Wykrywanie ataków sieciowych - lab 2

Zadanie 2

0089c86c601156d1e45bfbf400ae407efe559b67fd4a3ff413c09693 snortrules-snapshot-31210.tar.gz

Zadanie 3

Heartbleed

Plik: `snort3-server-other.rules`
Wiersz `998`

```
alert tcp $HOME_NET [21,25,443,465,636,992,993,995,2484] -> $EXTERNAL_NET any ( msg:"SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt"; flow:to_client,established,only_stream; content:"|18 03 00|",depth 3; byte_test:2,>,128,0,relative; content:"|02|",within 1,distance 2; metadata:policy balanced-ips drop,policy max-detect-ips drop,policy security-ips drop,ruleset community; service:ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30514; rev:11; )
```

Ostatnia reguła dodana do zestawu

Plik: `rules/snort3-malware-cnc.rules`
Wiersz: `5610`

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS ( msg:"MALWARE-CNC Win.Malware.Emotet cnc outbound connection attempt"; flow:to_server,established; http_cookie; content:"2inagDNzrlIOFmq7KST9DidO3LVnSmvD",fast_pattern,nocase; metadata:impact_flag red,policy max-detect-ips drop; service:http; reference:url,isc.sans.edu/forums/diary/Emotet+Returns/28044/; classtype:trojan-activity; sid:300059; rev:1; )
```

Zadanie 4

Plik: `rules/snort3-server-apache.rules`

Wiersz: `181`

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-APACHE
Apache HTTP server SSRF attempt"; flow:to_server,established; http_uri;
content:"?"; content:"unix:",distance 0,fast_pattern,nocase; content:"|
7C|",distance 0,nocase; content:"|3A 2F|",within 10; metadata:policy balanced-
ips drop,policy max-detect-ips drop,policy security-ips drop; service:http;
reference:cve,2021-40438; classtype:attempted-user; sid:58820; rev:1; )
```

Zasada wykrywa podatność server-side request forgery, występująca w serwerach HTTP Apache w wersji 2.4.48 i wcześniejszych. Podatność polega na mod_proxy, pozwalając na zdalne, nieautoryzowane wymuszenie na serwerze HTTP do przekierowania zapytań do dowolnych serwerów, ostatecznie umożliwiając pozyskanie lub podmienianie zasoów, które normalnie byłyby dla atakującego niedostępne

Zadanie 5

Plik: `rules/snort3-server-iis.rules`
Wiersz: `214`

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"SERVER-IIS
Microsoft Active Directory Federation Services wct parameter cross site
scripting attempt"; flow:to_server,established; http_uri; content:"/adfs/
ls/",fast_pattern,nocase; content:"wct=",nocase; pcre:"/[?&]wct=[^&]*?
([\x22\x27\x3c\x3e\x28\x29]|script|onload|src)/i"; metadata:policy max-detect-
ips drop; service:http; reference:cve,2015-1757;
reference:url,technet.microsoft.com/en-us/security/bulletin/ms15-062;
classtype:attempted-user; sid:34769; rev:3; )
```

Zasada wykrywa podatność cross-site scripting w adfs/ls w Active Directory Federation Services w systemie Microsoft Windows Server 2008 SP2, R2 SP1 i Server 2012. Pozwala zdalnemu atakującemu na wstrzyknięcie dowolnego skryptu lub kodu HTML przez parametr wtc.