Problem Analysis in ntopng

Matteo Biscosi
Many Security Features...

In ntopng we have many cybersecurity features:

- Alerts
- Asset Map
- Device/Mac Add. Tracking
- Flow Alerts Analyzer
- Historical Flows
- Historical Charts
- Host Map
- Inactive Local Hosts
- Periodicity Map
- Ports Analysis
- Service Map
- Traffic Rules
- Vulnerability Scan
- SNMP
- ...

*Highlighted features are new*
...but few are know/used

Of all the cybersecurity features we have, usually users:

• Know very few of them
• Don't know how to use them
• Don't know how to combine them
Problem Analysis

• Let's explore those features one by one, analyze them and understand how they can be used for traffic analysis

• See in real scenarios their effectiveness
Alerts
Alerts are really important because they report strange behaviors in the network. However:

- A lot of alerts are triggered
- Too many informations

The result is:

Do not look at them

**WRONG**
Tune Alerts (1/3)

Let's tune checks in order to use them as better as possible:

- Disable not useful checks for the network
- Tune correct threshold where possible
- Exclude specific alerts in certain cases (Enterprise M License)

(After tuning alerts, even more useful recipients can be used)
Closed network, except for a couple of hosts, there shouldn't be many flows towards remote hosts.

Average active flows 30, maybe a little high.

Score too low as the average is 250.
Tune Alerts (3/3)

New classification: 
Require Attention & All

Exclude this alert type towards this host!

Are we interested in periodic flows? Otherwise disable the alert
Flow Alerts Analyzer

Outlier: an observation that deviates much from other observations
After tuning the Alerts, indicators regarding the score are much more useful.

"Normal" behavior

Outlier: an observation that deviates much from other observations.
Hosts Tracking

Detect unexpected hosts connecting to the network (with no permission) or trying to attack other local hosts.

It can be detected in a few ways:

• Device/MAC address Tracking (Live)
• Inactive Local Hosts (After the host disconnects)
• SNMP (Live)
• Historical Flows (After)
Device/MAC Address Tracking

What's he doing here?

When did it happen?

Do you have a network where hosts do not** must** disconnect?

*Available from Enterprise M License*
## Inactive Local Hosts

<table>
<thead>
<tr>
<th>Host: 192.168.2.237</th>
<th><img src="#" alt="Link to Host Details" /></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC Address / Device Type</strong></td>
<td>00:04:96:E4:AA:CD</td>
</tr>
<tr>
<td><strong>IP Address / Network</strong></td>
<td>192.168.2.237</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>192.168.2.237</td>
</tr>
</tbody>
</table>

### Table View

<table>
<thead>
<tr>
<th>Actions</th>
<th>Host</th>
<th>Name</th>
<th>MAC Address</th>
<th>Manufacturer</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.125</td>
<td></td>
<td>00:0C:29:0A:8F:CE</td>
<td>VMware, Inc.</td>
<td>08/04/2023 14:34:08</td>
<td>08/04/2023 14:34:10</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.115</td>
<td></td>
<td>00:0C:29:22:5E:66</td>
<td>VMware, Inc.</td>
<td>08/04/2023 14:34:08</td>
<td>08/04/2023 14:34:10</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.39</td>
<td></td>
<td>00:0C:29:37:0D:05</td>
<td>VMware, Inc.</td>
<td>09/15/2023 15:30:01</td>
<td>09/15/2023 15:30:06</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.180</td>
<td></td>
<td>00:0C:29:41:8D:56</td>
<td>VMware, Inc.</td>
<td>08/04/2023 14:34:08</td>
<td>08/04/2023 14:34:10</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.45</td>
<td></td>
<td>00:0C:29:4C:06:6B</td>
<td>VMware, Inc.</td>
<td>09/01/2023 10:34:30</td>
<td>09/01/2023 10:34:32</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.113</td>
<td></td>
<td>00:0C:29:29:56:11:96</td>
<td>VMware, Inc.</td>
<td>08/03/2023 14:51:15</td>
<td>08/03/2023 14:51:18</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.86@2464</td>
<td>desktop-8v8r41</td>
<td>00:0C:29:6C:7D:F6</td>
<td>VMware, Inc.</td>
<td>08/23/2023 17:09:19</td>
<td>08/23/2023 17:12:58</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.86@384 [Test vlan]</td>
<td>desktop-8v8r41</td>
<td>00:0C:29:6C:7D:F6</td>
<td>VMware, Inc.</td>
<td>08/23/2023 17:09:20</td>
<td>08/23/2023 17:09:25</td>
</tr>
<tr>
<td><img src="#" alt="Expand" /></td>
<td>192.168.2.86@2223</td>
<td>desktop-8v8r41</td>
<td>00:0C:29:6C:7D:F6</td>
<td>VMware, Inc.</td>
<td>08/23/2023 17:09:20</td>
<td>08/23/2023 17:09:25</td>
</tr>
</tbody>
</table>
### SNMP

<table>
<thead>
<tr>
<th>Interface Index</th>
<th>MAC Address</th>
<th>IP Associated</th>
<th>Manufacturer</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>04:92:26:5C:97:35</td>
<td>fe80:692:26ff:fe5c:9735</td>
<td>ASUSTek COMPUTER INC.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>MyDevice (PLC1) [04:18:D6:06:83:5A]</td>
<td>142.250.184.78 and 4 more Hosts</td>
<td>Ubiquiti Inc</td>
<td>Router/Switch</td>
</tr>
<tr>
<td>2</td>
<td>00:B0:28:00:00:01</td>
<td>fe80:20c:29ff:fe5c:66b</td>
<td>Extreme Networks, Inc</td>
<td>Router/Switch</td>
</tr>
<tr>
<td>2</td>
<td>00:0C:29:4C:06:6B</td>
<td>fe80:20c:29ff:fe5c:66b</td>
<td>VMware, Inc</td>
<td>Computer</td>
</tr>
<tr>
<td>2</td>
<td>3C:4A:92:90:E0:80</td>
<td>192.168.2.169</td>
<td>Hewlett Packard</td>
<td></td>
</tr>
</tbody>
</table>

*Available from Enterprise M License*
Historical Flows

Which activity this host did while it was connected?

SNMP Traffic sent/received by host devel

*Available from Enterprise M License
Flow Tracking
Flows Tracking

We could start from flows, instead of analyzing hosts activity, identifying and discovering suspicious (malicious) traffic.

There are different ways to do it:
• Service/Periodicity/Assets Map
• Server Ports Analysis (Ports Analysis)
Inside the network (local traffic), who is talking to whom?

Is this local traffic legit or not?

*Available from Enterprise L License*
Service Map

Highly effective against Lateral Movements. The service map purpose is to show the traffic between local hosts:

• By using a Learning Period it is possible to let the map learn acceptable local flows and mark the others as denied

• Find possible open ports
Which are the periodic flows in a network? Is it okay to have them?

Is this periodic traffic okay?
Periodicity Map

Used to identify Periodic flows:

• Discover the frequency, observations, ...
• Find improper connections (e.g. ssh)
Who is this SMTP Server?

Which are the asset available in the network?
Asset Map

Identify the asset available in a network:

- SMTP, IMAP, POP, DNS, NTP servers
- Identify possible infected hosts, showing themselves as one of those servers
Why is there SMTP traffic on port 2500?

Why is there TLS traffic on port 44445?
Traffic Rules & Vulnerabilities Scan

• Create custom traffic alerts on Interfaces, Hosts, SNMP Hosts, ...

• Actively scan hosts for their open ports, vulnerabilities, ecc.

We will see more later on with Nicolò...
Historical Charts
Historical Charts

*Available from Enterprise L License
Historical Charts (1/2)

Historical charts page is one of the most important ones for traffic/cybersecurity analysis:

• Useful to identify traffic anomalies
• One of the starting point for traffic analysis
Historical Charts

What's this drop? zoom in and analyze the traffic (drag and drop the area to zoom in)
**Historical Charts**

<table>
<thead>
<tr>
<th>Application</th>
<th>Traffic</th>
<th>Percentage</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
<td>75.04 TB</td>
<td>40.4 %</td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td>30.77 TB</td>
<td>16.6 %</td>
<td></td>
</tr>
<tr>
<td>FTP_DATA</td>
<td>15.19 TB</td>
<td>8.2 %</td>
<td></td>
</tr>
<tr>
<td>IMAPS</td>
<td>10.14 TB</td>
<td>5.5 %</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropbox</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Half the traffic, one of the two exporters was not exporting?
Try it

Now let's use a couple of pcaps to check how to use all these cybersecurity tools