Cracking Active Directory Passwords with AS-REP Roasting

blog.netwrix.com/2022/11/03/cracking_ad_password_with_as_rep_roasting

One critical way that attackers gain access to an IT environment and escalate their privileges is by stealing user password hashes and cracking them offline. We covered a method for harvesting service account passwords in our post on Kerberoasting. Here we will explore a technique that works against certain user accounts, AS-REP Roasting. We'll cover how adversaries perform AS-REP Roasting using the Rubeus tool and how you can defend your organization against these attacks.

Handpicked related content:

[Free Guide] Password Policy Best Practices for Strong Security in AD

What is AS-REP Roasting?

AS-REP Roasting is a technique that enables adversaries to steal the password hashes of user accounts that have Kerberos preauthentication disabled, which they can then attempt to crack offline.

When preauthentication is enabled, a user who needs access to a resource begins the Kerberos authentication process by sending an Authentication Server Request (AS-REQ) message to the domain controller (DC). The timestamp on that message is encrypted with the hash of the user's password. If the DC can decrypt that timestamp using its own record of the user's password hash, it will send back an Authentication Server Response (AS-REP) message that contains a Ticket Granting Ticket (TGT) issued by the Key Distribution Center (KDC), which is used for future access requests by the user.

Learn more about the attack:

[Netwrix Attack Catalog] AS-REP Roasting Attack using Rubeus

However, if preauthentication is disabled, an attacker could request authentication data for any user and the DC would return an AS-REP message. Since part of that message is encrypted using the user's password, the attacker can then attempt to brute-force the user's password offline.

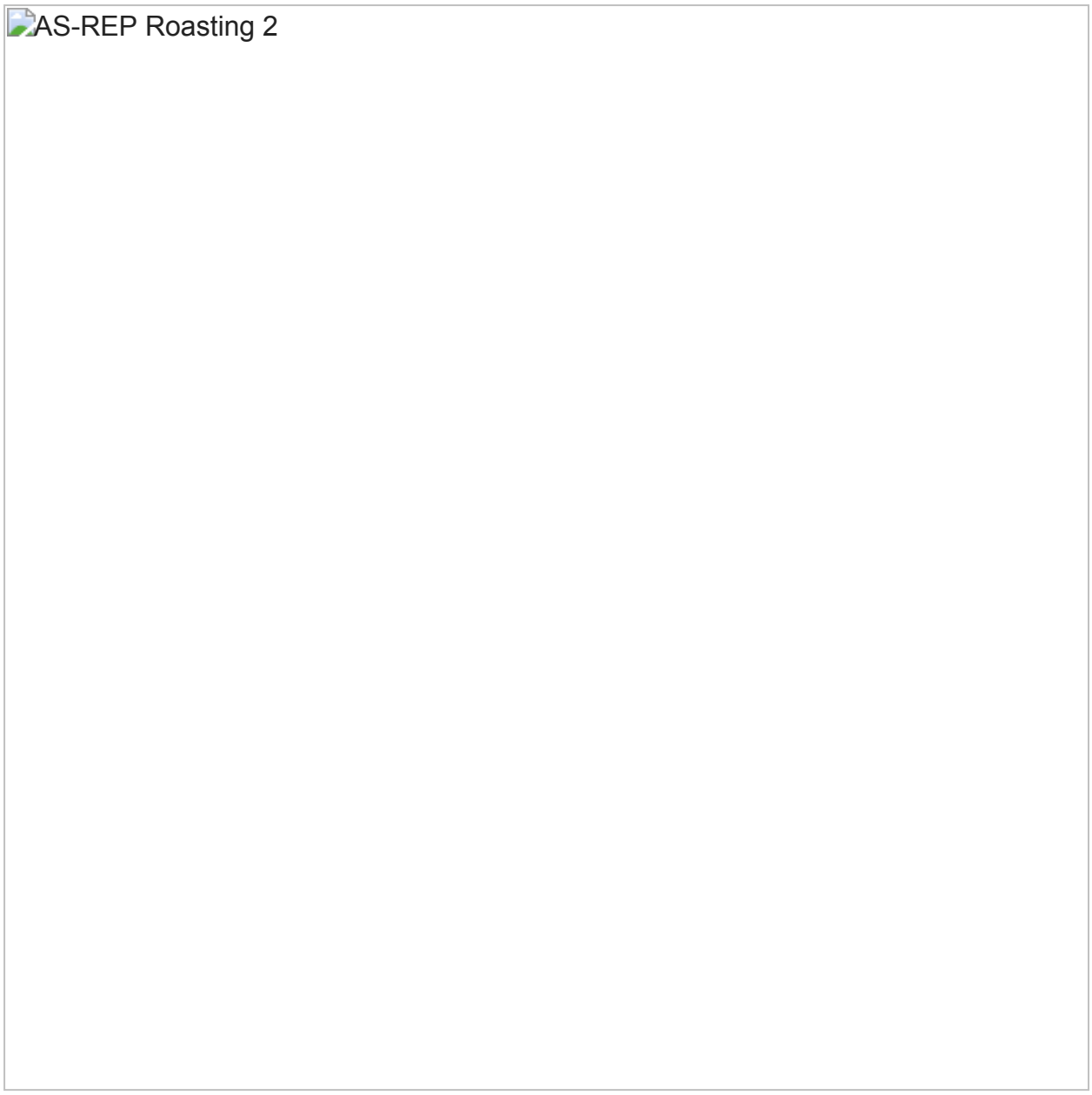
Luckily, preauthentication is enabled by default in Active Directory. However, it can be disabled for a user account using the setting shown below:

Performing AS-REP Roasting with Rubeus

Using Rubeus, you can easily perform AS-REP Roasting to see how this attack would work in your environment. Simply issue the following command:

```
Rubeus.exe asreproast
```

This will automatically find all accounts that do not require preauthentication and extract their AS-REP hashes for offline cracking, as shown here:

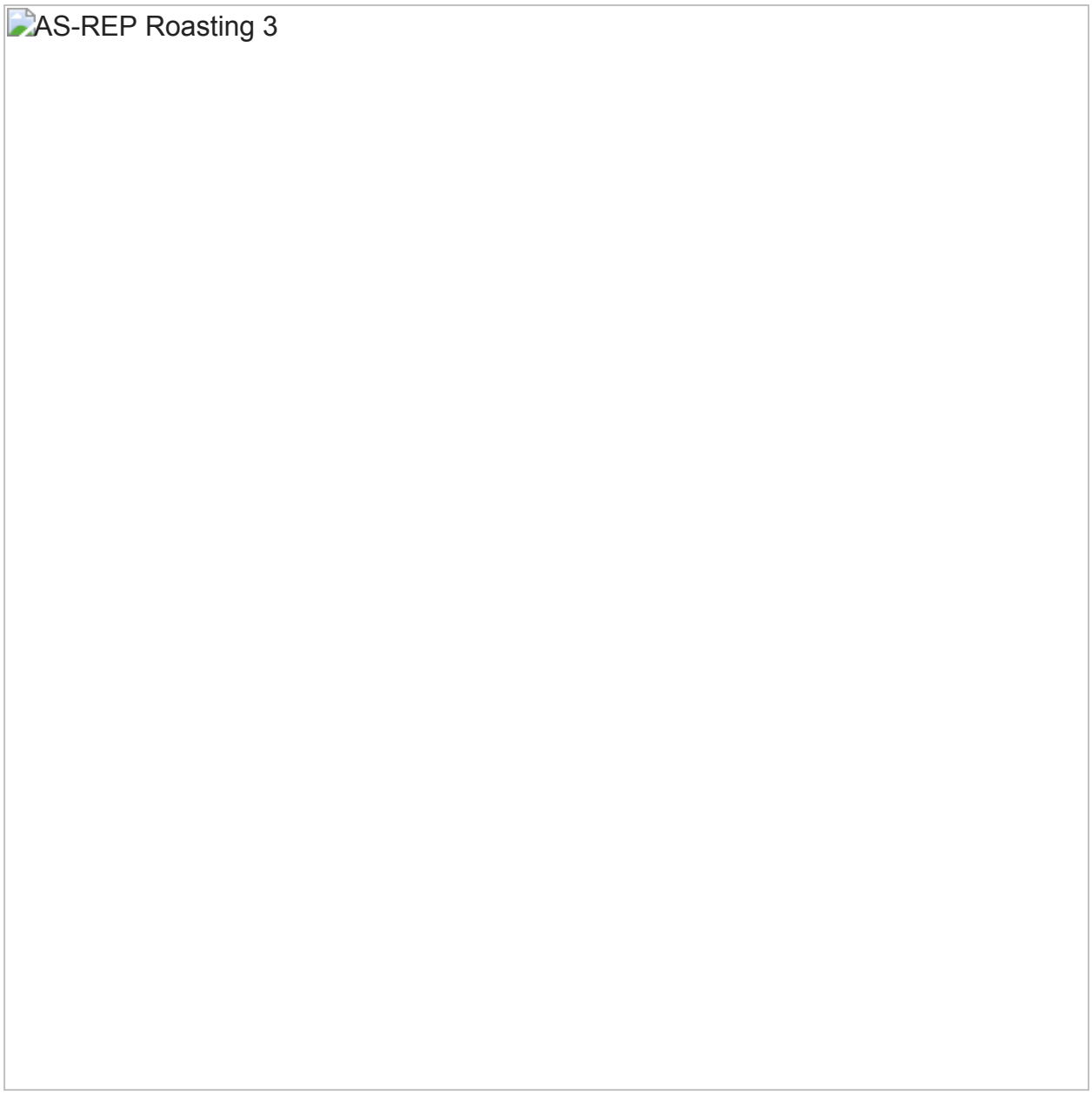


Let’s take this example one step further and extract the data in a format that can be cracked offline by Hashcat. This command will output the AS-REP hash information to a text file:

```
Rubeus.exe asreproast /format:hashcat /outfile:C:\Temp\hashes.txt
```

Then it’s straightforward to use Hashcat to crack the hashes that were found. We simply need to specify the right hash-mode code for AS-REP hashes, our hash file, and a dictionary to use to perform the brute-force password guessing:

```
hashcat64.exe -m 18200 c:\Temp\hashes.txt example.dict
```



Protecting Against AS-REP Roasting

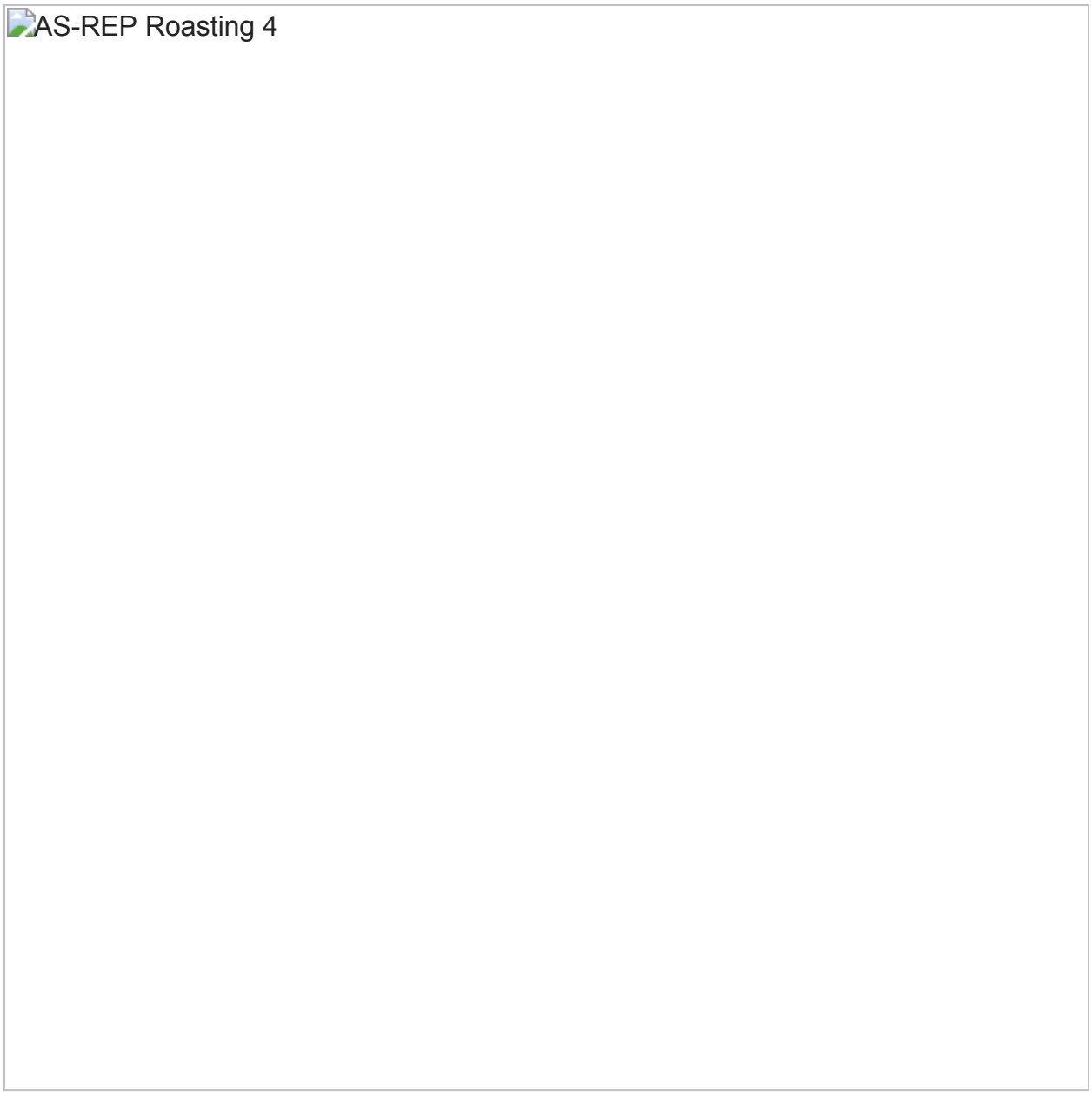
As you can see, AS-REP Roasting provides a simple way to steal the password hashes of user accounts that do not require preauthentication, with no special privileges required. Fortunately, there are several effective methods for defending against these attacks.

Identify Accounts that Do Not Require Preauthentication

The best way to block AS-REP Roasting attacks is to find all user accounts that are set to not require Kerberos preauthentication and then enable this setting. This script will find these vulnerable accounts:

```
Get-ADUser -Filter 'useraccountcontrol -band 4194304' -Properties
useraccountcontrol | Format-Table name
```

The output looks like this:



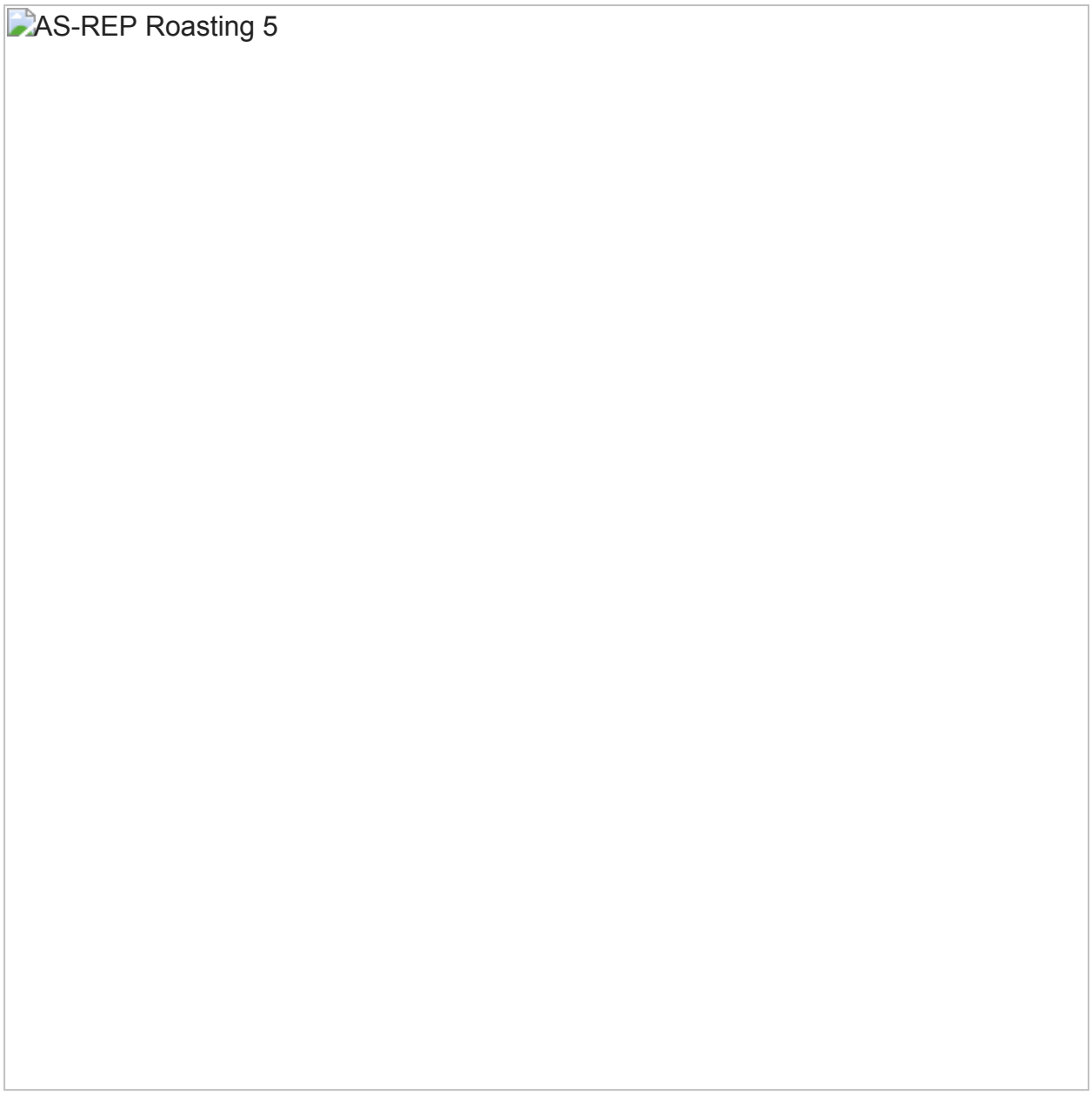
Password Strength

Another strong protection against AS-REP Roasting attacks is to require long, complex passwords that are difficult to crack even if an adversary manages to steal them. Using fine-grained password policies — especially for privileged accounts — is a great first step.

AD Privileges

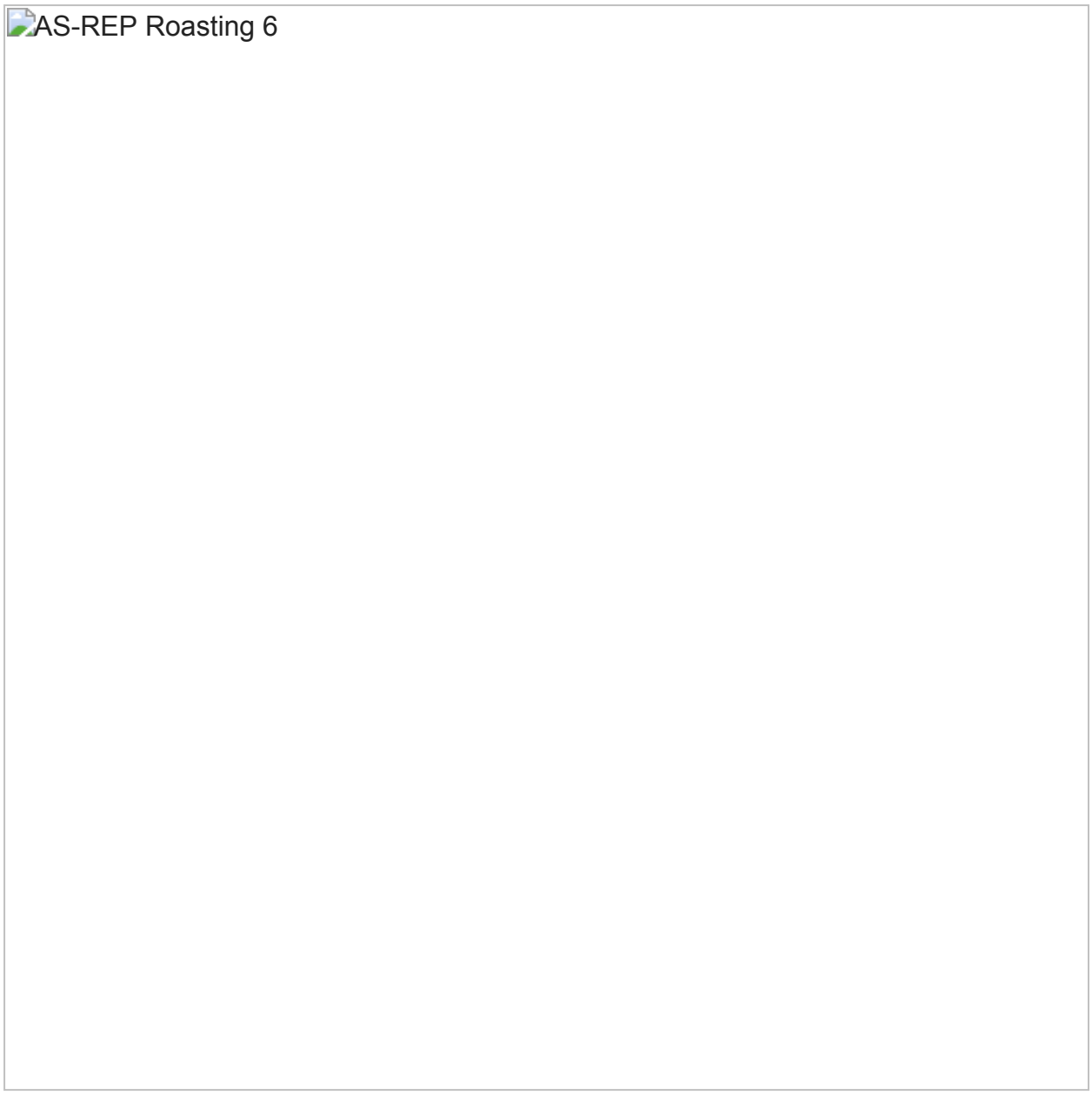
It's also crucial to know which user accounts have the permissions required to modify the setting that controls whether preauthentication is enabled, since they could disable it for just enough time to obtain the AS-REP hash and then enable it again. This query will list all access rights over user accounts that do not require preauthentication:

```
(Get-ACL "AD:\$((Get-ADUser -Filter 'useraccountcontrol -band
4194304').distinguishedname)").access
```

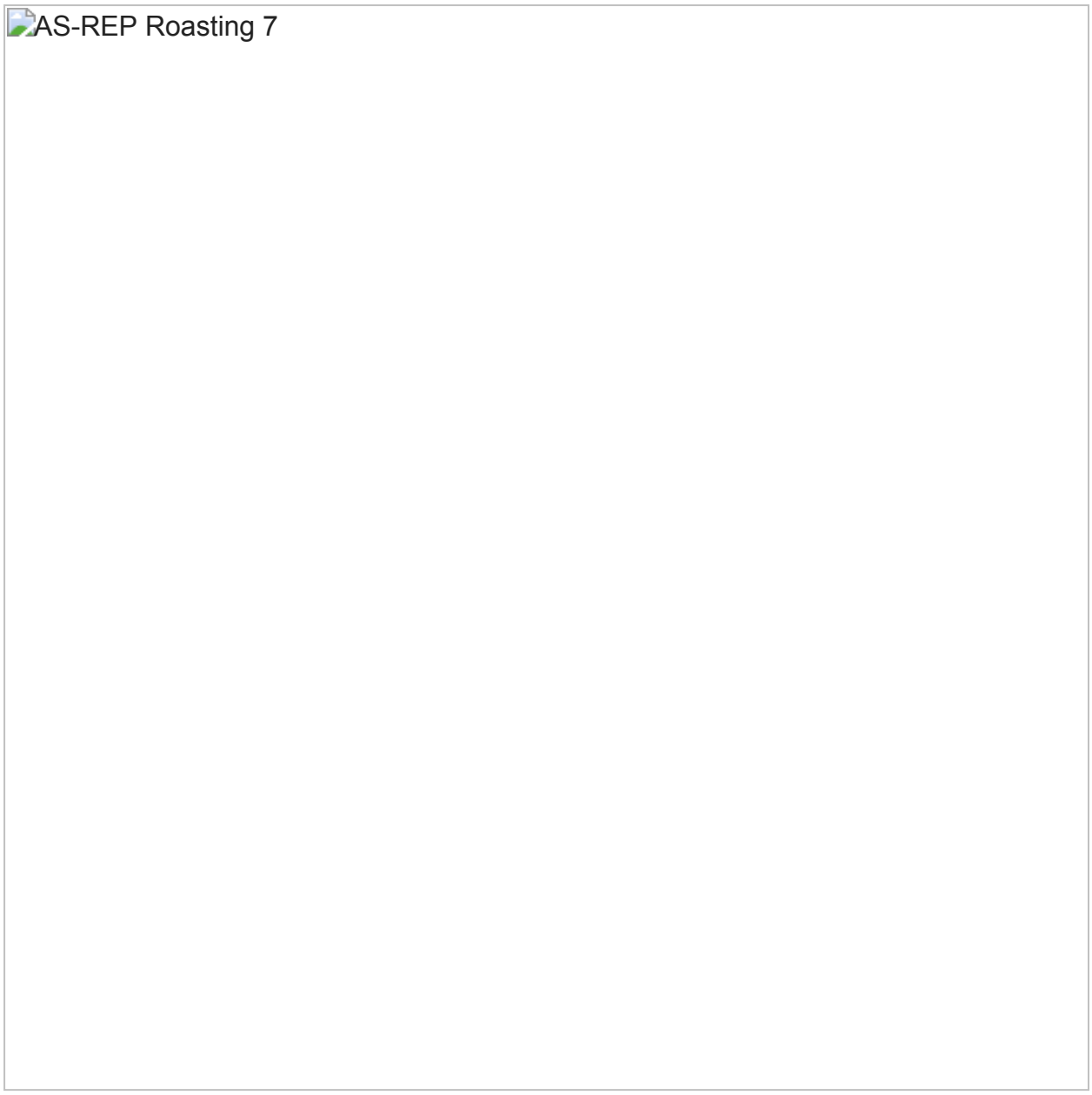


Change Monitoring

Finally, you should also monitor for disabling of Kerberos preauthentication. Event 4738 logs changes to this user setting:



Alternatively, you can monitor event ID 5136:



How can Netwrix help?

Secure your Active Directory from end to end with the Netwrix Active Directory Security Solution. It will enable you to:

- Uncover security risks in Active Directory and prioritize your mitigation efforts.
- Harden security configurations across your IT infrastructure.
- Promptly detect and contain even advanced threats, such as Kerberoasting, DCSync , NTDS.dit extraction and Golden Ticket attacks.
- Respond to known threats instantly with automated response options.
- Minimize business disruptions with fast Active Directory recovery.

FAQ

What does AS-REP stand for?

AS-REP stands for Authentication Service (AS) Response Message. It is a type of message transmitted between a server and a client during Kerberos authentication.

Which users are vulnerable to AS-REP roasting?

AS-REP Roasting can be used only against user accounts that have Kerberos preauthentication disabled

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.