pMap... The Silent Killer

BruCON 4, Ghent 2012
Gregory Pickett, CISSP, GCIA, GPEN
Chicago, Illinois

gregory.pickett@hellfiresecurity.com
Overview

- Stage Is Set
- Isolation Occurs
- Tensions Built
- Individuals
- End Game
See No Evil, Hear No Evil

ADMIT IT

When you shut off the lights in the basement, you get the fuck out of there.
Advertising

- Routers, Printers, Appliances, Windows, Apple, Linux, ... Everything?
- Broadcast and Multicast
- Resolve Names, Send Updates, Get Configuration, Find Services, Etc.
- It’s all about cooperation by sharing what you have
Listen to the "Crazy" guy
Implications

- Messaging to Educate Peers ... Can also Educate Attackers
- No Authentication ... Indiscriminate Distribution
- For Peer, Part of Cooperation
- For Attackers, Available Attack Surface
They travel in packs!
Underlying Protocol for Advertising
- Broadcasts and Multicast are over UDP
- Much of this traffic is server to server
- Server to Server ... fixed ports
- Unique Source and destination port pairs

<table>
<thead>
<tr>
<th>Source</th>
<th>SPort</th>
<th>Destination</th>
<th>DPort</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.234.63.160</td>
<td>47808</td>
<td>10.234.63.255</td>
<td>47808</td>
<td>BACnet-APDU</td>
</tr>
<tr>
<td>10.234.32.67</td>
<td>57621</td>
<td>10.234.63.255</td>
<td>57621</td>
<td>UDP</td>
</tr>
<tr>
<td>10.234.37.195</td>
<td>68</td>
<td>255.255.255.255</td>
<td>67</td>
<td>DHCP</td>
</tr>
<tr>
<td>10.234.32.36</td>
<td>138</td>
<td>10.234.63.255</td>
<td>138</td>
<td>BROWSER</td>
</tr>
<tr>
<td>10.234.36.199</td>
<td>1900</td>
<td>239.255.255.250</td>
<td>1900</td>
<td>SSDP</td>
</tr>
</tbody>
</table>
Asking for Directions...

NO TRESPASSING
VIOLATORS WILL BE SHOT
SURVIVORS WILL BE SHOT AGAIN
Multicast DNS (mDNS)

- **Name Resolution (Peer-to-Peer)**

- **Messages**
  - Same formats and operating semantics as conventional DNS
  - Based on "local" domain
  - Shared and unique records

- **Operations**
  - Queries and responses sent to 224.0.0.251
  - Utilizes UDP port 5353 for both resolvers and responders
Names

Device Type and Make

Name: eff-rsreagan.local
Type: A (Host address)
\(0.000\) = Class: IN (0x0001)
Time to live: 2 minutes
Data length: 4
Addr: 172.31.4.49 (172.31.4.49)

Name: bonnie-hoffman-adamss-iPod.local
Type: A (Host address)
\(0.000\) = Class: IN (0x0001)
Time to live: 2 minutes
Data length: 4
Addr: 172.31.3.103 (172.31.3.103)

Name: La-Toya-Rushs-iPhone.local
Type: A (Host address)
\(0.000\) = Class: IN (0x0001)
Time to live: 2 minutes
Data length: 4
Addr: 172.31.0.233 (172.31.0.233)

Name: Andrew-Stvrains-iPad.local
Type: A (Host address)
\(0.000\) = Class: IN (0x0001)
Time to live: 2 minutes
Data length: 4
Addr: 172.31.1.91 (172.31.1.91)
DNS Service Discovery (DNS-SD)

- Service Discovery (Peer-to-Peer)
- Works over standard and multicast DNS
- Fully Compliant
- Continuous Querying
- Shared “PTR” records
- Unique “SRV” and “TXT” records
## Services (SRV)

<table>
<thead>
<tr>
<th>Service: _tcp</th>
<th>Protocol: _tcp</th>
<th>Name: _tcp</th>
<th>Type: SRV</th>
<th>Weight: 0</th>
<th>Port: 22</th>
<th>Target: ti</th>
<th>Time to live: 2 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP 9200C</td>
<td>Protocol: _tcp</td>
<td>Name: _tcp</td>
<td>Type: SRV</td>
<td>Weight: 0</td>
<td>Port: 22</td>
<td>Target: ti</td>
<td>Time to live: 2 minutes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service: _tcp</th>
<th>Protocol: _tcp</th>
<th>Name: _tcp</th>
<th>Type: SRV</th>
<th>Weight: 0</th>
<th>Port: 22</th>
<th>Target: ti</th>
<th>Time to live: 2 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSC Servers</td>
<td>Protocol: http</td>
<td>Name: _tcp.local</td>
<td>Type: SRV</td>
<td>Weight: 0</td>
<td>Port: 22</td>
<td>Target: ti</td>
<td>Time to live: 2 minutes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service: _tcp</th>
<th>Protocol: _tcp</th>
<th>Name: _tcp</th>
<th>Type: SRV (Service location)</th>
<th>Weight: 0</th>
<th>Port: 22</th>
<th>Target: ti</th>
<th>Time to live: 2 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reno._tivo-videos._tcp.local</td>
<td>Protocol: tivo-videos</td>
<td>Name: _tcp.local</td>
<td>Type: SRV (Service location)</td>
<td>Weight: 0</td>
<td>Port: 22</td>
<td>Target: ti</td>
<td>Time to live: 2 minutes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service: _tcp</th>
<th>Protocol: _tcp</th>
<th>Name: _tcp</th>
<th>Type: SRV</th>
<th>Weight: 0</th>
<th>Port: 22</th>
<th>Target: ti</th>
<th>Time to live: 2 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA-0643AA_b1</td>
<td>Protocol: ra</td>
<td>Name: _tcp</td>
<td>Type: SRV (Service location)</td>
<td>Weight: 0</td>
<td>Port: 22</td>
<td>Target: ti</td>
<td>Time to live: 2 minutes</td>
</tr>
</tbody>
</table>

**Ports**
Device Type and Operating System

Device Type and Make

Model
Simple Service Discovery Protocol (SSDP)

- Service Discovery (Peer-to-Peer)
- Messages
  - HTTP over UDP
  - Methods for Advertisement and Discovery
  - Using SSDP-Specific Header Fields
- Operations
  - Notifications and Searches sent to 239.255.255.250 or 239.255.255.177
  - Utilizing UDP port 1900
Notifications (Location, Server)

Device Type, Make, and Operating System

| Server: | Linux/3.0.15-554452-user UPnP/1.0 CyberLinkJava/1.8 |
| Cache-Control: | max-age=310 |
| Cache-Control: | max-age=900 |
| Server: | Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0 |
| OPT: | "http://schemas.upnp.org/upnp/1.0/" ns-01 |
| 01-NSL: | 6b44de51ec3be5d1ca7c41592e93d |

Ports

Device Type, and Operating System
Ominous Fog...
Limitations

- **Broadcast and Multicast**
  - Listening (Layer-2 Boundaries)
    - Broadcast Domain
    - VLAN containment

- **Multicast**
  - Routers between the recipient and the source must be multicast enabled

- **mDNS**
  - Querying (Link-Local Response Only)
    - Responses only accepted from local-link
    - Responses only sent to the local-link
Defenders Aren't Interested...
Typical Perspective

- This is just Noise
- These hosts are behind a firewall
- Something Will Break!
Reign of Terror Begins!

SLAYING IN THE RAIN
What a glorious feeling
Attacker Introduced
pMapv1.00 for Windows

- Discovery, Scanning, and Fingerprinting via Broadcast and Multicast traffic
- Device Type, Make, Model, Service Configuration, and Versions
- Nmap-like output
- Stand-Alone or Agent Modes
- Metasploit script
Stalking The Prey...
First to Go
Demonstration (Local)
Demonstration (Remote)
Will They See Him Coming?
Detections

- Intrusion Detection/Prevention Systems
- Etherape
- Netflow/StealthWatch
Chase Begins
What Obstacles Are There?
Defenses

**Network**
- Firewalls
- Network Access Control
- Access Control Lists
- VLANs

**End-Point**
- Anti-Virus/Anti-Spyware/Anti-Spam
- Firewalls and Port Blocking
- Intrusion Prevention System
- Application Control
They run... but they can't get hide
Next to Die...
Demonstration (Factory)
Demonstration (Hotel)
Demonstration (Mall)
Killing Starts!
With This Foundation...

- Go Active ... Poke and Probe
- Exploit and Compromise
- Gain Footholds
- Continue The Fun
And The Attacker Is ...
Final Thoughts

- Hosts are now actively advertising their available attack surfaces
- Great for passive information gathering
- Information that can be used to discover, scan, and fingerprint them
- Making later targeting and attacking easier
pMap v1.00 for Windows
SHA-1: 4de0ac59f58f2b40e1efb6ea97c3fe264761bced

pMap v1.00 for Metasploit
SHA-1: 96251945997c2838d464c9d4059ad4456dd8c013

Updates → http://www.hellfiresecurity.com