Say Hello To ntopng 4.0

Cybersecurity, Scripting… and a New User Interface
Agenda

• ntopng 4.0: some numbers
• Motivation
• Main breakthroughs
  ◦ New look-and-feel
  ◦ Cybersecurity-related features
  ◦ Active monitoring
  ◦ Plugins
• Additional features
• Conclusions
ntopng 4.0: Some Numbers

• **One and half years** after ntopng 3.8

• **Community**
  ◦ 3,688 files changed
  ◦ 438,746 insertions / 238,350 deletions

• **Pro/Enterprise**
  ◦ 329 files changed
  ◦ 14,904 insertions / 10,273 deletions
ntopng 4.0: Motivation [1/3]

• Refresh its **look-and-feel**
  ◦ Modern look, customizable, more intuitive, optimized for wide-screens

• Focused on **cybersecurity**
  ◦ Augment network data with security intelligence indicators
ntopng 4.0: Motivation [2/3]

• **Simplify** the **analysis of heterogeneous traffic**
  ◦ Ability to create interfaces on-the-fly, matching certain patterns of traffic

• **Support for active monitoring**
  ◦ Don't just passively look at what's on the network
  ◦ Probe the network to make sure it behaves as expected
ntopng 4.0: Motivation [3/3]

• Make it more **extensible** to **facilitate** community contributions
  ◦ Easier for users and practitioners to extend ntopng functionalities without touching its core
A Refreshed Look-and-Feel
The New Web UI

- Always-Visible Status Bar
- Vertical Menu on the Left
The New Web UI: Skins
Focus on Cybersecurity
Cybersecurity: Why?

• **Increasingly relevant** in any environment (corporate, SMEs, SOHO, home)
  ◦ Protection of data is fundamental - and now also requested by law

• **Increasingly difficult** as
  ◦ There is no longer a clear line dividing the good from the bad
    • Think to people carrying personal devices at work
  ◦ A large part of the traffic is encrypted
    • Hard to understand what is in it
ntopng 4.0 and Cybersecurity

• **Behavioral protocol analyses** for encrypted and non-encrypted protocols, e.g.,
  - A Dropbox flow is uploading data outside the company network
  - A DNS query contains suspicious names
  - A TLS is likely originated by a malware application

• Generate **alerts** when suspicious traffic is found
Behavioral Protocol Analyses

• Aim is to **assess** (to some extent)
  ◦ How protocols are **(ab)used**
• Encrypted protocols (e.g., TLS) are not decrypted
  ◦ Decryption is unpractical
TLS Analysis

- Certificates analysis
  - Names, Validity
- Robustness of encryption
TLS Analysis: Alerts

Flow Alerts

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Duration</th>
<th>Count</th>
<th>Severity</th>
<th>Alert Type</th>
<th>Score</th>
<th>Drilldown</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>26/03/2020 17:59:30</td>
<td>1</td>
<td>Error</td>
<td>! Potentially Dangerous Protocol</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Old TLS Version**: Trigger an alert when an old (and possibly unsecure) TLS version is detected.
- **TLS Certificate Expired**: Trigger an alert when an expired TLS certificate is detected.
- **TLS Certificate Issues**: Trigger an alert when a mismatched TLS certificate is detected.
- **TLS Unsafe Ciphers**: Trigger an alert when unsafe TLS ciphers are detected.

Showing 1 to 4 of 4 rows
## Additional Behavioral Protocol Analyses

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
<th>Values</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklisted Country</td>
<td>!</td>
<td>Trigger an alert when hosts contact or are contacted by the specified co...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blacklisted Flow</td>
<td>!</td>
<td>Trigger an alert when a blacklisted host or domain is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Exfiltration</td>
<td>!</td>
<td>Trigger alerts when a possible data exfiltration activity is detected</td>
<td></td>
<td>Disable</td>
</tr>
<tr>
<td>Device Application Not Allowed</td>
<td>!</td>
<td>Trigger an alert when an unusual application is detected for a device. R...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Data Exfiltration</td>
<td>!</td>
<td>Trigger alerts when a DNS data exfiltration activity is detected</td>
<td></td>
<td>Disable</td>
</tr>
<tr>
<td>Elephant Flows</td>
<td>!</td>
<td>Trigger an alert when a flow exchanges more than the configured bytes vo...</td>
<td>&gt; 1 GB (L2R), &gt; 1 GB (R2L). Exce...</td>
<td></td>
</tr>
<tr>
<td>Invalid DNS Query</td>
<td>!</td>
<td>Trigger an alert when a possibly malicious DNS query is detected</td>
<td>sophosxl.net</td>
<td></td>
</tr>
<tr>
<td>Long Lived</td>
<td>!</td>
<td>Trigger an alert when a flow lasts more than the configured duration</td>
<td>&gt; 01:00. Exceptions: Database</td>
<td></td>
</tr>
<tr>
<td>Malicious Signature</td>
<td>!</td>
<td>Trigger an alert when a possibly malicious signature is detected</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Simplifying the Analysis of Heterogeneous Traffic
Sub-Interfaces: Why? [1/2]

• **(Corporate) network traffic** is often **heterogeneous**
  ◦ Employees network
  ◦ Core company servers
  ◦ Guests network
  ◦ ...

• Logical separation done with
  ◦ VLANs
  ◦ Subnets
  ◦ ...
Sub-Interfaces: Why? [2/2]

• Having all the traffic "mixed" in a single interface not of help for the analysts
  ◦ Hard to tell X and Y apart, difficult to do root-cause analyses
• Need to partition the traffic into meaningful subsets
Automatic Traffic Partitioning

• Automatically divert the traffic of an interface into logical **sub-interfaces**

• Criteria such as
  ◦ NetFlow/sFlow exporter IP address
  ◦ VLAN ID
  ◦ SNMP Interfaces
Custom Traffic Partitioning

- Sometimes a single criteria is not enough and custom disaggregation is required
- ntopng 4.0 allows to define sub-interfaces with BPF-like filters
Active Monitoring
Active Monitoring: Why?

• Important hosts in the network
  ◦ Offering critical services
    • Backup
    • VPN
    • NAS
• They must be always available and fully functional
Active Monitoring in ntopng 4.0

• ntopng 4.0 active monitoring probes hosts on a minute-by-minute basis
• Check **reachability of hosts** and **availability of their services**
  - ICMP/ICMPV6
  - HTTP/HTTPS
• ⚠ Alerts when hosts are unreachable or have high Round Trip Time (RTT)
Monitoring Hosts RTT
Historical Host RTT
# RTT-Based Alerts

## Engaged Alerts

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Duration</th>
<th>Severity</th>
<th>Alert Type</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:22 ago</td>
<td>01:22</td>
<td>Warning</td>
<td>! RTT</td>
<td>RTT too high for <a href="http://ntop.org">http://ntop.org</a> (178.62.197.130) [148.95 ms &gt; 25 ms].</td>
<td>Disable</td>
</tr>
<tr>
<td>01:22 ago</td>
<td>01:22</td>
<td>Warning</td>
<td>! RTT</td>
<td>RTT too high for <a href="https://one.one.one.one">https://one.one.one.one</a> (1.1.1.1) [419.44 ms &gt; 200 ms].</td>
<td>Disable</td>
</tr>
<tr>
<td>03:23 ago</td>
<td>03:23</td>
<td>Warning</td>
<td>! RTT</td>
<td>Host icmp6://2001:4860:4860::8888 is unreachable.</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Something for the Developers:
Extensibility
ntopng 4.0 Extensibility: Why?

• Ease community contributions
• Desire to turn ntopng into something which is really opensource
  • Open source means being on GitHub
  • Open source means free
  • Open source means easily extensible by community contributors
ntopng 4.0 Extensibility: Plugins

- **Move** most of the **functionalities** from the C/C++ core to **plugins**
  - Redesign ntopng architecture
- **Plugins are Lua scripts** executed by ntopng periodically or on an event-driven basis
Plugin Functionalities

• Plugins are executed
  ◦ **Periodically**: every min/5min/hour/day
  ◦ **On events**: e.g., when a new flow is detected, when a flow goes idle

• A developer can use plugins to "tap" into hosts, flows, and other network elements

• **APIs** to interact with the core
  ◦ **Pull** data **from the core**
    • e.g., read host traffic, read nDPI-dissected data
  ◦ **Push** data **into the core**
    • e.g., trigger alerts, set flow statues
Other Plugin Functionalities

• **Create Web UI pages** and **write timeseries** - RTT monitoring is implemented with a plugin!

• **Add menu entries**

• **Monitor the status of the host** on top of which ntopng is running

• **Check status and health of ntopng** itself
# Configuring Plugins

In this section, we will configure the plugins for traffic alerting and monitoring. We will focus on the `Traffic Alert` plugin, which is used to trigger alerts when the Layer 2 bytes delta (sent plus received) exceeds a certain threshold.

### Traffic Alert Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Description</th>
<th>Values</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Alert</td>
<td></td>
<td>Trigger an alert when the Layer 2 bytes delta (sent + received) exceeds ...</td>
<td>&gt; 30000 Bytes (Minute), &gt; 30000...</td>
<td>Disable, Edit, View</td>
</tr>
<tr>
<td>SYN Scan Victim Alert</td>
<td></td>
<td>Trigger an alert when the number of received SYN/s (with no response) exceeds ...</td>
<td>&gt; 30 SYN/s (Minute)</td>
<td>Disable, Edit, View</td>
</tr>
<tr>
<td>SYN Scan Attacker Alert</td>
<td></td>
<td>Trigger an alert when the number of sent SYN/s (with no response) exceeds ...</td>
<td>&gt; 50 SYN/s (Minute)</td>
<td>Disable, Edit, View</td>
</tr>
<tr>
<td>SYN Flood Victim Alert</td>
<td></td>
<td>Trigger an alert when the number of received SYN/min exceeds the threshold...</td>
<td>&gt; 50 SYN/min (Minute)</td>
<td>Disable, Edit, View</td>
</tr>
<tr>
<td>Traffic Alert</td>
<td></td>
<td>Trigger an alert when the Layer 2 bytes delta (sent + received) exceeds ...</td>
<td>&gt; 30000 Bytes (Minute), &gt; 30000...</td>
<td>Disable, Edit, View</td>
</tr>
</tbody>
</table>

To configure the `Traffic Alert` plugin, follow these steps:

1. **Enable/Disable**: You can enable or disable the plugin from the main menu.
2. **Timeframe**: Choose the time interval for the alert (Minute, 5 Minutes, Hourly, Daily).
3. **Threshold**: Set the threshold value for the alert.
4. **Values**: Specify the values for the alert conditions.
5. **Action**: Click on the action buttons to disable, edit, or view the plugin settings.

### Example Configuration

- **Name**: Traffic Alert
- **Category**: Traffic
- **Description**: Trigger an alert when the Layer 2 bytes delta (sent + received) exceeds a certain threshold.
- **Values**: > 30000 Bytes (Minute), > 30000...
- **Action**: Disable, Edit, View

By configuring the `Traffic Alert` plugin, you can effectively monitor and alert on network traffic anomalies, ensuring a secure and efficient network environment.
Plugins: Hands On

• Examples at https://github.com/ntop/ntopng/tree/dev/scripts/plugins

• Docs at https://www.ntop.org/guides/ntopng/plugins

• Video at https://www.youtube.com/watch?v=4ljkAhhCH8M
Other ntopng 4.0 Functionalities
Multi-Tenancy [1/2]

• (W)ISP, transit and other Internet providers use ntopng to provide services to their customers
  ◦ Security services
  ◦ Billing

• ntopng 4.0 becomes (really) multi-tenant
  ◦ Admin/non-admin users with different privileges
  ◦ Different users have access to different portions of
    • Traffic
    • Alerts
    • Local Networks
Multi-Tenancy [2/2]
Multi-Language

• Several languages supported thanks to community contributors
  ◦ English
  ◦ Italian
  ◦ Japanese
  ◦ German
  ◦ Czech
  ◦ Portuguese
Traffic-to-Process Visibility [1/2]

• **Associate flows with** the originating process and other process metadata
  ◦ Process
  ◦ Process Owner
  ◦ Docker container
  ◦ …

• ntopng 4.0 integrates with **nprobe-agent**, a packet-less probe capturing designed to capture these associations
Traffic-to-Process Visibility [2/2]

### Recently Active Flows

<table>
<thead>
<tr>
<th>Application</th>
<th>Protocol</th>
<th>Client</th>
<th>Server</th>
<th>Duration</th>
<th>Breakdown</th>
<th>Actual Thpt</th>
<th>Total Bytes</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>HTTP</td>
<td>root &gt; curl</td>
<td>127.0.0.1</td>
<td>0:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Flow Peers [Client/Server]
- Client: `ubuntu18:9974` - Last Seen: 11/30/2019 11:40:45 (00:50 ago)
- Server: `nProbe` - Last Seen: 11/26/2019 11:40:45 (00:50 ago)

#### Client Process Information
- User Name: `root`
- PID/Name: `/bin/bash`

#### Additional Flow Elements
- Flow exporter IPv4 Address: `ubuntu18`
Conclusions

• Releasing ntopng 4.0 brings several breakthroughs with its ~0.5 million of new lines of code

• A renewed look-and-feel of the Web UI offers the best experience on wide-screens and guarantee the important information is always visible

• Strong focus on security offers augmented visibility and increased protection against cyberthreats

• Active monitoring guarantee the network has expected behaviors

• A new pluggable architecture makes it more open for community contributions