Boas Práticas no Tratamento de Incidentes de Segurança

Italo Valcy da Silva Brito[1,2]
Luciano Porto Barreto[1,2]
Thiago Lima Bomfim de Jesus[1,2]
Jerônimo Aguiar Bezerra[1,2]

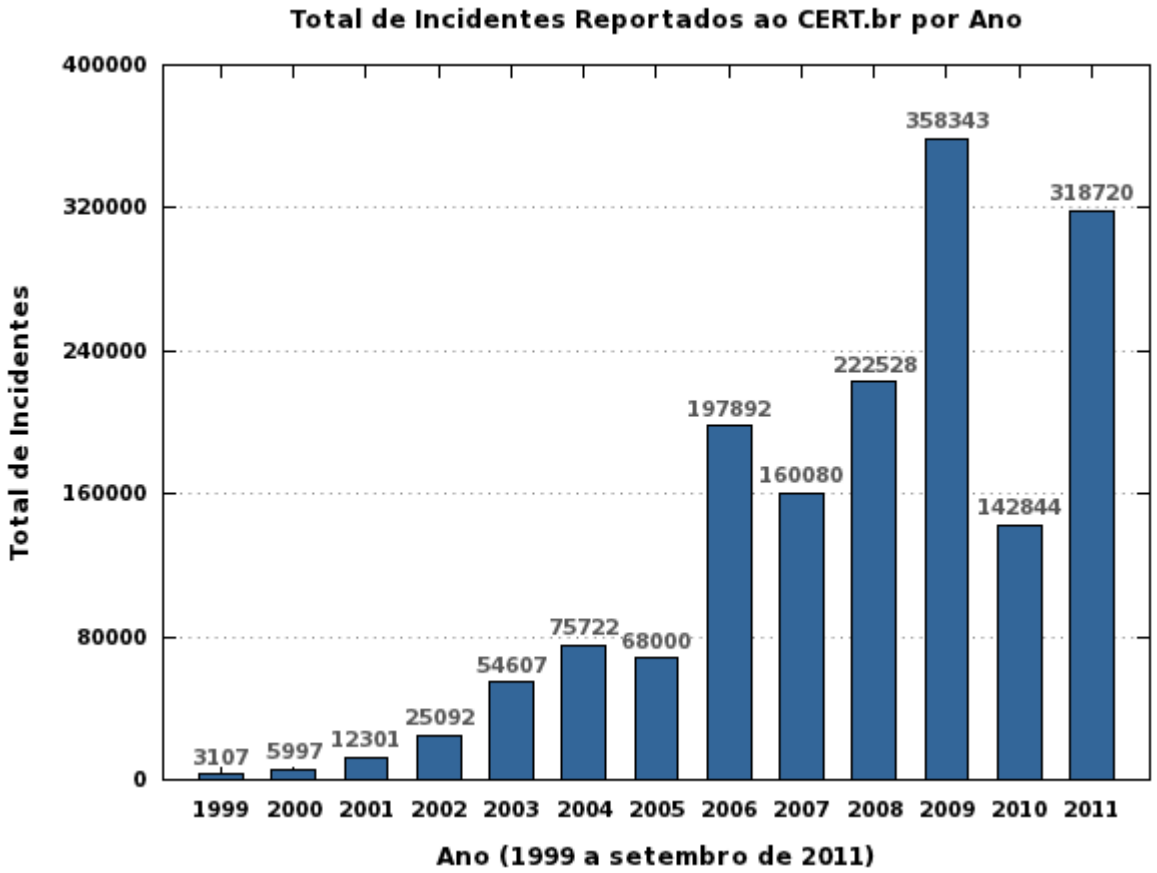
[1]Universidade Federal da Bahia (UFBA)
Salvador, BA – Brasil

[2]Grupo de Resposta a Incidentes de Segurança – Bahia/Brasil (CERT.Bahia)
Ponto de Presença da RNP na Bahia (PoP-BA/RNP)
Salvador, BA – Brasil

GTS-18, 03/Dez/2011

Motivação

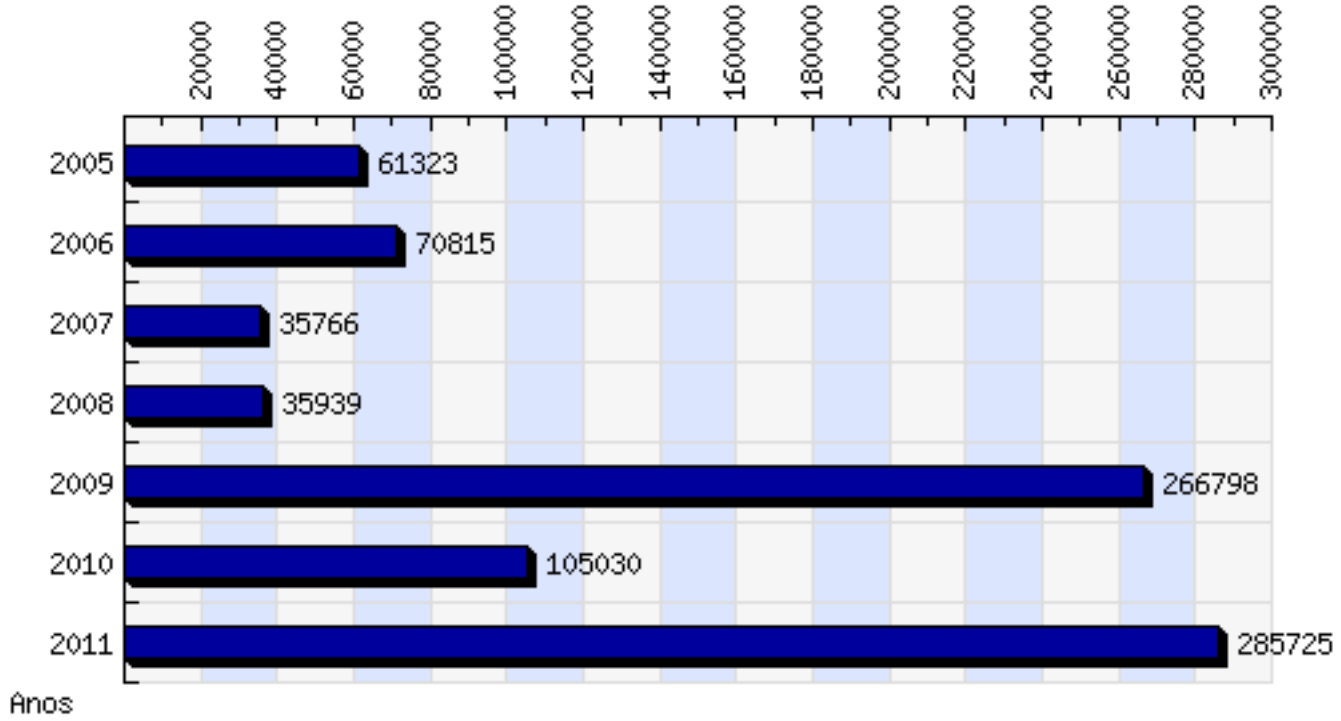
Estatísticas do CERT.br



Fonte: http://www.cert.br/stats/incidentes/

Motivação

Estatísticas do CAIS/RNP



Fonte: http://www.rnp.br/cais/estatisticas/

Motivação

Estatísticas do CERT.Bahia

- Estatísticas do CERT.Bahia (dados coletados entre Jan/2010 e Jun/2011):
  - **1778** notificações do tipo *host possivelmente infectado com vírus/worm* (88.3%);
  - **79** notificações de *envio de spam* (3.9%);
  - **48** notificações relacionados à *violação de copyright* (2.4%);
  - Dentre outros

Fonte: http://certbahia.pop-ba.rnp.br/Estatisticas

Motivação

Dificuldades da resposta a incidentes

- Grande desafio para equipes de segurança
  - Volume de notificações, heterogeneidade, tecnologias (e.g. NAT e DHCP)
- Limitação de equipe e carência de ferramentas especializadas
- Inviável e custoso o tratamento/intervenção manual em redes corporativas (e.g. máquinas infectadas com software malicioso).

Importante: automatização do processo de tratamento

Motivação

Combate a código malicioso

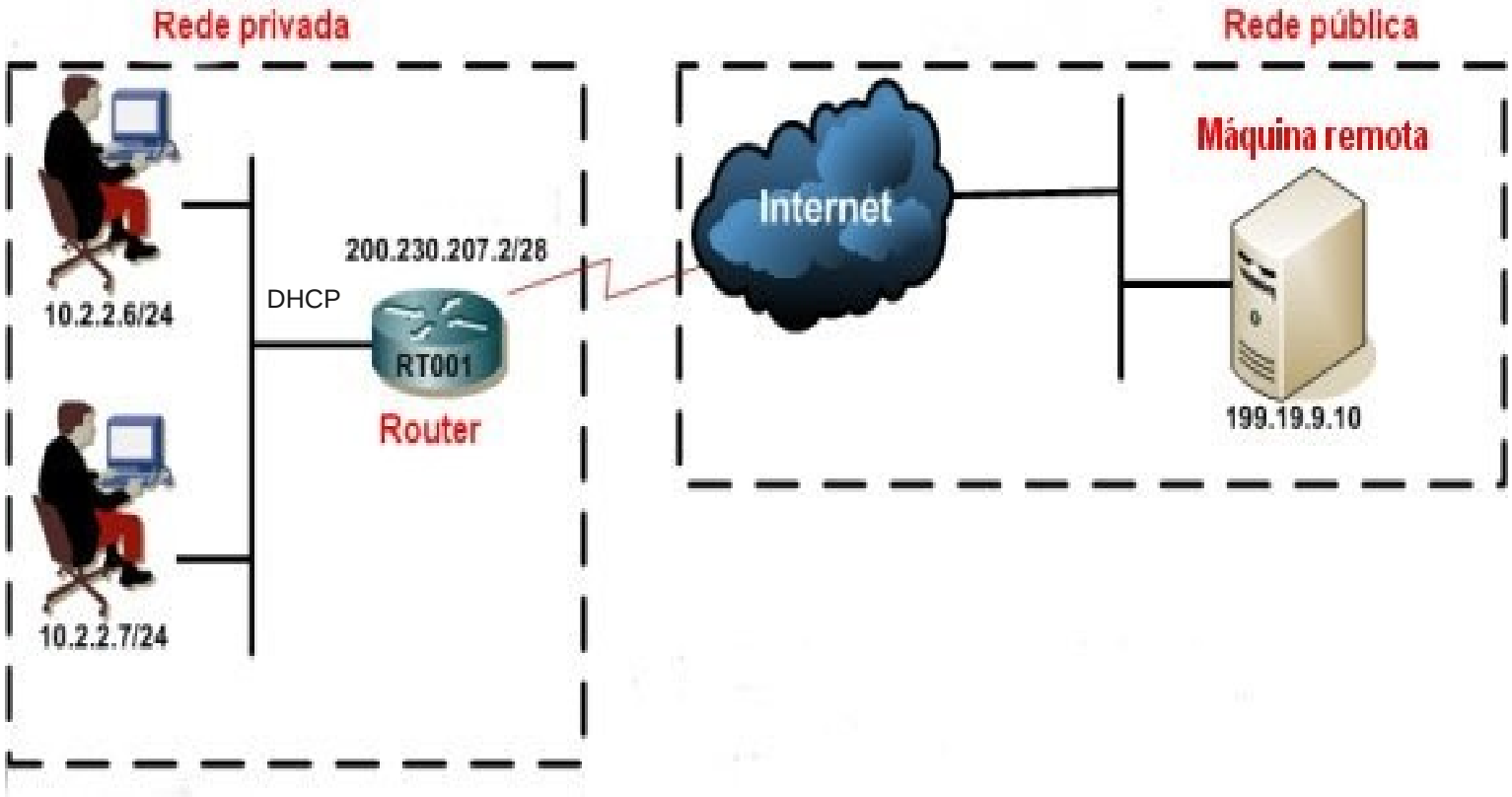
- Grande quantidade de hosts infectados com malware (bots/worm)
  - Hosts utilizados para ataques em larga escala (e.g., envio de spam, ataques DDoS, etc.)
- Atividade maliciosa contribuindo para ineficiência ou esgotamento dos recursos na rede
  - Impacto financeiro e na qualidade da rede
- Atacantes explorando a infraestrutura da rede brasileira nos ataques em larga escala (e.g., NRI/RNP – 10Gbps)

Necessário: estratégias céleres de contenção e mitigação de atividade maliciosa

Motivação

Contexto

- Supomos o seguinte cenário (comum nas instituições ligadas ao nosso CSIRT)



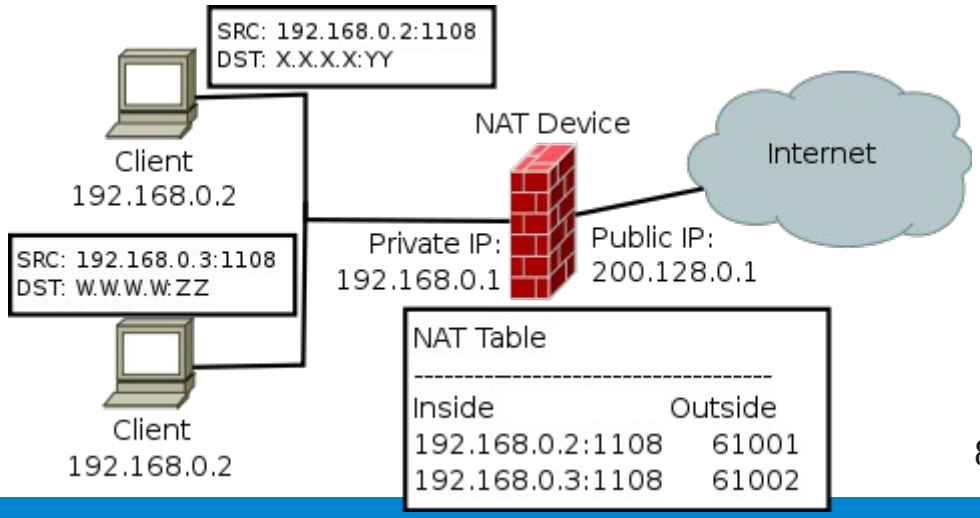
- Interesse: incidentes ***gerados*** pela instituição

Motivação

Principais dificuldades do tratamento de incidentes - NAT

Network Address Translation (NAT)

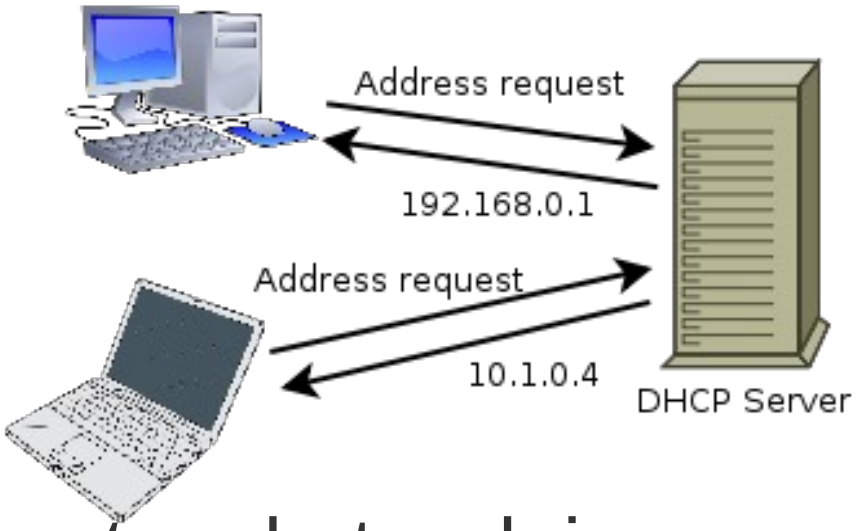
- Técnica NAT44 + RFC 1918
- Problema:
  - Dificuldade em determinar, com precisão, o endereço IP interno mapeado no endereço externo*
  - Suporte à *logging* nos dispositivos de NAT
    - *iptables não suporta*
  - Busca nos *logs*



** Em alguns casos a porta de origem original precisa ser alterada*

Principais dificuldades do tratamento de incidentes - DHCP

Dynamic Host Configuration Protocol (DHCP)



- Problema: um *host* pode ter dois ou mais endereços IP por dia, semana ou mês (*lease time*); um IP pode pertencer a mais de um host
  - Complexo correlacionar *IP e host no tempo*

Principais dificuldades do tratamento de incidentes - *Logs*

Registros (logs) do sistema

- Problema: volume de dados para salvaguarda e análise
- Exemplo da Rede UFBA: *logs* de NAT (valores médios diários em Nov/2010)
  - 3.9GB por arquivo sem compactação
  - Mais de 7 milhões de registros de traduções NAT

Motivação

Rede UFBA (rede de campus)

- Presente em 4 municípios
- Três campus na sede:
  - > 60 edifícios
  - > 400 switches gerenciáveis / ~ 150 VLANs ativas
  - > 12k dispositivos
  - > 150 pontos de acesso sem fio ativos e conhecidos
    - > 400 em 2012
  - 100% do backbone conectado ao CPD via fibra ótica
  - 3 routers principais + firewall redundante
- Heterogeneidade de equipamentos e software

Motivação

Estado da arte

- Soluções proprietárias (e.g., Cisco CSA)
  - Alto custo de implantação
  - Heterogeneidade da rede
- Soluções de tratamento de incidentes manual

Motivação

Estado da arte

- Soluções proprietárias (e.g., Cisco CSA)
  - Alto custo de implantação
  - Heterogeneidade da rede
- Soluções de tratamento de incidentes manual
- Ignorar as notificações de incidentes

```
# /etc/aliases
security@instituicao.domain: /dev/null
```

Nossa proposta

- Duas propostas para o ciclo de tratamento de incidentes:
  - Honeypots na rede interna (por VLAN)
  - Ferramenta para tratamento automatizado de incidentes de segurança: TRAIRA
- Contribuições:
  - Detecção antecipada de atividade maliciosa
  - Análise e Contenção automatizados de *hosts* envolvidos em um incidente de segurança
  - Baixo custo e Eficiência no Tratamento de Incidentes
  - Independente da tecnologia e equipamentos de rede utilizados (rede heterogênea)
  - Facilidade de aplicação em outras instituições

Escopo da palestra

- ***Detecção*** antecipada de atividade maliciosa
- ***Análise*** automatizada de notificações
- ***Contenção*** do *host* responsável pelo incidente
- Resultados e projetos futuros

Detecção antecipada

Uso de honeypot nas VLANs acadêmicas da rede

- *"Um* honeypot *é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido"*[1] (baixa e alta interatividade)
  - Não divulgado => Todo acesso potencialmente suspeito
- Geralmente hospedados em endereços públicos na Internet
  - Sujeitos à Firewalls do tipo filtro de pacote

[1] - Honeypots: Tracking Hackers, Lance Spitzner

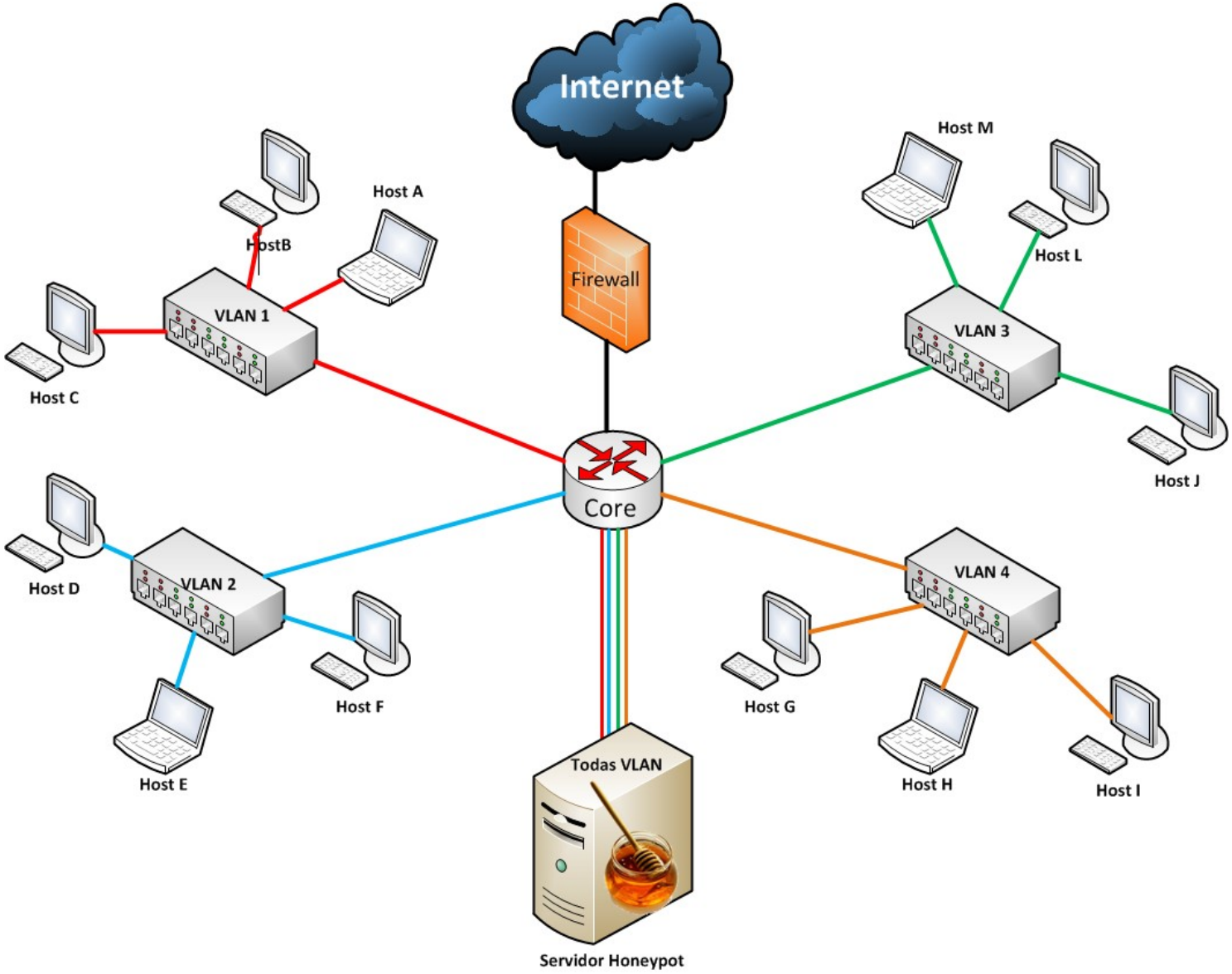
Detecção antecipada

Uso de honeypot nas VLANs acadêmicas da rede

- Um *honeypot* é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido (baixa e alta interatividade)
  - Não divulgado => Todo acesso potencialmente suspeito
- Geralmente hospedados em endereços públicos na Internet
  - Sujeitos à Firewalls do tipo filtro de pacote
- Proposta: **usar honeypots na rede interna**

Detecção antecipada

Uso de honeypot nas VLANs acadêmicas da rede



Detecção antecipada

Uso de honeypot nas VLANs acadêmicas da rede

- Objetivo: colocar honeypots para detectar atividade maliciosa nas VLANs da Universidade
- Plataforma: *honeyd*[2] modificado para tratar VLANs (baixa interatividade)
- Principais desafios:
  - Tráfego de descoberta de serviços no honeypot
  - Frequência de geração das notificações
  - Quais VLANs monitorar

[2] - http://www.honeyd.org/

Análise automatizada

- UFBA tem uma taxa média semanal de 50 incidentes de segurança
- Além disso, outros fatores agravam:
  - NAT
  - DHCP “dinâmico”
  - Carência de pessoal
- Proposta: **automatizar o processo de tratamento de incidentes**

Análise automatizada

TRAIRA – Tratamento de Incidentes de Rede Automatizado

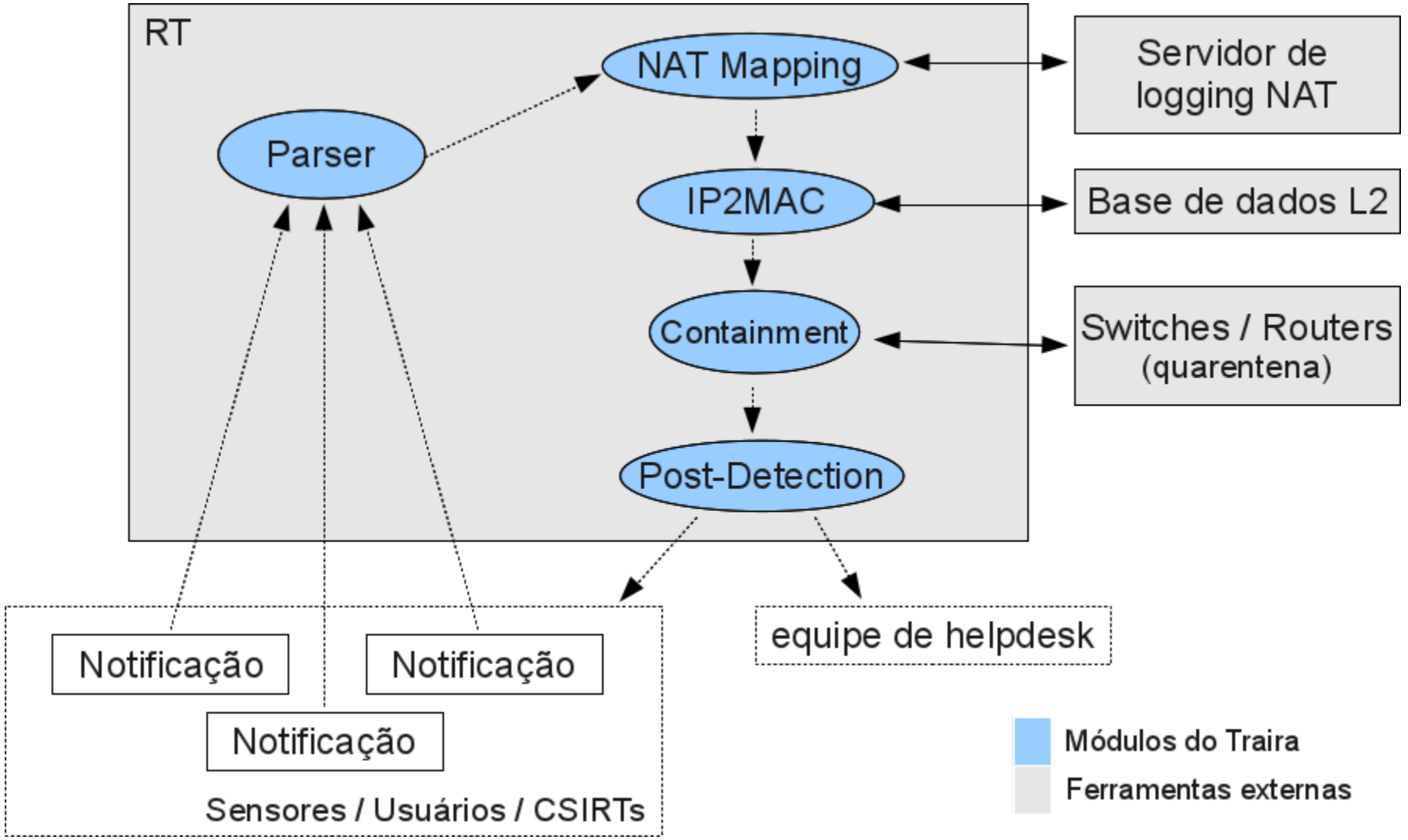
- TRAIRA: Ferramenta para automatização do tratamento de incidentes de segurança
  - Contexto: Rede UFBA, CERT.Bahia
- Características:
  - Modular, extensível
  - Fácil implantação em ambientes heterogêneos
  - Relatórios/Estatísticas automáticos
  - Geração automática de Resposta

TRAIRA – Tratamento de Incidentes de Rede Automatizado

- Objetivo principal: efetuar a detecção, identificação e isolamento da máquina geradora do incidente.
- Plataforma: desenvolvido em *Perl* como extensão do *Request Tracker* (RT) – ferramenta livre para tratamento de incidentes
  - Cerca 2.500 linhas de código
- Baseado no ciclo de vida da resposta a incidentes[3]:

[3] - Computer Security Incident Handling Guide, Scarfone et. al. 2008, NIST

TRAIRA – Arquitetura



TRAIRA – Fluxo de execução

honeypot

outros sensores

CSIRT

Prezado(a) responsavel pela InstituicaoTeste,

O endereco IP 200.128.99.1 foi detectado como possivelmente infectado e propagando virus. Abaixo seguem algumas evidencias coletadas:

53164 | 200.128.99.1 | 2010-03-31 22:50:20 srcport 51774 | (GMT-3) | PoP-BA/RNP
53164 | 200.128.99.1 | 2010-04-01 10:38:11 srcport 59441 | (GMT-3) | PoP-BA/RNP
53164 | 200.128.99.1 | 2010-04-01 10:58:00 srcport 59441 | (GMT-3) | PoP-BA/RNP
53164 | 200.128.99.1 | 2010-04-01 13:10:30 srcport 24475 | (GMT-3) | PoP-BA/RNP

TRAIRA

helpdesk

CSIRT

Prezados,

Segue abaixo uma relacao <IP | MAC | UNIDADE> das maquinas detectadas como possivelmente comprometidas com virus/worm. Favor realizar o tratamento das maquinas (ex: anti-virus, etc.).

10.1.0.8 | 00:16:3e:ef:dc:6b | Rede_Lab1

Prezados,

Com base na notificacao abaixo, foi detectada 1 maquina possivelmente infectada em nossa rede interna. O tratamento dessa maquina ja foi iniciado.

Obrigado pela notificacao.

TRAIRA::Parser

- ***TRAIRA::Parser*** é o módulo responsável pelo recebimento da notificação e pela extração das informações essenciais ao tratamento do incidente (e.g., endereço IP e Porta de origem, data e horário)

- O Parser a ser usado em uma notificação é definido pelo *From* e *Subject* da notificação

TRAIRA::NATMapping

- ***TRAIRA::NATMapping*** é o módulo que faz o mapeamento entre o IP externo e IP interno

Desafios:

- Não é suficiente buscar por IP, nem IP+PORTA
- Problema da correspondência temporal
  - É difícil, na prática, manter relógios sincronizados
  - Duração do NAT
  - Suporte pelos *vendors*. Ex: IPTables/Netfilter não suporta!
    - Proposta: ***NFCT-SNATLOG***

TRAIRA::NATMapping

TRAIRA::NATMapping – casamento de padrão nos *logs*, baseado na configuração do ambiente:

- Segmento de rede
- *Driver* de NATMapping (iptables / asa_cisco, etc)
- Arquivo de *log*
- Tolerância temporal

Exemplo:

Rede	NATMapping	Arquivo de *log*
200.128.99.0/24	`Traira::NATMapping::asa_cisco`	`/var/log/local4-%Y%m%d.log`
200.128.196.0/23	`Traira::NATMapping::iptables`	`/var/log/nfct-snatlog-%Y-%m-%d.log`
200.128.197.0/28	`Traira::NATMapping::asa_cisco`	`/var/log/local4-%Y%m%d.log`
200.128.199.0/24	`Traira::NATMapping::none`	–

TRAIRA::IP2MAC

- O endereço IP pode não ser uma identificação precisa do host:
  - Para redes que atribuem IP dinâmico via DHCP, um mesmo IP pode ser usado por diversas máquinas ao longo do dia
  - Fácil de ser alterado pelo usuário
- Opção: utilizar endereço MAC
- Requisito: consultar a tabela ARP dos roteadores

TRAIRA::IP2MAC

- No entanto...
  - A tabela ARP é dinâmica
- Consequência: precisamos de um mecanismo, ou software, que armazene o histórico da tabela ARP
- No TRAIRA, utiliza-se o L2M[4] como base de consulta para o histórico da tabela ARP
- O módulo IP2MAC recebe uma lista de IPs internos, data e hora de acesso, consulta o L2M e acrescenta o MAC e VLAN de cada tupla

[4] L2M (Layer 2 Manager) é um software desenvolvido pela UFBA e CERT.Bahia para gerenciamento de recursos da camada de enlace.

TRAIRA::Containment

- **Contenção**: cessar propagação de atividade maliciosa até o tratamento efetivo do *host*

- Desafios da contenção manual:
  - Tempo de exposição do dispositivo infectado
  - Horário não comercial

- Listamos três possibilidades de contenção:
  - Bloqueio do *host* no roteador daquela VLAN
  - Bloqueio do *host* no *switch* gerenciável mais próximo
  - Traslado do *host* para VLAN de quarentena

TRAIRA::Containment

- Implementação atual:
  - A contenção está implementada na sua forma mais simples: bloqueio do *host* no roteador
  - Além disso, a contenção é “dependente” do L2M
  - *whitelist* para evitar bloqueio em VLANs críticas

- Melhor caso: VLAN de quarentena
  - Requisito: suporte à MAC-based VLAN (ou via ACL)
  - Nos testes realizados na UFBA (3com, D-Link, Extreme Networks), apenas UM implementava

Resultados e Projetos futuros

Detecção antecipada

- ~ 300 incidentes notificados pelo honeypot: 07 abril à 07 Julho / 2011
  - Scans de rede
  - Propagação de vírus
- Redução das notificações externas
- Detecção de incidentes em VLANs importantes

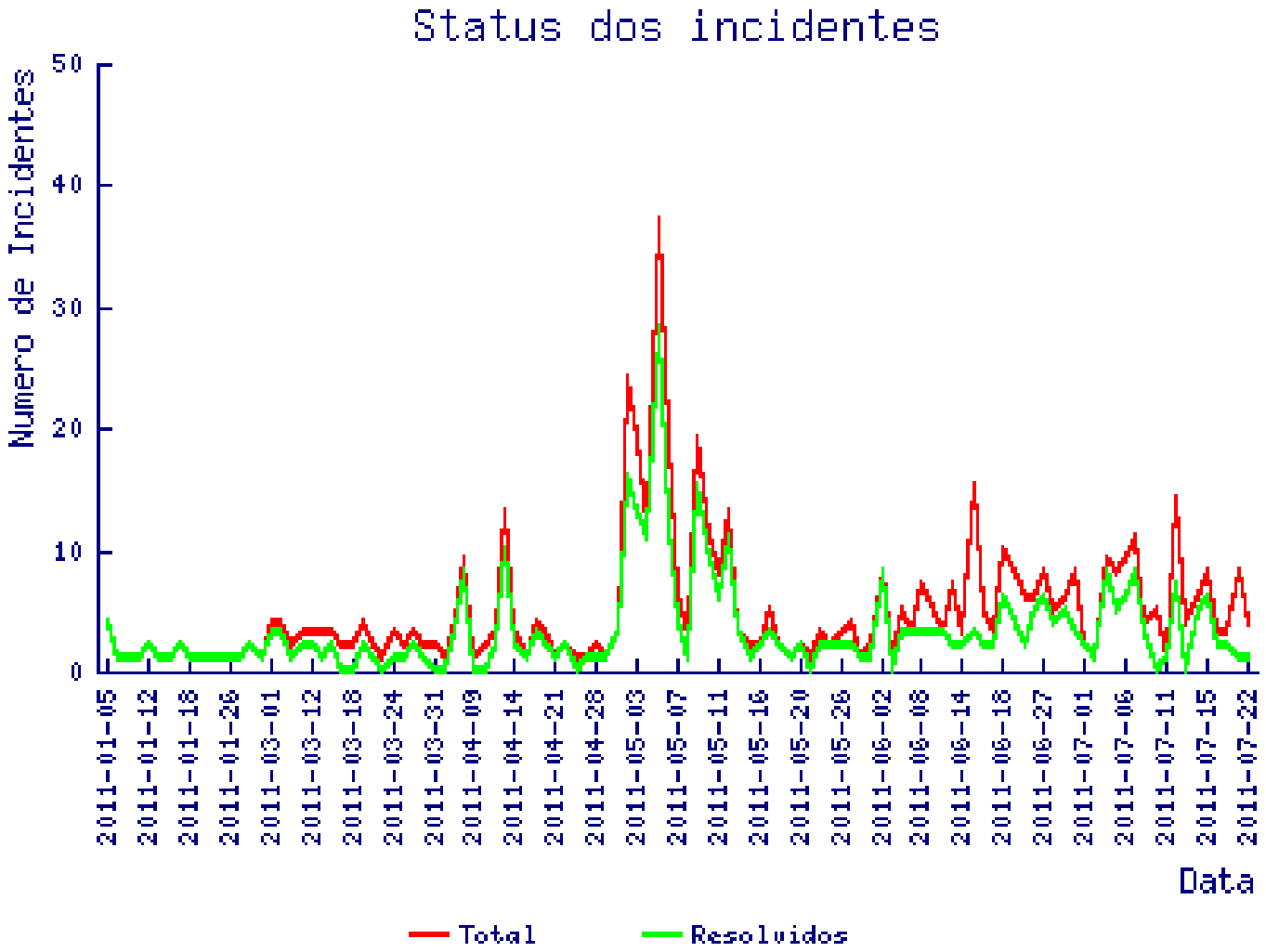
Resultados e Projetos futuros

Análise automatizada – TRAIRA

- Estudo de caso na rede UFBA
  - Em produção desde setembro/2010, tratando em média 5 a 10 notificações diariamente (cada notificação contém cerca de 20 incidentes)
- Geração de estatísticas
  - Situação e taxa de tratamento dos incidentes
  - Segmentação de incidentes por VLAN
  - Identificação de máquinas reincidentes
- Tratamento de incidentes *online*
  - Eficiência no tratamento / resposta

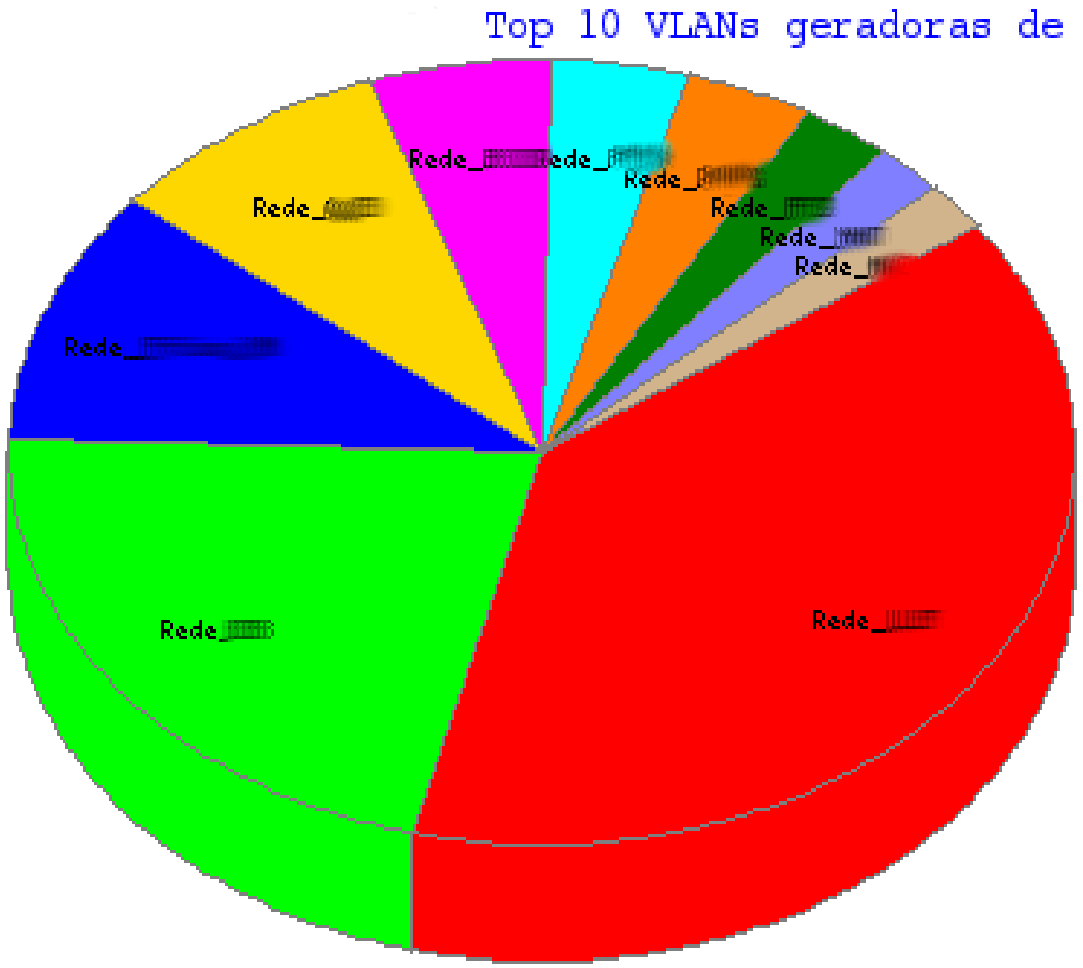
Resultados e Projetos futuros

- Situação e taxa de tratamento dos incidentes



Resultados e Projetos futuros

- Segmentação de incidentes por VLAN



VLAN	Ocorrencias
Rede_	111
Rede_	62
Rede_	30
Rede_	25
Rede_	16
Rede_	12
Rede_	11
Rede_	8
Rede_	6
Rede	6

Conclusões

- Contribuição: automatizar o tratamento a incidentes
  - Detecção, identificação e isolamento da máquina geradora do incidente
- Requisitos de implantação são triviais e pouco onerosos
- TRAIRA é usado como base no processo de tratamento de incidentes de segurança da rede de campus da UFBA
  - Piloto em outras instituições brasileiras

Conclusões

Trabalhos futuros

- Novas estratégias de detecção antecipada (análise de fluxos, queries DNS, etc.)
- Otimização no armazenamento e consulta dos logs, principalmente das traduções NAT
- Padronização para notificações de incidentes (e.g. IDMEF)
- Extensão para outros mapeamentos de endereço de rede (e.g. proxy http)
- Adicionar suporte a outros *drivers* de NAT (e.g. PFSense/FreeBSD)

Obrigado!!!
;-)

Perguntas?

CERT.Bahia <certbahia@pop-ba.rnp.br>