FingerBank - open DHCP fingerprints database

no it's not about a bank of fingers...

Presentation Plan

- Device fingerprinting, passive fingerprinting, DHCP fingerprinting
- Defensive use cases
- Offensive use cases
- FingerBank announcement
- FingerBank's future

Who I am

Olivier Bilodeau

- System architect working at Inverse inc
- PacketFence lead developer since 2009
- Teaching InfoSec to undergraduate in Montreal
- ...

  new father, Open Source nuts, enjoying CTFs a lot, android developer, brewing beer

Social stuff

- twitter: **@packetfence** / identi.ca: **@plaxx**
- delicious: **plaxxx** / linkedin: **olivier.bilodeau**

Device fingerprinting reminder

Identifies software or hardware components

Various types

- Operating Systems
- Devices
- Browsers
- Web Server
- Web Applications

Two approaches of gathering fingerprints

- Active
  - Pros: On demand
  - Cons: Detectable, sometimes intrusive
- Passive
  - Pros: Stealth
  - Cons: not on demand

Passive fingerprinting reminder

- Networks are really noisy
- Some protocols use broadcast
- Just wait for the goods to come to you
- LAN fingerprinting

  mDNS, TCP, ARP, DHCP, ...
- WAN fingerprinting

  honeypots

DHCP Fingerprinting reminder

- The pervasiveness and broadcast nature of DHCP makes it compelling
- IP Helpers (UDP Helper Address) makes it very easy to collect centrally
- Rarely spoofed

DHCP Fingerprinting reminder (contd.)

DHCP Elements to fingerprint

- DHCP retransmission timing (actual vs in packet)
- IP TTL on DHCP packets
- DHCP Options (55: requested parameters, 60: vendor id, ...)
- Number and order of option 55 is particularly precise and interesting

Defensive Use Cases

- Easy Operating System Inventory
  - Even more powerful if IP-Helpers use DHCP Option 82
- NAC integration to blacklist end-of-life OS
  - ex: Win 2000 and earlier
- NAC integration to automatically allow dumb devices (shh!)

Offensive Use Cases

- Stealth LAN Recon!
- ...
- Any other ideas?

Why FingerBank?

- There are User-Agent databases out there
- There are snort signature databases out there
- What about DHCP Fingerprints?
- Consolidate information hidden in silos
- Regroup communities that would benefit from sharing this information
- Raise awareness about this easy to use technique

What is FingerBank?

A website dedicated to sharing DHCP fingerprint and tools.

- Two extensive DHCP fingerprint databases (PacketFence, Satori)
- DHCP fingerprinting tools
- Mailing list

Who's backing FingerBank?

- Eric Kollman - Satori
- David LaPorte - PacketFence founder
- Olivier Bilodeau - PacketFence lead developer

FingerBank's future

Based on community participation

- Improve fingerprint sharing tools
- Consolidate data formats
- Room for new tools
  - a pentester oriented one
- Support and share about new passive fingerprint types?

That's it

I hope you enjoyed! See you in the debriefing room.

twitter: **@packetfence** / identi.ca: **@plaxx**

delicious: **plaxxx** / linkedin: **olivier.bilodeau**

References

- DHCP Fingerprinting
  - Using DHCP for Passive OS Identification, BlackHat Japan 2007, David LaPorte, Eric Kollmann, http://myweb.cableone.net/xnih/download/bh-japan-laporte-kollmann-v8.ppt
- Users of current DHCP Fingerprint databases
  - PacketFence, http://www.packetfence.org
  - Satori, http://myweb.cableone.net/xnih/
- Other fingerprinting tools
  - nmap, http://www.nmap.org/
  - Blind Elephant, http://TODO
  - p0f, http://TODO
  - SinFP, http://TODO
- Inspiration
  - Browser ID Strings, http://www.zytrax.com/tech/web/browser_ids.htm
  - Emerging Threats, http://www.emergingthreats.net