clipboard)-
ctrl+shift+c.v -putty qradar console- enter –

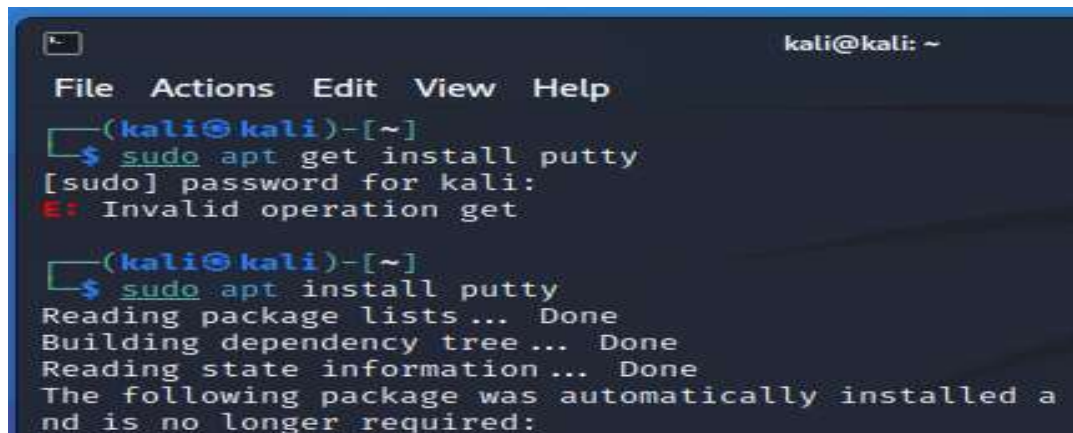
(than It will appear)

-

This is in Linux

- install putty (SSH and telnet client) in
ubuntu Linux

- open terminal
- sudo apt-get install putty



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt get install putty  
[sudo] password for kali:  
E: Invalid operation get  
  
(kali@kali)-[~]  
$ sudo apt install putty  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following package was automatically installed a  
nd is no longer required:
```

- pwd- y/n-y-enter-dash home-search putty-
-

<https://www.youtube.com/watch?v=mP6hX9gKvyY>

- (Part-3)

- Linux terminal- ipaddr
- Qradar - ping linuxip –
Root@kali- systemctl statusrsyslog.service
-systemctl statusrsyslog.service
-sudonano /etc/rsyslog.conf - enter – afterthis line-
\$includingconfig /etc/rsyslog.d/*.conf
- ‘.’ (send all log to) @(udp)if one more(tcp) qradarip (send to qradar) :514(port) – ctrl o - enter

- ‘.’@ qradar ip:514
- systemctl restartrsyslog.service- pswd

-qradar console on browser – log activities
- click on add filter
- in parameter – source ip [indexed]
- operator – equals
- in value – ip of linux machine- add filter
- select an option - real time streaming

- Lets try to create log on linux machine
- Sudoadduserqradar
- Cat /etc/passwd | grepqradar

Qradar:x:1025:::/home/qradar:/bin/sh

Qradar(this is user):x:1025:::/home/qradar(these are the dir):/bin/sh(this is the shell)

- Lets look those events – qradar console –
- And click on first event – see info–(parsing data from payload) – payload (here event without parsing) – then check first event-sec – so on.. – provide you all detail -
-

[geeksforgeeks.org/getting-started-with-rsyslog-in-linux/](https://www.geeksforgeeks.org/getting-started-with-rsyslog-in-linux/)
-link

<https://www.youtube.com/watch?v=Dmf2iwRqATl>

-vi /etc/rsyslog.conf

<https://www.youtube.com/watch?v=5RrMNs4K51c>

- **Second methods - start after local host logit:root-new password-retype new password**
-
- **root@localhost~1# cat /etc/redhat-release**
- **root@localhost~1# du -h**
- **root@localhost~1# df -h** (minimum installation is done)
- **root@localhost~1# ls**
- **root@localhost~1# ./setup**
- **accept term – enter**
- **press space**
- **End – q-enter**
- **Continue y/n – y**
-
-
-
-