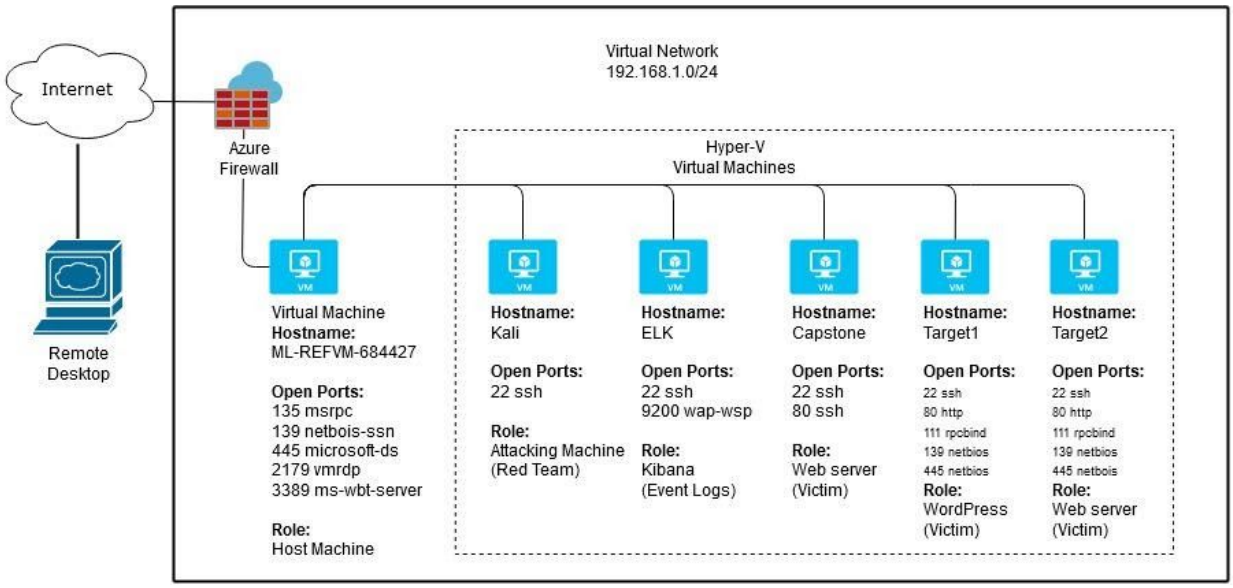
Blue Team: Summary of Operations

Table of Contents

Network Topology

The following machines were identified on the network:



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**
  - OpenSSH
  - Apache httpd 2.4.10
  - RPCbind
  - Samba port 139
  - Samba port 445

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-21 10:54 PST

Nmap scan report for 192.168.1.110
Host is up (0.00096s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.0017s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernl
```

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.)

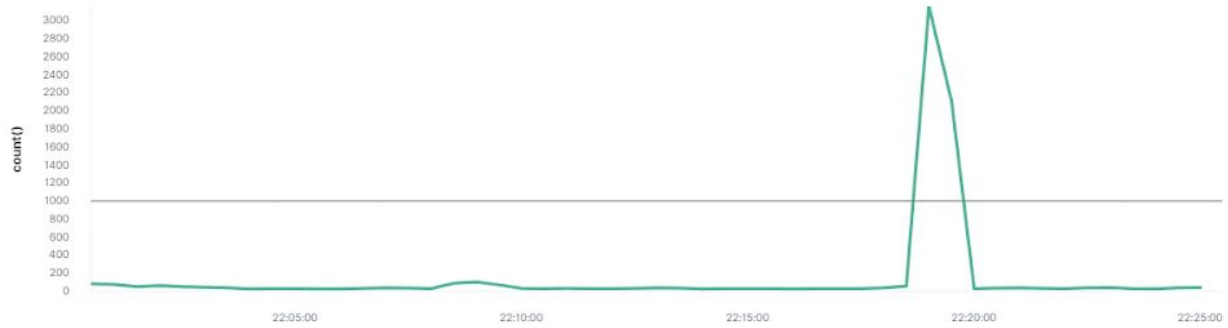
Excessive HTTP Errors

Excessive HTTP Errors is implemented as follows:

- Metric: This alert monitors for any HTTP Response Status Codes with an error code
- Threshold: 400 or more errors within 5 minutes
- Vulnerability Mitigated: This alert would identify possible brute-force attacks such as hydra
- Reliability: Screenshots show that it has fired during the attempted attack making the threshold set accurate.

Trigger time	State
2020-11-28T22:23:27+00:00	▷ Firing
2020-11-28T22:22:27+00:00	▷ Firing
2020-11-28T22:21:26+00:00	▷ Firing

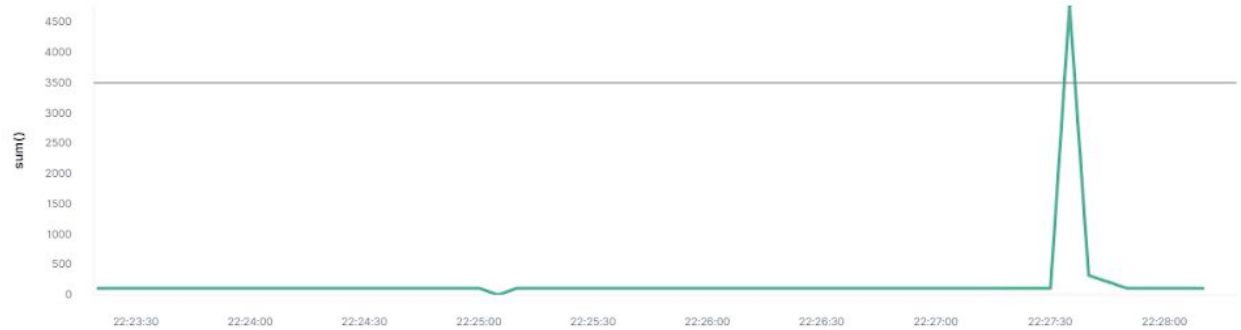
Trigger time	State
2020-11-28T22:20:26+00:00	▷ Firing
2020-11-28T22:19:27+00:00	▷ Firing



HTTP Request Size

HTTP Request Size is implemented as follows:

- Metric: This alert monitors for HTTP Request Bytes
- Threshold: HTTP request bytes exceeds 3500 in one minute
- Vulnerability Mitigated: This alert identifies a possible nmap scan. It sees the amount of GET or POST requests and if it goes over 3500 alerts.
- Reliability: Screenshot shows the setup is correct.

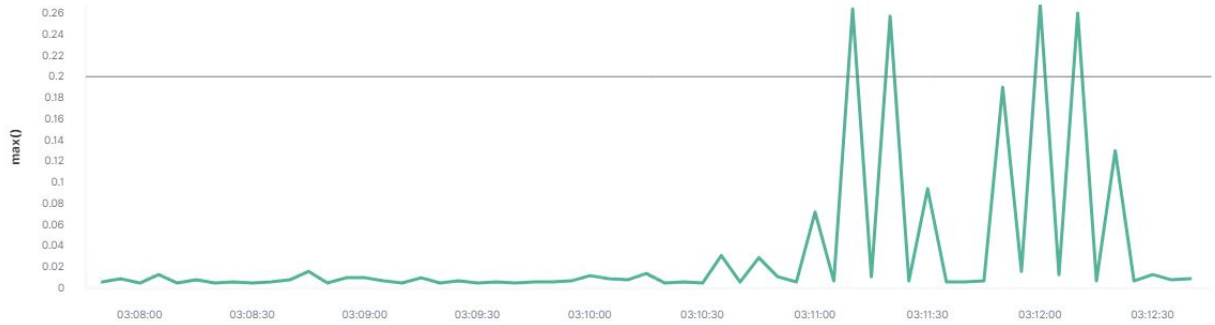


Trigger time	State
2020-11-28T22:28:27+00:00	▷ Firing

CPU Usage
CPU Usage is implemented as follows:

- Metric: Alerts on CPU usage
- Threshold: CPU usage is above 20% on a machine.
- Vulnerability Mitigated: CPU usage could be a result of possible malware or an attack on the machine. An example is a mult-threaded brute-force attack such as hydra.
- Reliability: The screenshot below shows four times where the alert triggered. We missed one alert slightly below the current threshold so to finetune things we should lower the threshold slightly.

2020-12-01T03:30:14+00:00	▷ Firing
2020-12-01T03:29:14+00:00	▷ Firing
2020-12-01T03:28:14+00:00	▷ Firing



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:

Weak Password Policy

- Patch: Implement a user password policy that restricts the number of failed login attempts
- Why It Works: Restricting failed login attempts with a lockout of the account after a set number of fails a brute-force attack will fail quickly.

HTTP Request Size

- Patch: A simple update to the .htaccess file will fix the enumeration of the wordpress site.
- Why It Works: Updating the .htaccess file would configure the apache web server to prevent directory indexing.

CPU Usage

- Patch: Implement end-point protection
- Why It Works: If the high CPU usage is being caused by malware on the target machine end-point protection can be implemented to quarantine the malware.