NETWORK SECURITY

Scott Hand
Melanie Rich-Wittrig
Enrique Jimenez
Chapter 2

...In Which Firewalls Are Erected, Packets Are Snorted, And Pwnage Denied
TOPICS COVERED

- Host Software Firewalls – iptables
- Network Firewalls – pfSense
- Intrusion Detection Systems – Security Onion
- Web Firewall – mod_security
EXAMPLE NETWORK ARCHITECTURE

- **DMZ**
- **External Network**
- **Internal Network**
- **IDS**
- **Network Firewall**
- **Reverse Proxy**
- **Web Firewall**
- **Internet User**
- **Web/Mail/etc. Servers**
- **DMZ**
- **Host Firewall**
- **Internal Network**
- **Internet**
- **External Network**

**Diagram Components:**
- **Internal Users**
- **Internal Network**
- **Internet User**
- **Internet**
SETTING UP YOUR ENVIRONMENT

- VMWare Workstation
  - Use the Network Editor to add a new private network
  - Set whatever subnet configuration you want
  - Disable VMWare DHCP, we will use our gateway (pfSense) to do that
- Other stuff – you can accomplish the same thing with Player and VirtualBox
SOFTWARE FIREWALLS

Iptables
SOFTWARE FIREWALLS

- Internal Network
- Internal Users
- Host Firewall
- Network Firewall
- IDS
- External Network
- Internet User
- Web/Mail/etc. Servers
- Reverse Proxy
- DMZ
- Web Firewall
- Internet
- External Network
OVERVIEW

• Last chance to detect and stop malicious traffic going into an end-point
• First change to detect and stop malicious traffic coming from an end-point
• All incoming packets are subjected to a chain of rules
• The first applicable rule is applied and the next packet is examined
TRY IT YOURSELF…

• Iptables comes installed in most Debian distributions (as well as others)

• Tutorial can be found here: https://help.ubuntu.com/community/IptablesHowTo

• Make sure to try on a server you can access physically first – you might lock yourself out
pfSense

NETWORK FIREWALLS
NETWORK FIREWALLS

- DMZ
- External Network
- Internal Network
- Network Firewall
- IDS
- Host Firewall
- Internal Users
- Internal Network
- Web/Mail/etc. Servers
- Reverse Proxy
- Web Firewall
- Internet User
- Internet
- External Network
- DMZ
- Internal Users
OVERVIEW

- First line of defense from external sources
- Separates external network (Internet) from internet network and DMZ
- Dedicated server with multiple network interfaces
PFSENSE

- We’ll be using pfSense as a network firewall
- It’s a full UNIX distribution
- Based on FreeBSD
- Uses pf for packet filtering
- Easy to setup and configure
- Offers lots of packages like snort, mod_security, etc.
  - Beware: Some of the packages are poorly maintained and suck. YMMV
TRY IT YOURSELF…

• Using VMWare Workstation, create a new private network without enabled DHCP
• Create a virtual machine (Linux 2.6) with a bridged interface and a private network interface
• Set WAN to bridged NIC and LAN to private NIC
• Enabled the DHCP server on the LAN for pfSense
• Everything should work right out of the box now, other VMs on the private network should be able to access the Internet
INTRUSION DETECTION SYSTEMS
OVERVIEW

- Uses a network tap to listen promiscuously to all traffic on that network
- Uses rules and heuristics to identify threats
- Does not act on threats – that’s an IPS (Intrusion Prevention System)
- Tags events and classifies them based on threat
- Able to detect malicious activity where endpoints might have trouble
SECURITY ONION

• Xubuntu Linux distribution that comes supplied with network analysis goodies
• Intrusion Detection Systems:
  • Snort – Popular free signature-based IDS
  • Bro – IDS that uses signatures as well as heuristics and high level traffic analysis
• Lots of monitoring and analysis tools
  • Snorby
  • Squert
  • ELSA
  • Sguil
TRY IT YOURSELF…

- Add a new VM and install Security Onion
- Wait FOREVER while it installs updates (sudo apt-get update && sudo apt-get upgrade -y)
- Switch it to the private network with your pfSense machine
- We don’t need a network tap because the VM’s network adapter is able to listen to network traffic promiscuously out of the box
mod_security

WEB APPLICATION FIREWALLS
WEB APPLICATION FIREWALL

- Internal Users
  - Internal Network
  - Host Firewall
  - IDS

- Internet User
  - Internet

- External Network
  - DMZ
  - Reverse Proxy
  - Web/Mail/etc. Servers
  - DMZ Web Firewall

- Internal Users
  - Internal Network
  - Network Firewall
OVERVIEW

• Sits in front of web applications and detects malicious input
• Defends against threats such as
  • SQLi
  • XSS
  • CSRF
  • Automated scanners
• Two configurations:
  • Web server – Runs on top of web server on that machine and filters traffic
  • Reverse proxy – Traffic is analyzed and filtered before reaching wen-point web server
TRY IT YOURSELF…


- Some rules, such as filtering numerical IP addresses, will be too restrictive

- Keep an eye on the log and remove whatever rules are causing issues

- Run some scanners (w3af for example) against it and laugh at the resulting failure