pMap ... The Silent Killer



BruCON 4, Ghent 2012



Hellfire Security

Gregory Pickett, CISSP, GCIA, GPEN Chicago, Illinois

gregory.pickett@hellfiresecurity.com

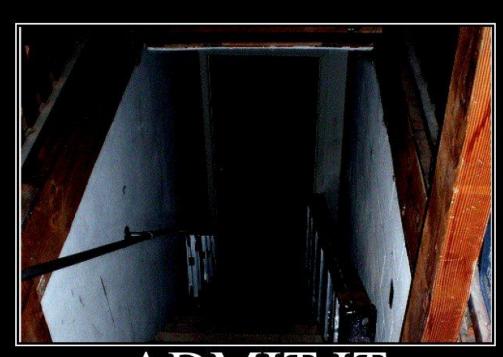


Overview

- 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!





UDP

- 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

Source	SPort	Destination		Protocol
10.234.63.160	47808	10.234.63.255	47808	BACnet-APDU
10.234.32.67	57621	10.234.63.255	57621	UDP
10.234.37.195	68	255.255.255.255	67	DHCP
10.234.32.36	138	10.234.63.255	138	BROWSER
10, 234, 36, 199	1900	239, 255, 255, 250	1900	SSDP

Device Type











Asking for Directions . . .





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

```
⊟ eff-rsreagan.local: type A, class IN, cache flush, addr 172.31.4.49
   Name: eff-rsreagan.local
   Type: A (Host address)
                                                                    Device
   .000 0000 0000 0001 = Class: IN (0x0001)
   1. . . . . . . . . = Cache flush: True
                                                                    Type and
   Time to live: 2 minutes
   Data length: 4
                                                                    Make
   Addr: 172.31.4.49 (172.31.4.49)
■ bomnie-hoffman-adamss-iPod.local: type A, class IN, cache flush, addr 172.31.3.103
    Name bonnie-hoffman-adamss-iPod.local
    Type: A (Host address)
    La-Toya-Rushs-iPhone.local: type A, class IN, cache flush, addr 172.31.0.233
       Name: La-Toya-Rushs-iPhone.local
       Type: A (Host address)
       .000 0000 0000 0001 = class: IN (0x0001)

= Andrew-StVrains-iPad.local: type A, class IN, cache flush, addr 172.31.1.91
            Name : Andrew-StVrains-iPad. local
            Type: A (Host address)
            .000 0000 0000 0001 = Class: IN (0x0001)
            1... - cache flush: True
            Time to live: 2 minutes
            Data length: 4
            Addr: 172.31.1.91 (172.31.1.91)
```

Name



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)

```
■ MSC Servers (MAC000FE500039D)._http._tcp.local: type SRV

⊨ hp 9200C Dig = timur._ssh._
                               Service: SC Servers (MAC000FE500039D)
   Service: p
                 Service: i
                               Protocol: http
   Protocol:
                 Protocol:
                               Name: _tcp.local
   Name: _tcp
                 Name: _tcp
                               Type: SRV (Service location)
   Type: SRV
                 Type: SRV
   .000 0000
                               .000 0000 0000 0001 = class: IN (0x0001)
                 .000 0000
                               1... ....
                 1...
                               Time to live: 2 minutes
   Time to li
                 Time to li
   Data lengtl
                 Data lengt
   Priority:
                 Priority:
   Weight: 0
                 Weight: 0
   Port:(21)
                 Port: (22)
                                                                    MOUSESTERMENT
   Target: NP
                 Target: ti
BA-0643AA._bla 0024369BE274@d Reno._tivo-videos._tcp.local: type SRV, class IN
   Service: A-0
                   Service: 024
                                  Service: eno
   Protocol: b
                                  Protocol: tivo-videos
                  Protocol: ra
   Name: _tcp.
                  Name: _tcp.1
                                  Name: _tcp.local
   Type: SRV (
                                  Type: SRV (Service location)
                  Type: SRV (S
   .000 0000 00
                   .000 0000 00
                                  .000 0000 0000 0001 = class: IN (0x0001)
                                  1... .... ...
   Time to live
                  Time to live
                                  Time to live: 2 minutes
   Data length:
                  Data length:
                                  Data length: 13
   Priority: 0
                  Priority: 0
                                  Priority: 0
   Weight: 0
                  Weight: 0
                                  Weight: 0
   Port: (4301)
                  Port: (5000)
                                  Port: (8101)
                  Target: dave
   Target: BA-
                                  Target: Reno.loca
```

Ports



Services (SRV, TXT)

```
⊕ PO6LC872652._ipp._tcp.local: type_SRV, class IN, cache flush, priority 0, weight 0

■ P06LC872652._ipp._tcp.local: type TXT, class IN, cache flush

   Name: PO6LC872652._ipp._tcp.local
   Type: TXT (Text strings)
                                                           Device Type
   .000 0000 0000 0001 = class: IN (0x0001)
   Make and Model
   Time to live: 4 minutes
   Data length: 255
   Text: txtvers=1
                                                           Service Setup
   Text: qtotal=1
   Text: pdl=application/postscript,application/vnd.hp-PCL,application/vnd.hp-PCLXL
   Text: rp=p061c872652
   Text: ty=HP Color LaserJet 4700
   Text: product=(HP Color LaserJet 4700)
   Text: priority=60
   Text: adminurl=http://p06lc872652.local.
   Text: note=AP14B (Erika Rivera)
   Text: Transparent=T
  ■ Reno._tivo-videos._tcp.local: type TXT, class IN, cache flush
     Name: Reno._tivo-videos._tcp.local
                                                       Device Type and Make
     Type: TXT (Text strings)
     .000 0000 0000 0001 = class: IN (0x0001)
                                                       Version
     Time to live: 1 hour, 15 minutes
                                                      Service Setup
     Data length: 98
     Text: swversion=1.95a
     Text: path=/TiVoConnect?Command=QueryContainer&Container=%2fian_FileVideo
     Text: protocol=http
 ⊞ Remo._tivo-videos._tcp,local: type SRV, class IN, cache flush, priority 0, weight 0
```



Services (SRV, TXT)

Device Type

and

Operating

System

```
timur [00:1c:c4:ad:2b:1c] workstation._tcp.local: type SRV, class IN
    Service: imur [00:1c:c4:ad:2b:1c]
    Protocol: workstation
    Name: _tcp.local
    Type: SRV (Service location)
    .000 0000 0000 0001 = Class: IN (0x0001)
    1..... = Cache flush: True
    Time to live: 2 minutes
    Data length: 14
    Priority: 0
    Weight: 0
    Port: 9
    Target: timur.local
```

```
□ Litterbox _device-info._tcp.local: type TXT, class IN

Name: Litterbox._device-info._tcp.local

Type: TXT (Text strings)

.000 0000 0000 0001 = class: IN (0x0001)

0... ... = Cache flush: False

Time to live: 1 hour, 15 minutes

Data length: 20

Text: model=MacBookPro8,1

Model
```



Simple Service Discovery Protocol (SSDP)

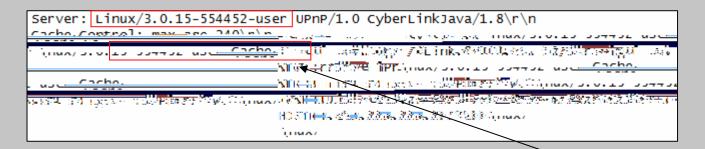
- Service Discovery (Peer-to-Peer)
- Messages
 - HTTP over UDP
 - Methods for Advertisement and Discovery
 - Using SSDP-Specific Header Fields
- Operations
 - Notifications and Searches sent to 239.255.255.250 or 239.255.255.177
 - Utilizing UDP port 1900





Notifications (Location, Server)

Device Type, Make, and Operating System



Host:239.255.250:1900\r\n
NT:upnp:rootdevice\r\n
NTS:ssdp:alive\r\n
Location:http://10.152.31.27:2869/upnphost/udhisapi.dll?content=uuid:
USN:uuid:fc0107a7-3065-4046-b427-bdf205f6086d::upnp:rootdevice\r\n
Cache-Control:max-age=900\r\n
Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
OPT:"http://schemas*upnp.org/upnp/1/0/"; ns=01\r\n
01-NLS:6b44dde51ec3be55de1ca7c41592e93d\r\n
\r\n

Device Type, and Operating System

Ports



Ominous Fog . . .





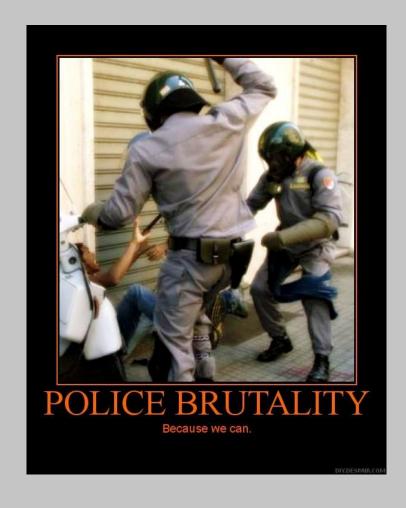
Limitations

- 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!

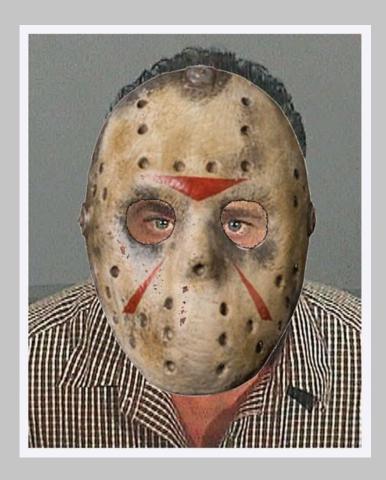


Reign of Terror Begins!





Attacker Introduced





pMap v1.00 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



Demonstration (Basic Usage)





Stalking The Prey . . .





First to Go ...





Demonstration (Local)





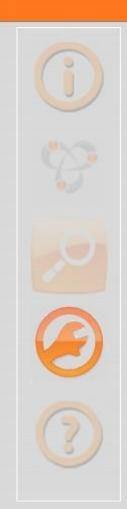
Demonstration (Remote)





Will They See Him Coming?





Detections

- Intrusion Detection/Prevention Systems
- **#** Etherape
- Netflow/StealthWatch





Chase Begins





What Obstacles Are There?





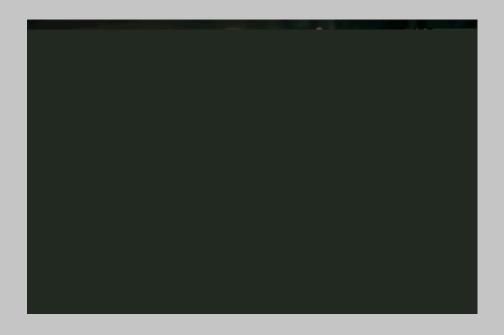
Defenses

- 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



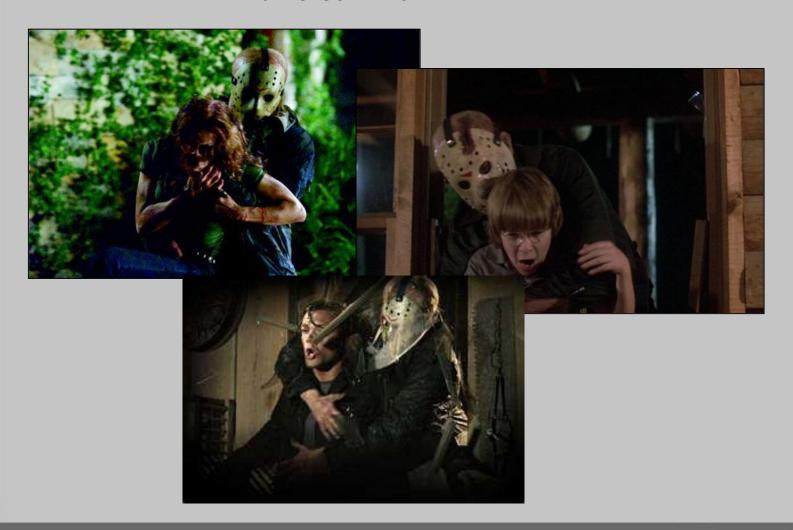


They run . . . but they can't get hide





Next to Die ...





Demonstration (Factory)





Demonstration (Hotel)



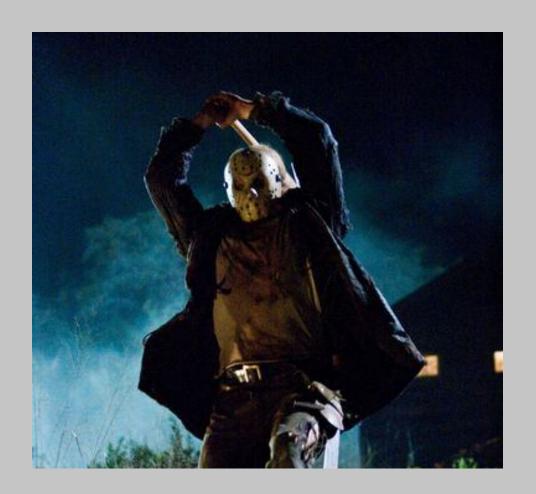


Demonstration (Mall)





Killing Starts!



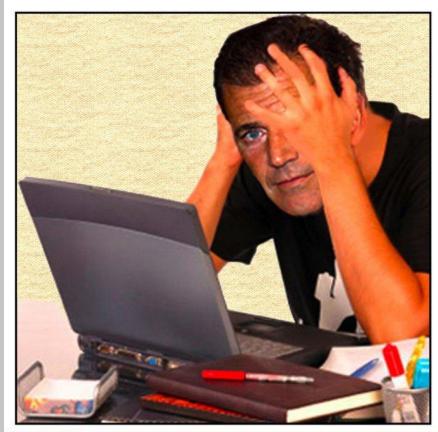


With This Foundation . . .

- Go Active ... Poke and Probe
- Exploit and Compromise
- Gain Footholds
- Continue The Fun



And The Attacker Is ...



FreakingNews.com



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



Tools

- pMap v1.00 for WindowsSHA-1: 4de0ac59f58f2b40e1efb6ea97c3fe264761bced
- pMap v1.00 for Metasploit
 SHA-1: 96251945997c2838d464c9d4059ad4456dd8c013

Updates → http://www.hellfiresecurity.com



