# Detecting Password Spraying

## Password Spraying

Unlike traditional brute-force attacks, where an attacker tries numerous passwords for a single user account, `password spraying` distributes the attack across multiple accounts using a limited set of commonly used or easily guessable passwords. The primary goal is to evade account lockout policies typically instituted by organizations. These policies usually lock an account after a specified number of unsuccessful login attempts to thwart brute-force attacks on individual accounts. However, password spraying lowers the chance of triggering account lockouts, as each user account receives only a few password attempts, making the attack less noticeable.

An example of password spraying using the Spray tool can be seen below.

```
┌──(kali㉿kali)-[~/tools/Spray]
└─$ sudo ./spray.sh -smb 10.0.10.100 users.txt passwords-English.txt 100 30

Spray 2.1 the Password Sprayer by Jacob Wilkin(Greenwolf)

15:08:00 Spraying with password: Users Username
15:08:00 Spraying with password: Winter2016
15:08:00 Spraying with password: Winter2017
15:08:01 Spraying with password: Winter16
15:08:01 Spraying with password: Winter17
15:08:01 Spraying with password: Winter12
15:08:02 Spraying with password: Spring2016
15:08:02 Spraying with password: Spring2017
15:08:02 Spraying with password: Spring16
15:08:02 Spraying with password: Spring17
15:08:03 Spraying with password: Spring12
15:08:03 Spraying with password: Summer2016
15:08:03 Spraying with password: Summer2017
15:08:04 Spraying with password: Summer16
15:08:04 Spraying with password: Summer17
15:08:04 Spraying with password: Fall2016
15:08:04 Spraying with password: Fall2017
15:08:05 Spraying with password: Fall1234
15:08:05 Spraying with password: Autumn2016
15:08:05 Spraying with password: Autumn2017
15:08:06 Spraying with password: Autumn16
15:08:06 Spraying with password: Autumn17
```

### Password Spraying Detection Opportunities

Detecting password spraying through Windows logs involves the analysis and monitoring of specific event logs to identify patterns and anomalies indicative of such an attack. A common pattern is multiple failed logon attempts with `Event ID 4625 - Failed Logon` from different user accounts but originating from the same source IP address within a short time frame.

Other event logs that may aid in password spraying detection include:

- `4768 and ErrorCode 0x6 - Kerberos Invalid Users`
- `4768 and ErrorCode 0x12 - Kerberos Disabled Users`
- `4776 and ErrorCode 0xC000006A - NTLM Invalid Users`
- `4776 and ErrorCode 0xC0000064 - NTLM Wrong Password`
- `4648 - Authenticate Using Explicit Credentials`
- `4771 - Kerberos Pre-Authentication Failed`

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.

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

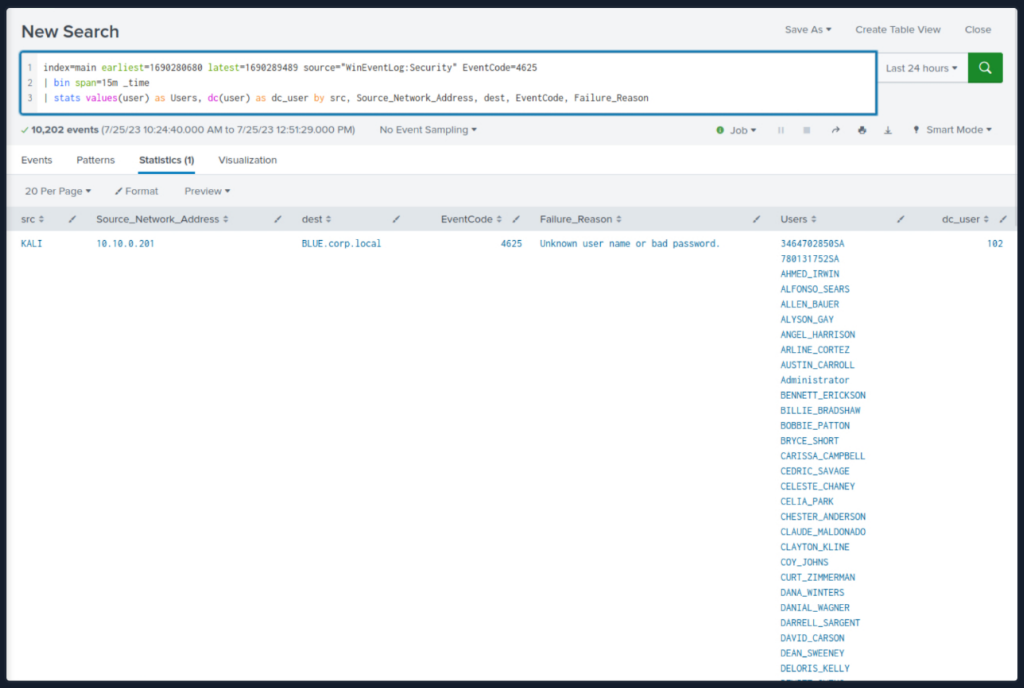
# Detecting Password Spraying With Splunk

Now let's explore how we can identify password spraying attempts, using Splunk.

**Timeframe**: `earliest=1690280680 latest=1690289489`

Detecting Password Spraying

```
index=main earliest=1690280680 latest=1690289489 source="WinEventLog:Security" EventCode=4625
| bin span=15m _time
| stats values(user) as Users, dc(user) as dc_user by src, Source_Network_Address, dest, EventCode,
```




**Search Breakdown**:

- `Filtering by Index, Source, and EventCode`: The search starts by selecting events from the main index where the source is `WinEventLog:Security` and the `EventCode` is `4625`. This EventCode represents failed logon attempts in the Windows Security Event Log.
- `Time Range Filter`: The search restricts the time range of events to those occurring between the Unix timestamps 1690280680 and 1690289489. These timestamps represent the earliest and latest times in which the events occurred.
- `Time Binning`: The `bin` command is used to create `time buckets of 15 minutes` duration for each event based on the `_time` field. This step groups the events into 15-minute intervals, which can be useful for analyzing patterns or trends over time.
- `Statistics`: The `stats` command is used to aggregate events based on the fields `src`, `Source_Network_Address`, `dest`, `EventCode`, and `Failure_Reason`. For each unique combination of these fields, the search calculates the following statistics:
  - `values(user) as Users`: All unique values of the `user` field within each group.
  - `dc(user) as dc_user`: The distinct count of unique values of the `user` field within each group. This represents the number of different users associated with the failed logon attempts in each group.

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 142ms

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) and enter the targeted user on SQLSERVER.corp.local as your answer.

sa

Submit

Previous Next

Mark Complete & Next