# TTP Detail – T1558.004

## TTP Information

Name: AS-REP Roasting

Description: Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by [Password Cracking](https://attack.mitre.org/techniques/T1110/002) Kerberos messages.(Citation: Harmj0y Roasting AS-REPs Jan 2017)   
  
Preauthentication offers protection against offline [Password Cracking](https://attack.mitre.org/techniques/T1110/002). When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user’s password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user’s password.(Citation: Microsoft Kerberos Preauth 2014)  
  
For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline [Password Cracking](https://attack.mitre.org/techniques/T1110/002) attacks similarly to [Kerberoasting](https://attack.mitre.org/techniques/T1558/003) and expose plaintext credentials. (Citation: Harmj0y Roasting AS-REPs Jan 2017)(Citation: Stealthbits Cracking AS-REP Roasting Jun 2019)   
  
An account registered to a domain, with or without special privileges, can be abused to list all domain accounts that have preauthentication disabled by utilizing Windows tools like [PowerShell](https://attack.mitre.org/techniques/T1059/001) with an LDAP filter. Alternatively, the adversary may send an AS-REQ message for each user. If the DC responds without errors, the account does not require preauthentication and the AS-REP message will already contain the encrypted data. (Citation: Harmj0y Roasting AS-REPs Jan 2017)(Citation: Stealthbits Cracking AS-REP Roasting Jun 2019)  
  
Cracked hashes may enable [Persistence](https://attack.mitre.org/tactics/TA0003), [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), and [Lateral Movement](https://attack.mitre.org/tactics/TA0008) via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: SANS Attacking Kerberos Nov 2014)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* Rubeus