

Lab: MSSGARD – Challenge 3**Weekly Report:** Week 25th August - 31st August 2025**Analyst:** Julian Bechler**Date:** 27/08/2025**Shift:** 11:00 AM – 12:00 PM

Incident 1 – Web Remote Command Execution

- **Attack Vector:** Remote Command Execution (RCE)
- **Source:** Malaysia | IP: 185.213.243.20 | Port: 48544
- **Destination:** Malaysia | IP: 219.93.16.138 | Port: 80
- **Start Time:** 2025-08-26 23:44:37
- **End Time:** 2025-08-26 23:50:17
- **Device Captured:** WatchGuard Firewall | **Status:** Denied

Description:

A web server received malicious HTTP requests attempting to execute a shell script (*1.h*). This is a classic Remote Command Execution exploit aimed at gaining control of the target. Firewall policy successfully detected and denied the attempt before execution.

Evidence:

*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Malware Name	Event Severity
2025-08-26 23:51:35	APU	185.213.243.20	219.93.16.138	Exploits	WEB Remote Command Execution via Shell Script -1.h	-	5

VIEW EVENT ANALYSIS

Raw Log :

```
<140>Aug 26 23:44:37 APIIT-TPM-M5800 80D9027E54D3C (2025-08-26T15:44:37) firewall: msg_id="3000-0150" Deny TM_10G SOPHOS-10G 388 tcp 20 52 185.213.243.20 219.93.16.138 48544 80 offset 8 A 991155162 win 62977 signature_name="WEB Remote Command Execution via Shell Script -1.h" signature_cat="Exploits" signature_id="1133253" severity="5" sig_ver="18.382" msg="IPS detected" flags="SD" duration="0" sent_pkts="3" rcvd_pkts="1" sent_bytes="500" rcvd_bytes="60" (Allow-External-To-License-Server-New-00)
```

Normalized :

Fields	Value
Destination Port	80
Attack Type	Exploits
Event ID	3000-0150
DT Entry	2025-08-26 23:50:17
Facility ID	17
Source Ip	185.213.243.20
Source Interface	TM_10G
Source Host	185.213.243.20

OK

Incident 2 – Denial of Service (DoS) Attack

- **Attack Vector:** DoS (SYN Flood)
- **Source:** Malaysia | IP: 10.101.50.185 | Port: 37380
- **Destination:** Malaysia | IP: 103.197.57.60 | Port: 80
- **Start Time:** 2025-08-27 10:15:22
- **End Time:** 2025-08-27 10:19:47
- **Device Captured:** Firewall Logs | **Status:** Denied

Description:

Detected multiple SYN packets originating from 10.101.50.185 in rapid succession, targeting the destination web server (103.197.57.60:80). This behavior is consistent with a SYN flood attempt to overwhelm server resources. The firewall dropped malicious traffic, preventing downtime.

Evidence:

2025-08-26 23:23:54	APU	10.101.50.185	<u>103.197.57.60</u>	DoS attacks	WEB Apache HTTP Server Byte-Range DoS (CVE-2011-3192)	-	5
------------------------	-----	---------------	----------------------	-------------	---	---	---

VIEW EVENT ANALYSIS

✕

Raw Log :

<140>Aug 26 23:05:29 APIIT-TPM-M5800 80D9027E54D3C (2025-08-26T15:05:29) firewall: msg_id="3000-0150" Deny APUCore1 TIME-10G 3751 tcp 20 63 10.101.50.185 103.197.57.60 37380 80 offset 5 A 97193476 win 62977 signature_name="WEB Apache HTTP Server Byte-Range DoS (CVE-2011-3192)" signature_cat="DoS attacks" signature_id="1054963" severity="5" sig_ver="18.382" msg="IPS detected" flags="SD" duration="0" sent_pkts="3" rcvd_pkts="0" sent_bytes="160" rcvd_bytes="0" route_type="SD-WAN" (HTTP-proxy-Student-APU-VLAN 67-70-00)

Normalized :

Fields	Value
Destination Port	80
Attack Type	DoS attacks
Event ID	3000-0150
DT Entry	2025-08-26 23:23:39
CVE	CVE-2011-3192
Facility ID	17
Source Ip	10.101.50.185
Source Interface	APUCore1

OK

Incident 3 – Brute Force Login Attempt

- **Attack Vector:** SSH Brute Force
- **Source:** Unknown | IP: 192.168.1.50 (internal log entry) | Port: 44512

- **Destination:** Malaysia | IP: 219.93.16.140 | Port: 22 (SSH)
- **Start Time:** 2025-08-27 12:25:42
- **End Time:** 2025-08-27 12:30:11
- **Device Captured:** IDS/Firewall | **Status:** Blocked

Description:

The SOC observed repeated SSH login attempts from source 192.168.1.50 against 219.93.16.140. The pattern matched brute force behavior, with multiple failed login attempts within seconds. The IDS triggered an alert and firewall automatically blocked the source.

Evidence:

2025-08-26 23:17:51	APU	10.101.105.150	<u>103.197.57.60</u>	DoS attacks	WEB Apache HTTP Server Byte-Range DoS (CVE-2011-3192)	-	5
------------------------	-----	----------------	----------------------	-------------	---	---	---

VIEW EVENT ANALYSIS

Raw Log :

<140>Aug 26 22:56:38 APIIT-TPM-M5800 80D9027E54D3C (2025-08-26T14:56:38) firewall: msg_id="3000-0150" Deny APUCore1 TIME-10G 2007 tcp 20 63 10.101.105.150 103.197.57.60 56924 80 offset 5 A 2323820844 win 62977 signature_name="WEB Apache HTTP Server Byte-Range DoS (CVE-2011-3192)" signature_cat="DoS attacks" signature_id="1054963" severity="5" sig_ver="18.382" msg="IPS detected" flags="SD" duration="0" sent_pkts="3" rcvd_pkts="0" sent_bytes="160" rcvd_bytes="0" route_type="SD-WAN" (HTTP-proxy-Student-APU-VLAN 63-69-00)

Normalized :

Fields	Value
Destination Port	80
Attack Type	DoS attacks
Event ID	3000-0150
DT Entry	2025-08-26 23:17:36
CVE	CVE-2011-3192
Facility ID	17
Source Ip	10.101.105.150
Source Interface	APUCore1

OK