Penetration Test Exercise 0a0

Esteban Calvo

2023-10-16

Contents

1 Technical Report

1.1 Finding: *Network User Compromised*

Severity Rating

Risk Factor: High **CVSS Base Severity Rating: 8.3** AV:N AC:L PR:N UI:N S:C C:L I:L A:L

Vulnerability Description

A list of hashes was found using a mimikatz exploit. This list was used against a list of known hashes to find the credentials of a network user. This attack revealed the credentials of one user.

Confirmation method

The hashes that had been previously found must be formatted in **user:hash** format. The use of the John the Reaper tool along with the rockyou wordlist must be employed as follows

```
john --wordlist=<pathToRockYou.txt> --format=NT passwordHashes.txt
```

Mitigation or Resolution Strategy

It is recommended to change all user passwords and to make sure that the hashes are checked against well known wordlists such as rockyou and that more password requirements are enforced such as longer password lengths as is recommended by NIST Publication 800-63B. Creating more complex passwords checked against dictionaries and longer passwords must be employed to prevent this kind of attack from occurring again.

2 Attack Narrative

2.1 Formatting

The lsadump with the local Security Account Manager (SAM) NT hashes was used for this exercise. The specifications for the John the Ripper tool specified that it must be in **user:hash** format and therefore the file was formatted as follows for all users

```
Administrator:d9a8...dab9
```

2.2 Password Cracking

As stated above, John the Ripper was used as follows

```
john --wordlist=<pathToRockYou.txt> --format=NT passwordHashes.txt
```

which revealed the following partially hidden password and login

```
User: d.darkblood
Password: De...09
```

2.3 MITRE ATT&CK Framework TTPs

TA0006: Credential Access
    T1110: Brute Force
        .002: Password Cracking