



Positive Thinking

Strategy for Information Security



About Me

- Chris Byrd, CISSP, CCNA certified
- Senior Security Administrator
- Laclede Gas Company
- cbyrd@lacledegas.com



What we will cover

- What is Positive Thinking in Security?
- A short history of firewalls
- Host-based security
- Demonstrations



What is Positive Thinking?

- Enumerating Good instead of Bad
- Enumerating Bad is the same idea as “default permit”
- Understanding your business and technology environment



Why this is important

- Information Security is a chess game against many opponents
- While IT Security Spending has increased...
- So has the number of successful attacks



Demonstrations

- We will use Metasploit framework and Auditor CD
 - Metasploit is a framework for penetration testing
 - Auditor CD includes many utilities for pen-testing
- Simulated network for ACME Industries



How We Got Here

- Security Vendors sell products on features other than Security
- Security is viewed as something that should be non-interruptive to business
- Users don't notice security when it works



A Short History of Firewalls

- NAT/Packet Filtering
- Application Proxy
- Stateful Inspection
- Deep Packet Inspection
- Intrusion Prevention Systems

Packet Filtering

- Simple idea, but it worked
- Basic premise of packet filtering:
 - Allow the known good, block everything else
- Applications existed which defied simple packet filtering
 - FTP
 - Opens a control channel back to the initiator



Stateful Inspection

- Adds state tracking to the packet filter firewall
- Contains protocol specific handlers
- Often configured with a “permit any outbound” rule



Stateful Inspection Cons

- Although stateful inspection firewalls are a “enumerate good” technology when properly configured...
- Individual rules are “open highways” that do not validate traffic



Demonstration – Stateful inspection

- Exploit IIS .printer buffer overflow
- Meterpreter return traffic on 80



Application Proxy

- Hosts do not communicate through the firewall, but to the firewall
- Limits request to standard compliance
- Limited to the supported protocols



Demonstration – Application Proxy

- Exploit IIS .printer buffer overflow
- Meterpreter return traffic on port 80

- Exploit IIS .printer buffer overflow
- Passivex return traffic



DPI/IPS

- Combines Stateful Inspection firewall with signature based detection
- Tries to identify the “bad”
- High rate of false positives...
- Or high rate of false negatives



Host Based Security

- Anti-Malware
 - Anti-Virus
 - Anti-Spyware
- Host-based firewalls
- HIPS



Anti-Malware

- Fundamentally negative rules
- Requires constant updating
- Some vendors have switched to hourly
- Misses new attacks



Demonstration – Anti-Virus

- SpearPhishing using executable
- Passivex payload



Anti-Malware

- Statistics



Application Monitoring

- In some ways, opposite of Anti-Virus
- Identifies good applications
- Use a learn mode to determine what exists in user population
- Can monitor application hooking – using a good app to do bad things



Demonstration – App Monitoring

- SpearPhishing using executable
- Passivex payload



Software development

- Positive thinking done during planning, not development
- Identify all possible user input



Desktop Security

- Do they really need to:
 - Manage their screensaver
 - Install applications
 - Install new devices
- Desktop security is another place for “deny all”