



# PacketFence

*...because good fences make good neighbors*

Michael Garofano, Director of IT, Harvard KSG

Kevin Amarin, Sr. Security & Systems Engineer, Harvard KSG

David LaPorte, Manager Network Security, Harvard (not present today)

[mgarofano@ksg.harvard.edu](mailto:mgarofano@ksg.harvard.edu)

[kamarin@ksg.harvard.edu](mailto:kamarin@ksg.harvard.edu)

[david\\_laporte@harvard.edu](mailto:david_laporte@harvard.edu)

# Agenda

- Academic Issues
- Perimeter & Internal Security
- PacketFence features
- Inline vs. Passive (out of line)

# Academic Issues

- Help Desk Support
  - Limit spread of Worms
  - Identify infected user
  
- DMCA (movie/music download violations)
  - IP to user mapping

# Academic Issues

## ■ Inventory

- List of MAC's and owners

## ■ Gather Statistics

- Get the more money!
- Number of IP's, infections, helpdesk time, etc, active nodes,

# Academic Issues

- Open vs. closed environment
  - Professors and students want unfettered access to the internet
- You can take your FIREWALL and put it...
  - Some things break:
    - Videoconferencing (H.323), Games (UDP non-statefull firewall), P2P, IM etc...

# Average Network Security

- Perimeter security
  - Firewalls, IDS, IPS, Router ACLs
- Current architecture
  - “Hard on the outside soft on the inside”
- Hard to protect the “inside”
- 60-80% of attacks originate from systems on the internal network (behind the firewall)

# Worms wreak havoc

- August 11, 2003 Blaster and Welchia/Nachi
- How did the worms get in? We block all types of traffic from the internet? (especially RPC)  
LAPTOPS!!!!
- Backdoors bypass perimeter defenses:
  - Roaming users
  - VPN
  - Wireless
  - Dialup

# Internal Network Protection/Control

- Mirage Networks (ARP)

- qRadar (ARP)

- Wholepoint (ARP)

- RNA networks (ARP)

- Tipping Point (inline)

- Etc..

- Cisco (NAC)

- Trend Micro (NAC)

- Symantec (NAC)

- Microsoft (NAP Q2-2005)

- Juniper (TNC)

- Foundry Networks (TCC)

- Etc..

- Internal Network Security Funding 2004

- More then \$80M (\$13M Sept)

# What is PacketFence

- Open-source network registration and worm mitigation solution
  - Co-developed by Kevin Amorin and David LaPorte
  - Captive portal
    - Intercepts HTTP sessions and forces client to view content
    - Similar to NoCatAuth, Bluesocket
  - 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

# Features

## ■ Worm mitigation

- Signature and anomaly based detection
- Action based response
  - Optional isolation of infected nodes
- Content specific information
  - Empower users
  - Provides remediation instruction specific to infection

## ■ Network scans

- Preemptively detect and trap vulnerable hosts

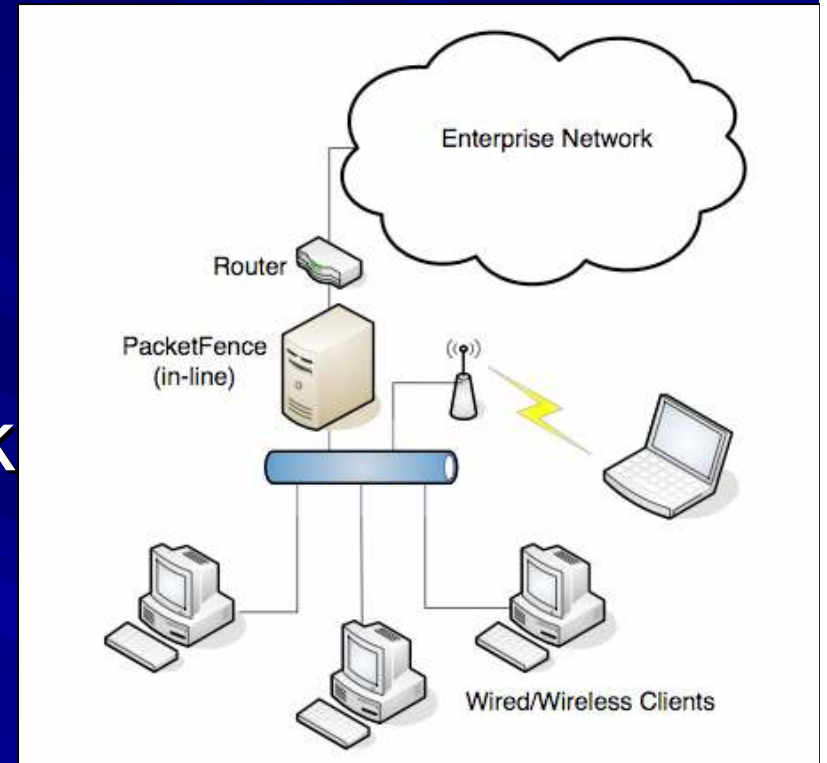
# Features

## ■ Remediation

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

# Inline

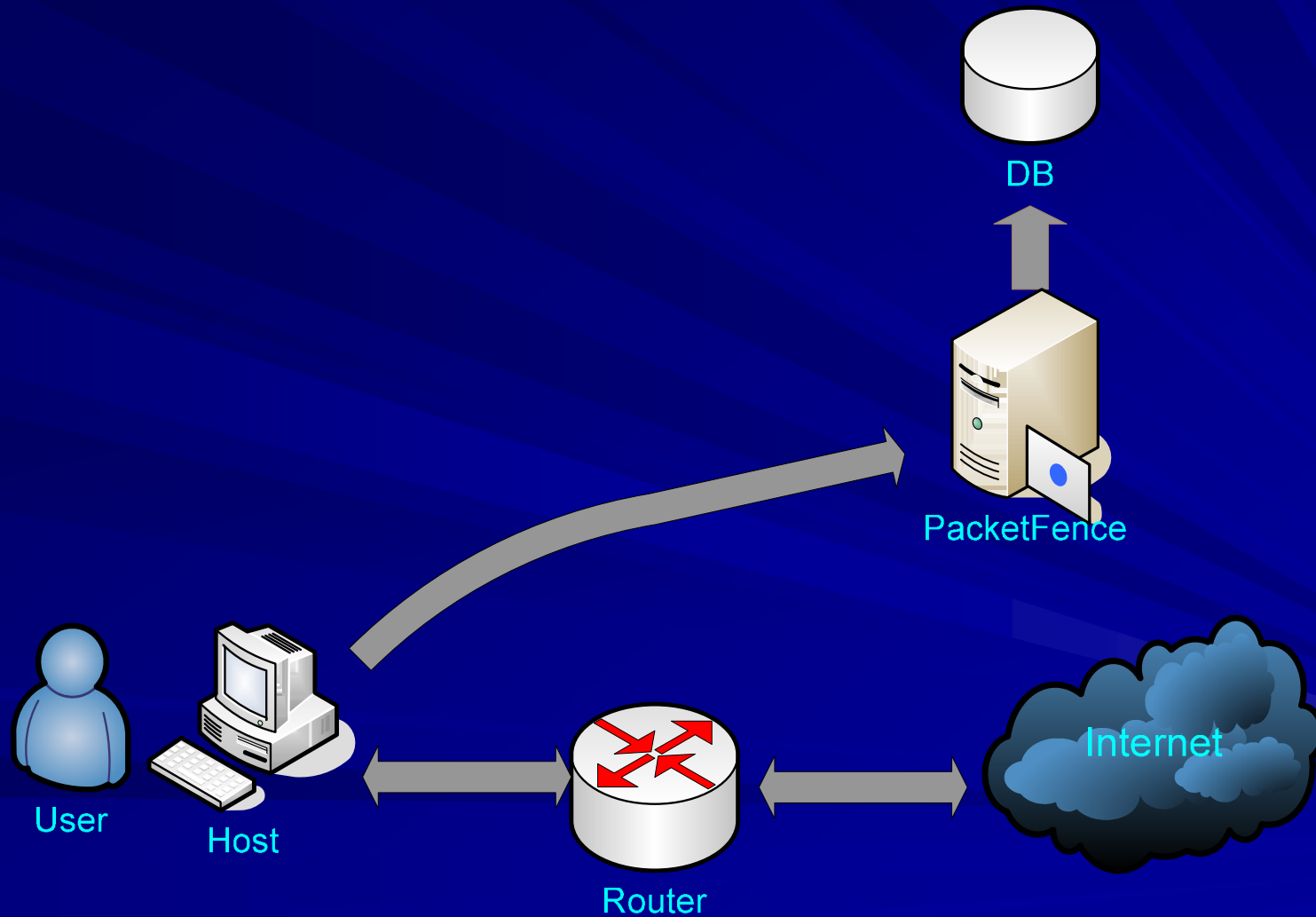
- Security bottleneck
  - immune to subversion
- Fail-closed
- Performance bottleneck
- Single point of failure



# 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

# Passive Architecture



# Why ARP?

- Trusting

- Easy to manipulate

- RFC826 1982

- OS independent

- Windows 95,98,ME,2k,xp,mac both type 1 & 2

- Linux only type 1

- Solaris ICMP & type 2 or 1

# Methods of Isolation

## ■ ARP

- Change the router's ARP entry on the local system to enforcement point

## ■ DHCP

- Change DHCP scope (reserved IP with enforcer gateway)
- or Change DNS server to resolve all IP's to Enforcer

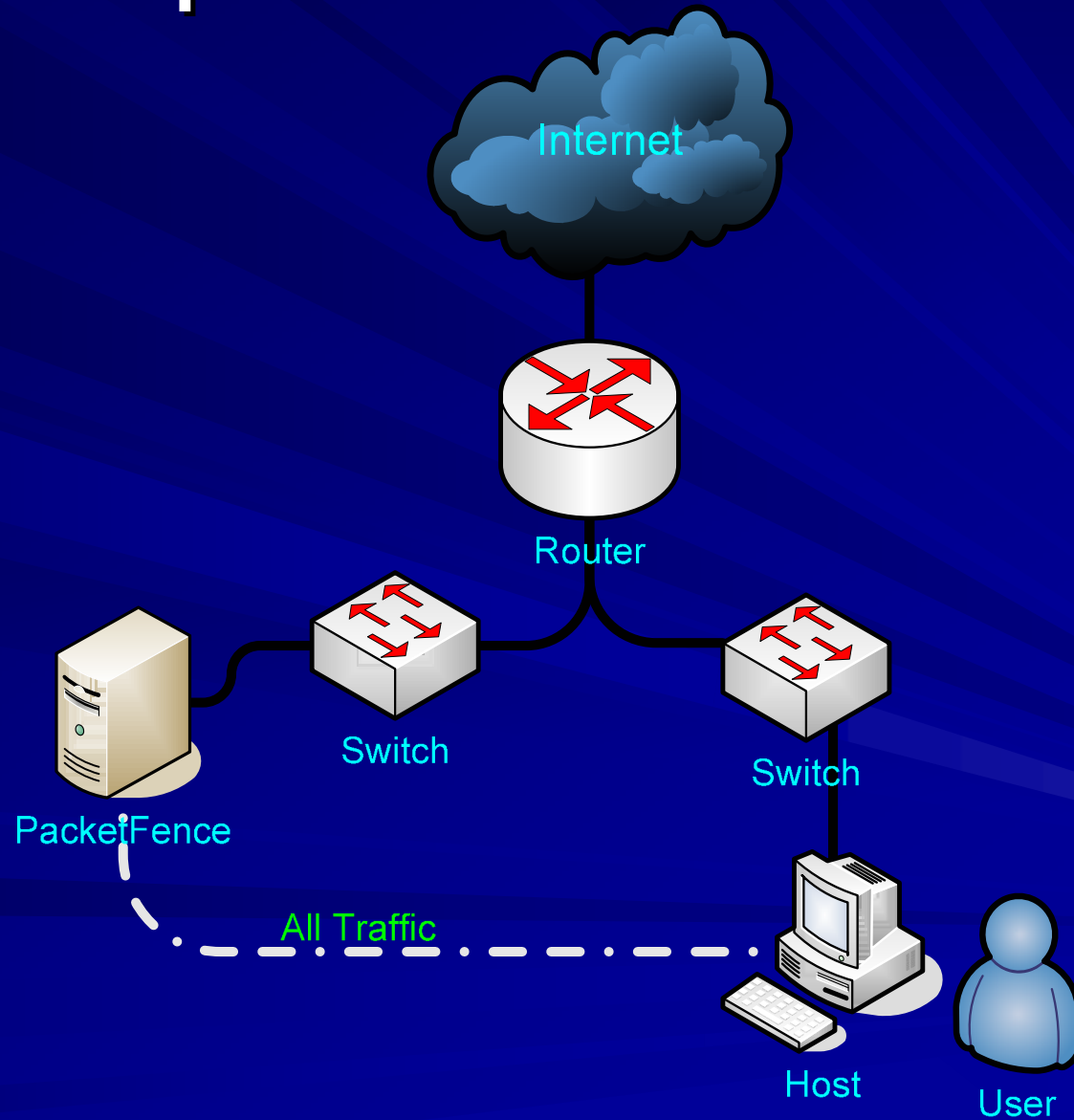
## ■ VLAN switch

- Switch host to an isolation network with enforcer as the gateway

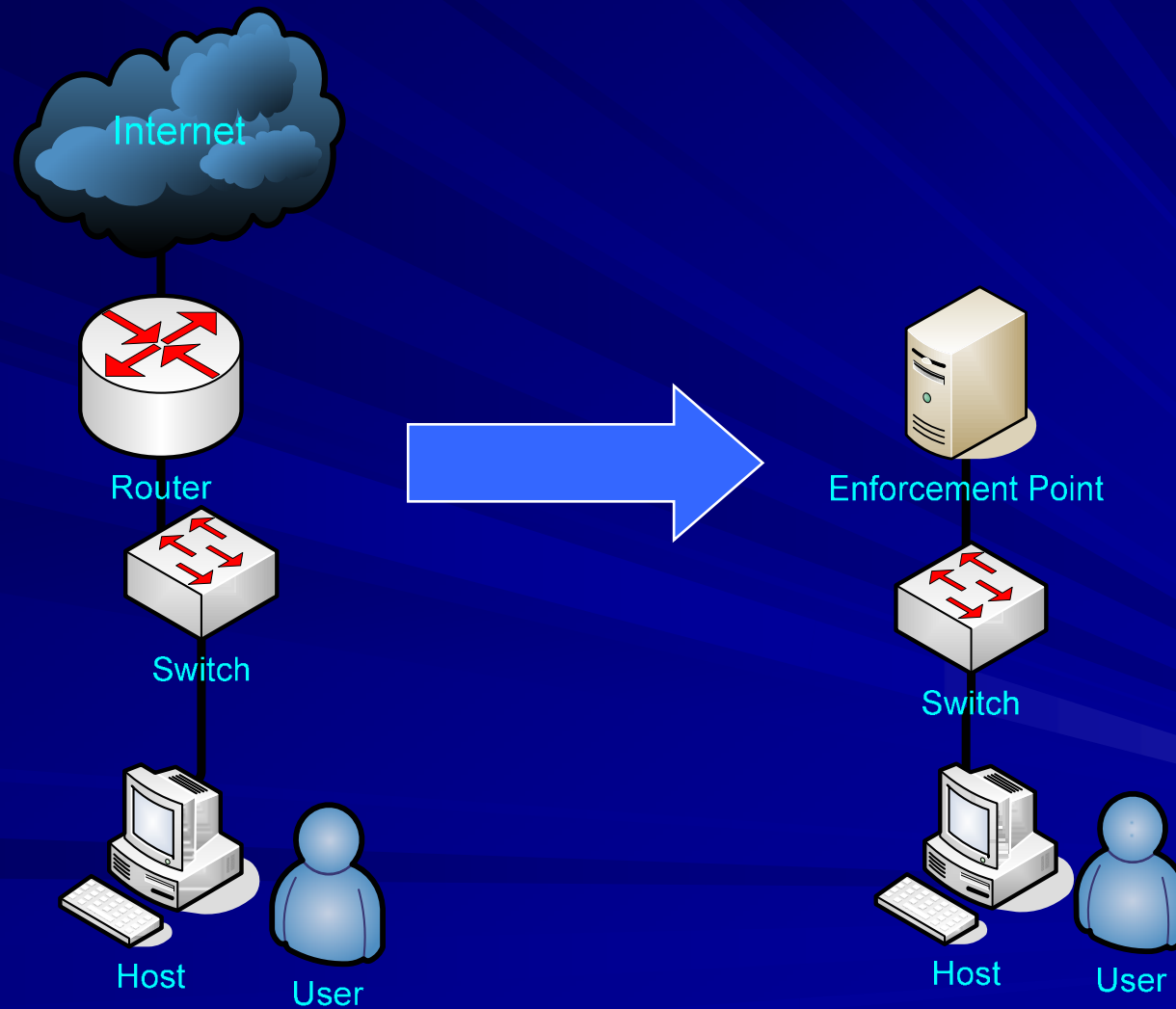
## ■ If all else fails... Blackhole

- Router dynamic update
- Firewall/ACL update
- Disable switch port

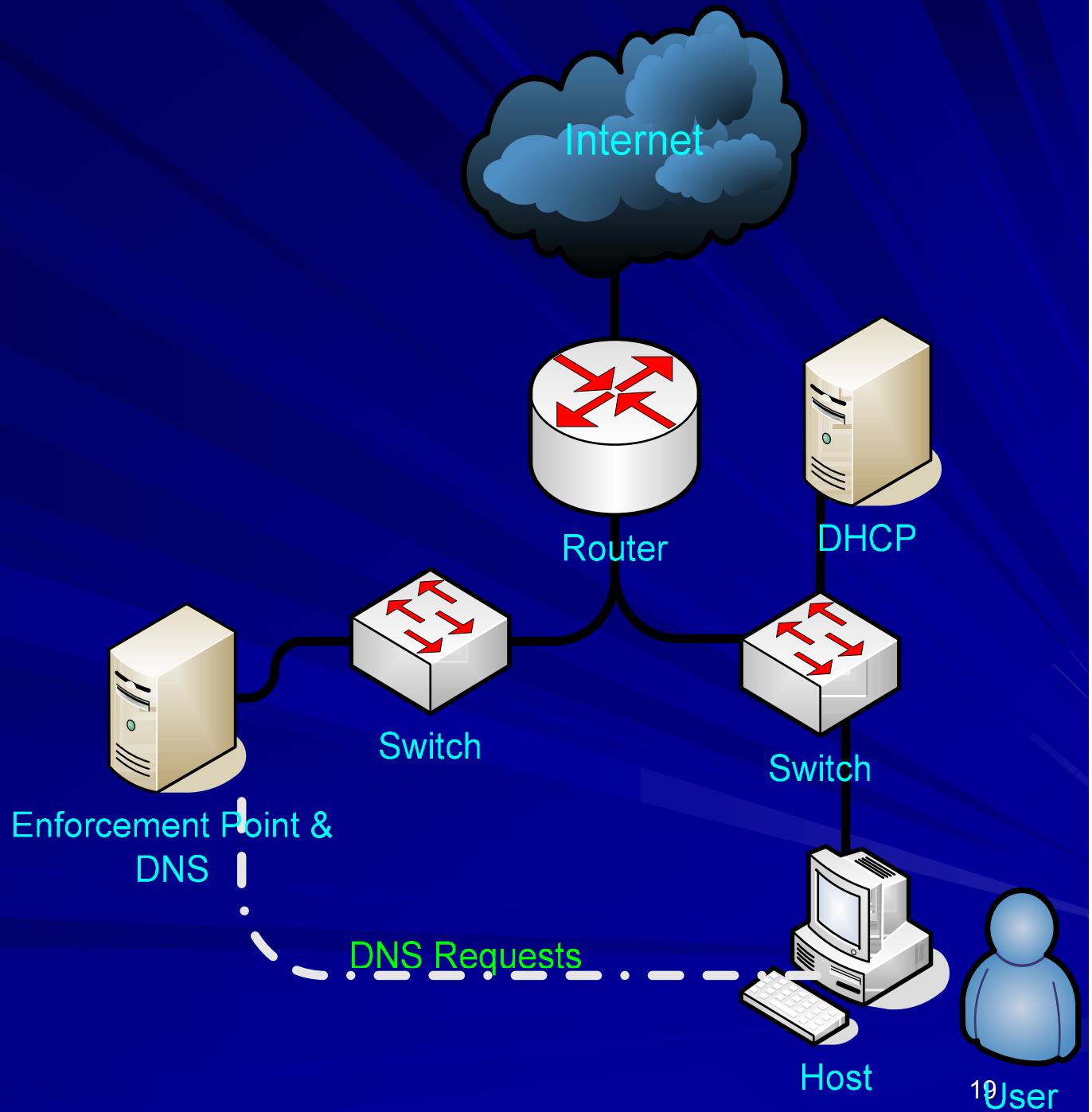
# ARP Manipulation



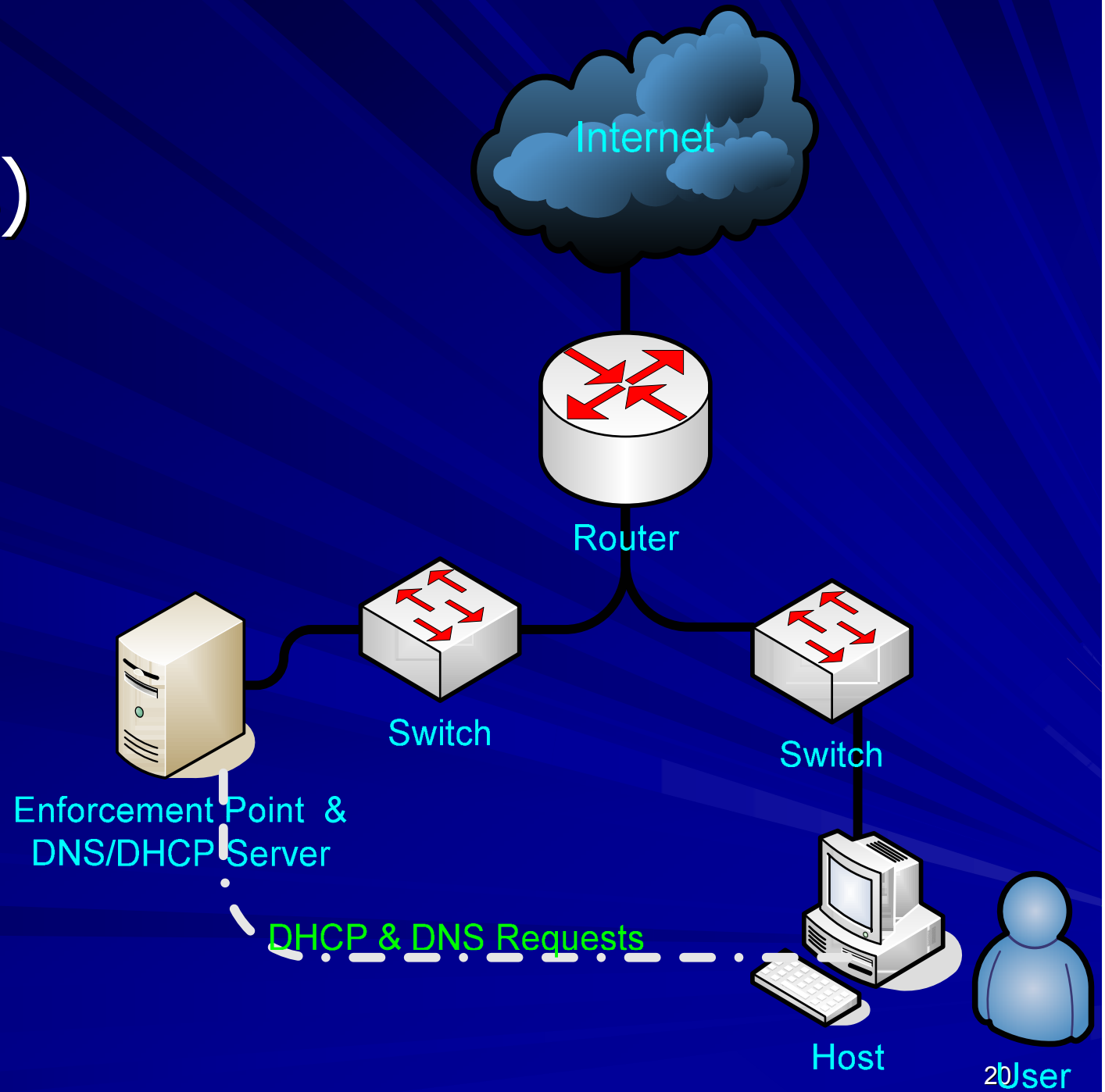
# VLAN Change (Futures)



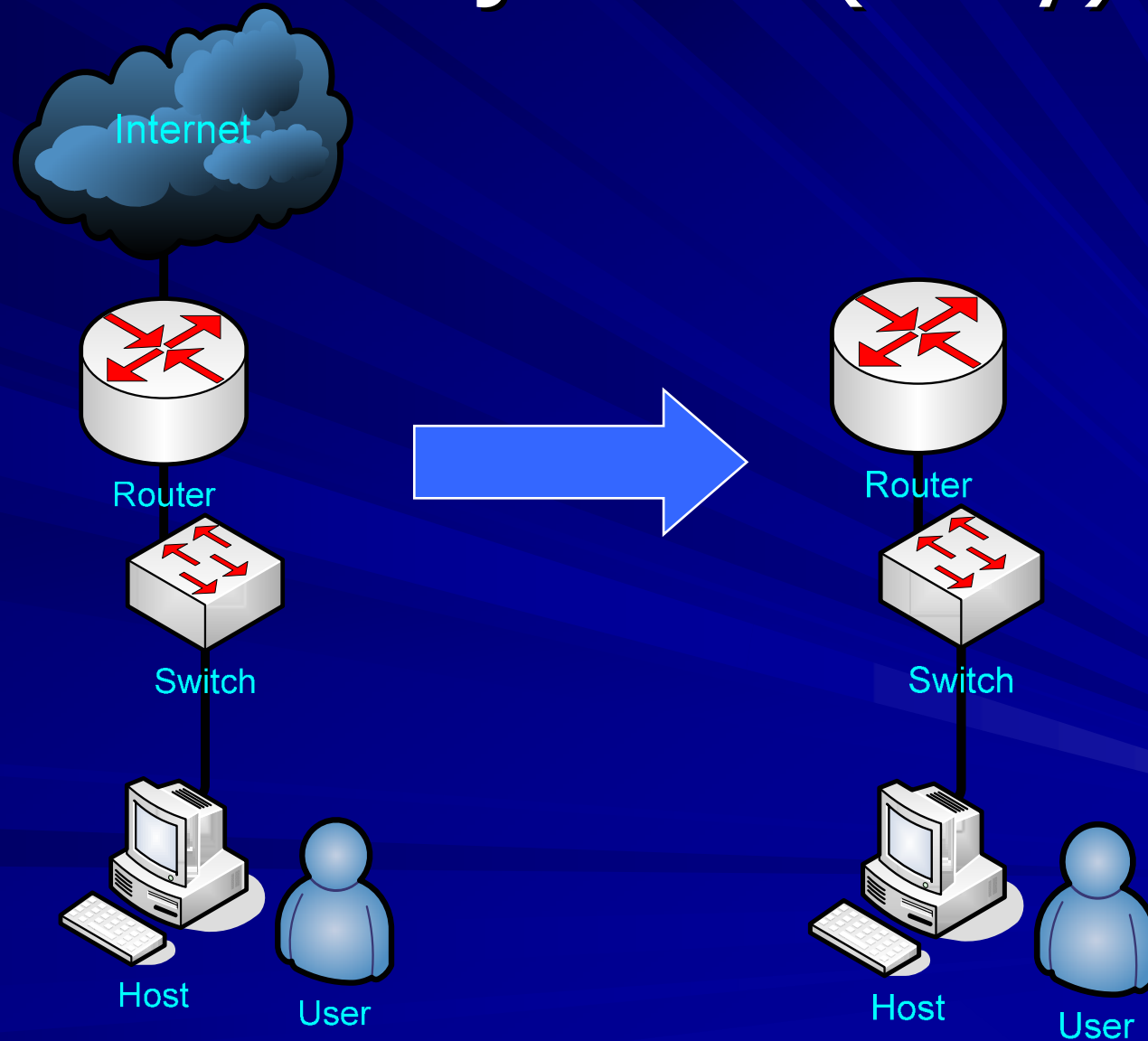
# DNS (Futures)



# DHCP (Futures)



# Blackhole Injection (risky)





































Person Node Violation Class Report Scanning Administration

View Add

admin logo

-Filter-

MAC	Identifier	Regdate	Lastskip	Status	Agent	Computer Name	Edit
00:01:03:2c:3a:e1 1		2005-02-02 14:08:54	2005-02-02 14:08:54	unreg		D422CF01	 
00:01:03:32:dc:32 1		2005-01-11 11:51:28	2005-01-11 11:51:28	unreg		undef	 
00:02:b3:06:0b:8b 1		2005-01-26 16:32:33	2005-01-26 16:32:33	unreg		undef	 
00:02:b3:2f:9c:16 1		2005-01-01 13:33:31	2005-01-01 13:33:31	unreg		QUACKERS	 
00:03:47:90:86:4e 1		2005-01-19 10:11:17	2005-01-19 10:11:17	unreg		undef	 
00:03:93:db:a2:54 1		2005-01-03 09:25:31	2005-01-14 16:07:07	unreg	Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/125.5.5 (KHTML, like Gecko) Safari/85	undef	 
00:07:0e:c0:24:a0 1		2005-02-10 20:21:39	2005-02-10 20:21:39	unreg		undef	 
00:07:50:bb:f3:00 1		2005-01-03 14:24:42	2005-01-03 14:24:42	unreg		undef	 
00:07:e9:b3:07:43 1		2005-01-27 16:45:11	2005-01-27 16:45:11	unreg		undef	 
00:09:6b:02:a0:a0 uid=jsilva,ou=People,dc=harvard,dc=edu		2005-01-11 14:23:44	2005-01-11 14:23:44	reg	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041107 Firefox/1.0	undef	 
00:09:6b:06:b6:87 uid=bmollo,ou=People,dc=harvard,dc=edu		2005-01-14 10:44:47	2005-01-14 10:44:47	reg	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)	DREAMING	 
00:09:6b:10:5a:52 uid=bdash,ou=People,dc=harvard,dc=edu		2005-01-11 14:24:06	2005-01-11 14:24:06	reg	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	bobo	 
00:09:6b:13:48:11 uid=plavbee,ou=People,dc=harvard,dc=edu		2005-01-11 14:30:16	2005-01-11 14:30:16	reg	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	undef	 
00:09:6b:30:2f:c6 1		2005-01-28 11:36:22	2005-01-28 11:36:22	unreg		undef	 
00:09:6b:42:6d:7b uid=idonnell,ou=People,dc=harvard,dc=edu		2005-01-11 14:23:17	2005-01-11 14:23:17	reg	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)	undef	 
00:09:6b:7a:df:86 uid=cterenzi,ou=People,dc=harvard,dc=edu		2005-01-11 16:08:15	2005-01-11 16:08:15	reg	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	undef	 
00:09:6b:d0:98:ba 1		2005-01-03 09:30:28	2005-01-03 09:30:28	unreg		undef	 

Add a Scan Schedule

Host/Range

Scan For

PHATBOT

Schedule

- Scan Now  
 Repeating Schedule

Time



Daily

Weekly

Monthly

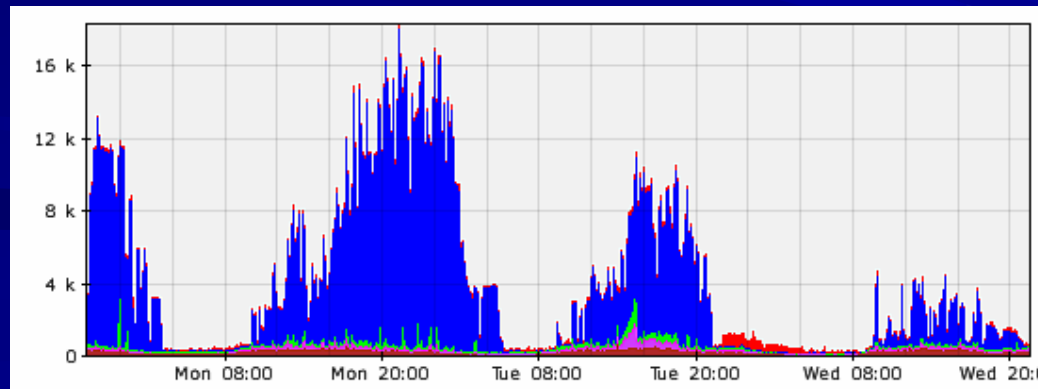
Add Schedule

Current Schedules

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

# Implementations

- All current deployments are “passive” mode
- Several residential networks and 2 schools
  - ~4500 users
  - 3781 registrations
  - ~125 violations
- Nachi / Sasser, Agobot, Gaobot, etc / IRC bots



# Thanks!!!

- Hot “fun” topic!

- Questions?

- Software available at:

<http://www.packetfence.org>

# References

- <http://www.ece.cmu.edu/~lbauer/papers/policytr.pdf>
- <ftp://www6.software.ibm.com/software/developer/library/ws-policy.pdf>
- <http://www9.org/w9cdrom/345/345.html>
- [http://www.sans.org/resources/policies/Policy\\_Primer.pdf](http://www.sans.org/resources/policies/Policy_Primer.pdf)
- [http://www.cs.sjsu.edu/faculty/stamp/students/Silky\\_report.pdf](http://www.cs.sjsu.edu/faculty/stamp/students/Silky_report.pdf)
- Harvard University network security Best practices – Scott Bradner