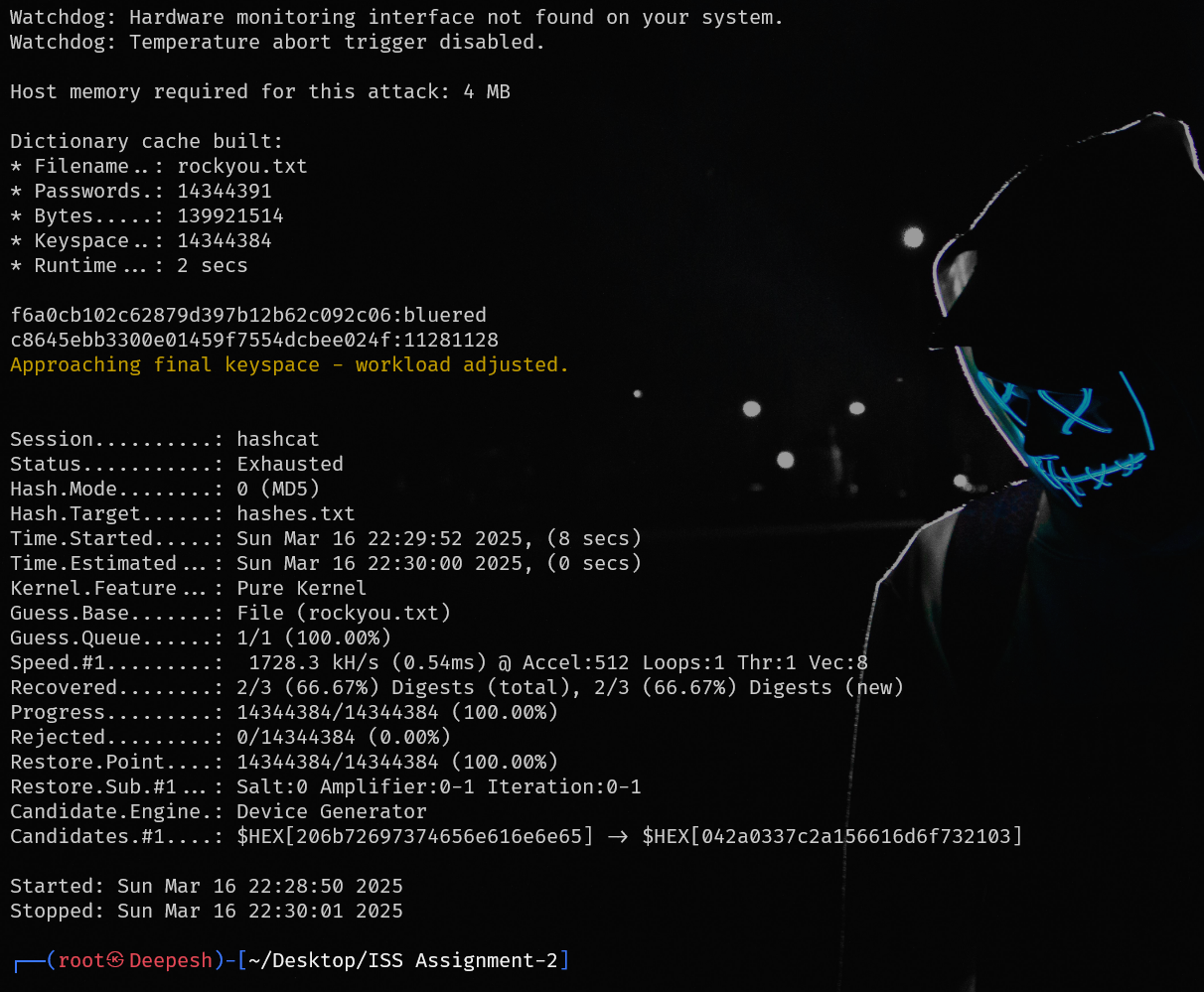
**ASSIGNMENT-2**

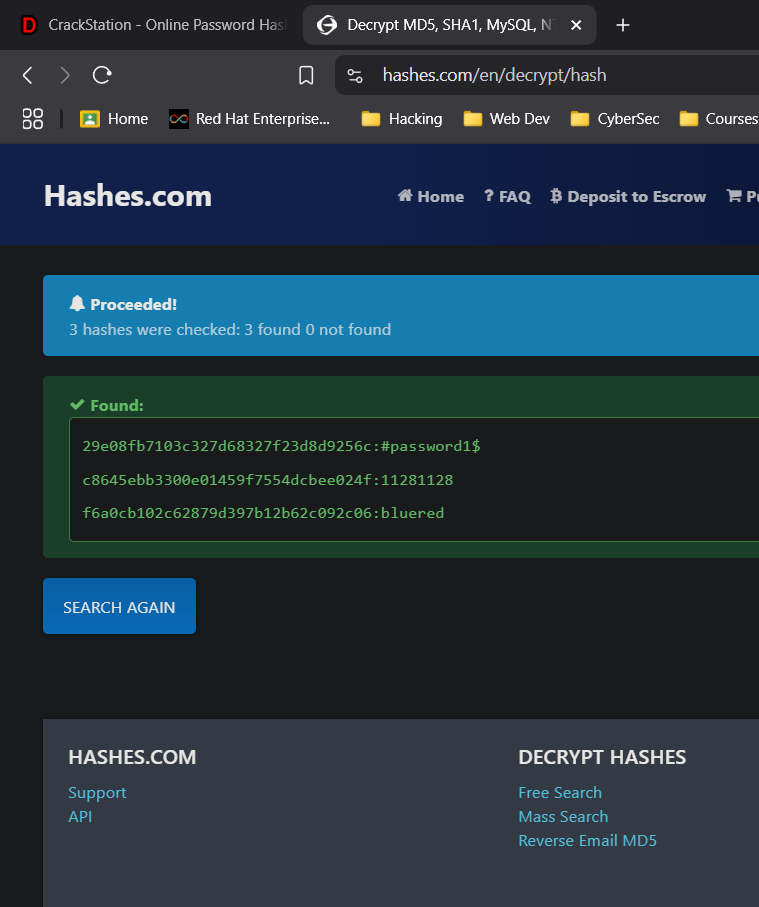
**(Deepesh Patil – 112215055)**

SubLab-1: Cracking MD5 Password Hashes using Hashcat/John the Ripper

**COMMAND:**

hashcat -m 0 -a 0 hashes.txt rockyou.txt –force





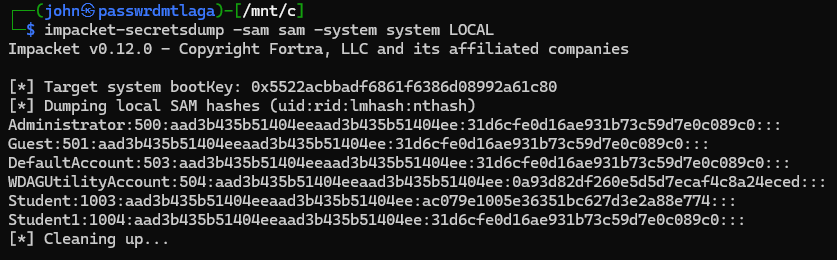
|  |  |  |
| --- | --- | --- |
| **USER** | **HASHES** | **PASSWORD** |
| student | 29e08fb7103c327d68327f23d8d9256c | #password1$ |
| jsmith | f6a0cb102c62879d397b12b62c092c06 | bluered |
| jtripper | c8645ebb3300e01459f7554dcbee024f | 11281128 |

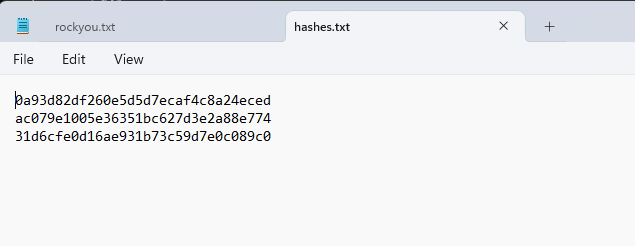
# SubLab-2: Cracking Windows NTLM Password Hashes using Hashcat

### Retrieving NTLM Hashes using “impacket”:

**COMMAND:**

Impacket-secretsdump -sam sam -system system LOCAL



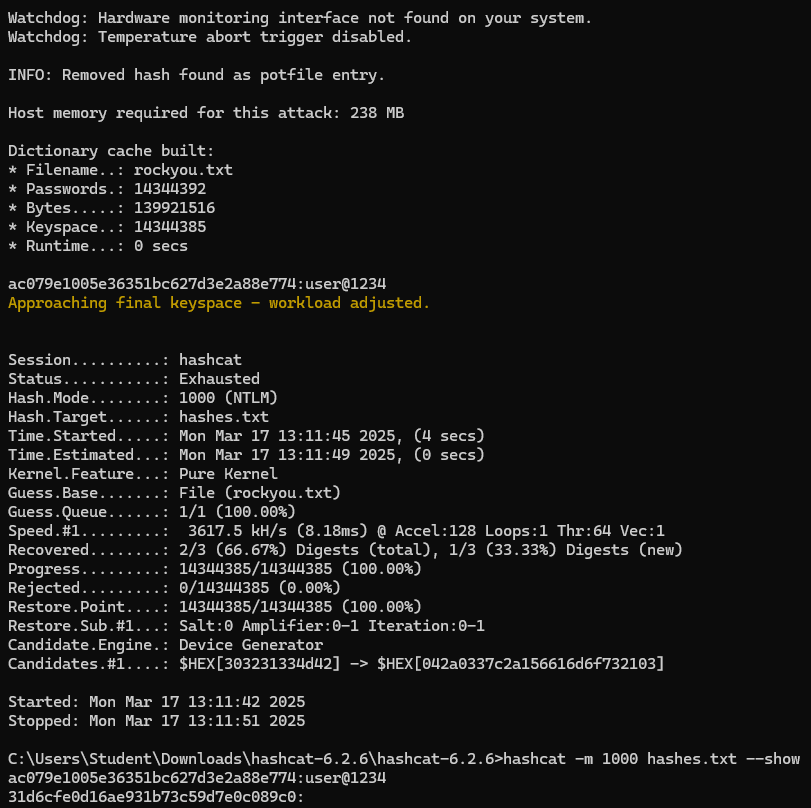


### Cracking the Hashes using Hashcat:

**COMMAND:**

hashcat -m 1000 -a 0 hashes.txt rockyou.txt --force

hashcat -m 1000 hashes.txt --show



|  |  |  |
| --- | --- | --- |
| **USER** | **HASH** | **PASSWORD** |
| student | ac079e1005e36351bc627d3e2a88e774 | user@1234 |
| Guest | 31d6cfe0d16ae931b73c59d7e0c089c0 | <empty/no password> |

# SubLab-3: Cracking SHA512 Password Hashes using Hashcat/John the Ripper

### Password Cracking for “root”:

**COMMAND**:

hashcat -m 1800 root.txt example.dict --rules=/usr/share/hashcat/rules/best64.rule --force

hashcat -m 1800 root.txt –show



### Password Cracking for “iiit”

**COMMAND**:

hashcat -m 1800 iiit.txt iiit\_words.txt --rules=/usr/share/hashcat/rules/best64.rule --force

hashcat -m 1800 iiit.txt --show

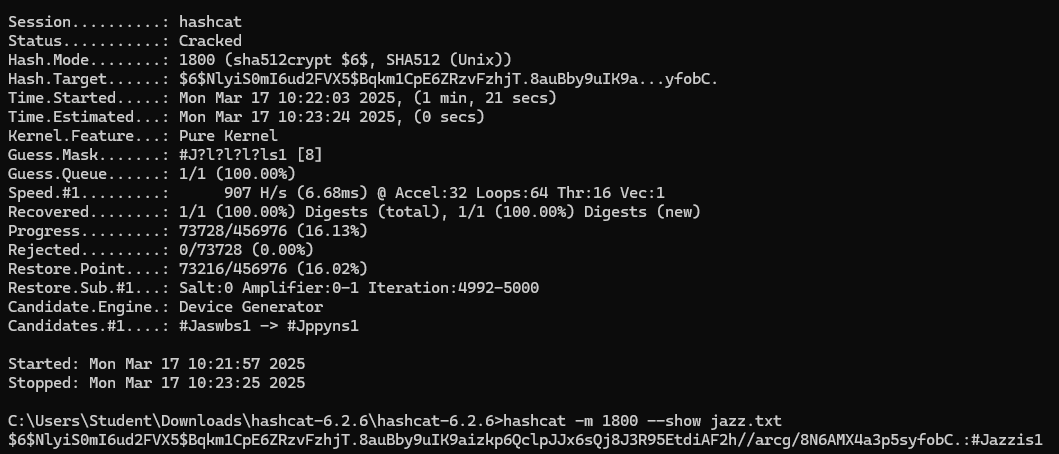


### Password Cracking for “jazz”

**COMMAND**:

hashcat -m 1800 -a 3 jazz.txt "#?u?l?l?l?l?l1" --force

hashcat -m 1800 jazz.txt –show



|  |  |  |
| --- | --- | --- |
| **USERNAME** | **HASH** | **PASSWORD** |
| root | $6$JL.TO.lFJwABA7sa$fy8wh8dIxHg59.vpWDPo1Xotmz3snO  VTo0dGay0m.nNhya13GQZmXu2eTNmu5bGMfYjH  Wss70u0dq6n4JOs9f1 | Nickjonas |
| iiit | $6$R6WMQ54VhiUKK8wV$YgHU9GJAhGUffgm0ixWPwsv  6A4J5Y3v6eeVjejn85D9pU6mScZm338C.YOt0/C2  M3sfMVdO5BkLAKVganONBg/ | Iiitp@2016& |
| jazz | $6$NlyiS0mI6ud2FVX5$Bqkm1CpE6ZRzvFzhjT.8auBby9uIK9aizk  p6Q clpJJx6sQj8J3R95EtdiAF2h//arcg/8N6AMX4a3p5syfobC. | #Jazzis1 |