

Vulnerability and Threat Analysis

RIS430 NAA

Assignment 5

User Inventory Report

Prepared By Group 10,

Khondoker Ishmum Muhammad (155895212)

Aryan Santosh Saindane (136235215)

Ananthu Krishna Vadakkeppatt (154290217)

Syed Mujahid Hamid Ali (161202213)

Table of Content

Overview03

User Inventory04

Overview

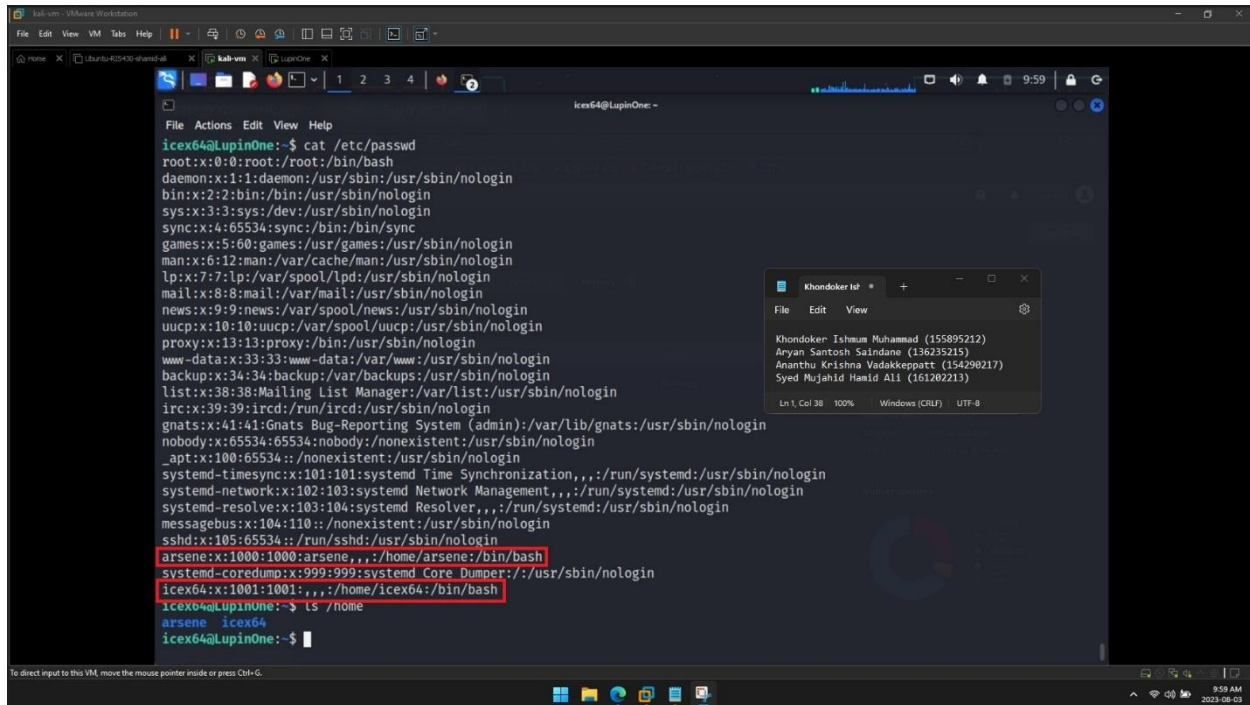
This report aims to present an overview of the users in the Lupin One VM along with other details. It serves as a crucial component of our security assessment, ensuring that user accounts are well-managed.

- Two users were found; arsene and icex64.
- Both accounts seem to be non-root.
- The passwords could not be found as they appear to be store in some secure way. We tried using different password cracking tools and various dictionary attacks, but we failed.
- Due to this, we can conclude that these passwords have a very high level of strength and security attached to them.

User Inventory

To get the number of users in the Lupin One VM, I ran the following commands:

- `cat /etc/passwd`
- `ls /hosts`



```
File Actions Edit View Help
icex64@LupinOne:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/ssh:/usr/sbin/nologin
arsene:x:1000:1000:arsene,,:/home/arsene:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
icex64:x:1001:1001:,,:/home/icex64:/bin/bash
icex64@LupinOne:~$ ls /home
arsene icex64
icex64@LupinOne:~$
```

Host	Username	Password	Strength of Password
192.168.99.129	arsene	Not found	Very Strong
	icex64	Not found	Very Strong

From this table, we can analyze that there were two users, whose passwords we could not get as they were stored in some secure location. We even tried through multiple password cracking and various attacks, but still failed.