



IPv6検証報告書

2011年6月8日
ISOG-J WG2

本報告書の取り扱いについて

- 責任

- 本文書の情報は、限られた検証環境における結果に基づくものであり、全ての環境で同一の結果を保証するものではありません。

- 転載および引用について

- 日本セキュリティオペレーション事業者協議会 (Information Security Operation providers Group Japan、略称: ISOG-J) が公開している各種資料は、公序良俗に反する目的・内容でない限り、以下の条件にて自由にご利用いただくことができます。但し、著作権はISOG-Jに帰属します。
- 掲載箇所に出典を明記すること (ISOG-J および当該資料名)。
- 報告書内の集計データを独自に再編して新たなグラフを作成するなど、報告書内の情報を加工して使用する場合は「引用」ではなく「参考」と表記すること。
- 引用先が、出典を記載する事ができないもの場合は、口頭にて出典を明らかにすること。
- リンクによる引用の場合は、資料データファイルに対する直接のリンクではなく、当該ページへのリンクとすること。

目次

1. 前提および目的
2. 実施日程
3. 検証環境
4. ネットワーク構成
5. 検証内容
6. IPv6環境での攻撃状況
7. 各社コメント
8. 課題
9. 今後の取り組み
10. 参加企業、参加者
11. 参考URL

1. 前提および目的

IPv4アドレス枯渇を目前に控え、IPv6を利用した生活が目前に迫っている。しかし、現在では一部の組織や製品のみがIPv6に対応している状況であり、本格的な対応は不十分な状態である。特にセキュリティ製品およびセキュリティサービスにおいてはIPv6の対応準備が不十分である。ユーザ企業においてIPv6の導入が進むことが想定される現在において、我々セキュリティオペレーションに関係する事業者もIPv6に対応しなければならない。このような現状を踏まえ、今回参加企業がIPv6のテスト環境に各自セキュリティ機器やネットワーク機器を持ち寄り、製品の検証を行った。この検証において得られた知見を本報告書にまとめる。

2. 実施日程

検証期間：2011年2月15日～2011年2月25日

3. 検証環境

- JNSA ラボネット
 - 主催: JNSA U40部会 ラボネットWG
<http://www.jnsa.org/active/2010/u40.html>
- テストベッド
 - 主催: IPv6普及・高度化推進協議会 ビジネステストベッドWG
<http://www.v6pc.jp/jp/entry/wg/2010/05/v4exh-testbed.phtml>

設置機器

| ベンダー名 | 製品名 | ソフトウェアバージョン | 種別 | 設置場所 |
|------------------|----------------------------------|----------------------|----------|------------|
| BlueCoat | BlueCoatSG | SG5.5 | Proxy | テストベッド |
| CheckPoint | UTM-1 270 | R70.1 | Firewall | |
| IBM | IBM Security Network IPS GX4004 | 4.3 | IPS | |
| Cisco | IPS 4255 | 7.0(4)E4 | | |
| | ASA 5540 | ASA 8.24 , ASDM 6.41 | | |
| McAfee | Network Security Platform I-2700 | 4.1.5.117 | | |
| Juniper Networks | SSG | | | |
| Microsoft | Windows 7 | | OS | JNSA ラボネット |
| | Windows Server 2003 | | | |
| | Windows Server 2008 | | | |
| - | CentOS 5.5 | | | |

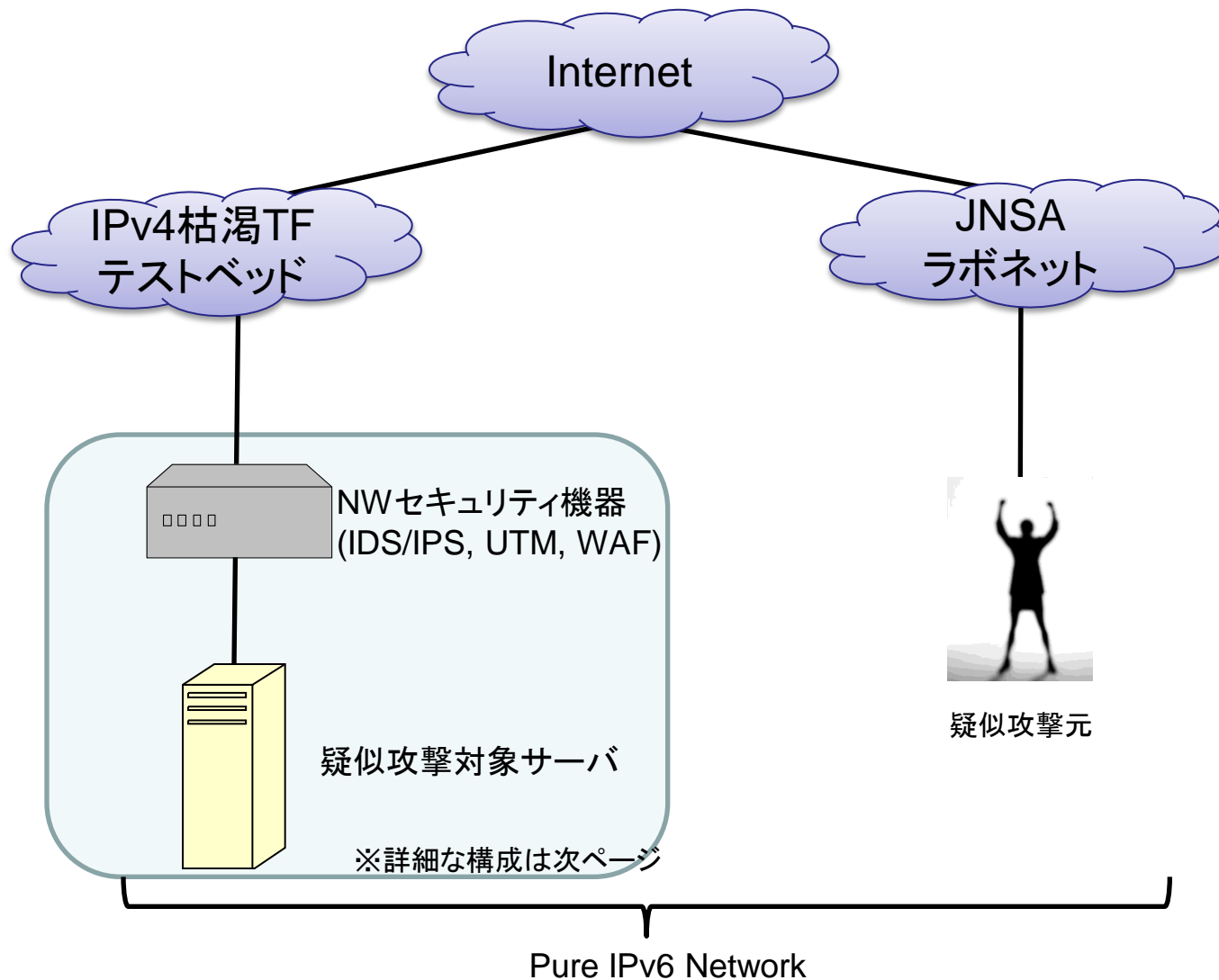
実験でを使用したソフトウェア一覧

| ソフトウェア名 | 参照URL |
|--------------|---|
| Ping / Ping6 | Windows、Unix標準ツール |
| Nmap | http://nmap.org/ |
| Nessus | http://www.nessus.org/nessus/intro.php |
| Netcat (※) | http://www.sphinx-soft.com/tools/index.html |
| Netsparker | http://www.mavitunasecurity.com/ |
| THC-IPV6 | http://www.thc.org/thc-ipv6/ |

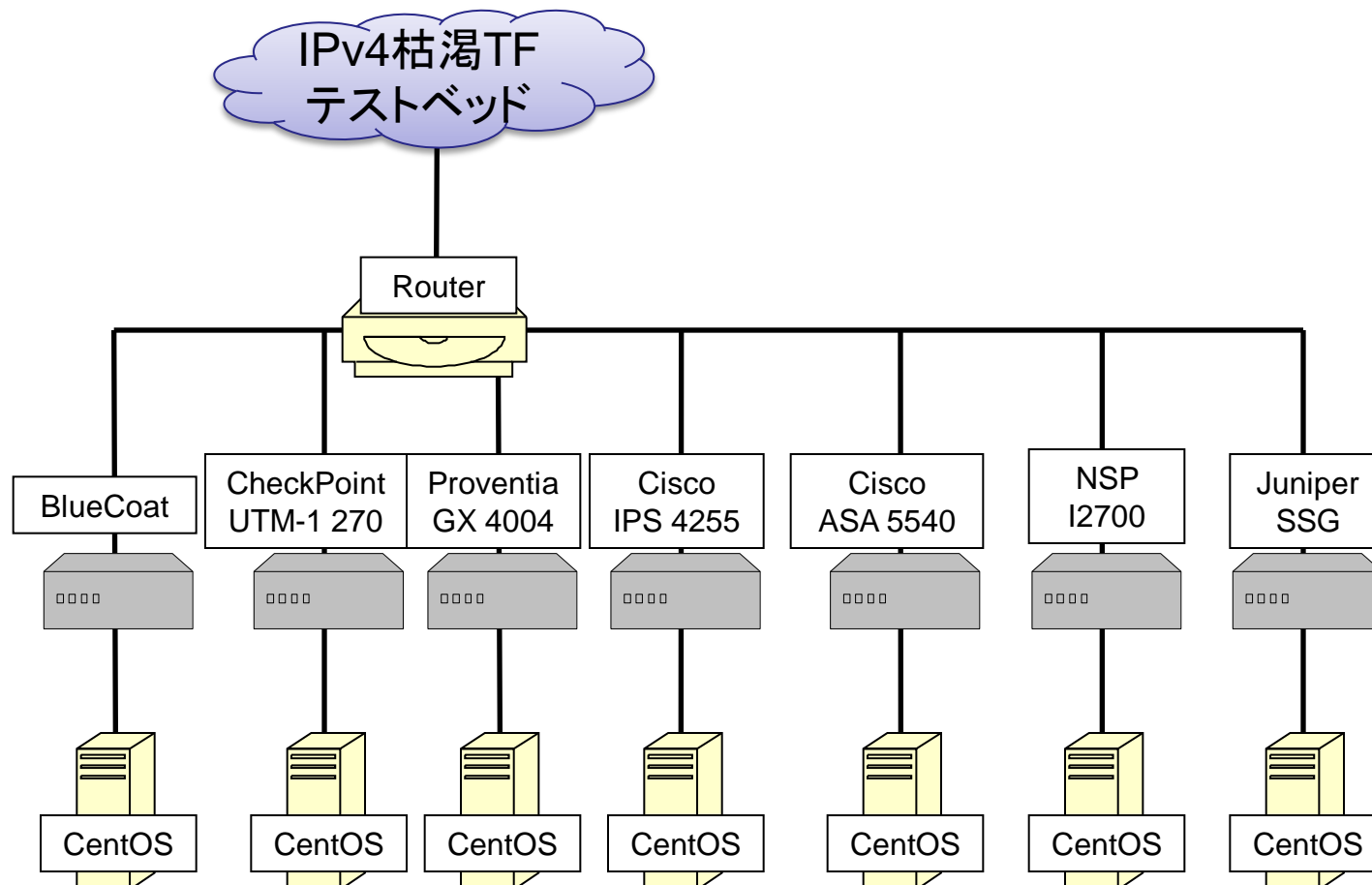
※ Netcatは以下もIpv6で使用可

<http://www.deepspace6.net/projects/netcat6.html>

4. 検証ネットワーク構成(全体概要図)



検証ネットワーク構成図 (IPv4枯渇TF側概要図)



5. 検証内容

- IPv6環境におけるネットワークオペレーションの検証
 - 検証環境
 - 検証項目
- CheckPoint UTM-1
 - ログの出力形式
- IBM Security Network IPS
 - thc-ipv6 によるスキャンを実施
- Cisco ASA
 - システム情報
 - 検証項目
- Cisco IPS
 - システム情報
 - 検証の結果気づいたこと
- McAfee NSP
 - システム情報
 - 検証項目

実施検証内容(IPv6ネットワーク検証): 検証環境

■ システム情報

- Attacker :

CentOS (xxx.yyy.zzz.185 / 2001:DB8::1:103)

Windows XP (2001:DB8::1:155)

- Victim :

CentOS (xxx.yyy.zzz.214 / 2001:DB8::214)

実施検証内容(IPv6ネットワーク検証): IPv6アドレスの設定

■ AttackerにIPアドレスを設定する

• Windows XP(設定コマンド)

```
C:¥Documents and Settings¥nds> ipv6 install  
C:¥Documents and Settings¥nds> netsh interface ipv6 set address "ローカル エリア接  
続" 2001:DB8::1:155
```

• Cent OS(設定後)

```
[root@cent5 ~]# ifconfig  
eth0    Link encap:Ethernet HWaddr 00:0C:29:22:51:50  
        inet addr:172.16.0.104 Bcast:172.16.0.255 Mask:255.255.255.0  
        inet6 addr: 2001:DB8::1:104/64 Scope:Global  
        inet6 addr: fe80::20c:29ff:fe22:5150/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
        RX packets:3439450 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:3720004 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:3057553688 (2.8 GiB) TX bytes:3096710499 (2.8 GiB)  
        Interrupt:177 Base address:0x1400
```

実施検証内容(IPv6ネットワーク検証): pingの実行

■ Attacker (Windows XP)からVictimに対してping、ping6を送信する

・ ping

```
C:¥Program Files¥Nmap>ping 2001:DB8::213

Pinging 2001:DB8::213 with 32 bytes of data:

Reply from 2001:DB8::213: time=16ms
Reply from 2001:DB8::213: time=16ms
Reply from 2001:DB8::213: time=16ms
Reply from 2001:DB8::213: time=19ms

Ping statistics for 2001:DB8::213:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 19ms, Average = 16ms
```

・ ping6

```
C:¥Program Files¥Nmap>ping6 2001:DB8::213

Pinging 2001:DB8::213
from 2001:DB8::1:155 with 32 bytes of data:

Reply from 2001:DB8::213: bytes=32 time=16ms
Reply from 2001:DB8::213: bytes=32 time=16ms
Reply from 2001:DB8::213: bytes=32 time=15ms
Reply from 2001:DB8::213: bytes=32 time=16ms

Ping statistics for 2001:DB8::213:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 16ms, Average = 15ms
```

※ ping / ping6 コマンド両方通信可能だった。オペレーション時にコマンド間違いに注意

実施検証内容(IPv6ネットワーク検証):DNSの通信

- Windows Server 2008 からIPv6 Enableサイト(www.ij.ad.jp)および、IPv6 Disableサイト(iij.marsflag.com)に接続してDNSクエリの挙動を確認する

| No. | Time | Source | Destination | Protocol | Info |
|------|------------|-----------------|--------------|-----------------------|---|
| 1891 | 600.012406 | Cfisco_72:98:84 | | CDP/VTP/DTP/PagP/UDLD | CDP Device ID: JNSARBSW01 Port ID: GigabitEthernet0/4 |
| 1892 | 638.301319 | 172.16.0.105 | | DNS | Standard query A www.ij.ad.jp |
| 1893 | 638.303788 | | 172.16.0.105 | DNS | Standard query response A |
| 1894 | 638.315079 | 172.16.0.105 | | DNS | Standard query AAAA www.ij.ad.jp |
| 1895 | 638.327026 | | 172.16.0.105 | DNS | Standard query response AAAA 2001: |
| 1896 | 639.037719 | 172.16.0.20 | | BROWSE | Domain/Workgroup Announcement WORKGROUP, NT workstation, Domain Enur |
| 1897 | 639.846235 | 2001: | | TCP | 49260 > http [SYN] Seq=0 win=8192 Len=0 MSS=1440 WS=8 SACK_PERM=1 |
| 1898 | 639.854018 | 2001: | | TCP | http > 49260 [SYN, ACK] Seq=0 Ack=1 win=5760 Len=0 MSS=1304 SACK_PERM=1 |
| 1899 | 639.856908 | 2001: | | TCP | 49260 > http [ACK] Seq=1 Ack=1 win=66304 Len=0 |
| 1900 | 639.874578 | 2001: | | HTTP | GET / HTTP/1.1 |
| 1901 | 639.885687 | 2001: | | TCP | http > 49260 [ACK] Seq=1 Ack=747 win=725 |
| 1902 | 639.890400 | 2001: | | HTTP | HTTP/1.1 304 Not Modified |
| 1903 | 639.899350 | 172.16.0.105 | | DNS | Standard query A ij.marsflag.com |
| 1904 | 639.906156 | | 172.16.0.105 | DNS | Standard query response A |
| 1905 | 639.906944 | 172.16.0.105 | | DNS | Standard query AAAA ij.marsflag.com |
| 1906 | 639.911211 | 172.16.0.105 | | DNS | Standard query A metrics.ij.ad.jp |
| 1907 | 639.916756 | 172.16.0.105 | | DNS | Standard query A tracer02.a-cast.jp |
| 1908 | 639.920350 | | 172.16.0.105 | DNS | Standard query response |
| 1909 | 639.921596 | 172.16.0.105 | | TCP | 49261 > http [SYN] Seq=0 win=8192 Len=0 MSS=1440 WS=8 SACK_PERM=1 |
| 1910 | 639.922032 | 172.16.0.105 | | TCP | 49262 > http [SYN] Seq=0 win=8192 Len=0 MSS=1440 WS=8 SACK_PERM=1 |
| 1911 | 639.922396 | 172.16.0.105 | | TCP | 49263 > http [SYN] Seq=0 win=8192 Len=0 MSS=1440 WS=8 SACK_PERM=1 |
| 1912 | 639.922717 | 172.16.0.105 | | TCP | 49264 > http [SYN] Seq=0 win=8192 Len=0 MSS=1440 WS=8 SACK_PERM=1 |
| 1913 | 639.923019 | 172.16.0.105 | | TCP | 49265 > http [SYN] Seq=0 win=8192 Len=0 MSS=1440 WS=8 SACK_PERM=1 |

IPv4の名前解決

IPv6の名前解決

IPv6でHTTP通信

ij.marsflag.comに
AAAAのQueryij.marsflag.comはIPv6
EnableではないのでIPv4で
HTTP通信

実施検証内容 (IPv6ネットワーク検証) : nmapの実行

- Attacker (CentOS) から Victim に対して IPv6 で nmap を実行する

```
[lac@cent5 ~]$ nmap -6 2001:DB8::213
```

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2011-02-15 17:09 JST
```

```
Interesting ports on 2001:DB8::213:
```

```
Not shown: 1676 closed ports
```

```
PORT      STATE  SERVICE
```

```
22/tcp    open   ssh
```

```
80/tcp    open   http
```

```
443/tcp   open   https
```

```
5060/tcp   filtered sip
```

```
Nmap finished: 1 IP address (1 host up) scanned in 12.775 seconds
```


実施検証内容(IPv6ネットワーク検証): netcatの実行

■ Attacker (Windows XP) から Victim に対して IPv6 で netcat を実行する

```
C:¥Documents and Settings¥nds¥デスクトップ¥IPv6関連ツール>nc6.exe 2001:DB8::213 80  
GET / HTTP/1.0
```

```
HTTP/1.1 403 Forbidden
```

```
Date: Tue, 15 Feb 2011 17:25:54 GMT
```

```
Server: Apache/2.2.3 (CentOS)
```

```
Accept-Ranges: bytes
```

```
Content-Length: 5043
```

```
Connection: close
```

```
Content-Type: text/html; charset=UTF-8
```

```
以下略
```

IPv6環境でのUTM-1動作状況

The screenshot shows the SmartView Tracker interface with a table of network logs. Two callout boxes are present:

- IPv4アドレス表示カラム**: Points to the 'Source' and 'Destination' columns.
- IPv6アドレス表示カラム**: Points to the 'IPv6 Source' and 'IPv6 Destination' columns.

| Source | Destination | IPv6 Source | IPv6 Destination | Proto | Rule | Source Port |
|------------------|------------------|------------------|------------------|-----------|------|-------------|
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | ipv6-icmp | 2 | |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | ipv6-icmp | 2 | |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | ipv6-icmp | 2 | |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 56198 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 56198 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 50728 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 50611 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 50710 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 50711 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 50711 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 35348 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 35349 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 35350 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 35351 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 35352 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 37440 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 37440 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 60159 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | http |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 51081 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 53606 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 38257 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 38258 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | http |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 55430 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 55430 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | http |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 47724 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 47724 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | 59880 |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | http |
| 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | 2001.███.███.███ | TCP | tcp | http |

UTM-1ログ(抜粋)

```
"Number" "Date" "Time" "Interface" "Origin" "Type" "Action" "Service" "Source Port" "Source" "Destination" "Protocol" "Rule" "Rule Name" "Current Rule Number" "User"
"Partner" "Community" "Information" "IPv6 Destination" "IPv6 Source" "Product"
"433" "16Feb2011" "14:44:04" "br0" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0; message_info:
Loopback address spoofing" "ff02::1:ff00:0" ":" "VPN-1 Power/UTM"
"460" "17Feb2011" "15:53:26" "Lan1" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ff1f:7c2b" ":" "VPN-1 Power/UTM"
"461" "17Feb2011" "15:53:26" "Lan1" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ff00:241" ":" "VPN-1 Power/UTM"
"17096" "18Feb2011" "14:09:53" "DMZ" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ffb:3bec" ":" "VPN-1 Power/UTM"
"17097" "18Feb2011" "14:09:56" "DMZ" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ff00:211" ":" "VPN-1 Power/UTM"
"17102" "18Feb2011" "14:11:28" "DMZ" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ffb:3bec" ":" "VPN-1 Power/UTM"
"17103" "18Feb2011" "14:11:32" "DMZ" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ff00:211" ":" "VPN-1 Power/UTM"
"17104" "18Feb2011" "14:11:35" "DMZ" "utm-1" "Log" "Accept" "" "" "" "" "ipv6-icmp" "2" "" "2-Standard" "" "" "" "inzone: External; outzone: DMZ; service_id: icmp-proto;
ICMP: Echo Request; ICMP Type: 128; ICMP Code: 0" "2001:DB8::2:a8" "2001:DB8::211" "VPN-1 Power/UTM"
"17108" "18Feb2011" "14:12:22" "External" "utm-1" "Log" "Accept" "" "" "" "" "ipv6-icmp" "2" "" "2-Standard" "" "" "" "inzone: DMZ; outzone: External; service_id: icmp-proto;
ICMP: Echo Request; ICMP Type: 128; ICMP Code: 0" "2001:DB8::211" "2001:DB8::2:a8" "VPN-1 Power/UTM"
"17112" "18Feb2011" "14:13:26" "External" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ff9d:15c6" ":" "VPN-1 Power/UTM"
"17113" "18Feb2011" "14:13:30" "External" "utm-1" "Alert" "Drop" "" "" "" "" "ipv6-icmp" "" "" "" "" "" "ICMP: Neighbor Solicitation; ICMP Type: 135; ICMP Code: 0;
message_info: Loopback address spoofing" "ff02::1:ff00:210" ":" "VPN-1 Power/UTM"
"17117" "18Feb2011" "14:14:16" "External" "utm-1" "Log" "Accept" "http" "59642" "" "" "tcp" "2" "" "2-Standard" "" "" "" "service_id: http" "2001:DB8::211" "2001:DB8::2:a8"
"VPN-1 Power/UTM"
"17139" "18Feb2011" "14:19:06" "External" "utm-1" "Log" "Accept" "" "" "" "" "ipv6-icmp" "2" "" "2-Standard" "" "" "" "inzone: DMZ; outzone: External; service_id: icmp-proto;
ICMP: Echo Request; ICMP Type: 128; ICMP Code: 0" "2001:DB8::211" "2001:DB8::2:a8" "VPN-1 Power/UTM"
"17142" "18Feb2011" "14:19:36" "External" "utm-1" "Log" "Accept" "http" "60749" "" "" "tcp" "2" "" "2-Standard" "" "" "" "service_id: http" "2001:DB8::211" "2001:DB8::2:a8"
"VPN-1 Power/UTM"
```

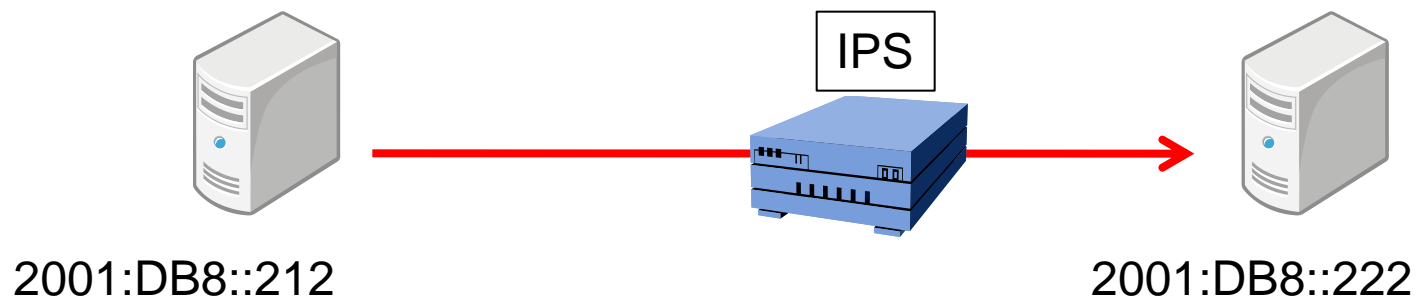
実施検証内容 (IBM Security Network IPS)

■ システム情報

- 設置機器: IBM Security Network IPS GX4004
- ソフトウェア: Firmware 4.3 / XPU 31.020
- 設定
 - Attack/Audit 全シグネチャ有効、Inline Simulationモード









■ Attacker、Victim

- Attacker : 2001:DB8::212
- Victim : 2001:DB8::222



実施検証内容 (IBM Security Network IPS) : ツールによる攻撃

■ thc-ipv6 によるスキャンを実施する

| IssueID | Event Name | Severity | Source IP | Target IP | Protocol | Protection Domain | VlanID | Status | Time |
|-------------------------|--|---|-----------------------------------|-----------------------------------|-------------------|------------------------|--------|---|----------------------|
| 2108002 | IPv6 Fragment Overlap |  | 2001:████████:212 | 2001:████████:222 | 0 | Global | |  | 25 Feb 2011 12:31:41 |
| 2110227 | IPv6 Invalid Hop by Hop Header |  | 2001:████████:212 | 2001:████████:222 | 0 | Global | |  | 25 Feb 2011 12:25:28 |
| 2108002 | IPv6 Fragment Overlap |  | 2001:████████:212 | 2001:████████:222 | 0 | Global | |  | 25 Feb 2011 12:25:51 |
| 2110227 | IPv6 Invalid Hop by Hop Header |  | 2001:████████:212 | 2001:████████:222 | 0 | Global | |  | 25 Feb 2011 12:25:28 |

IPv6異常パケットを検知

→シグネチャが存在する攻撃についてはIPv4の場合と比べて検知機能の差異は認められなかった

実施検証内容 (Cisco ASA)

■ システム情報

- 設置機器: CISCO ASA 5540
 - 設定
 - Firewall : ASA 8.24 , ASDM 6.41 , TransParent モード
 - IPS: 6. XX、プロミスキャスモード
- ※ インラインモードはNSの通信を遮断したため(当該ルールをはずすことは可能)

■ Attacker、Victim

- Attacker: CentOS(JNSA) xxx.yyy.zzz.185 / 2001:DB8::1:103
- Victim : CentOS xxx.yyy.zzz.214 / 2001:DB8::214

実施検証内容 (Cisco ASA)

■ テスト項目

- 検知テスト
 - スtringマッチのシグネチャ
 - しきい値ベースのシグネチャ
- IPv6に特化した試験項目
 - イベントの連続検知時の取りこぼし
 - アラートフィルタの適用
 - UDS (User Defined Signature) の作成
 - イベント検知時のリセットパケット送信

※ 未実施の項目

THCツールの実行、IPv6によるシグネチャアップデート、ルーティングテーブルの確認
RA,NAのパケット確認
グローバルコリレーション機能はIPv6未対応

実施検証内容 (Cisco ASA) : 検知テスト (ストリングマッチのシグネチャ)

■ Victim サーバに対して、http://[2001:DB8::214]/etc/passwd送信する

```
evIdsAlert: eventId=1041420469087331987 severity=medium vendor=Cisco
originator:
  hostId: sensor
  appName: sensorApp
  applInstanceId: 414
time: 2011/02/22 07:38:06 2011/02/22 07:38:06 UTC
signature: description=Unix Password File Access Attempt id=3201 created=20010202 type=other version=S238
  subsigId: 1
  sigDetails: [ ¥x26=?.] /etc/passwd[ ¥x26=?]
  marsCategory: Penetrate/RetrievePassword/System
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 0.0.0.0
    port: 54725
    ipv6Address: locality=OUT 2001:DB8::1:103
  target:
    addr: locality=OUT 0.0.0.0
    port: 80
    ipv6Address: locality=OUT 2001:DB8::214
    os: idSource=unknown relevance=relevant type=unknown
context:
fromAttacker:
000000 47 45 54 20 2F 65 74 63 2F 70 61 73 73 77 64 20 GET /etc/passwd
(以下略)
```

正常に検知

参考：Cisco ASA センサとマネージャーのIPv6の表記の違い

■ センサでのIPv6の表記方法

```

participants:
  attacker:
    addr: locality=OUT 0.0.0.0
    port: 54725
    ipv6Address: locality=OUT 2001:DB8::1:103
  target:
    addr: locality=OUT 0.0.0.0
    port: 80
    ipv6Address: locality=OUT 2001:DB8::214
    
```

検知ログのIPアドレスの表記は「センサからの確認」「マネージャからの確認」では異なるので注意が必要

■ センサでのIPv6の表記方法 (Cisco IPSのマネージャ画面)

| Sig. Name | Sig. ID | Attacker IP | Victim IP | Actions Taken | Victim Port |
|-----------------------------------|---------|----------------------|----------------------|---------------|-------------|
| Unix Password File Access Attempt | 3201/1 | 2001: [REDACTED] 200 | 2001: [REDACTED] 213 | | 80 |
| Unix Password File Access Attempt | 3201/1 | 2001: [REDACTED] 200 | 2001: [REDACTED] 213 | | 80 |
| Unix Password File Access Attempt | 3201/1 | 2001: [REDACTED] 200 | 2001: [REDACTED] 213 | | 80 |
| Unix Password File Access Attempt | 3201/1 | 2001: [REDACTED] 200 | 2001: [REDACTED] 213 | | 80 |
| Unix Password File Access Attempt | 3201/1 | 2001: [REDACTED] 200 | 2001: [REDACTED] 213 | | 80 |
| Unix Password File Access Attempt | 3201/3 | 2001: [REDACTED] 200 | 2001: [REDACTED] 213 | | 80 |

実施検証内容 (Cisco ASA) : 検知テスト (しきい値ベースのシグネチャ)

■ Victim サーバに対して、nmapを実行する

```
evlDsAlert: eventId=1041420469087389965 severity=low vendor=Cisco
originator:
  hostId: sensor
  appName: sensorApp
  applInstanceId: 414
time: 2011/02/24 11:19:36 2011/02/24 11:19:36 UTC
signature: description=TCP SYN Port Sweep id=3002 created=20010202 type=other version=S2
  subSigId: 0
  marsCategory: Probe/PortSweep/Non-stealth
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 0.0.0.0
    port: 49379
    ipv6Address: locality=OUT 2001:DB8::1:103
  target:
    addr: locality=OUT 0.0.0.0
    port: 80
    port: 256
    port: 554
    port: 22
    port: 25
    port: 21
    ipv6Address: locality=OUT 2001:DB8::214
  os: idSource=unknown relevance=relevant type=unknown
```

正常に検知

実施検証内容 (Cisco ASA) : IPv6に特化した試験項目

■ イベントの連続検知時の取りこぼし数の検証

Victim サーバに対して、`http://[2001:DB8::214]/etc/passwd`を200～5000回連続送信した時の検知件数の比較 (帯域無負荷)

検知結果:

/etc/passwd連続送信時の検知件数

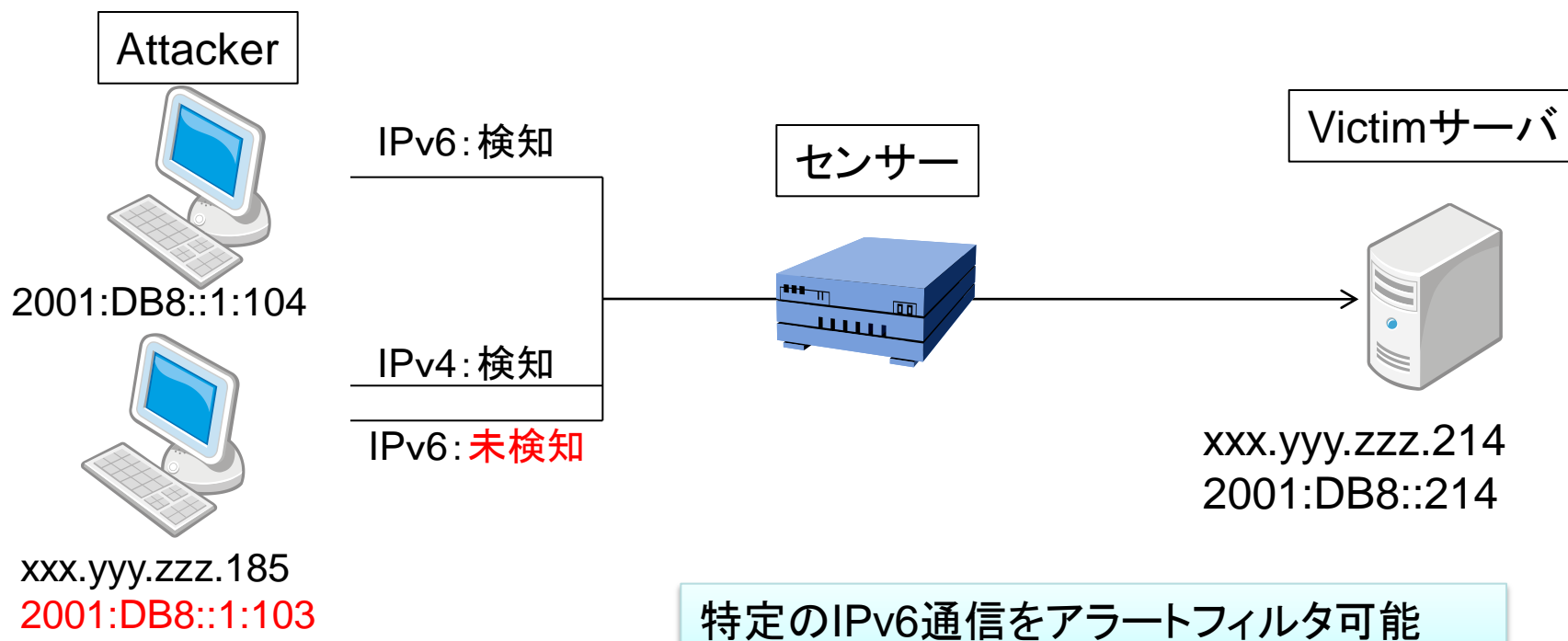
| プロトコル 送信回数 | 200回 | 1000回 | 5000回 |
|------------|------|-------|-------|
| IPv4 | 200 | 1000 | 5000 |
| IPv6 | 200 | 1000 | 5000 |

実施検証内容(Cisco ASA): IPv6に特化した試験項目

■ アラートフィルタの適用

JNSACentOS(2001:DB8::1:103)からのhttp://[2001:DB8::214]/etc/passwdを検知しないように設定

検知結果:



実施検証内容(Cisco ASA): IPv6に特化した試験項目

■ アラートフィルタ設定画面

Configuration > IPS > Policies > IPS Policies

| Name | Assigned Interfaces (or Pairs) | Signature Definition Policy | Event Action Override Policy | Anomaly Detection Policy |
|------|--|-----------------------------|---|--------------------------|
| vs0 | GigabitEthernet0/1.0 (Backplane Interface) | sig0 | rules0 (1 action overrides) HIGHRISK Deny Packet Inl... No | ad0 |

Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

| Name | Enabled | Sig ID | SubSig ID | Attacker (IPv4 / IPv6 / port) | Victim (IPv4 / IPv6 / port) | Risk Rating | Actions to Subtract |
|--------|---------|-----------|-----------|--|--|-------------|----------------------|
| Q00002 | No | 900-65535 | 0-255 | 0-65535 0.0.0.0-255.255.255.255 -0-FFFF.FFFF.FFFF.FFFF: 0-65535 | 0-65535 0.0.0.0-255.255.255.255 -0-FFFF.FFFF.FFFF.FFFF: 0-65535 | 0-100 | --None-- |
| Q00003 | Yes | 900-65535 | 0-255 | 0.0.0.0-255.255.255.255 -0-FFFF.FFFF.FFFF.FFFF: 0-65535 | 0.0.0.0-255.255.255.255 -0-FFFF.FFFF.FFFF.FFFF: 0-65535 | 0-100 | --None-- |
| Q00004 | Yes | 3201 | 0-255 | 0.0.0.0-255.255.255.255 [redacted] 103 0-65535 | 0.0.0.0-255.255.255.255 -0-FFFF.FFFF.FFFF.FFFF: 0-65535 | 0-100 | --None-- |
| Q00005 | Yes | 3201 | 0-255 | 0.0.0.0-255.255.255.255 [redacted] 104 0-65535 | 0.0.0.0-255.255.255.255 -0-FFFF.FFFF.FFFF.FFFF: 0-65535 | 0-100 | Reset Tcp Connection |

Apply Reset

11/02/24 6:09:27 UTC

実施検証内容 (Cisco ASA) : IPv6に特化した試験項目

■ UDSの作成:

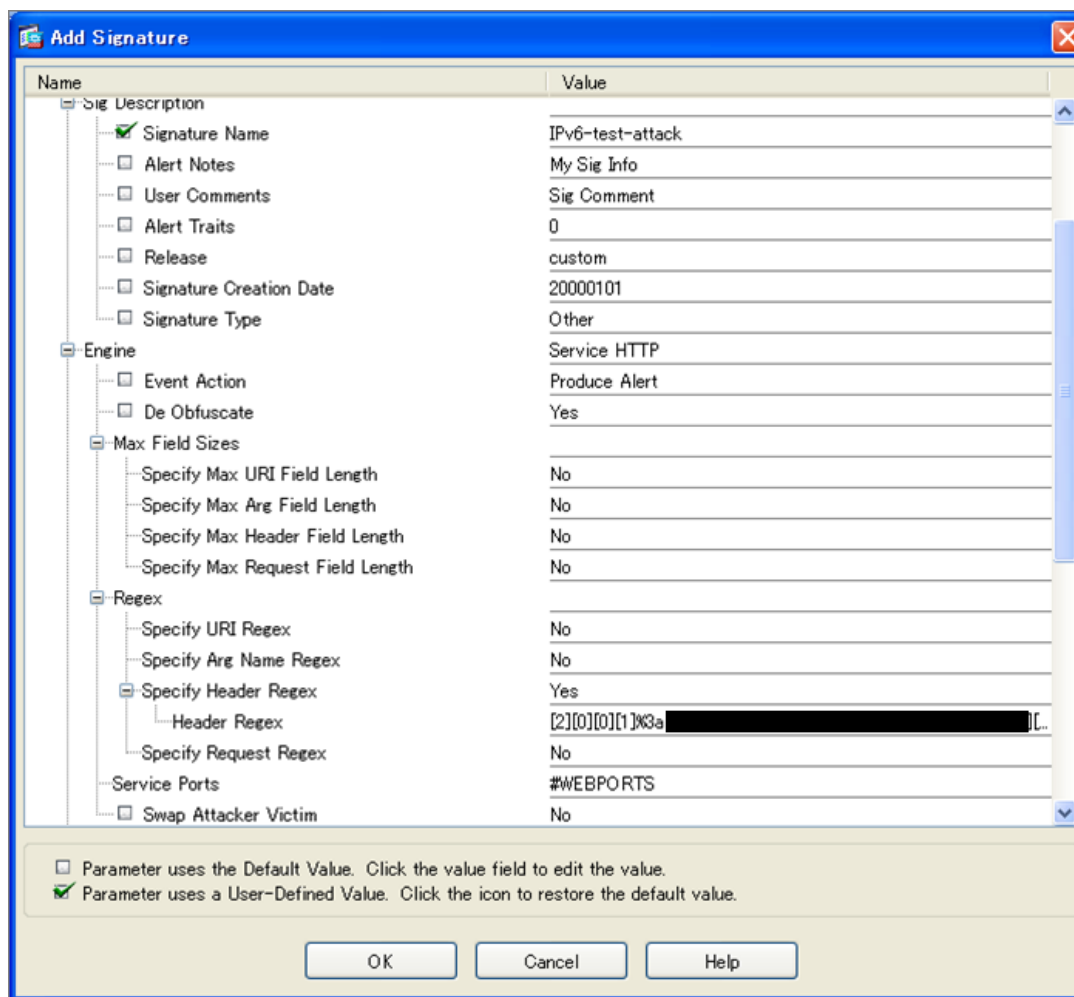
- ① host:2001:DB8::214を検知条件にしたシグネチャの作成
- ② DestIP:2001:DB8::214を検知条件にしたシグネチャの作成

検知結果: ①のみ検知

```
evlDsAlert: eventId=1041420469087390078 severity=medium vendor=Cisco
type=unknown
context:  originator:
  hostId: sensor
  appName: sensorApp
  applInstanceId: 414
time: 2011/02/24 13:43:02 2011/02/24 13:43:02 UTC
signature: description=IPv6-test-attack id=60000 created=20000101 type=other version=custom
  subsigId: 0
  sigDetails: detect attack packets via IPv6
  marsCategory: Info/Misc
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 0.0.0.0
    port: 34351
    ipv6Address: locality=OUT 2001:DB8::1:103
  target:
    addr: locality=OUT 0.0.0.0
    port: 80
    ipv6Address: locality=OUT 2001:DB8::214
os: idSource=unknown relevance=relevant
```

実施検証内容(Cisco ASA): IPv6に特化した試験項目

■ UDSの設定画面

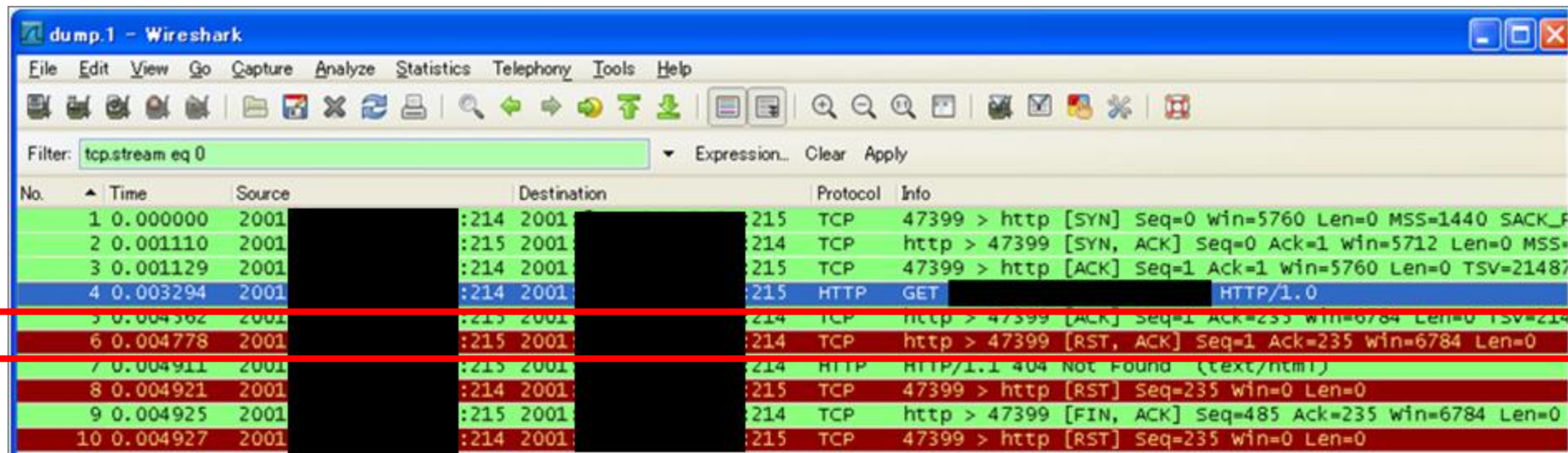


実施検証内容 (Cisco ASA) : IPv6に特化した試験項目

■ イベント検知時のリセットパケット送信:

特定シグネチャを検知した時に送信先にリセットパケットを送信し、セッションを終了させる

検知結果:



The image shows a Wireshark packet capture window titled 'dump.1 - Wireshark'. The filter is 'tcp.stream eq 0'. The packet list shows a sequence of events: a SYN packet (No. 1), a SYN-ACK packet (No. 2), an ACK packet (No. 3), an HTTP GET request (No. 4), a TCP ACK packet (No. 5), a TCP RST, ACK packet (No. 6), an HTTP 404 Not Found response (No. 7), a TCP RST packet (No. 8), a TCP FIN, ACK packet (No. 9), and a final TCP RST packet (No. 10). The RST packets (Nos. 6, 8, and 10) are highlighted in red, indicating the detection of a reset signal.

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|--------|-------------|----------|---|
| 1 | 0.000000 | 2001 | :214 2001 | TCP | 47399 > http [SYN] Seq=0 win=5760 Len=0 MSS=1440 SACK_F |
| 2 | 0.001110 | 2001 | :215 2001 | TCP | http > 47399 [SYN, ACK] Seq=0 Ack=1 win=5712 Len=0 MSS+ |
| 3 | 0.001129 | 2001 | :214 2001 | TCP | 47399 > http [ACK] Seq=1 Ack=1 win=5760 Len=0 TSV=21487 |
| 4 | 0.003294 | 2001 | :214 2001 | HTTP | GET HTTP/1.0 |
| 5 | 0.004362 | 2001 | :215 2001 | TCP | http > 47399 [ACK] Seq=1 Ack=235 win=6784 Len=0 TSV=214 |
| 6 | 0.004778 | 2001 | :215 2001 | TCP | http > 47399 [RST, ACK] Seq=1 Ack=235 win=6784 Len=0 |
| 7 | 0.004911 | 2001 | :215 2001 | HTTP | HTTP/1.1 404 Not Found (text/html) |
| 8 | 0.004921 | 2001 | :214 2001 | TCP | 47399 > http [RST] Seq=235 win=0 Len=0 |
| 9 | 0.004925 | 2001 | :215 2001 | TCP | http > 47399 [FIN, ACK] Seq=485 Ack=235 win=6784 Len=0 |
| 10 | 0.004927 | 2001 | :214 2001 | TCP | 47399 > http [RST] Seq=235 win=0 Len=0 |

IPv6アドレスにRSTパケット送信

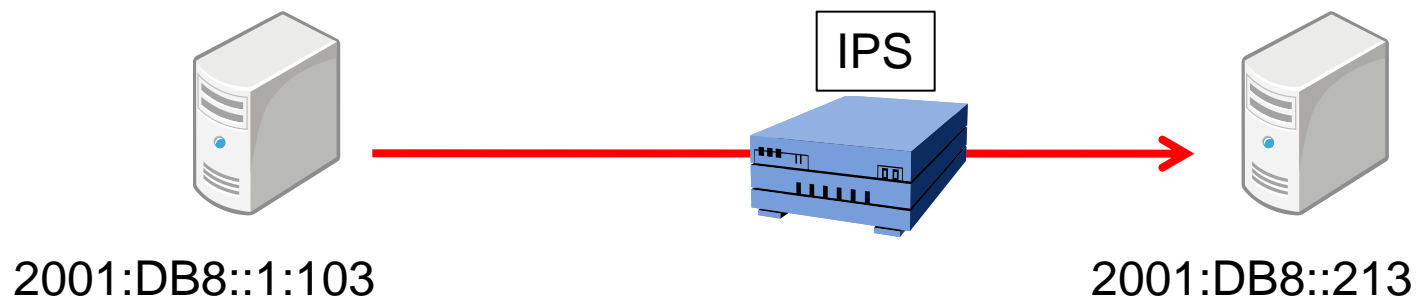
実施検証内容 (CiscoIPS)

■ システム情報

- 設置機器: CiscoIPS 4255
- ソフトウェア: Firmware 7.0(4)E4 / Signature S547～S549 (期間中自動アップデート)
- 設定
 - 有効シグネチャ: メーカーデフォルト + IPv6関連全て

■ Attacker、Victim

- Attacker : 2001:DB8::1:103
- Victim : 2001:DB8::213



CiscoIPS IPv6検知ログ

evlDsAlert: eventId=1297111995923644999 severity=informational vendor=Cisco

originator:

hostId: cisco-v7

appName: sensorApp

applInstanceId: 416

time: 2011/02/24 00:51:37 2011/02/24 09:51:37 JST

signature: description=Invalid IPv6 Header Traffic Class Field id=1706 created=20081031 type=other version=S365

subsigId: 0

sigDetails: Invalid IPv6 Header Traffic Class Field

marsCategory: Info/Misc

interfaceGroup: vs0

vlan: 0

participants:

attacker:

addr: locality=OUT **0.0.0.0**

ipv6Address: locality=OUT **fe80::xxx:222**

target:

addr: locality=OUT **0.0.0.0**

ipv6Address: locality=OUT **ff02::x:yyyy:214**

os: idSource=unknown relevance=relevant type=unknown

riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 25

threatRatingValue: 25

interface: ge0_0

protocol: IP protocol 58

IPv6特有のアラートに加え、「/etc/passwd」へのHTTPアクセス、nmapによるスキャンを検知できることを確認。

IPv6アドレスで検知されたアラートではIPv4の情報は0.0.0.0となる

IPv6アドレスが記録される
(IPv4で検知されたアラートには、
ipv6Address行はない)

CiscoIPS インターフェースによるIPv6表記の違い

- CiscoIPS本体に記録されるIPv6アドレス

participants:

attacker:

addr: locality=OUT 0.0.0.0

ipv6Address: locality=OUT **fe80::xxx:222**

target:

addr: locality=OUT 0.0.0.0

ipv6Address: locality=OUT **ff02::x:yyyy:217**

連続する「0」が省略された形式で記録される

- マネージャ(IME)上で表示されるIPv6アドレス

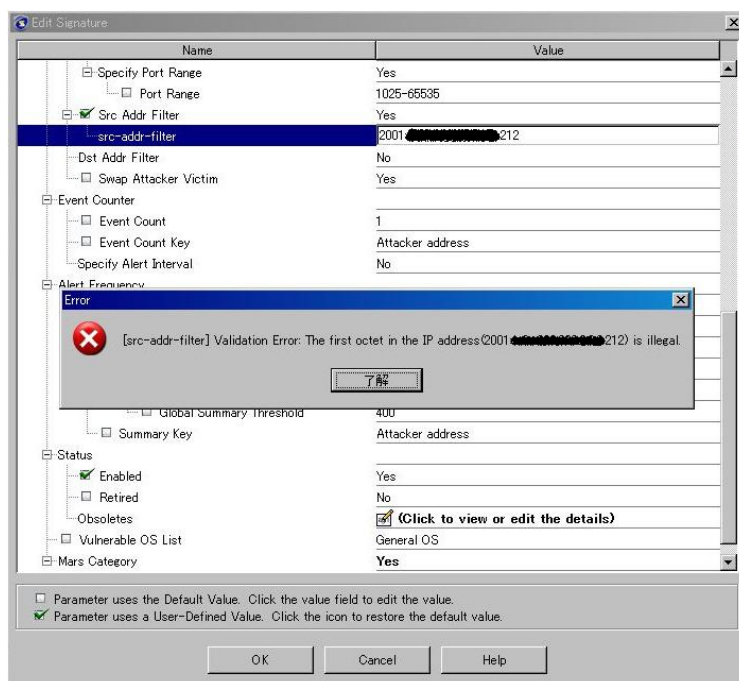
連続する「0」が省略されずに表示される

| Sig. Name | Sig. ID | Attacker IP | Victim IP |
|---|---------|-----------------------|-----------------------|
| ICMPv6 Neighbor Solicitation | 1621/0 | fe80: [redacted] :222 | ff02: [redacted] :217 |
| Invalid IPv6 Header Traffic Class Field | 1706/0 | fe80: [redacted] :222 | ff02: [redacted] :217 |
| ICMPv6 Neighbor Solicitation | 1621/0 | fe80: [redacted] :222 | ff02: [redacted] :217 |
| Invalid IPv6 Header Traffic Class Field | 1706/0 | fe80: [redacted] :222 | 0:0:0:0:0:0:0 |
| ICMPv6 Neighbor Solicitation | 1621/0 | fe80: [redacted] :222 | ff02: [redacted] :217 |

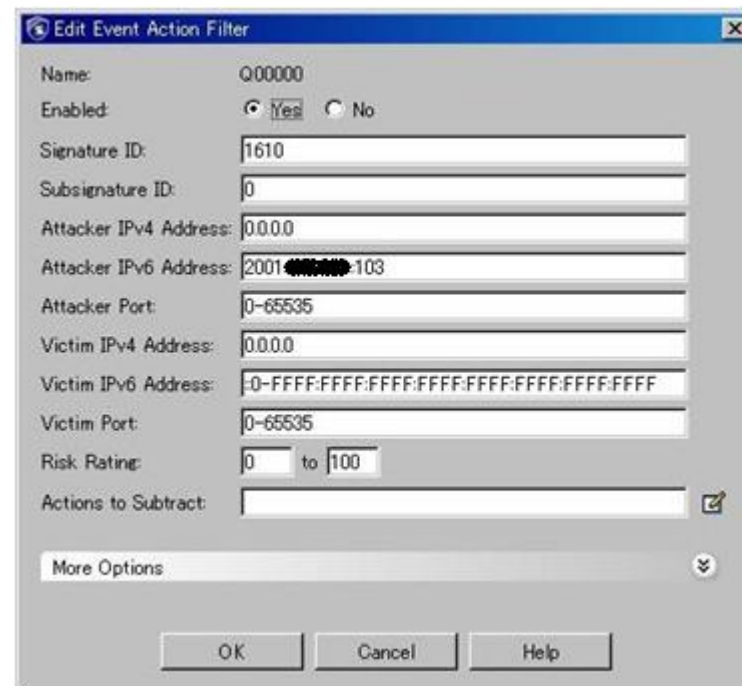
- Cisco ASAと同じ仕様と推察される。

CiscoIPSで気づいた点

- シグネチャカスタマイズでIPアドレスフィルタリング設定でIPv6アドレスを設定できない。
 - 代わりにフィルタルールでは、IPv6アドレスを設定可能。



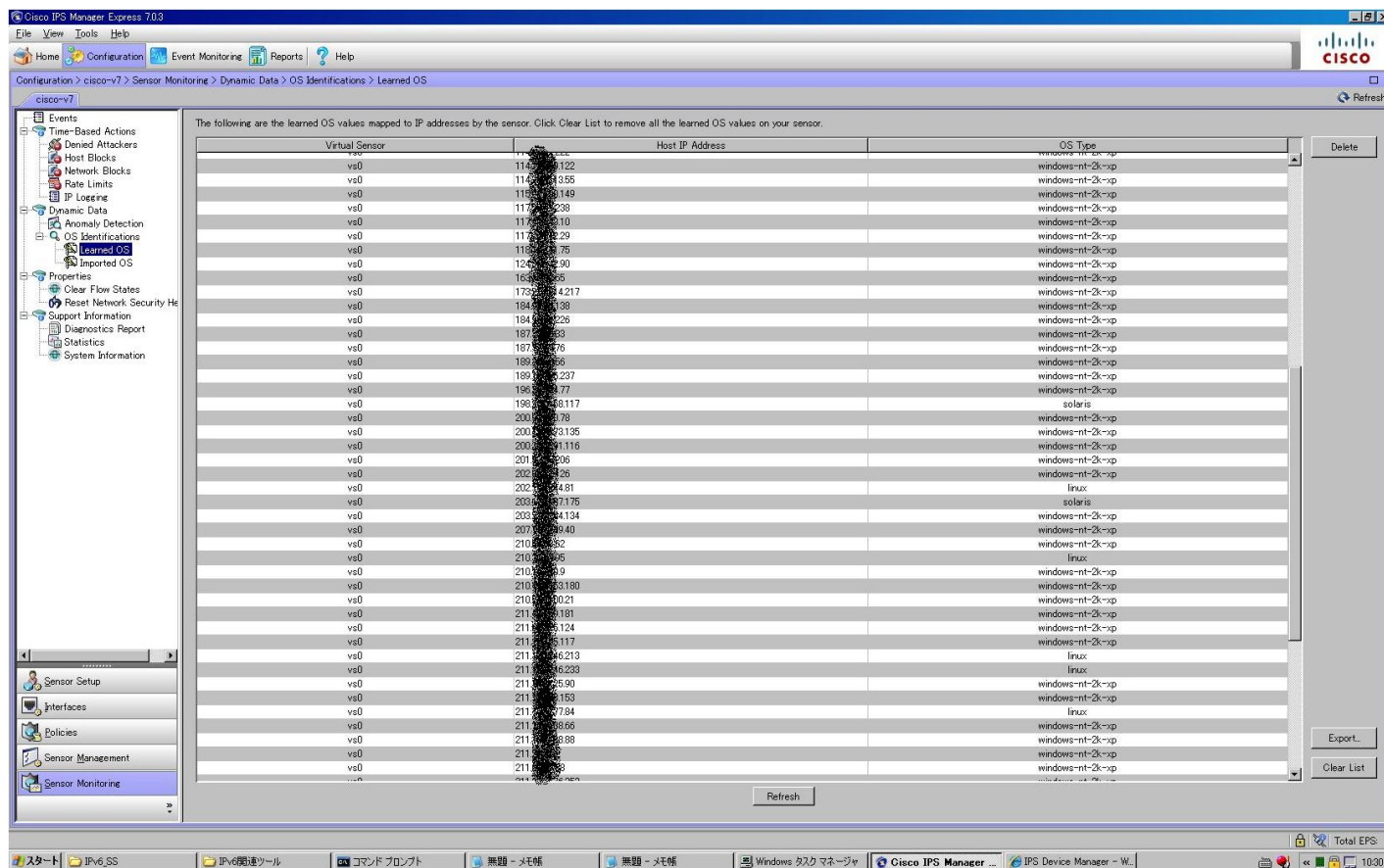
シグネチャカスタマイズでIPv6アドレスを設定できない。



フィルタルールでは、IPv6を設定可能。

CiscoIPSで気づいた点

- OS推測機能はIPv6では機能しない。



The screenshot displays the Cisco IPS Manager Express 7.0.3 interface. The main window shows the 'OS Identifications > Learned OS' page. A table lists the learned OS values mapped to IP addresses by the sensor. The table has three columns: Virtual Sensor, Host IP Address, and OS Type. The OS Type column shows various operating systems, including windows-nt-2k-xp, solaris, and linux. The table is partially obscured by a vertical black bar.

| Virtual Sensor | Host IP Address | OS Type |
|----------------|-----------------|------------------|
| vs0 | 114.0.0.122 | windows-nt-2k-xp |
| vs0 | 114.0.0.1355 | windows-nt-2k-xp |
| vs0 | 114.0.0.149 | windows-nt-2k-xp |
| vs0 | 117.0.0.238 | windows-nt-2k-xp |
| vs0 | 117.0.0.10 | windows-nt-2k-xp |
| vs0 | 117.0.0.29 | windows-nt-2k-xp |
| vs0 | 117.0.0.75 | windows-nt-2k-xp |
| vs0 | 12.0.0.90 | windows-nt-2k-xp |
| vs0 | 16.0.0.6 | windows-nt-2k-xp |
| vs0 | 172.0.0.4217 | windows-nt-2k-xp |
| vs0 | 184.0.0.88 | windows-nt-2k-xp |
| vs0 | 184.0.0.226 | windows-nt-2k-xp |
| vs0 | 187.0.0.83 | windows-nt-2k-xp |
| vs0 | 187.0.0.76 | windows-nt-2k-xp |
| vs0 | 189.0.0.6 | windows-nt-2k-xp |
| vs0 | 189.0.0.237 | windows-nt-2k-xp |
| vs0 | 198.0.0.77 | windows-nt-2k-xp |
| vs0 | 198.0.0.117 | solaris |
| vs0 | 200.0.0.78 | windows-nt-2k-xp |
| vs0 | 200.0.0.1395 | windows-nt-2k-xp |
| vs0 | 200.0.0.1116 | windows-nt-2k-xp |
| vs0 | 201.0.0.206 | windows-nt-2k-xp |
| vs0 | 202.0.0.26 | windows-nt-2k-xp |
| vs0 | 202.0.0.481 | linux |
| vs0 | 202.0.0.7175 | solaris |
| vs0 | 202.0.0.134 | windows-nt-2k-xp |
| vs0 | 207.0.0.40 | windows-nt-2k-xp |
| vs0 | 210.0.0.52 | windows-nt-2k-xp |
| vs0 | 210.0.0.95 | linux |
| vs0 | 210.0.0.9 | windows-nt-2k-xp |
| vs0 | 210.0.0.3180 | windows-nt-2k-xp |
| vs0 | 210.0.0.2021 | windows-nt-2k-xp |
| vs0 | 211.0.0.181 | windows-nt-2k-xp |
| vs0 | 211.0.0.124 | windows-nt-2k-xp |
| vs0 | 211.0.0.117 | windows-nt-2k-xp |
| vs0 | 211.0.0.6213 | linux |
| vs0 | 211.0.0.6233 | linux |
| vs0 | 211.0.0.590 | windows-nt-2k-xp |
| vs0 | 211.0.0.153 | windows-nt-2k-xp |
| vs0 | 211.0.0.784 | linux |
| vs0 | 211.0.0.866 | windows-nt-2k-xp |
| vs0 | 211.0.0.888 | windows-nt-2k-xp |
| vs0 | 211.0.0.2 | windows-nt-2k-xp |
| vs0 | 211.0.0.8 | windows-nt-2k-xp |

実施検証内容(NSP)

■ システム情報

- 設置機器: NSP I2700
- 設定
 - センサーバージョン: 4.1.5.117
 - マネージャソフトウェアバージョン: 不明

■ Attacker、Victim

- Attacker: CentOS(IPv4枯渴TF)
xxx.yyy.zzz.214 / 2001:DB8::214
- Victim : CentOS xxx.yyy.zzz.215 / 2001:DB8::215

※ NSPに設置したVictimサーバが外部との通信がとれなかったためローカル環境で検証

実施検証内容(NSP)

■ テスト項目

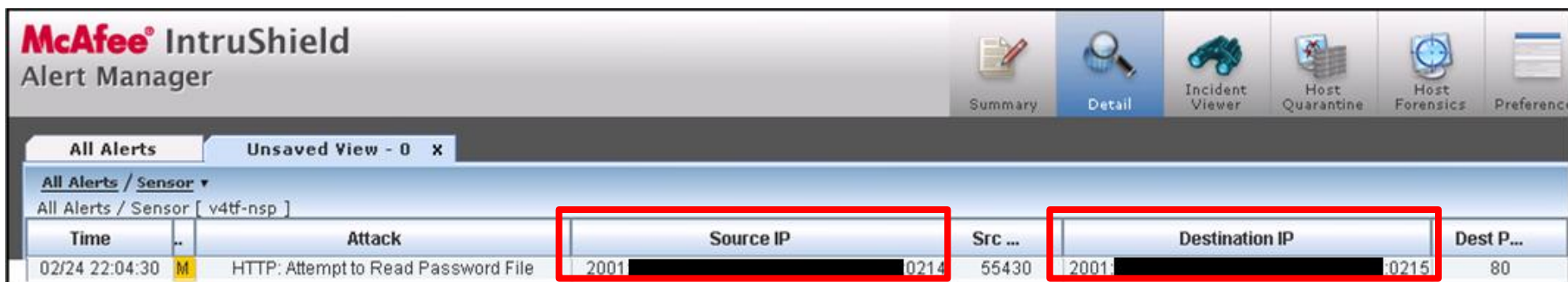
- 検知テスト
 - ベンダシグネチャ
 - リコネッサンスポリシー
- IPv6に特化した試験項目
 - イベントの連続検知時の取りこぼし
 - アラートフィルタの適用
 - UDSの作成
 - イベント検知時のリセットパケット送信

※ 未実施の項目

THCツールの実行、IPv6によるシグネチャアップデート、ルーティングテーブルの確認
RA,NAのパケット確認

実施検証内容(NSP): 検知テスト(ベンダシグネチャ)

- Victim サーバに対して、`http://[2001:DB8::215]/etc/passwd`送信する



The screenshot shows the McAfee IntruShield Alert Manager interface. The main window displays a table of alerts. The first alert is highlighted, showing the following details:

| Time | Attack | Source IP | Src ... | Destination IP | Dest P... |
|------------------|-------------------------------------|---------------|---------|----------------|-----------|
| 02/24 22:04:30 M | HTTP: Attempt to Read Password File | 2001:DB8::214 | 55430 | 2001:DB8::215 | 80 |

正常に検知

実施検証内容(NSP): 検知テスト(リコネッサンスポリシー)

- Victim サーバに対して、nmapを実行する

| Time | Attack | SrcIP | Src Port | DestIP | Dest Port |
|------------------------------------|-----------------------|------------------------------------|----------|------------------------------------|-----------|
| Thu Feb 24 20:25:24 JST 2011 | TCP: SYN Port Scan | 2001:0DB8:0000:0000:0000:0000:0214 | 0 | 2001:0DB8:0000:0000:0000:0000:0215 | 0 |

正常に検知

実施検証内容(NSP):IPv6に特化した試験項目

■ イベントの連続検知時の取りこぼし数の検証

Victim サーバに対して、http://[2001:DB8::215]/etc/passwdを200～5000回連続送信した時の検知件数の比較

検知結果:

/etc/passwd連続送信時の検知件数

| プロトコル 送信回数 | 200回 | 1000回 | 5000回 |
|------------|------|-------|-------|
| IPv4(無負荷) | 200 | 1000 | 5000 |
| IPv6(無負荷) | 200 | 1000 | 5000 |
| IPv6(負荷) | 200 | - | - |

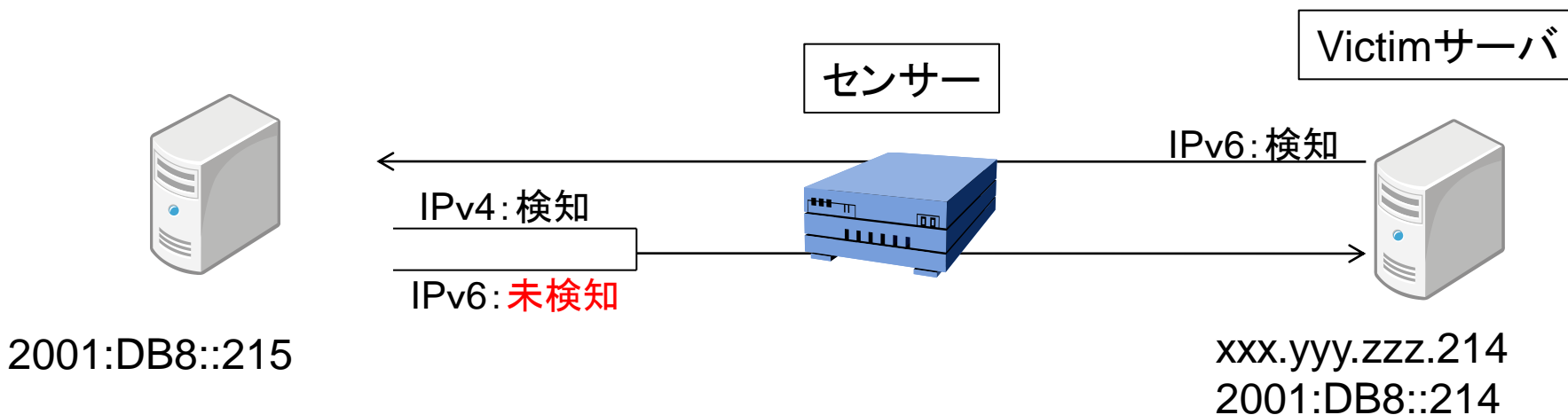
※ 負荷は1GBのファイルダウンロードを10セッション接続中に検証

実施検証内容(NSP): IPv6に特化した試験項目

■ アラートフィルタの適用

CentOS(2001:DB8::214)あてのhttp://[2001:DB8::214]/etc/passwdを検知しないように設定

検知結果:



特定のIPv6通信をアラートフィルタ可能

実施検証内容(NSP):IPv6に特化した試験項目

■ UDSの作成:

- ① host:2001:DB8::215を検知条件にしたシグネチャの作成
- ② DestIP:2001:DB8::215を検知条件にしたシグネチャの作成

検知結果: ①のみ検知

Alert Details

Alert

| | | | | |
|--------------------------|-----------------------------|----------------------|---------------------|---|
| Attack Name: | UDS-ipv6.test-ipv6attack | Interface: | 1A-1B | View/Edit Attack Response |
| Sensor ID: | v4tf-nsp | State: | Unacknowledged | Save As Evidence Report |
| Severity: | 6 | Alert ID: | 5595735068410317399 | Block |
| Time: | 2011-02-25 10:56:28.000 JST | Direction: | Inbound | Show Packet Log |
| Domain: | My Company | Subcategory: | --- | Advanced Configuration |
| Category: | --- | Detection Mechanism: | --- | |
| Result Status: | Maybe Successful | VLAN ID: | - NA - | |
| Vulnerability Relevance: | Unknown | | | |
| Policy Name: | All-Inclusive With Audit | | | |

Exploit

| | | | |
|-----------------------------|----------------------|-----------------------|-------------------------|
| Exploit ID: | 1 | Name: | Signature-1298598249957 |
| Network Protocol: | tcp | Application Protocol: | http |
| Source IP: | 2001:[REDACTED]:0214 | Source Port: | 55291 |
| Destination IP: | 2001:[REDACTED]:0215 | Destination Port: | 80 |
| Benign Trigger Probability: | High | | |

Signature #1:
This signature matches against one or more of the following strings:

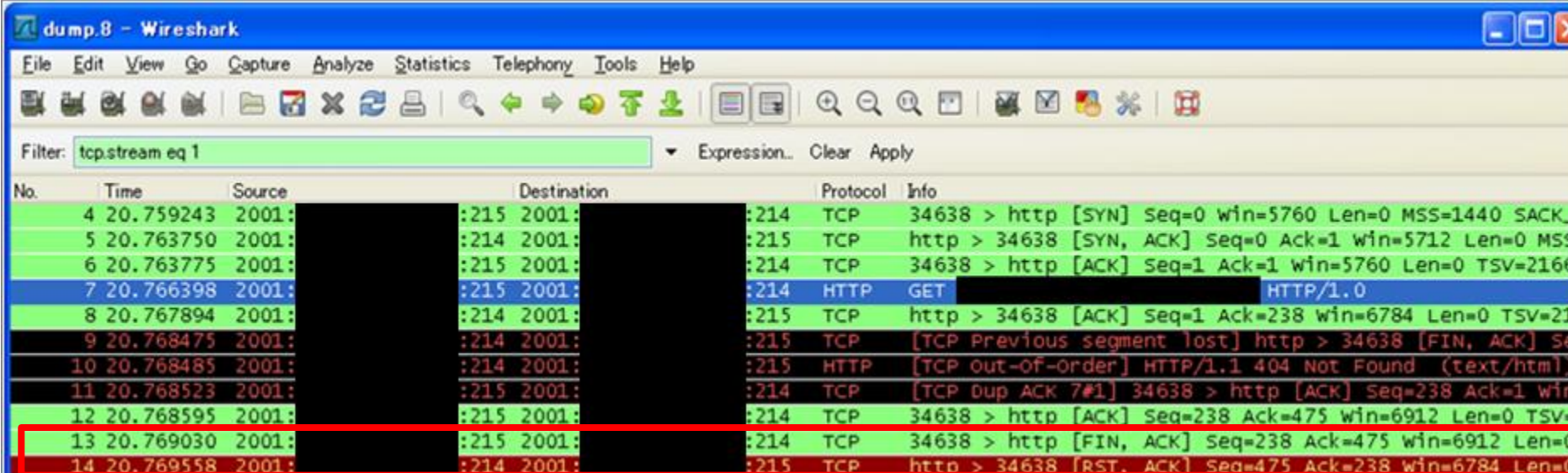
- "2001[REDACTED]215"

< Prev Alert Next Alert > Close

実施検証内容(NSP):IPv6に特化した試験項目

- イベント検知時のリセットパケット送信:
特定シグネチャを検知した時に送信先にリセットパケットを送信し、セッションを終了させる

検知結果:



The image shows a Wireshark packet capture window titled 'dump.8 - Wireshark'. The filter is set to 'tcpstream eq 1'. The packet list shows several packets, with packet 14 highlighted in red, indicating an RST packet. The packet details for packet 14 show a TCP RST packet with Seq=475, Ack=238, and Win=6784.

| No. | Time | Source | Destination | Protocol | Info |
|-----|-----------|--------|--------------|----------|---|
| 4 | 20.759243 | 2001:: | ::215 2001:: | TCP | 34638 > http [SYN] Seq=0 win=5760 Len=0 MSS=1440 SACK_F |
| 5 | 20.763750 | 2001:: | ::214 2001:: | TCP | http > 34638 [SYN, ACK] Seq=0 Ack=1 win=5712 Len=0 MSS= |
| 6 | 20.763775 | 2001:: | ::215 2001:: | TCP | 34638 > http [ACK] Seq=1 Ack=1 win=5760 Len=0 TSV=21663 |
| 7 | 20.766398 | 2001:: | ::215 2001:: | HTTP | GET [REDACTED] HTTP/1.0 |
| 8 | 20.767894 | 2001:: | ::214 2001:: | TCP | http > 34638 [ACK] Seq=1 Ack=238 win=6784 Len=0 TSV=217 |
| 9 | 20.768475 | 2001:: | ::214 2001:: | TCP | [TCP Previous segment lost] http > 34638 [FIN, ACK] Seq |
| 10 | 20.768485 | 2001:: | ::214 2001:: | HTTP | [TCP out-of-order] HTTP/1.1 404 Not Found (text/html) |
| 11 | 20.768523 | 2001:: | ::215 2001:: | TCP | [TCP Dup ACK 7#1] 34638 > http [ACK] Seq=238 Ack=1 Win |
| 12 | 20.768595 | 2001:: | ::215 2001:: | TCP | 34638 > http [ACK] Seq=238 Ack=475 win=6912 Len=0 TSV=2 |
| 13 | 20.769030 | 2001:: | ::215 2001:: | TCP | 34638 > http [FIN, ACK] Seq=238 Ack=475 win=6912 Len=0 |
| 14 | 20.769558 | 2001:: | ::214 2001:: | TCP | http > 34638 [RST, ACK] Seq=475 Ack=238 win=6784 Len=0 |

IPv6アドレスにRSTパケット送信

6. IPv6環境での攻撃状況

- IPv6アドレスを持つvictimに対する攻撃は発生しなかった

7. 各社コメント①

■ 初体験の感想

- IPv6アドレス打つのが面倒くさい！
- インターネット越しのIPv6 pingでv6通信初体験！これだけで大騒ぎ。
- アドレス指定に [] が必要と知って驚愕した。
- route tableやneighbor cacheを確認するコマンドがわからない。

■ IPv6表記について

- 某社では、RFCに則ったルールを使っている
- 業界標準みたいなものがあると、お客さんも混乱がないのではないか。
- 報告書の記載の仕方でお客さんにいろいろ注文をつけられるかも。
- 緊急連絡する際もメールに書いて伝えるのか？
- 製品設定画面などにIPv6アドレスを表示する場所全てでコピー&ペーストできるようにしてほしい。
- IPv6アドレスを読み上げる方法にもルールがほしい。
- ログを一覧表記したときに省略表記されてしまうとカラムがずれるので、省略表記有無のモードを実装してほしい。
- 本報告書用に記載するアドレス変換が大変だった。

7. 各社コメント②

■ IPv6対応にむけて

- IPv6対応とはこういうものだという基準がない。
→ メーカーがIPv6対応しているという製品に対し項目を並べたアンケートをお願いする。○×つけて返してもらってはどうか。
- FQDNを記載する際にIPv4・IPv6のどちらなのかを明記する必要がある。
- 同じホストにIPv4・IPv6が振られている場合、紐付けが必要

■ 疑問点

- ARP Spoofingの対策を実装していても、RA Spoofing(?)対策は実装されていないかも。RFC的にどうなのか？
- Linux(Redhat系)でサブネット付きでアドレス書くとき/48で書いても/64になってしまう。なぜ？指定する意味なし？
- DNSの逆引き登録はちゃんとやるのか？(SPAMブラックリスト管理とかどうなる？)

7. 各社コメント③

■ 運用設計に関して

- デュアルスタックの場合、監視対象が2倍以上となる設計が必要 (IPv6アドレスがいっぱい振られるのでどこまでやるのか?)
- IPアドレスの伝達方法に注意が必要
- ネットワーク導通確認にデフォルトゲートウェイを指定する手法が通用しない (リンクローカルが自動で振られるため、同一セグメントのデフォルトゲートウェイにはpingが通ってしまう)
- お客様の運用も変えてもらう必要もある

■ その他の感想

- 座学だけじゃなくて、実際に手を動かさないと理解できない
- デュアルスタック環境でのトラブルシューティングが大変そう。
- 会社に評価環境が必要。
- 通信させるまでは大変だったけど、通信の中身はアドレスがIPv6になっただけで、あとはあまり変わらない。

8. 課題

■ 本検証作業に関する課題

- IPv6に関するオペレーションは初めてだったので、初期設定に時間がかかった（pingを打つことさえもWebで調べながら。。。）
- 一般的なセキュリティ機器の検証は行ったが、IPv6に特化した脆弱性等の踏み込んだ検証を実施できなかった

■ 今後の課題

- オペレータやエンジニアを対象にしたIPv6のハンズオン教育（オペレーション／セキュリティ、IPv4との差分）が必要
- 以下の業務に携わる人々が自由にIPv6の検証ができる環境が必要
 - ・製品の開発/評価
 - ・サービスの運用/受入
 - ・IPv6環境を必要とするお客様をもつSler
- IPv6対応製品を導入する際は事前の運用設計（監視内容、キャパシティ、障害切り分け、お客様との認識合わせ）が必要

9. ISOG-J における今後の取り組み

■ IPv6 関連のハンズオンを継続 (JNSA の Lab 環境※を活用)

- デュアルスタック環境でのパフォーマンス検証
- IPv6 固有の脆弱性への攻撃に関する検証 (セキュリティ機器への攻撃 / 監視対象システムへの攻撃)
- その他

■ IPv6に関する知識の共有

- IPv6 関連のセキュリティ問題を WG2 で取り上げる
- 各社の IPv6 関連 TIP を共有する (設計、運用、機器関連、etc.)
- JNSA IPv6 WG / U40 との連携

※JNSA参加企業はJNSA Lab環境を利用可能

10. 参加企業、参加者一覧

| 参加企業 (ISOG-J) | | 参加者 |
|---------------------------|--------------|--|
| 株式会社インターネットイニシアティブ | | 加藤 雅彦、齋藤 聖 |
| 日本アイ・ビー・エム株式会社 | | 落合 宏俊、朝長 秀誠、梨和 久雄、窪田 豪史、小原 正法、井上 博文、近藤 和弘 |
| NECネクサソリューションズ株式会社 | | 駒崎 修、中西 克彦、谷口 由夏 |
| NTTコムテクノロジー株式会社 | | 渡邊 守登、門田 剛 |
| NTTデータ・セキュリティ株式会社 | | 小林 稔 |
| 株式会社 Kaspersky Labs Japan | | 前田 典彦、出澤 貴之 |
| 富士通株式会社 | | 河原林 広、佳山 こうせつ |
| 株式会社日立情報システムズ | | 丹京 真一、折田 彰 |
| 株式会社ラック | | 川口 洋、川崎 基夫、天野 一輝、許 先明、品川 亮太郎、阿部 正道、浅倉 なおみ、堀江 亘 |
| Special Thanks | 株式会社ISAO | 米沢 晋 (JNSAラボネットWG) |
| | 日本電気株式会社 | 一宮 隆祐 (JNSAラボネットWG) |
| | トレンドマイクロ株式会社 | 林 憲明 (JNSA IPv6 WG) |

11. 参考URL

- IPv6 Neighbor Discovery (ND) Trust Models and Threats
<http://www5d.biglobe.ne.jp/~stssk/rfc/rfc3756j.html>
- ステートレス自動設定に関する問題、マルチキャストに関する問題など
http://www.kanadas.com/investigation-j/2007/11/ipv6_10.html
- IPv6ネットワークを作ろう
<http://www.hieda.net/pcnwb/ipv6/index.htm>

