CDnetsec.com

Intrusion Prevention System Evasion Techniques

Thomas Wilhelm

Security Consultant

- Education
  - Masters Degrees in:
    - Computer Science
    - Management
- Author since 2007
  - Professional Penetration Testing
  - Ninja Hacking
  - Netcat Power Tools
  - Penetration Testing's Open Source Toolkit, V2
- Certifications
  - ISSMP, CISSP, SCSECA, SCNA, SCSA, IEM/IAM

John Spearing

Operations Manager @ Crystal Defense

- Education
  - Masters Degrees:
    - Computer Science
    - Organizational Behavior
- Co-Founder and Operations Manager for "Crystal Defense Network Security Solutions"
  - MSSP on the Colorado Front Range

Why are you here?

- Learn to identify and evade an Intrusion Prevention System
- Understand how an IPS is typically deployed, and identify non-typical deployments
- Rules, rules, rules
- COTS IPS systems

What do you need?

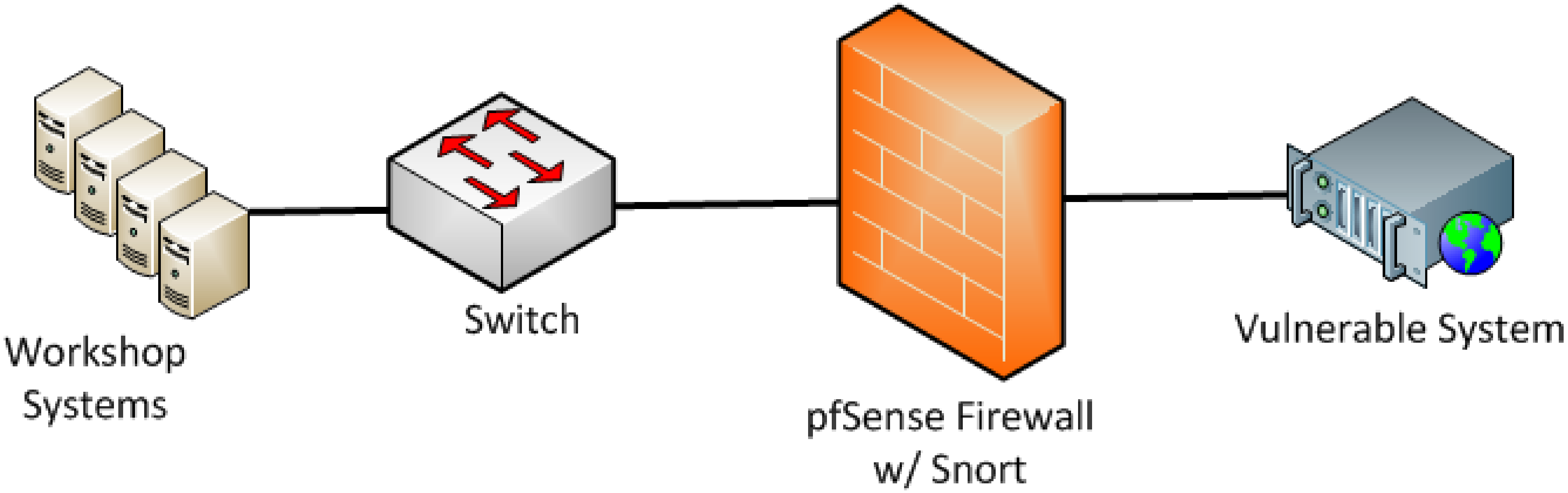
- Pre-installed Kali Linux
  - Prefer to have it as the main OS, not virtualized
- CAT5 cable of sufficient length
  - We didn't know in advance how the rooms would be, so please bear with us when we get everyone connected
- Patience
  - 4 hours, 4 tasks, a LOT of network congestion
  - This is a HOSTILE NETWORK!!

How this workshop will… work

- Do / Don't
  - Everyone is here to learn, so don't impede others
  - Embrace other people's genius
  - Workshop = Group Effort, work as a team
  - Workshop != Taking over someone else's keyboard
  - We're here to learn, not be pedantic over terms
  - 99% will be done via shared screen – please make sure you can see the presentation

About the Lab

- Lab configuration for the workshop



Agenda

- COTS IDS/IPS products
- Rules
- Encryption and tunneling
- Timing attacks
- Traffic manipulation
- Resource consumption*

Hands-On Lab

Let’s begin!

Thanks for Joining Us!

- Any feedback, please send to: info@CDnetsec.com