Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

Kali
- Operating System: Linux
- Purpose: Attacker VM
- IP Address: 192.168.1.90

Capstone
- Operating System: Linux
- Purpose: Host/Victim VM
- IP Address: 192.168.1.105

Target 1
- Operating System: Linux
- Purpose: Host/Victim VM
- IP Address: 192.168.1.110

Target 2
- Operating System: Linux
- Purpose: Host/Victim VM
- IP Address: 192.168.1.110

ELK
- Operating System: Linux
- Purpose: Log capture/aggregation/analysis VM
- IP Address: 192.168.1.105

Description of Targets

Fill in the following:

- Two VMs on the network were vulnerable to attack: Target 1 [IP address 192.168.1.110] and Target 2 [IP address 192.168.1.115].

- Each VM functions as an Apache web server and has SSH enabled, so ports `80` and `22` are possible ports of entry for attackers.

Monitoring the Targets

This scan identifies the services below as potential points of entry:

- **Target 1**
    - Open ports
    - WordPress server
    - Mysql database

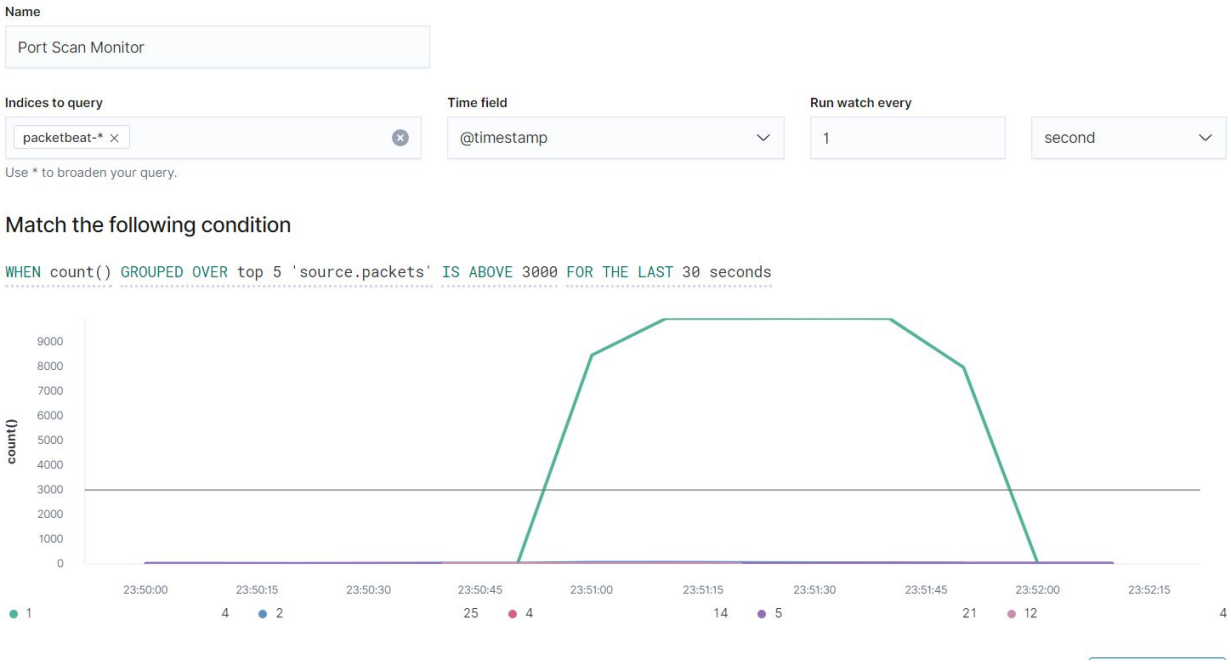
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

Name of Alert 1 - Port Scan Monitor

Port Scan Monitor is implemented as follows:

- Metric: HTTP source packets (source.packets)
- Threshold: over 3000 source packets over a 30-second time period
- Vulnerability Mitigated: Network scan to locate open ports of entry
- Reliability: The reliability and accuracy of this alert is quite high. It consistently and accurately picked up the packet counts of nmap scans.

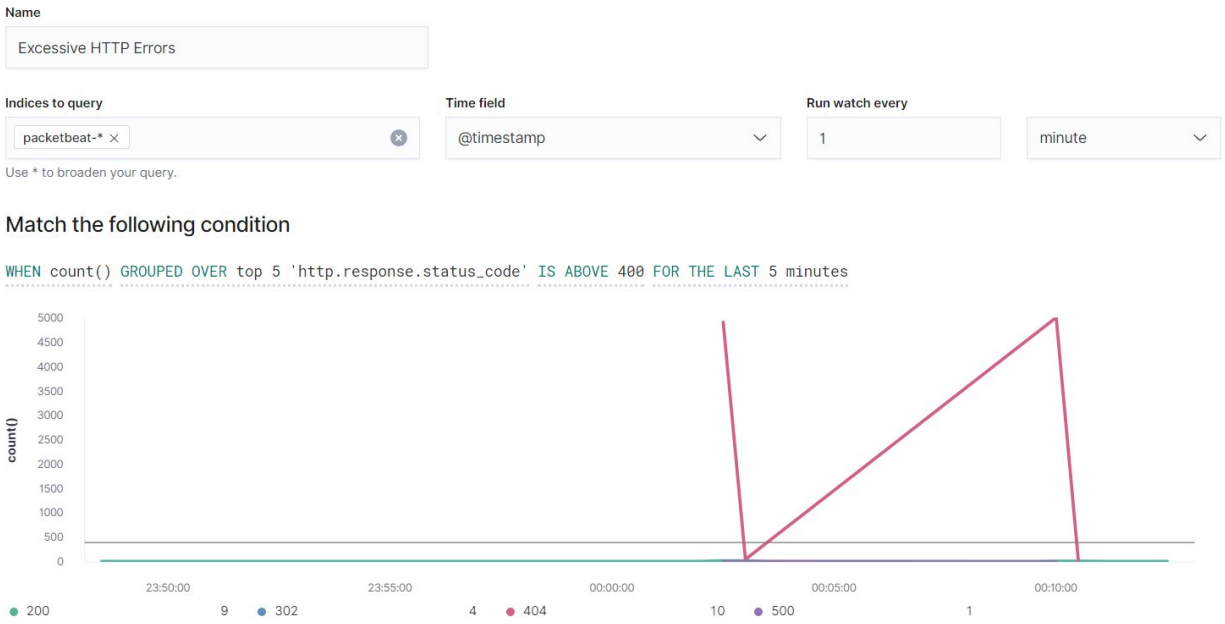
Alert results after a nmap scan over subnet 192.168.1.0/24



Name of Alert 2 - Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

- Metric: HTTP response status codes
- Threshold: 400 over a 5-minute timeframe
- Vulnerability Mitigated: WordPress server
- Reliability: The reliability and accuracy of this alert is quite high. It consistently and accurately picked up the wpscan scans for services. As wpscan uses brute force tactics to identify items in a network, this alert picked up most all errored status codes (400 +, 500+ range).



Name of Alert 3 - HTTP Request Size Monitor

HTTP Request Size Monitor is implemented as follows:

- Metric: HTTP request bytes
- Threshold: Over 3500 bytes over a 1 minute timeframe
- Vulnerability Mitigated: none
- Reliability: This alert never fired.

Name of Alert 4 - CPU Usage Monitor

CPU Usage Monitor is implemented as follows:

- Metric: Total system process CPU usage
- Threshold: Over 50% CPU usage over a 5- minute timeframe
- Vulnerability Mitigated: none
- Reliability: This alert never fired.

Suggestions for Going Further

Suggest a patch for each vulnerability identified by the alerts above. Remember: alerts only detect malicious behavior. They do not prevent it. It is not necessary to explain how to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

Vulnerability 1 - Open SSH port 22 exposed via nmap scan

- Patch: Setting to shut ports, block network access to any IP address that exceeds the Port Scan Monitor threshold.
- Why It Works: Does not allow IP address to further investigate or act against the network system.

Vulnerability 2 - WordPress web server - finding usernames with wpscan

- Patch: Encrypt all usernames within WorkPress web server. Temporarily or permanently block further network access to any IP address that exceeds the Excessive HTTP Errors alert threshold.
- Why It Works: Does not show usernames within WordPress once the WordPress enumeration scan has been made. Blocking access halts further action from the offending IP address.

Vulnerability 3 - SSH allowed login with weak user authentication

- Patch: Block SSH authority from all user accounts. Grant SSH authority to only authorized user accounts (ie, system admins).
- Why It Works: Hardens unauthorized system access from all users other than few users who may need SSH logins, such as system administrators.
- Patch: Force complex passwords upon creation and reset. Reject attempts to reset a password that has been already used.
- Why It Works: Makes password hacking from users outside of the network much more difficult.

Vulnerability 4 - Authentication controls - plain-text mysql username and password found in file.

- Patch: run process that deletes username and password information from undesignated directory locations. Encrypt and store all system usernames and passwords in a secure location.
- Why It Works: Removes detection of system credentials from unauthorized users.

Vulnerability 5 - Weak sudo permission protocols

- Patch: For all user accounts, block sudo access attempts (set response to sudo command as “Unauthorized User”). For any few authorized user accounts (i.e., system

admin), force password entry for sudo requests (set sudo command response to “Password: “)

- Why It Works: Removes root system access for all unauthorized users, giving it only to those needing it through a required password.