### **Cybersecurity 401**

**Module 9 - Pentesting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 42 - Pass the Hash with Mimikatz**

## 

## 

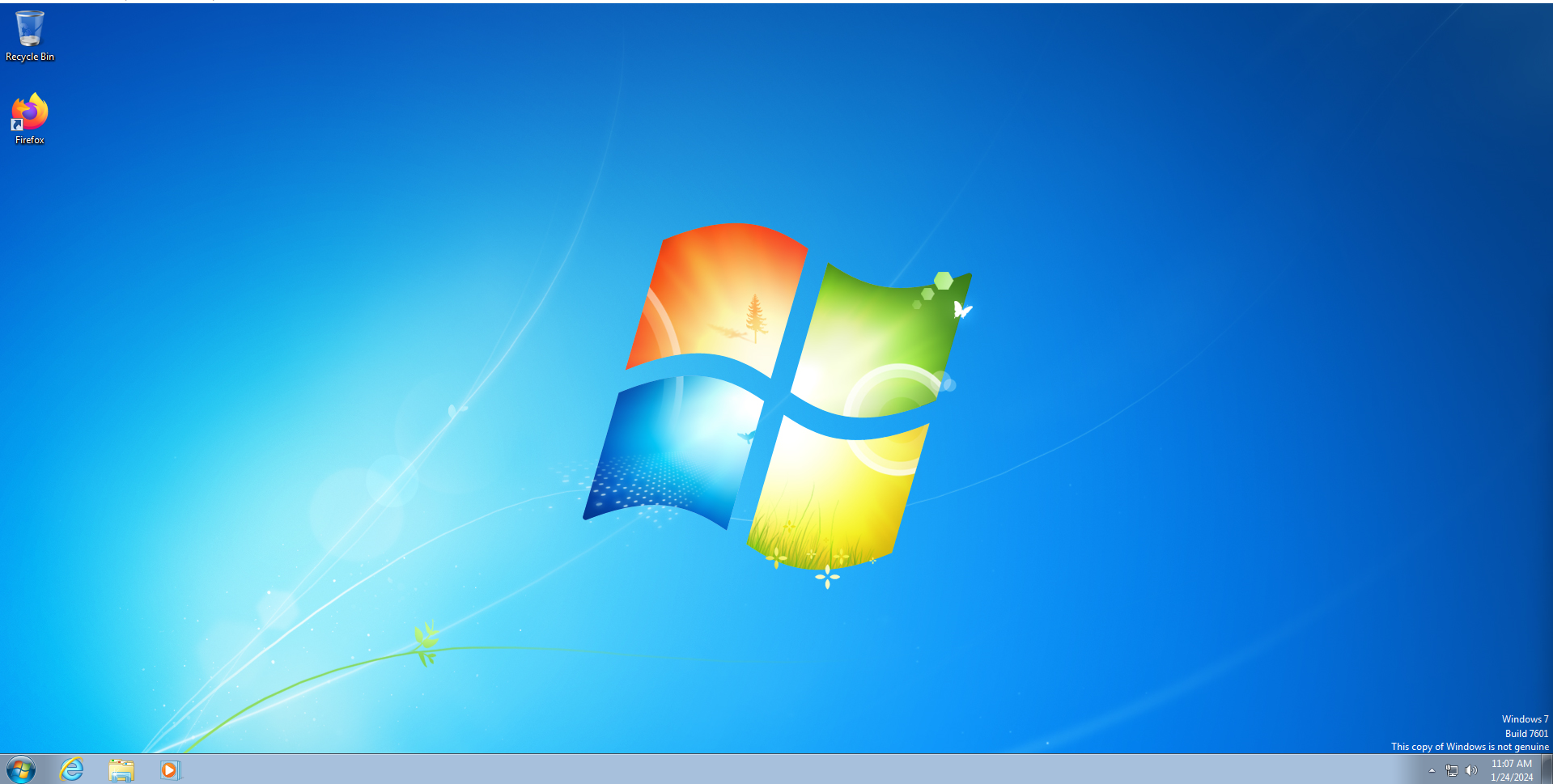
**| Rodrigo Brasil 01/2024 |**

### 

### **Part 1: Staging**

You will need two target systems for this exercise.

* class-42-target1-win7.ova (credentials are labuser/labuser)



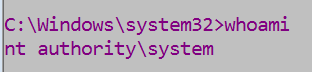
* class-42-target2-win7.ova (credentials are labuser/labuser)



### 

### **Part 2: Someone Pass the Hash!**

* Follow the [Pass the Hash Tutorial](https://cqureacademy.com/blog/identity-theft-protection/pass-hash-attack-tutorial) to achieve an administrator shell from target1 to target2.
  + Dump the hashes of local user accounts and identify the hash of the secret NT Administrator user.
  + Using the included tools in C:\Tools, create a local terminal that assumes the identity of the secret NT Administrator user.



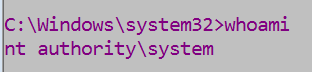
* + Abuse your newfound powers to establish a persistent administrator shell to class-42-target2-win7.
* Create a file on target2’s desktop. Once you’re able to remotely manipulate the target computer as the Administrator user, this portion of the lab is complete.

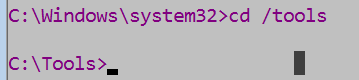
*At this point in a cyber attack or pentest, you could use Mimikatz to “pivot” from computer to computer, or deliver a custom malware payload that opens up additional opportunities to infiltrate the organization’s systems.*

* Document the process and include screenshots of key steps taken.

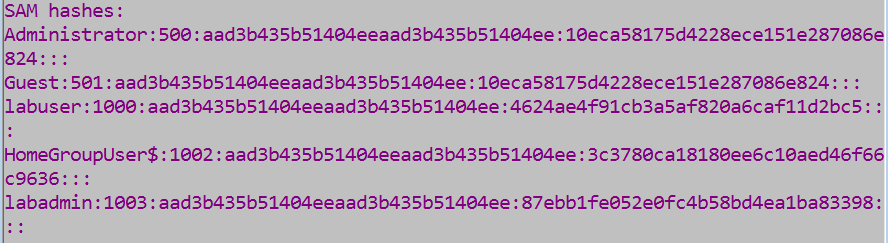
### 

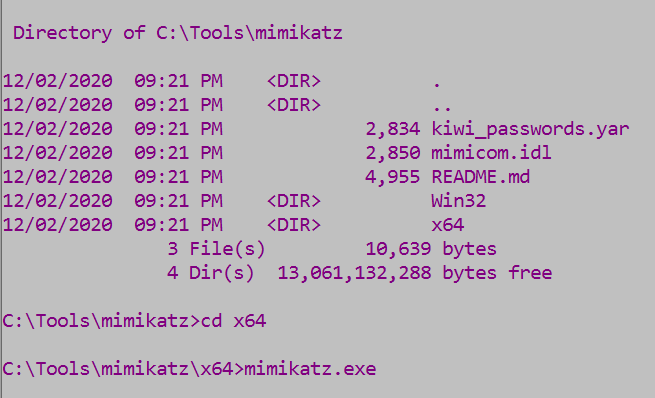
### 



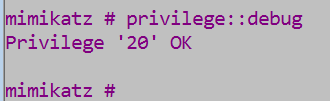


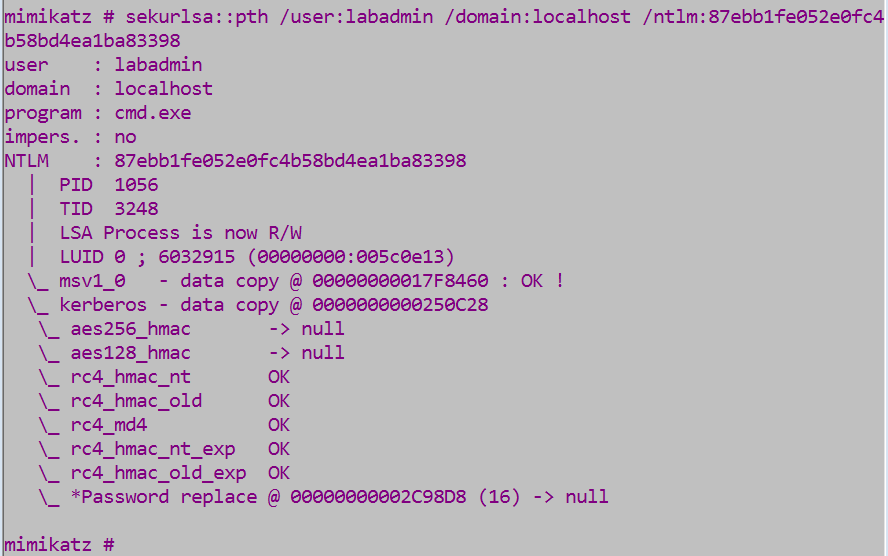


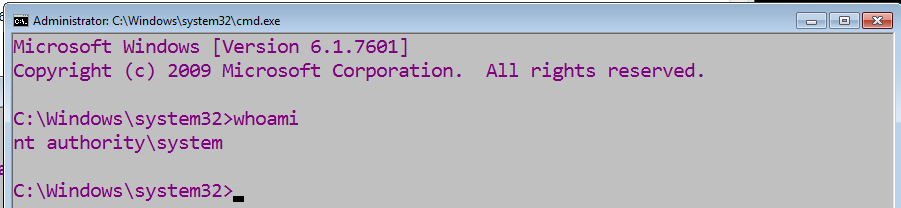




### 







### 

### **Part 3: Blogging**

Writing blog articles is common practice in the security world. Making useful or interesting contributions to the community is a great way to get your name out there! In this segment, try your hand at writing a blog article about the lab today. Answer the following and include screenshots of key steps taken/challenges faced.

* What is Mimikatz?
* How does the “pass the hash” attack technique work?
* What conditions are required in order for this attack to succeed?
* What steps did you take?
* What challenges did you face in learning this attack technique?
* What are some concluding thoughts on hacking Windows after your learned Mimikatz?

Here’s an outline you can follow.

* Introduction
* Synopsis
* Terms
* Tools used
* Attack scenario
* Attack vector
* Conclusion

You don’t have to post this on the internet if you don’t want to. Do write this in the voice of a security blogger and submit it as your Google Doc today.