



Monkey In The

Middle Attack

Hangin on with Ubuntu

(arpWall projekt snapshot)

# OUR TASK

- Spoiler, Intro, about
- Arp brief, Arp attack
- Ubuntu, arpwatrch, swatch, gtk2-perl, arpWall
- Shortcut, Conclusion

# SPOILER

**Believe me !**, there isn't any monkey  
was harm for this presentation

# INTRO

- I am **y3dips**
- **Stuck** in IT Security & Hacking since 2002
- Wrote articles, tips&tricks, advisories
- Founder of **echo.or.id** & **ubuntulinux.or.id**
- Another **Comp/Inet/Net:Security Junkie**

# ABOUT A MONK EY

- It Could`ve be **every Man/Woman**
- **Always Mess Around**
- Know Nothing
- Less knowledge
- Using some friendly tools  
(cain & abel)
- A **kiddie**



# ARP BRIEF

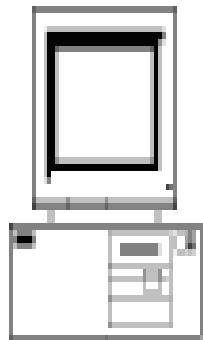
- Address Resolution Protocol
- Map IP network addresses to the hardware addresses

```
y3dips@tarantula:~$ arp -a  
speedgate.war.net (192.168.1.1) at 00:04:76:F7:85:41 [ether] PERM on eth0
```

Node 1

IP Address: 10.0.0.99

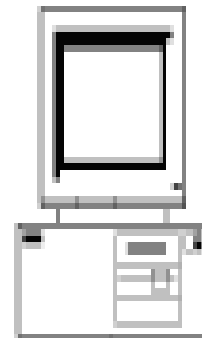
MAC Address: 00-60-08-52-F9-D8



Node 2

IP Address: 10.0.0.1

MAC Address: 00-10-54-CA-E1-40



ARP Request

SHA: 00-60-08-52-F9-D8

SPA: 10.0.0.99

THA: 00-00-00-00-00-00

TPA: 10.0.0.1

ARP Reply

SHA: 00-10-54-CA-E1-40

SPA: 10.0.0.1

THA: 00-60-08-52-F9-D8

TPA: 10.0.0.99

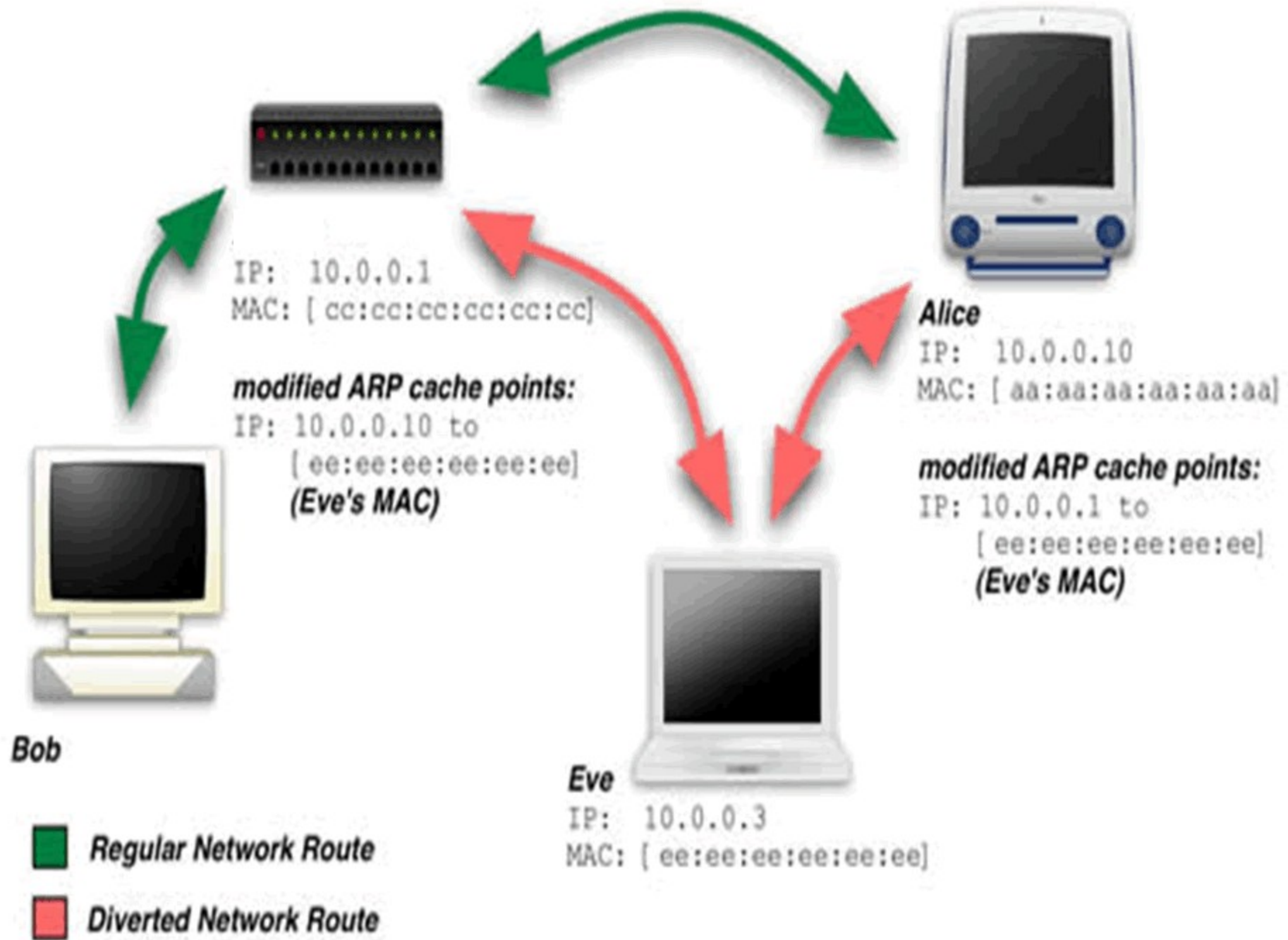
# ARP ATTA CK

- ARP spoofing aka ARP poisoning



# ARP ATTA CK (SPOOFING)

- Send 'fake' or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices (e.g switches)
- As a result frames intended for one machine can be mistakenly sent to another

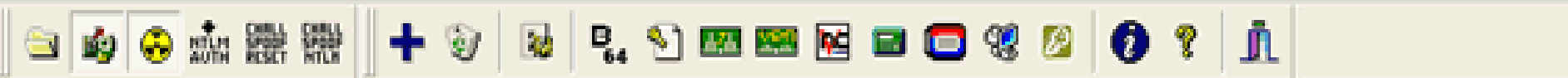


# ARP ATTA CK (IMP ACT)

- Sniff data frames
- Modify the traffic
- Stop the traffic (denial of services)

# Arp Attack (tools)

- ArpSpoofer.c
- Nemesis
- Dsniff
- Ettercap-NG
- Cain & Abel
- etc ...



- APR
  - APR-Cert
  - APR-DNS
  - APR-SSH-1 (0)
  - APR-HTTPS (0)
  - APR-RDP (0)
  - APR-FTPS (0)
  - APR-POP3S (0)
  - APR-IMAPS (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address:
Poisoning	192.168.1.77	00163685E47F	7	6	000476F78541	192.168.1...

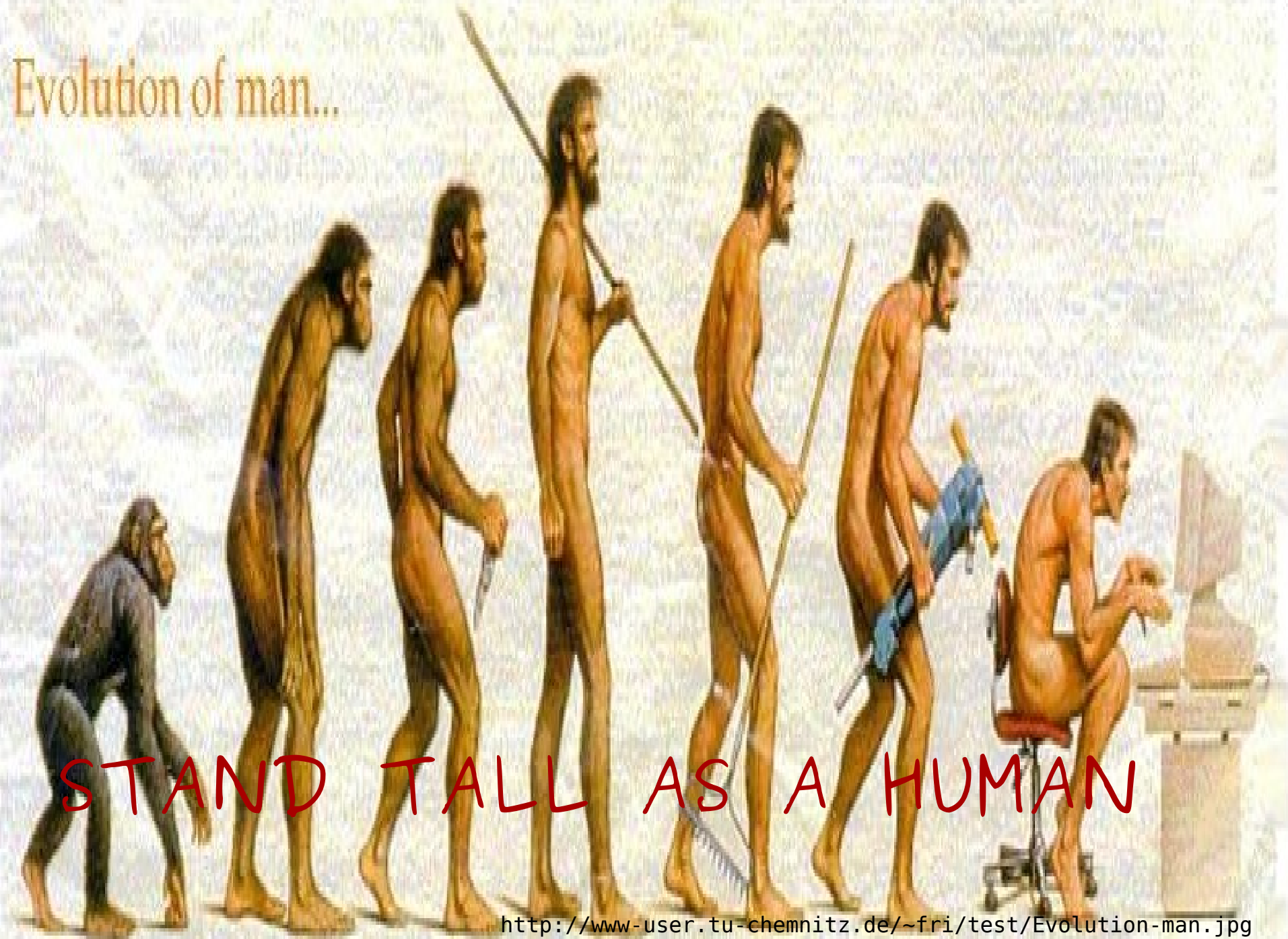
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address:
Full-routing	192.168.1.77	00163685E47F	14	14	000476F78541	216.155.1...
Full-routing	209.85.199.19	000476F78541	90	102	00163685E47F	192.168.1...
Full-routing	192.168.1.77	00163685E47F	63	49	000476F78541	149.9.1.1...
Full-routing	192.168.1.77	00163685E47F	11	10	000476F78541	66.249.8...

Configuration / Routed Packets





Evolution of man...



STAND TALL AS A HUMAN

# DEFENCE AS A HUMAN

- Ubuntu GNU/Linux
- Arpwatch
- Swatch
- Perl-gtk
- arpWall

# UBUNTU

- Ubuntu is an African word meaning 'Humanity to others'
- Community developed
- **Debian** GNU/Linux-based operating system
- 2004 (4.10/warty)
- Been **number 1** for a long time



# ARPWATCH

- Monitors mac addresses on your network and writes them into a file
- <http://freequaos.host.sk/arpwatch/>
  - Latest release arpwatch NG 1.7
- Sudo apt-get install arpwatch

```
indigo@tarantula:~$ sudo /etc/init.d/arpwatch restart
Stopping Ethernet/FDDI station monitor daemon: arpwatch.
Starting Ethernet/FDDI station monitor daemon: (chown arpwatch /var/lib/arpwatch/arp.dat) arpwatch.
indigo@tarantula:~$ tail -f /var/log/syslog
Jul 29 21:56:04 tarantula kernel: [11567.932000] atkbd.c: Use 'setkeycodes 55 <keycode>' to make it know
Jul 29 21:56:04 tarantula kernel: [11568.432000] atkbd.c: Unknown key pressed (translated set 2, code 0x
Jul 29 21:56:04 tarantula kernel: [11568.432000] atkbd.c: Use 'setkeycodes 55 <keycode>' to make it know
Jul 29 21:56:04 tarantula kernel: [11568.700000] atkbd.c: Unknown key released (translated set 2, code 0
Jul 29 21:56:04 tarantula kernel: [11568.700000] atkbd.c: Use 'setkeycodes 55 <keycode>' to make it know
Jul 29 21:56:05 tarantula dhclient: No DHCP OFFERS received.
Jul 29 21:56:05 tarantula dhclient: No working leases in persistent database - sleeping.
Jul 29 21:56:47 tarantula arpwatch: exiting
Jul 29 21:56:48 tarantula arpwatch: Running as uid=112 gid=116
Jul 29 21:56:48 tarantula arpwatch: listening on eth0
Jul 29 21:58:12 tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41) eth0
Jul 29 21:58:17 tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 29 21:58:17 tarantula arpwatch: reaper: pid 7930, exit status 1
Jul 29 21:58:41 tarantula arpwatch: ethernet mismatch 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41) eth0
Jul 29 21:58:41 tarantula arpwatch: flip flop 192.168.1.1 0:4:76:f7:85:41 (0:e0:6:9:2:5a) eth0
Jul 29 21:58:41 tarantula arpwatch: ethernet mismatch 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41) eth0
Jul 29 21:58:43 tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41) eth0
Jul 29 21:58:46 tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 29 21:58:46 tarantula arpwatch: reaper: pid 7949, exit status 1
Jul 29 21:58:46 tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory
Jul 29 21:58:46 tarantula arpwatch: reaper: pid 7948, exit status 1
```

# SWATCH

- The active log file monitoring tool
- <http://swatch.sourceforge.net/>
  - Latest rilis version 3.2.1
- Sudo apt-get install swatch

```
y3dips@tarantula:~$ tail -f /var/log/messages
```

```
Jul 29 19:45:25 tarantula kernel: [ 3729.700000] scsi4 : SCSI emulation for USB Mass Storage devices
Jul 29 19:45:30 tarantula kernel: [ 3734.700000] scsi 4:0:0:0: Direct-Access      USB2.0   Mobile Disk        1.00 PQ: 0 ANSI: 2
Jul 29 19:45:30 tarantula kernel: [ 3734.700000] SCSI device sdb: 2015231 512-byte hdwr sectors (1032 MB)
Jul 29 19:45:30 tarantula kernel: [ 3734.700000] sdb: Write Protect is off
Jul 29 19:45:30 tarantula kernel: [ 3734.704000] SCSI device sdb: 2015231 512-byte hdwr sectors (1032 MB)
Jul 29 19:45:30 tarantula kernel: [ 3734.704000] sdb: Write Protect is off
Jul 29 19:45:30 tarantula kernel: [ 3734.704000] sdb: sdb1
Jul 29 19:45:30 tarantula kernel: [ 3734.812000] sd 4:0:0:0: Attached scsi removable disk sdb
Jul 29 19:45:30 tarantula kernel: [ 3734.812000] sd 4:0:0:0: Attached scsi generic sgl type 0
Jul 29 19:45:37 tarantula kernel: [ 3742.180000] usb 3-3: USB disconnect, address 4
Jul 29 19:49:55 tarantula kernel: [ 4000.104000] usb 3-3: new high speed USB device using ehci_hcd and address 5
Jul 29 19:49:55 tarantula kernel: [ 4000.236000] usb 3-3: configuration #1 chosen from 1 choice
Jul 29 19:49:55 tarantula kernel: [ 4000.308000] scsi5 : SCSI emulation for USB Mass Storage devices
Jul 29 19:50:00 tarantula kernel: [ 4005.332000] scsi 5:0:0:0: Direct-Access      USB2.0   Mobile Disk        1.00 PQ: 0 ANSI: 2
Jul 29 19:50:00 tarantula kernel:
Jul 29 19:50:00 tarantula kernel:
Jul 29 19:50:00 tarantula kernel:
Jul 29 19:50:01 tarantula kernel:
Jul 29 19:50:01 tarantula kernel:
Jul 29 19:50:01 tarantula kernel:
```

```
.swatchrc (~) - VIM
File Edit View Terminal Tabs Help
2 exec echo "FlashDisk Baru dikoneksikan"
  echo bold
  exec echo "-----"
```

```
y3dips@tarantula:~$ sudo swatch -c /home/indigo/.swatchrc -t /var/log/messages
```

```
y3dips@tarantula:~$ sudo swatch -c /home/y3dips/.swatchrc -t /var/log/messages
```

```
*** swatch version 3.2.1 (pid:6479) started at Sun Jul 29 19:52:42 WIT 2007
FlashDisk Baru dikoneksikan
Jul 29 19:52:49 tarantula kernel: [ 4173.952000] usb 3-3: new high speed USB device
-----
```

# GTK2-PERL

- The collective name for a set of perl bindings for **Gtk+ 2.x** and various related libraries
- These **modules** make it easy to write **Gtk** and **Gnome** applications
- <http://gtk2-perl.sourceforge.net/>



use Perl;

```
#!/usr/bin/perl -w
```

```
use Gtk2 -init;
```

```
my $window = Gtk2::Window->new ('toplevel');
```

```
my $button = Gtk2::Button->new ('awas arp attack');
```

```
    $button->signal_connect (clicked => sub { Gtk2->main_quit });
```

```
    $window->add ($button);
```

```
    $window->show_all;
```

```
    Gtk2->main;
```

AR PW ATCH

SW AT CH

G TK 2 - PE RL

---

?

indigo@tarantula:~\$ sudo /etc/init.d/arpwatch restart  
Stopping Ethernet/FDDI station monitor daemon: arpwatch.  
Starting Ethernet/FDDI station monitor daemon: (chown arpwatch

tarantula kernel: [11568.700000] atkbd.c: Unknown key pressed (translated from 0x00000000 to 0x00000000)  
tarantula kernel: [11568.700000] atkbd.c: Use 'setkeycodes 55 <keycode>  
tarantula dhclient: No DHCP OFFERS received.  
tarantula dhclient: No working leases in persistent database - sleeping  
tarantula arpwatch: exiting  
tarantula arpwatch: Running as uid=112 gid=116  
tarantula arpwatch: listening on eth0  
tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41)  
tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory  
tarantula arpwatch: reaper: pid 7930, exit status 1  
tarantula arpwatch: ethernet mismatch 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41)  
tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41)  
tarantula arpwatch: ethernet mismatch 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41)  
tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:41)  
tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory  
tarantula arpwatch: reaper: pid 7949, exit status 1  
tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory  
tarantula arpwatch: reaper: pid 7948, exit status 1

Ln 5, Col 26 INS

indigo@tarantula:~\$ sudo swatch -c /home/indigo/.swatchrc -t /var/log/syslog &  
[1] 8486  
indigo@tarantula:~\$  
\*\*\* swatch version 3.2.1 (pid:8486) started at Thu Jul 26 22:12:09 WIT 2007

indigo@tarantula:~\$

Applications Places  
arp-  
awas arp attack

1

2

3

4

5

# ARPWALL

- This tools will give an early warning when **arp attack occurs** and will *simply block the connection*
- <http://arpwall.sf.net> (ver 0.0.1)
- Based on **arpwall + swatch + gtk2perl**
- Need time? And idea?

Welcome to **arpWall** projekt official site

this site are still under construction ... for a while u could browse [here](#)

A stack of browser window thumbnails is shown on the left side of the page. Each thumbnail has a title bar that reads "arp-attack" followed by window control icons. Overlaid on the bottom-most thumbnail are two error messages in a white box with a black border: "ARP ATTACK OCCURS!!".

# SHORTCUT

- Set Static Arp Table
- Sudo arp -s [ip] [mac address]

```
arp -s 192.168.1.1 00-04-76-f7-85-41
```

- Would be a problem
- Still Not 100% surely Secure



- APR
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (27)
- APR-RDP (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.1.1	000476F78541	1234	0	00163685E47F	192.168.1.77

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	216.155.193.160	000476F78541	24	0	00163685E47F	192.168.1.77
Half-routing	209.85.147.83	000476F78541	196	0	00163685E47F	192.168.1.77
Half-routing	217.172.47.239	000476F78541	4	0	00163685E47F	192.168.1.77
Half-routing	216.176.189.68	000476F78541	1257	0	00163685E47F	192.168.1.77
Half-routing	216.139.194.229	000476F78541	521	0	00163685E47F	192.168.1.77
Half-routing	198.107.144.20	000476F78541	491	0	00163685E47F	192.168.1.77
Half-routing	81.22.99.133	000476F78541	123	0	00163685E47F	192.168.1.77
Half-routing	209.85.143.164	000476F78541	57	0	00163685E47F	192.168.1.77
Half-routing	209.85.143.99	000476F78541	85	0	00163685E47F	192.168.1.77
Half-routing	68.142.233.183	000476F78541	3	0	00163685E47F	192.168.1.77
Half-routing	213.236.208.100	000476F78541	14	0	00163685E47F	192.168.1.77
Half-routing	66.249.81.121	000476F78541	13	0	00163685E47F	192.168.1.77
Half-routing	209.85.143.97	000476F78541	39	0	00163685E47F	192.168.1.77

# CONCLUSION

- Fix MAC for each device port
- Using another good Authentication than using MAC address
- Good Network Configuration
- Segmentation (e.g VLAN)
- Monitoring machine

## CONCLUSION ( END USER )

- Using arpwatcH-ng, X-arp, arp-guard, or other arp-defend-application
- using Secure connection (SSL, SSH, IPSec) even still potentially attacked



THATS ALL

FOLKZ

**Have Somethin to Discuss?**

(talk talk talk)