GEEK SQUAD —

Inmates built computers hidden in the ceiling, connected them to prison network

A Rogue Raspberry PI Hacked NASA's JPL Network

By Ryan Whitwam on June 20, 2019 at 12:26 pm | Comment
Craig Bowser
GCDA, GSEC, GCED
555 Mentor

Rapid Recognition and Response to Rogues
Day 37:
They still do not suspect I am a mere cat.
• Network Scans – Scan regularly and perform diffs on each scan

• Tools – Install and deploy

• Custom tools – Build, deploy and install
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Known, but outdated – Approved device, but does not have all required agents/proper configs.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.
IP & MAC & Hostname

..........Maybe OS

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

......Signal information... some
1.1.1.1
OS
Open ports (w/ service guess)
MAC
Hostname
AD Membership
Possible Vendor
Results from Vulnerability Scan
Installed Agents
Network location

Provider
Physical location

Link to SIEM to pull up all related events related to that IP

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, SNMP, or CAM tables

Provider:
Often comes with WIDS information

Physical location:
CAM tables, tool API, or approx location from WIDS
<table>
<thead>
<tr>
<th>DHCP-MAC</th>
<th>Date Found</th>
<th>DHCP-HOST</th>
<th>Scope</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></td>
<td>192.168.1.105</td>
<td>Hewlard Packard</td>
<td>Y</td>
</tr>
<tr>
<td>6C-01-A8-C0</td>
<td>5/26/2019</td>
<td>BAD_ADDRESS</td>
<td>192.168.1.108</td>
<td>INVALID OUI</td>
<td>Y</td>
</tr>
<tr>
<td>00-0C-29-3A-F2-60</td>
<td>5/26/2019</td>
<td>UBUNTU.SCOUTS.LOCAL</td>
<td>192.168.1.110</td>
<td>VMWare</td>
<td>Y</td>
</tr>
</tbody>
</table>

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

https://github.com/ericmccullough/r2d
"It's always fit perfectly before."
Rogue Inquisitor

https://github.com/reswob10/RogueInquisitor

< logo here TBD>
source2:
  name: DHCP
  filename: c:/tools/files/dhcp.csv
  MAC_Column: 1
  IP_Column: 0
  Host_Column: 2
  color: grey
  weight: 1
  enabled: 1
  ports:
    - appname: Tanium
      port: 5123
      weight: 2
    Rogue_Score: -5
    Good_Score: 3
Splunk Demo
How do we protect our networks?
Protections

Inventory of Known Devices
NAC/Port Security
802.1x
Physical Security
Zero Trust Model
User Education
• Large number of possible rogues?
• Devices that have limited information?
• Can legit users/devices self remediate?
• Tool Improvement
  • Add APIs
  • Add output options