

# GoodSecurity Penetration Test Report

JasonScherer [@JobeCorp.com](mailto:JasonScherer@JobeCorp.com)

11/16/2021

## 1.0 High-Level Summary

### Scenario

In the previous class, you set up your SOC and monitored attacks from JobeCorp. Now, you will need to design mitigation strategies to protect VSI from future attacks.

You are tasked with using your findings from the Master of SOC activity to answer questions about mitigation strategies.


### System Requirements

You will be using the Splunk app located in the Ubuntu VM.

## 2.0 Findings

### Part 1: Windows Server Attack

- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.
  - The two top results:
    - On 3/25/2020 from 11:40 AM to 2:40 AM: `a user account was locked out.` user\_a was affected.
    - On 3/25/2020 from 9:00 AM to 11:00 AM: `An attempt was made to reset an account's password.` user\_k was affected.
  - The company should employ an "Account Lockout Policy." This lockout policy will allow user error but will also allow brute force attacks. Threshold can be set to 10 per the Windows Security recommendation.

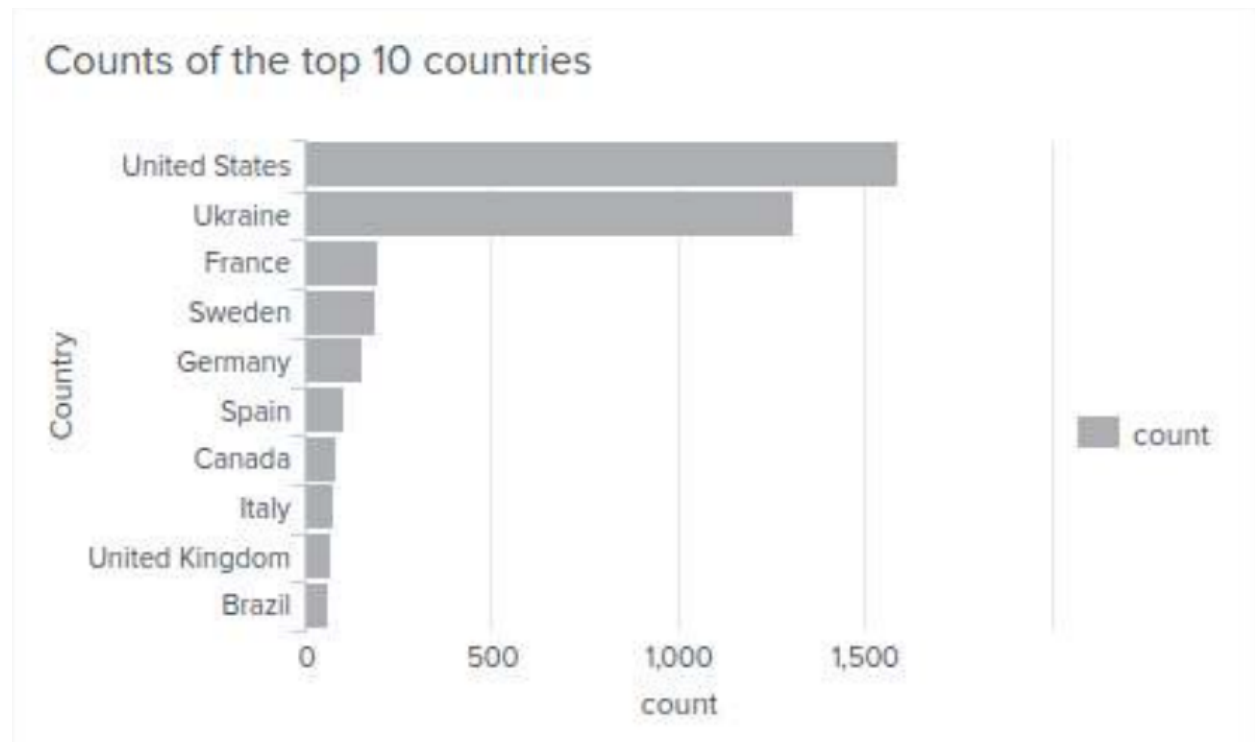
New Search			Save As ▾	Create Table View	Close
source="windows_server_attack_logs.csv"   top limit=20 signature				All time ▾	
✓ 5,949 events (before 6/19/21 8:18:04.000 AM) No Event Sampling ▾			Job ▾		Verbose Mode ▾
Events (5,949)	Patterns	Statistics (15)	Visualization		
20 Per Page ▾	Format	Preview ▾			
signature ↕		count ↕		percent ↕	
An attempt was made to reset an accounts password		2128		35.770718	
A user account was locked out		1811		30.442091	
An account was successfully logged on		432		7.261725	
Domain Policy was changed		143		2.403765	
The audit log was cleared		142		2.386956	
A user account was changed		137		2.302908	
A privileged service was called		136		2.286099	
A process has exited		134		2.252479	
A computer account was deleted		133		2.235670	
A user account was deleted		130		2.185241	
A logon was attempted using explicit credentials		130		2.185241	
System security access was removed from an account		128		2.151622	
Special privileges assigned to new logon		127		2.134813	
System security access was granted to an account		123		2.067574	
A user account was created		115		1.933098	

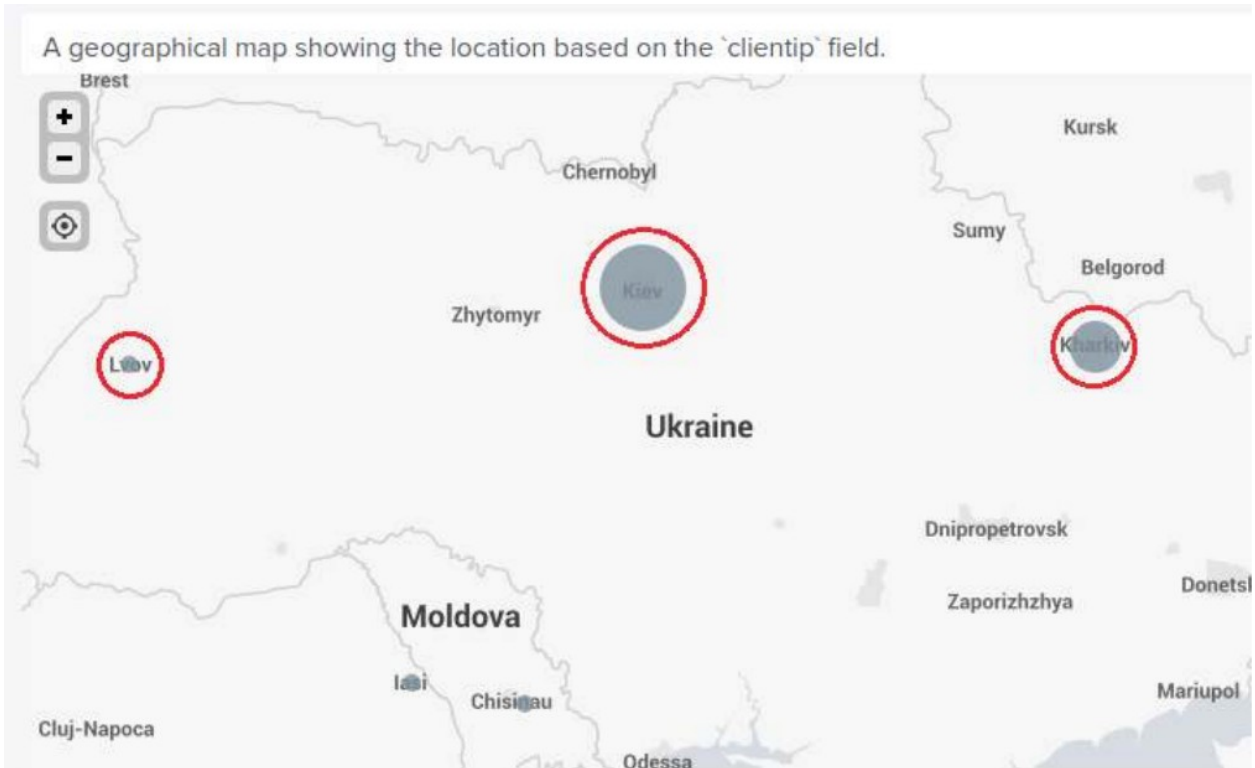
- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?
  - There are a number of recommendations for preventing Brute Force Attacks:
    - Account lockouts with delays to accommodate legitimate failed attempts.
    - Use Captcha to validate login attempts.
    - Ensure the root user is not accessible via SSH by editing the file: sshd\_config file.
    - Use unique login URLs.
    - Require 2 Factor Authentication.

## Part 2: Apache Webserver Attack

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
- Provide a screen shot of the geographic map that justifies why you created this rule.

Using the search command: `source="apache_attack_logs.txt" | iplocation clientip | top limit=10 Country`





In addition to source IPs from the United States a large volume of Ips were from the Ukraine. Specifically from three cities; Kiev with 872, Kharkiv 432, and Lvov with 5, totalling 1309 IPs. Given this data a mitigation could be to block all incoming HTTP traffic from the Ukraine in the firewall settings.

VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.

- What other rules can you create to protect VSI from attacks against your webserver?
- Conceive of two more rules in "plain english".
- Hint: Look for other fields that indicate the attacker.

- Based upon the different HTTP methods we can find the POST method has been used 1296 times on 3/25/2020 7:00 PM – 9:00 PM. The post URI is /VSI\_Account\_logon.php. Based on this there best mitigation strategies are using Account lockouts with delays set at 10 attempts and 2 Factor Authentication.