Imię i nazwisko: Wojciech Sitek
Numer indeksu: 293148
Stanowisko: p139-k07
Zespół: Wojciech Sitek, Dawid Brzozowski

Sprawozdanie BSS Systemy IDS 2019

5.1.1.1

Uruchomiono program *tcpdump* bez filtrów poleceniem:
tcpdump –ln
Zaobserwowano ruch w ramach sieci lokalnej – różne protokoły oraz różne maszyny źródłowe i docelowe. Oto kilka reprezentatywnych rekordów:

```
10:52:30.584399 arp who-has 192.168.160.21 tell 192.168.160.232
10:52:30.671056 arp who-has 192.168.160.232 tell 192.168.160.21
10:52:31.943661 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.44:31:92:8a:d6:de.8007, length 47
10:52:33.943592 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.44:31:92:8a:d6:de.8007, length 47
10:52:34.681650 IP 192.168.160.239.17500 > 255.255.255.255.17500: UDP, length 158
10:52:34.685702 IP 192.168.160.239.17500 > 192.168.160.255.17500: UDP, length 158
10:52:35.943559 STP 802.1w, Rapid STP, Flags [Forward], bridge-id 8000.44:31:92:8a:d6:de.8007, length 47
```

Widoczne są między innymi protokoły arp, stp, ip, wifi. Główną funkcją procesów powodujących ten ruch jest podtrzymanie połączenia sieci i znajomości sąsiadów przez maszyny, a także od czasu do czasu przesłanie informacji niezbędnych dla programu.

5.1.1.2 Ruch z wybranego protokołu i z wybranych adresów

Ruch, gdzie hostem jest wybrany adres IP. Polecenie:
tcpdump –ln host 192.168.160.21

```
10:53:22.608155 arp who-has 192.168.160.21 tell 192.168.160.222
10:53:22.610789 arp who-has 192.168.160.222 tell 192.168.160.21
```

Ruch, gdzie filtrujemy ruch pakietów ARP:
Tcpdump –ln arp

```
10:49:30.657341 arp who-has p139-k07 tell galeon2.ii.pw.edu.pl
10:49:30.663531 arp reply p139-k07 is-at e0:d5:5e:8b:7a:d8 (oui Unknown)
10:49:31.143571 arp who-has galeon2.ii.pw.edu.pl tell p139-k07
10:49:31.143844 arp reply galeon2.ii.pw.edu.pl is-at 00:50:56:be:8f:fa (oui Unknown)
10:49:35.662678 arp who-has p139-k07 tell galeon
10:49:35.662703 arp reply p139-k07 is-at e0:d5:5e:8b:7a:d8 (oui Unknown)
10:49:35.751559 arp who-has galeon tell p139-k07
10:49:35.751855 arp reply galeon is-at 00:50:56:be:71:08 (oui Unknown)
```

5.1.1.3 Znaleźć parametry sieci

Adres serwera DNS. Polecenie: tcpdump –ln port domain

```
11:02:08.750631 IP 192.168.160.187.54296 > 192.168.160.10.53: 29859+ A? www.facebook.com. (34)
11:02:08.750989 IP 192.168.160.187.54296 > 192.168.160.10.53: 35400+ AAAA? www.facebook.com. (34)
11:02:08.753794 IP 192.168.160.10.53 > 192.168.160.187.54296: 29859 2/2/4 CNAME[|domain]
11:02:08.791451 IP 192.168.160.10.53 > 192.168.160.187.54296: 35400 2/2/4 CNAME[|domain]
```

Wniosek: na adresie 192.168.160.10 znajduje się serwer DNS.

Adresu kilku innych maszyn: tcpdump –ln net 192.168.0.0 mask 255.255.0.0
11:05:45.415914 IP 192.168.160.222.1900 > 239.255.255.250.1900: UDP, length 514
11:05:45.462798 IP 192.168.160.222.1900 > 239.255.255.250.1900: UDP, length 514
11:05:47.680680 arp who-has 192.168.160.21 tell 192.168.160.224
11:05:47.709274 arp who-has 192.168.160.224 tell 192.168.160.21
11:05:49.575560 arp who-has 192.168.160.18 tell 192.168.160.187
11:05:49.575882 arp reply 192.168.160.18 is-at 00:50:56:be:8f:fa

5.1.2.4

Przeskanowano maszynę o adresie podanym przez Prowadzącego: nmap 194.29.168.142
11:26:05.311749 IP p139-k07.45404 > pmr.ii.pw.edu.pl.echo: S 3990591625:3990591625(0) win 4096 <mss 1460>
11:26:05.311930 IP p139-k07.45404 > pmr.ii.pw.edu.pl.572: S 3990591625:3990591625(0) win 4096 <mss 1460>
11:26:05.311946 IP p139-k07.45404 > pmr.ii.pw.edu.pl.2108: S 3990591625:3990591625(0) win 2048 <mss 1460>
11:26:05.311962 IP p139-k07.45404 > pmr.ii.pw.edu.pl.5101: S 3990591625:3990591625(0) win 2048 <mss 1460>
11:26:05.311971 IP p139-k07.45404 > pmr.ii.pw.edu.pl.335: S 3990591625:3990591625(0) win 3072 <mss 1460>
11:26:05.311979 IP p139-k07.45404 > pmr.ii.pw.edu.pl.966: S 3990591625:3990591625(0) win 2048 <mss 1460>
11:26:05.311989 IP p139-k07.45404 > pmr.ii.pw.edu.pl.839: S 3990591625:3990591625(0) win 4096 <mss 1460>
11:26:05.409412 IP p139-k07.45405 > pmr.ii.pw.edu.pl.943: S 3990526088:3990526088(0) win 4096 <mss 1460>
11:26:05.409437 IP p139-k07.45405 > pmr.ii.pw.edu.pl.1475: S 3990526088:3990526088(0) win 4096 <mss 1460>
11:26:05.409459 IP p139-k07.45405 > pmr.ii.pw.edu.pl.5192: S 3990526088:3990526088(0) win 4096 <mss 1460>
11:26:05.409469 IP p139-k07.45405 > pmr.ii.pw.edu.pl.7634: S 3990526088:3990526088(0) win 2048 <mss 1460>
11:26:05.409478 IP p139-k07.45405 > pmr.ii.pw.edu.pl.185: S 3990526088:3990526088(0) win 2048 <mss 1460>
11:26:05.409487 IP p139-k07.45405 > pmr.ii.pw.edu.pl.383: S 3990526088:3990526088(0) win 4096 <mss 1460>
11:26:05.409504 IP p139-k07.45405 > pmr.ii.pw.edu.pl.247: S 3990526088:3990526088(0) win 1024 <mss 1460>
11:26:05.409530 IP p139-k07.45405 > pmr.ii.pw.edu.pl.678: S 3990526088:3990526088(0) win 4096 <mss 1460>
11:26:05.409541 IP p139-k07.45405 > pmr.ii.pw.edu.pl.193: S 3990526088:3990526088(0) win 4096 <mss 1460>
11:26:05.409557 IP p139-k07.45405 > pmr.ii.pw.edu.pl.1680: S 3990526088:3990526088(0) win 1024 <mss 1460>
11:26:05.409567 IP p139-k07.45405 > pmr.ii.pw.edu.pl.20005: S 3990526088:3990526088(0) win 3072 <mss 1460>

Zostały w ten sposób uzyskane informacje o otwartych portach na maszynie pmr.ii.pw.edu.pl. Nmap przeprowadził skan wielu dostępnych portów, czego skrót został przedstawiony powyżej (osiągnięty za pomocą polecenia *tcpdump src host p139-k07 and dst host 192.29.168.142*). Ślad tcpdump pozostawił pakiety wysłane na kolejne porty sprawdzanej maszyny.

Fingerprinting

Aby zbadać system operacyjny maszyny, wykonano polecenie *nmap –O 194.29.168.142*. Oto wyniki otrzymane przez program tcpdump:
11:23:19.172579 IP p139-k07.51686 > pmr.ii.pw.edu.pl.auth: . ack 1 win 32768 <wscale 10,nop,mss 265,timestamp 4294967295 0,sackOK>
11:23:19.197697 IP p139-k07.51687 > pmr.ii.pw.edu.pl.auth: FP 516593833:516593833(0) win 65535 urg 0 <wscale 15,nop,mss 265,timestamp 4294967295 0,sackOK>
11:23:20.322328 IP p139-k07.51668 > pmr.ii.pw.edu.pl.ssh: S 3100130277:3100130277(0) win 1 <wscale 10,nop,mss 1460,timestamp 4294967295 0,sackOK>
11:23:20.323057 IP pmr.ii.pw.edu.pl.ssh > p139-k07.51668: S 4218557155:4218557155(0) ack 3100130278 win 28960 <mss 1460,sackOK,timestamp 309893841 4294967295,nop,wscale 7>
11:23:20.323092 IP p139-k07.51668 > pmr.ii.pw.edu.pl.ssh: R 3100130278:3100130278(0) win 0
11:23:20.422441 IP p139-k07.51669 > pmr.ii.pw.edu.pl.ssh: S 3100130278:3100130278(0) win 63 <mss 1400,wscale 0,sackOK,timestamp 4294967295 0,eol>
11:23:20.423086 IP pmr.ii.pw.edu.pl.ssh > p139-k07.51669: S 2054562952:2054562952(0) ack 3100130279 win 28960 <mss 1460,sackOK,timestamp 309893851 4294967295,nop,wscale 7>
11:23:20.423121 IP p139-k07.51669 > pmr.ii.pw.edu.pl.ssh: R 3100130279:3100130279(0) win 0
11:23:20.522554 IP p139-k07.51670 > pmr.ii.pw.edu.pl.ssh: S 3100130279:3100130279(0) win 4 <timestamp 4294967295 0,nop,nop,wscale 5,nop,mss 640>

11:23:20.523215 IP pmr.ii.pw.edu.pl.ssh > p139-k07.51670: S 1346426123:1346426123(0) ack 3100130280 win 28960 <mss 1460,nop,nop,timestamp 309893861 4294967295,nop,wscale 7>
11:23:20.523249 IP p139-k07.51670 > pmr.ii.pw.edu.pl.ssh: R 3100130280:3100130280(0) win 0
11:23:20.622665 IP p139-k07.51671 > pmr.ii.pw.edu.pl.ssh: S 3100130280:3100130280(0) win 4 <sackOK,timestamp 4294967295 0,wscale 10,eol>
11:23:20.623389 IP pmr.ii.pw.edu.pl.ssh > p139-k07.51671: S 3358579445:3358579445(0) ack 3100130281 win 28960 <mss 1460,sackOK,timestamp 309893871 4294967295,nop,wscale 7>
11:23:20.623423 IP p139-k07.51671 > pmr.ii.pw.edu.pl.ssh: R 3100130281:3100130281(0) win 0
11:23:20.722777 IP p139-k07.51672 > pmr.ii.pw.edu.pl.ssh: S 3100130281:3100130281(0) win 16 <mss 536,sackOK,timestamp 4294967295 0,wscale 10,eol>
11:23:20.723476 IP pmr.ii.pw.edu.pl.ssh > p139-k07.51672: S 1280746650:1280746650(0) ack 3100130282 win 28960 <mss 1460,sackOK,timestamp 309893881 4294967295,nop,wscale 7>
11:23:20.723510 IP p139-k07.51672 > pmr.ii.pw.edu.pl.ssh: R 3100130282:3100130282(0) win 0

W wynikach programu nmap znajduje się krótki opis prawdopodobnego systemu operacyjnego, wersji jądra systemu itp. na danej maszynie. Znajduje się on poniżej. Fingerprinting odbywał się przez wysyłanie specjalnie spreparowanych niestandardowych pakietów na różne porty maszyny i oczekiwanie na odpowiedzi – które są różne zależnie od systemu – i na tej podstawie wysnucie wniosków przez program nmap.

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
113/tcp closed auth
443/tcp open https
Aggressive OS guesses: Linux 2.6.15 - 2.6.20 (87%), HP Brocade 4100 switch; or Actiontec MI-424-WR, Linksys WRVS4400N, or Netgear WNR834B wireless broadband router (86%), HP Brocade 4Gb SAN switch (86%), Linksys WRT300N wireless broadband router (86%), FreeBSD 6.2-RELEASE (86%), Linksys WAP54G WAP (86%), Broadband router (Actiontec GT701-WG or GT724-WG; BeWAN 770G ADSL2+; D-Link 500T; Linksys WAG54G v2, WAG354G, or RTP300; Netgear DG834G, or WELL PTI-850G), or Canon imageRUNNER C2620 printer (85%), Linux 2.4.20 (85%), HP 4200 PSA (Print Server Appliance) model J4117A (85%), Linux 2.6.20 (Ubuntu 7.04 server, x86) (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime: 35.869 days (since Wed Apr 10 14:34:22 2019)

Snort

Uruchomiono program snort ze wszystkimi dostępnymi regułami. Nie wykonano skanowania programem ping z powodu przeoczenia. Oto wyniki typowych logów:

NOTIFY * HTTP/1.1
Host:239.255.255.250:1900
NT:urn:schemas-upnp-org:device:MediaServer:1
NTS:ssdp:alive
Location:http://192.168.160.223:2869/upnphost/udhisapi.dll?content=uuid:cf43c114-d5d8-4998-b3d3-2802306f2cc3
USN:uuid:cf43c114-d5d8-4998-b3d3-2802306f2cc3::urn:schemas-upnp-org:device:MediaServer:1
Cache-Control:max-age=900
Server:Microsoft-Windows/6.3 UPnP/1.0 UPnP-Device-Host/1.0
OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS:f8301e5caee09cd02572164cbf219ad0

Priority Count: 5
Connection Count: 10

IP Count: 1
Scanner IP Range: 192.168.160.187:192.168.160.187
Port/Proto Count: 10
Port/Proto Range: 21:1723

Własna reguła „NEGATYTWNE”

Zaprojektowano własną regułę i umieszczono w pliku local.rules. Oto jej treść:
alert tcp 194.29.168.142 80 -> any any (msg:"Wykryto napis negatywny";content:"NEGATYWNY";nocase;sid:9996;rev:1;)

Po uruchomieniu programu snort i otwarciu strony tak.html, w której znajdował się oznaczony napis, w alertach pojawił się log systemowy, informujący o wykryciu niechcianego napisu „NEGATYWNY”. Oto jego treść:

[**] [1:9996:1] Wykryto napis negatywny [**]
[Priority: 0]
05/16-12:13:30.003797 194.29.168.142:80 -> 192.168.160.187:44886
TCP TTL:63 TOS:0x0 ID:64180 IpLen:20 DgmLen:375 DF
AP Seq: 0xC7EFC8CA Ack: 0x33351814 Win: 0xE3 TcpLen: 32
TCP Options (3) => NOP NOP TS: 310194809 2315411097