Ex0a0 Report

Benjamin Ruddy

2022-10-31

Contents

Technical Report

Introduction

Finding: *Weak and commonly exploited password on domain account*

Severity Rating: 4.0

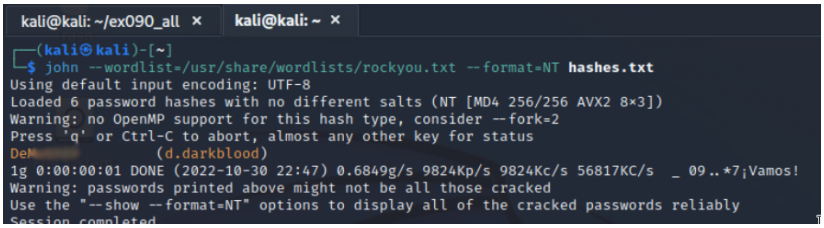
CVSS Base Severity Rating: 4.0 AV:L AC:L PR:N UI:N S:U C:H I:N A:N

Vulnerability Description

User `d.darkblood` on the ARTSTAILOR domain contains a weak, commonly exploited password that is available on a variety of online password lists, or "word lists," that attackers often employ to gain access to accounts.

Should an attacker gain access to the Windows password hashes, such as with a Man-in-the-Middle attack or through exploitation of an individual host on the network, this would allow them to quickly achieve lateral movement to the d.darkblood account.

Confirmation method



Mitigation or Resolution Strategy

As per the NIST SP 800-63B publication, it is good practice to compare user passwords against a common list ("blacklist") of passwords that have been breached many times in the past. In this case, it is recommended that users check if the password they are using for their domain accounts is present in the following list, available online:

https://github.com/praetorian-inc/Hob0Rules/blob/master/wordlists/rockyou.txt.gz

Attack Narrative

This exercise was relatively straightforward considering the work done here involves the successful post-exploitation of Exercise090, which provided us with

various hashes through `mimikatz`.

What follows is our procedure to attempt password cracking with these aforementioned hashes.

Our hashes

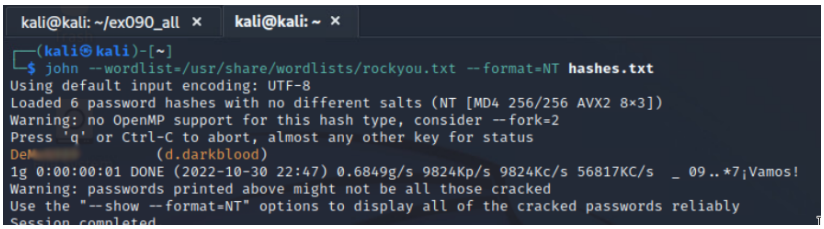
To briefly summarize our hash dumping methods, we used the following modules from the `mimikatz` program:

```
token::elevate
pirivilege::debug
sekurlsa::logonPasswords
lsadump::sam
```

Running these on the costumes.artstailor.com machine with the administrator account we created through the exploit in Ex090, we were able to successfully dump various stored password hashes from memory. These were then stored on the remote server at plunder.prob3.com for the password-cracking activity in this exercise.

Password Cracking

After compiling all our hashes into a separate texts files (separate files for each hash type, in the format `username:hash`) and running John The Ripper on them with the `rockyou.txt` word list, we achieved a successful crack with the hash of user 'd.darkblood'. The following screen capture blurs most of the password to protect the privacy of the account:



For details on remediation strategies, please refer ot the **Technical Report** section.

MITRE ATT&CK Framework TTPs

TA0006: Credential Access
- **T1574:** Brute Force
  - **.002:** Password Cracking