

# Detecting Overpass-the-Hash

## Overpass-the-Hash

Adversaries may utilize the **Overpass-the-Hash** technique to obtain Kerberos TGTs by leveraging stolen password hashes to move laterally within an environment or to bypass typical system access controls. Overpass-the-Hash (also known as **Pass-the-Key**) allows authentication to occur via Kerberos rather than NTLM. Both NTLM hashes or AES keys can serve as a basis for requesting a Kerberos TGT.

### Attack Steps:

- The attacker employs tools such as Mimikatz to extract the NTLM hash of a user who is currently logged in to the compromised system. The attacker must have at least local administrator privileges on the system to be able to extract the hash of the user.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 2560090 (00000000:0027105a)
Session           : NewCredentials from 0
User Name         : SYSTEM
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 8/1/2023 7:22:43 AM
SID               : S-1-5-18

msv :
[00000003] Primary
* Username : Administrator
* Domain   : corp.local
* NTLM     : fc525c9683e8fe067095ba2ddc971889

tspkg :
wdigest :
* Username : Administrator
* Domain   : corp.local
* Password : (null)

kerberos :
* Username : Administrator
* Domain   : corp.local
* Password : (null)

ssp : KO
credman :

Authentication Id : 0 ; 911055 (00000000:000de6cf)
Session           : Interactive from 1
User Name         : JERRI_BALLARD
```

- The attacker uses a tool such as Rubeus to craft a raw AS-REQ request for a specified user to request a TGT ticket. This step does not require elevated privileges on the host to request the TGT, which makes it a stealthier approach than the Mimikatz Pass-the-Hash attack.

```
C:\Users\JENNY_HICKMAN\tools>.\\Rubeus.exe asktgt /user:Administrator /domain:lab.internal.local /rc4:fc525c9683e8fe067095ba2ddc971889 ptt

Rubeus

v1.6.1

[*] Action: Ask TGT

[*] Using rc4_hmac hash: fc525c9683e8fe067095ba2ddc971889
[*] Building AS-REQ (w/ preauth) for: 'lab.internal.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFwDCCBbygAwIBBaEDAgEwOoIEVjCCBLphggS2MIIesqADAgEFoRQObEkx8QI5JT1RFUK5BTC5MT0NB
TKInMCwgAwIBAgEeMBwbBmtYnRndBsSbGfILmLudGVybWFsLmxvY2Fso4IEajCCBGagAwIBeqEDAgEC
ooIEWASCBFQAR6gWCrFn+1lYsVdLiLBfa92aFr84p+UlyK3oCbH0e1MPLrnnHlAW3EYUH+e2cT/ZAwLI
JSD9YAZLKNSEdXD4prDnEEIJcCX4rqCHmCuDQ0DQukTUQ19QrtEfXb+TXH1iqbTG8IMkteaqb3gLMHzy
```

- Analogous to the Pass-the-Ticket technique, the attacker submits the requested ticket for the current logon session.

## Overpass-the-Hash Detection Opportunities

**Mimikatz's** Overpass-the-Hash attack leaves the same artifacts as the Pass-the-Hash attack, and can be detected using the same strategies.

[Resources](#)[Go to Questions](#)

### Table of Contents

#### Leveraging Windows Event Logs

- [Detecting Common User/Domain Recon](#) ✓
- [Detecting Password Spraying](#) ✓
- [Detecting Responder-like Attacks](#) ✓
- [Detecting Kerberoasting/AS-REProasting](#) ✓
- [Detecting Pass-the-Hash](#) ✓
- [Detecting Pass-the-Ticket](#) ✓
- [Detecting Overpass-the-Hash](#) ✓
- [Detecting Golden Tickets/Silver Tickets](#) ✓
- [Detecting Unconstrained Delegation/Constrained Delegation Attacks](#) ✓
- [Detecting DCSync/DCShadow](#) ✓

#### Leveraging Splunk's Application Capabilities

- [Creating Custom Splunk Applications](#) ✓

#### Leveraging Zeek Logs

- [Detecting RDP Brute Force Attacks](#) ✓
- [Detecting Beaconing Malware](#) ✓
- [Detecting Nmap Port Scanning](#) ✓
- [Detecting Kerberos Brute Force Attacks](#) ✓
- [Detecting Kerberoasting](#) ✓
- [Detecting Golden Tickets](#) ✓
- [Detecting Cobalt Strike's PSEXec](#) ✓
- [Detecting Zerologon](#) ✓
- [Detecting Exfiltration \(HTTP\)](#) ✓
- [Detecting Exfiltration \(DNS\)](#) ✓
- [Detecting Ransomware](#) ✓

#### Skills Assessment

Rubeus, however, presents a somewhat different scenario. Unless the requested TGT is used on another host, Pass-the-Ticket detection mechanisms may not be effective, as Rubeus sends an AS-REQ request directly to the Domain Controller (DC), generating **Event ID 4768 (Kerberos TGT Request)**. However, communication with the DC (**TCP/UDP port 88**) from an unusual process can serve as an indicator of a potential Overpass-the-Hash attack.

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at [http://\[Target IP\]:8000](http://[Target IP]:8000) and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

## Detecting Overpass-the-Hash With Splunk (Targeting Rubeus)

Now let's explore how we can identify Overpass-the-Hash, using Splunk.

**Timeframe:** **earliest=1690443407 latest=1690443544**

Detecting Overpass-the-Hash

```

index=main earliest=1690443407 latest=1690443544 source="XmlWinEventLog:Microsoft-Windows-Sysmon/Op
| eventstats values(process) as process by process_id
| where EventCode=3
| stats count by _time, Computer, dest_ip, dest_port, Image, process
| fields - count

```

New Search

Save As
Create Table View
Close

1
index=main earliest=1690443407 latest=1690443544 source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" (EventCode=3 dest\_port=88 Image!=\*lsass.exe) OR EventCode=1
2
| eventstats values(process) as process by process\_id
3
| where EventCode=3
4
| stats count by \_time, Computer, dest\_ip, dest\_port, Image, process
5
| fields - count

Last 24 hours

1 event (7/27/23 7:36:47.000 AM to 7/27/23 7:39:04.000 AM)
No Event Sampling

Job

Events
Patterns
Statistics (1)
Visualization

20 Per Page
Format
Preview

_time	Computer	dest_ip	dest_port	Image	process
2023-07-27 07:36:50	BLUE.corp.local	10.10.0.20	88	C:\Users\LANDON_HINES\Downloads\Rubeus.exe	Rubeus.exe asktgt /user:Administrator /domain:corp.local /rc4:fc525c9683e8fe67095ba2ddc971889

### VPN Servers

**Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3

Medium Load

PROTOCOL

UDP 1337
TCP 443

DOWNLOAD VPN CONNECTION FILE

### Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK

139ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

☐ Enable step-by-step solutions for all questions ⓘ ✨

## Questions

Answer the question(s) below to complete this Section and earn cubes!



Download VPN  
Connection File

Target(s): [Click here to spawn the target system!](#)

+ 1 📦 Employ the Splunk search provided at the end of this section on all ingested data (All time) to find all involved images (Image field). Enter the missing image name from the following list as your answer. Rubeus.exe, \_\_.exe

rundll32.exe

Submit

← Previous

Next →

✔ Mark Complete & Next

