

## Network topology –

Although it is stated that there are 4 instances, the host discovery identified 5 instances total within the 192.168.100.32/27 subnet. Perhaps, one was intended for testing purposes and not terminated.

Scans

Settings

bypxtd

Host Discovery

[Back to My Scans](#)

Configure

Audit Trail

Launch

Export

Hosts 5

Vulnerabilities 3

History 1

Filter

Search Hosts

5 Hosts

Host	Vulnerabilities
192.168.100.60	5
192.168.100.54	4
192.168.100.37	3
192.168.100.55	2
192.168.100.33	2

Scan Details

Name: Host Discovery

Status: Completed

Policy: Host Discovery

Scanner: Local Scanner

Start: Today at 5:28 PM

End: Today at 5:38 PM

Elapsed: 9 minutes

Vulnerabilities

## Nessus scan results –

### Advanced scan –

Most of the instances contain only low vulnerabilities, so a preliminary report of only screenshots will be provided. However, 192.168.100.55 and 192.168.100.60 contain vulnerabilities of medium or above so I will provide recommendations on how to fix those two instances along with the screenshots.

Scans

Settings

bypxtd

Advanced Scan

[Back to My Scans](#)

Configure

Audit Trail

Launch

Export

Hosts 5

Vulnerabilities 27

History 1

Filter

Search Hosts

5 Hosts

Host	Vulnerabilities
192.168.100.55	37
192.168.100.60	12
192.168.100.54	11
192.168.100.37	10
192.168.100.33	1

Scan Details

Name: Advanced Scan

Status: Completed

Policy: Advanced Scan

Scanner: Local Scanner

Start: Today at 5:30 PM

End: Today at 5:43 PM

Elapsed: 14 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (1), High (1), Medium (1), Low (1), Info (1).

Advanced scan / 192.168.100.33 –

Scans

Settings

bypxtd

Advanced Scan / 192.168.100.33

Configure

Audit Trail

Launch

Export

Vulnerabilities

2

Switch Host 192.168.100.33

Filter

Search Vulnerabilities

2 Vulnerabilities

Sev	Name	Family	Count	
LOW	DHCP Server Detection	Service detection	1	
INFO	Nessus Scan Information	Settings	1	

Host Details

IP: 192.168.100.33

Start: Today at 5:31 PM

End: Today at 5:43 PM

Elapsed: 13 minutes

KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Advanced scan / 192.168.100.37 –

Scans

Settings

bypxtd

Advanced Scan / 192.168.100.37

Configure

Audit Trail

Launch

Export

Vulnerabilities

9

Switch Host 192.168.100.37

Filter

Search Vulnerabilities

9 Vulnerabilities

Sev	Name	Family	Count	
MIXED	SSH (Multiple Issues)	Misc.	2	
INFO	SSH (Multiple Issues)	General	2	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Nessus SYN scanner	Port scanners	1	
INFO	Service Detection	Service detection	1	
INFO	SSH Server Type and Version Information	Service detection	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	Traceroute Information	General	1	

Host Details

IP: 192.168.100.37

Start: Today at 5:31 PM

End: Today at 5:42 PM

Elapsed: 11 minutes

KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Scans

Settings

bypxtd

Advanced Scan / 192.168.100.37 / SSH (Multiple Issues)

Configure

Audit Trail

Launch

Export

Vulnerabilities

9

Search Vulnerabilities 2 Vulnerabilities

Sev	Name	Family	Count	
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1	
INFO	SSH Algorithms and Languages Supported	Misc.	1	

Scan Details

Name: Advanced Scan

Status: Completed

Policy: Advanced Scan

Scanner: Local Scanner

Start: Today at 5:30 PM

End: Today at 5:43 PM

Elapsed: 14 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

## Advanced scan / 192.168.100.54 –

Scans

Settings

bypxtd

Advanced Scan / 192.168.100.54

Configure

Audit Trail

Launch

Export

Vulnerabilities

9

Switch Host

192.168.100.54

Filter

Search Vulnerabilities

9 Vulnerabilities

Sev	Name	Family	Count	
MIXED	SSH (Multiple Issues)	Misc.	2	
INFO	SSH (Multiple Issues)	General	2	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Service Detection	Service detection	1	
INFO	SSH Server Type and Version Information	Service detection	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	Traceroute Information	General	1	

Host Details

IP: 192.168.100.54


Start: Today at 5:31 PM

End: Today at 5:42 PM

Elapsed: 11 minutes

KB: [Download](#)

Vulnerabilities



Critical

High

Medium

Low

Info

Scans

Settings

bypxtd

Advanced Scan / 192.168.100.54 / SSH (Multiple Issues)

Configure

Audit Trail

Launch

Export

Vulnerabilities

9

Search Vulnerabilities

2 Vulnerabilities

Sev	Name	Family	Count	
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1	
INFO	SSH Algorithms and Languages Supported	Misc.	1	

Scan Details

Name: Advanced Scan

Status: Completed

Policy: Advanced Scan


Scanner: Local Scanner

Start: Today at 5:30 PM

End: Today at 5:43 PM

Elapsed: 14 minutes

Vulnerabilities



Critical

High

Medium

Low

Info

## Advanced scan / 192.168.100.55 –

### SSL self-signed certificate / Plugin #57582

The self-signed certificate is plausible if the server is only for personal use. However, if the instance were to be deployed for public access then the self-signed certificate would deter clients to use the service as it is not guaranteed by valid certificate authorities. So, clients may think the server they are accessing is false. To fix this, I would recommend purchasing or installing a CA certificate.

### SSL certificate cannot be trusted / Plugin #51192

The certificate is not trusted likely because it is not approved by a certified authority. Again, I would recommend purchasing or installing a CA certificate.

### SSL medium strength cipher suites supported / Plugin #42873

The instance supports SSL ciphers with medium strength encryption. Medium strength encryption is easier for attackers to bypass if they are on the same network. It appears only port 3389 is affected so it should be reconfigured to support high strength encryption in order to resolve the issue.

## SMB signing required / Plugin #57508

Signing helps in confirming packet authenticity. Therefore, eliminating attacks such as 'man-in-the-middle' and ensuring packet security. To enable SMB signing on the windows system, navigate to 'policy settings' then ensure 'Microsoft network server. Digitally sign communications' is set to 'always'.

## Terminal services doesn't use network level authentication (NLA) only / Plugin #58453

Terminal services uses other means of authentication other than network level. By enabling network level authentication only, it will strengthen authentication and prevent attacks such as 'man-in-the-middle'. It will also protect the remote host from malicious users by authenticating before the remote desktop protocol connection is established. Simply enable network level authentication on windows by navigating to 'settings' and then 'remote'.

The screenshot shows the Burp Suite interface with the following components:

- Header:** Scans, Settings, byportd, and a user icon.
- Breadcrumb:** Advanced Scan / 192.168.100.55
- Buttons:** Configure, Audit Trail, Launch, Export.
- Switch Host:** 192.168.100.55
- Vulnerabilities:** 20
- Filter:** Search Vulnerabilities, 20 Vulnerabilities
- Vulnerability Table:**

Sev	Name	Family	Count	
MIXED	SSL (Multiple Issues)	General	9	
MIXED	Microsoft Windows (Multiple Issues)	Misc.	3	
INFO	DCE Services Enumeration	Windows	8	
INFO	SMB (Multiple Issues)	Windows	6	
INFO	TLS (Multiple Issues)	Service detection	2	
INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Device Type	General	1	
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
INFO	Inconsistent Hostname and IP Address	Settings	1	
INFO	Local Checks Not Enabled (info)	Settings	1	
INFO	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	Windows	1	
INFO	Nessus Scan Information	Settings	1	
INFO	No Credentials Provided	Settings	1	
INFO	OS Identification	General	1	
INFO	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)	Misc.	1	
INFO	RDP Screenshot	General	1	
INFO	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)	Misc.	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	Windows Terminal Services Enabled	Windows	1	
- Host Details:**
  - IP: 192.168.100.55
  - DNS: EC2AMAZ-2UE81OF.ec2.internal
  - OS: Windows Server 2016 Datacenter 14393
  - Start: Today at 5:31 PM
  - End: Today at 5:40 PM
  - Elapsed: 9 minutes
  - KB: [Download](#)
- Vulnerabilities:**
  - Donut chart showing distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Scans
Settings
bypxtd

Advanced Scan / 192.168.100.55 / SSL (Multiple Issues)
Configure
Audit Trail
Launch
Export

Vulnerabilities 20
Search Vulnerabilities 9 Vulnerabilities

Sev	Name	Family	Count	
MEDIUM	SSL Certificate Cannot Be Trusted	General	1	
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	1	
MEDIUM	SSL Self-Signed Certificate	General	1	
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	SSL Session Resume Supported	General	1	

**Scan Details**
Name: Advanced Scan  
Status: Completed  
Policy: Advanced Scan  
Scanner: Local Scanner  
Start: Today at 5:30 PM  
End: Today at 5:43 PM  
Elapsed: 14 minutes

**Vulnerabilities**

Scans
Settings
bypxtd

Advanced Scan / 192.168.100.55 / Microsoft Windows (Multiple Issues)
Configure
Audit Trail
Launch
Export

Vulnerabilities 20
Search Vulnerabilities 3 Vulnerabilities

Sev	Name	Family	Count	
MEDIUM	SMB Signing not required	Misc.	1	
MEDIUM	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Misc.	1	
INFO	Terminal Services Use SSL/TLS	Misc.	1	

**Scan Details**
Name: Advanced Scan  
Status: Completed  
Policy: Advanced Scan  
Scanner: Local Scanner  
Start: Today at 5:30 PM  
End: Today at 5:43 PM  
Elapsed: 14 minutes

**Vulnerabilities**

Advanced scan / 192.168.100.60 –

SSH weak algorithms supported / Plugin #90317

The instance is configured to use arcfour, which is a weak encryption that can be easily cracked compared to other encryption methods. To disable arcfour encryption, edit the /etc/ssh/sshd/sshd\_config file to exclude arcfour. Then, restart the sshd service by executing the command 'sudo service sshd restart'.

Scans Settings bypttd

Advanced Scan / 192.168.100.60 Configure Audit Trail Launch Export

Vulnerabilities 9 Switch Host 192.168.100.60

Filter Search Vulnerabilities 9 Vulnerabilities

Sev	Name	Family	Count
MIXED	SSH (Multiple Issues)	Misc.	3
INFO	Nessus SYN scanner	Port scanners	3
INFO	SSH (Multiple Issues)	General	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Service Detection	Service detection	1
INFO	SSH Server Type and Version Information	Service detection	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Traceroute Information	General	1

**Host Details**

IP: 192.168.100.60  
 Start: Today at 5:31 PM  
 End: Today at 5:42 PM  
 Elapsed: 11 minutes  
 KB: [Download](#)

**Vulnerabilities**

Scans Settings bypttd

Advanced Scan / 192.168.100.60 / SSH (Multiple Issues) Configure Audit Trail Launch Export

Vulnerabilities 9 Search Vulnerabilities 3 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	SSH Weak Algorithms Supported	Misc.	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
INFO	SSH Algorithms and Languages Supported	Misc.	1

**Scan Details**

Name: Advanced Scan  
 Status: Completed  
 Policy: Advanced Scan  
 Scanner: Local Scanner  
 Start: Today at 5:30 PM  
 End: Today at 5:43 PM  
 Elapsed: 14 minutes

**Vulnerabilities**

## Red Hat Instance –

User accounts created – The accounts `usr_redhat_w`, `usr_redhat_m`, and `usr_redhat_s` were created.

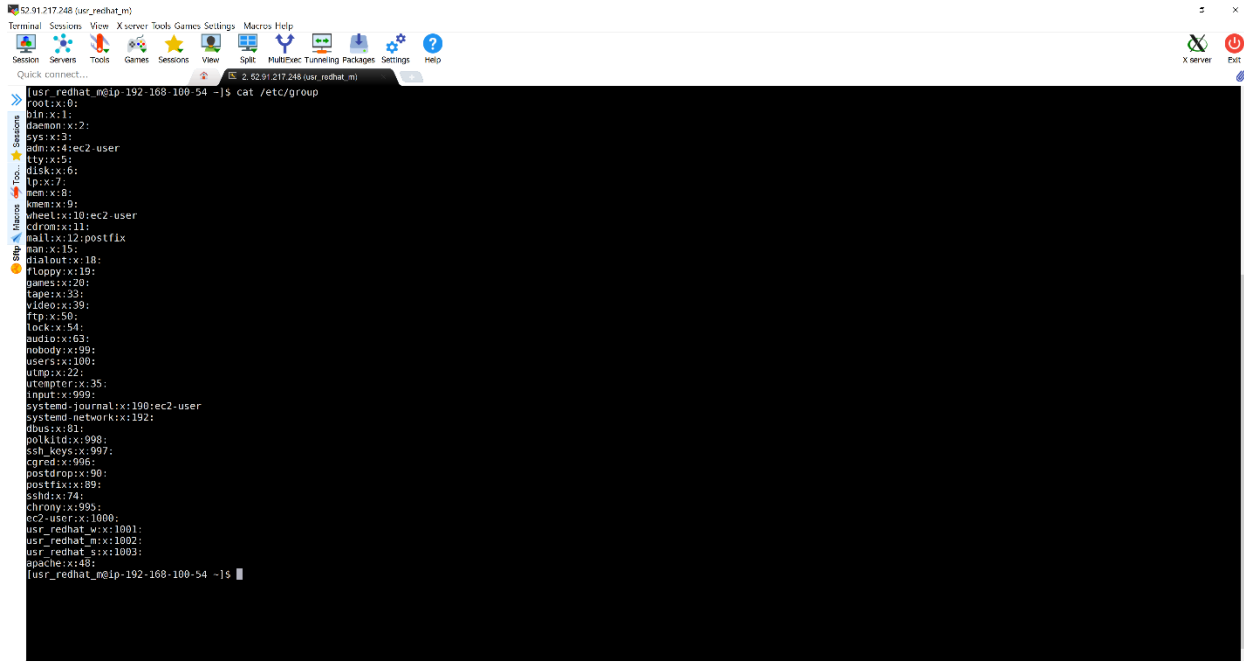
```

52.91.217.248 (usr_redhat_m)
Terminal Sessions View Split Multitasking Packages Settings Help
Quick connect: 2 2, 62.91.217.248 (usr_redhat_m)
[usr_redhat_m@ip-192-168-100-54 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
system-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:system message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
sblinux:74:74:privilege separated SSH:/var/empty/sshd:/sbin/nologin
chrony:x:998:995:/var/lib/chrony:/sbin/nologin
oc2-user:x:1000:1000:Cloud User:/home/oc2-user:/bin/bash
usr_redhat_w:x:1001:1001:/home/usr_redhat_w:/bin/bash
usr_redhat_m:x:1002:1002:/home/usr_redhat_m:/bin/bash
usr_redhat_s:x:1003:1003:/home/usr_redhat_s:/bin/bash
apache:x:48:48:apache:/usr/share/httpd:/sbin/nologin
[usr_redhat_m@ip-192-168-100-54 ~]$
  
```

UNREGISTERED VERSION Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

## Type of accounts –

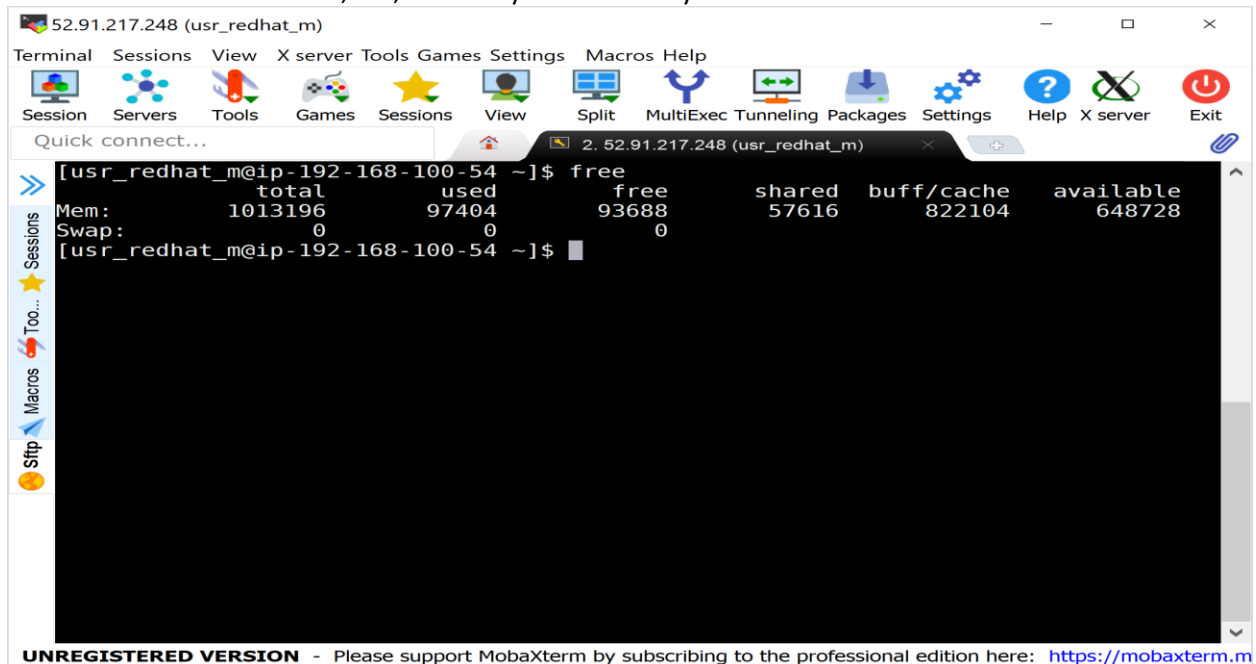
The users `usr_redhat_w`, `usr_redhat_m`, `usr_redhat_s` are not in group 'wheel'. Only `ec2-user` in group 'wheel'.



```
[usr_redhat_m@ip-192-168-100-54 ~]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:ec2-user
tty:x:5:
disk:x:6:
lp:x:7:
men:x:8:
kmem:x:9:
wheel:x:10:ec2-user
cdrom:x:11:
mail:x:12:postfix
man:x:13:
print:x:18:
floppy:x:19:
games:x:20:
tape:x:23:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
uucp:x:22:
utempter:x:35:
input:x:999:
systemd-journal:x:100:ec2-user
systemd-network:x:192:
dbus:x:81:
polkitd:x:998:
ssh_keys:x:997:
cgred:x:996:
postdrop:x:90:
postfix:x:89:
sshd:x:74:
chrony:x:990:
ec2-user:x:1000:
usr_redhat_w:x:1001:
usr_redhat_m:x:1002:
usr_redhat_s:x:1003:
apache:x:48:
[usr_redhat_m@ip-192-168-100-54 ~]$
```

## Total memory –

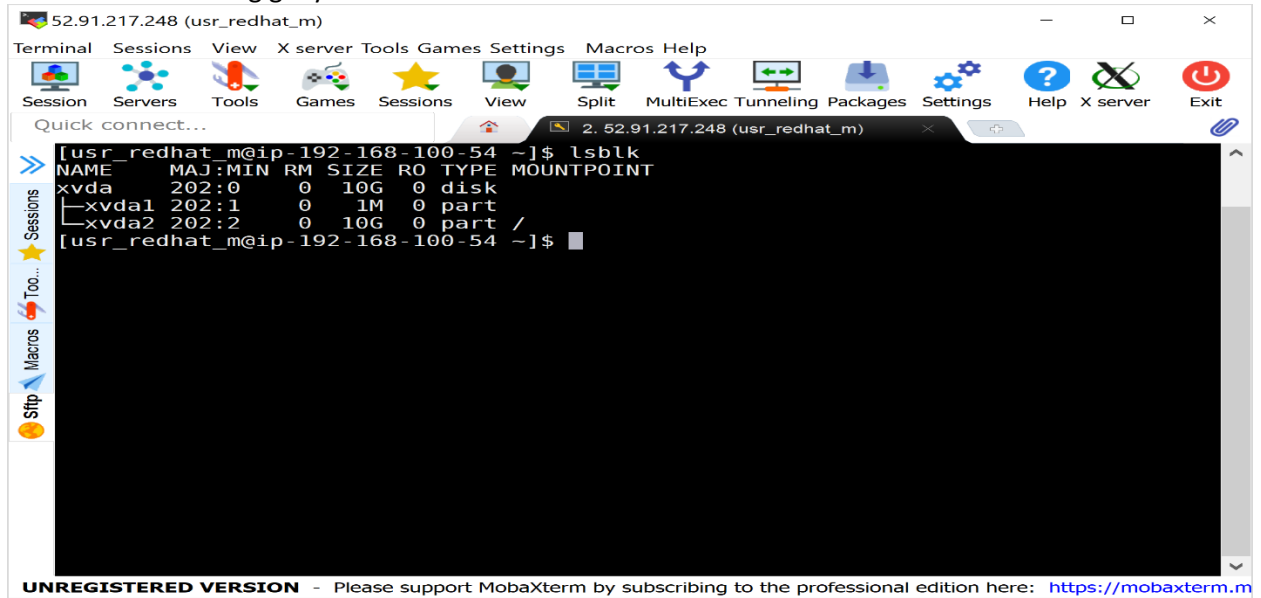
The instance has a total of 1,013,196 kilobytes in memory.



```
[usr_redhat_m@ip-192-168-100-54 ~]$ free
              total        used        free      shared    buff/cache   available
Mem:           1013196          97404          93688         57616         822104         648728
Swap:              0              0              0
[usr_redhat_m@ip-192-168-100-54 ~]$
```

Total HDD –

The instance has 10 gigabytes in HDD.



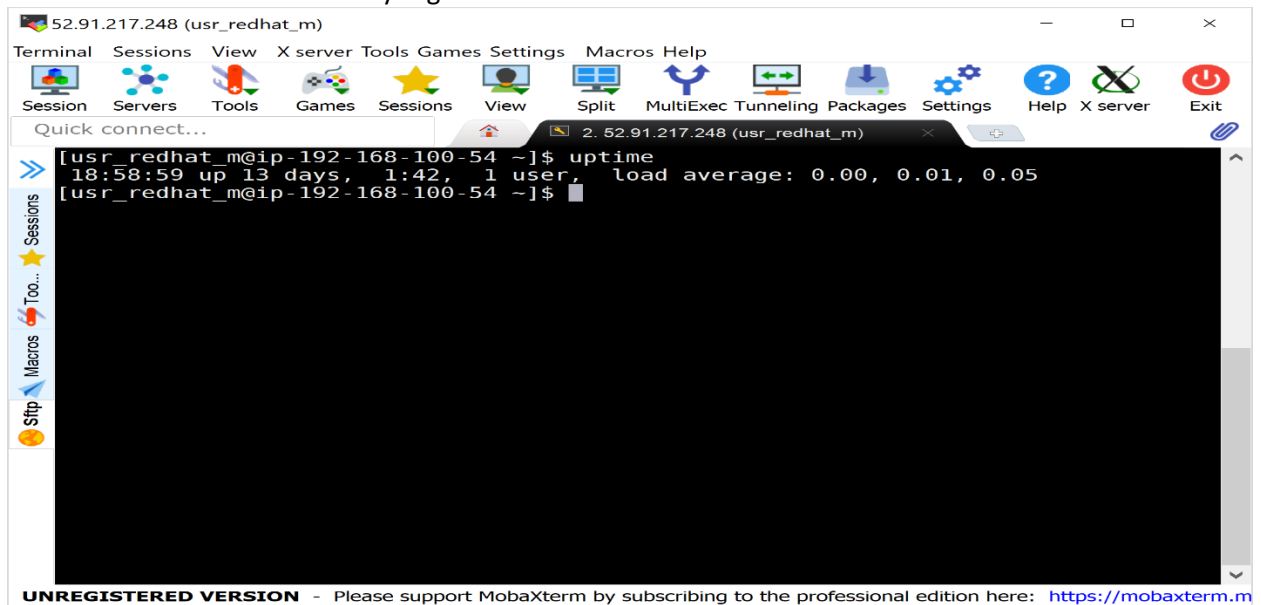
A screenshot of the MobaXterm application window. The title bar shows the IP address 52.91.217.248 and the session name (usr\_redhat\_m). The menu bar includes Terminal, Sessions, View, X server, Tools, Games, Settings, and Macros. The toolbar contains icons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, Settings, Help, X server, and Exit. A sidebar on the left has icons for Sessions, Tools, Macros, and Sftp. The main terminal area shows a command prompt where the user has entered 'lsblk'. The output is a table of disk information.

```
[usr_redhat_m@ip-192-168-100-54 ~]$ lsblk
NAME        MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda        202:0    0  10G  0 disk 
├─xvda1     202:1    0   1M  0 part 
└─xvda2     202:2    0  10G  0 part /
```

At the bottom of the window, a message reads: **UNREGISTERED VERSION** - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.m>

Instance creation –

The instance was created 13 days ago.



A screenshot of the MobaXterm application window, similar to the one above. The terminal shows the user entering the 'uptime' command. The output displays the system's uptime as 13 days, 1 hour, 42 minutes, and 1 second, along with the current user and load averages.

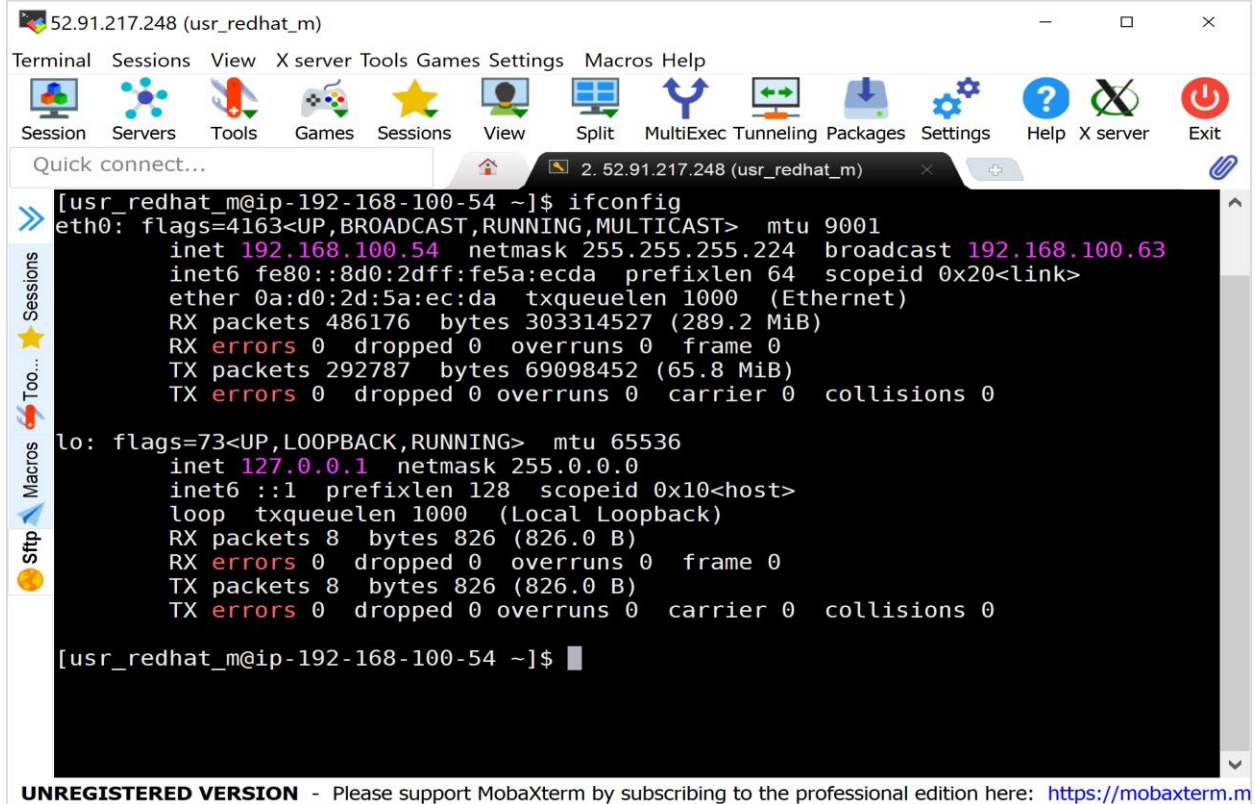
```
[usr_redhat_m@ip-192-168-100-54 ~]$ uptime
18:58:59 up 13 days, 1:42, 1 user, load average: 0.00, 0.01, 0.05
[usr_redhat_m@ip-192-168-100-54 ~]$
```

At the bottom of the window, a message reads: **UNREGISTERED VERSION** - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.m>



## Network configuration –

The instance has an IP of 192.168.100.54 and netmask of 255.255.255.224.



```
52.91.217.248 (usr_redhat_m)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect... 2. 52.91.217.248 (usr_redhat_m)
[usr_redhat_m@ip-192-168-100-54 ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 192.168.100.54 netmask 255.255.255.224 broadcast 192.168.100.63
    inet6 fe80::8d0:2dff:fe5a:ecda prefixlen 64 scopeid 0x20<link>
    ether 0a:d0:2d:5a:ec:da txqueuelen 1000 (Ethernet)
    RX packets 486176 bytes 303314527 (289.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 292787 bytes 69098452 (65.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

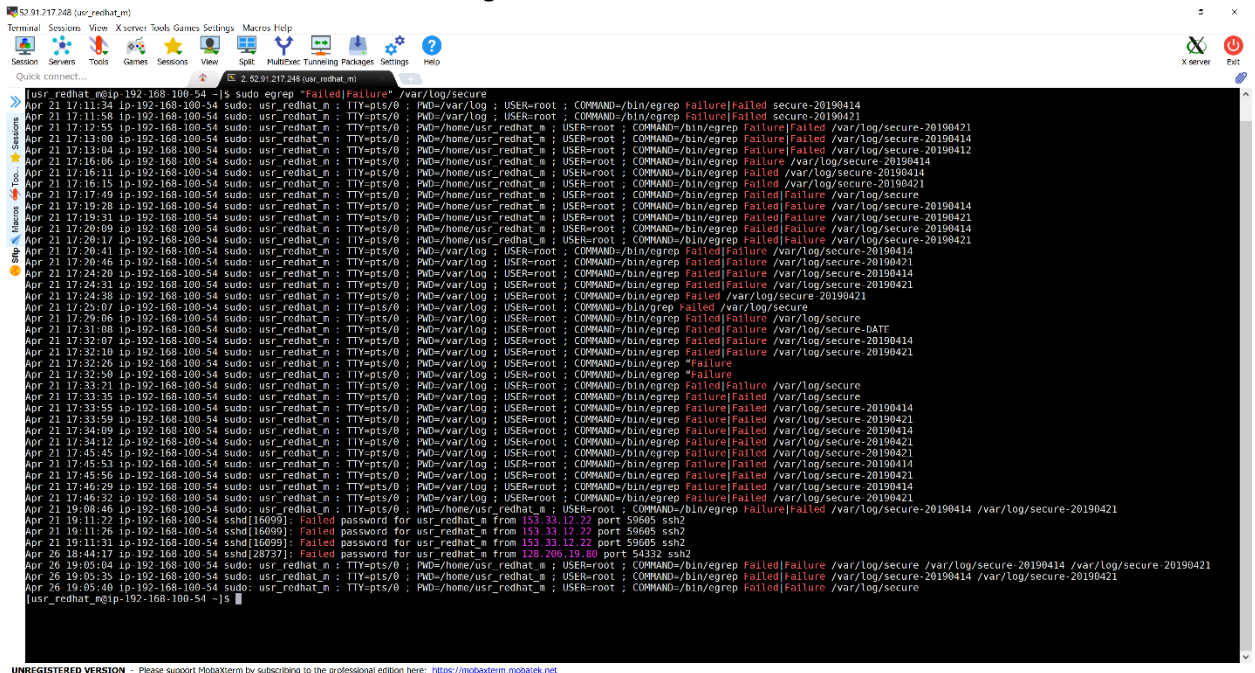
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 826 (826.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 826 (826.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[usr_redhat_m@ip-192-168-100-54 ~]$
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.m>

## Failed login –

The 2 IP addresses who have failed to login are 153.33.12.22 and 128.206.19.80.



```
52.91.217.248 (usr_redhat_m)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect... 2. 52.91.217.248 (usr_redhat_m)
[usr_redhat_m@ip-192-168-100-54 ~]$ sudo egrep "Failed|Failure" /var/log/secure
Apr 21 17:11:54 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:11:58 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:12:55 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:13:00 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:13:04 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190412
Apr 21 17:16:06 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:16:11 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:16:15 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:17:49 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:19:28 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:19:29 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:20:09 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:20:17 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:20:41 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:20:46 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:24:20 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:24:31 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:24:38 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:25:07 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:29:06 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure
Apr 21 17:31:08 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-bate
Apr 21 17:32:07 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:32:10 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:32:26 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure
Apr 21 17:32:48 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:33:21 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure
Apr 21 17:33:35 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure
Apr 21 17:33:55 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:33:59 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:34:09 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:34:12 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:45:45 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:45:53 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:45:56 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 17:46:29 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414
Apr 21 17:46:32 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190421
Apr 21 19:08:46 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414 /var/log/secure-20190421
Apr 21 19:11:22 ip-192-168-100-54 sshd[16090] : Failed password for usr_redhat_m from 153.33.12.22 port 59605 ssh2
Apr 21 19:11:76 ip-192-168-100-54 sshd[16090] : Failed password for usr_redhat_m from 153.33.12.22 port 59605 ssh2
Apr 21 19:11:31 ip-192-168-100-54 sshd[16099] : Failed password for usr_redhat_m from 128.206.19.80 port 54332 ssh2
Apr 26 18:44:17 ip-192-168-100-54 sshd[20973] : Failed password for usr_redhat_m from 128.206.19.80 port 54332 ssh2
Apr 26 19:05:04 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure /var/log/secure-20190414 /var/log/secure-20190421
Apr 26 19:05:35 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure-20190414 /var/log/secure-20190421
Apr 26 19:05:48 ip-192-168-100-54 sudo: usr_redhat_m : TTY=pts/0 ; PWD=/home/usr_redhat_m ; USER=root ; COMMAND=/bin/egrep Failed|Failure /var/log/secure
[usr_redhat_m@ip-192-168-100-54 ~]$
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>