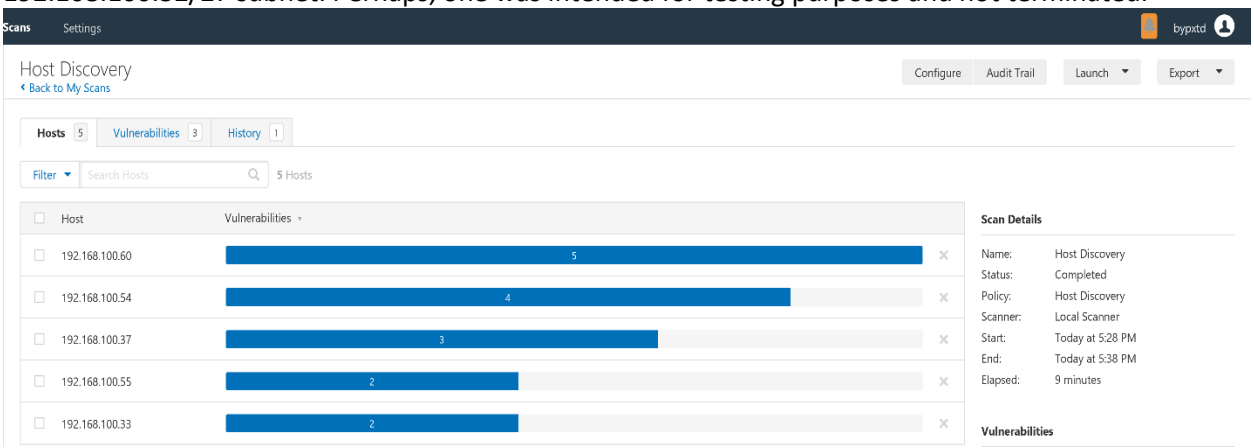
Network topology –

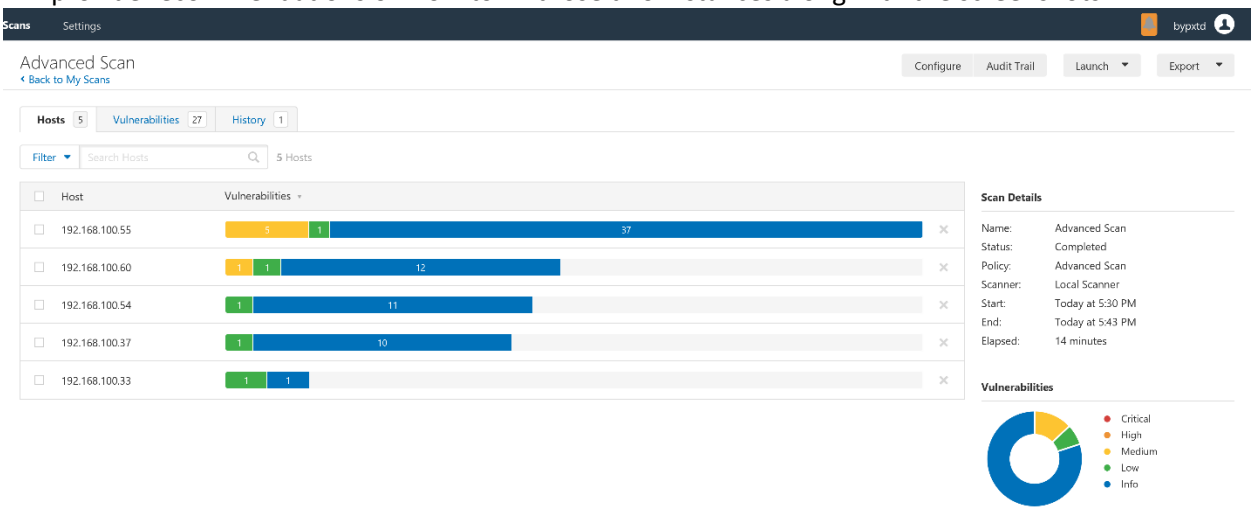
Although it is stated that there are 4 instances, the host discovery identified 5 instances total within the 192.168.100.32/27 subnet. Perhaps, one was intended for testing purposes and not terminated.



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.



Advanced scan / 192.168.100.33 –

Scans Settings bypxtd

Advanced Scan / 192.168.100.33
‹ Back to Hosts

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
‹ Back to Hosts

Configure Audit Trail Launch Export

Vulnerabilities 9

Switch Host 192.168.100.37

Filter Search Vulnerabilities 9 Vulnerabilities

Sev	Name	Family	Count
MIXED	2 SSH (Multiple Issues)	Misc.	2
INFO	2 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)
‹ Back to Vulnerabilities

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

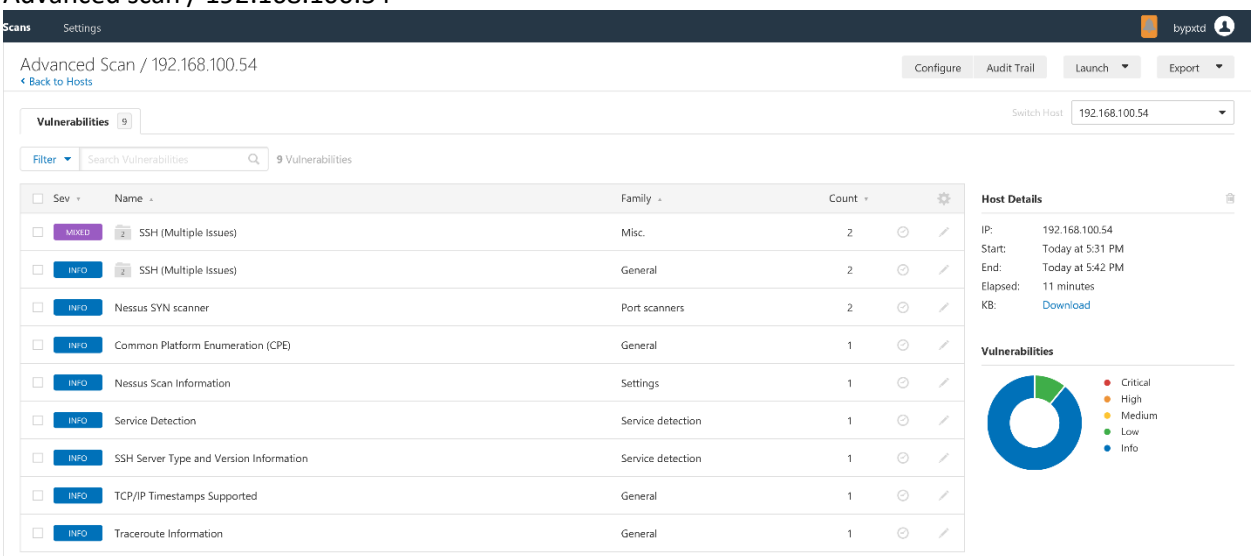
Scan Details

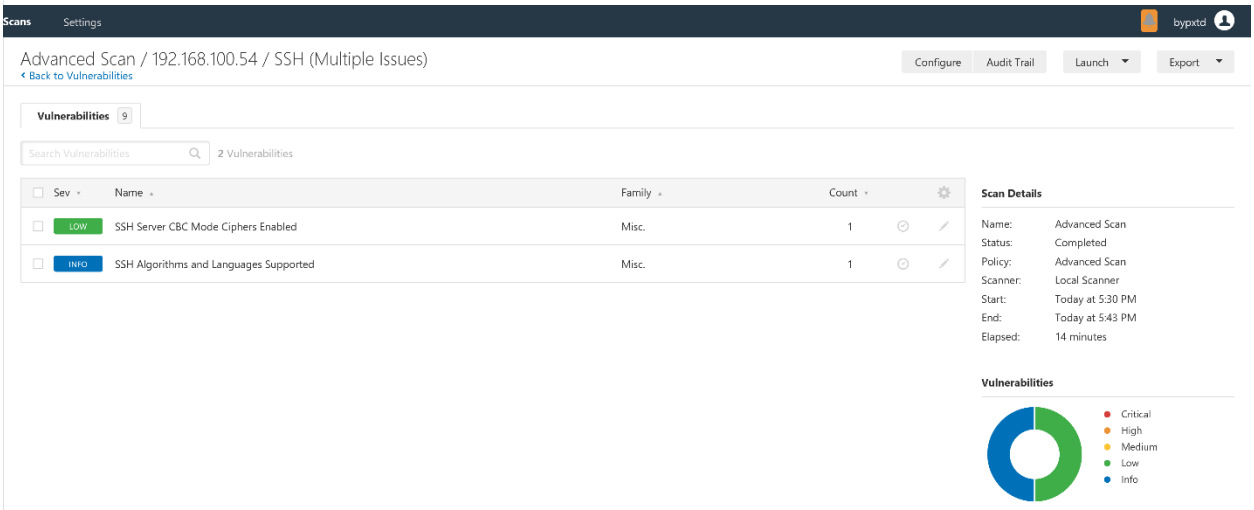
Name:	Advanced Scan
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	Today at 5:30 PM
End:	Today at 5:43 PM
Elapsed:	14 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Advanced scan / 192.168.100.54 –





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

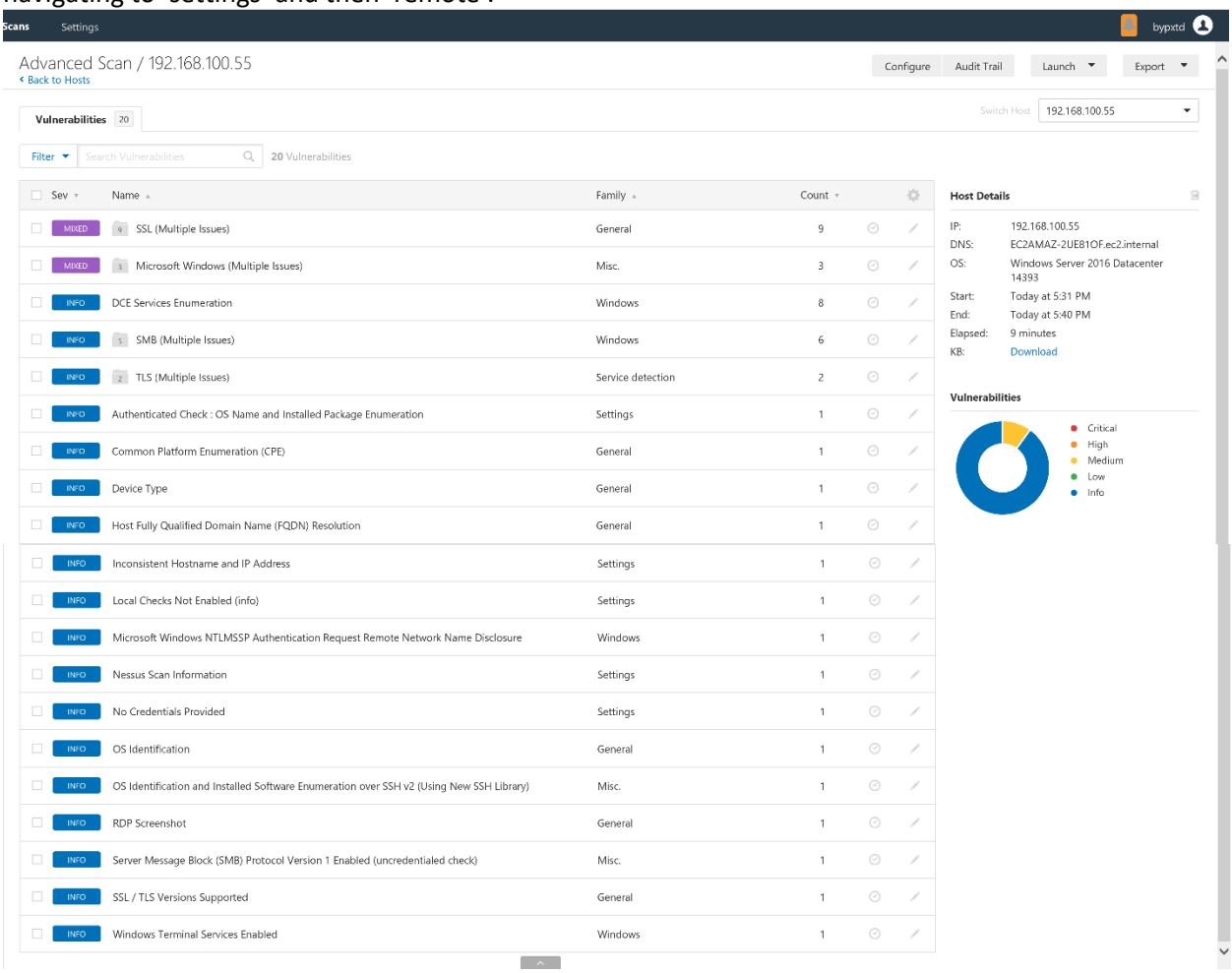
The certificate is not trusted likely because it is not approved by a certified authority. Again, I would recommend purchasing or installing a CA certificate.

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’.



Scans Settings bypxtd

Advanced Scan / 192.168.100.55 / SSL (Multiple Issues)

‹ Back to Vulnerabilities

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)

‹ Back to Vulnerabilities

Configure Audit Trail Launch Export

Vulnerabilities 20

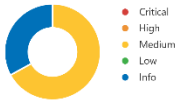
Search Vulnerabilities 3 Vulnerabilities

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

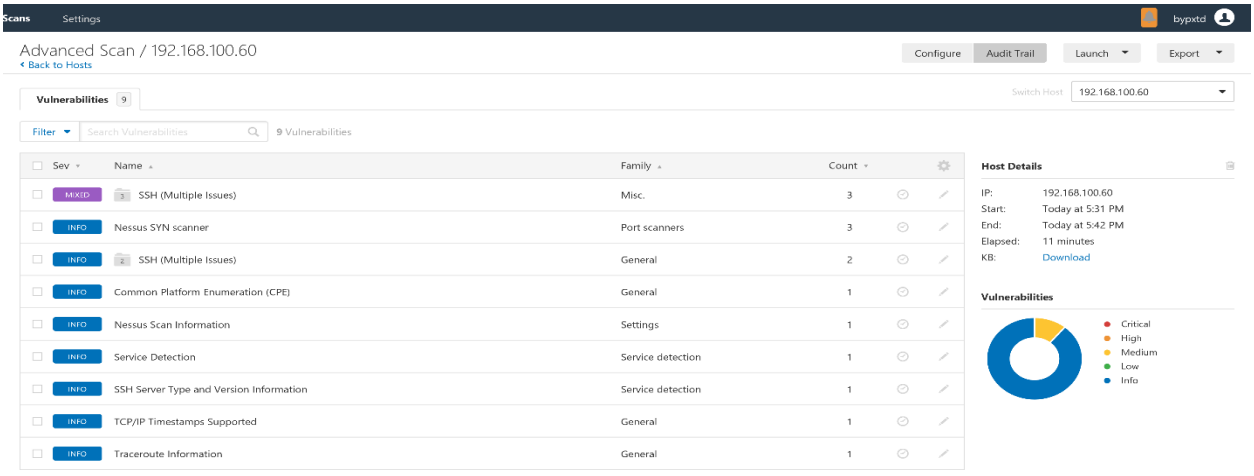
Scan Details

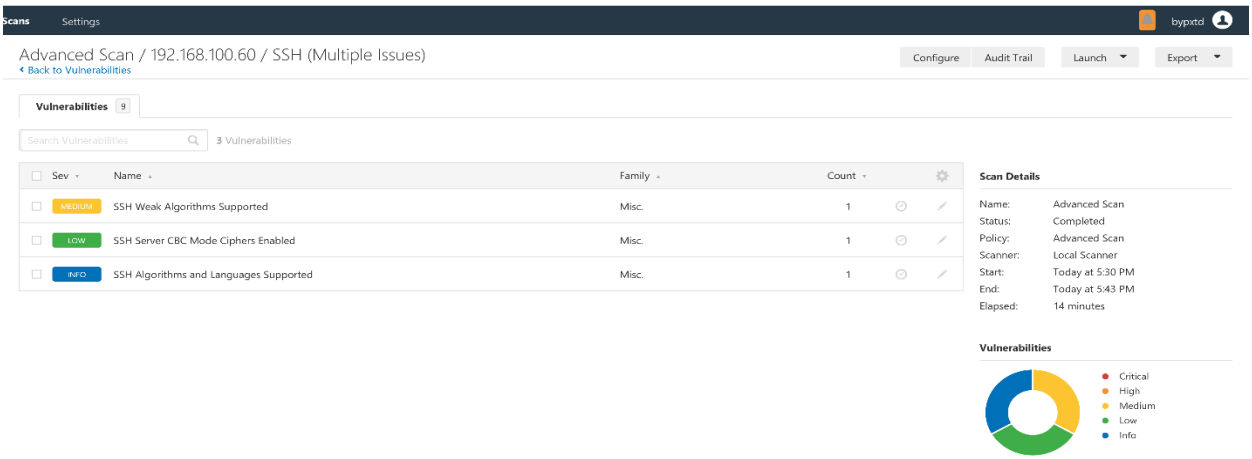
Name: Advanced Scan
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Start: Today at 5:30 PM
End: Today at 5:43 PM
Elapsed: 14 minutes

Vulnerabilities



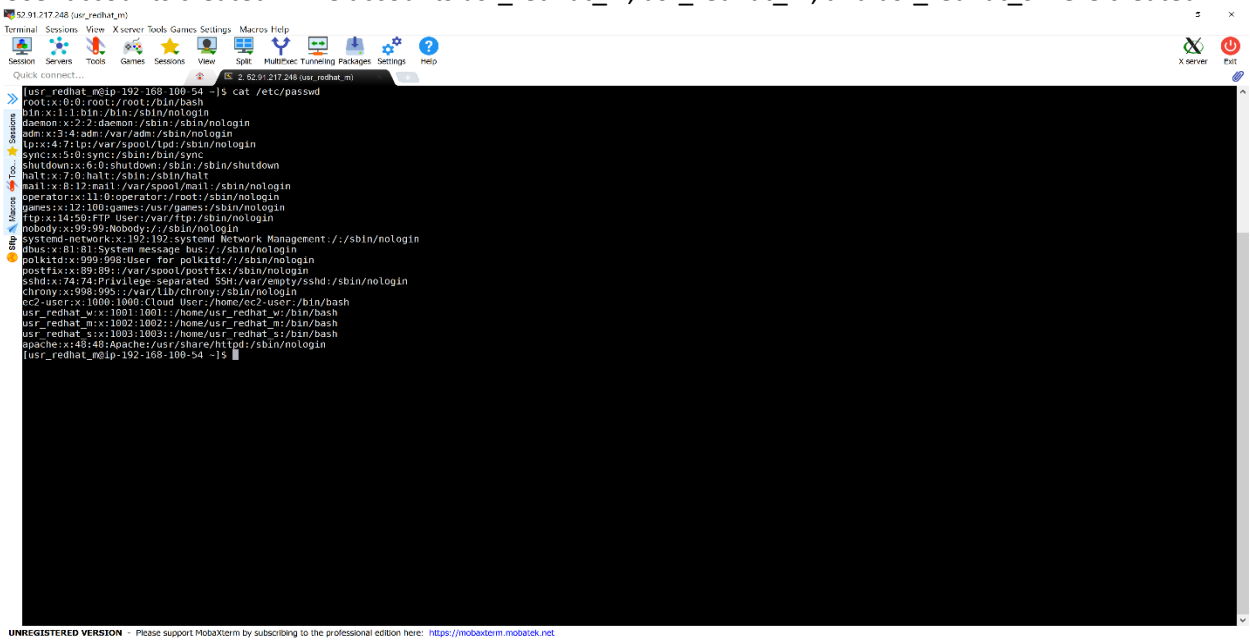
Advanced scan / 192.168.100.60 –
SSH weak algorithms supported / Plugin #90317
The instance is configured to use arcfour, which is a weak encryption that can be easily cracked compared to other encryption methods. To disable arcfour encryption, edit the /etc/ssh/sshd/sshd_config file to exclude arcfour. Then, restart the sshd service by executing the command ‘sudo service sshd restart’.





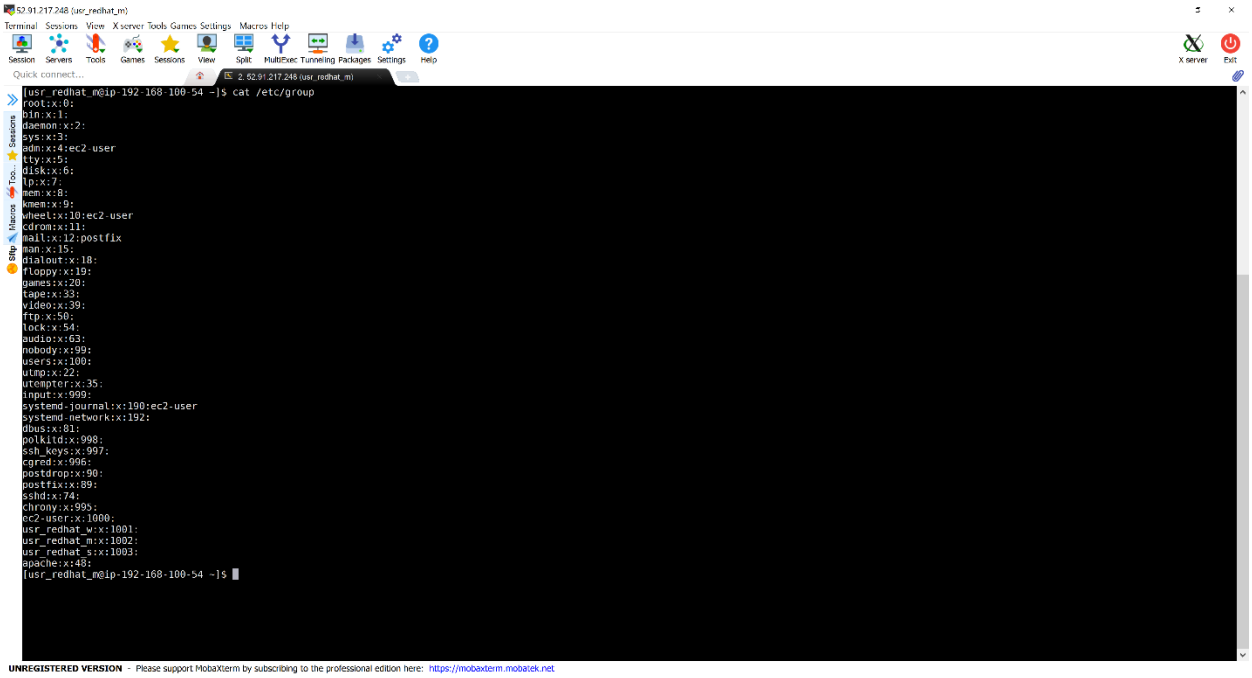
Red Hat Instance –

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



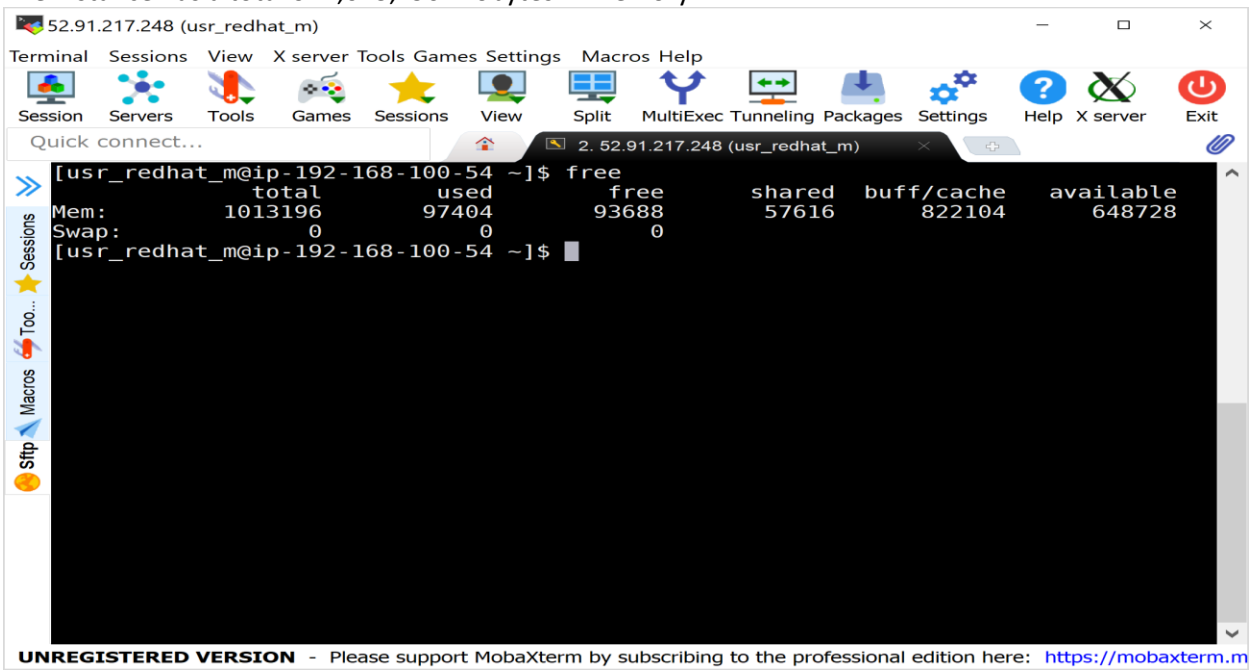
Type of accounts –

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



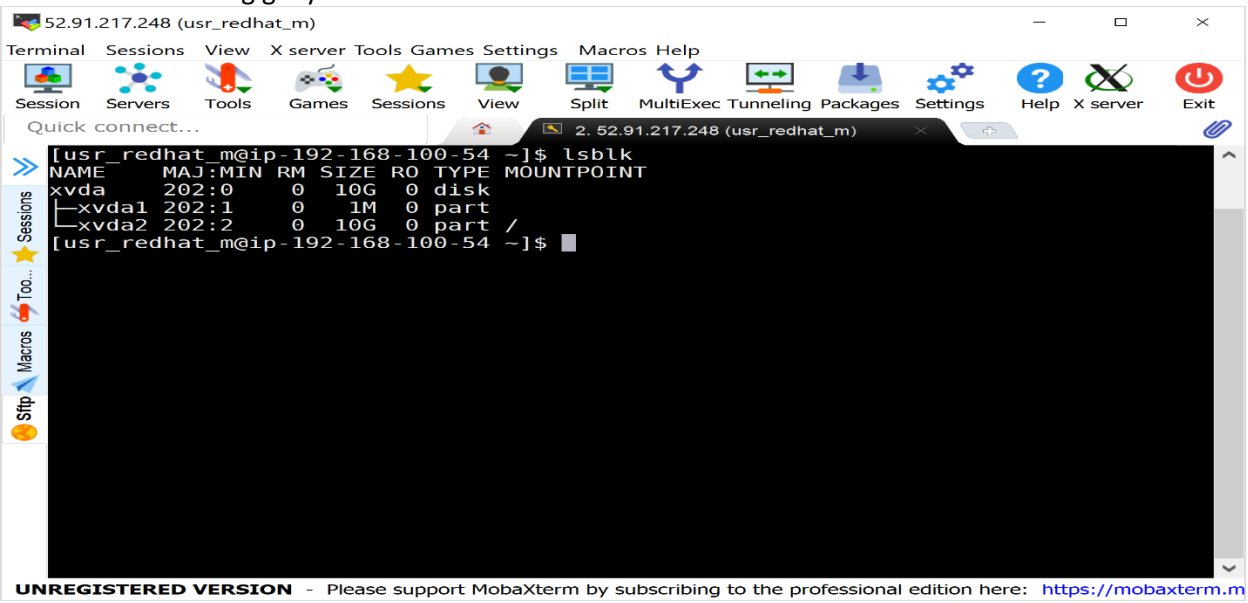
Total memory –

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



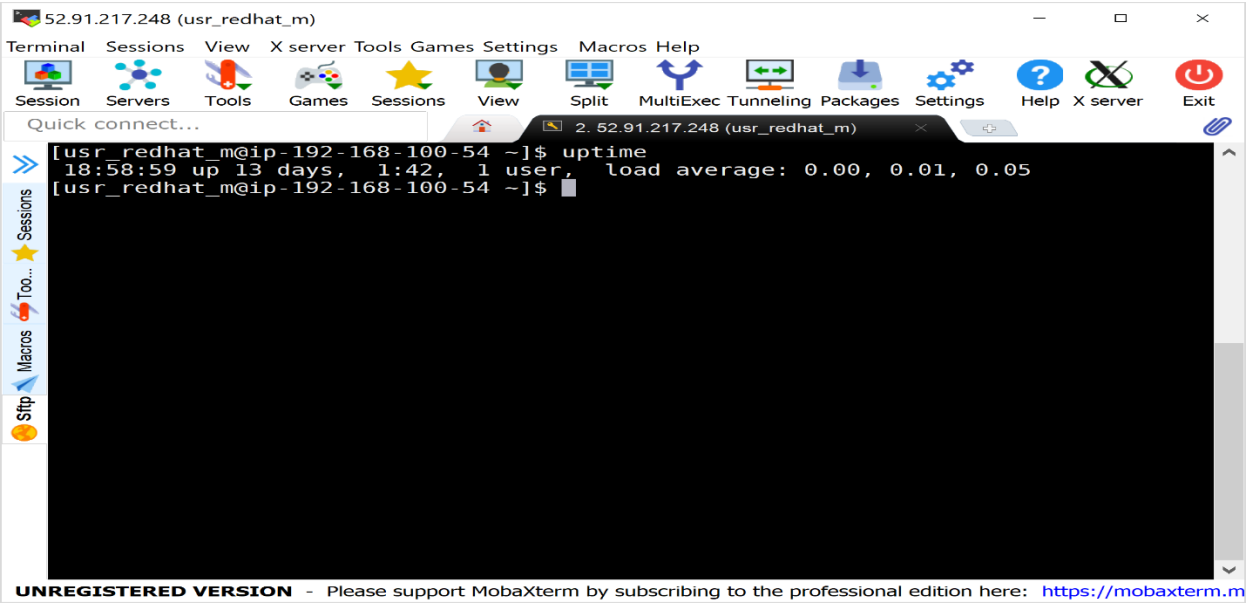
Total HDD –

The instance has 10 gigabytes in HDD.



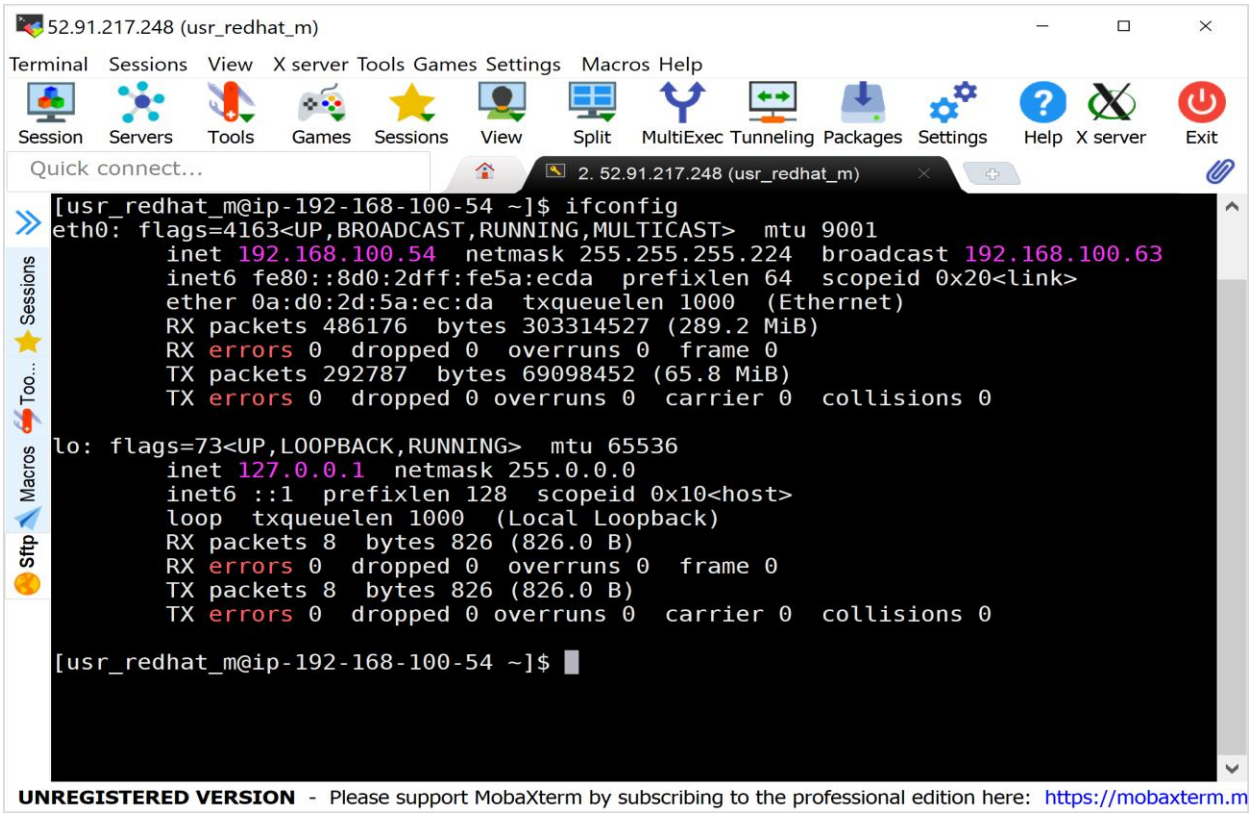
Instance creation –

The instance was created 13 days ago.



Network configuration –

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



Failed login –

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