GPP Passwords

Description

`SYSVOL` is a network share on all Domain Controllers, containing logon scripts, group policy data, and other required domain-wide data. AD stores all group policies in `\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`. When Microsoft released it with the Windows Server 2008, `Group Policy Preferences` (`GPP`) introduced the ability to store and use credentials in several scenarios, all of which AD stores in the policies directory in `SYSVOL`.

During engagements, we might encounter scheduled tasks and scripts executed under a particular user and contain the username and an encrypted version of the password in XML policy files. The encryption key that AD uses to encrypt the XML policy files (the `same` for all Active Directory environments) was released on Microsoft Docs, allowing anyone to decrypt credentials stored in the policy files. Anyone can decrypt the credentials because the `SYSVOL` folder is accessible to all 'Authenticated Users' in the domain, which includes users and computers. Microsoft published the AES private key on MSDN:

2.2.1.1.4 Password Encryption

Article • 02/14/2019 • 2 minutes to read

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Also, as a reference, this is what an example XML file containing an encrypted password looks like (note that the property is called `cpassword`):

```
<?xml version="1.0"?>
<Groups clsid="A">
<User clsid="A">
<Properties action="C" fullName="svc-iis" descrption="" cpassword="qRI/NPQtItGsMjwMkhF7ZDvK6n9KlOhBZ/XShO2IZ80"
changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" userName="svc-iis"/>
</User>
</Groups>
```

Attack

To abuse `GPP Passwords`, we will use the Get-GPPPassword function from `PowerSploit`, which automatically parses all XML files in the Policies folder in `SYSVOL`, picking up those with the `cpassword` property and decrypting them once detected:

GPP Passwords

```
PS C:\Users\bob\Downloads> Import-Module .\Get-GPPPassword.ps1
PS C:\Users\bob\Downloads> Get-GPPPassword

UserName  : svc-iis
NewName   : [BLANK]
Password  : abcd@123
Changed   : [BLANK]
File      : \\EAGLE.LOCAL\SYSVOL\eagle.local\Policies\{73C66DBB-81DA-44D8-BDEF-20BA2C27056D}\
```

Cheat Sheet
Go to Questions

Table of Contents

Setting the stage
Introduction and Terminology
Overview and Lab Environment

Attacks & Defense
Kerberoasting
AS-REProasting
GPP Passwords
GPO Permissions/GPO Files
Credentials in Shares
Credentials in Object Properties
DCSync
Golden Ticket
Kerberos Constrained Delegation
Print Spooler & NTLM Relaying
Coercing Attacks & Unconstrained Delegation
Object ACLs
PKI - ESC1

Skills Assessment
Skills Assessment

My Workstation
OFFLINE
Start Instance
∞ / 1 spawns left

```
            Machine\Preferences\Groups\Groups.xml
NodeName  : Groups
Cpassword : qRI/NPQtItGsMjwMkhF7ZDvK6n9KlOhBZ/XShO2IZ80
```

```
PS C:\Users\bob\Downloads> Get-GPPPassword

UserName  : svc-iis
NewName   : [BLANK]
Password  : abcd@123
Changed   : [BLANK]
File      : \\EAGLE.LOCAL\SYSVOL\eagle.local\Policies\{73C66DBB-81DA-44D8-BDEF-20BA2C27056D}\
Machine\Preferences\Groups
            \Groups.xml
NodeName  : Groups
Cpassword : qRI/NPQtItGsMjwMkhF7ZDvK6n9KlOhBZ/XShO2IZ80
```

Prevention

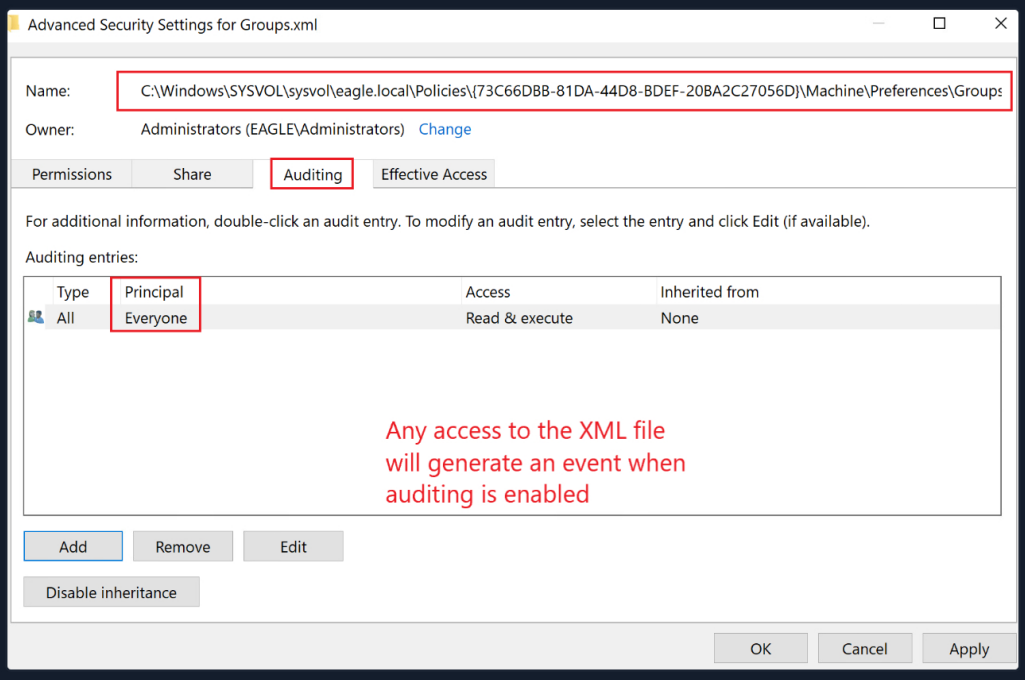
Once the encryption key was made public and started to become abused, Microsoft released a patch (KB2962486) in 2014 to prevent caching credentials in GPP. Therefore, GPP should no longer store passwords in new patched environments. However, unfortunately, there are a multitude of Active Directory environments built after 2015, which for some reason, do contain credentials in SYSVOL. It is therefore highly recommended to continuously assess and review the environment to ensure that no credentials are exposed here.

It is crucial to know that if an organization built its AD environment before 2014, it is likely that its credentials are still cached because the patch does not clear existing stored credentials (only prevents the caching of new ones).

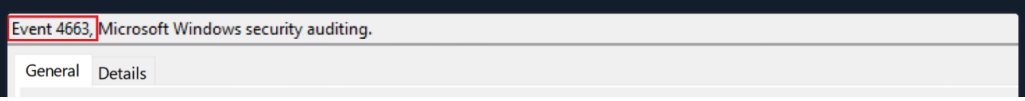
Detection

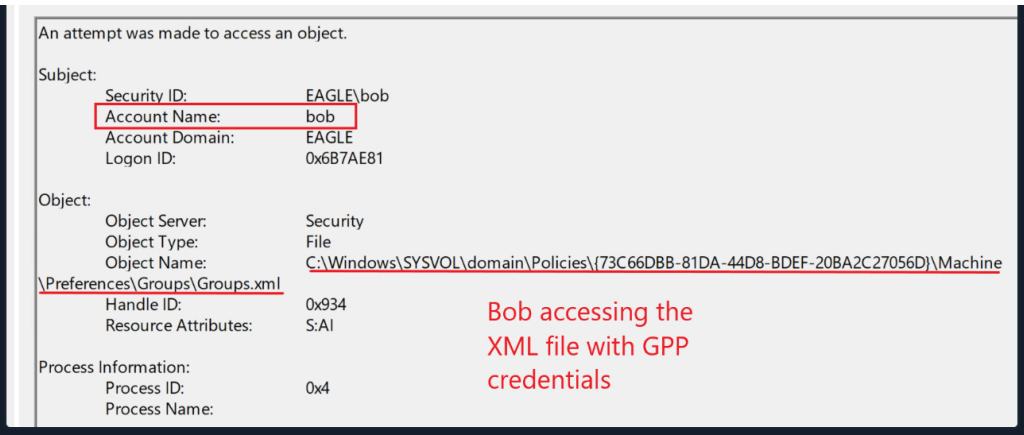
There are two detection techniques for this attack:

- Accessing the XML file containing the credentials should be a red flag if we are auditing file access; this is more realistic (due to volume otherwise) regarding detection if it is a dummy XML file, not associated with any GPO. In this case, there will be no reason for anyone to touch this file, and any attempt is likely suspicious. As demonstrated by Get-GPPPasswords, it parses all of the XML files in the Policies folder. For auditing, we can generate an event whenever a user reads the file:

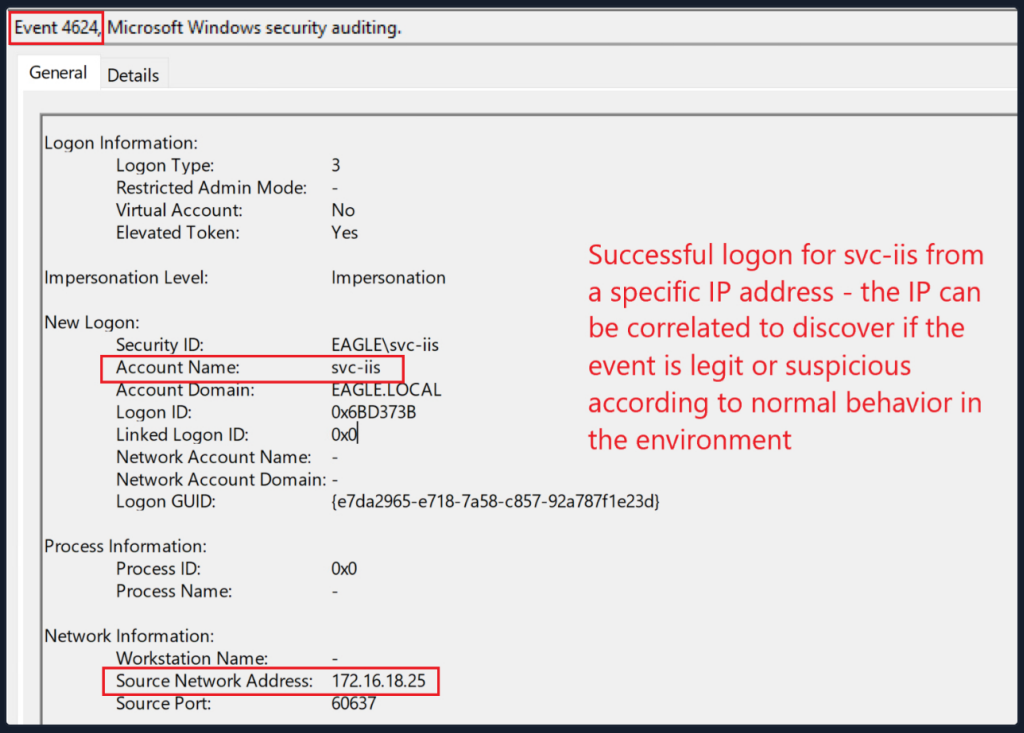


Once auditing is enabled, any access to the file will generate an Event with the ID 4663:





- Logon attempts (failed or successful, depending on whether the password is up to date) of the user whose credentials are exposed is another way of detecting the abuse of this attack; this should generate one of the events `4624` (`successful logon`), `4625` (`failed logon`), or `4768` (`TGT requested`). A successful logon with the account from our attack scenario would generate the following event on the Domain Controller:



In the case of a service account, we may correlate logon attempts with the device from which the authentication attempt originates, as this should be easy to detect, assuming we know where certain accounts are used (primarily if the logon originated from a workstation, which is abnormal behavior for a service account).

Honeypot

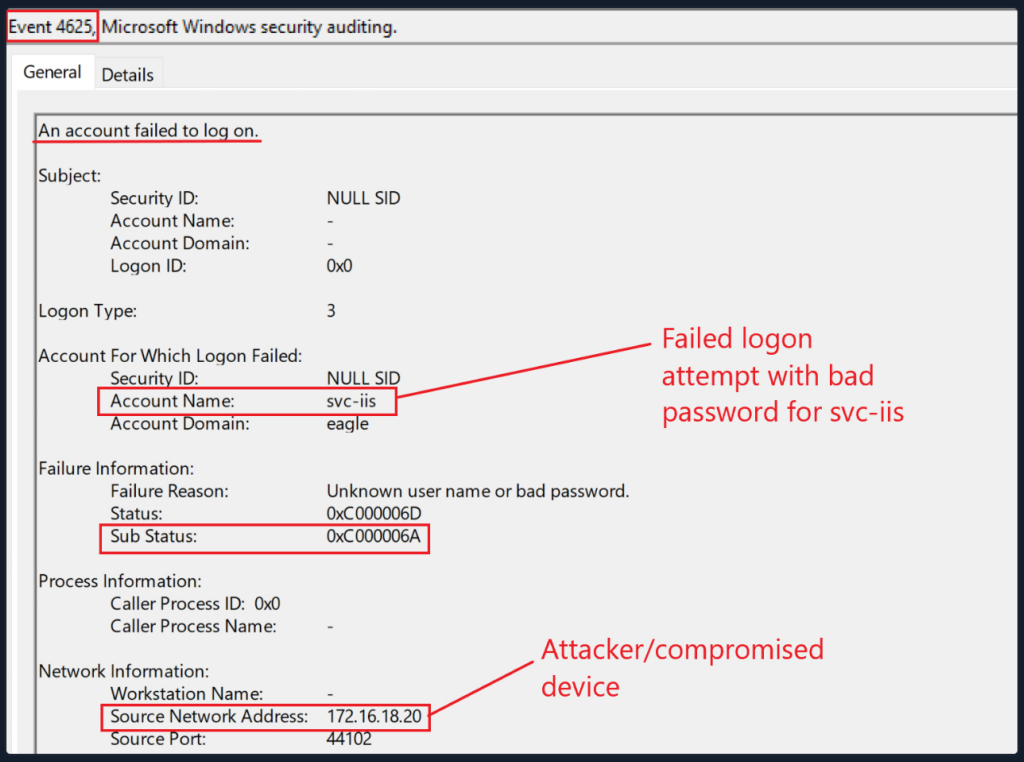
This attack provides an excellent opportunity for setting up a trap: we can use a semi-privileged user with a `wrong password`. Service accounts provide a more realistic opportunity because:

- The password is usually expected to be old, without recent or regular modifications.
- It is easy to ensure that the last password change is older than when the GPP XML file was last modified. If the user's password is changed after the file was modified, then no adversary will attempt to login with this account (the password is likely no longer valid).
- Schedule the user to perform any dummy task to ensure that there are recent logon attempts.

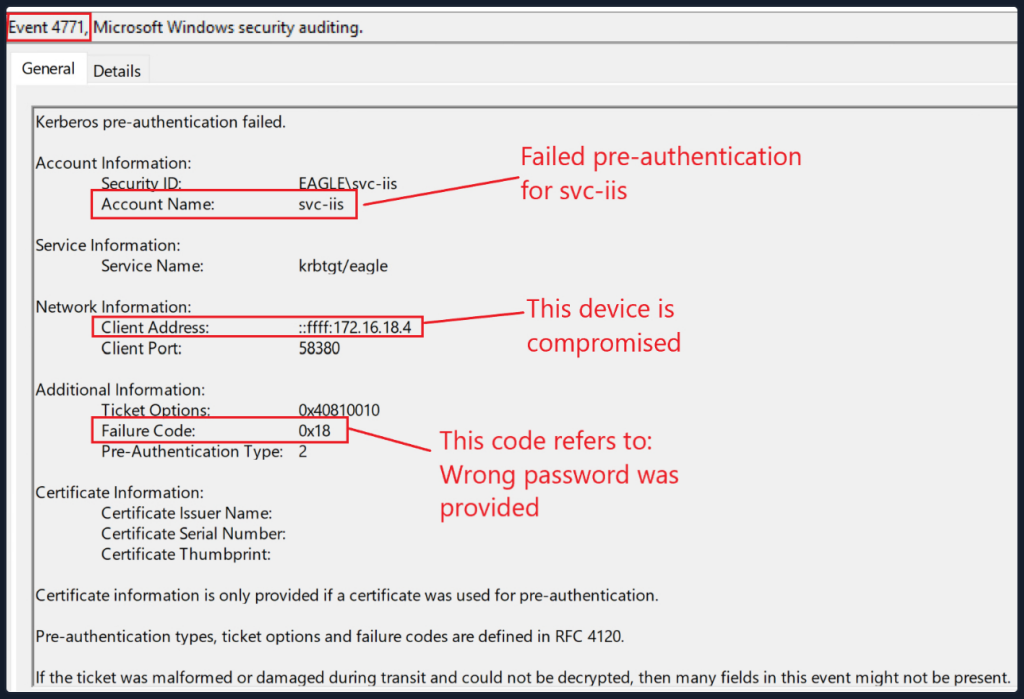
When we do the above, we can configure an alert that if any successful or failed logon attempts occur with this service account, it must be malicious (assuming that we whitelist the dummy task logon that simulates the logon activity in the alert).

Because the provided password is wrong, we would primarily expect failed logon attempts. Three event IDs (4625, 4771, and 4776) can indicate this; here is how they look for our playground environment if an attacker is attempting to authenticate with a wrong password:

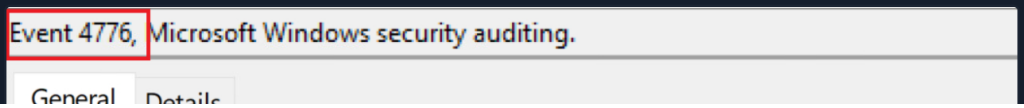
- 4625

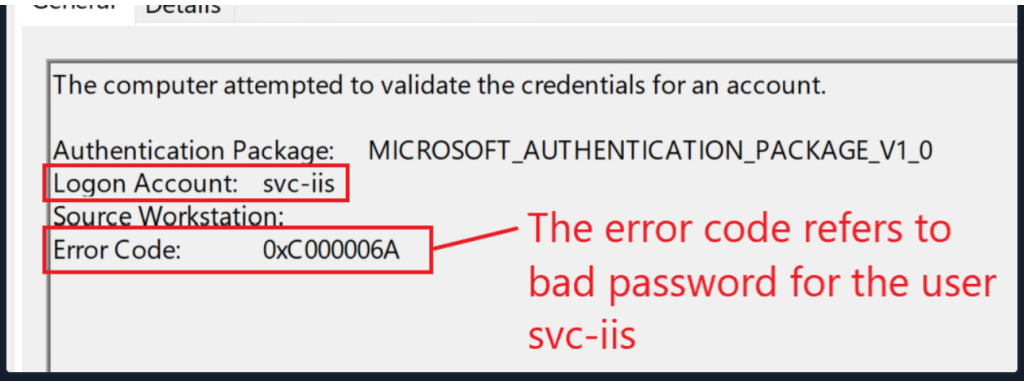


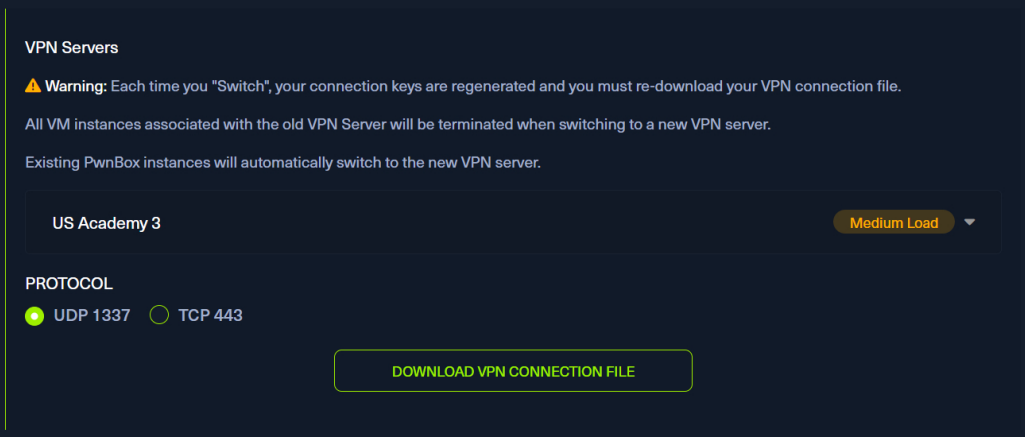
- 4771

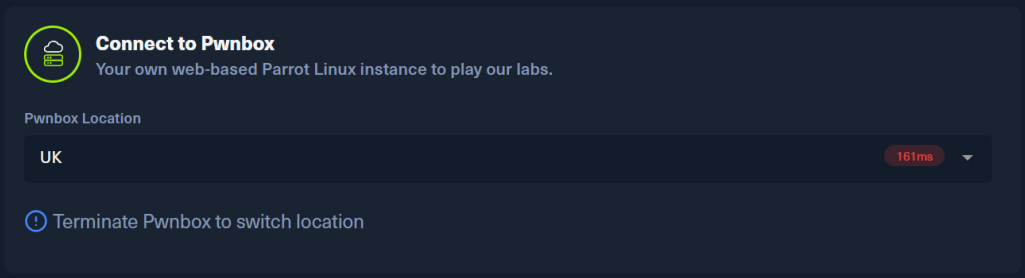


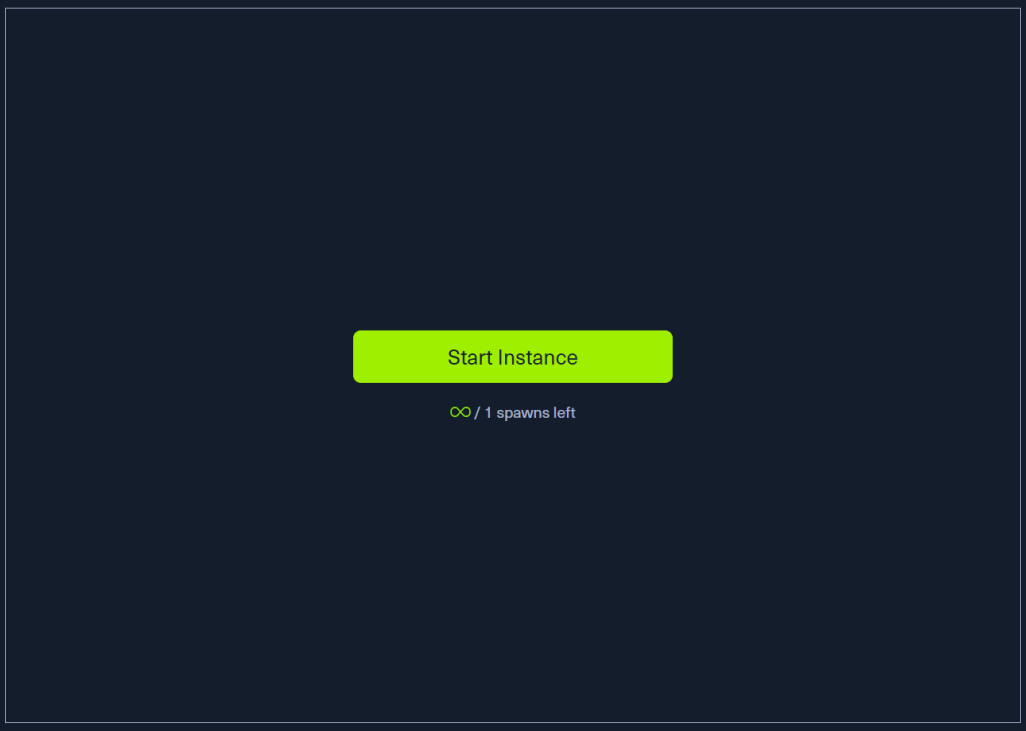
- 4776











Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Download VPN Connection File

Target(s): Click here to spawn the target system!

RDP to with user "bob" and password "Slavi123"

+ 1 Connect to the target and run the Powersploit Get-GPPPassword function. What is the password of the svc-iis user?

abcd@123

Submit Hint

+ 1 After running the previous attack, connect to DC1 (172.16.18.3) as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the Access Mask of the generated events?

0x80

Submit Hint

Previous Next

Mark Complete & Next