Passive Asset Detection System

Recon 2005

Matt Shelton
matt@mattshelton.com

Overview

- Who
- Why
- What
- How
- Future
- Demonstration
- Questions

Asset Data

- A set of characteristics describing a network host.
- Ex. Open Ports, Running Services, Operating System, etc.

Who

- Security Engineer for a Managed Security Services Provider (MSSP)
- Founder of Passive Asset Detection System (PADS)

Why

- IDS Analysis
  - Alert Context
  - Investigations
  - Filtering / Tuning
- Vulnerability Management
- Policy Monitering

Active Scanner Shortcomings

- Network Resource Intensive
- Host Intrusive
- Immediately Out of Date
- Network Access Required

Passive Scanner Shortcomings

- Service banner must be advertised
- Encrypted services are hard to fingerprint
- Passive scanners can only report what they see

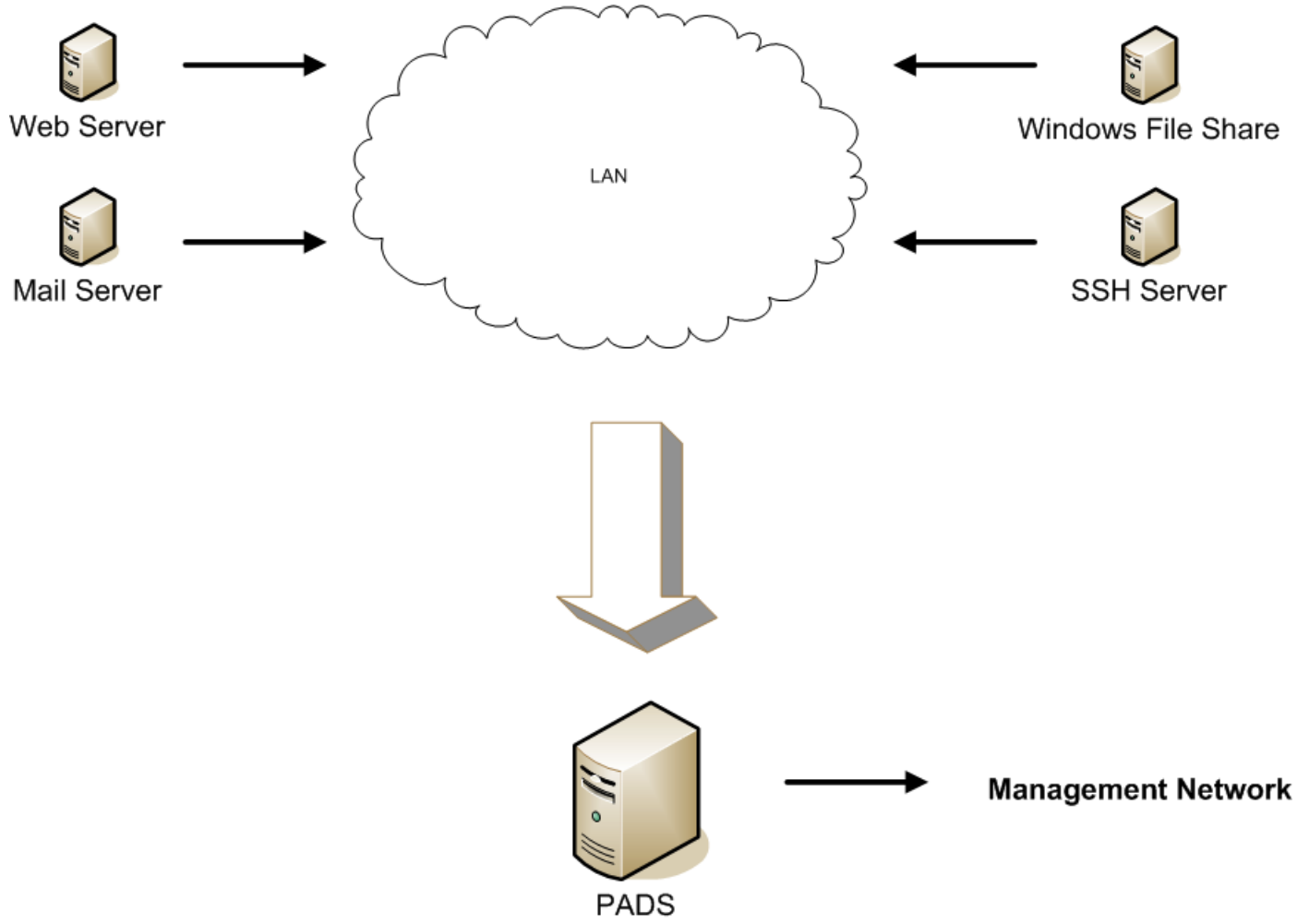
Passive Scanners

- Commerical
  - Sourcefire RNA
  - Tenable Security NeVO
- Open Source
  - p0f

What

- Passive Asset Detection System (PADS)
- http://passive.sourceforge.net
- http://www.mattshelton.com/recon2005
- Intelligent Network Sniffer
  - Libpcap
  - PCRE Signatures

Diagram


Web Server
Mail Server
LAN
Windows File Share
SSH Server
PADS
Management Network

Goals

- Passive
- Portable
- Lightweight

New Release

- PADS v1.2
  - Server Oriented
  - Tiered Architecture
  - Configuration Files
  - Internal Rewrites

How

- Looks at 3 types of traffic
  - TCP
    - Ex: Port 22, OpenSSH 3.8.1
  - ARP
    - Ex: 00:B0:D0:92:2F:17 (Dell Computer Corp.)
  - ICMP

Filters

- Filter Networks
- Ex. pads -n “192.168.0.0/24,10.10.10/16”

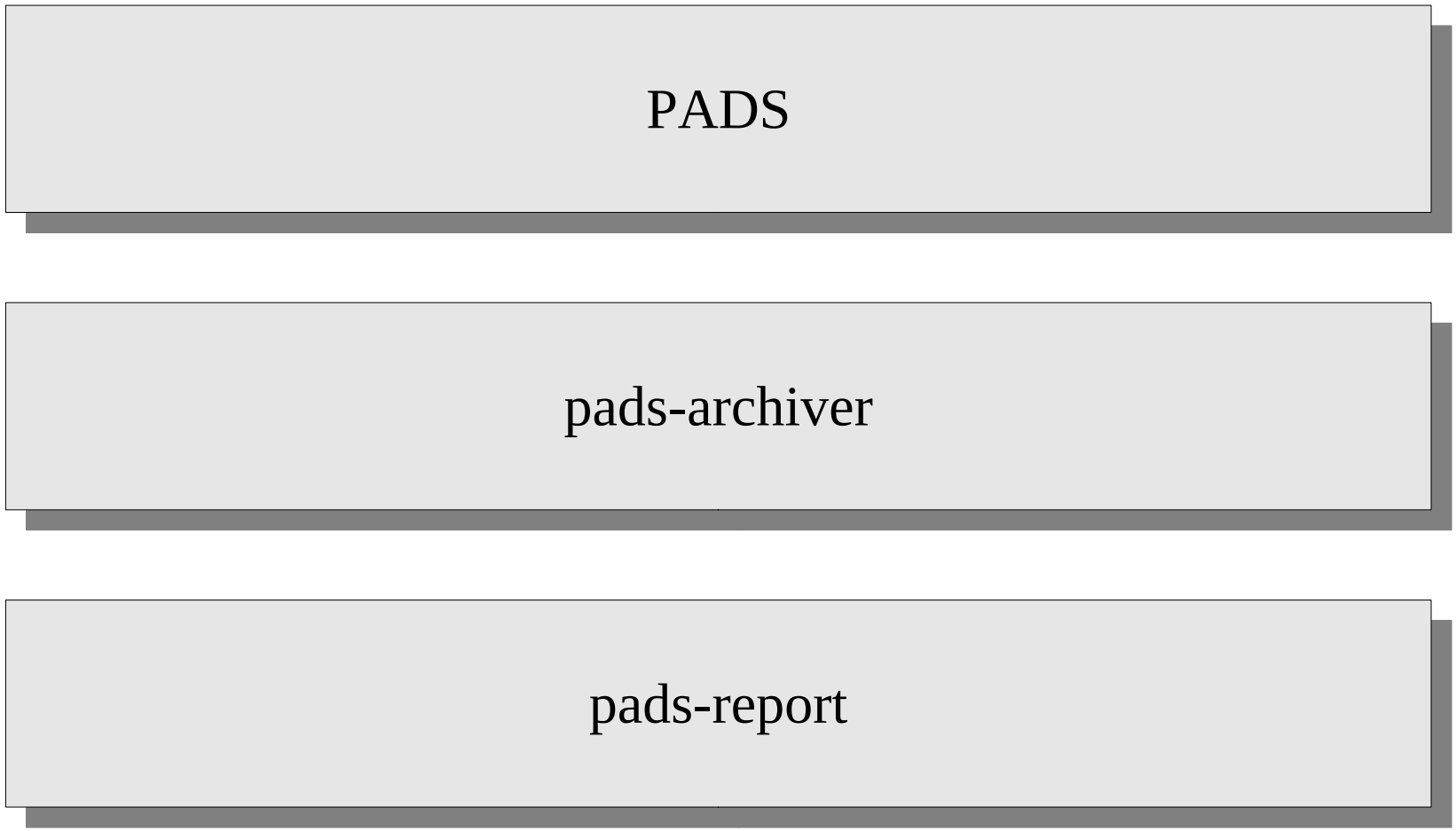
Signatures

```
ssh,v/OpenSSH/$2/Protocol $1/,SSH-([.\d]+)-OpenSSH[_-](\S+)
www,v/Apache/$1/$2/,Server: Apache\/([\S]+)[\s]+\((.*)\)
www,v/Microsoft-IIS/$1//,Server: Microsoft-IIS\/([\S]+)[\r\n]
ssl,v/OpenSSL///,^\x16\x03\0\0J\x02\0\0F\x03\0
imap,v/Cyrus IMAP4 Server/$1//,\* OK [-.\w]+ Cyrus IMAP4 v([-.\w]+) server ready
vnc,v/VNC//Protocol $1/,RFB ([\S]+)\n
rdp,v/Remote Desktop Protocol//Windows 2000 Server/,\x03\0\0\x0b\x06\xd0\0\0\x12.\0
smtp,v/Postfix SMTP//$1/,^220 ([-.\w]+) ESMTP Postfix
ftp,v/FreeBSD ftpd/$2/$1/,220 ([-.\w]+) FTP server \(Version (6.0\w+)\) ready.\r\n
rdp,v/Remote Desktop Protocol//Windows 2000 Server/,\x03\0\0\x0b\x06\xd0\0\0\x12.\0
```

Banner Grabbing

- Banner grabbing introduced in v1.2
- Ex. pads -d banners.pcap
- Records the first 5 packets of a connection, stops if the service has been identified.
- Resource Intensive
- Helpful with signature development

Tiered Architecture



PADS

- Detection Engine
- Output
  - Screen
  - CSV
  - FIFO

pads-archiver

- Storage Engine
- Moves data into permanent storage
- Input
  - FIFO
- Output
  - CSV
  - Syslog
  - MySQL
  - PostgreSQL

pads-report

- Generates NMAP-like Reports
- Input
  - CSV

NMAP-like Report

```
1 ----------------------------------------------------
IP:       10.10.10.1
MAC(s):   0:06:25:78:20:75   (2005/06/11 12:58:11)
VENDOR:   Linksys WPC11 v2.5
ICMP:     Enabled

Port  Service    Application
80    www        Unknown HTTP (HTTP/1.1)

2 ----------------------------------------------------
IP:       10.10.10.83
MAC(s):   8:00:20:A0:14:A5   (2005/06/11 12:58:11)
VENDOR:   Sun Microsystems Inc.

Port  Service    Application
22    ssh        OpenSSH 3.8.1 (Protocol 2.0)
80    www        Apache/1.3.29 (Unix) PHP/4.3.10 mod_ssl/2.8.16
```

Security Enhancements

- Privilege Lowering
  - setuid(), seteuid()
  - setgid(), setegid()
- String Library
  - Better String Library
  - Paul Hsieh
  - http://bstring.sourceforge.net

Future

- More Protocols
  - UDP
  - ICMP (Destination Unreachable, etc.)
  - DHCP
  - Layer 2 (VLAN Tagging, CDP, etc.)

Future

- Detection Preprocessors
  - Independent modules with access to the entire libpcap packet
  - Long Term Analysis
  - OS Identification

Future

- New Robust Signature Language
  - Client / Server
  - Non-PCRE Signatures
- Signatures
- Performance

Proof It Works

Live Demonstration

Questions, Comments, Criticism?