

# *Project Dreddnaught*



# *Part 1: The Opening Act*

“Please Captain, not in front of the Klingons.”  
-- Spock, Star Trek V: The Final Frontier

# *Basics of Network Security*

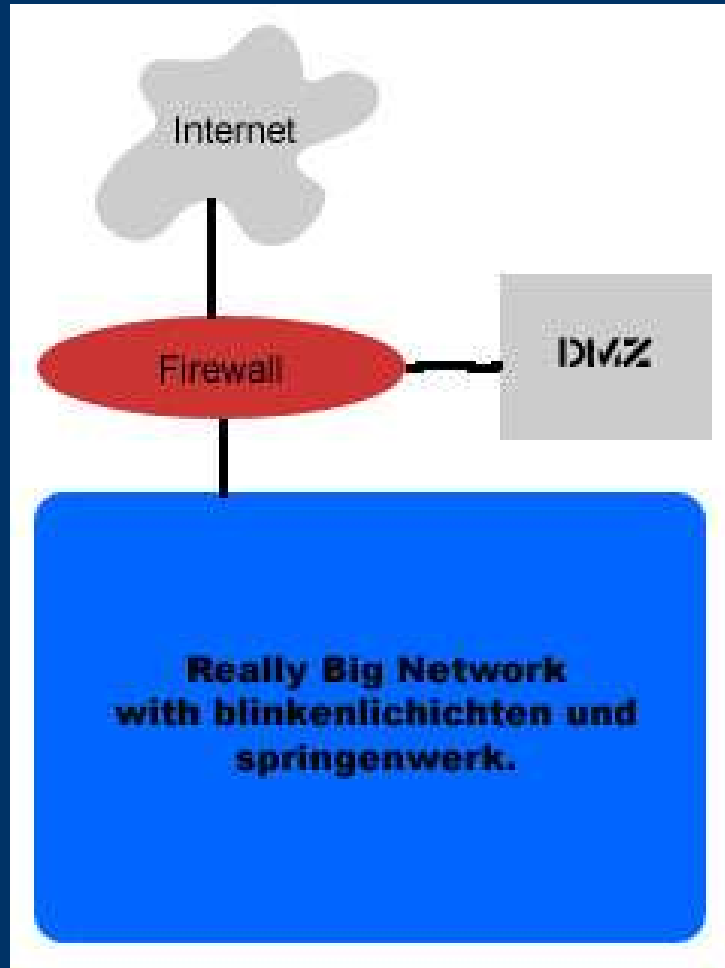


The Onion Model

Security Through  
Layers

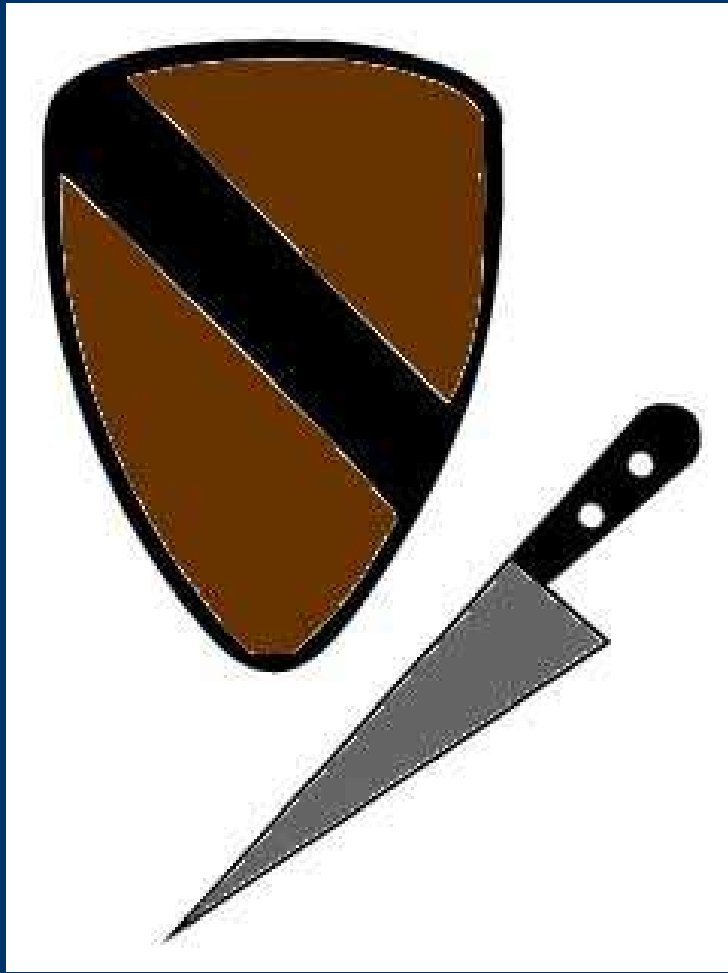


# Network Layer



- Firewalls.
- DMZ.
- Virtual Private Networking.

# ***CONSTANT VIGILANCE!*** ***(The Layer of Infinite Paranoia)***



- Intrusion Detection.
- Log Monitoring.
- Probing Mechanisms.
- Host Integrity Monitoring.
- Data Collection and Analysis.

# System Layer



- Good Passwords and Security Policies.
- Up-to-date Software.
- Installing Operating System Patches and Updates.
- Learning How to “Herd Cats.”

## *Part 2: The Big Show*

“Klingons never do anything small, do you?”  
-- Commander Riker, Star Trek: Insurrection

---

---

# *Project Dreddnaught*



## *Part 3: The Hidden Agents*

“The crew has responded with the dedication I've come to expect from them... And like a thousand other commanders on a thousand other battlefields, I wait for the dawn.”

--Captain Jean-Luc Picard, *Star Trek: Nemesis*

---

---

# *Loyoppix:S*

Loyoppix:S is a GNU/Linux distribution that boots and runs completely from cd. This distribution features Snort 2.4.2 and a few other network security tools.

Available for download at:  
<http://webpages.cs.luc.edu/~loyoppix/>

---

---

## *Part 4: The Silent Audience*

“It'll be nice to have a first contact where no-one's thinking about charging weapons.”  
--Commander Tucker , Enterprise

# *Passive Ethernet Tap*

- Creates permanent access for passive monitoring.
  - Monitoring device sees the same traffic as if it were in-line.
  - Render the attached monitoring device invisible to the network, eliminating it as an attack target for certain network attacks.
- 
-