Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

- Unknown VM
  - **Operating System**: Microsoft Windows XP
  - **Purpose**:
  - **IP Address**: 192.168.1.1
- ELK Server
  - **Operating System**: Linux
  - **Purpose**: ELK stack gives you the ability to aggregate logs from all your systems and applications, analyze these logs, and create visualizations for application and infrastructure monitoring, faster troubleshooting, security analytics, and more.
  - **IP Address**: 192.168.1.100
- Capstone VM
  - **Operating System**: Linux
  - **Purpose**: The vulnerable target VM that students can use to test alerts. Filebeat and Metricbeat will forward logs to the ELK machine.
  - **IP Address**: 192.168.1.105
- Target 1
  - **Operating System**: Linux
  - **Purpose**: Exposes a vulnerable WordPress server. Sends logs to ELK
  - **IP Address**: 192.168.1.110
- Target 2
  - **Operating System**: Linux
  - **Purpose**: A more difficult WordPress target. Should be ignored unless all other portions of the project are completed. Sends logs to ELK.
  - **IP Address**: 192.168.1.115
- Kali
  - **Operating System**: Linux
  - **Purpose**: A standard Kali install that will be used to attack other machines.

- **IP Address**: 192.168.1.90

Description of Targets

The target of this attack was: Target 1 (192.168.1.110)

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

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

Excessive HTTP Errors

Alert 1 is implemented as follows:

- **Metric**: packetbeat
- **Threshold**: Above 400
- **Vulnerability Mitigated**: Alert can be used to detect enumeration of web pages and Denial of Services Attacks
- **Reliability**: Trigger is somewhat reliable. It is good when a large number of requests come in at once such as our wpscan. However, it can be triggered by small harmless events. The key here is to focus on the quantity.

HTTP Request Size Monitor

Alert 2 is implemented as follows:

- **Metric**: packetbeat
- **Threshold**: 3500
- **Vulnerability Mitigated**: Malicious code could be smuggled inside an http request, this alert will warn us for large HTTP requests.
- **Reliability**: A typical HTTP request is 700-800 bytes. This trigger warns us when the byte size of http requests exceeds 3500 in 1 minute. This does not seem like the most reliable monitor because this was an event that triggered a lot, even when we weren't attacking the VM.

CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: metricbeat
- **Threshold**: 0.5

- **Vulnerability Mitigated**: High CPU usage is a sign a system's resources are being exhausted. This can be caused by many things including malware or a DoS attack.
- **Reliability**: This alert is not the most reliable because it seems to have been triggered even when we weren't attacking the machine and we were doing normal functions.

Suggestions for Going Further (Optional)

- Each alert above pertains to a specific vulnerability/exploit. Recall that alerts only detect malicious behavior, but do not stop it. For each vulnerability/exploit identified by the alerts above, suggest a patch. E.g., implementing a blocklist is an effective tactic against brute-force attacks. It is not necessary to explain *how* to implement each patch.
    - How to prevent wpscans:
        - Remove Unwanted Headers
        - Disable Your WordPress RSS Feed
        - Disable WordPress Emoji's
        - Remove WordPress Meta Generator Tags
        - Modify Your NGINX Configuration To Block WPScan
    - How to prevent DoS attacks:
        - Monitor and analyze network traffic
        - Limit broadcasting
        - Protect endpoints
        - Dial in firewalls
    - How to prevent potentially malicious http requests
        - Deny all POST requests (if possible)
        - Deny POST requests using HTTP 1.0
        - Whitelist POST requests for certain resources
        - Control POST via referrer
    - How to prevent malare
        - Keep apps and OS up to date
        - Keep anti-virus and anti-malware signatures up to date
        - Don't click suspicious links or go to suspicious sites

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. 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:

- SSH port is open
    - **Patch**:
        - cd /etc/rc.d
        - Ls
        - rm -f rc.x -- where 'x' is the service name.
        - e.g) rm -f /etc/rc.d/rc.sshd

    - **Why It Works**: This way the ssh service is closed and no one can ssh into VM. If that is not feasible you can Allowlist certain IP addresses to ssh and deny all the rest.
- Port 445 Microsoft-ds is open
    - **Patch**: Make sure you have the latest version of Microsoft-DS SMB file sharing. Disable this port.
    - **Why It Works**: Having up to date apps and services is the best way to protect against known exploits. Disabling the port will prevent anyone from using it maliciously.
- Port 111 with rpcbind is open
    - **Patch**: Close port. Either block it with the firewall or disable it with
    - systemctl stop rpcbind
    - systemctl disable rpcbind
    - **Why It Works**: Disabling the port will ensure no one can use it maliciously.