AS-REP Roasting

redfoxsec.com/blog/as-rep-roasting

Karan Patel July 15, 2023

- July 15, 2023
- Active Directory
- Karan Patel

Kerberos is a network authentication protocol used to provide secure authentication over a non-secure network. While it is an essential component of network security, it can also be exploited by hackers to gain unauthorized access to sensitive information. In this article, we will take a deep dive into one such exploitation technique, AS-REP Roasting.

We will explore the basics of Kerberos, the difference between AS-REP Roasting, Kerberoasting, and Golden Ticket attacks, and the tools required to perform an AS-REP Roasting attack.

Understanding Kerberos

Before we delve into the specifics of AS-REP Roasting, it is important to understand the basics of Kerberos. Kerberos is a protocol that enables secure authentication between a client and a server over a non-secure network. The protocol relies on a trusted third-party

service called the Key Distribution Center (KDC) to authenticate users and services on the network.

When a user logs in to a Kerberos-enabled network, the user's computer sends a request to the KDC for a ticket-granting ticket (TGT). The KDC verifies the user's credentials and sends a TGT back to the user's computer. The TGT contains a session key that can be used to authenticate the user to other services on the network.

AS-REP Roasting: An Overview

AS-REP Roasting is an exploitation technique that targets the Kerberos protocol. It allows an attacker to retrieve password hashes for users that do not require pre-authentication. Pre-authentication is an initial stage in Kerberos authentication that prevents brute-force attacks. If a user has "Do not use Kerberos pre-authentication" enabled, an attacker can recover a Kerberos AS-REP encrypted with the user's RC4-HMAC'd password and attempt to crack this ticket offline.

Key Differences Between AS-REP Roasting, Kerberoasting, and Golden Ticket Attacks

To better understand AS-REP Roasting, it is important to differentiate it from other Kerberos attacks, including Kerberoasting and Golden Ticket attacks.

AS-REP Roasting

AS-REP Roasting is an attack that retrieves user hashes that can be brute-forced offline. If the user has "Do not use Kerberos pre-authentication" enabled, an attacker can recover a Kerberos AS-REP encrypted with the user's RC4-HMAC'd password and attempt to crack this ticket offline.

Kerberoasting

Kerberoasting is an attack that retrieves application service hashes that can be brute-forced offline. This attack targets Kerberos service tickets rather than TGTs.

Golden Ticket

If an attacker possesses the password hash for the KRBTGT account, they can create a golden ticket. This type of ticket allows the attacker to produce authentication material for any account located in the Active Directory. Once they have a golden ticket, they can use it to request ticket granting services (TGS) tickets that will grant them access to specific resources. To obtain TGS, attackers must communicate with the Key Distribution Center (KDC), which operates on domain controllers within the Active Directory domain.

Tools Required for AS-REP Roasting

To perform an AS-REP Roasting attack, you will need the following tools:

- exe
- ASREPRoast PowerShell Script
- Impacket

Rubeus.exe

Rubeus.exe is a tool that can be used to perform various Kerberos-related attacks, including AS-REP Roasting. To use Rubeus.exe, simply run the command Rubeus.exe asreproast to dump the user account hashes used to encrypt the timestamp. These hashes can then be saved in a text document for offline password cracking.

ASREPRoast PowerShell Script

The ASREPRoast PowerShell script is another tool that can be used to perform an AS-REP Roasting attack. To use the script, download it from the official repository on Github and import the module in PowerShell. Then, run the command Invoke-ASREPRoast to extract the user hash with the AS_REP message.

Impacket

Impacket is a collection of Python classes that can be used to craft and decode network packets. The GetNPUsers.py script, which is part of the Impacket collection, can be used to attempt to list and get TGTs for those users that have the property 'Do not require Kerberos pre-authentication' set (UF*DONT*REQUIRE_PREAUTH).

Performing an AS-REP Roasting Attack

Now that we have a basic understanding of AS-REP Roasting and the tools required to perform an attack, let's dive into the specifics of performing an AS-REP Roasting attack.

Enabling "Do not require pre-authentication" for a user

By default, "Do not require pre-authentication" is disabled for domain users. To test an AS-REP Roasting attack, we will need to enable this setting for a user. Once all prerequisites required to perform this attack are in place, we can enable "Do not require pre-authentication" for a user.

Using Rubeus.exe for AS-REP Roasting

To use Rubeus.exe for AS-REP Roasting, simply run the command Rubeus.exe asreproast. This will dump the user account hashes used to encrypt the timestamp. These hashes can then be saved in a text document for offline password cracking.

```
.\Rubeus.exe asreproast /format:<hashcat/john> /outfile:<output>
```

Using the ASREPRoast PowerShell Script for AS-REP Roasting

To use the ASREPRoast PowerShell script for AS-REP Roasting, download it from the official repository on Github and import the module in PowerShell. Then, run the command Invoke-ASREPRoast to extract the user hash with the AS_REP message.

```
Import-Module .\ASREPRoast.ps1
Invoke-ASREPRoast
Invoke-ASREPRoast | select -ExpandProperty Hash
```

Using Impacket for AS-REP Roasting

To use Impacket for AS-REP Roasting, run the GetNPUsers.py script with the appropriate parameters. This will extract the user hash with the AS_REP message, which can then be used for offline password cracking.

```
python GetNPUsers.py <domain_name>/<domain_user>:<domain_user_password> -request -format <hashcat/john> -outputfile <output>
```

Cracking with a Dictionary of Passwords

```
hashcat -m 18200 -a 0 <output> <passwords_file>
john --wordlist=<passwords_file> <output>
```

TL;DR

AS-REP Roasting is a potent technique that can be used to exploit the Kerberos protocol. By enabling “Do not require pre-authentication” for a user, an attacker can retrieve password hashes that can be cracked offline. The tools required to perform an AS-REP Roasting attack are readily available, making it an accessible technique for both hackers and security professionals. It is essential to understand the basics of Kerberos and the difference between AS-REP Roasting, Kerberoasting, and Golden Ticket attacks to protect against these types of attacks.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you are looking to improve your organization’s security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems, and provide recommendations to remediate them.**

Join us on our journey of growth and development by signing up for our comprehensive **courses.**

PreviousExploiting Active Directory Certificate Services (AD CS)
NextResource-Based Constrained Delegation (RBCD) Attack

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025
When Hackers Hit the Road: The Jaguar Land Rover Cyberattack
September 05, 2025
This Is the Hacker’s Swiss Army Knife. Have You Heard About It?