Lateral Movement to the Cloud with Pass-the-PRT

blog.netwrix.com/2023/05/13/pass-the-prt-overview

Jeff Warren

Attackers use a variety of tactics to spread laterally across on-premises Windows machines, including Pass-the-Ticket, Pass-the-Hash, Overpass-the-Hash and Golden Tickets attacks. But similar techniques are also effective in moving laterally from a compromised workstation to connected cloud resources, bypassing strong authentication measures like MFA.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

This article explains how attackers can perform lateral movement to the cloud with an attack called Pass-the-PRT.

What is a PRT?

A primary refresh token (PRT) is similar to a Kerberos ticket-granting ticket (TGT) — both are used to provide single sign-on (SSO). But while a TGT is for Windows systems, a PRT enables you to log into a Windows 10 device and then access Azure and Microsoft 365 resources without having to re-authenticate. The Windows 10 device must be Azure-joined or hybrid Azure-joined.

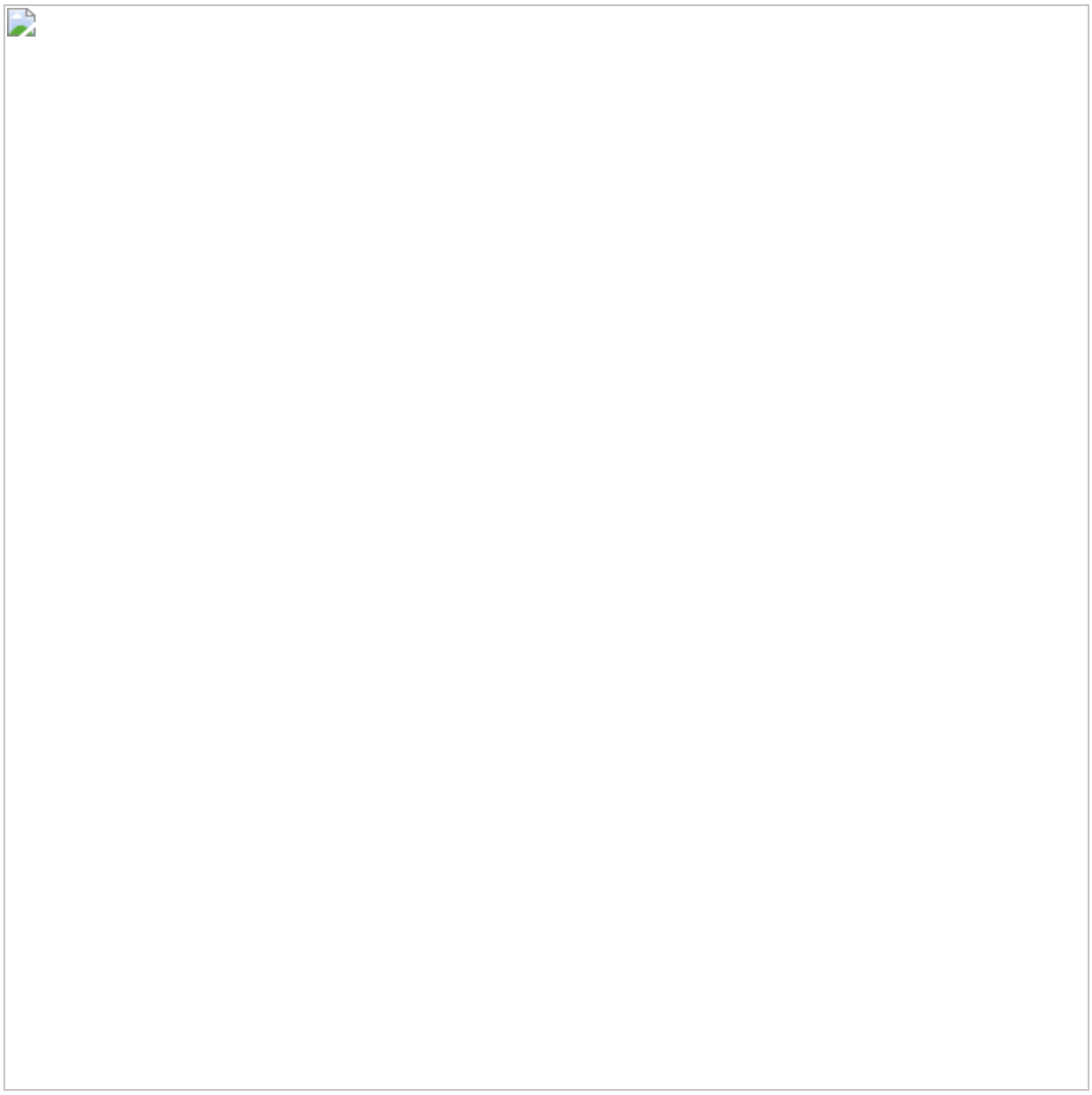
Here's an overview of how this process works: When you log in, your Windows 10 device will communicate with the Windows 10 Cloud Authentication Provider. Its Azure plug-in will validate your credentials and return a PRT and a session key. Your device will re-encrypt the session key with its Trusted Platform Module (TPM) and then store both the key and the PRT in LSASS. Then, when you attempt to log into a website using a browser that supports SSO to Azure (either Edge or Chrome with the Windows 10 extension), the Cloud Authentication Provider will create a PRT cookie for the browser and use that cookie to get tokens from Azure AD. Azure AD will validate the PRT cookie and let you in.

(If you want to go deeper, check out the Microsoft documentation, Jairo Cadena's summary of PRT and SSO, this article on PRT by Dirk-jan Mollema, and the ROADtoken and RequestAADRefreshToken projects on GitHub.)

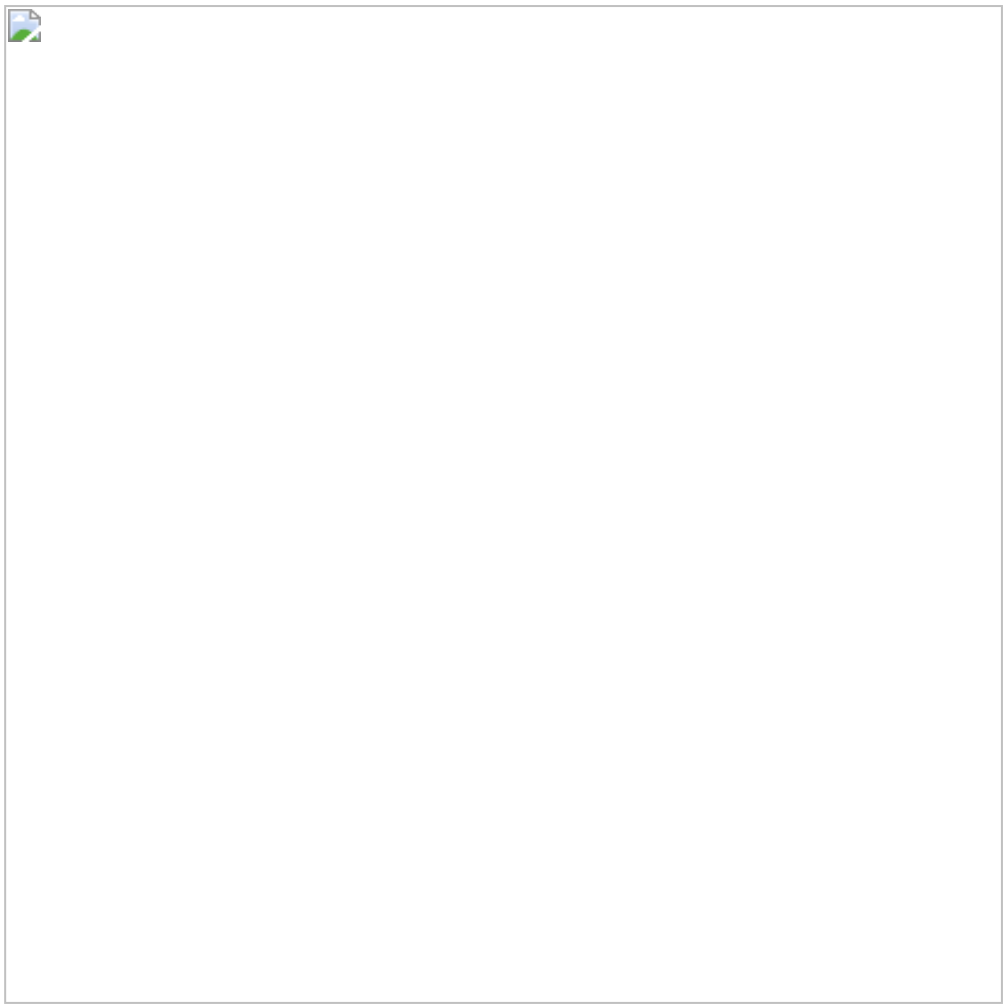
To see whether you have a PRT, run this command:

```
Dsregcmd.exe /status
```

In the SSO State section, check **AzureAdPrt**; if it is set to YES, you have a PRT.



If it is set to NO, use the command below to check whether your device is joined to Azure AD, since that is required for PRTs to be issued.



Performing a Pass-the-PRT Attack

If an adversary manages to get a user's PRT and session key, they can create PRT cookies that give them access to web resources as that user, bypassing any conditional access requirements in place. A PRT is valid for 14 days, so they have access for up to 2 weeks unless the account is disabled.

Let's walk through exactly how we can perform such an attack.

Prerequisite: We have compromised a Windows 10 device that has a PRT issued to it, and we have local admin privileges on that machine.

Overview of steps:

1. Extract the PRT from LSASS and save it for later.
2. Extract the session key.
3. Decrypt the session key and use it using a DPAPI masterkey. We've learned about that in the Pass-the-Cookie attack and will use the same approach.
4. Using the decrypted Session Keyto obtain the derived key and the context.This is needed to create our PRT cookie. The derived key is what is used to sign the JWT for the cookie.
5. From any system, use the PRT, the derived key and the context to create a new PRT cookie.

6. Import the cookie into our Chrome browser session. Now we will be authenticated to websites as the user — without ever knowing their password or having to handle any MFA prompts.

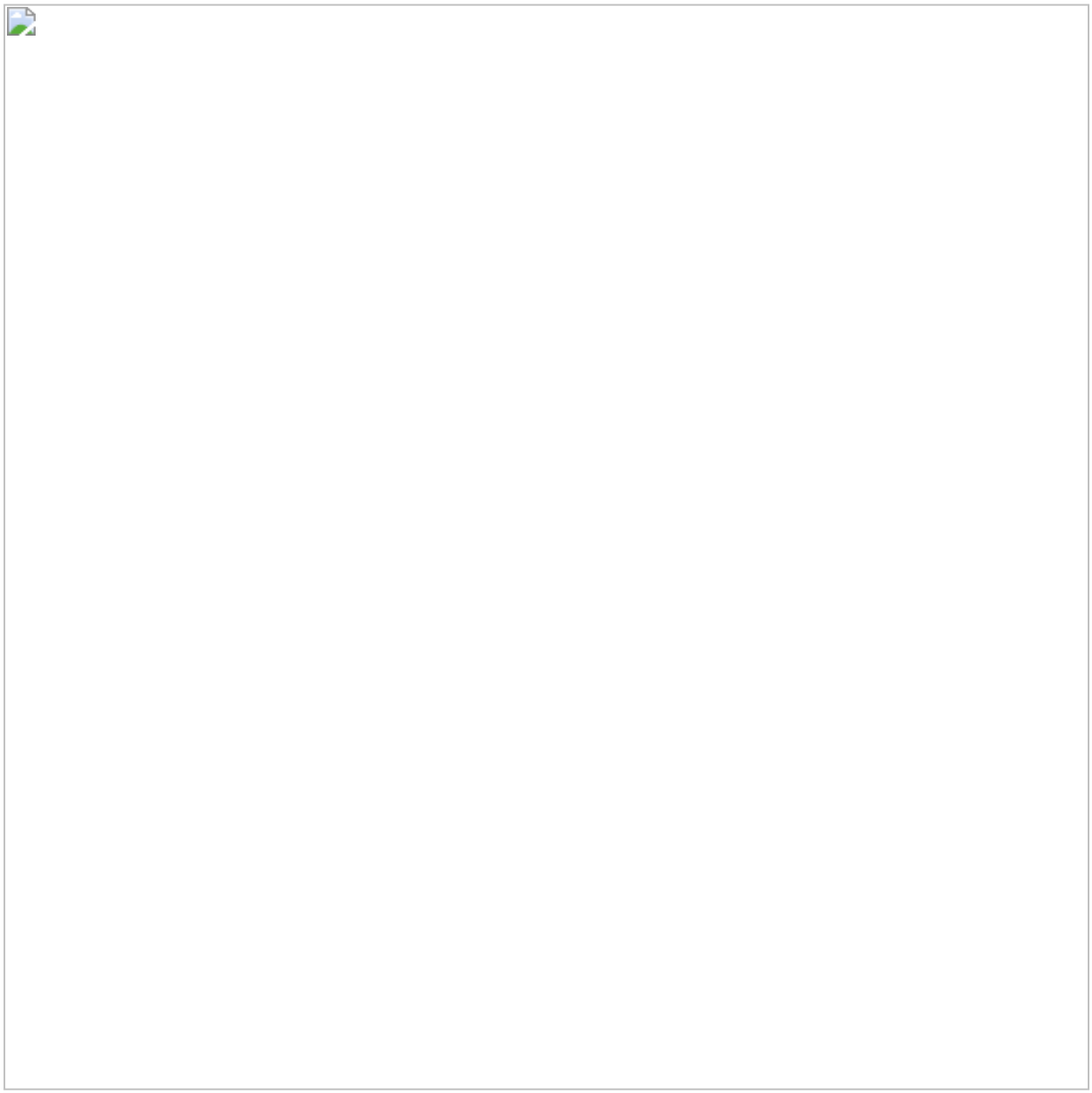
Let's dive deeper into each step.

Step 1. Extract the PRT from LSASS.

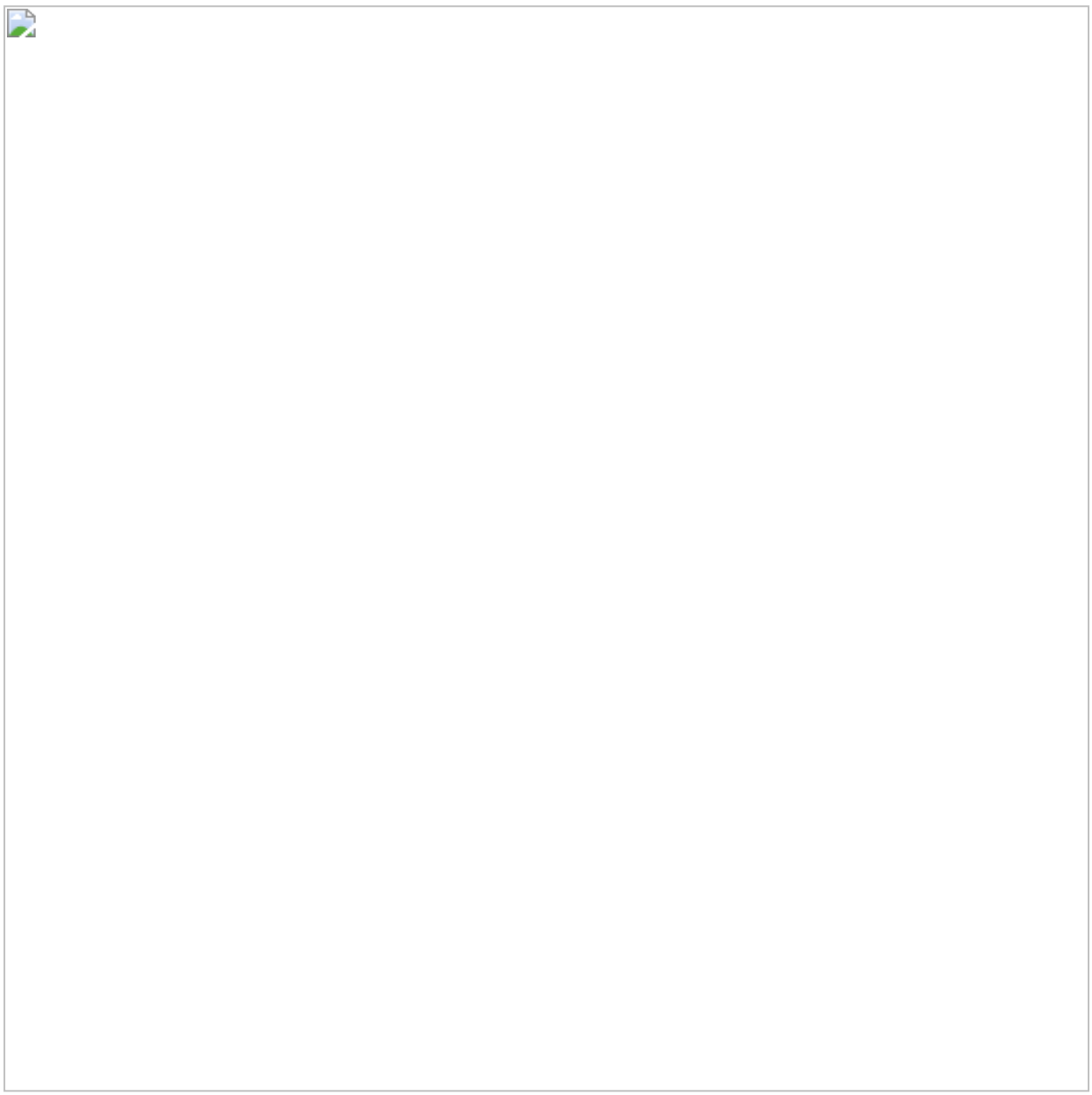
To see PRT data for the machine we have compromised, we use the following command in Mimikatz release 2.2.0 20200807 or later:

```
Privilege::debug
Sekurlsa::cloudap
```

Here is the output. We will copy the part labeled **PRT** and save it for later.

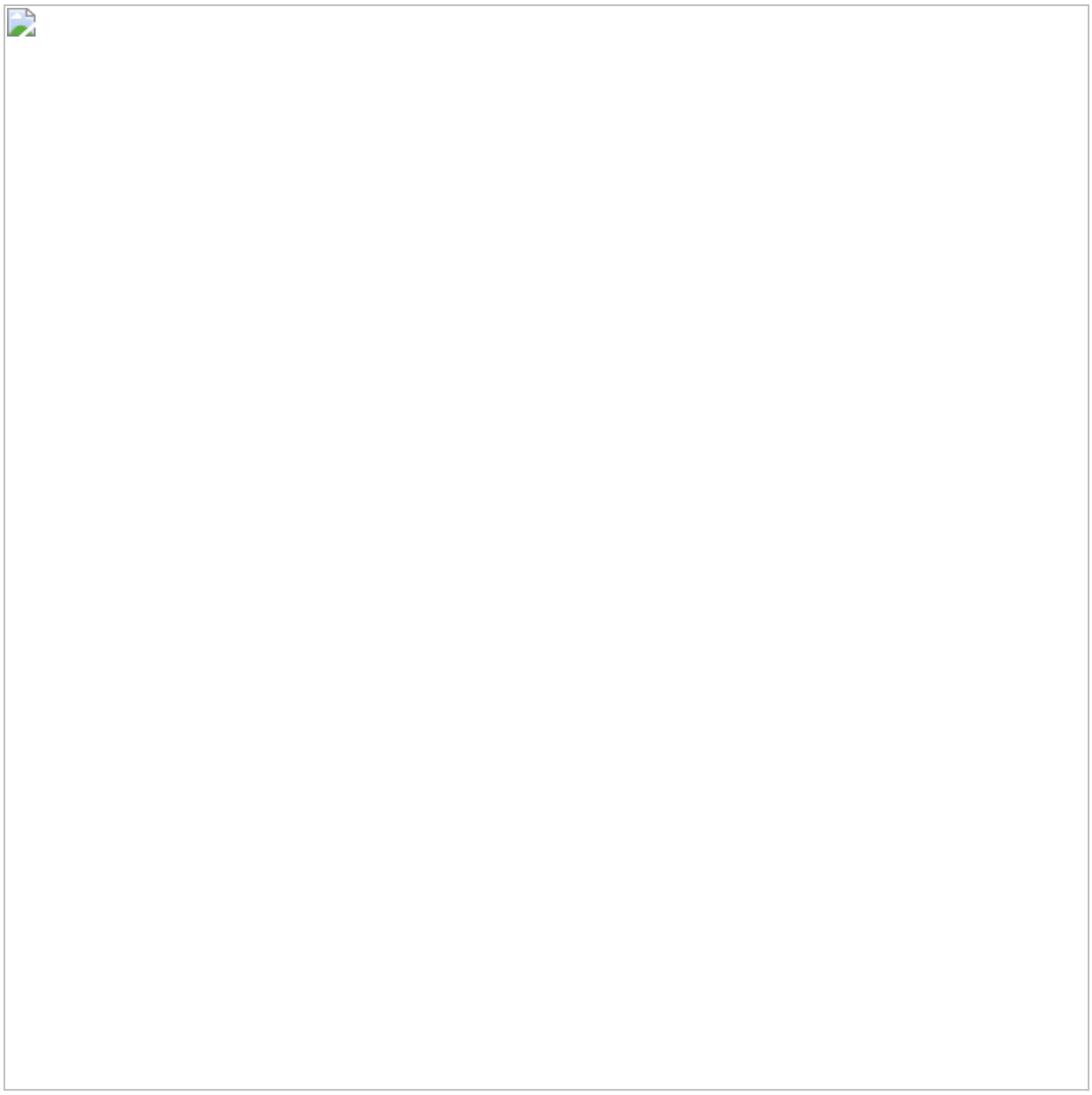


If you don’t see any PRT data, check whether the device is Azure AD joined by running the command **dsregcmd /status** as shown earlier. If **AzureAdPrt** is set to **YES**, check what version of Windows 10 the machine is running; in our lab, we needed to upgrade to at least version 1909 for the attack to work.



Step 2. Extract the Proof of possession key.

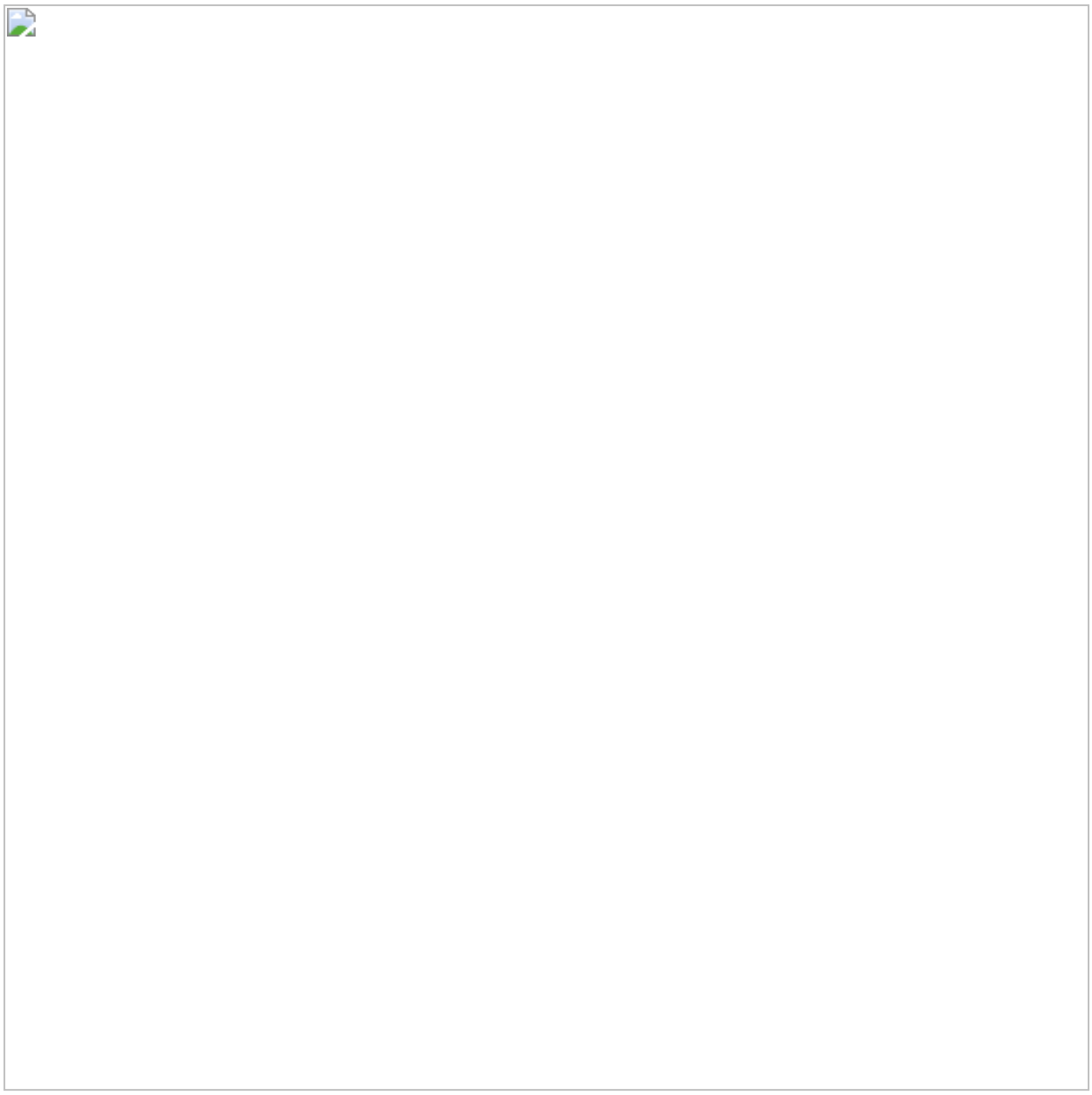
Now we will extract the session key or “ProofOfPosessionKey”, which is highlighted below. This is encrypted and we will need to use our DPAPI masterkeys to decrypt it.



Step 3. Decrypt the session key.

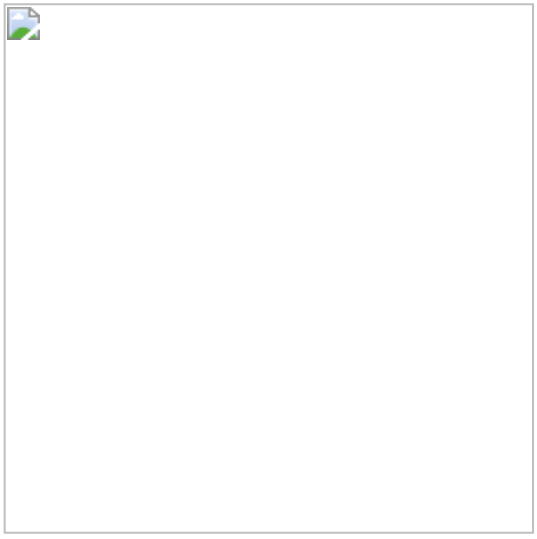
Now we will elevate our privileges to SYSTEM and to run under the computer context to be able to use the DPAPI masterkey to decrypt the session key:

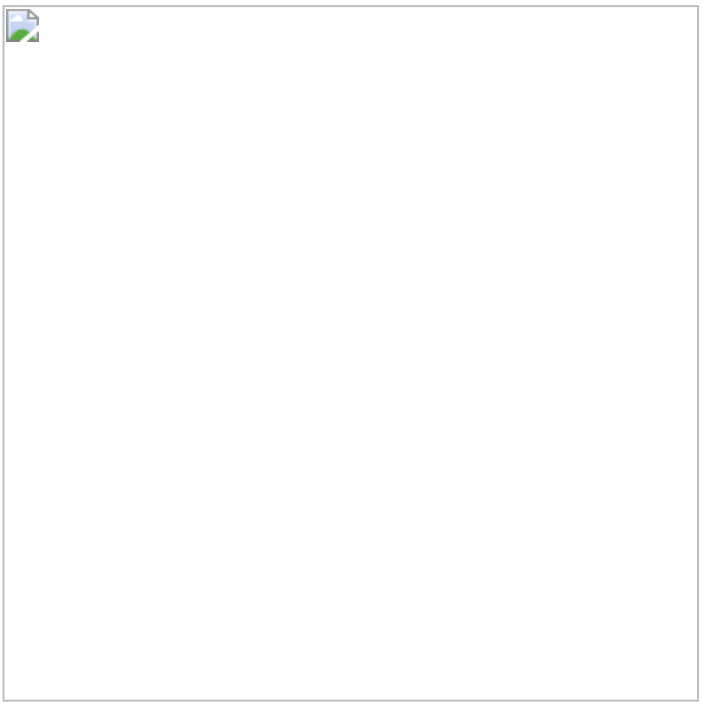
```
Token::elevate
Dpapi::cloudapkd /keyvalue:[PASTE ProofOfPosessionKey HERE] /unprotect
```



Now we will copy two values. The first is the Context value:

And the second is the Derived Key value:



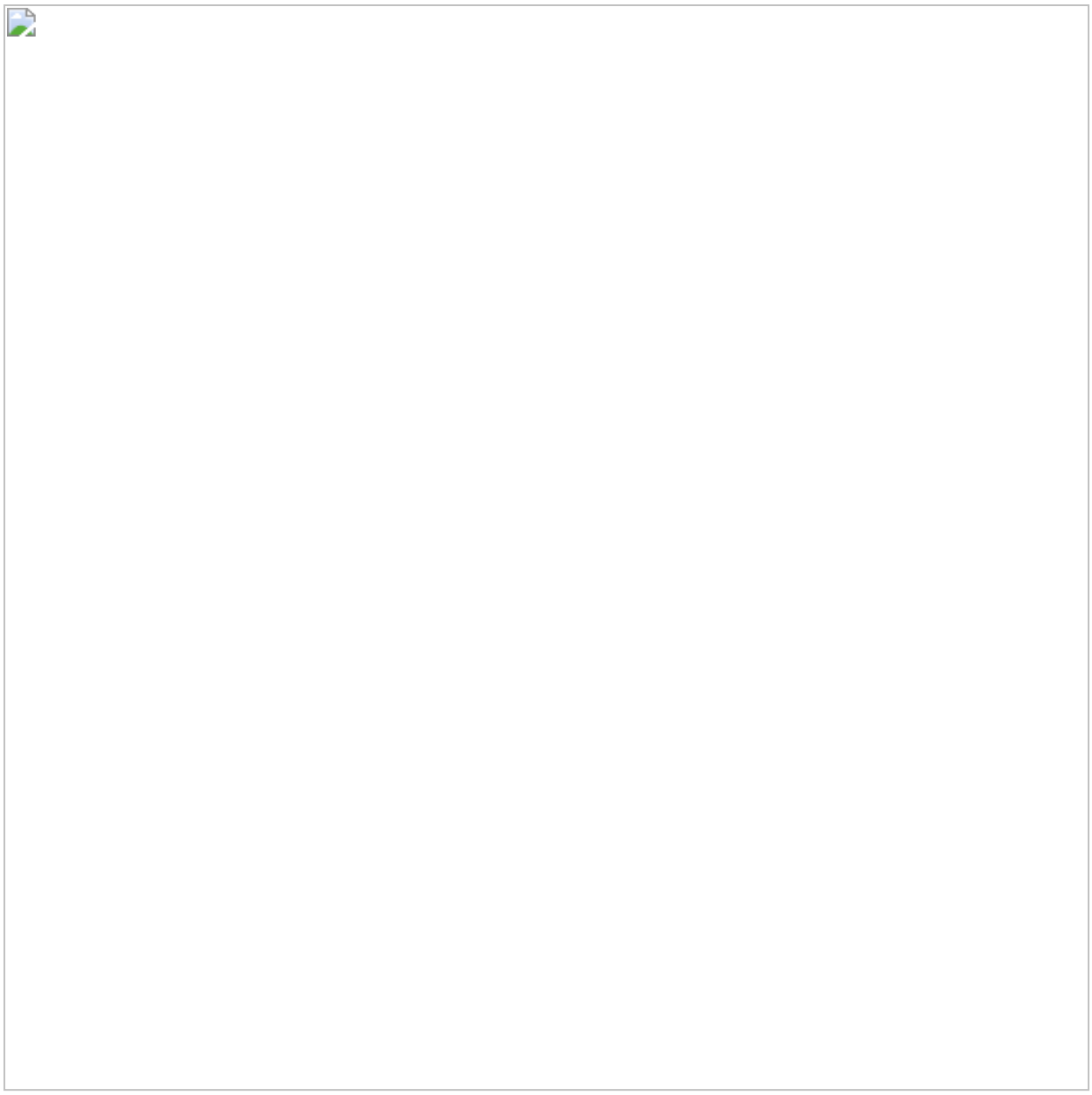


Step 4. Generate PRT cookies.

We can perform the rest of this attack from any workstation. To generate PRT cookies, we simply run the following command:

```
Dpapi::cloudapkd /context:[CONTEXT] /derivedkey:[DerivedKey] /Prt:[PRT]
```

The output will include a signed PRT cookie after **Signature with key**. Copy that text.



Step 5. Inject the PRT cookie into a browser session.

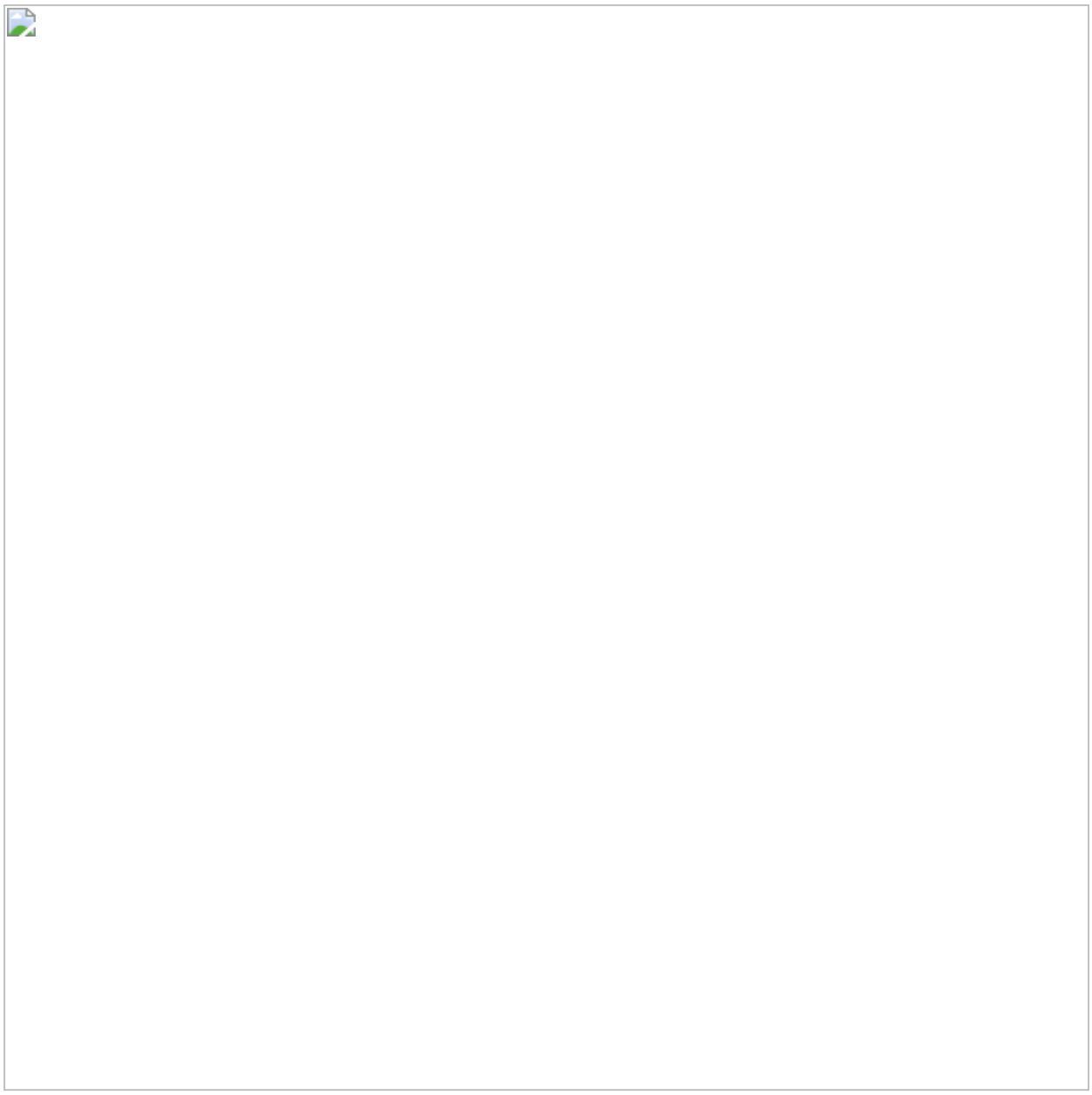
Launch Google Chrome in incognito mode and navigate to https://login.microsoftonline.com. When you are prompted for your login data, right-click anywhere on the page, and then choose **Inspect** to open the dev tools for Chrome.

Go to the Application tab, double-click **Cookies**, and click **login.microsoftonline.com**. In the pane on the right, in the top action bar, click the circle with a diagonal slash to clear all existing cookies.

Then double-click an empty row in the table and add the following new cookie:

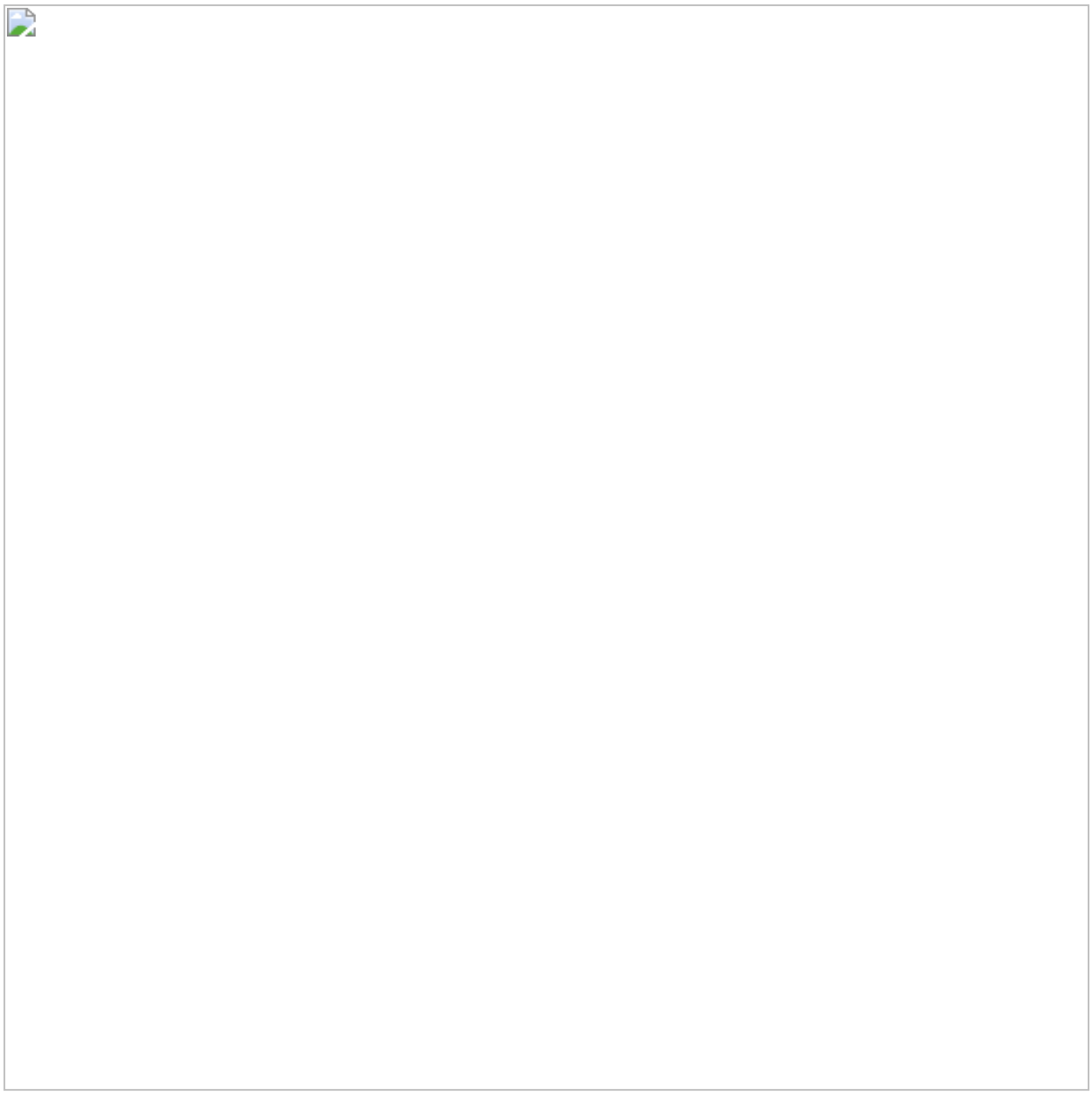
```
Name: x-ms-RefreshTokenCredential
Value: [Paste your output from above]
HttpOnly: Set to True (checked)
```

Leave other fields to their default values.



Refresh the page and make sure the cookie hasn’t disappeared. If it did, you may have made a mistake and have to go through the process again.

Navigate to https://login.microsoftonline.com again and it should automatically log you in as the compromised user:



Protecting against Pass-the-PRT Attacks

Pass-the-PRT attacks are difficult to detect because they abuse legitimate SSO processes. One useful strategy is to use endpoint protection software that can detect the use of Mimikatz, which is run in the first stage of the attack.

However, prevention is even better than detection. Remember that Pass-the-PRT is a lateral movement technique; to perform it, the intruder needs to have already gained access to a machine. With a tool like the Netwrix Active Directory Security Solution, you can prevent malefactors from gaining that foothold in your environment in the first place.

In addition, this attack requires local administrative rights. Using endpoint management software like Netwrix PolicyPak, you remove these powerful rights from users without hurting their productivity. In addition, you can prevent computers from launching malicious software and even secure their browser settings.

Jeff Warren