II WTR PoP-BA

II Workshop de Tecnologias de Redes do PoP-BA

Mini-curso:

Tratamento de Incidentes de Segurança com o TRAIRA

www.pop-ba.rnp.br/wtr

Realização:

POP-BA

Apoio:

UFBA

CPD - UFBA

RNP

Minicurso *Tratamento de Incidentes de Incidentes de Segurança com o TRAIRA*

II Workshop de Tecnologias de Redes do POP-BA
Ponto de Presença da RNP na Bahia

Italo Valcy <italo@pop-ba.rnp.br>

19 e 20 de setembro de 2011

Licença de uso e atribuição

Agenda

- Fundamentos do Tratamento de Incidentes de Segurança
  - Impacto do NAT e DHCP na fase de detecção
- TRAIRA :: Tratamento de Incidentes de Rede Automatizado
- Implantação do TRAIRA
  - RT (*Request Tracker*)
  - L2M
  - Configuração do TRAIRA
  - Validação do cenário

CERT.Bahia :: Grupo de Resposta a Incidentes de Segurança – Bahia/Brasil

Sobre o CERT.Bahia

- CSIRT (Grupo de Resposta a Incidentes de Segurança)

- Missão:

Auxiliar as instituições conectadas ao POP-BA/RNP na prevenção, detecção e tratamento dos incidentes de segurança, além de criar e disseminar boas práticas para uso e administração seguros das Tecnologias de Informação e Comunicação (TIC).

Quem somos?

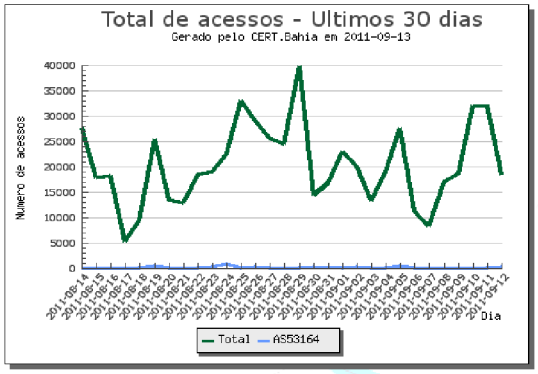
- Coordenação Técnica/Acadêmica
  - Luiz Claudio Mendonça (CPD/UFBA)
  - Prof. Luciano Barreto (DCC/UFBA)
  - Jerônimo Aguiar (CPD/UFBA)

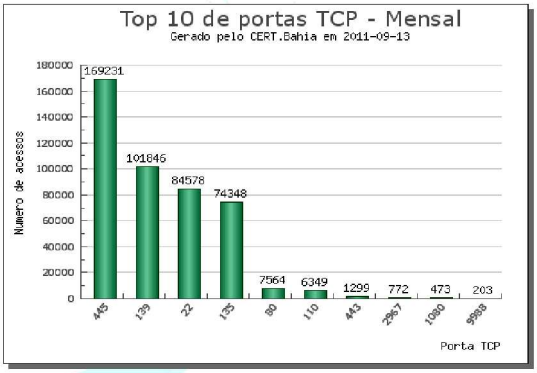
- Operação
  - Italo Valcy
  - Thiago Bomfim
  - Rafael Gomes

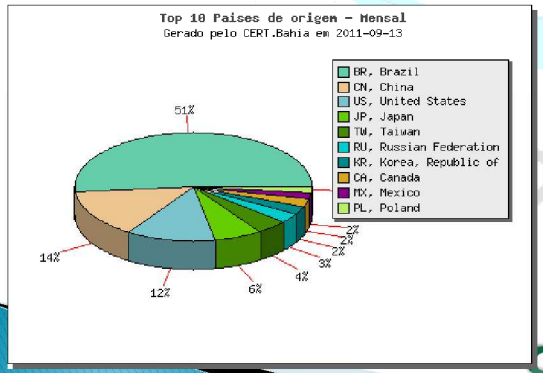
Serviços do CERT.Bahia

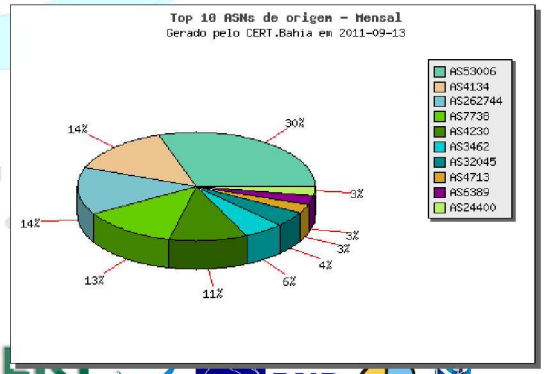
- Palestras / Treinamentos / Documentação
  - Campanhas de Segurança:
  - Campanha DNSSEC
  - Campanha de segurança nas Instituições
  - Piloto para armadilha de SPAM
  - ...
- Sensores para monitoramento e alerta de incidentes de segurança

Estatísticas do CERT.Bahia









Estatísticas do CERT.Bahia

- De Jan/2010 à Jun/2011

Tipo de incidente	Qtd. Tickets
Host possivelmente infectado com Virus/Worm	1762
Envio de Spam	79
Tentativas de obter acesso não autorizado a sistemas ou dados	75
Violação de copyright	43
Outros	20
Total	**1979**

Estatísticas do CERT.Bahia

De Jan/2010 à Jun/2011

- Total de incidentes: 1979
  - Fechado por falta de resposta do cliente: 913
  - Incidente resolvido: 1062

Como o CERT.Bahia pode ajudar?

- Sistema de controle de chamados
  - https://suporte.pop-ba.rnp.br
- Palestras e treinamentos
- Software de tratamento de incidentes (TRAIRA)
  - Detecção e armazenamento de NATs
  - Detecção da máquina que gerou o incidente
  - Bloqueio da máquina para tratamento futuro

Fundamentos do Tratamento a Incidentes de Segurança

Motivação

- Aumento do número de incidentes de segurança na Internet
  - Atividades preventivas são importantes, porém **nem todos os incidentes podem ser evitados** [Scarfone et al. 2008]
- Necessidade de estabelecimento de um Processo de Tratamento de Incidentes

Eventos e Incidentes de Segurança

- Segundo [Scarfone et al. 2008] um ***evento*** é qualquer ocorrência observável em um sistema ou na rede
  - Ex: usuário que inicia uma sessão SMTP, servidor web que recebe requisição HTTP, etc.
- Já um ***evento adverso*** é aquele que tem consequência negativa para a instituição
  - Ex: flooding de pacotes na rede, uso não autorizado de sistemas, etc.
- Consideraremos apenas eventos adversos relacionados à segurança do software dos computadores

Eventos e Incidentes de Segurança

- Segundo [CERT.br 2006] um ***incidente de segurança*** é um evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores
- Alguns exemplos:
  - Negação de Serviço
  - Código Malicioso
  - Acesso não autorizado
  - Uso inapropriado (violação de direitos autorais)

Eventos e Incidentes de Segurança

- Genericamente, [Scarfone et al. 2008] define um ***incidente de segurança*** como violação, ou suspeita de violação, de:
  - política de segurança da informação
  - política de uso aceitável
  - padrão de práticas de segurança de uma instituição
- Mais informações sobre esses documentos:
  - [CERT.br 2006]

Notificações de Incidentes de Segurança

- Principais causas de incidentes:
  - Ataques automatizados feitos por programas maliciosos (e.g. *bot* ou *worm*)
  - Pessoas mal intencionadas, usando ou não ferramentas automatizadas
- Em ambos os casos é importante alertar o responsável pelo sistema, organização ou rede em questão:
  - Notificações de Incidentes de Segurança
- Grande parte das notificações são enviadas pelos CSIRTs (Grupos de Resposta a Incidentes de Segurança)

Notificações de Incidentes de Segurança

- Dados essenciais a serem incluídos em uma notificação:
  - *logs* completos que evidenciem o incidente
  - data, horário e *timezone* (fuso horário) dos logs
  - endereço de origem do ataque, incluindo IP e porta da conexão

Tratamento de Incidentes de Segurança

- O tratamento de incidentes de segurança envolve três funções [CERT/CC 2010]:
  - Notificação do incidente
  - Análise do incidente
  - Resposta ao incidente
- O tratamento sistemático e efetivo de incidentes exige a definição de um ***processo de resposta a incidentes de segurança***. Exemplos:
  - Ciclo de vida da resposta a incidentes [Scarfone et. al. 2008]
  - Processo de tratamento de incidentes de segurança da UFRGS [Ceron et. al. 2009]

Tratamento de Incidentes de Segurança

- Ciclo de vida da resposta a incidentes [Scarfone et. al. 2008]:

Tratamento de Incidentes de Segurança

Preparação

- Fase inicial que envolve o estabelecimento de um CSIRT, aquisição de ferramentas, etc.
- Medidas essenciais:
  - Atualização dos SO's e aplicações (anti-vírus, *patches*, etc.);
  - Garantir o registro das atividades dos usuários (logs dos sistemas);
  - Armazenamento seguro dos logs dos sistemas;

Tratamento de Incidentes de Segurança

Detecção e Análise

- Nesta etapa deve-se detectar ou identificar de fato a existência de um incidente
- Principais atividades:
  - Recebimento e validação da notificação, extração dos principais dados sobre o Incidente
  - Verificação nas bases de IDS/IPS, anti-vírus ou logs do sistema
  - Consulta na base de conhecimento sobre os incidentes reportados no passado

Tratamento de Incidentes de Segurança

Contenção, Mitigação e Recuperação

- Assim que o incidente é detectado e analisado, deve-se iniciar mecanismos de contenção para evitar que ele se propague ou afete outros recursos da rede
- Inicia-se então o trabalho para mitigação e recuperação dos sistemas afetados.
  - Importante: ***política de backup***

Tratamento de Incidentes de Segurança

Ações Pós-Incidente

- Esta etapa consiste em avaliar o processo de tratamento de incidentes e verificar a eficácia das soluções adotadas.
- Discutir as *lições aprendidas* com o CSIRT
- Resposta à notificação enviada

Importância do Tratamento e Resposta a Incidentes

- Lentidão, leniência no tratamento do incidente, bem como a reincidência podem gerar sanções severas e indesejáveis
  - Ex: bloqueio de acesso, recusa de e-mails, etc
- Assim, é *essencial* que cada incidente seja TRATADO e RESPONDIDO
- Para entidades da Administração Pública Federal:
  - Norma Complementar nº 03/IN01/DSIC/GSIPR (PSI)
  - Norma Complementar nº 05/IN01/DSIC/GSIPR (ETIR)
  - Norma Complementar nº 08/IN01/DSIC/GSIPR (IR)
  - Mais: http://dsic.planalto.gov.br/legislacaodsic/53

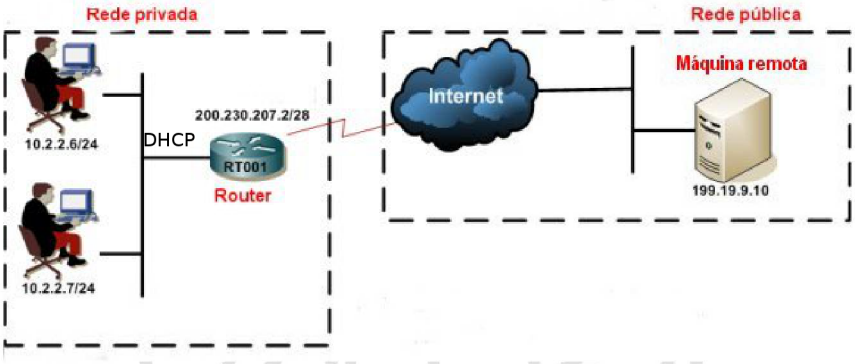
Principais Dificuldades

- Cada uma daquelas fases requer ações específicas de mitigação ou controle.
- Para incidentes que são gerados por uma instituição, alguns fatores podem dificultar seu tratamento, exemplo:
  - Tradução de Endereços de Rede (NAT)
  - Configuração dinâmica de rede nos hosts (DHCP)
  - Análise dos registros do sistema (logs)
  - Quantidade de notificações *versus* atribuições do CSIRT
  - ...

Principais Dificuldades

Antes de continuar...

- Estamos supondo o seguinte cenário de rede (bastante comum nas instituições):



- Estamos interessados nos incidentes que são *gerados* pela instituição

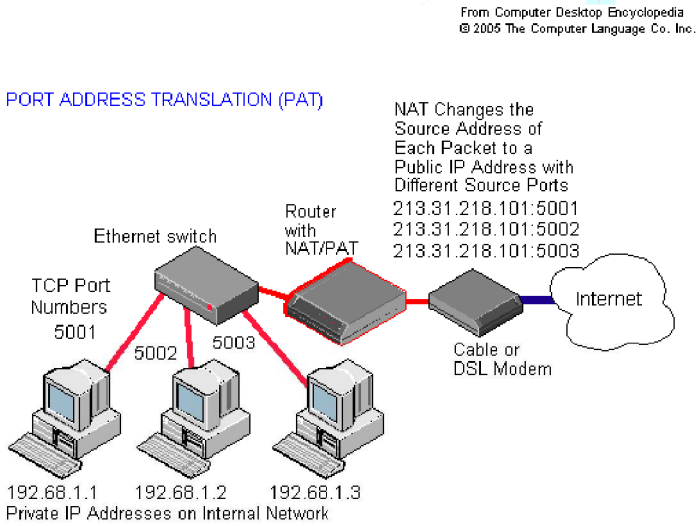
Principais Dificuldades – NAT

Network Address Translation (NAT)

- Permiti que, com um único IP roteável, ou um pequeno conjunto deles, vários hosts (RFC 1918) possam trafegar na Internet
- Tipos:
  - NAPT (Network Address and Port Translation)
  - SNAT (Source NAT)
  - DNAT (Destination NAT)

Principais Dificuldades – NAT

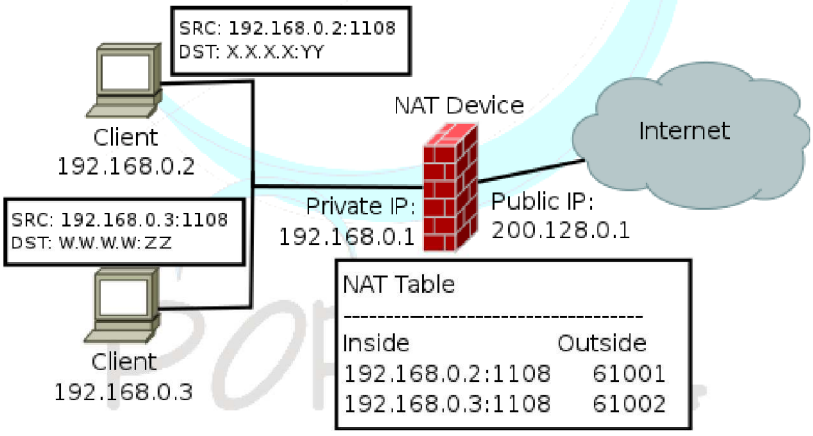
Network Address Translation (NAT)



Principais Dificuldades – NAT

Network Address Translation (NAT)

- Em alguns casos, a porta de origem original precisa ser alterada:



Principais Dificuldades – NAT

Network Address Translation (NAT)

- Desvantagem: dificuldade em determinar, com precisão, o endereço IP interno mapeado no endereço externo
  - Suporte à *logging* nos dispositivos de NAT
  - Busca nos *logs*

Principais Dificuldades – DHCP

Dynamic Host Configuration Protocol (DHCP)

- Configuração automática de parâmetros de rede nos clientes. Principais utilizações:
  - Provedores de acesso (endereços temporários)
  - Configuração automática de máquinas na rede interna (RFC 1918)
- Um host pode ter dois ou mais endereços IP por dia, semana ou mês (*lease time*)

Principais Dificuldades – DHCP

Dynamic Host Configuration Protocol (DHCP)

- Desvantagem: Mapeamento *IP-host* não garantido
  - Opção: utilizar os endereços MAC (Media Access Control) como identificador “único” dos hosts.

Principais Dificuldades – LOGs

Registros do Sistema (Logs)

- Um ***log*** é um registro dos eventos que ocorrem nos sistemas ou na rede de uma organização
- Os logs são um recurso essencial para os processos de auditória dos sistemas. Não obstante, dado seu volume e variedade, necessita-se de políticas de gerenciamento dos logs:
  - Processo que envolve a geração, transmissão, armazenamento, análise e descarte dos logs

Principais Dificuldades – LOGs

Registros do Sistema (Logs)

- Para eficácia no tratamento de incidentes, deve-se certificar-se sobre a configuração de *logging* dos sistemas ainda na fase de preparação.
- Já na fase de detecção, deve-se, por exemplo: buscar nos logs do dispositivo de NAT por uma ocorrência do IP, porta de origem, data e hora, que estejam em conformidade com aqueles enviados na notificação.

Estado da arte

SCARFONE, K.; GRANCE, T.; MASONE, K. Computer Security Incident Handling Guide.

- Fornece um guia completo para o tratamento de incidentes de segurança, direcionado a times de segurança novos e já estabelecidos.
- Defini as diretivas necessárias a um CSIRT para Resposta a Incidentes de Segurança

Estado da arte

KAISER, J. et al. Automated resolving of security incidents as a key mechanism to fight massive infections of malicious software.

- Os autores propõe um sistema onde o próprio usuário poderia tratar incidentes que envolvem seus hosts
  - PRISM (Portal for Reporting Incidents and Solution Management)
- Notificações internas no formato IDMEF
- Não trata de questões como o NAT/DHCP

Estado da arte

FARNHAM, G. Cisco Security Agent and Incident Handling.

- Sistema proprietário da Cisco baseado em HIPS, onde cada host da rede deve ter um agente instalado responsável por aplicar as políticas de segurança naquele host
- Desvantagens: custo de implantação e adequação à ambientes heterogêneos

Estado da arte

Ceron, J. et. al. (2009). O processo de tratamento de incidentes de segurança da UFRGS.

- Apresenta uma visão geral sobre o processo de tratamento de incidentes usado na UFRGS
- Também baseia-se nas etapas definidas em [Scarfone et. al. 2008], porém as etapas são executadas de forma manual
- O artigo não fala como o mapeamento de IP externo e host foi resolvido

Estado da arte

A maioria dos CSIRTs usa sistemas de *helpdesk* (sistemas de chamados), para gerenciar os incidentes de segurança:

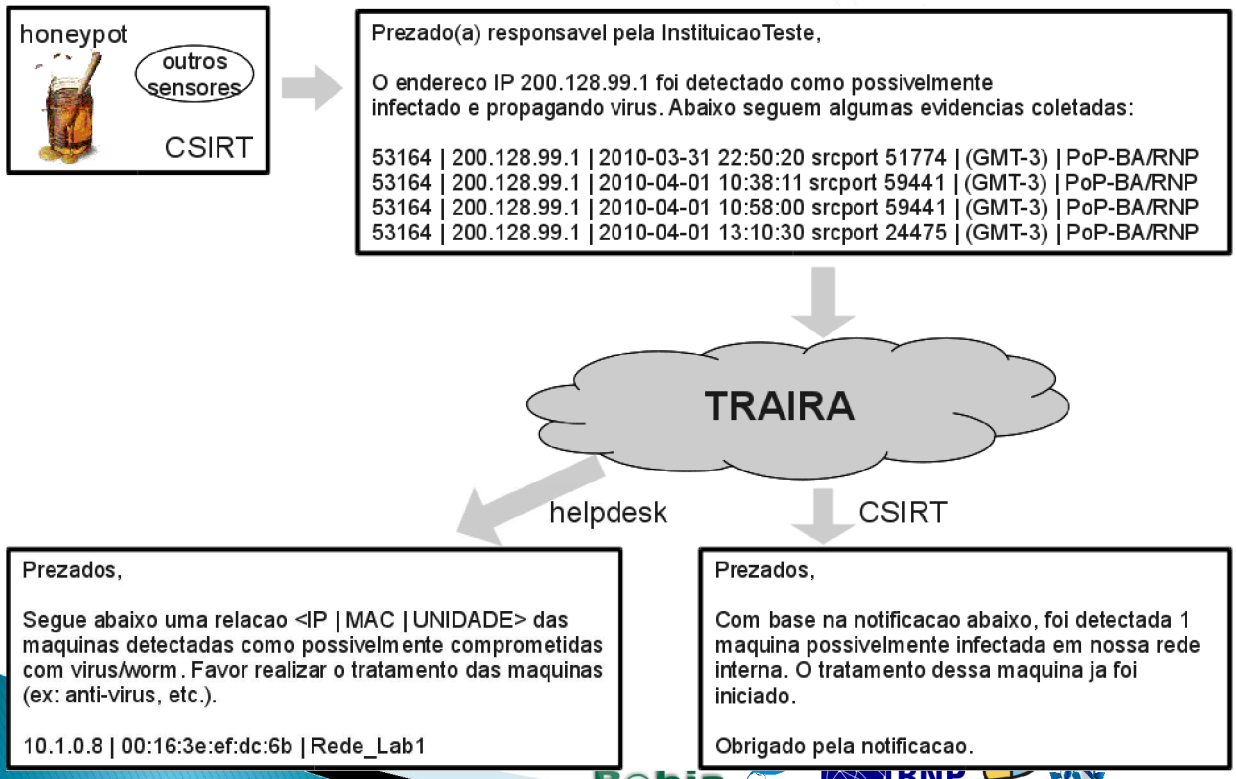
- Request Tracker (RT)
- Open Source Ticket Request System (OTRS)
- RT + RTIR
- Customizações das ferramentas

TRAIRA: Tratamento de Incidentes de Rede Automatizado

TRAIRA

- Software desenvolvido em *Perl*, como extensão do RT (*Request Tracker*), para tratamento automatizado dos incidentes de segurança
- Atua em todas as fases do processo de tratamento de incidentes:
- Automatiza o procedimento de detecção, identificação e isolamento da máquina geradora do incidente.

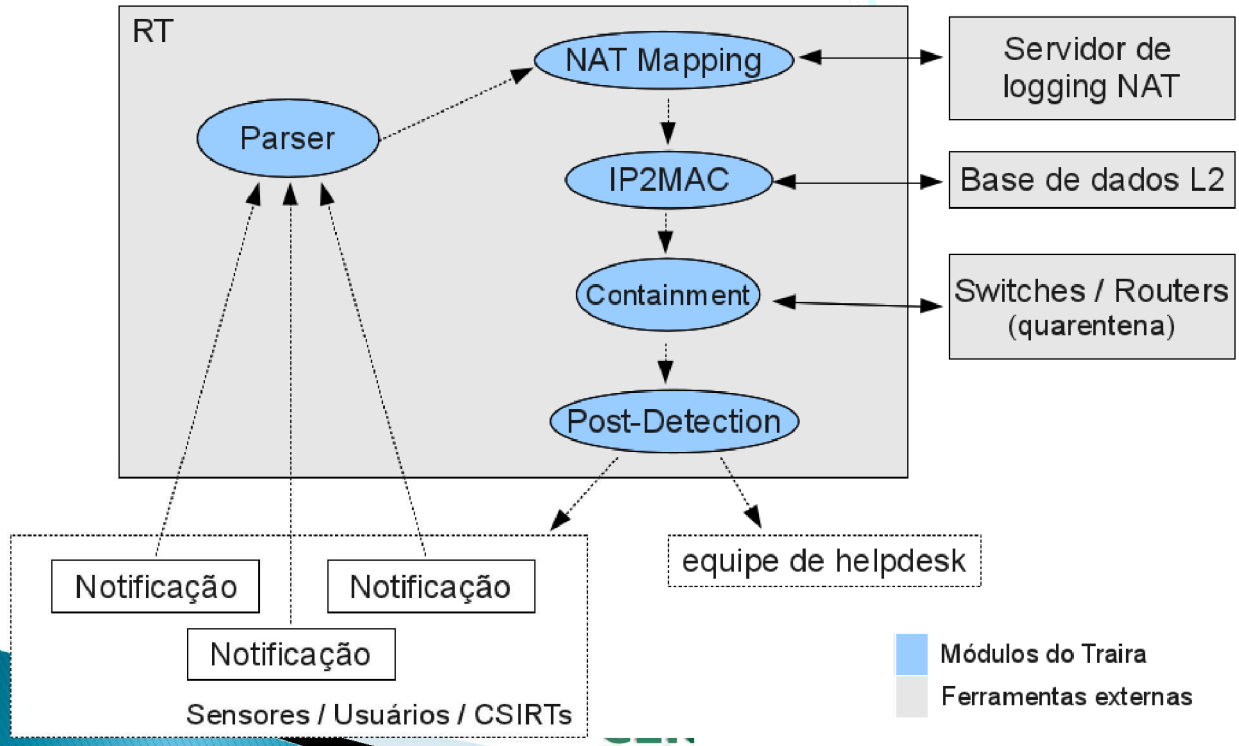
TRAIRA – Fluxo de execução



TRAIRA – Fluxo de execução

1. Submissão de notificações de incidentes ao TRAIRA
2. TRAIRA roda o parser, para extração de informações importantes (IP, Porta, Data/Hora)
3. Busca nos logs do NAT
4. Busca no L2M
5. Notificação ao helpdesk/operação
6. Resposta à entidade que notificou o incidente

Arquitetura do TRAIRA



TRAIRA::Parser

- ***Parser***: é o módulo responsável pelo recebimento da notificação e pela extração das informações essenciais ao tratamento do incidente: 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
- Vamos a um exemplo...

TRAIRA::Parser

Exemplo de notificação enviada pelo CERT.Bahia para *InstituicaoTeste*

```
Subject: Aviso de deteccao de Virus/Worm com origem em 200.128.99.1 (InstituicaoTeste)
From: PoP-BA Security Team <incidentes@pop-ba.rnp.br>
To: Instituicao Teste CSIRT <security@instituicaoteste.edu.br>

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

Pedimos a gentileza de verificar. Caso tenha alguma duvida, favor entrar em contato.

Atenciosamente,
--
CERT.Bahia :: Grupo de Resposta a Incidentes de Seguranca da Bahia/Brasil
PoP-BA/RNP :: Ponto de Presenca da RNP na Bahia
Tel.: +55 71 3283-6098
```


TRAIRA::Parser

Parser para notificações enviadas pelo CERT.Bahia

From	`incidentes@pop-ba.rnp.br`
Subject	`Aviso de deteccao de Virus/Worm com origem em [0-9.]{7,15} \(InstituicaoTeste\)`
Código do *parser*	`my $IP = '[0-9.]{7,15}';` `my $DATE = '[0-9-]{10}';` `my $TIME = '[0-9:]{8}';` `my $PORT = '[0-9]+';` `if ($line =~ /^53164 | ($IP) \| ($DATE) ($TIME) srcport ($PORT)\b.*$/) {` `  my ($date, $time) = $self->AdjustTimezone($2, $3, '-0300');` `  return ($date, $time, $1, $4);` `}` `return undef;`

TRAIRA::Parser

Resultado da execução do módulo Traira::Parser sobre a notificação da Listagem

#	Data	Hora	IP externo	Porta externa
1	2010-04-01	01:50:20	200.128.99.1	51774
2	2010-04-01	13:38:11	200.128.99.1	59441
3	2010-04-01	13:48:00	200.128.99.1	59441
4	2010-04-01	16:10:30	200.128.99.1	24475

TRAIRA::NATMapping

- O NAT dificulta a identificação precisa do host que provocou um incidente de segurança
- O módulo *NAT Mapping* do TRAIRA, faz o mapeamento entre o IP externo e IP interno
- Dificuldades desse mapeamento:
  - Diversidade de dispositivos NAT (logs diferentes)
  - Volume de dados a serem processados
    - Na UFBA são mais de 7 milhões de registros de traduções NAT por dia (média de Nov/2010)
  - Correspondência temporal

TRAIRA::NATMapping

- Problema da correspondência temporal
  - É difícil, na prática, manter relógios sincronizados
  - Uma tradução NAT possui duração temporal, assim o log pode não representar diretamente o momento em que ela ocorreu... como registrar?
    - Apenas horário de início?
    - Horário de início e fim?
    - Horário final + duração? (preferível)

Vamos a um exemplo...

TRAIRA::NATMapping

Exemplos de *logs* de traduções NAT no *firewall* ASA da Cisco

```
1  Apr  1 01:50:54 172.16.254.1 %ASA-0-305012: Teardown dynamic UDP translation from
       int_in:10.1.0.8/51386 to int_out:200.128.99.1/51774 duration 0:00:30
2  Apr  1 13:39:56 172.16.254.1 %ASA-0-305012: Teardown dynamic TCP translation from
       int_in:192.168.0.37/60523 to int_out:200.128.99.1/59441 duration 0:02:30
3  Apr  1 13:50:57 172.16.254.1 %ASA-0-305012: Teardown dynamic TCP translation from
       int_in:10.2.0.44/50071 to int_out:200.128.99.1/59441 duration 0:03:00
4  Apr  1 16:12:28 172.16.254.1 %ASA-0-305012: Teardown dynamic UDP translation from
       int_in:10.1.10.9/60818 to int_out:200.128.99.1/24475 duration 0:02:21
```

TRAIRA::NATMapping

Resultado da execução do módulo Traira::Parser sobre a notificação da Listagem

#	Data	Hora	IP externo	Porta externa
1	2010-04-01	01:50:20	200.128.99.1	51774
2	2010-04-01	13:38:11	200.128.99.1	59441
3	2010-04-01	13:48:00	200.128.99.1	59441
4	2010-04-01	16:10:30	200.128.99.1	24475

Exemplos de *logs* de traduções NAT no *firewall* ASA da Cisco

```
1 Apr  1 01:50:54 172.16.254.1 %ASA-0-305012: Teardown dynamic UDP translation from
    int_in:10.1.0.8/51386 to int_out:200.128.99.1/51774 duration 0:00:30
2 Apr  1 13:39:56 172.16.254.1 %ASA-0-305012: Teardown dynamic TCP translation from
    int_in:192.168.0.37/60523 to int_out:200.128.99.1/59441 duration 0:02:30
3 Apr  1 13:50:57 172.16.254.1 %ASA-0-305012: Teardown dynamic TCP translation from
    int_in:10.2.0.44/50071 to int_out:200.128.99.1/59441 duration 0:03:00
4 Apr  1 16:12:28 172.16.254.1 %ASA-0-305012: Teardown dynamic UDP translation from
    int_in:10.1.10.9/60818 to int_out:200.128.99.1/24475 duration 0:02:21
```


TRAIRA::NATMapping

No exemplo anterior pudemos observar:

- Todas as máquinas acessam a Internet com um único endereço IP
- É possível inferir o horário de início do NAT a partir do horário de fim menos a duração
- Não é suficiente buscar por IP+PORTA
  - 200.128.99.1:59441 ocorre duas vezes
- Correspondência de horários: a tupla 200.128.99.1:51774 não aparece no horário exato da notificação
  - Definição da *Tolerância Temporal*

TRAIRA::NATMapping

Configuração:

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

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::NATMapping

Resultado da execução do módulo Traira::Parser sobre a notificação da Listagem

#	Data	Hora	IP externo	Porta externa
1	2010-04-01	01:50:20	200.128.99.1	51774
2	2010-04-01	13:38:11	200.128.99.1	59441
3	2010-04-01	13:48:00	200.128.99.1	59441
4	2010-04-01	16:10:30	200.128.99.1	24475

⇩

Resultado da execução do módulo Traira::NATMapping sobre os incidentes

#	Data	Hora	IP interno
1	2010-04-01	01:50:20	10.1.0.8
2	2010-04-01	13:38:11	192.168.0.37
3	2010-04-01	13:48:00	10.2.0.44
4	2010-04-01	16:10:30	10.1.10.9

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 / software que armazene o histórico da tabela ARP
- No TRAIRA, utiliza-se o L2M como base de consulta para o histórico da tabela ARP

TRAIRA::IP2MAC (L2M)

L2M :: Layer 2 Manager

- Software desenvolvido pela UFBA e pelo CERT.Bahia para gerenciamento de recursos em camada 2 (enlace).
- O L2M permite, via interface web, uma série de consultas para um host (por IP ou MAC), por exemplo, horário de entrada e saída
- Permite saber quantas máquinas estão acessando a rede nesse momento, nos últimos 15 dias, etc.

TRAIRA::IP2MAC

- Assim, 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;

- Usando os exemplos anteriores, temos:

#	Data	Hora	IP interno	MAC	VLAN
1	2010-04-01	01:50:20	10.1.0.8	00:16:3e:ef:dc:6b	Rede_Lab1
2	2010-04-01	13:38:11	192.168.0.37	00:16:3e:ad:1c:6e	Rede_InstA
3	2010-04-01	13:48:00	10.2.0.44	00:16:3e:bb:2a:3b	Rede_Wireless
4	2010-04-01	16:10:30	10.1.10.9	00:16:3e:fa:ca:1a	Rede_Lab2

TRAIRA::Containment

- Uma vez que o host é detectado, o TRAIRA pode realizar a contenção daquele host para evitar que o mesmo continue propagando atividade maliciosa enquanto não é tratado por uma equipe de campo.

- Listamos três possibilidades de contenção:
  - Bloqueio do host no roteador daquela VLAN
  - Bloqueio do host no switch gerenciável mais próximo
  - Mover o 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 totalmente dependente do L2M

- Melhor caso: VLAN de quarentena
  - Requisito: suporte à MAC-based VLAN (ou via ACL)
  - Na pesquisa que realizamos com importantes fabricantes, apenas UM deles possui essa funcionalidade

TRAIRA::PostDetection

- A etapa de Pós-detecção no TRAIRA é implementada por duas ações:
  - Acionamento da equipe de campo (helpdesk) para realizar o tratamento da máquina (anti-vírus, reinstalação, etc.)
  - Resposta à equipe que enviou a notificação

TRAIRA::PostDetection

Exemplo de e-mail enviado à equipe de *helpdesk* para bloqueio/desinfecção do *host*

```
1  Subject: Solicitacao de bloqueio/desinfeccao de maquina com virus/worm
2  From: Instituicao Teste CSIRT <security@instituicaoteste.edu.br>
3  To: Helpdesk Instituicao Teste <helpdesk@instituicaoteste.edu.br>
4
5  Prezados,
6
7  Segue abaixo uma relacao <IP | MAC | VLAN> das maquinas detectadas como
8  possivelmente comprometidas com virus/worm. Favor realizar o tratamento
9  das maquinas (ex: anti-virus, etc.).
10
11 10.1.0.8 | 00:16:3e:ef:dc:6b | Rede_Lab1
12
13 Atenciosamente,
14 --
15 TRAIRA :: Tratamento de Incidentes de Rede Automatizado.
16 Instituicao Teste CSIRT
```

Estatísticas do TRAIRA

- Um recurso fundamental aos CSIRTs é as estatísticas: elas ajudam os CSIRTs a detectar tendências, prever futuros ataques em grande escala, direcionar atividades, eficácia do tratamento, dentre outros.

- A implementação atual do TRAIRA fornece os seguintes gráficos:
  - Gráfico de incidentes por VLAN
  - Quantidade de incidentes por dia
  - MACs reincidentes

Estatísticas do TRAIRA

PRACTICAL ™
RT para rt-traira

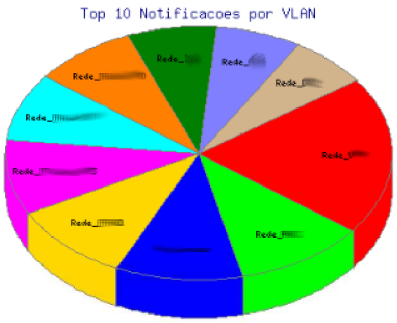
Início · Busca Simples · Tiquetes · Ferramentas · Configuração · Preferências · Aprovação

Offline · Relatórios · Meu Dia · Traira

Traira :: Relatorios

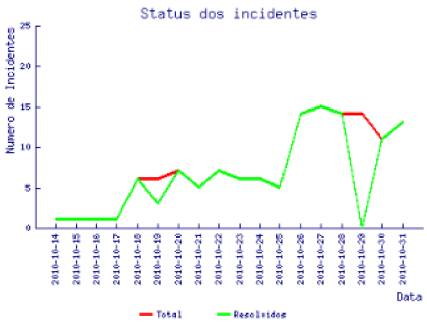
Tratar Incidente · Relatorios · Configuracao · Parsers · Acoes

Top 10 VLANs que mais geram incidentes



VLAN	Ocorrencias
Rede_	51
Rede_	28
	27
Rede_	26
Rede_	24
Rede_	22
Rede_	22
Rede_	19
Rede_	18
Rede_	17

Status dos incidentes



Requisitos de implantação

- Registro remoto dos eventos de tradução de NAT (SNAT)
- Histórico sobre a associação entre endereços IP e MAC dos *hosts*
- *Request Tracker* (RT)
- Banco de dados

Integração com RT

- O *Request Tracker* (RT) é um sistema de chamados, de distribuição livre, bastante usado como ferramenta de apoio à central de serviços das instituições
  - Interface web / E-mail
  - Tíquetes / Filas / Ações / etc.
  - Extensões
- O TRAIRA requer um ambiente funcional do RT, mas não exclusivo*

* dependo do cenário usado, pode ser mais seguro manter uma instalação isolada para o TRAIRA

Integração com RT

Configurações:

- FILA para incidentes de segurança
- Configurações do mapeamento NAT
- Timezone do sistema
- Mapeamento IP -> MAC (parâmetros do L2M)
- Registrar os *parsers*
- Habilitar/Desabilitar contenção automática

Mais informações

- TRAIRA: uma ferramenta para Tratamento de Incidentes de Segurança. Autor: Italo Valcy; In: Trabalho de Graduação DCC/UFBA – Salvador – BA – Brasil. Dezembro de 2010
  - http://homes.dcc.ufba.br/~italo/monografia.pdf
- TRAIRA: Tratamento de Incidentes de Rede Automatizado. Autores: Italo Valcy; Jerônimo Bezerra; In. V Workshop de TI das IFES - Florianópolis - SC - Brasil. Abril de 2011.
  - http://www.pop-ba.rnp.br/files/traira-v-wtiifes.pdf

Avaliação sobre o TRAIRA

- Cenário atual:
  - Muitos incidentes e poucos recursos de segurança (equipe e ferramentas)
  - Uso extensivo de NAT e DHCP
  - Consequência: pouca resposta a incidentes
- Proposta: automatizar o tratamento a incidentes
  - TRAIRA: detecção, identificação e isolamento da máquina geradora do incidente
- O TRAIRA permite integração com o RTIR para gerenciamento de um incidente de segurança

Avaliação sobre o TRAIRA

- Requisitos de implantação do TRAIRA são simples
- Principal requisito: suporte a *logging* das traduções SNAT

Próximos passos:

- Piloto com clientes
- Novas funcionalidades
- Integração com RTIR

TRAIRA: Instalação e Configuração

TRAIRA: instalação e configuração

- Registro remoto dos logs de NAT
  - Verifique seu firewall/roteador
  - Estudo de caso: Netfilter/IPTables
- Histórico do mapeamento IP -> MAC
  - L2M
- RT
- Instalação e configuração do TRAIRA

Logging do NAT

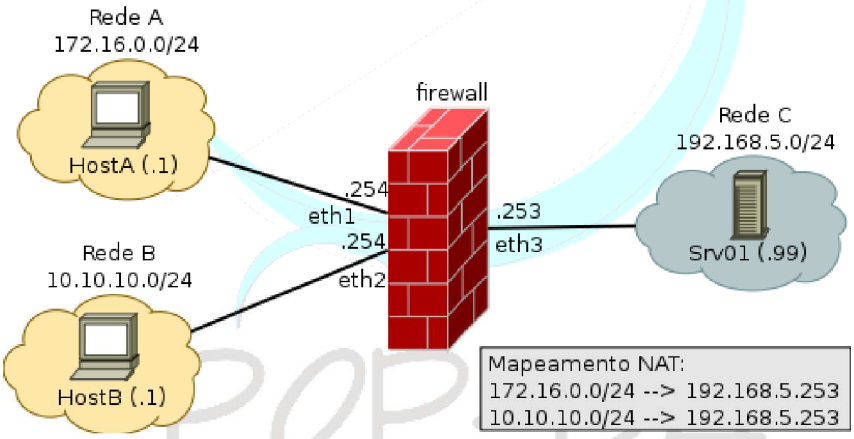
- Dependente do dispositivo de NAT usado na instituição. Já validamos com:
  - ASA/Cisco
  - Netfilter/IPTables
- Gostaríamos de fazer pilotos com outras instituições para validação do TRAIRA
- Estudo de caso: Netfilter/IPTables

Netfilter/IPTables

- Netfilter é o firewall nativo do Linux, permite filtro de pacotes, tradução de endereços (NAT/NAPT) e outras manipulações de pacotes
- IPTables é uma aplicação cliente para manipular as regras do Netfilter (frontend)
- Bastante usado nas instituições
- Problema: **O IPTables não faz registro das traduções NAT de forma adequada.**

Netfilter/IPTables

- Vamos a um exemplo para entender o problema. Suponha o seguinte cenário:



Netfilter/IPTables

- Comandos do IPTables para implementar o cenário de SNAT apresentado anteriormente

1. `iptables -t nat -A POSTROUTING -o eth3 -s 172.16.0.0/24 -j SNAT --to-source 192.168.5.253`
2. `iptables -t nat -A POSTROUTING -o eth3 -s 10.10.10.0/24 -j SNAT --to-source 192.168.5.253`

- Após a execução desses comandos, a chain POSTROUTING da tabela NAT do iptables fica assim:

#Regra	Prot.	In	Out	Orig.	Dest.	Ação
1	all	*	eth3	172.16.0.0/24	0.0.0.0/0	SNAT (to:192.168.5.253)
2	all	*	eth3	10.10.10.0/24	0.0.0.0/0	SNAT (to:192.168.5.253)

Netfilter/IPTables

- Como habilitar o logging das traduções NAT nesse cenário?

Netfilter/IPTables

- Como habilitar o logging das traduções NAT nesse cenário?
- Suposta solução:

1. `iptables -t nat -I POSTROUTING 1 -o eth3 -s 172.16.0.0/24 -j LOG --log-prefix 'SNAT '`
2. `iptables -t nat -I POSTROUTING 3 -o eth3 -s 10.10.10.0/24 -j LOG --log-prefix 'SNAT '`

- *`iptables -t nat -L POSTROUTING -n -v`*:

#Regra	Prot.	In	Out	Orig.	Dest.	Ação
1	all	*	eth3	172.16.0.0/24	0.0.0.0/0	LOG (prefixo 'SNAT ')
2	all	*	eth3	172.16.0.0/24	0.0.0.0/0	SNAT (to:192.168.5.253)
3	all	*	eth3	10.10.10.0/24	0.0.0.0/0	LOG (prefixo 'SNAT ')
4	all	*	eth3	10.10.10.0/24	0.0.0.0/0	SNAT (to:192.168.5.253)

Resolve?

Netfilter/IPTables

Host A (172.16.0.1)

```
nc -p 40000 192.168.5.99
```

Host B (10.10.10.1)

```
nc -p 40000 192.168.5.99
```

Firewall: Log do iptables para conexões do netcat acima

```
1 Nov 20 09:47:07 firewall kernel: [32385.753454] SNAT IN= OUT=eth3 SRC=172.16.0.1
    DST=192.168.5.99 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=52200 DF PROTO=TCP SPT=40000 DPT=80
    WINDOW=5840 RES=0x00 SYN URGP=0
2 Nov 20 09:47:08 firewall kernel: [32386.479462] SNAT IN= OUT=eth3 SRC=10.10.10.1
    DST=192.168.5.99 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=18925 DF PROTO=TCP SPT=40000 DPT=80
    WINDOW=5840 RES=0x00 SYN URGP=0
```

Srv01 (192.168.5.99): monitoramento com tcpdump

```
1 09:47:07.615051 IP 192.168.5.253.40000 > 192.168.5.99.80: Flags [S], seq 3428346057, win
    5840, options [mss 1460,sackOK,TS val 9478945 ecr 0,nop,wscale 2], length 0
2 09:47:07.627116 IP 192.168.5.253.40000 > 192.168.5.99.80: Flags [.], ack 128236544, win 1460,
    options [nop,nop,TS val 9478948 ecr 46727625], length 0
3 09:47:08.439314 IP 192.168.5.253.1024 > 192.168.5.99.80: Flags [S], seq 2237520910, win 5840,
    options [mss 1460,sackOK,TS val 9475555 ecr 0,nop,wscale 2], length 0
4 09:47:08.445493 IP 192.168.5.253.1024 > 192.168.5.99.80: Flags [.], ack 122234339, win 1460,
    options [nop,nop,TS val 9475555 ecr 46727831], length 0
5 ...
```


NFCT-SNATLOG

- Disponível? (GPL)
  - http://github.com/italovalcy/nfct-snatlog/
- Como instalar?
  - doc/INSTALL
- Como usar?

```
/usr/sbin/nfct-snatlog --daemon
```

- Onde ficam os logs?

```
tail -f /var/log/syslog
```

NFCT-SNATLOG

Host A (172.16.0.1)

```
nc -p 40000 192.168.5.99
```

Host B (10.10.10.1)

```
nc -p 40000 192.168.5.99
```

Firewall: Log do NFCT-SNATLOG para conexões do netcat acima

```
1 Nov 20 09:49:17 firewall nfct-snatlog: [SNAT_LOG] proto=tcp o-src=172.16.0.1 o-spt=40000
    t-src=192.168.5.253 t-spt=40000 duration=130s
2 Nov 20 09:49:18 firewall nfct-snatlog: [SNAT_LOG] proto=tcp o-src=10.10.10.1 o-spt=40000
    t-src=192.168.5.253 t-spt=1024 duration=130s
```

Srv01 (192.168.5.99): monitoramento com tcpdump

```
1 09:47:07.615051 IP 192.168.5.253.40000 > 192.168.5.99.80: Flags [S], seq 3428346057, win
    5840, options [mss 1460,sackOK,TS val 9478945 ecr 0,nop,wscale 2], length 0
2 09:47:07.627116 IP 192.168.5.253.40000 > 192.168.5.99.80: Flags [.], ack 128236544, win 1460,
    options [nop,nop,TS val 9478948 ecr 46727625], length 0
3 09:47:08.439314 IP 192.168.5.253.1024 > 192.168.5.99.80: Flags [S], seq 2237520910, win 5840,
    options [mss 1460,sackOK,TS val 9475555 ecr 0,nop,wscale 2], length 0
4 09:47:08.445493 IP 192.168.5.253.1024 > 192.168.5.99.80: Flags [.], ack 122234339, win 1460,
    options [nop,nop,TS val 9475555 ecr 46727831], length 0
5 ...
```


NFCT-SNATLOG

Análise de desempenho

- Viabilidade de uso do NFCT-SNATLOG
- Vantagens no *logging* remoto
- Desvantagem no uso de muitas máquinas por IP de NAT

NFCT-SNATLOG

Prática: Instalar o NFCT-SNATLOG na máquina virtual do Firewall e configurar o envio dos logs para servidor de gerencia.

L2M :: Mapeamento IP -> MAC

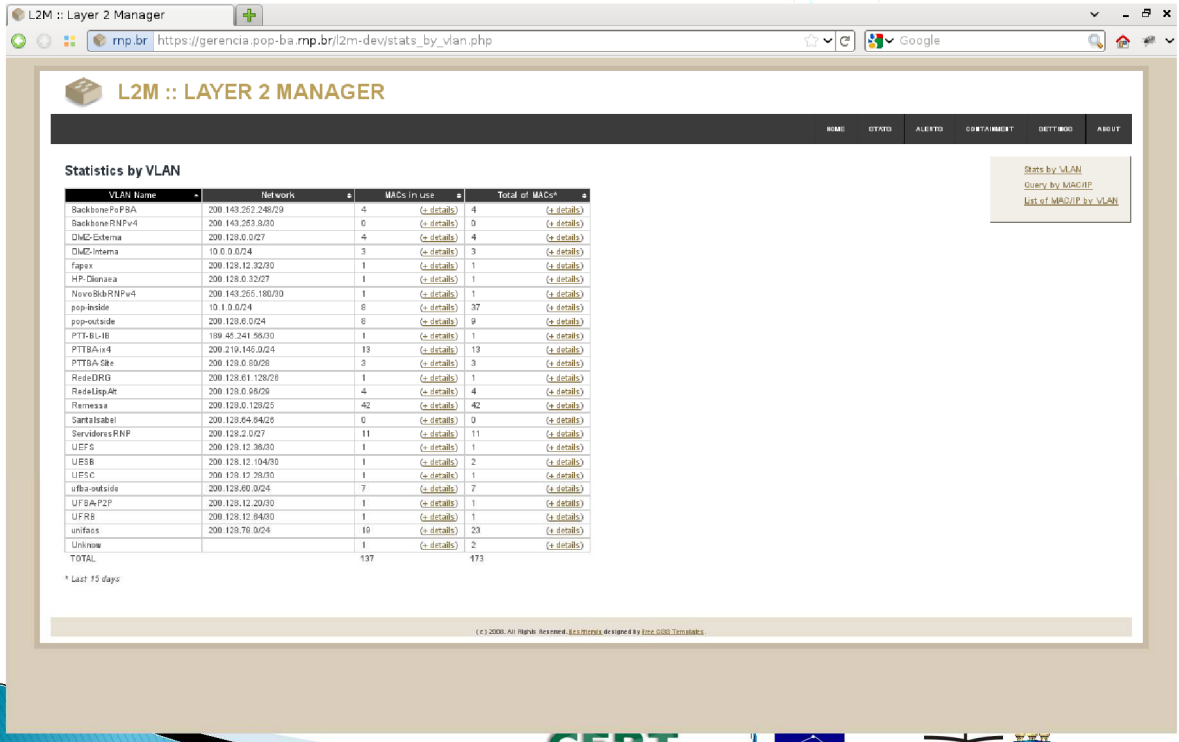
- Software desenvolvido pela UFBA e pelo CERT.Bahia para atuar no gerenciamento da camada de enlace (Layer 2)
  - Armazena um histórico sobre a tabela ARP dos roteadores
  - Atua no bloqueio de MAC's nos roteares
- Interface web, desenvolvida em PHP
- Disponível para download (GPL):
  - http://www.pop-ba.rnp.br/files/sw/l2m.tar.gz

L2M :: Mapeamento IP -> MAC

- Permite consulta da tabela ARP via:
  - SNMP (RFC1213-MIB::atPhysAddress)
  - Script (Expect / ShellScript / etc.)
    - Requer o desenvolvimento do script

- Informações disponíveis:
  - Utilização da rede no momento e nos últimos 15 dias
  - Quantidade de hosts por VLAN
  - Histórico de acesso de um host (por IP e por MAC)
  - etc...

L2M :: Mapeamento IP -> MAC



L2M :: Mapeamento IP -> MAC

Requisitos:

- Apache + PHP + PostgreSQL

Configuração:

- Restrição de acesso à Interface
- Adição de roteadores
- Adição de redes
- Configuração do *poller* no CRON
- Configuração dos parâmetros de contenção (bloqueio) – Opcional

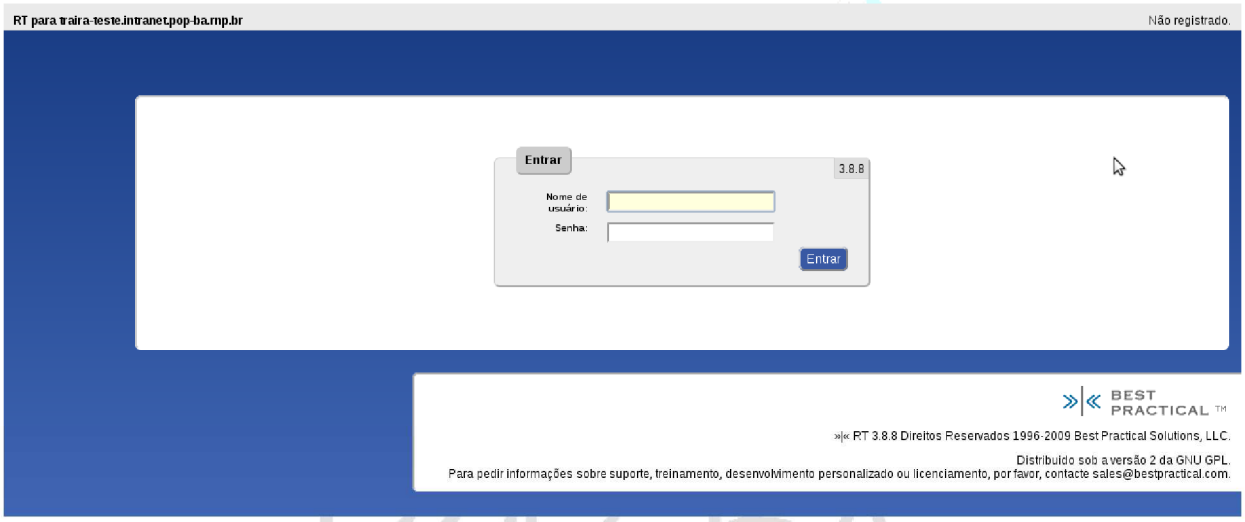
L2M :: Mapeamento IP -> MAC

Pratica: Configurar o L2M na máquina Gerencia e habilitar a consulta da tabela ARP do Firewall.

RT :: Request Tracker

- Sistema de chamados/bugs, distribuído sobre licença GPL.
  - Permite criação de tíquetes via interface web e e-mails.
  - Autenticação em base de dados externas (LDAP)
  - Permite instalação de extensões
- Requisitos:
  - Apache + Perl + (MySQL || PostgreSQL || SQLite)
  - Integração com servidor de e-mails

RT :: Request Tracker



RT :: Request Tracker

Pratica: instalar o RT na máquina gerência e configurar a abertura de chamados via e-mail.

RT :: TRAIRA

- Desenvolvido em Perl (linguagem do RT)
- Distribuído sobre licença GPL
- Disponível para download
  - http://www.pop-ba.rnp.br/files/sw/rt-traira.tar.gz
- Documentação:
  - http://certbahia.pop-ba.rnp.br/traira

RT :: TRAIRA

Pratica: Instalação e configuração do TRAIRA no RT

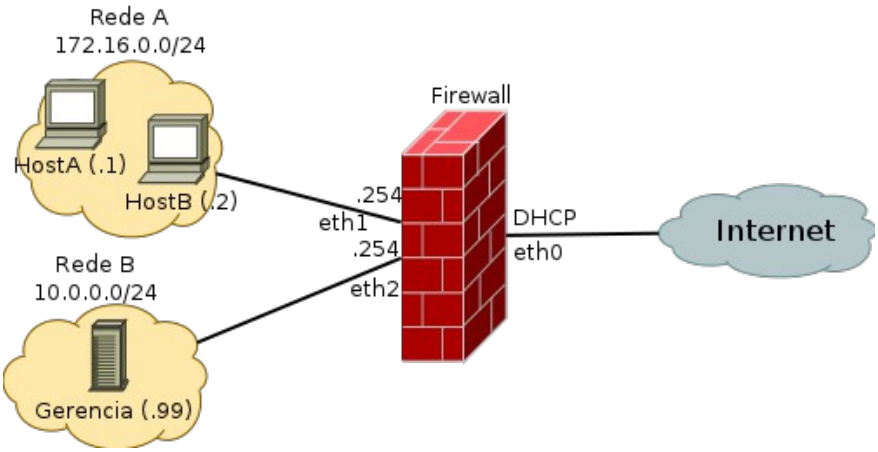
- Testar ambiente

Referências

- Scarfone, K., Grance, T., and Masone, K. (2008). Computer Security Incident Handling Guide. NIST Special Publication, 800–61;
- CERT.br (2006). Cartilha de Segurança para Internet. Parte VII: Incidentes de Segurança e Uso Abusivo da Rede;
- CERT/CC (2010). Computer Segurity Incident Response Team FAQ.
- Ceron, J. et. al. (2009). O processo de tratamento de incidentes de segurança da UFRGS. In: IV Workshop de TI das IFES, 2009.

II WTR do POP-BA

II Workshop de Tecnologias de Redes
Ponto de Presença da RNP na Bahia
Instrutor: Italo Valcy
Monitor: Thiago Bomfim

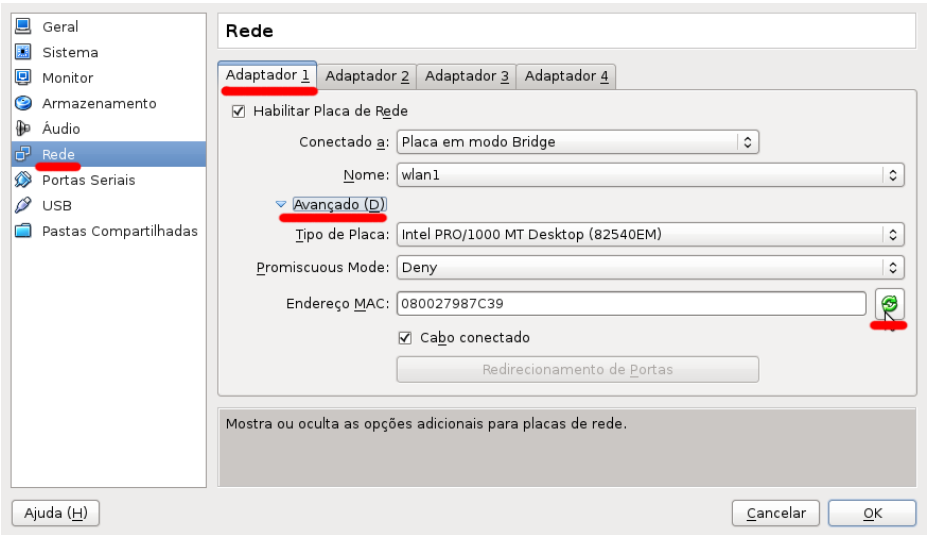


Material necessário para as práticas:

- Virtualbox (versão 4.1.0 ou superior)
- Máquinas virtuais disponibilizadas pelo instrutor (firewall.ova, Gerencia.ova, HostA.ova e HostB.ova)

Importe cada uma dessas máquinas no Virtualbox (*Arquivo > Importar Appliance*), mas não as inicie ainda (veja a configuração abaixo antes).

Antes de iniciar as máquinas, precisaremos alterar o endereço MAC da máquina *Firewall* pois ela será conectada diretamente à interface de rede do hospedeiro e, se não alterarmos, teremos problemas de MACs duplicados na rede. Para alterar o MAC da máquina Firewall clique com o botão direito do mouse sobre a máquina e escolha a opção “Configurações”; em seguida escolha as opções de “Rede” e no “Adaptador 1” clique em “Avançado (D)” e clique no botão de Refresh ao lado do MAC. Veja na figura abaixo:



Prática 01: Instalação e Configuração do NFCT-SNATLOG no Firewall

Este laboratório visa apresentar aos alunos os passos para configuração do NFCT-SNATLOG, permitindo a geração dos logs de traduções NAT realizadas pelo Netfilter/IPTables.

Parte 01: Instalação do NFCT-SNATLOG

Os passos abaixo devem ser executados na máquina Firewall, a menos que outra máquina seja explicitamente citada.

Faça o download do pacote do nfct-snatlog (já foi feito o download na pasta /root):

```
wget http://www.pop-ba.rnp.br/files/sw/nfct-snatlog.tgz
```

Instale as dependências (já estão instaladas):

```
apt-get install make gcc libnetfilter-conntrack-dev
```

Compilação do software:

```
tar -xzf nfct-snatlog.tgz
cd nfct-snatlog
make
make install
```

Com os comandos acima, você terá instalado o NFCT-SNATLOG em /usr/sbin/nfct-snatlog. Para executá-lo precisaremos carregar alguns módulos do kernel:

```
modprobe nf_conntrack
modprobe nf_conntrack_ipv4
modprobe nf_conntrack_netlink
```

E finalmente carregar o daemon:

```
/usr/sbin/nfct-snatlog --daemon
```

OBS: a configuração acima é volátil, o que significa que quando a máquina for reiniciada ela será perdida. Para carregar a configuração na inicialização do sistema, você deve criar um script no init.d (ou equivalente), porém essa configuração não será abordado no curso (na máquina virtual essa configuração foi feita no /etc/rc.local apenas para demonstração).

Para testarmos o funcionamento do NFCT-SNATLOG, vamos monitorar os logs no Firewall e realizar uma conexão TCP de uma das máquinas clientes. Para isso, execute o seguinte comando no Firewall:

```
tail -f /var/log/syslog
```

(para finalizar a visualização do log, tecle CTRL+C)

Agora, na máquina Host A, execute o seguinte comando:

```
wget http://www.pop-ba.rnp.br/Site/
```

Volte ao monitoramento do Firewall e verifique a geração dos logs (observe que deve demorar cerca de 120 segundos para a mensagem aparecer – discuta com seus colegas sobre esse atraso)

Parte 02: Envio dos logs para um servidor remoto

Uma configuração importante para garantir segurança e escalabilidade em ambientes desse tipo é a implantação de um servidor de logs remoto. Nessa parte da prática, vamos configurar o Firewall para enviar os logs do NFCT-SNATLOG para o servidor de Gerencia.

Para isso, na máquina **Gerencia**, precisaremos editar a configuração do syslog-ng. Para isso, edite o

arquivo /etc/syslog-ng/syslog-ng.conf e acrescente as seguintes linhas (elas já existem no final do arquivo para facilitar, então apenas descomente-as):

```
source s_udp { udp(port(514)); };
filter f_nfct-snatlog { facility(local4) and program("nfct-snatlog"); };
destination d_nfct-snatlog { file("/var/log/firewall/nfct-snatlog-${YEAR}${MONTH}${DAY}.log"
group("www-data")); };
log { source(s_udp); filter(f_nfct-snatlog); destination(d_nfct-snatlog); };
```

Em seguida, precisamos criar a pasta que armazenará os logs e setar algumas permissões:

```
mkdir /var/log/firewall
chown root.www-data /var/log/firewall
chmod 750 /var/log/firewall
```

Agora precisamos reiniciar o daemon do syslog-ng:

```
/etc/init.d/syslog-ng restart
```

Na máquina **Firewall**, edite o arquivo /etc/syslog-ng/syslog-ng.conf e acrescente as seguintes linhas (elas já existem no final do arquivo para facilitar, então apenas descomente-as):

```
destination d_logserver { udp("10.0.0.99" port(514)); };
filter f_nfct-snatlog { facility(local4); };
log { source(s_src); filter(f_nfct-snatlog); destination(d_logserver); };
```

Em seguida, reinicie o daemon do syslog para carregar

```
/etc/init.d/syslog-ng restart
```

Para testar a configuração acima, execute um acesso na máquina Host A (comando wget) e monitore o log em Gerencia (/var/log/firewall/nfct-snatlog-XXXXX.log).

OBS: Em um ambiente de produção, é recomendável a configuração do rotacionamento dos logs do Firewall, inclusive comprimindo-os. Essa configuração, no entanto, não será abordada neste mini-curso.

Prática 02: Instalação e Configuração do L2M em Gerencia

Este laboratório visa apresentar aos alunos os passos para configuração do L2M na máquina Gerencia para coleta e armazenamento da tabela ARP do Firewall.

Parte 01: Instalação do L2M

Os passos abaixo devem ser executados na máquina Gerencia, a menos que outra máquina seja explicitamente citada.

Faça o download do pacote do L2M:

```
wget http://www.pop-ba.rnp.br/files/sw/l2m.tgz
```

Descompacte o tarball na pasta do servidor web:

```
tar -xzf /root/l2m.tgz -C /var/www/
```

Precisamos criar o banco de dados para o L2M (apenas para ilustração, vamos usar a senha do banco "wtr2011", porém em um ambiente de produção recomenda-se usar uma senha aleatória e forte, por exemplo criada através do utilitário *mkpasswd*). Os passos são os seguintes.

- O primeiro passo é criar o usuário, para isso execute o seguinte comando (ao ser questionado sobre a senha, informe "wtr2011"):

```
su - postgres -c "createuser l2musr -S -D -R -P"
```

- O próximo passo é criar o banco de dados sob a propriedade do novo usuário. Para isso, execute o seguinte comando:

```
su - postgres -c "createdb l2mdb -O l2musr"
```

- Finalmente vamos dar permissão total sobre o banco criado para o usuário em questão:

```
su - postgres -c "psql -c \"GRANT ALL PRIVILEGES ON database l2mdb TO l2musr;\""
```

Agora, edite o arquivo /var/www/l2m/include/config.php e altere os parâmetros do banco de dados:

```
$db_host = 'localhost';
$db_name = 'l2mdb';
$db_user = 'l2musr';
$db_pass = 'wtr2011';
```

O próximo passo é criar as tabelas no banco de dados (ao ser questionado pela senha, informe "wtr2011" – a mesma usada anteriormente):

```
cd /var/www/l2m
psql -U l2musr -d l2mdb -h localhost -f docs/create.pgsql.sql
```

Acesse a interface do L2M e verifique se está funcionando corretamente (faremos a configuração na próxima seção). Para acessar a interface do L2M, utilize o IP do Firewall na interface eth0 (o comando "ifconfig eth0" deve listar tal IP):

```
http://<IP-Firewall-eth0>/l2m/
```

Precisamos configurar o poller do L2M. O poller é o script que periodicamente realizará as consultas nas tabelas ARP dos roteadores cadastrados e habilitados. Para habilitar o poller do L2M, adicione o script poller.php para execução no CRON, através dos seguintes comandos:

```
cd /var/www/l2m/
chown root.root docs/cron.d-l2m
chmod +x docs/cron.d-l2m
mv docs/cron.d-l2m /etc/cron.d/l2m
```

Parte 02: Configurando as consultas no L2M

A configuração do L2M que faremos consistirá nos seguintes itens:

- Adicionar os roteadores que monitoraremos
- Adicionar as VLANs
- Configurar os parâmetros para contenção (bloqueio) de hosts

O primeiro passo é configurar os roteadores que iremos monitorar, através da opção *Settings* > *Router Settings* > *Add Router*. Adicionaremos o roteador Firewall, que será consultado via SCRIPT (linux-ssh.sh) e deixaremos ele desabilitado enquanto finalizamos a configuração. Os parâmetros de configuração são:

- Name: firewall
- IP Addr: 10.0.0.254
- Query type: script
- Script path: linux-ssh.sh
- Disabled router: SIM (deixar o roteador desabilitado)

Para que o script linux-ssh.sh funcione corretamente, necessitaremos executar comandos remotamente, usando o protocolo SSH. A configuração do SSH para esse ambiente é um pouco mais complexa que o usual (e.g. autenticação baseada em chave pública, restrição de comandos, etc.) e não será abordada nesse curso. Assim, as máquinas virtuais que você recebeu já estão preparadas para execução do script. Caso deseje entender a configuração, recomendamos a leitura da seguinte referência:

http://www.pop-ba.rnp.br/Site/L2MLinuxScripts

O próximo passo é configurar as VLANs que monitoraremos. Apesar de nosso cenário na prática não possuir VLANs, vamos criar três delas para representar a topologia de rede que idealizamos. Para isso acesse a opção *Settings > VLAN Settings > Add VLAN*, e crie as VLANs conforme parâmetros a seguir:

- VLAN ID: 100
- VLAN Name: RedeExterna
- Network: ***<Informar a rede do laboratório (consulte o instrutor)>***
- Router: firewall

- VLAN ID: 200
- VLAN Name: RedeDMZ
- Network: 10.0.0.0/24
- Router: firewall

- VLAN ID: 300
- VLAN Name: RedeLabs
- Network: 172.16.0.0/24
- Router: firewall

Vamos voltar à configuração dos roteadores e habilitar a consulta ao Firewall: *Settings > Router Settings > editar o firewall > desmarcar opção "Disable router"*.

Para testar o funcionamento do script, aguarde o tempo da próxima consulta (a cada 5 minutos) e acesse a tabela de estatísticas para ver os MACs armazenados (*Stats > Stats by VLAN*).

Parte 03: Configurando o bloqueio no L2M

Nessa seção vamos analisar uma configuração básica de contenção (bloqueio) no L2M. O bloqueio será feito em um servidor Linux, usando o firewall nativo Netfilter/IPTables. Nesse curso, alguns detalhes de configuração serão omitidos a fim de agilizar o processo. Outras formas de bloqueio são possíveis, a exemplo do bloqueio via EXPECT, ou até mesmo via SNMP. Caso tenha interesse em testar o bloqueio em outros ambientes, entre em contato com o PoP-BA para desenvolvermos scripts alternativos.

Toda a configuração de chaves SSH e execução de comandos remoto já foi previamente realizada, bastando apenas alterar alguns parâmetros no L2M. Precisaremos editar a configuração do roteador (firewall) e das VLANs.

Acesse *Settings > Router Settings > editar firewall* e configure os seguintes parâmetros:

- Block Script: block-linux-ssh.sh
- Unblock Script: unblock-linux-ssh.sh

Acesse *Settings > VLAN Settings > editar VLAN 100, 200 e 300,* e configure os seguintes parâmetros:

- VLAN 100
  - Router interface: eth0
  - ACL Name: (deixe em branco)
- VLAN 200
  - Router interface: eth2

    - ACL Name: (deixe em branco)
- VLAN 300
    - Router interface: eth1
    - ACL Name: (deixe em branco)

Agora vamos tentar bloquear um host através do formulário em *Containment*. Forneça os dados abaixo:

- MAC Address: 08:00:27:dd:22:04
- VLAN: RedeLabs (VLAN 300)
- Block!

Para testar se o bloqueio teve sucesso (além da mensagem de retorno na interface), vamos acessar a máquina Host A e checar se ela consegue acessar algum recurso na rede:

```
ping -c 4 10.0.0.99
```

Agora realize o desbloqueio na mesma tela do L2M e verifique se a máquina volta a ter acesso à rede.

Prática 03: Instalação e Configuração do RT em Gerencia

O RT é usado como base para instalação do TRAIRA. Você pode aproveitar um ambiente existe e apenas adicionar a extensão do TRAIRA ou configurar um novo ambiente dedicado ao tratamento de incidentes de segurança. A vantagem dessa segunda abordagem é que você pode ter um servidor com acesso mais restrito, aumentando a segurança do ambiente.

Nesse mini-curso, o RT já encontra-se instalado e com configurações básicas. Um passo-a-passo para instalação do RT pode ser encontrado no seguinte endereço:

http://certbahia.pop-ba.rnp.br/HowToRT

O instrutor fornecerá uma visão geral sobre os passos de configuração.

Acesse a interface do RT e verifique se está funcionando corretamente (faremos a configuração na próxima seção). Para acessar a interface do RT, utilize o IP do Firewall na interface eth0 (o comando “ifconfig eth0” deve listar tal IP), usuário será “wtr2011” e senha “wtr2011”:

```
http://<IP-Firewall-eth0>/rt/
```

Prática 04: Instalação e Configuração do TRAIRA em Gerencia

Esta prática visa mostrar os passos necessários para instalação e configuração do TRAIRA na máquina Gerencia.

Parte 01: Instalação do TRAIRA

Faça o download do pacote do TRAIRA:

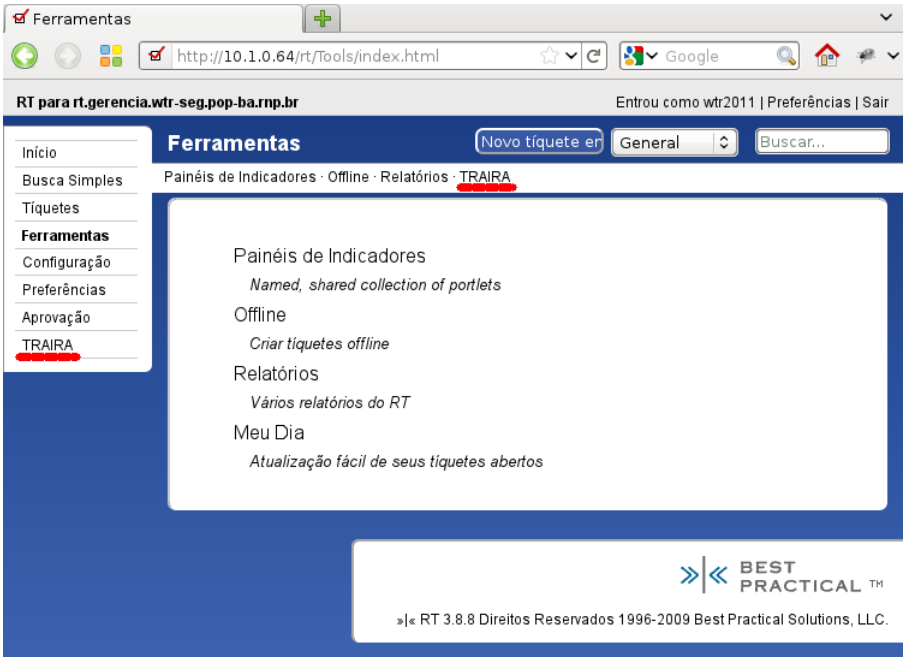
```
wget http://www.pop-ba.rnp.br/files/sw/rt-traira.tgz
```

Descompacte o pacote do TRAIRA no diretório raiz do RT:

```
tar -xzf /root/rt-traira.tgz -C /
chown -R root.root /usr/share/request-tracker3.8
```

Parte 02: Configuração do TRAIRA

Caso o TRAIRA tenha sido instalado corretamente, você terá uma nova opção nos menus do RT, conforme pode ser visto na imagem abaixo.



O TRAIRA estará acessível no menu principal do RT (menu à esquerda) ou através de *Ferramentas > TRAIRA*. As configurações necessárias serão listas abaixo.

O primeiro passo é criar um fila que será usada para o tratamento de incidentes. Para isso, acesse o menu *Configuração > Filas > Criar* e informe as seguintes informações:

- Nome da Fila: Security
- Descrição: Tratamento de Incidentes de Segurança
- Endereço para resposta: security@gerencia.wtr-seg.pop-ba.rnp.br
- Endereço para comentário: security-comment@gerencia.wtr-seg.pop-ba.rnp.br
- Criar

Além de criar a fila, gostaríamos de permitir a criação de chamados via e-mail. Para isso, precisaremos editar o arquivo /etc/aliases e acrescentar o seguinte (remove as entradas anteriores referentes ao alias `security` caso existam):

```
security: "| /usr/bin/procmail -a Security -a correspond"
security-comment: "| /usr/bin/procmail -a Security -a comment"
```

Não esqueça de executar o newalias para gerar os aliases acima:

```
newaliases
```

Agora definimos os filtros de criação de chamados de incidentes no procmail. Disponibilizamos uma versão básica de filtros do procmail no /root/configs, para ativá-la basta executar:

```
cp /root/configs/procmailrc /etc/procmailrc
```

Uma vez que a fila foi criada, vamos dar permissão para que qualquer usuário possa criar chamados nessa fila (um controle de acesso mais restritivo pode ser feito no procmail). Para isso, acesse o menu *Configuração > Filas > Segurity > Direitos de Acesso do Grupo,* no grupo "Todos" adicione a permissão "CriarTiquete" (basta selecionar essa opção e clicar em Salvar no rodapé da página).

Em seguida, vamos informar as configurações básicas do TRAIRA, para isso acesse o menu

Ferramentas > *TRAIRA* > *Configuracao* e preencha os seguintes campos:

- Nome da Fila: Security
- Tratamento automático: Habilitado
- Mapeamento Net2NAT:
  - Rede: 0.0.0.0/0
  - Disp. NAT: iptables
  - Arq. Log: /var/log/firewall/nfct-snatlog-%Y%m%d.log
  - *Add Net2NAT*
- IP2MAC Config – Consulta IP/MAC:
  - URL de Consulta: http://localhost/l2m/query.php?ip=$ip&date=$date&time=$time
  - Usuario p/ Consulta: (deixar em branco)
  - Senha p/ Consulta: (deixar em branco)
  - Realm p/ Consulta: (deixar em branco)
- IP2MAC Config – Bloqueio/Desbloqueio de MACs:
  - URL de bloqueio: http://localhost/l2m/block.php?mac=$mac&vlan=$vlan
  - URL de desbloqueio: http://localhost/l2m/unblock.php?mac=$mac&vlan=$vlan
  - Usuario p/ Bloq/Desb: (deixar em branco)
  - Senha p/ Bloq/Desb: (deixar em branco)
  - Realm p/ Bloq/Desb: (deixar em branco)

Com os parâmetros acima, já termos uma configuração funcional do TRAIRA. Vamos agora criar um parser para testarmos as notificações. Para isso, acesse o menu *Ferramentas* > *TRAIRA* > *Parsers* e preencha os seguintes campos em "Criar/Editar/Remover um parser":

- Nome do parser: certbahia-ssh-attack-teste
- From regex: certbahia@pop-ba.rnp.br
- Subject regex: Ataque ssh-brute force com origem em [0-9.]{7,15}
- Código do parser: pode usar o mesmo do exemplo, alterando apenas o número do AS, de 9999 para 53164. O código completo fica assim:

```
my $SPC = '[[:space:]]';
my $IP  = '[0-9.]{7,15}';
my $DATE = '[0-9-]{10}';
my $TIME = '[0-9:]{8}';
my $PORT = '[0-9]+';

if ($line =~ /^53164$SPC\|$SPC($IP)$SPC\|$SPC($DATE)$SPC($TIME)${SPC}srcport$SPC($PORT)\b.*$/ ) {
   my ($date, $time) = $self->AdjustTimezone($2, $3, '-0300');
   return ($date, $time, $1, $4);
}

return undef;
```

- Salvar

A fim de testar nossa configuração, vamos gerar algumas tentativas de ataque de força bruta SSH para um host de monitoramento que o instrutor criou. Verifique com o instrutor o endereço IP do sensor. Para realizar o ataque, foi criado um script simples nas máquinas Host A e Host B, o /root/ssh-brute-force.sh. Assim, execute os seguintes comandos em cada uma das máquinas HostA e HostB (simultaneamente):

/root/ssh-brute-force.sh IP-SENSOR /root/user-list /root/pass-list

Peça, então, para o instrutor reportar o incidente de segurança gerado para o TRAIRA que você configurou.

Agora, acesse a interface web do TRAIRA e verifique o tíquete que foi gerado na fila Security.

Habilite o bloqueio automático, através do menu *Ferramentas* > *TRAIRA* > *Acoes* e na seção de "Contencao" marque a opção "*Bloquear Host*".

Gere outros incidentes de segurança com os mesmos passos anteriores e peça para o instrutor reportar novamente os incidentes de segurança. Verifique agora se o host foi bloqueado na mensagem do tíquete e também diretamente no firewall (use o comando "iptables -L -n -v" para listar as regras do Netfilter/IPTables).

Boa prática! Em caso de dúvidas, não hesite em consultar o instrutor.