

# UMIT PROJECT



<http://www.umatproject.org>

Luís A. Bastião Silva - [luis.kop@gmail.com](mailto:luis.kop@gmail.com)

[www.twitter.com/luisbastiao](http://www.twitter.com/luisbastiao)

# Índice

- Umit Project
  - Áreas de interesse
  - História e Organização
  - Software Livre
- Umit
  - O que é?
  - Funcionalidade (Perfis, Inventário, Topologia, etc)
- PacketManipulator
- Futuro..?

# Umit Project

- Projecto na área redes informáticas
  - Teste de **Redes** Informáticas
  - **Segurança** nas redes informáticas
  - Teste de **vulnerabilidades**

# Umit Project

- Projecto nasceu em 2005
- Iniciado pela Insecure.org (Nmap)
- Suportado pelo Google Summer of Code entre 2005 e 2009
- Tornou-se uma organização independente desde 2007
- Organização de Software Livre

# Ferramentas de Rede

- **Detecção de Rede**

- Mapeamento de Rede
- Um interface do Nmap, etc
- Detecção de dispositivos Bluetooth

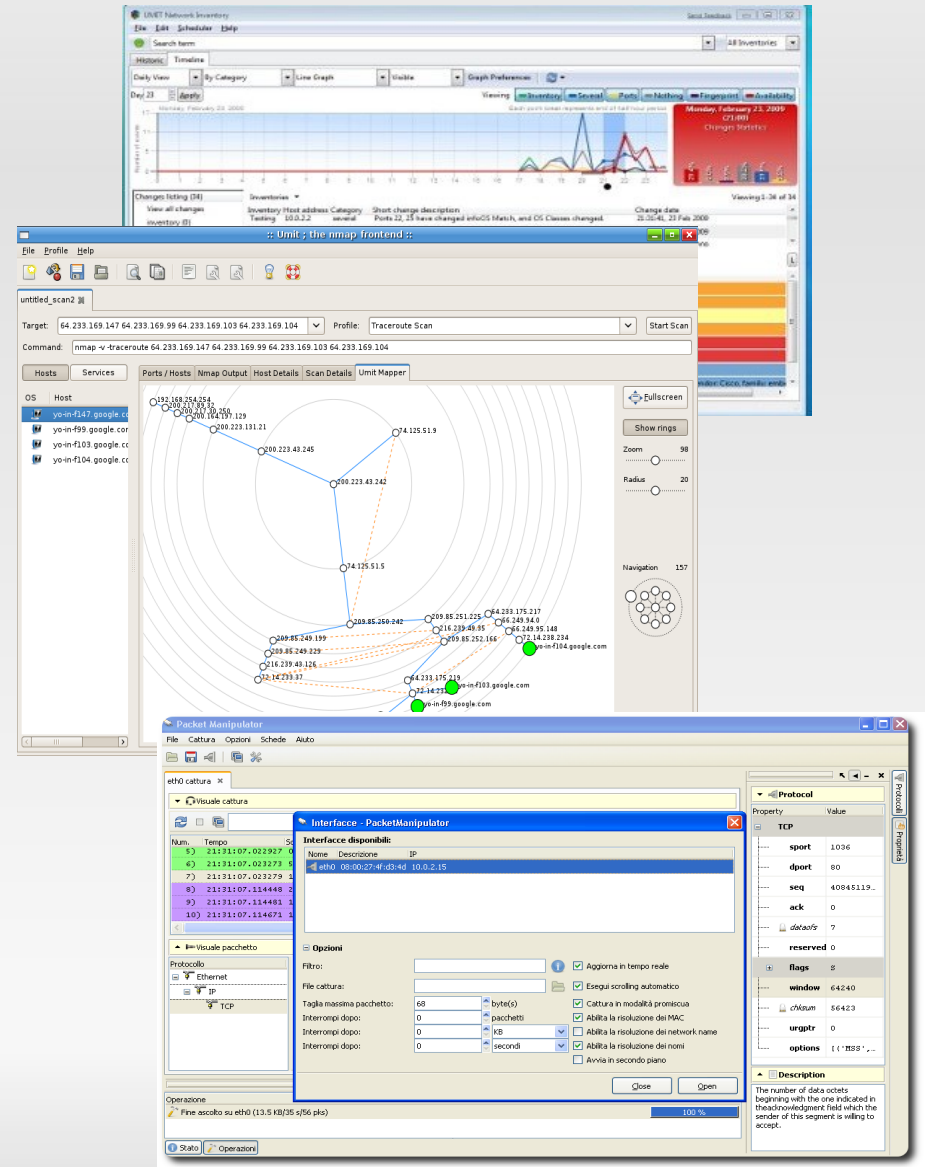
- **Manipulação de Pacotes de rede/Sniffing**

- Criação de pacotes e injectar na rede
- Sniffing de Pacotes
- Interface Gráfico



# Network tools available

- Umit Network Scanner
- UmitWeb
- Umit Bluetooth Scanner
- UMPA
- PacketManipulator



# Umit Network Scanner

0 que é?

# Umit Network Scanner

- Nmap Security Scanner front-end
  - Tirar partido de todas as funcionalidades do Nmap
- Usabilidade
- Fácil de usar por iniciantes
- Útil para *experts* (Guardar, Carregar, Gerir Scans)

# À descoberta na rede..

- Mais que um scan ao mesmo tempo
- Separadores
- Seleccionar um **Perfis** por cada scan
  - Descoberta sistemas operativos, serviços, etc.
- Mostrar facilmente **todas as estações da rede**
- Mostrar todos os serviços e estações a utilizar um determinado serviço

# Umit Network Scanner

Umit

Scan Tools Profile Help

New Scan Command Wizard Save Scan Open Scan Stop Scheduler Report a bug Help

Operating System Detection on 192.168.1.0/24

Target: 192.168.1.0/24 Profile: Operating System Detection Scan

Command: nmap -O -v 192.168.1.0/24

OS	Host
	login.router 192.168.1.1 (00:30:0A)
	bastiao-desktop 192.168.1.3 (00:C)
	192.168.1.4

Nmap Output Ports / Hosts Host Details Scan Details Topology

Up time: Not available  
Last boot: Not available

Addresses  
IPv4: 192.168.1.4  
IPv6:  
MAC:

Operating System  
Name: Apple Mac OS X 10.5 - 10.5.5 (Leopard) (Darwin 9.0.0 - 9.5.0)  
Accuracy: 100%

Ports used  
Port-Protocol-State: 3306 - tcp - open  
Port-Protocol-State: 1 - tcp - closed  
Port-Protocol-State: 34418 - udp - closed

OS Class

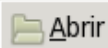
TCP Sequence

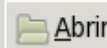
# Comparação de relatórios

- Comparar dois resultados distintos
- Colorir as diferenças
- Comparação gráfica..

# Comparação de relatórios

Compare Results




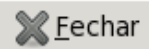
Scan Result 1: scan1.usr 

Scan Result 2: scan2.usr 

Comparison

	Section	Property	Original value	Current value
▶ M	Scan Info			
▶	Host 192.168.1.4			
▼ M	Host 192.168.1.3			
M	LastBoot		Wed Jul 8 13:39:33 2009	Wed Jul 8 14:24:07 2009
U	OS Match		Linux 2.6.13 - 2.6.25	Linux 2.6.13 - 2.6.25
▶ M	Extraports			
▼ M	Ports			
▼ M	22			
N	State		open	
N	Service Name		ssh	
N	Protocol		tcp	
N	Service Conf		3	
▶	80			
▶	111			
▶	139			
▶	445			

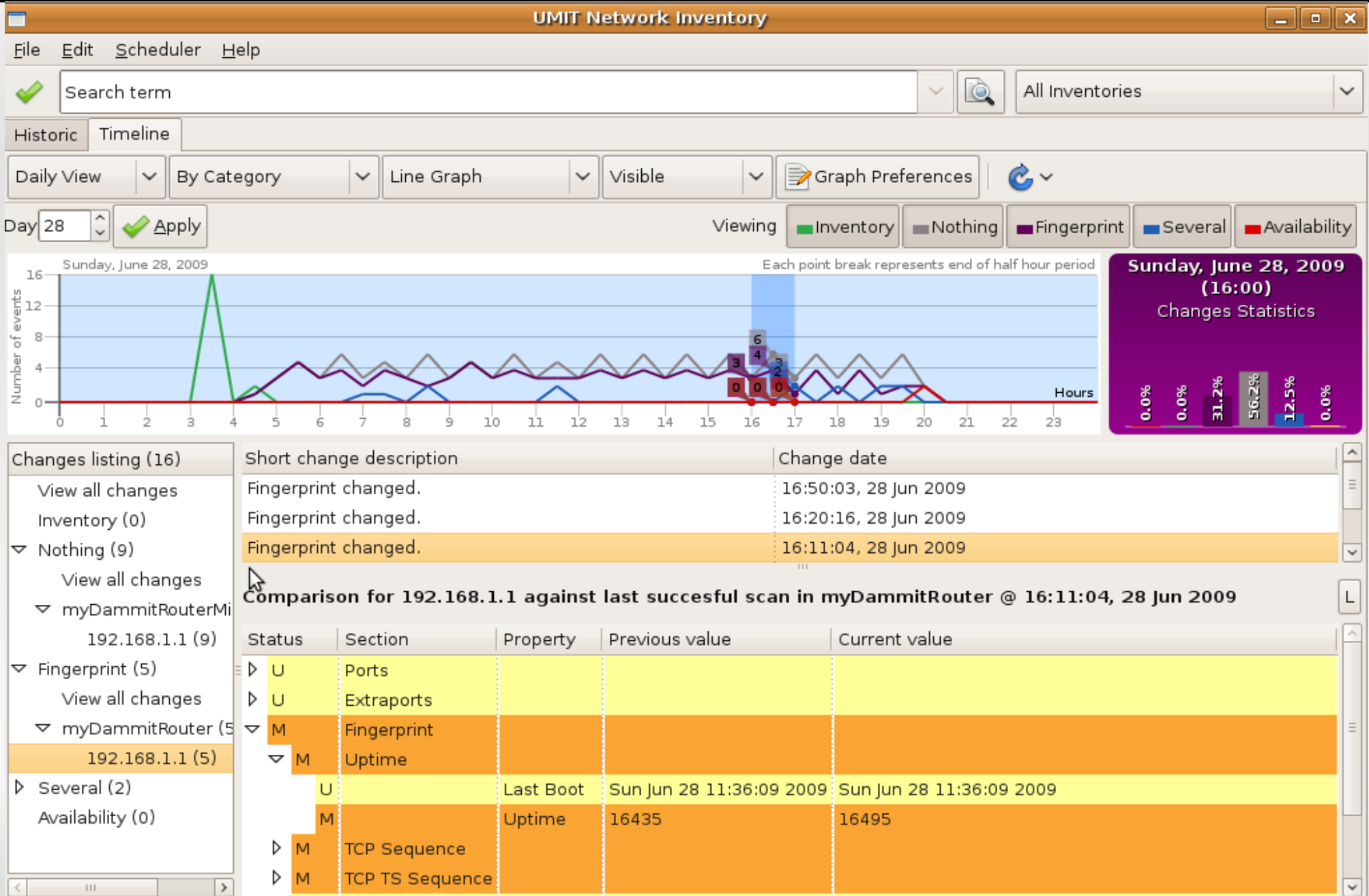
Text Mode | Compare Mode |  Enable colored diffies

# Inventory/Scheduler

- **Agendar** um scan para correr em segundo plano
  - Guardar o histórico da rede
  - Enviar relatório **via email**
  - Adicionar relatório à base de dados
- **Inventário de Rede**
  - Linha temporal
  - Diferenças temporais no histórico da rede
  - Pesquisa nos relatórios

# Network Inventory



# Umit Mapper – Topologia de Rede

- Topologia de Rede em forma Radial
- Exploração da rede através da visualização gráfica

# Topologia de Rede

Umit

Scan Tools Profile Help

Operating System Detection on 192.168.1.4 x untyped\_scan3 x Quick traceroute on google.com/28 scamenmap.org/28 x untyped\_scan5 x

Target: google.com/28 scamenmap.org/28 Profile: Quick traceroute Scan

Command: nmap -PN -p80 --traceroute google.com/28 scamenmap.org/28

Hosts Services

OS	Host
	gw-in-f96.google.com 74.125.67.100
	gw-in-f97.google.com 74.125.67.98
	74.125.67.98
	gw-in-f99.google.com 74.125.67.100
	google.com 74.125.67.100
	gw-in-f101.google.com 74.125.67.105
	gw-in-f102.google.com 74.125.67.106
	gw-in-f103.google.com 74.125.67.107
	gw-in-f104.google.com 74.125.67.108
	74.125.67.105
	74.125.67.106
	74.125.67.107
	74.125.67.108
	74.125.67.109
	74.125.67.110
	74.125.67.111
	scamenmap.org 64.13.134.49
	insecure.org 64.13.134.49

Ports / Hosts Nmap Output Host Details Scan Details Topology

Tools

Controls Fisheye Fullscreen

gw-in-f101

p0-0-0.MAR1.Fremont-CA.us.xo.net

p0-0.chr1.fremont-ca.us.xo.net

ip65-46-255-94.z255-46-65.customer.elgix.net

sectools.org scanme.nmap.org apress.com ip65-46-255-94.z255-46-65.customer.elgix.net

cust-134-55.titan.net cust-134-56.titan.net ns1.titan.net ns2.titan.net nsw.c www.titan.net

Action

Red

Interpolation

Layout

View

Enable

address

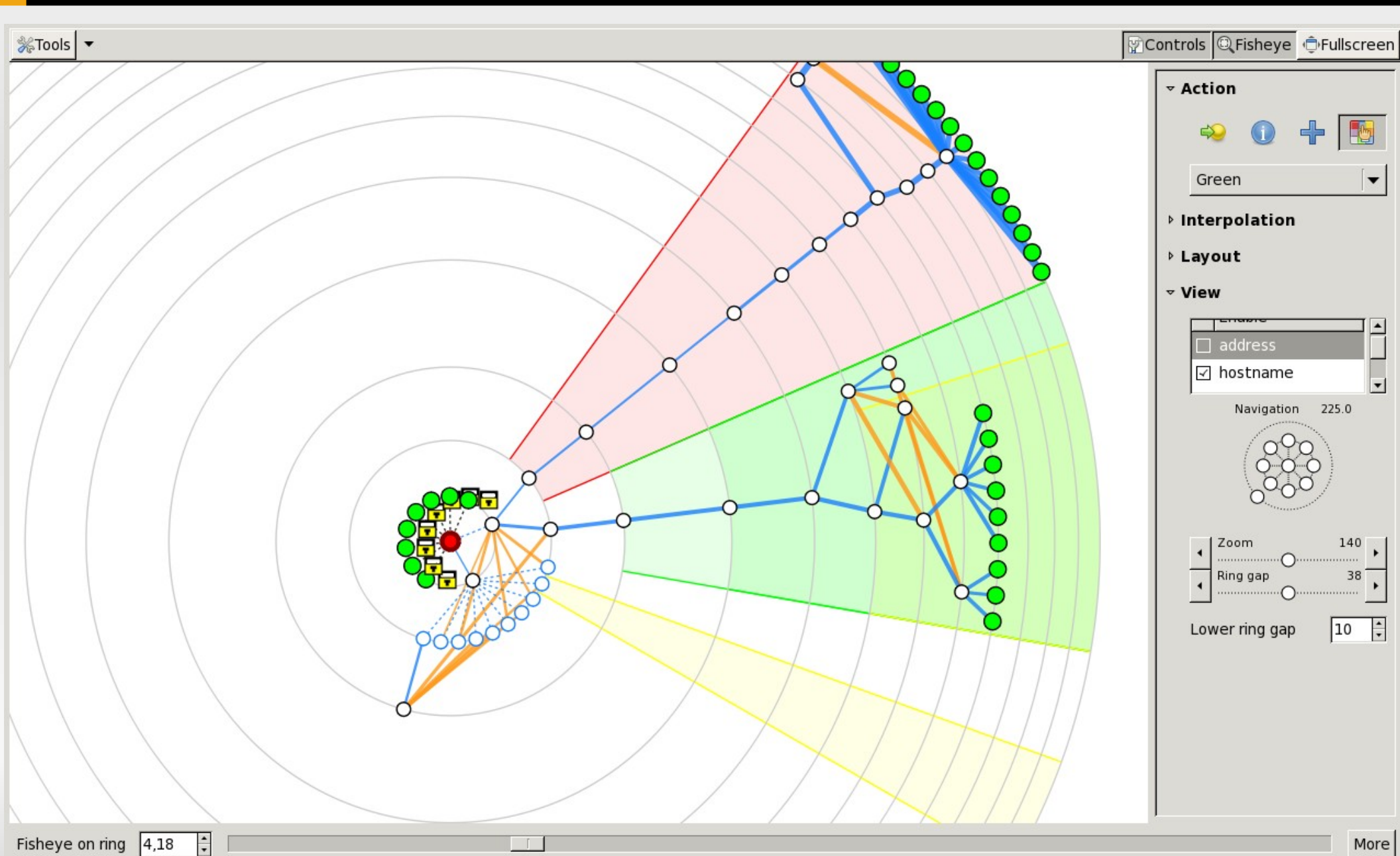
hostname

Navigation 225.0

Fisheye on ring 9.63

More

# Topologia de Rede



# Umit Web

“O UmitWeb é uma interface **Web** para o Network Scanner. O objectivo do projecto é fazer fácil e rapidamente os **scans remotamente**. Apenas é necessário um Web Browser com ligação à Internet e assim conectar à rede local e verificar o seu estado..”

# UmitWeb

Umit :: The nmap frontend

http://localhost:8059/js/




Command Wizard Compare Results Open Scan Save Scan

## UMIT The nmap Frontend

Target:  Profile:



Command:

**Hosts** Services

OS	Host
	login.router
	bastiao-desktop
	192.168.1.4

Ports/hosts Nmap Output **Host Details** Scan Details

**Host Details**

- Comment
- Host Status
  - State: up
  - Open ports: 2 
  - Filtered ports: 0
  - Closed ports: 998
  - Scanned ports: 1000
  - Up time: 149030
  - Last boot: Tue Jul 7 11:41:21 2009 
- Addresses
  - IPV4: 192.168.1.1
  - IPV6:
  - MAC: 00:30:0A:1E:E1:00
- Hostnames
- Operating System
  - Name: Linux 2.4.9 - 2.4.18 (likely embedded)
  - Accuracy: 

100%
- Ports Used
- OS Class
- TCP Sequence

Concluído

6

# Packets Manipulation/Sniffing

PacketManipulator

# PacketManipulator

- Interface Gráfica
- Administradores de Rede podem **criar pacotes**
  - Enviar pacotes para a rede
- Sniffing dos Pacote
- Editar os pacotes e criar **uma sequência de pacotes**

# PacketManipulator

The screenshot displays the Packet Manipulator application window. The title bar reads "Packet Manipulator". The menu bar includes "File", "Capture", "Options", "Views", and "Help". The interface is divided into several sections:

- Protocols/Properties:** A sidebar on the left showing TCP properties such as `spo: 53578`, `dpo: 5222`, `seq: 76740...`, `ack: 25373...`, `data: 8`, `rese: 0`, `flag: A`, `winc: 65535`, `chks: 27915`, `urg: 0`, and `opti: [ ('NO...`.
- en1 capture x Unsaved sequence x:** A central pane showing a "Sniff perspective" of network traffic. It contains a table with columns: No., Time, Source, Destination, Protocol, and Info.
- Finished sniffing on en1 (22.7 KB/14 s/86 pks):** A yellow notification bar.
- Packet perspective:** A pane at the bottom showing a detailed view of a packet. It includes a "Protocol" dropdown set to "TCP", a hex dump, and a corresponding ASCII dump.
- Status Bar:** A bottom section with three green checkmarks and text: "PacketManipulator 0.2 started on posix", "Using scapy as backend", and "What do you wanna pwn today?".

No.	Time	Source	Destination	Protocol	Info
76)	14:26:47.625175	192.168.1.4	209.85.229.125	TCP	Ether / IP / TCP 192.168.1.4:53578 > 209.85.229.125:jabber_clie...
77)	14:26:47.626252	209.85.229.125	192.168.1.4	TCP	Ether / IP / TCP 209.85.229.125:jabber_client > 192.168.1.4:535...
78)	14:26:47.626287	192.168.1.4	209.85.229.125	TCP	Ether / IP / TCP 192.168.1.4:53578 > 209.85.229.125:jabber_clie...
79)	14:26:47.651489	209.85.229.125	192.168.1.4	TCP	Ether / IP / TCP 209.85.229.125:jabber_client > 192.168.1.4:535...
80)	14:26:47.651547	192.168.1.4	209.85.229.125	TCP	Ether / IP / TCP 192.168.1.4:53578 > 209.85.229.125:jabber_clie...
81)	14:26:47.653131	209.85.229.125	192.168.1.4	TCP	Ether / IP / TCP 209.85.229.125:jabber_client > 192.168.1.4:535...
82)	14:26:47.653165	192.168.1.4	209.85.229.125	TCP	Ether / IP / TCP 192.168.1.4:53578 > 209.85.229.125:jabber_clie...
83)	14:26:47.859266	209.85.229.125	192.168.1.4	TCP	Ether / IP / TCP 209.85.229.125:jabber_client > 192.168.1.4:535...

Protocol	Hex	ASCII
00	00 30 0A 1E E1 00 00 1E C2 9E 78 F7 08 00 45 00	.0.....X...E.
01	00 34 80 F2 40 00 40 06 41 52 C0 A8 01 04 D1 55	.4..@.@.AR....U
02	E5 7D D1 4A 14 66 2D BD A3 AE 97 3D 76 BA 80 10	.}.J.f-....=v...
03	FF FF 6D 0B 00 00 01 01 08 0A 31 02 9C C9 35 04	..m.....1...5.
04	C9 4D	M

# Próximos desenvolvimentos..

- Quick Scan
  - Umit Scanner *spotlight-style*
- ZION
  - Novo método para descobrir sistemas operativos
- UMPA - Novas funcionalidades
- Framework de Auditoria (Passiva e Activa)
- Bluetooth Sniffing (usando hardware específico)

# The Bourne Ultimate

The screenshot displays a network scanner interface with several components:

- Hosts List:** A table of IP addresses and their corresponding hostnames.
- Services:** A list of services running on the hosts, including ftp, rpsbind, http, unknown, telnet, netbios-ssn, ipp, sometimes-ftp, nfs, ssh, and msft-ds.
- Terminal:** A terminal window showing the output of the 'show tag 443' command, including the last login time and the start of an email message.
- Email Content:** An email from adrian.spanno@guardian.co.uk to simon.ross@guardian.co.uk with the subject 'flight details conf ASAP'. The body contains flight information for Flight (MSC)-2538 and Flight (MSC)-2539.
- Bottom Panel:** A navigation bar with tabs for POLICY, OUTSIDE, INSIDE, LOOP, and SPS, and a status bar showing the current host and service.

IP	Host
194.6.1.219	
196.23.147.34	
200.52.4.82	
202.105.130.19	
202.110.220.14	
196.40.43.34	
200.61.6.50	
202.105.230.226	
202.9.136.40	
200.21.225.82	
202.103.6.170	
202.106.139.80	
202.99.225.45	
200.21.225.82	
202.103.6.170	
202.106.139.80	
202.100.122.30	

```
loading....
Chain 14, UMIT Recover from SMTP- smtp.guardian.co.uk
File 23
From: adrian.spanno@guardian.co.uk
Subject: flight details conf ASAP
Date: 17:53:21 80T
To: simon.ross@guardian.co.uk
Return-Path: <adrian.spanno@guardian.co.uk>
Delivery-Date: 17:48:55 +0100
Received: from mail.guardian.co.uk ([195.72.171.30]) by mail.guardian.net.uk with esmtp (Exim 4.52)
id 1DshWf-00023o-8b for simon.ross@guardian.co.uk; 17:48:55 +0100
Envelope-To: simon.ross@guardian.co.uk
Message-Id: <64070046A0F712458139A7E11326731112055A@guardian.co.uk> Mime-Version: 1.0

Ross, Simon mr

Flight-(MSC)-2538 Fri 17 Nov 2006

Outbound
Flight 2538
Status:
Class of Service:
Depart: 06:00 AM
Fri 17 Nov 2006

Non-stop
Confirmed (HK)
Euro (M)
Arrive: 08:00 AM
Fri 17 Nov 2006

Heathrow Arpt (LTR)
London
Terminal N

Citta Di Torino Arpt (TRN)
Turin
Terminal C

Eticket ref no: 2897XH
Travel services ref no: UK938934

Flight-(MSC)-2539 Fri 17 Nov 2006

Return
Flight 2539
Status:
Class of Service:
Depart: 12:00 PM
Fri 17 Nov 2006

Non-stop
Confirmed (HK)
Euro (M)
Arrive: 1:05 PM
Fri 17 Nov 2006

Citta Di Torino Arpt(TRN)
Turin
Terminal C

Heathrow Arpt (LTR)
London
Terminal N
```

# Como ajudar?

- Reportar problemas
- Traduções
- Envolvimento com a comunidade
- Design gráfico (imagens, icons, etc)
- Desenvolver (corrigir bugs, adicionar funcionalidades, plugins, etc)

# Obrigado pela vossa atenção!



**Junta-te a nós! :)**

**<http://www.umatproject.org>**

**<http://blog.umatproject.org>**

**<http://trac.umatproject.org>**

**[twitter.com/umatproject](https://twitter.com/umatproject)**