Brief Intro

- Who am I?
  - I’ve been in the IT industry for about 12 years
  - Worked with firewall systems for 6 years
  - Worked in both the public and private sections
What is a firewall?

- A firewall is a device that is installed at a junction point and is used to limit network traffic between networks.
Firewall Types

- Packet Filtering Firewalls
- Application (Proxy) Firewalls
- Stateful Inspection Firewalls
- Dynamic Packet Filtering Firewalls
- Kernel Proxy
Firewall Auditing Methodology

Phases

- Gather Documentation
- The Firewall
- The Rule Base
- Testing and Scanning
- Maintenance and Monitoring
Defining Scope

- Documentation
- Firewall Access
- Firewall Rule Base
- Approval Procedures
- External Testing
- Internal Testing
Phase I - General Documentation

- Security Policy
- Change Procedures
- Administrative Controls
- Network Diagrams
- IP Address Scheme
- Firewall Locations
Phase I - Firewall Documentation

- Firewall Vendor
- Software Version and Patch Level
- Hardware Platform
- Operating System Version and Patch Level
Phase II – The Firewall

- Access including physical
- Administrator training and knowledge
- Authentication
- OS Hardening
Phase III – The Rule Base

- Based on the Organization’s Security Policy
- Simplicity is the key
- Review each rule
  - Business reason
  - Owner
  - Host devices
  - Service Ports
- Most restrictive and least access stance
- Rule order
- Administration Rule
- ICMP Rule
- Stealth Rule
- Cleanup Rule
- Egress Rules
- Logging
Phase IV – Testing & Scanning

- Determine & Set Expectations
- Scan the firewall
- Scan host behind the firewall
- Ensure results match expectations
Phase V – Maintenance & Monitoring

- Change Management and Approval
- Log Review
- Disaster Recovery Plan
- Incident Response
- Backup and Recovery Procedures
- Log Storage
Firewall Rule Base Demo
Questions???
References and Additional Resources

- The CISSP Prep Guide
  - Ronald L. Krutz & Russell Dean Vines
  - Wiley Publishers
- Lance Spitzner’s
  - www.spitzner.net
  - White Paper - Auditing your Firewall Setup
  - White Paper - Building your Firewall Rule base
- Dameon D. Welch-Abernathy
  - www.phoneboy.com
  - Checkpoint Firewall-1/VPN-1 Resource site
- Checkpoint Technologies
  - www.checkpoint.com
- VicomSoft
  - www.firewall-software.com
  - White Paper - Firewall