Kerberoasting Attack & Detection Report

Date: [06-05-2025]

1. Overview of Kerberoasting

Kerberoasting is a post-exploitation attack technique used against Microsoft Active Directory environments. The main objective is to extract service account credentials without sending them over the network or triggering alerts from traditional intrusion detection systems.

In Active Directory, when a user wants to access a network service, the Kerberos authentication protocol issues a Ticket Granting Service (TGS) ticket. If a service account is configured with a Service Principal Name (SPN), it will have an associated TGS encrypted with the account's NTLM hash. An attacker with access to a domain-joined machine can request these tickets and extract the hashes for offline cracking.

This technique is especially dangerous because:

- It does not require elevated privileges beyond a regular domain user.
- It avoids detection since it uses legitimate Kerberos ticket requests.
- It targets weak passwords used by service accounts.

---

2. Home Lab Setup

Domain Controller

- **OS:** Windows Server 2019
- **Domain:** `lab.local`
- **Users:**

    - `natasha` (domain user)
    - `svc_sql` (service account)
- **SPN Configured:**
    - `MSSQLSvc/sql.lab.local:1433`

Client Machine

- **OS:** Windows 10 (joined to lab.local)
- Used to simulate domain user behavior

Attacker Machine

- **OS:** Parrot OS / Kali Linux
- **Tools:** Rubeus, Hashcat

SIEM Solution

- **Wazuh Manager on Ubuntu**
- Wazuh agent installed on the Domain Controller
- Kibana used for log visualization

---

3. Attack Execution Steps

Step 1: Gain Access as a Domain User

Logged into the Windows 10 machine as `natasha`.

Step 2: Request TGS for Service Accounts

- Transferred `Rubeus.exe` to the Windows machine
- Ran:

```
Rubeus.exe kerberoast
```

- Tool enumerates accounts with SPNs and requests TGS tickets

Step 3: Extract Service Ticket Hash

- Rubeus outputs TGS ticket hash in Hashcat format
- Saved output to `hashes.txt`

Step 4: Crack Hash with Hashcat

- Transferred `hashes.txt` to attacker machine
- Ran:

```
hashcat -m 13100 hashes.txt /usr/share/wordlists/rockyou.txt --force
```

- Revealed the weak password if successful

---

4. Detection & Analysis Using SIEM (Wazuh)

Monitored Event

- Windows Event ID 4769: A Kerberos service ticket was requested

Detection Strategy

- Wazuh logs event from Domain Controller
- Alert triggers when:

    - TGS is requested using RC4 encryption
    - High frequency of TGS requests

Kibana Analysis

- Filtered by `Event ID 4769` and `svc_sql`
- Verified timestamp and source IP

Recommendations

- Monitor for unusual SPN requests
- Use honeypot service accounts
- Require strong passwords or use Managed Service Accounts (MSAs)
- Enable log correlation and alerting rules

---

5. Outcome

- Retrieved NTLM hash for `svc_sql`
- Cracked weak password offline
- SIEM detected suspicious TGS activity and generated alert
- Detection successful using Wazuh + Kibana

---

6. Lessons Learned

- Kerberoasting is stealthy but detectable
- Even regular domain users can launch it
- Weak service account passwords are a major risk
- SIEM integration in a lab proves critical for real-world readiness

---

7. Next Steps

- Simulate other attacks (Pass-the-Ticket, DCSync, Golden Ticket)
- Integrate Sigma rules with Wazuh
- Expand log correlation for better visibility
- Develop an incident response workflow based on detection

Report Created By:
Simpal Kumari
Cybersecurity Enthusiast | Blue Team | SOC Analyst

Tools Used: Rubeus, Hashcat, Windows Server 2019, Parrot OS, Wazuh, Kibana