PASSIVE FINGERPRINTING WITH SURICATA

PRESENTED BY:
JEREMY GROVE
WHO AM I

• Security Engineer at Quadrant Information Security
• Quadrant is an MSSP
• Role is to improve to support functions
• Just finished my Masters in Cyber Security and Information Assurance
  • WINK WINK ^^^^^ LOOK HERE!! ^^^^^ WINK WINK
WHAT IS FINGERPRINTING?

- **Fingerprinting** is the use of information to correlate data sets in order to identify network services, operating system number and version, software applications, databases, configurations and more.
REASONS TO USE SURICATA

• Other programs
  • Require another tool to watch
  • No control of signatures
  • Depends on developer for updates

• Suricata
  • Integrates with current tool set and workflow
  • Low cost
  • Customizable
WHY FINGERPRINT?

• Greater environmental intelligence
• Improved signal to noise ratio
• Faster research and response
• Confidence in triage decisions
SYSTEM COMPONENTS

- Signatures
- Data Management
SIGNATURE CONTENT

• User Agents
  • Mozilla/5.0 (Linux; Android 9; SM-G965U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.62 Mobile Safari/537.36

• Ports
  • 80 HTTP
  • 445 SMB

• Many more
  • Server Response, Broadcast IP used, etc.
SIGNATURE KEYWORDS

• Located in Metadata
• Fingerprint_os
  • Free form for any OS
• Fingerprint_type
  • Server or Client
• Fingerprint_expire
  • Set to timeframe in seconds
EXAMPLE SIGNATURE

alert http $HOME_NET any -> any any (msg:"Samsung Galaxy S10";
flow:established,to_server; content:"User-Agent|3a| "; nocase;
http_header; content:"SM-G973"; nocase; threshold: type limit, track
by_src, seconds 3600, count 1; target: src_ip; metadata: fingerprint_os
android, fingerprint_type client, fingerprint_expire 86400;
classtype:fingerprint; sid:xxxxxxxxxxx; rev:1;)
DHCP

• Provides MAC address
  • Allows you tie the IP to a specific device

• Moved into the alert file for ingestion
  • Allows you keep a historical record of the MAC to IP relationship
DATA MANAGEMENT

- Process Flow
- Redis
- Elasticsearch
PROCESS FLOW

• Fingerprint alert created
PROCESS FLOW CONT.

• Data inserted into Redis
  • fingerprint:event:172.17.248.11:11000006
  • fingerprint:event:172.17.248.11:11000013
  • fingerprint:event:172.17.248.11:11000101
  • fingerprint:event:172.17.248.11:11000306
PROCESS FLOW CONT.
• Actual alert from generated from Suricata
• Meer checks Redis for relevant data
• Meer submits alert and fingerprint results to SQL
• SOC Console displays both alert and fingerprints for the analyst
• SOC intelligence increased and research time decreased
• YAY!!
• Why Redis?
  • Data handling is more dynamic
  • Originally put everything in MySQL

• Rule Keywords
  • metadata: fingerprint_os android, fingerprint_type client, fingerprint_expire 86400;
  • classtype:fingerprint;
ELASTICSEARCH

• Meer outputs to eve json file
• Includes fingerprint alert and DHCP
• Used for long term storage
  • Important when DHCP is considered
  • Allows for historical lookups
### Console Output

#### Fingerprinting

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Fingerprints</th>
<th>OS</th>
<th>Type</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.10.49</td>
<td>1</td>
<td>Server [1/1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.17.0.52</td>
<td>3</td>
<td>Windows [2/3]</td>
<td>Client [3/3]</td>
<td></td>
</tr>
</tbody>
</table>
### Fingerprinting

**FINGERPRINTS OF DEVICES ON YOUR NETWORK**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Fingerprints</th>
<th>OS</th>
<th>Type</th>
<th>MAC Address</th>
</tr>
</thead>
</table>

**Fingerprints for: 172.17.0.211**

<table>
<thead>
<tr>
<th>Fingerprint</th>
<th>OS</th>
<th>Type</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer User Agent</td>
<td>Windows</td>
<td>Client</td>
<td>24 Oct 2019 15:55:11 UTC</td>
</tr>
<tr>
<td>Internet Explorer 7.0</td>
<td>Windows</td>
<td>Client</td>
<td>24 Oct 2019 15:55:11 UTC</td>
</tr>
<tr>
<td>Internet Explorer 9.0</td>
<td>Windows</td>
<td>Client</td>
<td>24 Oct 2019 14:55:35 UTC</td>
</tr>
<tr>
<td>SMB server</td>
<td>Server</td>
<td></td>
<td>24 Oct 2019 14:41:07 UTC</td>
</tr>
</tbody>
</table>
### Finger Print Details

**Fingerprint**

Internet Explorer 7.0

**Timestamp**

24 Oct 2019 15:55:11 UTC

**OS**

Windows

**Type**

Client

**MAC Address**

64:00:60:8a:7f:00

**Source IP**

172.17.0.211

**Source Port**

59305

**Destination IP**

172.17.10.34

**Destination Port**

8090

**Payload**

POST

Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/jpeg, */*

Referer: 

Accept-Language: en-US

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; 

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

Host: 

Content-Length: 584

Connection: Keep-Alive

Cache-Control: no-cache

Cookie: JSESSIONID=5B28CE6CD8B2DCEC894371FC46542AAD

Close
**INDICATOR-SCAN SSH brute force login attempt**

### Event Information

- **EVENT ID**: 1.48
- **SENSOR**: Change Sensor Name
- **ALERT SEVERITY LEVEL**: Inconsequential
- **TIMESTAMP**: Wednesday, 2 Oct 2019 @ 08:35 AM EDT

### Fingerprinting Information

- **SOURCE**
  - Mac OS User Agent
  - Windows User Agent
  - Internet Explorer User Agent
  - Google Chrome User Agent
- **DESTINATION**
  - No destination fingerprints found

### Network Information

<table>
<thead>
<tr>
<th>SOURCE IP</th>
<th>DESTINATION IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SOURCE PORT</th>
<th>DESTINATION PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>61241</td>
<td>22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROTOCOL</th>
<th>IP VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REVERSED SOURCE NAME</th>
<th>REVERSED DESTINATION NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Not Available</td>
<td>Information Not Available</td>
</tr>
</tbody>
</table>
THANK YOU!!

• Meer
  • https://github.com/beave/meer

• Fingerprint Rules
  • NEED MORE!!! Feel free to help!
  • https://github.com/quadrantsec/fingerprint-rules