Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:

Target 1
- Operating System: Linux 3.x|4.x
- Purpose:Target 1
- IP Address: 192.168.1.110

Target 2
- Operating System:Linux 3.x|4.x
- Purpose:Target
- IP Address:192.168.1.115

Including a Gliffy or draw.io diagram is optional but highly encouraged.

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**
  - ssh
  - http
  - rpc

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

Excessive HTTP Errors is implemented as follows:

- Metric: packetbeeat
- Threshold: 5
- Vulnerability Mitigated: Network scanning
- Reliability: low

Name of Alert 2

HTTP Request Size is implemented as follows:

- Metric: Packetbeat
- Threshold: 3500 bytes in 1 minute
- Vulnerability Mitigated: unknown network scanning
- Reliability: TODO: Does this alert generate lots of false positives/false negatives? Rate as low, medium, or high reliability.

Name of Alert 3

CPU Usage Monitoring is implemented as follows:

- Metric: metricbeat
- Threshold: 50% in the last 5 minutes
- Vulnerability Mitigated: TODO
- Reliability: high.

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

- Patch: Download wp plugin to prevent wpscan from enumerating users and place it in the correct directory

Vulnerability 2

- Patch: Replace the common-password file with a file that contains a proper password policy.
- Why It Works: The more complex a password is the harder it becomes for an actor trying to gain credentials they shouldn't have access to.

Vulnerability 3

- Patch: Adjust permissions on the wp-config.php file.
- Why It Works: Restricting access to the main config file keeps actors from easily viewing it's contents.