Coursework

Unit 19 Homework: Protecting VSI from Future Attacks

Submitted By
Shaerul Haque Joarder

Part 1: Windows Server Attack

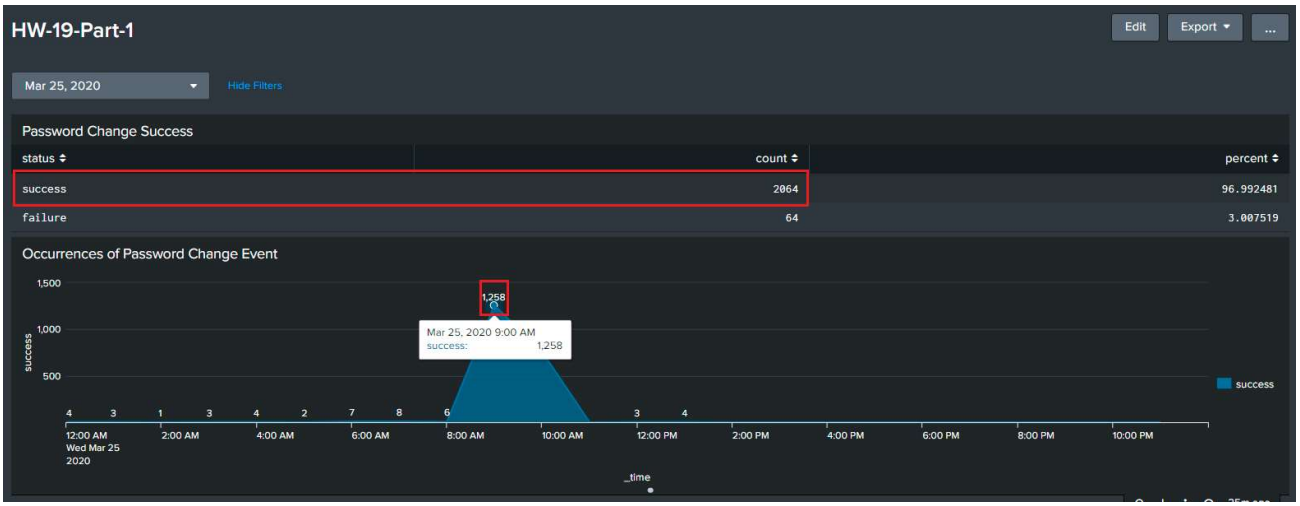
Note: This is a public-facing windows server that VSI employees access.

Question 1

- 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.

Answer:

Its evident from Splunk Analysis on the field key **signature** and value **"An attempt was made to reset an accounts password"** that the conducted attack happened between **8:00-11:00AM**. The peak occurrences count was **1258**. That took place exactly at **9:00AM**.



Remedy

- Configure Windows Account Lockout e.g. Microsoft's 10/15/15 recommendation [https://techcommunity.microsoft.com/t5/microsoft-security-baselines/configuring-account-lockout/ba-p/701040]
- Force Strong Password Selection (Character Mix, Length) Policy in place
- Force Periodic Password Change
- Applying Rate Limit from Same Source IP in Firewall/IPS
- Applying Captcha Security Image in web application
- Applying at least Two-Factor Authentication (Google® Authenticator, OTP over SMS etc.)
- Implementing SoC for Real-Time Threat Monitoring and actionable insights
- Home or remote users should be allowed through Secure VPN tunnel

Question 2

- 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?

Answer:

In addition to helping to prevent intrusions, account lockouts can also expose your organization to denial-of-service attacks and accidental lockouts, as attackers can easily deliberately lock out multiple accounts at once with the account lockout mechanism in place.

In this case, **Microsoft's 10/15/15 recommendation** is a good and optimal choice to follow. This notation has been explained below.

Setting's Name	Description	Recommended Value
Account lockout threshold	The number of failed logons attempts that trigger account lockout. If set to 0, account lockout is disabled, and accounts are never locked out.	10
Account lockout duration	The number of minutes that an account remains locked out before it's automatically unlocked. If set to 0, the account remains locked out until an administrator explicitly unlocks it.	15
Reset account lockout counter after	The number of minutes after a failed logon attempt before the bad-logon counter is reset to 0. The counter is also reset after a successful logon.	15

Part 2: Apache Webserver Attack:

Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
    - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screen shot of the geographic map that justifies why you created this rule.

Answer:

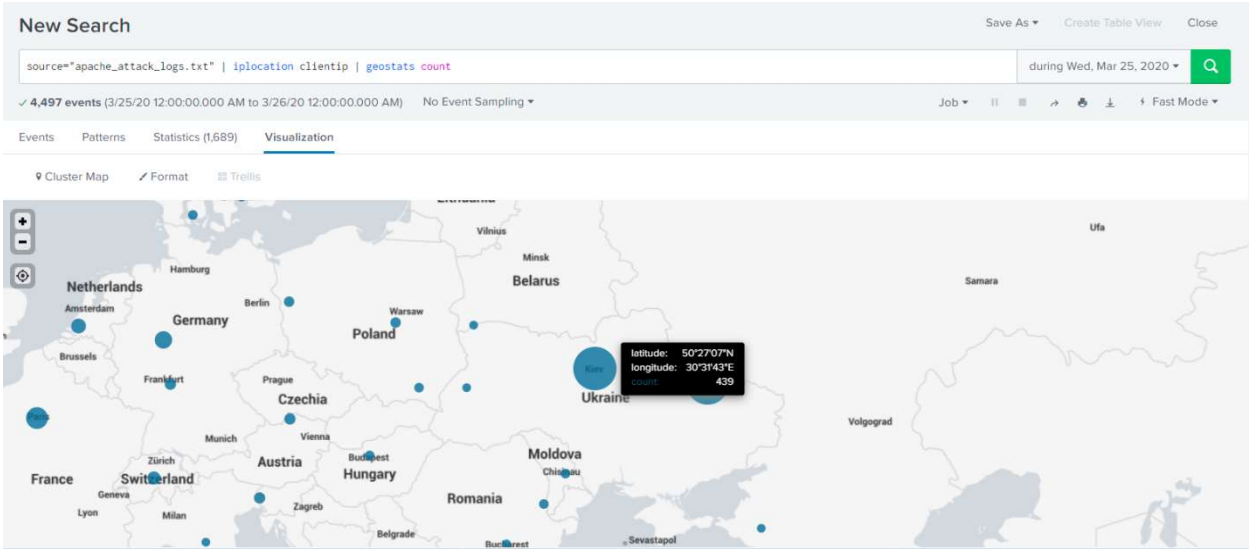
Generic Firewall rule Syntax:

<priority#> deny <protocol> from <source_ip> <source_port> to <destination_ip> <destination_port>

Plain English Description:

Block all incoming HTTP traffic where the source IP comes from the city of Kiev, country Ukraine.

Screen shot of the geographic map in Splunk®



Question 2

- 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.

Answer:

Blocking matched HTTP Headers for **`method, uri and useragent`** fields' key value can prevent malicious and repetitive attacks from VSI.