VIGILAR

Your Trusted Partner In Information Security®

VoIP Penetration Testing: Lessons Learned, Tools and Techniques

Jason Ostrom
Sr. Security Consultant

John Kindervag, CISSP, QSA
Sr. Security Architect

www.vigilar.com

Why?

- Low Awareness as to Security Threats to VoIP
- Publicly Accessible IP Phones
  - Waiting Areas
  - Conference Rooms
  - Hotel Rooms
- How easily can an Attacker Gain Privileged Access?

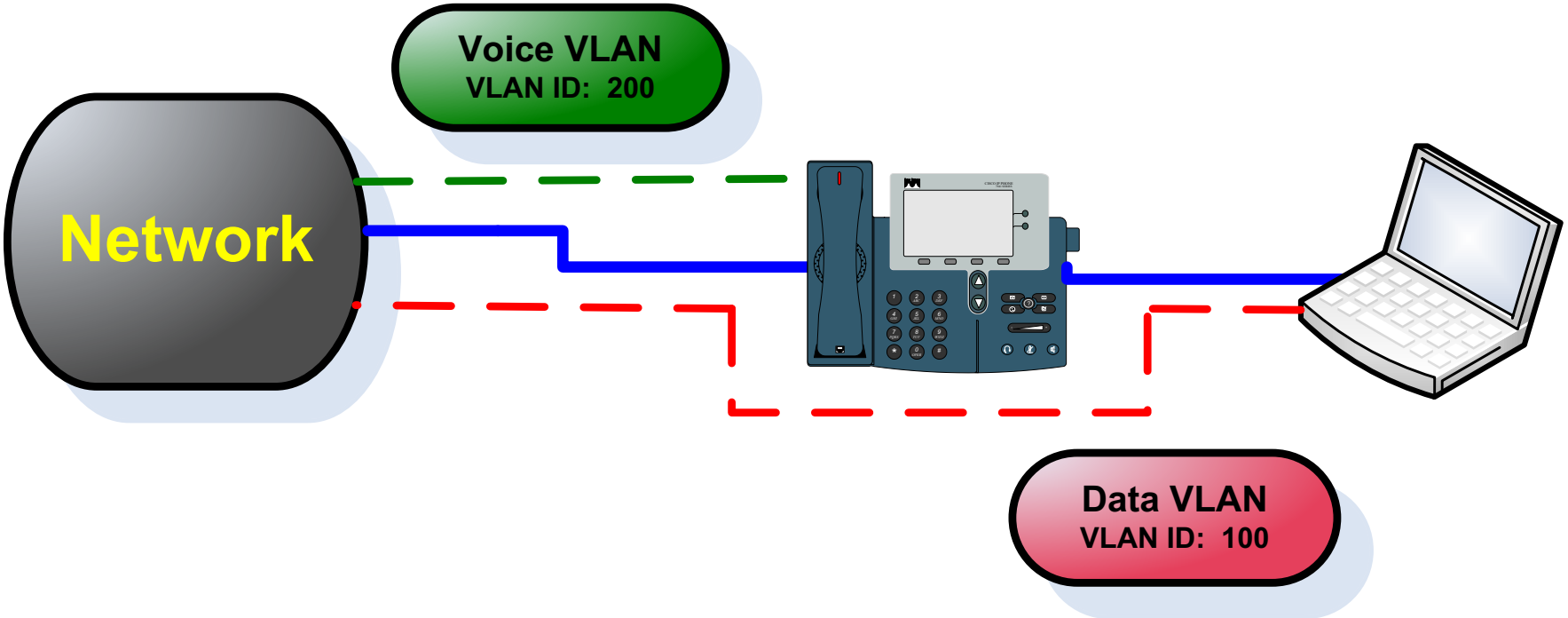
Voice VLAN

Legend

Ethernet Cable

Data Traffic

Voice Traffic



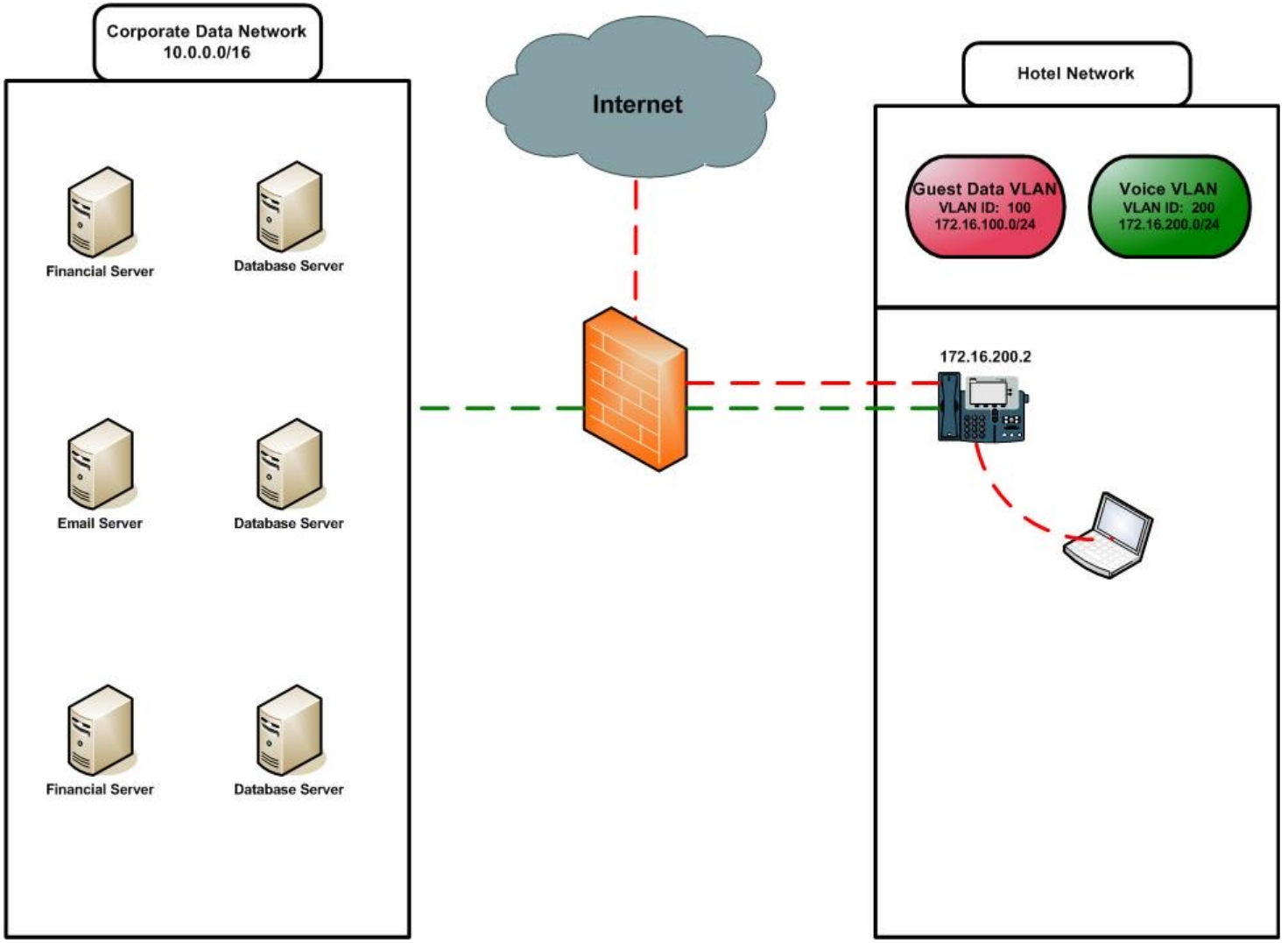
VIGILAR

Your Trusted Partner In Information Security®

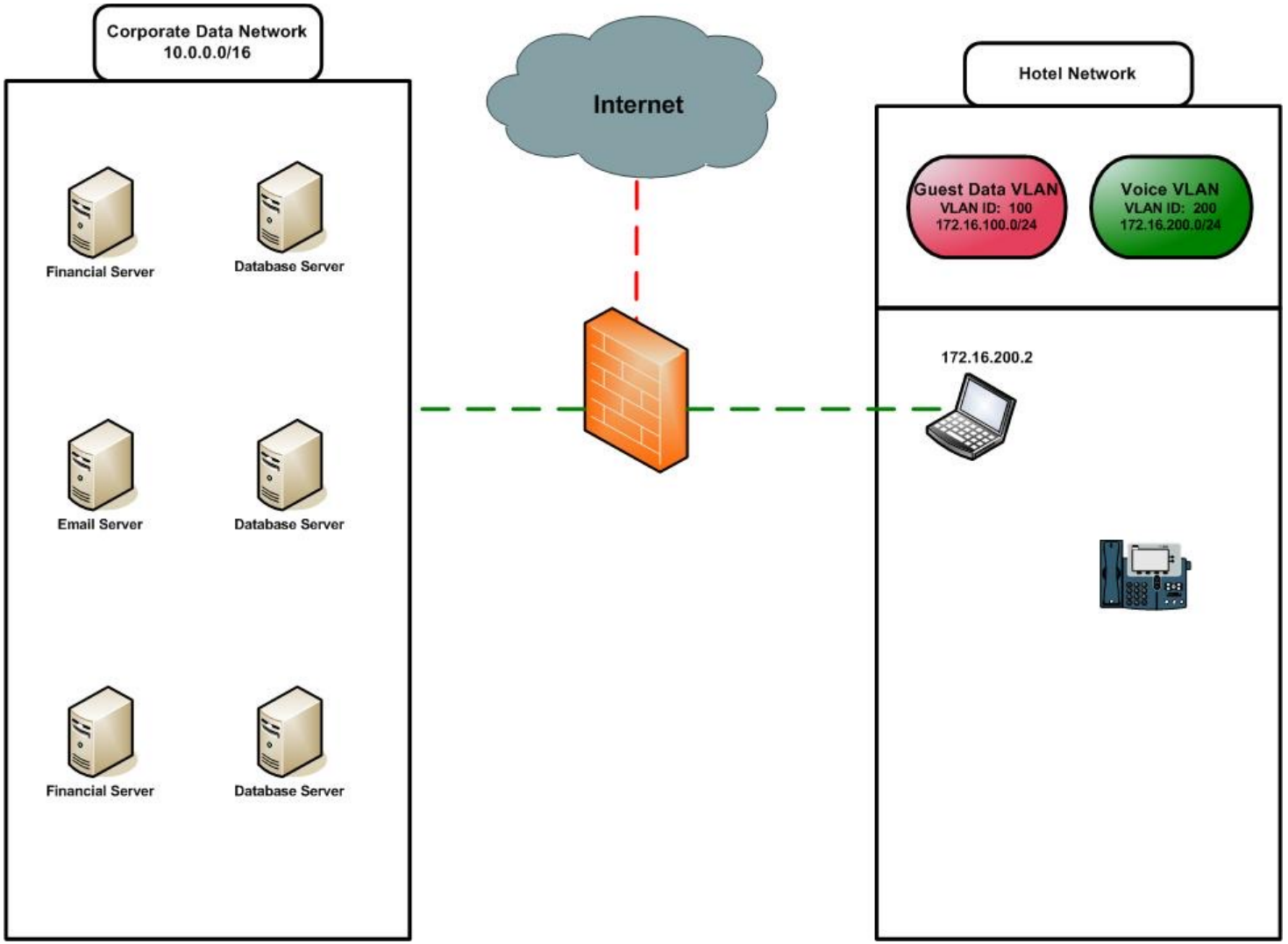
Live Demonstration

www.vigilar.com

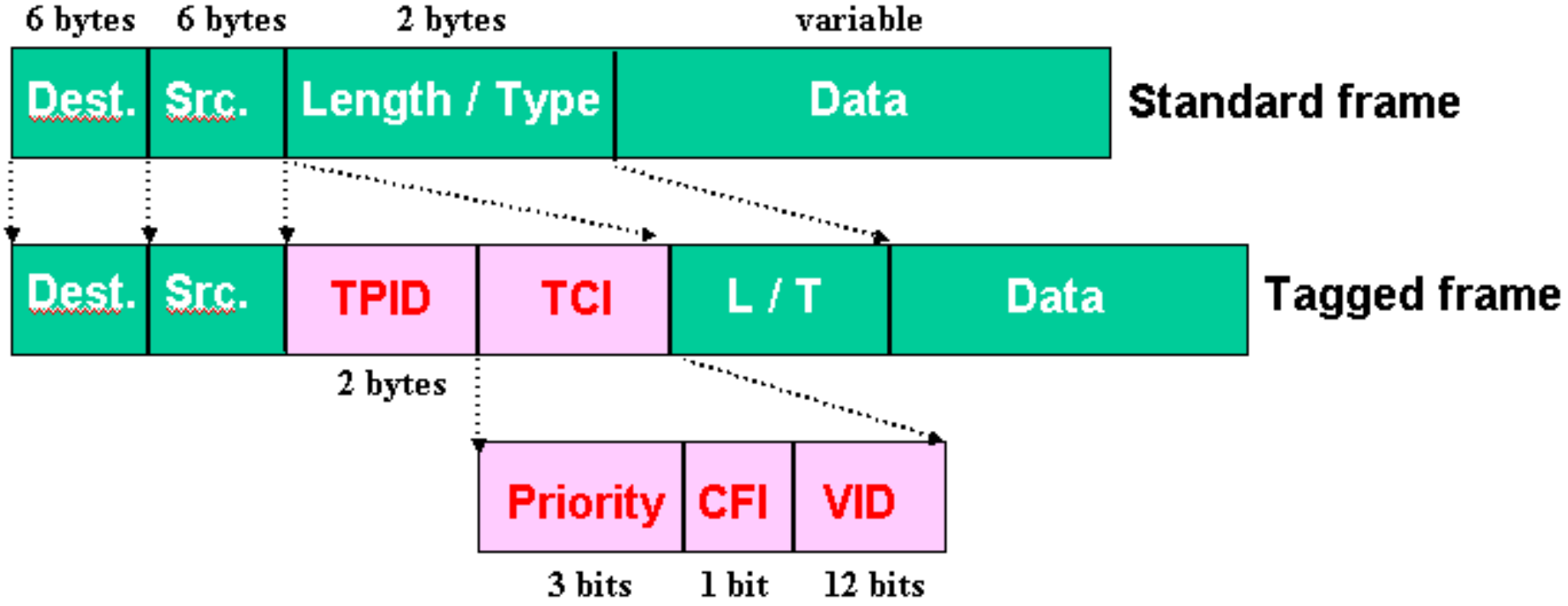
Customer VoIP Network



How this happens



Create a new VLAN Interface on the PC



VoIP Hopper:
Jumping from one VLAN to the Next!

A look at automating the collection of small information tokens and VLAN Hopping that can allow exploitation of VoIP Networks.

VoIP Hopper Information

- Project Download – http://voiphopper.sourceforge.net
- Security Focus Article
- http://www.securityfocus.com/infocus/1892

Q&A

Contact Information

Jason Ostrom, CCIE Security #15239, QSA
Sr. Security Consultant
jostrom@vigilar.com

John Kindervag, CISSP, QSA
Sr. Security Architect
jkindervag@vigilar.com

If you would like a copy of this presentation please contact:

marketing@vigilar.com