Day 37:

They still do not suspect I am a mere cat.
Rogue Speaker Alert!!!!
CIS Critical Control #1

Inventory of Authorized and Unauthorized Devices
Back door  Etc....  Malware Server
Man in the middle  Private business  Sniffer
Authorized Devices – Known, Approved (attributable), up to Date

Known, but outdated – Approved device, but does not have all required agents/proper configs.

Unauthorized – Know what it is and what it does, but it does not have permission to be on the network.

Unknown – Know IP, maybe know OS, ports, but not much else.
• Network Scans – Scan regularly and perform diffs on each scan
  • Simple, Free to Cheap to acquire
  • Time consuming to run, opportunities for inaccuracies, delay in detection and action

• Tools – Install and deploy
  • Always monitoring, comprehensive, capable of complex actions
  • Can be complex to install, configure and tune, expensive

• Custom tools – Build, deploy and install
  • Near perfect fit for your org, able to modify if org changes
  • Time consuming to build, danger of developer loss
1.1.1.1

.........Maybe OS

.........Maybe open ports

......Signal information... some
<table>
<thead>
<tr>
<th>1.1.1.1</th>
<th>Physical location</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Link to SIEM to pull up all related events related to that IP</td>
</tr>
<tr>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>AD Membership</td>
<td></td>
</tr>
<tr>
<td>Possible Vendor</td>
<td></td>
</tr>
<tr>
<td>Results from Vulnerability Scan</td>
<td></td>
</tr>
<tr>
<td>Installed Agents</td>
<td></td>
</tr>
<tr>
<td>Network location</td>
<td></td>
</tr>
<tr>
<td>Provider</td>
<td></td>
</tr>
</tbody>
</table>

**WHAT IF I TOLD YOU**

YOU COULD KNOW MUCH MORE
IP, MAC and Hostname:
  DHCP, IPAM, SCCM

AD Membership:
  WMI or PS query to AD

Possible vendor:
  Query against MAC OUI file

Vulnerability Scan:
  Query scanner API or results in SIEM
Installed Agents:
  Query tool API or compare to lookup table

Network location:
  Query tool API or CAM tables

Provider:
  Often comes with WIDS information

Physical location:
  CAM tables, tool API, or approx location from WIDS
Based on output stored in: \\fs02\R2D2\201905262114PossibleRogues.csv

Found 5 host(s) out of a total of 11 listed in the 1 DHCP scopes on 1 server(s).
1 of those found are on the blacklist.

00-0C-29-D5-62-D6 is on the blacklist
,MSEDGEWIN10.SCOUTS.LOCAL

DHCP name: mSEDGEWIN10.SCOUTS.LOCAL
IP address: 192.168.1.100
Lease exp.: 5/26/2019 7:01:39 PM
MAC address: 00-0C-29-D5-62-D6
Vendor OUI: UNKNOWN
Pingable: N
Scope desc: Workstations

Completed at 21:14 of 05/26/2019
<table>
<thead>
<tr>
<th>DHCP-MAC</th>
<th>Date Found</th>
<th>DHCP-HOST</th>
<th>ScopeIP</th>
<th>Lease VENDOR</th>
<th>Ping</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-0C-29-E4-48-10</td>
<td>5/26/2019</td>
<td>GIANTS.Scouts.LOCAL</td>
<td>192.168.1.101</td>
<td>### VMWare</td>
<td>N</td>
</tr>
<tr>
<td>40-A8-F0-3E-E8-7E</td>
<td>5/26/2019</td>
<td>192.168.1.105</td>
<td>#### Hewlard Packard</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>6C-01-A8-C0</td>
<td>5/26/2019</td>
<td>192.168.1.108</td>
<td>#### INVALID OUI</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>00-0C-29-3A-F2-60</td>
<td>5/26/2019</td>
<td>192.168.1.110</td>
<td>#### VMWare</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P4445</th>
<th>C$AV</th>
<th>EPO</th>
<th>P80</th>
<th>DH Link</th>
</tr>
</thead>
</table>

https://github.com/ericmccullough/r2d2
How do we protect our networks?
Protections

Inventory of Known Devices
NAC/Port Security
802.1x
Physical Security
Zero Trust Model
• Devices in non-discovery mode
• Configure everything with authentication and encryption
  • Acknowledge these have weaknesses
• Segment all BT enabled devices from the rest of your network
• Set number of PIN #s required to 10 or more

• REALIZE THAT MANY IOT DEVICES CANNOT DO ANY OF THESE!
• Large number of possible rogues?
• Devices that have limited information?
• Can legit users/devices self remediate?
• Tool Improvement

• Respond to Bluetooth Rogues
Conclusion

Enhance your logs
Speed your analysis
Shorten your reaction time

Secure your network
Craig L Bowser  @reswob10
Sr Security Engineer
GSEC, GCED, GCDA  CISSP

Mentor SEC555

http://www.shadowtrackers.net/blog
RASPBERRYPI.SCOUTS.LOCAL has a non .com domain
DHCP name: RASPBERRYPI.SCOUTS.LOCAL
IP address: 192.168.1.104
Lease exp.: 4/25/2019 8:14:19 PM
MAC address: B8-27-EB-6E-A1-C7
Vendor OUI: UNKNOWN
Pingable: Y
Scope desc: Workstations";"

MALACHI.SCOUTS.LOCAL has a non .com domain
DHCP name: MALACHI.SCOUTS.LOCAL
IP address: 192.168.1.106
Lease exp.: 4/25/2019 8:33:48 PM
MAC address: 78-2B-CB-96-CA-1F
<table>
<thead>
<tr>
<th>HOST</th>
<th>Ping</th>
<th>P4445</th>
<th>C $</th>
<th>SAV</th>
<th>EPO</th>
<th>P80</th>
<th>DHCP-Server</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-0C-29-C7-6E-C8</td>
<td>04/25/2019</td>
<td>MSEDGEWIN10.Scouts.LOCAL</td>
<td>Workstations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://sccm/sccm/Report.asp?ReportID=37&amp;variable=00%3A0C%3A29%3AC7%3A6E%3AC8">http://sccm/sccm/Report.asp?ReportID=37&amp;variable=00%3A0C%3A29%3AC7%3A6E%3AC8</a></td>
</tr>
</tbody>
</table>