SSgt Thomas Blauvelt

32 WPS/DOA | Nellis AFB, Nevada

**Defensive System Training - 2**

Lab: Windows Host Interrogation

Contents

[Lab: Threat Hunting with Powershell and Metasponse 2](#_Toc147061859)

[Overview 2](#_Toc147061860)

[Procedures 3](#_Toc147061861)

[Step 1. Configure Custom Index Patterns 3](#_Toc147061862)

|  |  |  |
| --- | --- | --- |
| **Symbols Table** | |  |
| **Symbol** | **Name** | **Meaning** |
| ✅ | **Note** | Detailed information that is required to fully understanding the concept or to be able to execute a procedure but is not necessarily related to a key learning objective. |
| **💡** | **Learning Point** | Information related to key learning objectives. |
| ⚠️ | **Warning** | Important information related to safety and security. |
| ✋ | **Raise Hand** | Raise your hand for instructor assistance. This is often used at critical points to validate your understanding of the material. |

# Lab: Threat Hunting with Powershell and Metasponse

## Overview

**Summary:** The purpose of this lab is to acquire the necessary knowledge and skills to effectively navigate PowerShell, Metasponse collectors, and generating sample data with Metasploit to investigate malicious cyber activity. Throughout the course of this lab, you will be creating the artifacts that you’ll be required to present during the assessment.

**Outcomes:** By the end of the lab, you will be able to perform the following:

* Generate malicious payloads with Metasploit
* Establish session with malicious payloads executed on Windows workstations
* Enumerate local Windows resources with Metasploit
* Create a malicious service executable with Metasploit
* Use Metasponse collectors to gather host information from Windows workstations
* Create Metasponse jobs and macros
* Use Microsoft SysInternals to triage Windows workstations
* Use PowerShell to gather host information from Windows workstations
* Use PowerShell to remotely gather host information from Windows workstations
* Use PowerShell to generate investigation artifacts

## Procedures

### Configure Custom Index Patterns

Index Patterns are used in ElasticSearch queries to identify the data that you want to explore. This allows the operator to query multiple indices or only one specific index depending upon how specific the pattern is. For example, you may want to run a query against both Sysmon logs and Windows Event Logs searching for process execution because Sysmon isn’t fully deployed in the environment. The two datasets likely reside in different indices because they contain a different schema. Another reason to use index patterns is because your indices are named based upon the rollover date. Instead of having one massive index with every log ever created in the environment, you may have multiple indices such as so-beats-2022.04.03 where the data at the end increments every X days or when the index reaches a certain size. You could create an index pattern such as so-beats-\* to query all of the logs that have ever existed, or you could query so-beats-2022-04-\* to only get logs from April 2022, thus reducing the amount of time it takes to return the query compared to querying every index.

1. Navigate to SecurityOnion by going to the following URL:
   1. **URL:** <https://192.168.10.4>
   2. **Username:** soadmin@lab.net
   3. **Password:** !QAZ2wsx
2. Go to **Tools → Kibana → Login**
3. Login with the following credentials:
   1. **Username:** soadmin@lab.net
   2. **Password:** !QAZ2wsx
4. Click on the three horizontal bars in the top, left-hand corner of the screen to open the main menu, then