How to Query for PowerShell Abuse Using the Elastic Stack

Task. Query for PowerShell abuse using the Elastic Stack.

Purpose. PowerShell is a command-line and scripting interface within the Windows operating system. Adversaries abuse PowerShell to download and execute malicious code. The Elastic Stack is a collection of services that allow you to ingest, search, and visual data.

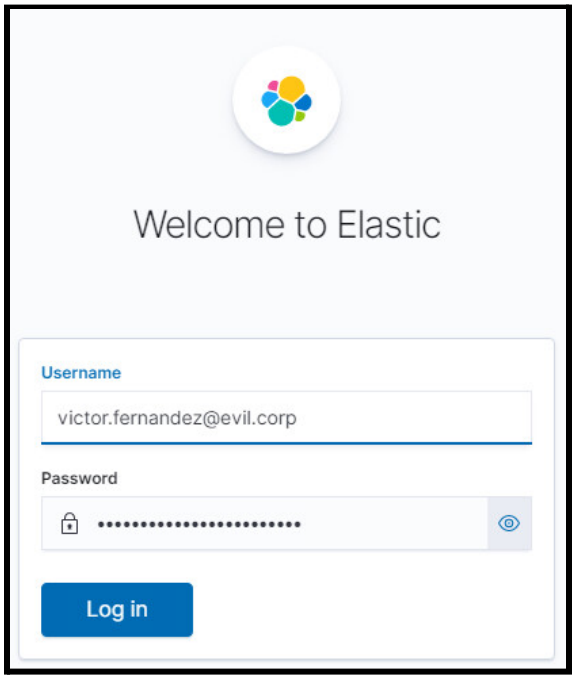
Conditions. PowerShell Script Block Logging is enabled. Windows Event Forwarding is configured. Winlogbeat is installed on a Windows Event Collector and shipping forwarded Windows Events to an Elastic Stack instance. You have access to said Elastic Stack instance.

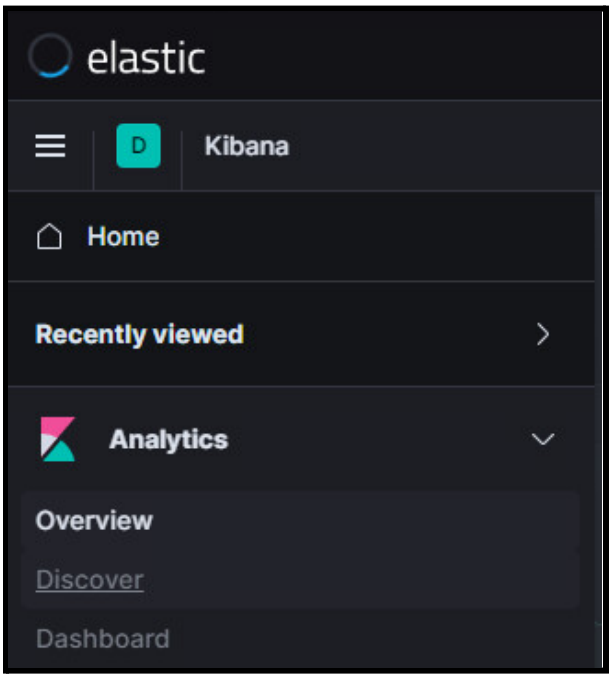
Standard. You were able to perform a query and determine if suspicious or malicious activity has occurred.

MITRE ATT&CK

- **Tactic:** Execution
- **Technique:** T1059 - Command and Scripting Interpreter
- **Sub-Technique:** T1059.001 - PowerShell

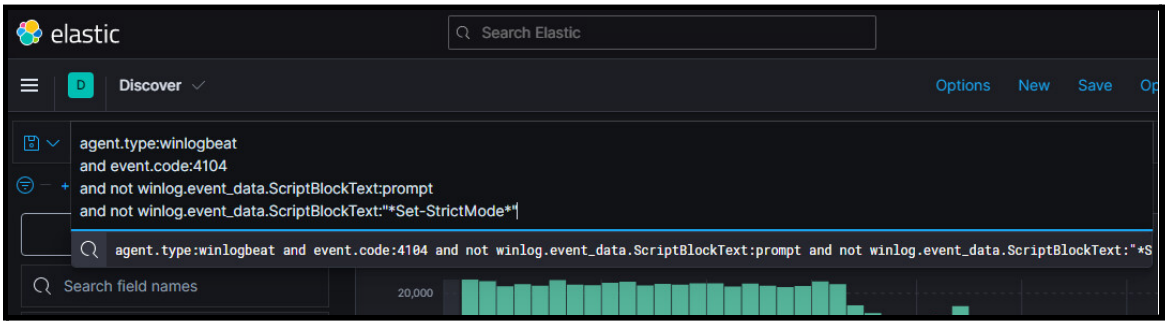
Step 1. Login to your Elastic Stack instance (this How-To uses the “Security Onion” platform). Click the Triple Bar symbol in the top-left corner to open the Navigation Bar. Under the “Analytics” section, click “Discover.”



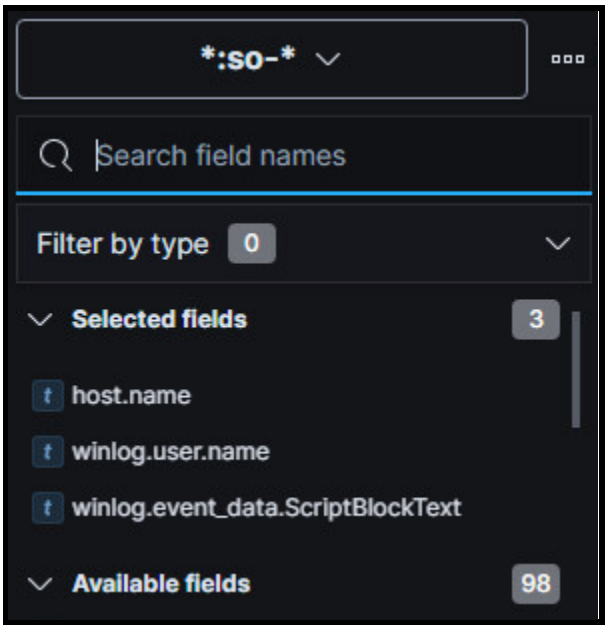


Step 3. Copy/paste your query into the “Search” bar and click “Update.” Below is one example.

```
agent.type:winlogbeat
and event.code:4104
and not winlog.event_data.ScriptBlockText:prompt
and not winlog.event_data.ScriptBlockText:"*Set-StrictMode*"
```



Step 4. Using the “Search field names” bar, search for and add the following fields: host.name, winlog.user.name, winlog.event_data.ScriptBlockText. Collapse the “Search field names” bar to make it easier to review your query result.



Step 5. Review your query result for suspicious and/or malicious activity.