

# Fences Make Good Neighbors

*Monitoring Academic Networks at the Port Level*



*Educause Security Conference*

*April 4, 5 2005*

*Washington DC*

Kevin Amorin  
Harvard University



# Topics

- ◆ Overview of the problems/needs
- ◆ Solutions
  - PacketFence
- ◆ Questions



# Network (In)security

- ◆ Perimeter security
  - Firewalls, IDS, IPS, Router ACLs
  - “Hard on the outside soft on the inside”
  - Leads to complacency
- ◆ 60-80% of attacks originate from systems on the internal network (behind the firewall)
  - VPN
  - Wireless
  - Dial-up



# Internal Network Protection/Control

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>◆ Mirage Networks (ARP)</li><li>◆ qRadar (ARP)</li><li>◆ Wholepoint (ARP)</li><li>◆ Tipping Point (Inline)</li><li>◆ Impluse</li><li>◆ Sourcefire</li><li>◆ Bradford (VLAN)</li></ul> | <ul style="list-style-type: none"><li>◆ Cisco/Perfigo (NAC/VLAN)</li><li>◆ Trend Micro (NAC)</li><li>◆ Symantec (NAC)</li><li>◆ Microsoft (NAP Q2-2005)</li><li>◆ Juniper (TNC)</li><li>◆ Foundry Networks (TCC)</li></ul> |
|---|--|



# Academic Issues

## ◆ Network Environment

- Worms
- Bot nets
- DMCA
- Policy violations
  - NATs
  - p2p applications

## ◆ Identity

- Who owns an infected/offending system?

## ◆ Support

- Do you want to be manning the helpdesk on move-in day?



# What is PacketFence

- ◆ Open-source network registration and worm mitigation solution
  - Co-developed by Kevin Amarin and David LaPorte
    - GUI developed by Randy Heins, UIS NOC
  - Captive portal
    - Intercepts HTTP sessions and forces client to view content
  - Based on un-modified open-source components



# Features

- ◆ Network registration
  - Register systems to an authenticated user
    - LDAP, RADIUS, POP, IMAP...anything Apache supports
  - Force AUP acceptance
  - Stores assorted system information
    - NetBIOS computer name & Web browser user-agent string
    - Presence of some NAT device
  - Stores no personal information
    - ID->MAC mapping only
  - Above data can provide a rough system inventory
  - Vulnerability scans
    - at registration
    - scheduled/ad hoc



# Features

- ◆ Worm mitigation
  - Behavioral and signature-based detection
  - Optional isolation of infected nodes
  - Self-remediation
    - Empower users
    - Provides remediation instruction specific to infection
- ◆ Network “inoculation”
  - Preemptively detect and trap vulnerable hosts



# Features

## ◆ Remediation

- Requires signature-based detect
- Provides user context-specific remediation instructions
- Redirection to the captive portal
  - via Proxy
  - via Firewall pass-through
- Helpdesk support number if all else fails



# Inline

- ◆ Security bottleneck
  - immune to subversion
- ◆ Fail-closed
- ◆ Performance bottleneck
- ◆ Single point of failure
- ◆ May not be necessary/preferable
  - academia

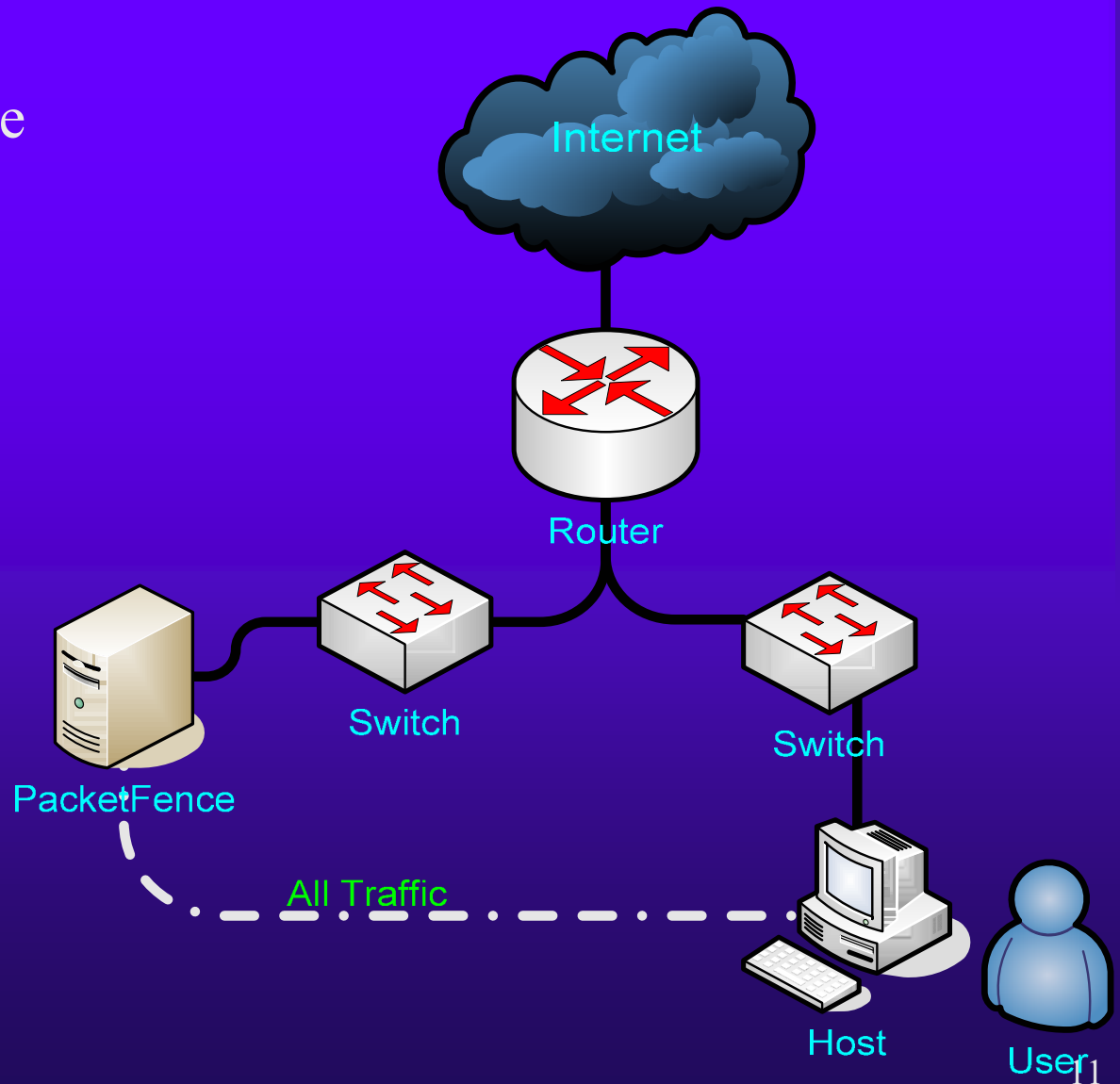


# Passive

- ◆ Fail-open solution
  - Preferable in academic environment
- ◆ No bandwidth bottlenecks
- ◆ Network visibility
  - Hub, monitor port, tap
- ◆ Easy integrating – no changes to infrastructure
  - plug and play (pray?)
- ◆ Manipulates client ARP cache
  - “Virtually” in-line

# ARP Manipulation

Man In the Middle  
(MiM) ARP  
poisoning





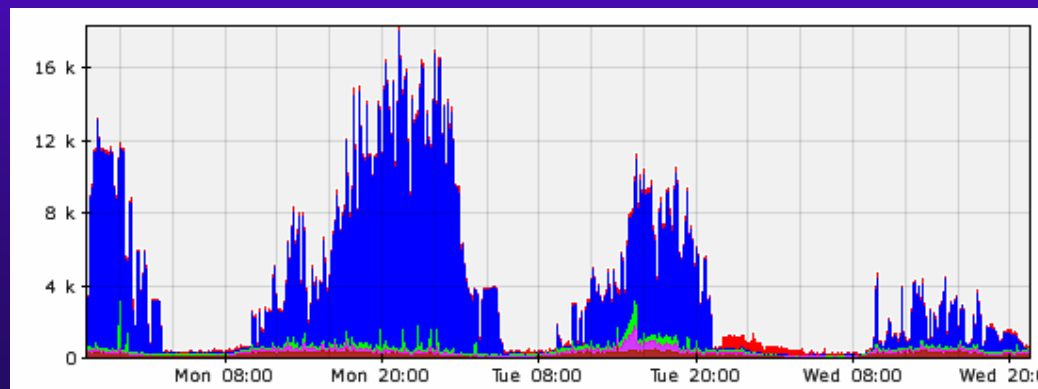
## Detection (optional)

- ◆ Traffic analysis
  - Anomaly based
  - Signature based
  - Time based
- ◆ Snort with small signature set & portscan
- ◆ Any signature and/or anomaly based detection tool can be used (“glue” will be necessary)



# Implementations

- ◆ All current deployments are “passive” mode
- ◆ Several residential networks and 2 schools
  - ~7076 systems
  - ~3934 registrations
  - ~225 violations
    - Nachi / Sasser, Agobot, Gaobot, etc / IRC bots





// packetfence //

PACKET FENCE

Person Node Violation Class Report Scanning Administration

View Add Lookup admin logout

-Filter-

Identifier	First Name	Last Name	Email	Phone	Address	City	State	Custom Info #1	Custom Info #2	Custom Info #3	Edit
1	Generic	User	none@none.com	617-222-555 60	ox	dddd	ddd	ja			
uid=bdash,ou=People,dc=harvard,dc=edu											
uid=bflan,ou=People,dc=harvard,dc=edu											
uid=bmollo,ou=People,dc=harvard,dc=edu											
uid=cbralott,ou=People,dc=harvard,dc=edu											
uid=cterenzi,ou=People,dc=harvard,dc=edu											
uid=dlaporte,ou=People,dc=harvard,dc=edu											
uid=egoodric,ou=People,dc=harvard,dc=edu											
uid=jbogolia,ou=People,dc=harvard,dc=edu											
uid=jsilva,ou=People,dc=harvard,dc=edu											
uid=kkokubo,ou=People,dc=harvard,dc=edu											
uid=ldonnell,ou=People,dc=harvard,dc=edu											
uid=mcevilly,ou=People,dc=harvard,dc=edu											
uid=plavbee,ou=People,dc=harvard,dc=edu											
uid=rhelms,ou=People,dc=harvard,dc=edu											
uid=shartman,ou=People,dc=harvard,dc=edu											

(16 results)

Done pf-dev.noc.harvard.edu Proxy: None



Browser window: // packetfence //

Navigation tabs: Person, Node, Violation, Class, Report, Scanning, Administration

Sub-tabs: Active, Registered, Unregistered, Active Unregistered, Active Registered, History, Graphs

admin logout

Filter options: -Filter-, -Start Date-, -Stop Date-, Submit

MAC	Identifier	Reg. Date	Last Skip	Status	User Agent	Computer Name	IP	Start Time	End Time	Last Seen
00:02:b3:2f:9c:16	1	2005-01-01 13:33:31	2005-01-01 13:33:31	unreg		QUACKERS	128.103.209.154	2005-04-03 22:35:33	0000-00-00 00:00:00	0000-00-00 00:00:00
00:03:47:90:86:4e	1	2005-01-19 10:11:17	2005-01-19 10:11:17	unreg		undef	128.103.209.157	2005-04-03 22:34:22	0000-00-00 00:00:00	0000-00-00 00:00:00
00:09:12:2a:7d:c0	1	2005-03-30 09:02:07	2005-03-30 09:02:07	unreg		undef	128.103.209.3	2005-04-03 22:31:45	0000-00-00 00:00:00	0000-00-00 00:00:00
00:09:44:55:74:00	1	2005-03-30 09:02:37	2005-03-30 09:02:37	unreg		undef	128.103.209.2	2005-04-03 22:31:42	0000-00-00 00:00:00	0000-00-00 00:00:00
00:b0:d0:22:1e:33	1	2004-12-31 00:52:32	2004-12-31 00:52:32	unreg		undef	128.103.209.13	2005-04-03 22:32:01	0000-00-00 00:00:00	0000-00-00 00:00:00

(5 results)

Export dialog: Select the fields you want to export

mac	pid	regdate	lastskip	status	user_agent	computername	ip	start_time	end_time	last_seen
00:02:b3:2f:9c:16	1	2005-01-01 13:33:31	2005-01-01 13:33:31	unreg	unreg	QUACKERS	128.103.209.154	2005-04-03 22:35:33	0000-00-00 00:00:00	0000-00-00 00:00:00

Done pf-dev.noc.harvard.edu Proxy: None



// packetfence //

// packetfence //

**PACKET FENCE**

Person Node Violation Class Report Scanning Administration

Violations Nessus admin logout

-Filter- X

Identifier	Description	Auto Enable	Max Enables	Grace	Priority	URL	Max Enable URL	Redirect URL	Button Text	Disabled
1100000	UNKNOWN	N	0	120	4	/content/1100000			Enable Network	Y
1100001	SASSER	Y	3	120	4	/content/1100001	/proxies/tools/stinger.exe		Enable Network	N
1100002	PHATBOT	Y	3	120	4	/content/1100002	/proxies/tools/stinger.exe		Enable Network	N
1100004	TROJANIRC	N	3	120	3	/content/1100004			Enable Network	N
1100005	NAT	Y	3	120	7	/content/1100005			Enable Network	Y
1100006	LSASS	Y	3	120	4				Enable Network	N
1200000	AUP	Y	0	1	2	/content/1200000			Accept AUP	N
1200001	SYSTEMSCAN	Y	3	120	9	/content/1200001			Enable Network	Y
1200002	REGCOMPLETE	Y	0	1	3	/content/1200002			Complete Registration	N

(9 results)

Done pf-dev.noc.harvard.edu Proxy: None



// packetfence //

// packetfence //

**PACKET FENCE**

Person Node Violation Class Report Scanning Administration

Nessus Scan Results Monitor File Depot admin logout

Add a Scan Schedule

Host/Range

Scan For

PHATBOT

Schedule

Scan Now

Repeating Schedule

Time

Daily [-----] [-----]

Day [-----] Time [-----]

Weekly [-----] [-----]

Date [-----] Time [-----]

Monthly [-----] [-----]

Add Schedule

Current Schedules

Scan ID	Date	Hosts	Vulnerabilities	Edit
0	1 2 ***	128.103.190.4 (1 result)	11890	



Browser window: // packetfence //

Navigation tabs: Person, Node, Violation, Class, Report, Scanning, Administration

Sub-navigation: Configuration, Status, Add User, UI Options

admin logout

### ALERTING

alerting.emalladdr	<input type="text" value="david_laporte@harvard.edu"/>	<input type="checkbox"/> Default
alerting.smtpserver	<input type="text" value="claven.harvard.edu"/>	<input type="checkbox"/> Default

### ARP

arp.listendevic	<input type="text" value="eth0"/>	<input checked="" type="checkbox"/> Default
arp.dhcp_timeout	<input type="text" value="10800"/>	<input type="checkbox"/> Default
arp.mode	<input type="text" value="pfmon"/>	<input checked="" type="checkbox"/> Default
arp.cleanshutdown	<input type="text" value="enabled"/>	<input checked="" type="checkbox"/> Default
arp.interval	<input type="text" value="60"/>	<input type="checkbox"/> Default
arp.strobe	<input type="text" value="enabled"/>	<input checked="" type="checkbox"/> Default
arp.gw_timeout	<input type="text" value="10800"/>	<input type="checkbox"/> Default
arp.timeout	<input type="text" value="86400"/>	<input type="checkbox"/> Default
arp.heartbeat	<input type="text" value="30"/>	<input type="checkbox"/> Default
arp.probe_interval	<input type="text" value="900"/>	<input checked="" type="checkbox"/> Default
arp.stuffing	<input type="text" value="enabled"/>	<input type="checkbox"/> Default

### DATABASE

database.pass	<input type="text" value="packet"/>	<input checked="" type="checkbox"/> Default
database.db	<input type="text" value="pf"/>	<input checked="" type="checkbox"/> Default
database.user	<input type="text" value="root"/>	<input checked="" type="checkbox"/> Default
database.port	<input type="text" value="3306"/>	<input checked="" type="checkbox"/> Default
database.host	<input type="text" value="localhost"/>	<input checked="" type="checkbox"/> Default

Done | pf-dev.noc.harvard.edu | Proxy: None



# Coming Soon...

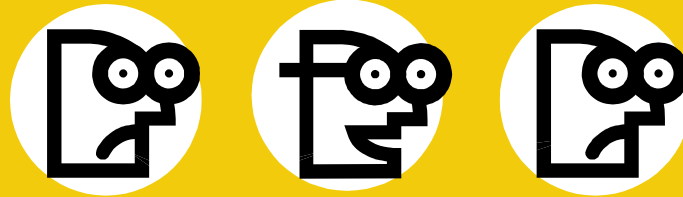
- ◆ Static IP/ARP Detection
- ◆ DHCP Combat
- ◆ Queue-based Violation/Registration
- ◆ Independent components
- ◆ Isolation mechanisms
  - DHCP
    - Change DHCP scope (reserved IP with enforcer gateway)
    - Change DNS server to resolve all IP's to Enforcer
  - Switch port manipulation
    - Change VLAN to isolation network
    - Disable port



# In Closing

## ◆ PacketFence

- Open-source
- Passive deployment
  - “plug and play”
  - no infrastructure changes needed
- Proactive and reactive remediation
- Extremely configurable



**It's QUESTION TIME !!**