Cyber Operations

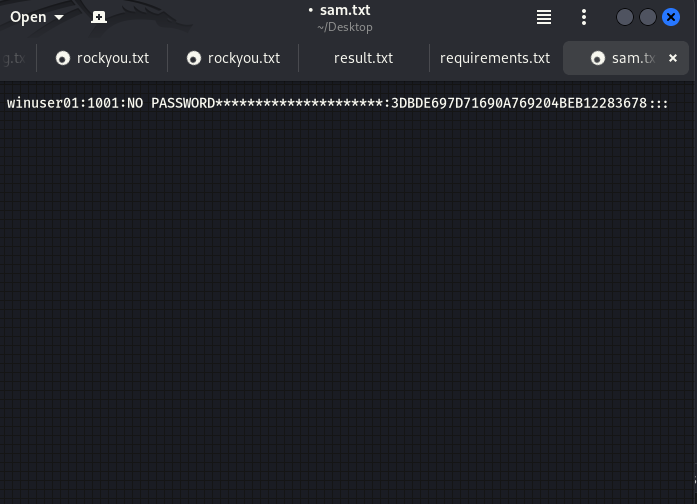
Unit 09 Password Auditing

# **Lab 07 - Offline Password Attacks**

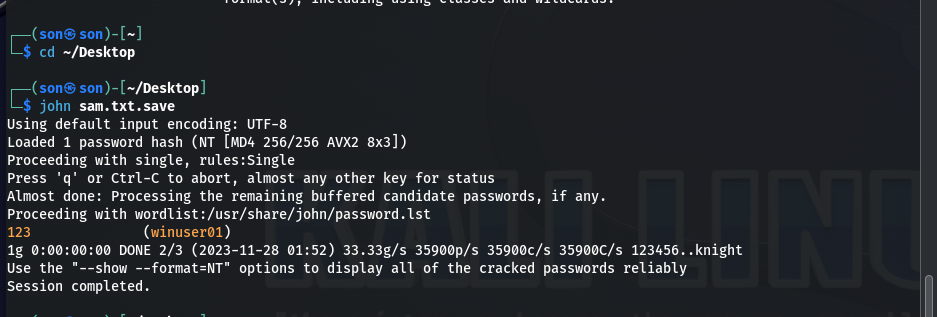
### **winuser01**

You have been given a file titled **sam.txt** that contains a Windows password hash for the **winuser01** account. Using any means necessary with tools such as John the Ripper, crack the password. Take a screenshot of the cracked password.

Tôi đặt mật khẩu cho user winuser01 là 123. Khi hash bằng PwDump 7 thì được kết quả như sau



Kết quả tôi đã crack được password của user winuser01

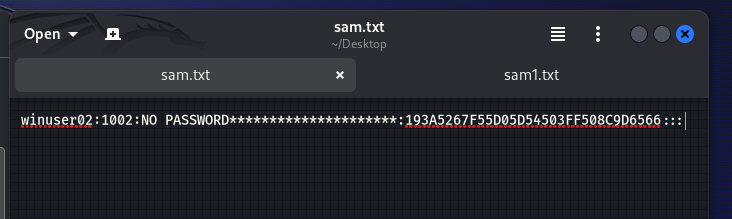


**Hint:** Nothing fancy here, just a normal run through with John will work.

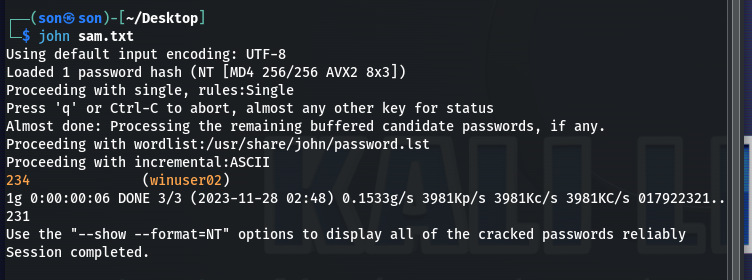
### **Winuser02**

In the same **sam.txt** file, there is a **winuser02** account. Again, crack the password and take a screenshot of the cracked password.

Tôi đặt mật khẩu cho user winuser02 là 234. Khi hash bằng PwDump 7 thì được kết quả như sau



Kết quả tôi đã crack được password của user winuser01



**Hint:** I hear the password policy on this machine isn’t real great. One of the standard wordlists should make short work of this one. I think this person was into online gaming and advertising, the site hosting everything got dumped in 2009…

### **unix01**

After gaining access to a remote UNIX box, you were able to pull the **passwd** and **shadow** files back to your machine.

Combine the files so that you are able to run them through a utility like John the Ripper.

Once they are combined, load up a wordlist and attempt to crack the password for the **unix01** account. Take a screenshot of the cracked password.

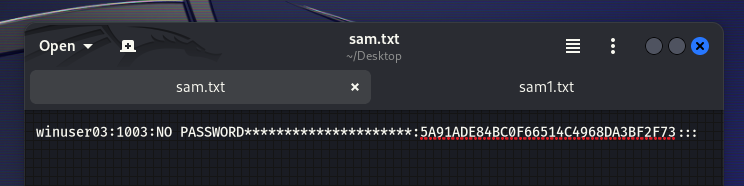
**Hint:** This system implemented a much better password policy than the Windows one. Through some OSINT analysis, we uncovered that the passwords must be between 6-8 characters long, and contains at least three of the following four complexity requirements: lowercase, number, printable symbol, uppercase

### **winuser03**

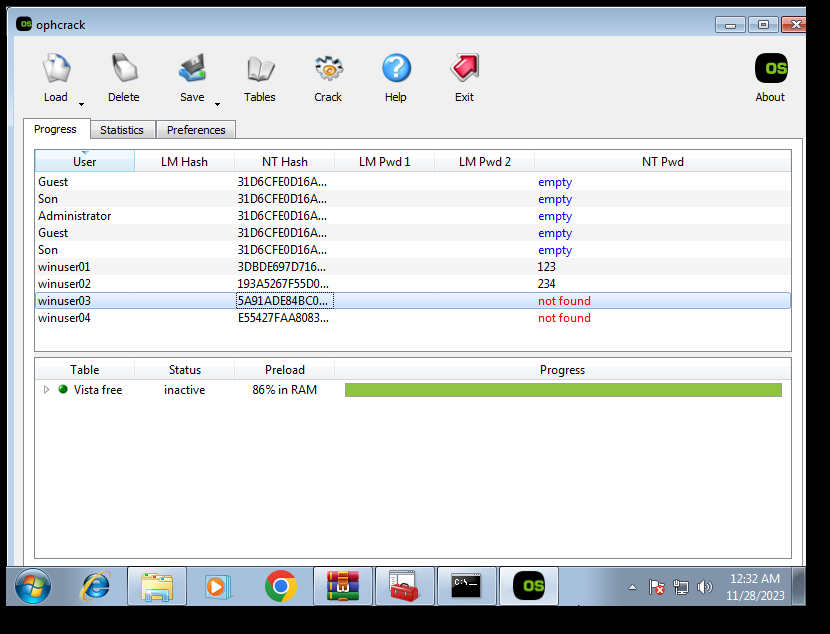
In the same **sam.txt** file, there is a **winuser03** account. Again, crack the password and take a screenshot of the cracked password.

Hint: I saw him typing in his password once during a security training he was giving. I bet that password was at least 20 characters long. Also, every time he sends an email response to me, he types in all caps like he’s shouting or something. Not sure if there’s anything there, but worth a try. Anyways, even though there is an LM hash, those only go up to 14 characters…go for the NTLM.

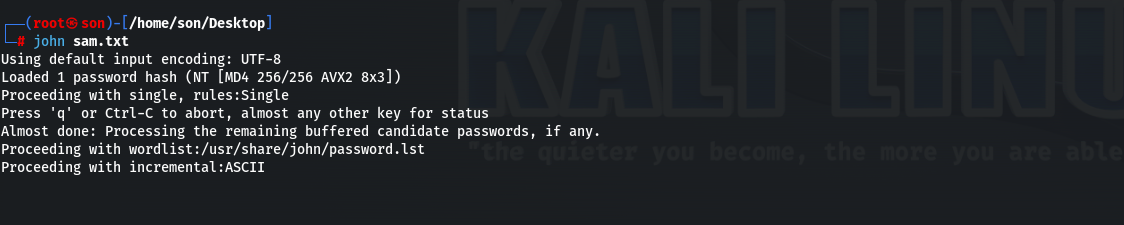
Tôi đặt mật khẩu cho user winuser03 là 0123456789abcdefghijk. Khi hash bằng PwDump 7 thì được kết quả như sau



Dùng OhpCrack không thể crack được password có độ phức tạp cao của user winuser03



Dùng John the Ripper thì phản hồi rất lâu (Có thể từ 1 – 2 tiếng)

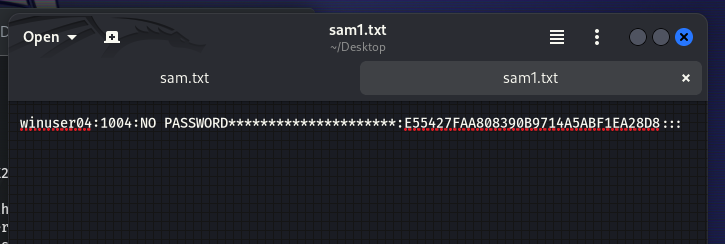


### **winuser04**

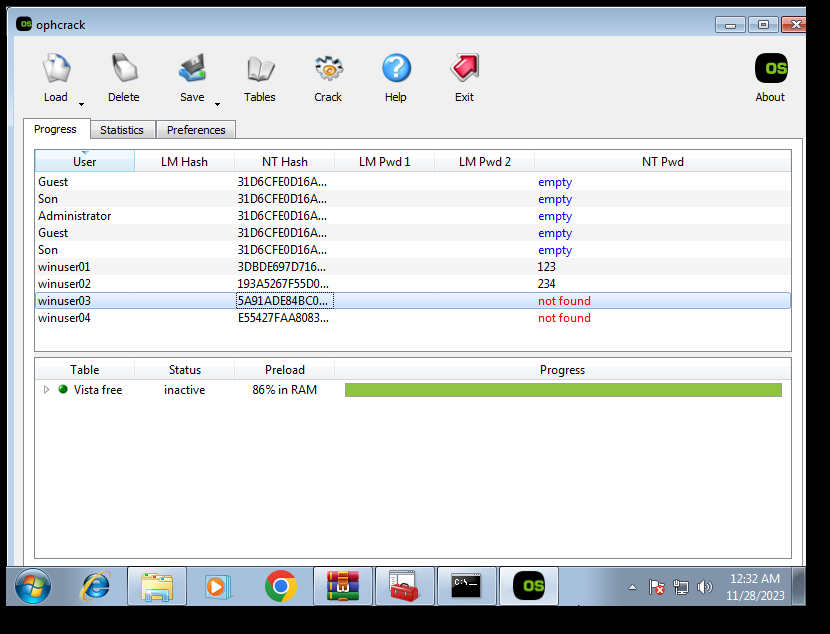
In the same **sam.txt** file, there is a **winuser04** account. Again, crack the password and take a screenshot of the cracked password.

**Hint:** This person is big into cyber, so big into cyber in fact, that’s all he says. Start with the word **cyber** and do some permutations to it. He was born between 1949 and 2019, and capitalized one of the letters in “cyber”.

Tôi đặt mật khẩu cho user winuser04 là Cyber19492019. Khi hash bằng PwDump7 thì được kết quả như sau



Dùng OhpCrack không thể crack được password có độ phức tạp cao của user winuser04



Dùng John the Ripper thì phản hồi rất lâu (Có thể từ 1 – 2 tiếng)

