Web Vulnerability Scan Triage in Splunk Using Fortigate UTM Logs

Overview

In this lab, I investigated a spike in web server resource usage by focusing on Fortigate UTM firewall telemetry in Splunk. The goal was to confirm whether the activity was a vulnerability scan, identify the scanner, attribute the source, identify the internal target, and capture the earliest scan time on a specific date.

SOC handoff summary

Classification: Suspicious web vulnerability scanning activity
Severity: Medium
Confidence: High
Scanner identified: Acunetix
Source IP: 40.80.148.42
Source country: United States
Target domain: imreallynotbatman.com
Target internal IP: 192.168.250.70
Earliest scan time on 2016 08 10: 15:36:45

Environment and data sources

Platform: Splunk Search and Reporting
Data source: Fortigate UTM firewall logs
Dataset: index botsv1
Sourcetype: fortigate_utm
Primary filters: imreallynotbatman.com and vulnerability

Investigation workflow and evidence

1. Triage and scope
   I constrained the investigation to Fortigate UTM logs because they were most likely to contain scan classification, enrichment fields, and clear web targeting context.

Primary search used

```
index="botsv1" sourcetype="fortigate_utm" "imreallynotbatman.com" "vulnerability"
```

2. Confirm the scanner tool
   I validated the scanner by reviewing raw events and confirming the scanner signature and labeling in the firewall telemetry.
   Finding: Acunetix

3. Attribute the scanning source
   I summarized events by source IP to identify the dominant origin of the scan traffic.
   Finding: 40.80.148.42

4. Identify the internal target
   I summarized events by destination IP to identify the internal asset being scanned.
   Finding: 192.168.250.70

5. Validate enrichment for source geography
   I used Fortigate enrichment fields and summarized by source country to confirm the geolocation reported in the logs.
   Finding: United States

6. Establish the earliest scan activity on the required date
   I filtered to 2016 08 10, sorted ascending by time, and pulled the earliest event to capture the first scan timestamp for that day.
   Finding: 15:36:45

Outcome and determination

The evidence confirms automated vulnerability scanning against imreallynotbatman.com, with a single dominant source IP and a consistent internal destination host. The activity is consistent with reconnaissance and should be treated as suspicious until validated against server side logs for any successful exploitation indicators.

Recommended response actions, production safe guidance

Immediate actions

• Block or rate limit 40.80.148.42 at the perimeter where appropriate
• Confirm whether the web server showed any successful exploitation indicators during the same window, using web server logs and endpoint telemetry

Hardening actions

• Review exposure and patch posture for the targeted web stack
• Add WAF rules or hardening controls to reduce scan effectiveness and alert fatigue

Detection improvements

• Create an alert for repeated vulnerability categorized requests targeting the same internal web asset
• Track first seen timestamps per source IP and target IP to quickly identify new scanners

Skills demonstrated

SIEM triage in Splunk with focused scoping
Firewall log analysis using Fortigate UTM telemetry and enrichment fields

Attribution and targeting analysis using statistical pivots

Timeline extraction and defensible reporting tied directly to log evidence