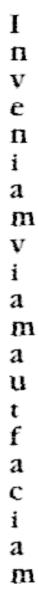
Passive Reconnaissance





"What is it?"

- Reconnaissance is defined as ... noun: the act of reconnoitring (especially to gain information about an enemy or potential enemy);
- Passive is generally descripted as unresponsive, inert
- The two concepts together mean to get something by doing nothing
- Remarkably easy

n



"History"

- Passive recon has been around as long as computers shoulder surfing
- Networking made it easier hubs / switches
- TCP made it easier broadcast traffic
- Tools made it easier pof / ettercap / wireshark / etc
- Progress has not diminshed the problem, only made it worse



"How is it done?"

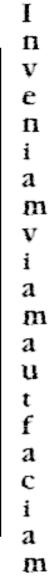
- Enable a network interface
- Do not give it a IP address
- Fire up tool of choice
- Watch what goes past
- You could use a SPAN/mirrored port
- You could use network tap device
- You could use a custom cable



"How bad is it?"

• Ummm Very!

<demo>





"Left field thoughts on passive recon"

- Blinken-lights what do you give away?
- Typing paterns what do you give away?
- Wireless could passive recon be any easier?
- Google not quite but close
- Firewall usage sorry I do not talk to windows machines
- Masquerading changing your profile
- Tempest hmmmm...
- Quantum crypto we can see you watching

 \mathbf{n}



Thank you for your attention

 $P0f - \underline{http://lcamtuf.coredump.cx/p0f.shtml}$

Ettercap - http://ettercap.sourceforge.net/

Linkcat - http://www.doxpara.com/paketto/

Tepreplay - http://tepreplay.synfin.net/

Networkminer - http://sourceforge.net/projects/networkminer/

Wireshark - http://www.wireshark.org/

n m

