Hacking Articles
Raj Chandel's Blog

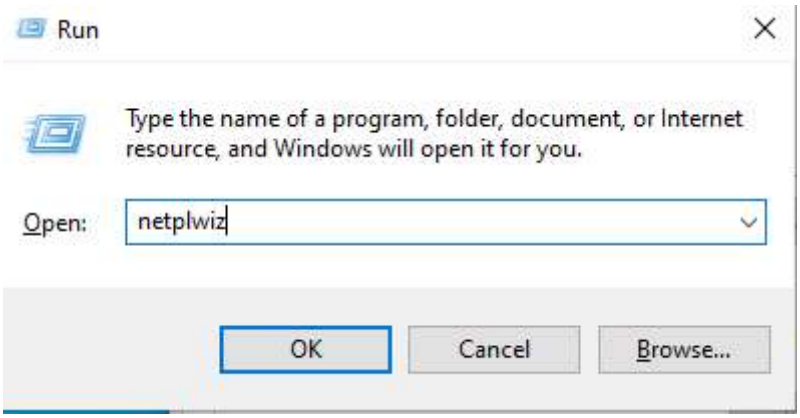
Credential Dumping: Windows Autologon Password

posted in RED TEAMING on DECEMBER 18, 2020 by RAJ CHANDEL

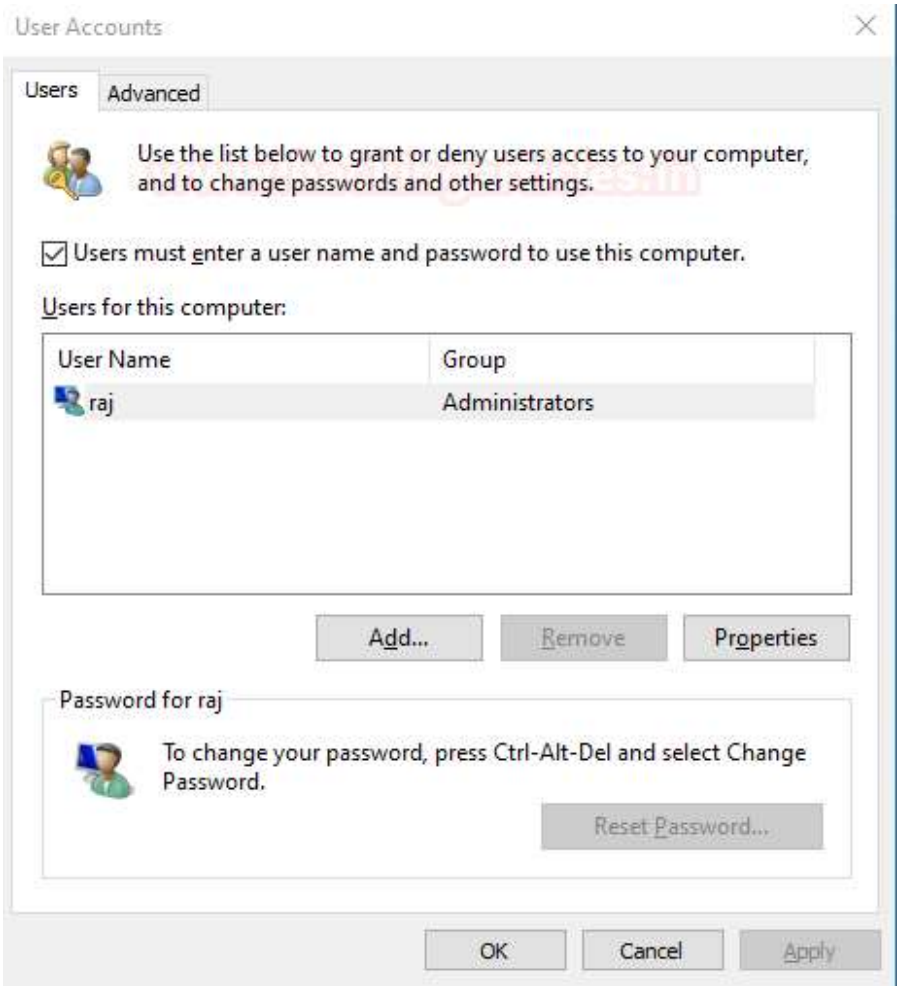
Autologon helps you to conveniently customize the built-in Autologon mechanism for Windows. Rather than waiting for a user to enter their name and password, Windows will automatically log in to the required user using the credentials you submit with Autologon, which are encrypted in the registry.

In this post, we will try to dump the stored autologin credentials with the help of two different tools.

Let's see the settings for autologin, first, you need to access the User Accounts Control Panel using **netplwiz** command inside the run prompt.



Choose the account for autologon, for example, we have selected user Raj.

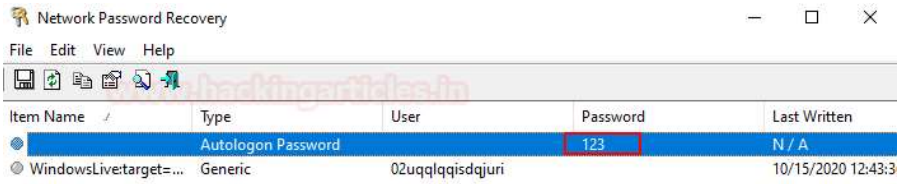


Enter your password once and then a second time to confirm it and uncheck the box "*Users must enter a user name and password to use this computer*" then click OK.

Method 1: Nirsoft-Network Password Recovery

Network Password Recovery is very easy to use, install and run the tool on the local machine whose password you chose to extract. It will dump the stored credential for the autologon account.

You can download this tool from **here**



Method 2: DecryptAutologon.exe

This tool can extract/decrypt the password that was stored in the LSA by SysInternals AutoLogo.

You can download its Compiled Version **HERE**

Run the downloaded .exe as shown in the given image, it will dump the password in the Plain text.

Author: Vishva Vaghela is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on 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
← BURP SUITE FOR PENTESTER: WEB SCANNER & CRAWLER

NEXT POST
HOGWARTS: BELLATRIX VULNHUB WALKTHROUGH →

1 Comment

→ CREDENTIAL DUMPING: WINDOWS AUTOLOGON PASSWORD

LESIBANA BO3
December 19, 2020 at 5:46 am

Hi, I really appreciate and want to thank you for your posts. I really learn a lot about your posts and want to specifically want to ask you to keep posting as I learn a lot about them. As a Director and Founder of my Company a Cyber and Digital Forensics Company in my country South Africa, I says THANK YOU

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

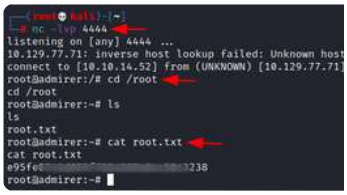
SUBSCRIBE

Join our Training Programs

Follow me on Twitter

Hacking Articles
@hackinarticles

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



Categories

- Cryptography & Steganography
- 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