**How to Query for Password Guessing Using the Elastic Stack**

**Task.** Query for logon failures using the Elastic Stack.

**Purpose.** Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. The Elastic Stack is a collection of services that allow you to ingest, search, and visual data (i.e., Windows Events). Logon types of interest are: 2 (local), 3 (network; sometimes generated by the “net use” command or RPC activity), and 10 (Terminal Services like Remote Desktop).

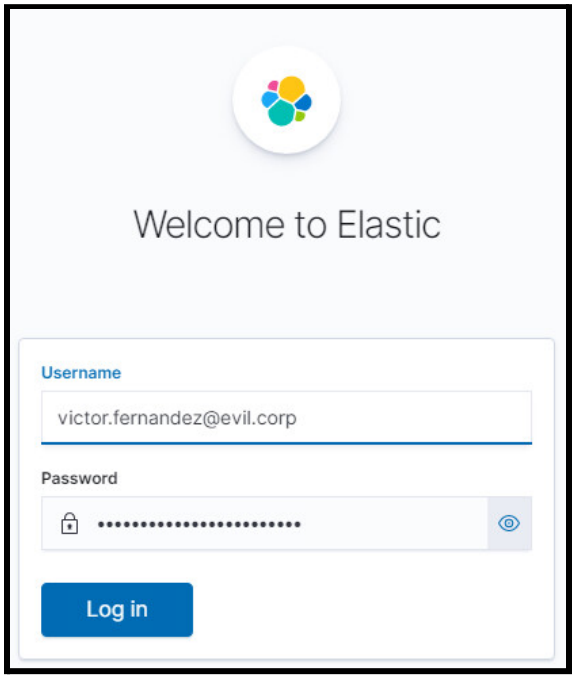
**Conditions.** Logon/logoff auditing is enabled. Windows Event Forwarding is configured. Winlogbeat is installed on a Windows Event Collector and shipping forwarded Windows Events to an Elastic Stack instance. You have access to said Elastic Stack instance.

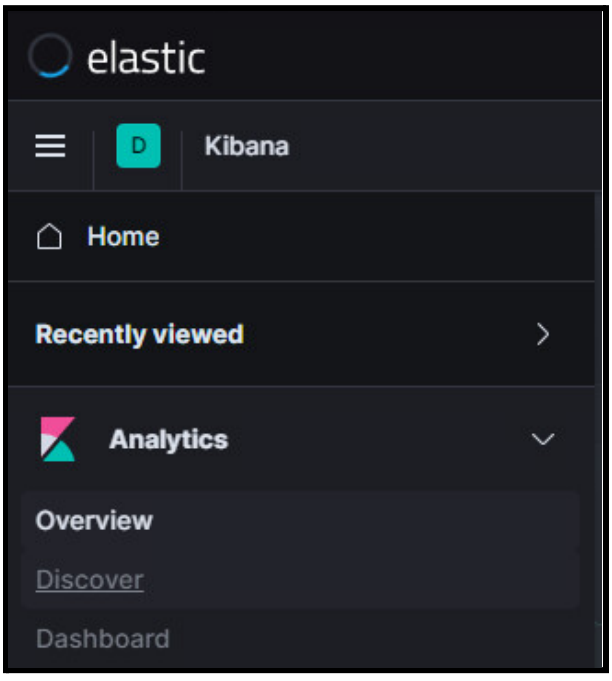
**Standard.** You were able to perform a query and determine if suspicious or malicious activity has occurred.

**MITRE ATT&CK**

- **Tactic:** Credential Access
- **Technique:** T1110 - Brute Force
- **Sub-Technique:** T1110.001 - Password Guessing

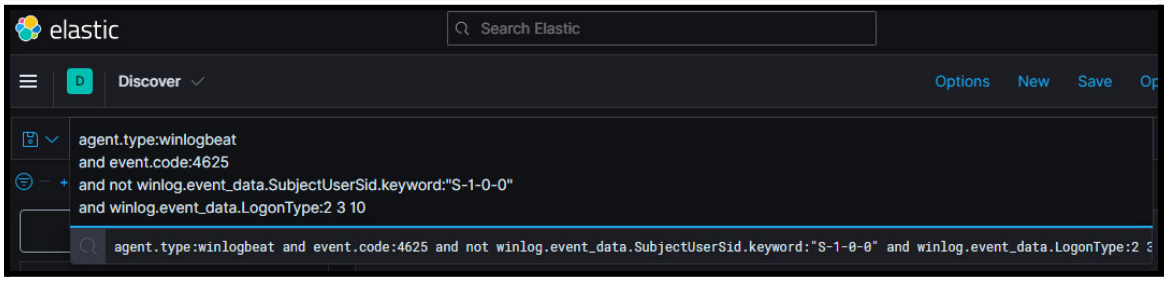
**Step 1.** Login to your Elastic Stack instance (this How-To uses the “Security Onion” platform). Click the Triple Bar symbol in the top-left corner to open the Navigation Bar. Under the “Analytics” section, click “Discover.”



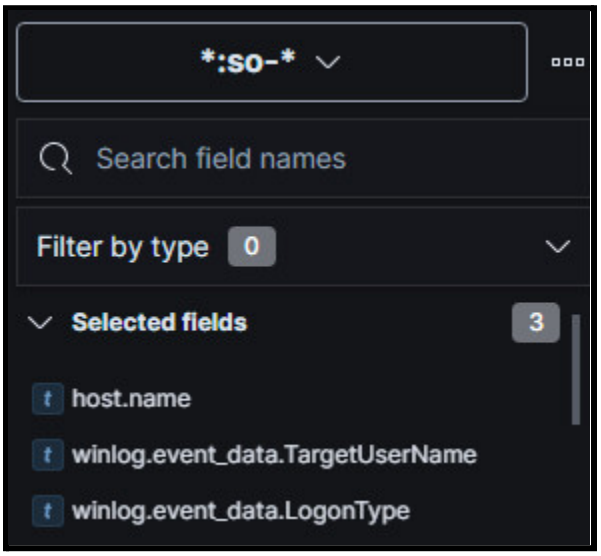



**Step 2.** Copy/paste your query into the “Search” bar and click “Update.” Below is one example.

```
agent.type:winlogbeat
and event.code:4625
and not winlog.event_data.SubjectUserSid:"S-1-0-0"
and winlog.event_data.LogonType:2 3 10
```




**Step 3.** Using the “Search field names” bar, search for and add the following fields: host.name, winlog.event_data.TargetUserName, and winlog.event_data.LogonType. Collapse the “Search field names” bar to make it easier to review your query result.




**Step 4.** Review your query result for suspicious and/or malicious activity.