Wykrywanie ataków sieciowych - lab 3

Zadanie 1

Udało się zidentyfikować wersje HTTP `1.1` i `2`.
Zrzut został zapisany w pliku `zad1.pcapng`

Zadanie 2

Plik: `snort3-server-webapp.rules`
Wiersz: `3256`

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22006 ( msg:"SERVER-WEBAPP Ulterius
web server directory traversal attempt"; flow:to_server,established;
content:"GET /c|3A|/",fast_pattern,nocase; metadata:policy max-detect-ips
drop,policy security-ips drop; service:http; reference:cve,2017-16806;
reference:url,github.com/rapid7/metasploit-framework/blob/
b533ec60190dcc4cf14ac18867b4b782b702b1ad/modules/auxiliary/admin/http/
ulterius_file_download.rb; classtype:web-application-attack; sid:45722;
rev:2; )
```

Plik: `snort3-server-webapp.rules`
Wiersz: `3674`

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-WEBAPP
WordPress Responsive Thumbnail Slider arbitrary PHP file upload attempt";
flow:to_server,established; http_uri; content:"/wp-admin/
admin.php",fast_pattern,nocase;
content:"page=responsive_thumbnail_slider_image_management"; http_client_body;
content:"<?"; metadata:policy max-detect-ips drop,policy security-ips drop;
service:http; reference:url,github.com/rapid7/metasploit-framework/blob/master/
modules/exploits/multi/http/wp_responsive_thumbnail_slider_upload.rb;
classtype:attempted-admin; sid:47832; rev:1; )
```

Zadanie 3

Aby przekonać IPS, że połączenie się zakończyło, można wykorzystać *TCP reset attack*. Polega on na wysłaniu sfałszowanego segmentu resetującego TCP, który wywołuje przerwanie połączenia TCP. Ze względu na czas, jaki atakujący potrzebuje, aby wykonać atak, jest on efektywny jedynie w konfugiracjach sieci, które wspierają długo żyjące połączenia.

Zadanie 4

```
preprocessor frag3_engine: policy Windows bind_to [3.3.3.3, 3.3.3.33]
```