**Week 18 SIEM**

**Step 1: Monitoring Vandalay's Web Servers**

1. Select **Ping** >> and **Execute Ping** (leave the other fields as they are)
   * Enter in the following hosts one at a time: 198.153.194.1 and 198.153.194.2 then click **Execute Ping**
2. Let the monitoring run and view the **results** page
3. Provide a screenshot of the results screen that displays the state of your web servers

### 

### 

### Step 2: The Need for Speed

Answer the following questions:

* Based on the report created, what is the approximate date and time of the attack?

Approximate date and time of attack:

2020-02-23, 14:30:00

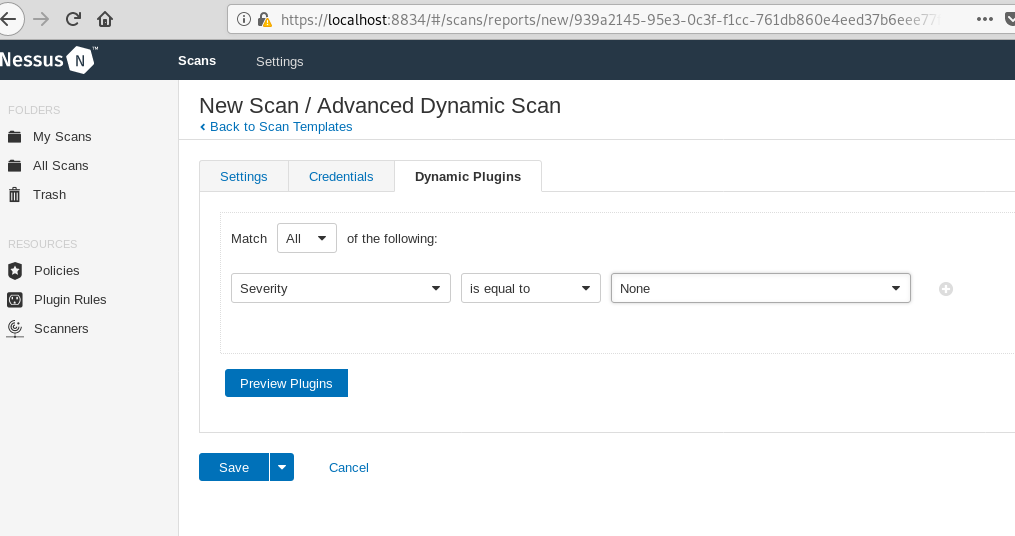
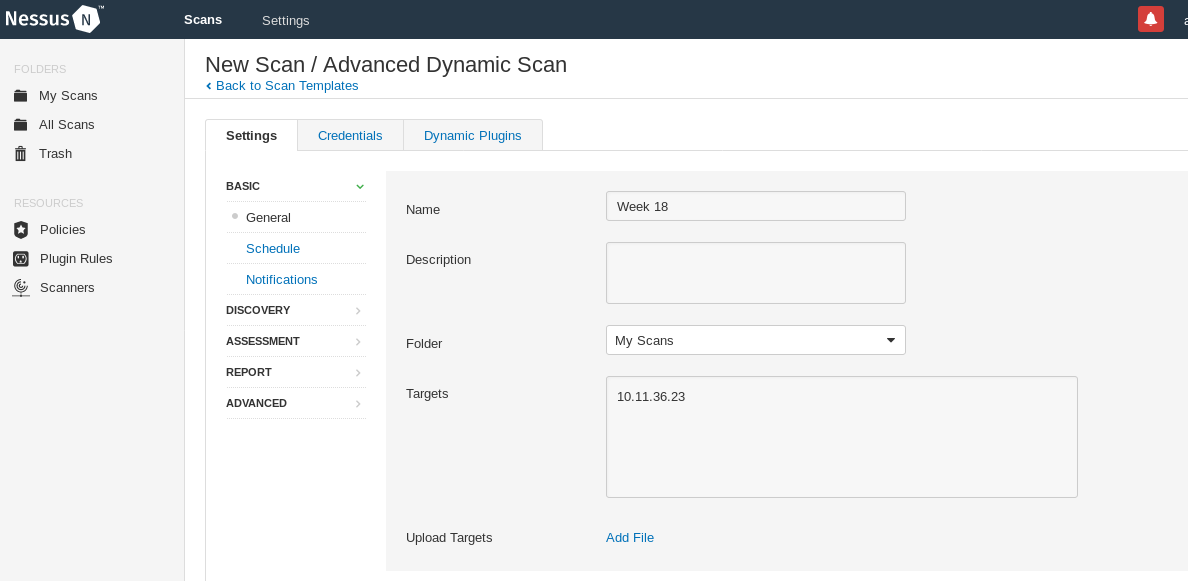
* How long did it take your systems to recover?

Duration of recovery:

9 hours before download/upload speeds fully recovered

### **Step 3: Are We Vulnerable?**

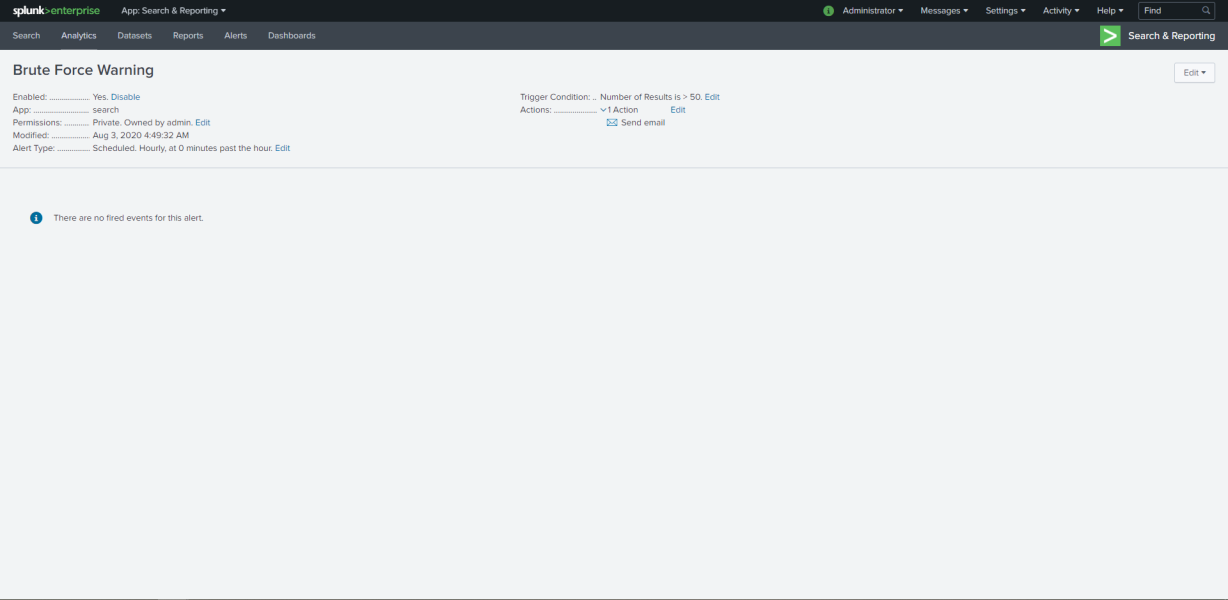
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.



**Step 4: Drawing the (base)line**

**Task:** Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

1. Upload the administrator login logs.



1. When did the brute force attack occur?

Time of the brute force attack:

02/21/2020 3:48:37.000 PM

1. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.

Baseline of normal activity:

10 bad logons per hour

1. Design an alert to check the threshold every hour and email the SOC team at [SOC@vandalay.com](mailto:SOC@vandalay.com) if triggered.

Threshold for brute force alert:

50+ logons per hour