Utilizando Honeypots para Medição de Atividade de Rede não Usual na Internet

Emerson Virti[1], Leandro Márcio Bertholdo[2], Liane Tarouco[1], Lisandro Granville[1]

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brasil

[2] Ponto de Presença da Rede Nacional de Pesquisas no Rio Grande do Sul (PopRS/RNP) – Porto Alegre –RS – Brasil

{emerson,berthold}@pop-rs.rnp.br, liane@penta.ufrgs.br, granville@inf.ufrgs.br

Abstract. *This article quantifies and analyzes the profile of the attacks carried out against Internet applications through the use of honeypots. The analysis is supported in the results derived from the implantation of honeypots in the Point of Presence of the Brasilian National Research and Education Network in the Rio Grande do Sul. In the first experiment, a structure of honeypots integrated to the Brazilian Honeypots Alliance was implemented. In the second esperiment, a vast mesh of honeypots was created, emulating it operation of approximately 65,000 computers. These experiments had allowed to register and to follow the vulnerabilities explored currently more.*

Resumo. *Este artigo, através do uso de honeypots, quantifica e analisa o perfil dos ataques realizados contra sistemas via Internet. A análise é apoiada nos resultados derivados da implantação de honeypots no Ponto de Presença da Rede Nacional de Pesquisa no Rio Grande do Sul. No primeiro experimento, foi implementado uma estrutura de honeypots integrados ao Consórcio Brasileiro de Honeypots. No segundo, criou-se uma vasta malha de honeypots, emulando-se a operação de aproximadamente 65.000 computadores. Esses experimentos permitiram registrar e acompanhar as vulnerabilidades mais exploradas atualmente.*

1. Introdução

No início da era dos computadores as redes foram projetadas com finalidade de pesquisa, onde o objetivo principal era permitir diversas formas de conectividade entre as partes que estivessem interagindo. Dessa forma, foi dada ênfase à interoperabilidade e não à segurança [Schneier 2001].

Com o avanço da Internet, milhões de pessoas e instituições estavam agora interligadas via rede mundial de computadores. A segurança passou a ser uma necessidade fundamental tornando-se foco de discussão das comunidades envolvidas com a tecnologia de redes [Schneier 2001].

Nesse contexto, os administradores de sistemas procuraram formas de poderem tornar suas redes mais seguras. Diversos mecanismos e soluções de segurança foram sendo cada vez mais utilizados. Entre esses, os mais difundidos são os *firewalls* e os Sistemas de Detecção de Intrusão *(IDS).* Entretanto, de uma postura meramente

passiva, começou-se a buscar atrair os atacantes para sistemas especialmente construídos de modo a propiciar a inspeção e o estudo das técnicas e estratégias de ataque, adotando assim uma postura mais ativa no combate aos incidentes na Internet. Tais sistemas foram denominados Honeypots e surgiram para atender a necessidade de compreender o perfil dos ataques bem como de detectar as últimas tendências relativas às vulnerabilidades mais exploradas [Franco 2004].

Este trabalho descreve alguns resultados obtidos em dois experimentos realizados utilizando honeypots no Ponto de Presença da Rede Nacional de Pesquisa (POP-RS). No primeiro experimento, os honeypots foram integrados ao Consórcio Brasileiro de Honeypots [Consórcio 2005], e, com a obtenção das estatísticas dos honeypots de todos os integrantes desse consórcio, pode-se tecer algumas análises relativas aos dados coletados. No segundo experimento, com o objetivo de mensurar um tipo de tráfego "não usual", também conhecido como ruído de fundo na Internet (Background Noise) [Linehan 2004], alguns honeypots foram configurados para responder por um grande espaço de endereçamento IP roteável, totalizando cerca de 65535 hosts emulados.

2. IDSs e Honeypots

Um sistema de detecção de intrusão (IDS) é um mecanismo de segurança cuja função principal é detectar atividades incorretas, maliciosas ou anômalas na rede. Esta ferramenta roda constantemente em *background* e não deve causar grandes interferências no funcionamento normal da rede. Quando esse mecanismo detecta alguma ação que seja suspeita ou ilegal ele é capaz de gerar uma notificação ao administrador de rede e, em alguns casos, pode tentar interagir com hosts, firewalls e roteadores para evitar ou amenizar os danos causados pelo incidente.

Mais recentemente, uma nova alternativa passou a ser utilizada envolvendo o uso de Honeypots e Honeynets [Spitzner 2003]. Em 1999, Lance Spitzner conectou à Internet um computador propositalmente executando aplicativos com vulnerabilidades conhecidas. A idéia seria que este sistema funcionaria como um pote de mel (daí o nome) atraindo os atacantes. Spitzner surpreendeu-se, pois em menos de 15 minutos, seu host já havia sido comprometido [Spitzner 2002]. Surgia então o conceito de Honeypot, ou seja, "um recurso de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um Honeypot poderá ser testado, atacado e invadido. Os honeypots por permitirem tais ataques mas por registrarem o que é feito, fornecem informações valiosas sobre as estratégias utilizadas pelos atacantes" [Spitzner 2002]. No episódio orquestrado por Spitzner, o invasor acabou percebendo que estava sendo monitorado e apagou os logs do sistema. Assim, mostrou-se necessária a construção de ambientes que pudessem melhor gerenciar e monitorar as atividades dos invasores e registrar de forma segura as ações no honeypot. Surgiram então as chamadas Honeynets: redes que têm em sua arquitetura, sub-redes de honeypots. Nessas redes, os administradores podiam criar ambientes mais seguros, tendo a possibilidade de guardarem em diferentes *hosts* os logs gerados [Franco 2004].

Com aumento no número de redes que empregavam honeypots em suas arquiteturas criou-se a necessidade de trocar informações relativas aos ataques e as descobertas de novos recursos a serem empregados no monitoramento da ação dos invasores. Com essa

finalidade existem hoje várias instituições no mundo integradas na chamada Honeynet Research Alliance [Honeynet 2005]. Um dos integrantes dessa aliança é o Brasil através do Consórcio Brasileiro de Honeypots [Consórcio 2005], cujo objetivo é aumentar a capacidade de detecção de incidentes e avaliar as tendências de ataques no espaço de endereçamento IP da Internet brasileira. Para isso, esse consórcio implantou uma rede distribuída de honeypots, buscando cobrir a maior parte do espaço de endereçamento IP da Internet no Brasil.

O estudo dos logs gerados na monitoração das honeynets brasileiras, atuando conjuntamente com os Grupos de Resposta a Incidentes de Segurança de Computadores já propiciou a divulgação de alguns alertas no *site* do CERT.BR [Consórcio 2005]. A partir de 07/03/2005, algumas estatísticas relativas aos acessos aos honeypots integrantes, começaram a ser divulgadas diariamente no *site* do Consórcio Brasileiro de Honeypots [Consórcio 2005].

O uso de honeypots e honeynets melhora a segurança das redes e seus sistemas. Bruce Schneier [Schneier 2004], perito criptográfico e fundador e diretor da Counterpane Internet Security, decompõe a segurança em três domínios distintos: prevenção, detecção e reação. Um honeypot será útil nas três categorias.

Um honeypot não impedirá um atacante de entrar na rede, mas como a totalidade do tráfego originado pelo intruso fica registrada e pode ser analisada, é possível obter informações que permitirão, em outra ocasião, bloquear o mesmo ataque. Ou seja, o honeypot não impede ataques à rede ou a uma determinada porta (firewall) de um sistema, não se constituindo pois em um sistema de detecção de intrusão. No entanto, como é mais simples para invadir, pode conseguir que os atacantes invistam seus esforços em atacá-lo, em vez de tentarem penetrar em servidores estratégicos.

No que se refere à detecção, os ganhos são mais consideráveis. A razão para isso é simples: se as ferramentas complementares, como os IDS de rede, forem expostas a grandes fluxos de tráfego, terão dificuldade em processá-los. Separar o tráfego útil do tráfego malicioso é, por vezes, muito difícil. Uma das estratégias dos *hackers* consiste em ocupar um IDS, de modo a fazê-lo gerar um grande número de alarmes. Os falsos positivos (falsos alarmes) e a filtragem dos dados úteis continuam a ser quesitos em que os IDS precisam ser aprimorados. Um honeypot não tem esta problemática, pois todo o tráfego originado ou destinado aos hosts emulados é, por definição, suspeito, porque não deveria haver tráfego para tais sistemas uma vez que não são anunciados ou registrados em serviços de nomes. Embora isto não signifique que os falsos positivos sejam impossíveis, a possibilidade de acontecer é bem menor do que com um IDS de rede.

Finalmente, a resposta (ou reação) é um quesito que precisa ser verificado com cuidado. A detecção de pouco vale quando não se tem uma capacidade de resposta adequada. Através da análise dos logs gerados no honeypot a equipe de segurança pode tomar medidas técnicas para a proteção contra a vulnerabilidade explorada e até buscar a identificação e a punição legal dos atacantes.

Para estudar o comportamento e a quantidade de tráfego hostil na rede, foi instalado um honeypot no POP-RS, utilizando o software honeyd. Esse honeypot é dito de baixa interatividade, pois apenas emula o comportamento de diversos sistemas operacionais

sem, no entanto, dar acesso ao real sistema operacional do computador onde o software é instalado.

2.1. Características do Honeyd

Seguindo a recomendação do Consórcio Brasileiro de Honeypots, para a instalação do honeypot no POP-RS foi escolhido a ferramenta de baixa interatividade Honeyd [Honeyd 2005]. Esse software possui capacidade de emular o funcionamento de diversos hosts, podendo, em cada um, simular a operação de um sistema operacional diferente. Para isso, objetivando aumentar a segurança e simular ao máximo as pilhas TCP/IP dos sistemas operacionais, o Honeyd capta o tráfego de rede através de um proxy ARP (Arpd) [Arpd 2005], utilizando bibliotecas específicas (Libnet e Libcap) [Libnet 2005] e não fazendo uso de qualquer socket do sistema operacional. Desse modo, quando instalado em um ambiente UNIX, o comando netstat, que demonstra as conexões de rede do host, não mostra as comunicações relativas ao honeypot. As trocas de mensagens entre o Honeyd e o sistemas invasores são transparentes ao sistema operacional. O honeyd trabalha apenas com os protocolos TCP, UDP e ICMP.

Através do honeyd é possível simular a existência de uma complexa rede de computadores. Esta rede pode simular a operação de vários hosts e roteadores, como, por exemplo, a estrutura apresentada na figura 2.1.1.

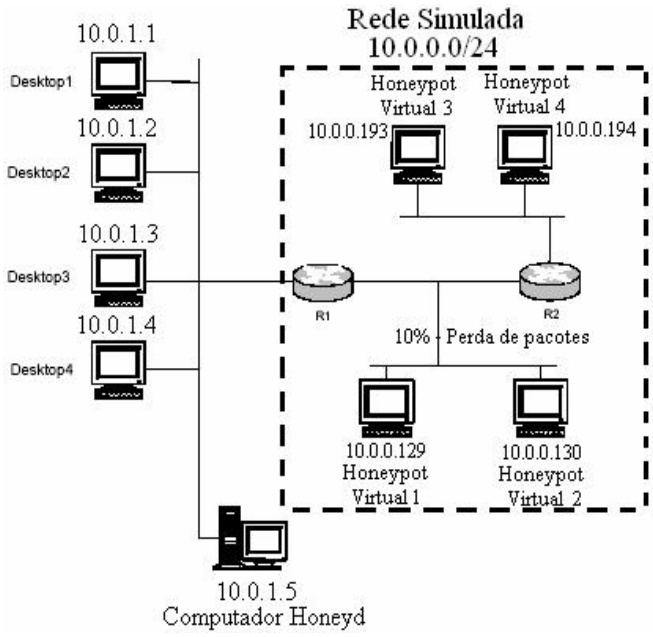

Figura 2.1.1: Simulação de uma rede usando Honeyd

Como forma de exposição das principais funcionalidades do Honeyd, a figura acima apresenta uma estrutura de honeynet utilizando esse software. Para o exemplo, foram utilizados endereços IP não roteáveis (bloco 10.0.0.0/8), porém, no sistema posto em produção, foram empregados endereços roteáveis. No caso apresentado, só existem 5 hosts reais: 4 desktops e um computador operando com Honeyd. Apesar desta máquina possuir o endereço 10.0.1.5, ela é capaz de responder a toda conexão a qualquer IP existente no bloco 10.0.0.0/24. Na configuração descrita na figura, dos 255 endereços disponíveis no bloco, apenas 6 foram utilizados: 4 para simular hosts e dois para

simular roteadores. Nessa configuração optou-se ainda por emular uma rede com 10% de perda de pacotes entre o roteador R1 e o roteador R2.

Para os objetivos desse projeto, a principal característica desejada foi a possibilidade do sistema registrar qualquer tentativa de acesso aos endereços IPs simulados pelo honeypot. Dessa forma, com a exposição do honeypot à Internet, pode-se verificar o número de acessos à determinadas portas e, com isso, ensejar uma pesquisa no intuito de avaliarmos as vulnerabilidades mais exploradas.

3. Experimento 1 – Integrando o Consórcio Brasileiro de Honeypots

No intuito de ter acesso às estatísticas dos logs gerados em todos os honeypots participantes do Consórcio Brasileiro de Honeypots, a integração do POP-RS ao consórcio foi uma premissa para a instalação do honeypot. Após o término dessa instalação, três membros do POP-RS puderam ter acesso aos e-mails criptografados que diariamente eram enviados a todos os responsáveis pelos honeypots integrantes do consórcio. Assim como nas estatísticas públicas divulgadas atualmente no site do consórcio [Consórcio 2005], nas estatísticas apresentadas apenas aos seus integrantes, dentre outras informações, aparecem as principais portas TCP e UDP com maior número de pacotes trafegados. A Figura 3.1 demonstra a localização de cada uma das instituições integrantes. O POP-RS foi incluído com o nome de CERT-RS (*Computer Emergency Response Team - Rio Grande do Sul*).

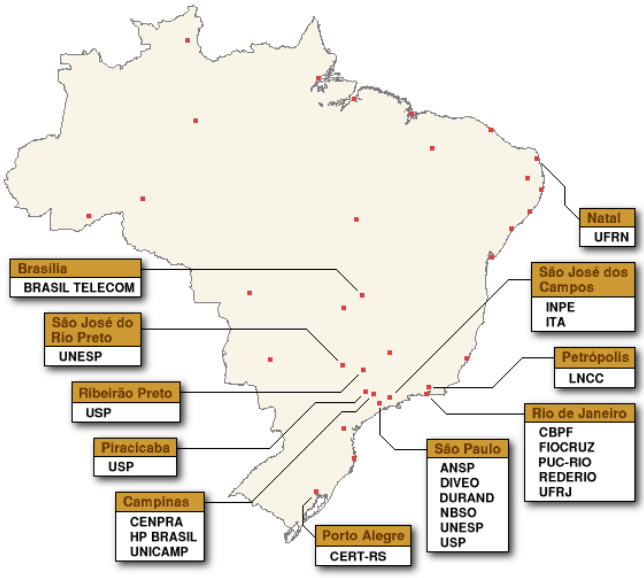

Figura 3.1: Brazilian Honeypots Alliance

3.1. Analisando Informações obtidas via Honeypot

Através da vinculação do POP-RS ao projeto honeynet.br, foi possível ter acesso às estatísticas de cada instituição integrante. Cada e-mail recebido correspondia aos dados referentes a uma instituição participante. Diariamente, eram recebidas 25 mensagens criptografadas contendo informações como a quantidade de pacotes recebidos, o

tamanho total dos logs e as portas TCP e UDP com maior quantidade de pacotes trafegados. Abaixo segue um demonstrativo dos dados coletados (Tabela 3.1.1).

DADOS RELATIVOS À MONITORAÇÃO DOS LOGS NA HONEYNET.BR	
Datas de Monitoração	DE 11/10/2004 à 09/11/2004
Quantidade de Dias de Monitoração	30 DIAS
Total de E-mails	690
Número Total de Pacotes	225.773.037
Tamanho Total dos Logs Gerados	5,74GB

Tabela 3.1.1 Dados relativos à monitoração dos logs na Honeynet.br

A apresentação do número de pacotes trafegados nos honeypots pode ser de grande utilidade na verificação das vulnerabilidades mais buscadas pelos atacantes. Em 22/06/2005, por exemplo, foi descoberta uma vulnerabilidade no software para backup Veritas [Veritas 2005]. Cinco dias depois, a porta 10000/TCP, utilizada pelo software, já aparecia entre as dez portas TCP com maior número de pacotes trafegados. A Figura 3.1.2 se refere às estatísticas públicas divulgadas no site do Consórcio Brasileiro de Honeypots no dia 27/06/2005, onde pode-se perceber a presença da porta utilizada pelo software.

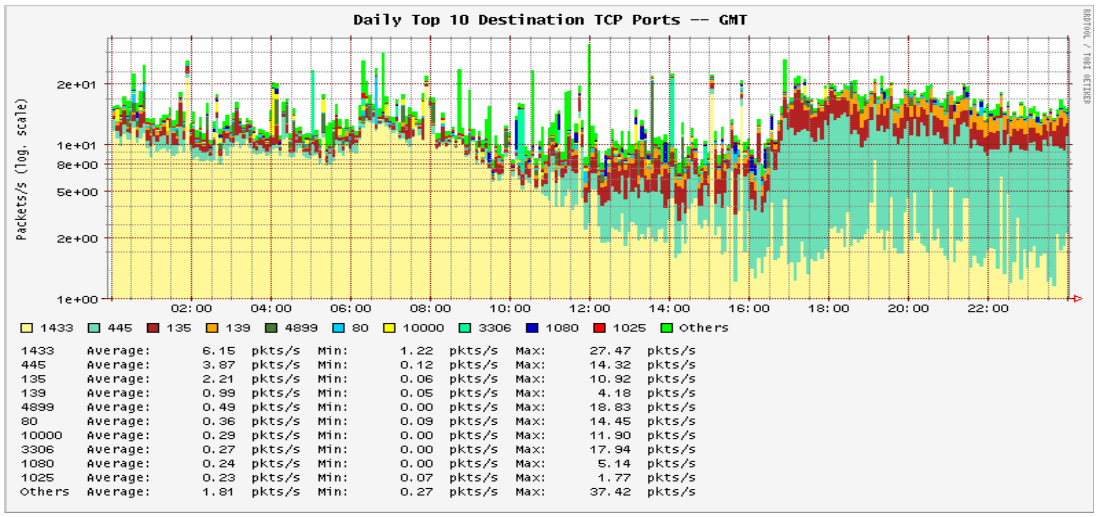

Figura 3.1.2: Presença da porta 10000/TCP entre as dez portas TCP com maior número de pacotes trafegados

Com os dados recebidos referentes ao número de pacotes TCP e UDP trafegados, através de pesquisa realizada foi possível compor um demonstrativo que elucida as vulnerabilidades mais procuradas na Internet na época da análise relatada neste trabalho. A seguir, esse demonstrativo é apresentado.

PORTAS TCP

Porta 445: 28.609.492 acessos.

microsoft-ds: é a porta destinada ao serviço de compartilhamento de arquivos no MS Windows. Estes acessos são tipicamente feitos por sistemas que tentam se conectar a arquivos que podem estar disponíveis caso o usuário não proteja seus arquivos compartilhados. Enquanto muitos desses acessos podem ser provenientes de vírus e vermes tentando se propagar, podem ser também oriundos de usuários maliciosos tentando se conectar ao computador desprotegido. Uma vez conectado esses invasores podem fazer download, upload ou até mesmo editar os arquivos compartilhados.

Porta 135: 13.241.238 acessos.

Loc-srv - comumente utilizado pelo serviço de *remote procedure call* (RPC). Alguns vermes como o W32.Blaster utilizam essa porta como forma de tentarem invadir o sistema vulnerável e se espalharem pela rede. Esse *worm,* particularmente, utiliza a vulnerabilidade do Microsoft RCP [Symantec 2004].

Porta 139: 3.828.526 acessos.

NETBIOS Session Service – é utilizado para compartilhamento de recursos no MS Windows. Assim como a porta 445/tcp, antes mencionada, é uma porta utilizada para a conexão aos arquivos compartilhados [CA200308 2003].

Porta 1433: 2.658.633 acessos.

Microsoft-SQL-Server – utilizado para conexões remotas ao banco de dados SQL. Alguns vermes como o W32.SQLExp.worm utilizam massivamente essa porta para tentarem fazer ataque DoS (*Deny of service*) [CERT 2002] .

Porta 5554: 2.120.208 acessos.

LSASS - o *Local Security Authority Subsystem Service* é um componente do sistema operacional Windows que atua no momento do login dos usuários. No final de 2003 [CVE 2004] foi publicada uma vulnerabilidade (*buffer overflow)* associada a esse software. Alguns worms como o W32.Sasser.Worm e suas variantes, utilizam dessa vulnerabilidade para se disseminarem na rede [Symantec 2004].

Porta 1080: 2.118.288 acessos.

Socks – Porta que, destinada ao uso de sockets, é utilizada pelo worm W32.Beagle. Esse verme constrói seu próprio serviço de e-mail para espalhar seus ataques massivos na Internet e abrir suas *backdoors,* utilizando a porta 1080/TCP [Symantec 2004].

Porta 1025: 1.875.409 acessos.

Atualmente é utilizada como RPC da Microsoft. Assim como a porta 135/TCP, é utilizada como forma de entrada de alguns worms. A vulnerabilidade que é explorada nessa porta foi publicada no mesmo artigo que

trata do problema de segurança no MS RPC da porta 135/TCP [Symantec 2004][MS0326 2004].

Porta 9898: 1.847.902 acessos.

Utilizada como *backdoor* de alguns trojans como o Backdoor.CrashCool e alguns vermes como o W32.Dabber [Symantec 2004].

Porta 1023: 1.777.006 acessos.

Trata-se de uma recente vulnerabilidade do Microsoft Windows (abril de 2004) consertada em agosto de 2004 [MS04011 2004]. Alguns worms como o W32.Sasser.E.Worm exploram essa vulnerabilidade e tentam abrir conexões nessa porta para instalar um servidor de FTP. Os clientes desses worms, através de massivos scans aos endereços da rede, tentam verificar se os computadores possuem conexões a tal porta.

Porta 80: 925.718 acessos.

http: tipicamente utilizado pelos servidores web. Muitos *exploits* tentam encontrar vulnerabilidades nesses servidores. O *exploit WebDav,* por exemplo, tenta invadir os servidores web utilizando tentativas de buffer overflow. Alguns vírus, como o Ninda, e alguns worms, como o Code Red, também utilizam esta porta no intuito de atacar os servidores web.

PORTAS UDP

Porta 137: 4.333.676 pacotes.

netbios-ns: *Netbios Name Service* é o sistema utilizado pelos sistemas operacionais Windows para encontrar informações relativas aos recursos oferecidos à Internet pelo hosts, tais como nome arquivos compartilhados, impressoras compartilhadas, nome do sistema, etc. Freqüentemente os scans destinados a essa porta são resultado da ação de alguns worms como BugBear e Opaserv que exploram os arquivos compartilhados na intenção de se propagarem.

Porta 53: 680.070 pacotes

domain: *Domain Name Service* é o serviço responsável pelo tradução entre nomes de hosts e endereços IP dos computadores. Aqui pode-se destacar algumas vulnerabilidades conhecidas no software mais comum para o serviço de DNS: o BIND.

Porta 1434: 177.384 pacotes.

ms-sql-m: Microsoft SQL Monitor é usado para monitorar o banco de dados Microsoft SQL. Devido a algumas vulnerabilidades conhecidas nesse serviço (Microsoft Security Bulletin MS02-039 and Microsoft Security Bulletin MS02-061) alguns worms como o W32.SQLExp tentam, através do envio de muitos pacotes de pequeno tamanho, ocasionar um ataque de DOS. Também explorando vulnerabilidades nesse serviço, o worm Slammer, no final de janeiro de 2003 conseguiu, em puçás horas, contaminar 400.000 servidores.

4. Experimento 2 - Ampliando a Utilização de Honeynets

Após o conhecimento das vulnerabilidades mais procuradas, o passo seguinte foi ampliar a utilização dos honeypots de baixa interatividade a fim de conseguir dados que levassem a detecção de máquinas contaminadas nas redes dos clientes do POP-RS. Dessa forma, desejava-se detectar tentativas de conexões aos honeypots partindo de computadores das próprias redes dos clientes desse ponto de presença, de forma a detectar infecções o mais rápido possível, evitando maiores estragos causados pelas contaminações aos computadores da rede.

Baseando-se no "princípio da proximidade", exposto por Thorsten Holz em sua tese "New Fields of Application for Honeynets" [Holz 2005], a maioria dos *malwares* (virus, vermes, cavalos de tróia), tentam atacar alvos próximos ao seu espaço de endereçamento (mesma sub-rede ou classe B). Isso indica que quanto mais próximo de uma máquina contaminada maiores as chances de se sofrer um ataque no início da contaminação (proximidade da referência). Dessa forma, foi proposta uma estrutura de supernets utilizando grandes blocos IP alocados para várias instituições mas sem uso real. Com a devida autorização das proprietárias dos endeços Ips, todas essas redes foram anunciadas via BGP4 e direcionadas para uma honeynet única, de forma a ela responder a um espaço de endereçamento equivalente a um classe B (65536 endereços IP) (vide figura 4.1).

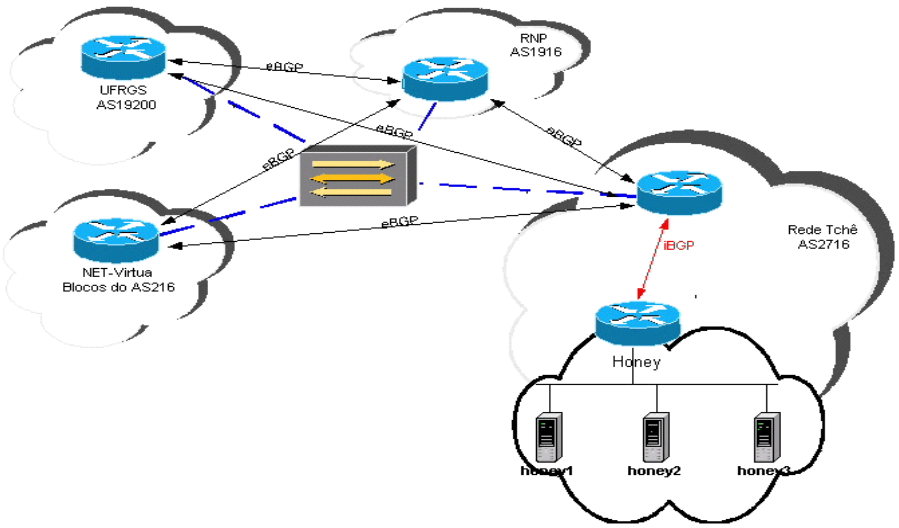

Figura 4.1: Esquema de roteamento utilizado

4.1 Resultados Alcançados

Pela verificação dos dados obtidos, foi detectada uma atividade não usual considerável, o que levou a inúmeras dificuldades para a implantação do projeto inicialmente proposto. Situações limites como a falta de processamento no roteador responsável pelo anúncio BGP das redes devido ao alto volume de pacotes por segundo (Figura 4.1.1) somados a falta de memória RAM devido à grande tabela ARP do switch, do roteador e

dos próprios servidores envolvidos, criaram a necessidade de fazer-se pequenos ajustes na solução inicialmente implementada.

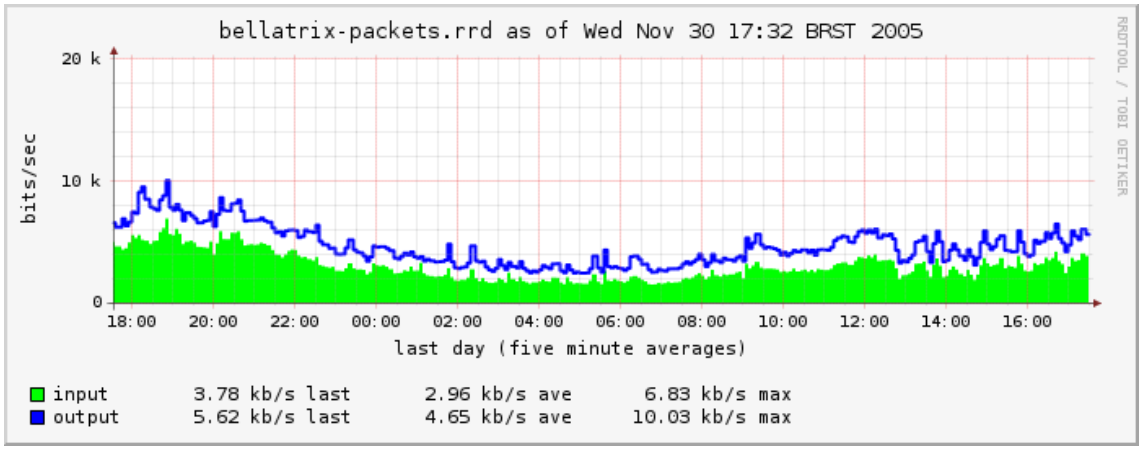

Figura 4.1.1: Número de pacotes por segundo para endereços Ips dos honeypots

Dentre os dados obtidos, o ruído verificado nesses endereços não utilizados surpreendeu em todos os sentidos, tais como o próprio volume de bits por segundo transferidos, que alcançou a cifra de Megabits por segundo (Figura 4.1.2). Ressalta-se que esse tráfego é considerado ruído porque ele simplesmente não deveria existir.

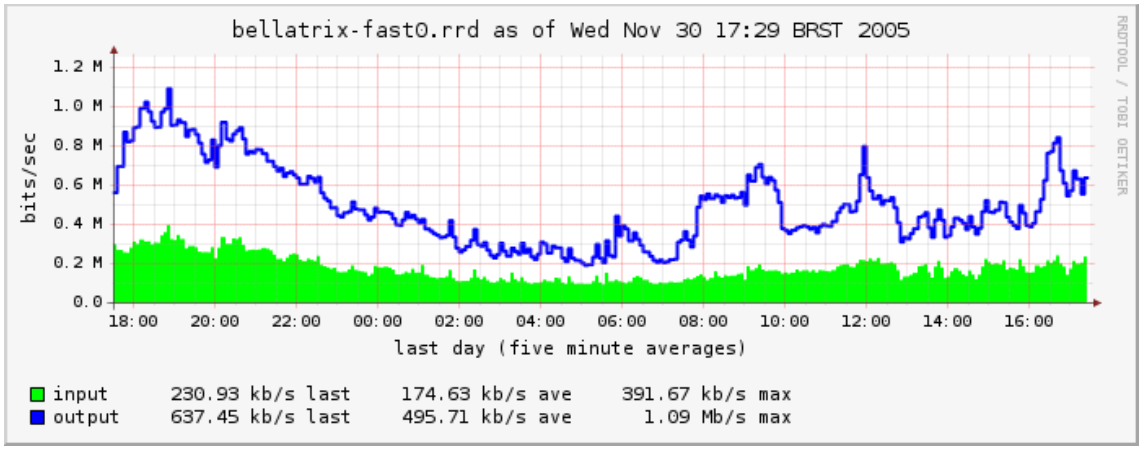

Figura 4.1.2: Volume de tráfego para endereços IP não usados

Dentro das supernets divulgadas via BGP, estavam blocos de instituições acadêmicas pré-CIDR (endereços IPV4 que não tinham 200 ou 201 como octeto inicial) e pós-CIDR. Foram utilizados endereços de redes domésticas (Cable-modem), blocos atribuídos à empresas e blocos acadêmicos. Cada um desses blocos está representado segundo a Tabela 4.1.3.

Espaço de Endereçamento	Total por dia	Total de scans por endereço IP	Média de scans por IP por hora
Acadêmico /18	32.145.835	1977,48	82,39 ~1,4 scan/min
Comercial /18	32.145.835	236,16	9,84 ~0,16 scan/min
Acadêmico /17	3.838.989	121,23	5,05 ~0,08 scan/min
Cablemodem /20	3.941.556	1272,85	53,4 ~ 0,89 scan/min

Tabela 4.1.3: Média das tentativas de acesso diárias segmentadas por classes de endereço

Outro ponto relevante que prova a proximidade de referência existente na Internet, onde os honeypots podem ser utilizados para a rápida detecção de máquinas contaminadas por *malwares* que efetuam varreduras a procura de vulnerabilidades, é comprovado na Figura 4.1.4. A figura apresenta os resultados dos endereços fontes dos acessos aos honeypots de uma instituição que utiliza um bloco pré-CIDR comparados à outra instituição que tem seus endereços IPV4 dentro do bloco 200.0.0.0/8 (atribuídos ao Brasil). Como pode-se perceber, para a instituição acadêmica, há uma maior tendência de sofrer tentativas de acesso ilegais vindas do exterior e não partindo de endereços brasileiros.

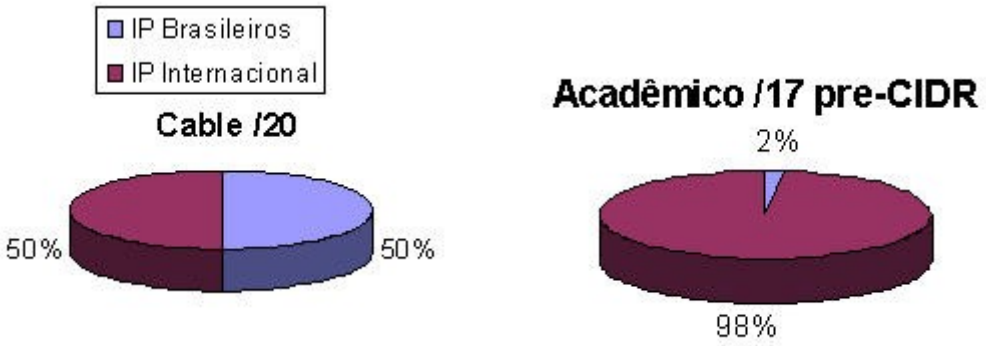

Figura 4.1.4: Quantidade de acesso quanto a sua origem

Os dados obtidos pelos honeypots permitem armazenar os conteúdos dos pacotes recebidos. Com esses dados pode-se fazer uma avaliação de tipos de *malwares* responsáveis pelas tentativas ilegais de acessos. Muitas vezes, no conteúdo dos pacotes enviados aos honeypots vêm tentativas de, através da exploração de alguma vulnerabilidade, fazer *download* de arquivos binários na intuito de contaminar a máquina destino de tais acessos. A Tabela 4.1.5 apresenta o resultados da verificação dos pacotes destinados a posta 445/TCP dos honeypots do POP-RS. Essa porta é associada ao serviço de compartilhamento de arquivos e impressoras no Windows.

Lista do 10 Malwares mais Usados	Sistema Operacional Origem
MSupdate.exe	Windows 96,93%
XPService.exe	Linux 2,98%
bling.exe	Solaris 0,04%
ccenmgr.exe	OpenBSD 0,03%
csexp.exe	FreeBSD 0,01%
hostin.exe	NetBSD 0,01%
intec.exe	Outros 0,01%
internet4.exe	
ipxroute32x.exe	
msfdfe.exe	

Tabela 4.1.5: Malwares mais procurados e sistema operacional mais fragilizado

5. Conclusões

Esse trabalho tem sua importância comprovada na análise dos resultados da implantação de uma grande arquitetura de honeypots nas dependências do POP-RS. Ao todo, foram emulados o equivalente a um classe B de endereçamento IPV4, ou seja, aproximadamente 65536 computadores virtuais. Cada um desses computadores tinha seu endereço IP (real - roteável) pertencentes ao espaço de endereçamento de algumas instituições conectadas ao POP-RS.

Através da vinculação com o Projeto Honeypots Distribuídos (de abrangência nacional), os logs gerados pelos honeypots do POP-RS foram compartilhados com a comunidade de segurança no site desse projeto [Consórcio 2005].

As respostas obtidas por este trabalho foram surpreendentes, pois demonstraram, em sua parte quantitativa, que cada computador conectado à Internet está exposto a um grande volume de tentativas maliciosas de acesso. Na parte qualitativa, foi-se verificado os serviços mais atacados e, pelo conteúdo dos pacotes recebidos, os arquivos binários que seriam executados caso os hosts aos quais tais acessos fossem destinados estivessem com vulnerabilidades na porta 445/TCP (compartilhamento de arquivos no Windows). Pela verificação dos endereços IP fonte dos pacotes, pôde-se ainda comprovar a hipótese da proximidade por referência (figura 4.1.4), onde os *malwares* geralmente procuram por vulnerabilidades em endereços IPs próximos ao espaço de endereçamento ao qual pertencem.

A relevância desses dados está ligada ao fato de apresentarem, de forma quantitativa e qualitativa, o perfil atual da segurança na Internet.

5. Referências

[Holz 2005]Holz,Thorsten New Fields of Application for Honeynets. Diploma Thesis, Department for Computer Science of Aachen University, Germany.

[Schneier 2001] Schneier, Bruce. Segredos e Mentiras Sobre a Proteção na Vida Digital. Rio de Janeiro: Campus, 2001.

[Franco 2004] Franco, Lúcio H; Barato, Luís G.; Montes, Antônio. Instalação e Uso de Honeypot de Baixa Interatividade – 17a Reunião do Grupo de Trabalho em Engenharia de Redes – GTER 17 – 2004 – on line – http://eng.registro.br/gter17/videos

[Honeynet 2005] Honeynet Research Alliance - on line – 2005
http://www.honeynet.org/alliance

[Consórcio 2005] Consórcio Brasileiro de Honeypots - on line – 2005
http://www.honeypots-alliance.org.br/index-po.html

[Spitzner 2002] Spitzner, Lance. Honeypots: Tracking Hackers. ed. Pearson, 2002

[Honeyd 2004] Developments of the Honeyd Virtual Honeypot, 2004
http://www.honeyd.org

[Libnet 2005] Libdnet Source, 2004 http://libdnet.sourceforge.net/

[Linehan 2004] Linehan, Eamonn. Internet Worm Detection as part of a Distributed Network Inspection System. Dissertação de Mestrado em Ciência da Computação. University of Dublin.

[Arpd 2004] Arpd Source, 2004 http://www.citi.umich.edu/u/provos/honeyd/

[Symantec 2005] Symantec United States, 2004 http://www.symantec.com/

[MS0326 2004] Microsoft Security Bulletin MS03-026, 2004
http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx

[CA200308 2003] CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares, 2003 - http://www.cert.org/advisories/CA-2003-08.html

[CERT 2002] Exploitation of Vulnerabilities in Microsoft SQL Server, 2002
http://www.cert.org/incident_notes/IN-2002-04.html

[CVE 2004] Common Vulnerabilities and Explosures, 2004
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533

[MS04011 2004] Microsoft Security Bulletin MS04-011, 2004
http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

[Veritas 2005] Veritas Backup Exec Remote Agent for Windows Servers
http://support.veritas.com/docs/276604

[Spitzner 2003]The Honeynet Project: Trapping the Hackers. IEEE SECURITY & PRIVACY, March/April-2003