FIRST Incident Response Fusion Course Lab Background Handout

Backing Information: Security Data Received

1. Low-level logs from Web servers exposed to the internet are automatically delivered to you. Your filtering mechanisms detected several suspicious HTTP requests. They did not match any specific attack signature but they were detected as anomalies and automatically reported to your security event collection system.

```
Information level: Low-Level

Source: Web server logs from servers exposed to the internet

Note: The filtering mechanisms detected several suspicious
requests. No specific attack signature was matched but they were
detected as anomalies and automatically reported to our security
event collection system.

HTTP Header:
```

```
POST
/%65%6d%62%65%64%2d%62%69%6e/%70%68%70?%2d%64+%61%6c%6c%6f%77%5f%
75%72%6c%5f%69%6e%63%6c%75%64%65%3d%6f%6e+%2d%64+%73%61%66%65%5f%
6d%6f%64%65%3d%6f%66%66+%2d%64+%73%75%68%6f%73%69%6e%2e%73%69%6d%
75%6c%61%74%69%6f%6e%3d%6f%6e+%2d%64+%64%69%73%61%62%6c%65%5f%66%
75%6e%63%74%69%6f%6e%73%3d%22%22+%2d%64+%6f%70%65%6e%5f%62%61%73%
65%64%69%72%3d%6e%6f%6e%65+%2d%64+%61%75%74%6f%5f%70%72%65%70%65%
6e%64%5f%66%69%6c%65%3d%70%68%70%3a%2f%2f%69%6e%70%75%74+%2d%64+%
63%67%69%2e%66%6f%72%63%65%5f%72%65%64%69%72%65%63%74%3d%30+%2d%6
4+%63%67%69%2e%72%65%64%69%72%65%63%74%5f%73%74%61%74%75%73%5f%65
%6e%76%3d%30+%2d%64+%61%75%74%6f%5f%70%72%65%70%65%6e%64%5f%66%69
%6cC%65%3d%70%68%70%3a%2f%2f%69%6e%70%75%74+%2d%6e HTTP/1.1
Host: -h
Content-Type: application/x-www-form-urlencoded
Content-Length: 396
```

2. You receive an automatic system alert indicating a possible DoS attack against your company firewall.

   This event was detected by one of your externally-facing network devices. It was transferred across your internal network by your Security Information and Event Management (SIEM) system and was presented to you. Note that your action might be to create a new rule to block the unwanted traffic, or contact your upstream provider, or escalate to Level 2. Think about your organization and reply based on that. It is totally acceptable that your answer differs from that of other students.

```
%FW-4-ALERT_ON: getting aggressive, count (83/500) current 1-min rate: 501
```

3. You work in a national CSIRT monitoring the feed delivering information about open addresses and ports, and the CSIRT receives an email from a third party with a sample of a new periodic detection indicator, Open DNS Resolver.

To: National CERT
From: Concerned Third Party
Subject: Reducing Open DNS Resolvers

Hi guys, great to talk to you on the phone last week. We have refined our collection mechanisms and output to best meet your needs. I have attached an example of the Open DNS Resolver output we are planning on delivering to you on a weekly basis.

All of our emails will have subject “Open DNS notification” and will contain exactly one attachment in the format presented here.

We look forward to a strong relationship moving forward,

Sincerely,
Third Party
(Attachment)

timestamp	ip	port	protocol	min_amplification	dns_version
2017-07-07	192.0.2.226	53	udp	1.381	no version
2017-07-07	192.0.2.242	53	udp	4.619	
2017-07-07	192.0.2.147	53	udp	4.619	Go away
2017-07-07	192.0.2.105	53	udp	1.381	
2017-07-07	192.0.2.158	53	udp	1.381	
2017-07-07	192.0.2.243	53	udp	3.8095	9.9.4-P1
2017-07-07	192.0.2.7	53	udp	1.381	dnsmasq-2.52
2017-07-07	192.0.2.231	53	udp	1.381	dnsmasq-2.57

4. Your weekly US-CERT bulletin announces a new vulnerability in Firefox.

```
Information level: Advisory
Source: National CERT bulletin
Text of Advisory:
```

Mozilla releases Security Updated
Published December 14, 2016

Mozilla has released security updates to address multiple vulnerabilities in Firefox and Firefox ESR. Exploitation of some of these vulnerabilities may allow a remote attacker to take control of an affected system.

Available updates include:

-- Firefox 50.1
-- Firefox ESR 45.6

Users and administrators are encouraged to review the Mozilla Security Advisories for Firefox and Firefox ESR and apply the necessary updates

5. You spot an advisory about a Foo-5 CMS attack by searching an independent research blog.

```
Information level: Advisory
Source: Independent Researcher Blog
Text of Advisory:
```

A new attack on Foo-5 CMS was discovered, which affects versions 4.0.0 to 4.2.7 that used a default installation bundle. Exploits an old, unpatched PHP interpreter that is bundled in the default installation package. Vendor was notified and the new installation package was released today.

Details of the attack:
- Only a single POST request is needed to successfully compromise a machine running a vulnerable Foo-5 installation.
- The query part of the request URL disables PHP security measures (including Suhosin extension)
- Observed attacks deliver unobfuscated PHP shellcode directly in the body of the HTTP request

Unfortunately, it will take at least several weeks until majority of sites that used the vulnerable package are updated, so more details are not released at this time.