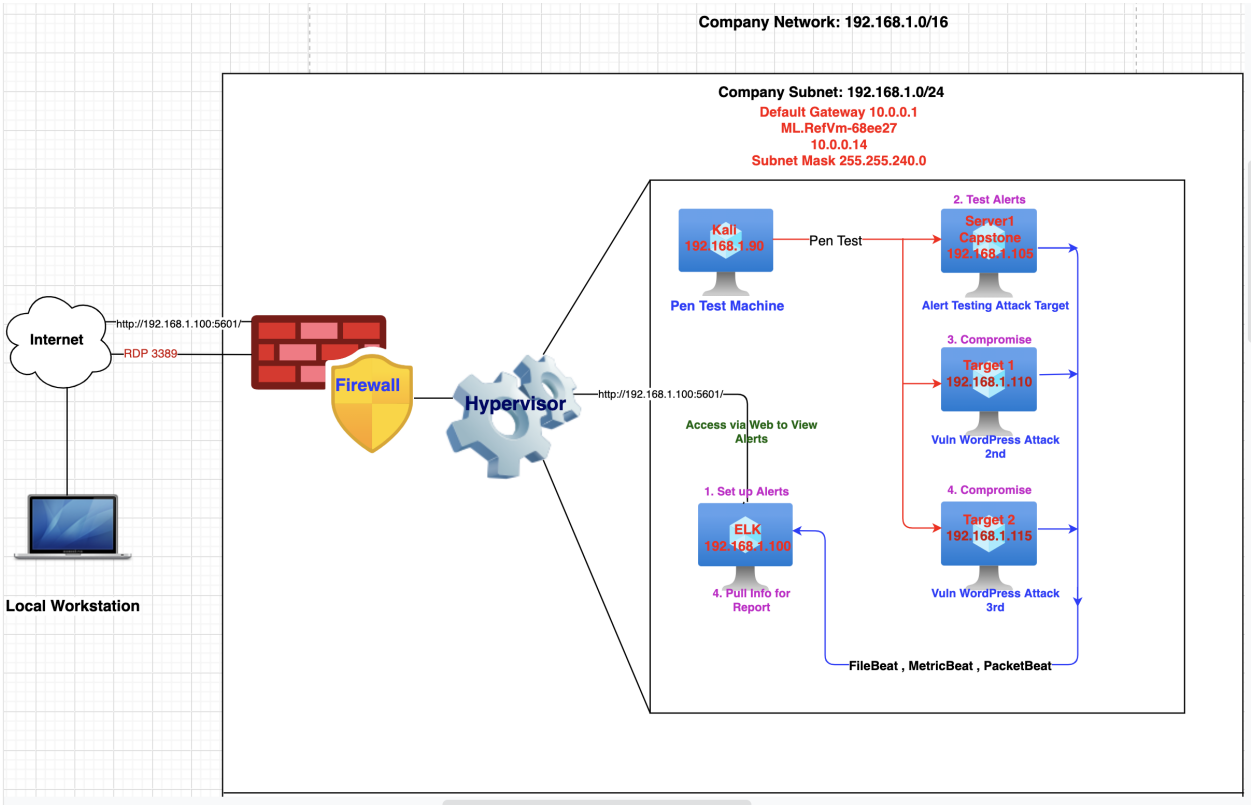
Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- **Network:**
- **Address Range:** 192.168.1.0/24
- **Netmask:** 255.255.255.0
- **Gateway:** 192.168.1.1
-

- **Machines:**
-
- **IPv4:** 10.0.0.14
- **Gateway:** 10.0.0.1
- **OS:** Windows
- **Hostname:** ML.RefVM-68ee27
-
- I**Pv4:**192.168.1.90
- **OS:** Linux
- **Hostname:** Kali
-
- **IPv4:** 192.168.1.105
- **OS:** Linux
- **Hostname:** Capstone
-
- **Pv4:** 192.168.1.110
- **OS:** Linux
- **Hostname:** Target1
-
- **Pv4:** 192.168.1.115
- **OS:** Linux
- **Hostname:** Target2
-
- **IPv4:** 192.168.1.100
- **OS:** Linux
- **Hostname:** ELK

Description of Targets

Fill in the following:

- Two VMs on the network were vulnerable to attack: Target 1 [192.168.1.110] and Target 2 [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**
    - List of Potentially vulnerable Services:
        - 80/tcp http apache httpd 2.4.10
        - 111/tcp rpcbind
        - 139/tcp netbios-ssn Samba smbd 3.x-4.x
        - 445/tcp netbios-ssn Samba smbd 3.x-4.x

- **Target 2**
    - List of Potentially vulnerableServices:
        - 22/tcp ssh
        - 80/tcp http apache httpd 2.4.10
        - 111/tcp rpcbind
        - 139/tcp netbios-ssn Samba smbd 3.x-4.x
        - 445/tcp netbios-ssn Samba smbd 3.x-4.x

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below: (Note: Add at least three alerts. You can add more if time allows.)

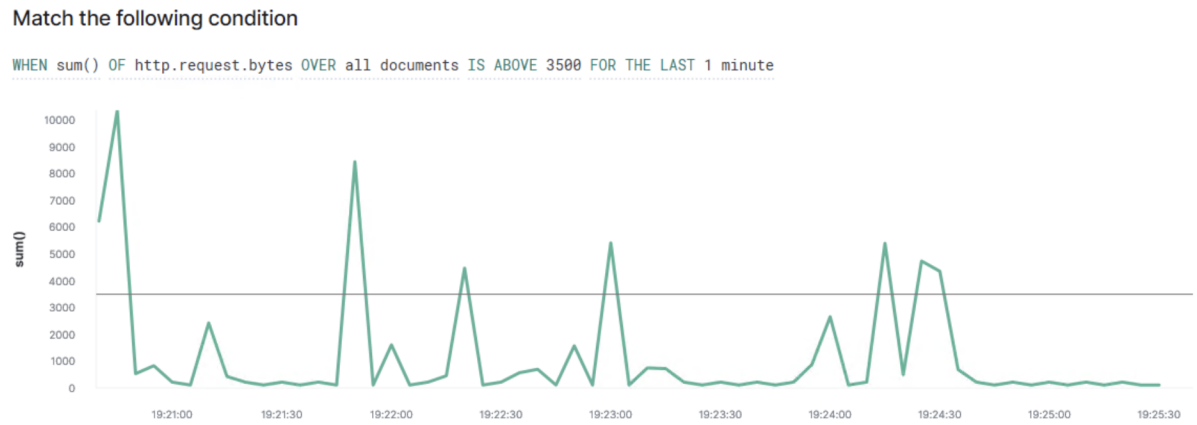
Name of Alert 1

[http request size monitor] is implemented as follows:

- Metric: http request size
- Threshold: 3500 in 1 min
- Vulnerability Mitigated: This is an indication of port scanning so we shold take these steps:
- Install a Firewall: A firewall can help **prevent** unauthorized access to your private network.
- ICMP traffic can be filtered
- An IP whitelist can be enabled
- Close the ports that are not needed
- TCP Wrappers: TCP wrapper can give administrators the flexibility to permit or deny access to the servers based on IP addresses or domain names.

- Reliability: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

No false positives. Especially when associated with a POST header



Name of Alert 2

[Excssive http errors monitor] is implemented as follows:

- Metric: Excssive http errors
- Threshold: 400 status in 1 min
- Vulnerability Mitigated: This is an indication of a brute force attack so take thse steps:
- Lock accounts after several failed login attempts
- Use tools like reCAPTCHA require users to complete simple tasks to login to a system.
- Requires everyone to create strong passwords

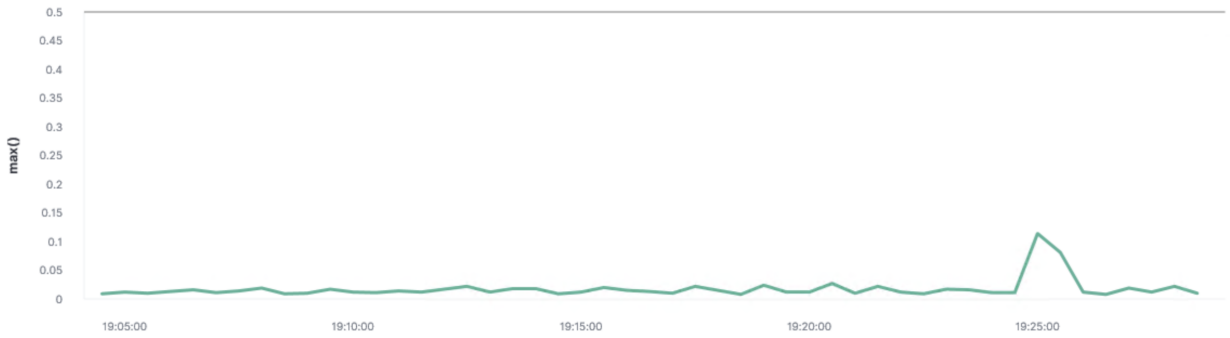
- Reliability: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.
  In general, yes this alert will create a lot of false positives

Name of Alert 3

[cpu usage monitor] is implemented as follows:

- Metric: cpu usage
- Threshold: 50% in 5 mins
- Vulnerability Mitigated: If there are any unauthorized processes running at any time
- Reliability: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

  Medium amount of false positives. There can be updates that will take up CPU



Note: If time allows, add more alerts.

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: Brute Forcing

- Patch: User blocking. If a user seems to be targeted for a brute force attack, lock the account.
- Why It Works: locking a user account can result in a failed brute force attempt, and a hacker cannot circumnavigate or continue the attack unless the account is unlocked

Vulnerability 2: unauthorized download/upload ftp transfers

- Patch:

Step 1: To disable PHP execution in the Uploads folder, simply create a .htaccess file in the Upload folder. You can find the folder in wp-content under public_html.

Step 2: Now open notepad (for Windows) or TextEdit (for Mac) to create a file. Include the following code and save this file as .htaccess (not .htaccess.txt):

BEGIN WordPress

<IfModule mod_rewrite.c>

RewriteEngine On

RewriteBase /

RewriteRule ^index\.php$ - [L] RewriteCond %{REQUEST_FILENAME} !-f

RewriteCond %{REQUEST_FILENAME} !-d

RewriteRule . /index.php [L] </IfModule>

END WordPress

<FilesMatch “\.(php|php\.)$”>

Order Allow,Deny

Deny from all

</FilesMatch>

Why It Works: This ensures that any file having .php will be caught and prevented from executing

Vulnerability 3: Ensure that logstash or other SIEM tools notify a sysadmin right away to prevent further damages

Patch:

- Why It Works: If a notification is received when excess CPU and processes are being used, a sysadmin can easily find which user is the culprit and lock them out.