What Is the Kerberos PAC?

blog.netwrix.com/2023/01/10/what-is-the-kerberos-pac

The Privileged Attribute Certificate (PAC) is an extension to Kerberos service tickets that contains information about the authenticating user and their privileges. A domain controller adds the PAC information to Kerberos tickets when a user authenticates in an Active Directory (AD) domain. When Kerberos ticket services are used to authenticate to other systems, they can retrieve the PAC from a user's ticket to determine their level of privileges without having to query the domain controller.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

This guide details several attacks that involve the Kerberos PAC, the limitations of PAC validation for defending against them, and how Netwrix solutions can help. It also answers frequently asked questions about the Kerberos PAC.

Attacks that Exploit the Kerberos PAC

Because PACs contain very valuable information, they are the target of multiple Windows AD attack techniques. Here are some of the top ones.

Privilege Escalation Attacks (CVE-2014-6324)

The PAC became a target for AD privilege elevation attacks when a vulnerability in the PAC validation algorithm in Windows Server version 2012 R2 and earlier was publicly disclosed in 2014. This vulnerability allows attackers to forge a PAC for any user account they've compromised and effectively make that user a Domain Admin.

The Windows cybersecurity team quickly addressed CVE-2014-6324 by releasing the MS14-068 update.

For complete information about the vulnerability and patch, read Microsoft's post. This attack was also covered in detail at Black Hat 2015 and on Adsecurity.org.

To test this vulnerability, you can use the Python Kerberos Exploitation Kit (PyKEK) or Kekeo.

Golden and Silver Tickets

Golden Tickets and Silver Tickets also allow attackers to leverage forged PACs in an Active Directory attack.

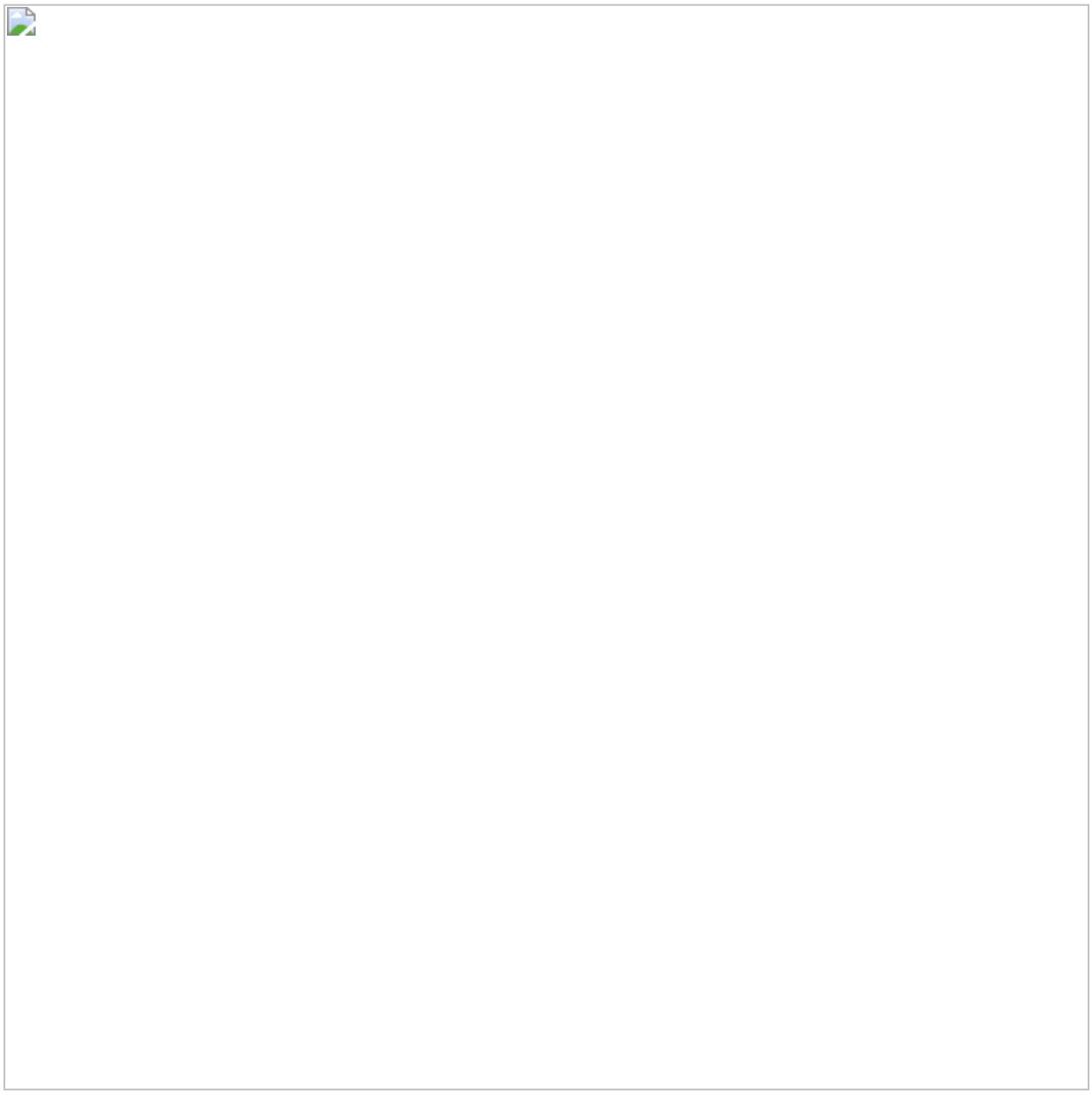
A Golden Ticket is a forged Kerberos ticket-granting ticket (TGT) created through a stolen KDC key. It allows attackers to create a valid Kerberos TGT for any user in the domain and manipulate that user's PAC to gain additional privileges. Golden Tickets are useful for

avoiding detection because adversaries can use seemingly innocuous accounts to perform privileged activities.

Similarly, Silver Tickets let attackers forge Active Directory PACs for ticket-granting service (TGS) tickets. However, unlike Golden Tickets, Silver Tickets give attackers rights to only a specific service on a specific host. TGS tickets are encrypted with the service's password hash, so if a threat actor steals the hash for a service, they can create TGS tickets for that service.

Sometimes service accounts have limited rights. A good example is an SQL service account that doesn't have system-level rights to the databases hosted on that SQL server. However, these accounts aren't safe since attackers can use Silver Tickets to forge PACs and give extra privileges to a service account with limited rights and then completely compromise their target.

As you can see below, Golden and Silver Tickets give users membership in privileged groups using RIDs such as 512 (Domain Admins) and 519 (Enterprise Admins).



PAC Validation

How can you implement security around forged PACs? PAC validation can help, though it is not a panacea.

PAC validation is controlled by the registry key ValidateKdcPacSignature, which is found at HKLMSYSTEMCurrentControlSetControlLsaKerberosParameters Setting this key to 0 will turn off PAC validation.

When PAC validation is enabled on a Windows system, the PAC of a user authenticating to that system will be checked against Active Directory to ensure its validity — but only when certain criteria are met.

Specifically, as Microsoft explains:

Windows OS sends the PAC validation messages to the NetLogon service of the DC when the service does not have the TCB privilege and it is not a Service Control Manager (SCM) service. The Local Security Authority Subsystem Service (LSASS) process will send PAC validation messages to the DC when the LSA client (the application server) is not running in the context of local system, network service, or local service; or it does not have SeTCBprivilege (Act as part of the operating system).

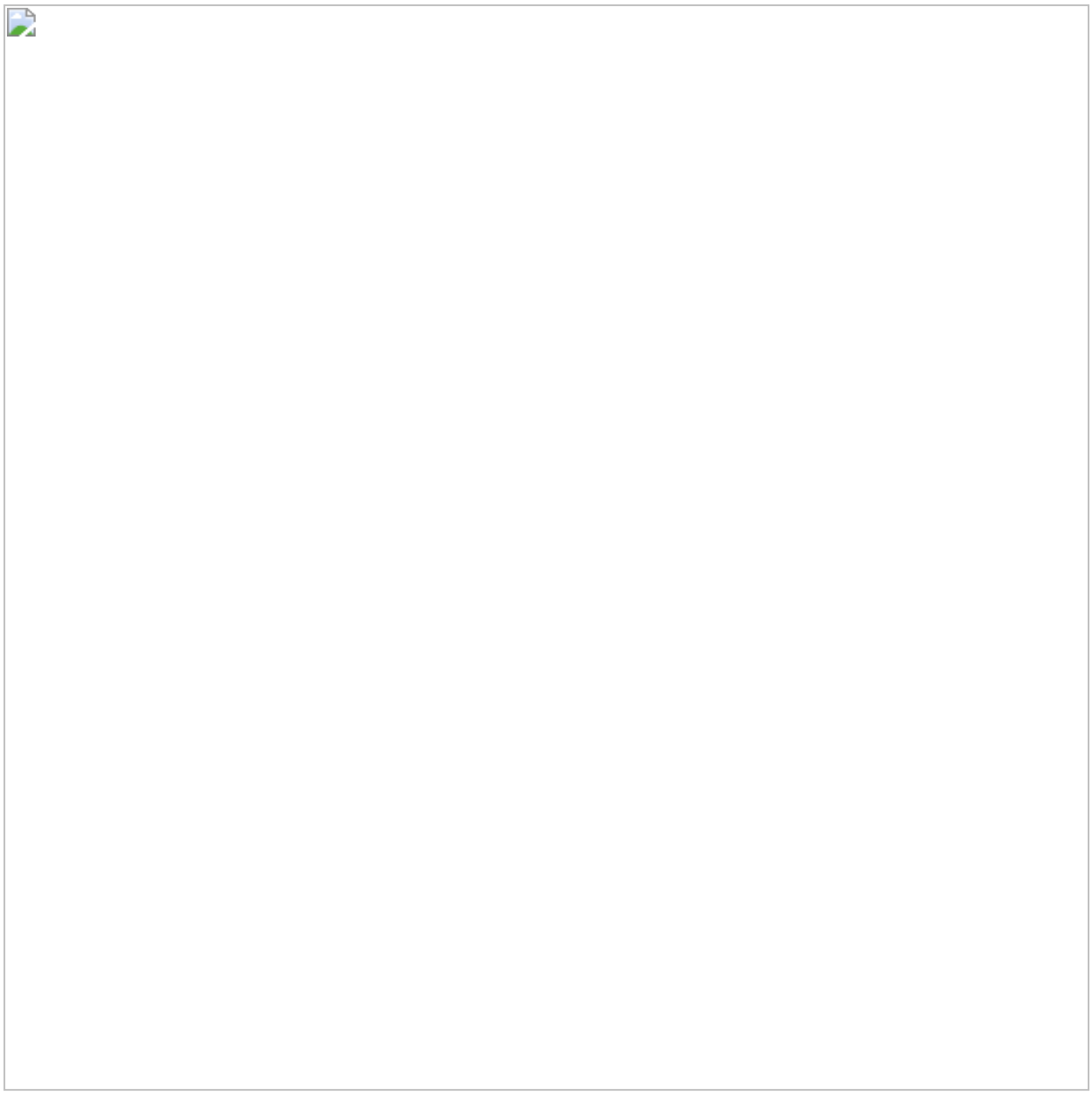
In other words, PAC validation does not prevent attackers from running Silver and Golden Tickets.In my testing, whether or not PAC validation, I was able to leverage Silver and Golden Tickets against a target system.

Exploring a User PAC

If you are interested in looking at a PAC for a user, Impacket, which comes with a script getPAC.py, is a great way to get started.

To test this in Windows, you should check out CommandoVM. This tool packages the getPAC.py script (and many others) as executable files so you don't have to worry about Python dependencies.

With the getPAC.py script, you can target any user without any special privileges and return their PAC settings and information:



As you can see, the script returns much more than group membership. To learn more about these results, info group keys and Kerberos group membership, check out Microsoft's documentation about the Privilege Attribute Certificatedatastructure.

How Netwrix Can Help

PAC client validation and scripts like getPAC.py can protect your users and data from unauthorized access. Unfortunately, they don't provide enough protection, especially if threat actors use Golden and Silver Tickets to forge PAC attacks.

That's where Netwrix's end-to-end Active Directory security solution comes in. Comprehensive, easy to use and secure, this threat detection tool can help you:

- Spot and remediate security risks through security assessments.
- Enable strong password policies and protect credentials from advanced threats.
- Replace standing privileged accounts with just-in-time, just-enough access.
- Detect sophisticated threats in time to prevent breaches.

- Verify, establish and strengthen security protocols.
- Generate required security reports for compliance audits.
- Automate responses to expected threats.
- Roll back unwanted Active Directory deletions and changes.
- Streamline full domain recovery to ensure continuity.

FAQ

What is the PAC in Kerberos?

The Privileged Attribute Certificate (PAC) is part of a Kerberos ticket. It contains information about the user's privileges and is used whenever they authenticate in an Active Directory domain.

What is PAC validation?

If enabled on a Windows system, PAC validation will check the validity of an authenticating user's PAC by comparing it against Active Directory. Unfortunately, enabling PAC validation will **not** prevent Golden Ticket and Silver Ticket attacks.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.