SpotLight: Sistema de Detecção, Monitorização e Isolamento a Intrusão

Bruno Castro[1], Edmundo Monteiro[1],

[1] Laboratório de Comunicações e Telemática
DEI/CISUC, Pólo II, Universidade de Coimbra
3030-290 Coimbra, Portugal
{bcastro,edmundo}@dei.uc.pt

Resumo
Neste artigo é apresentada uma solução aplicacional baseada nos conceitos de *HoneyNet* e *HoneyPot*, capaz de promover o incremento do nível de segurança numa dada infra-estrutura operacional. Para tal, discutem-se os objectivos, a arquitectura tecnológica/aplicacional implementada e os resultados obtidos durante a fase de piloto. Pensa-se que esta abordagem perante o tema da Segurança Informática, abrangendo os termos de detecção, prevenção e resposta aos riscos inerentes da Internet actual, constituirá uma base tecnológica de evolução para um conjunto de organizações que pretendam reforçar os seus níveis de "protecção" em ambientes empresariais. Da mesma forma, o artigo poderá ser considerado como válido cientificamente pela comunidade académica da área tecnológica em causa – Segurança Informática.

1 Introdução

A "segurança informática" é um requisito fundamental para o suporte da tecnologia Internet. Ou seja, é este o conceito que transforma a Internet de uma curiosidade académica numa séria ferramenta empresarial e corporativa. Os limites da segurança informática são os limites da Internet. E não existe indivíduo ou empresa fora dos limites e necessidades da segurança informática. Apesar dos riscos de segurança existentes na Internet, as empresas não têm outra alternativa senão participar neste mundo, ainda que inseguro. As perspectivas de novos mercados, novos clientes, novas receitas, novos modelos de negócio são de tal modo atractivas, que as empresas aceitam de bom grado sujeitarem-se a esses riscos de segurança iminentes. Não existe alternativa. Esta, mais do que qualquer outra, é a razão principal da segurança informática ser tão importante actualmente.

"*A Segurança Perfeita é um Mito!*" Não existe sistema, aplicacional ou tecnológico, completamente seguro. A conectividade implica sempre uma exposição ao risco e um consequente risco associado. Permitindo o acesso de utilizadores legítimos aos sistemas e à rede, local ou remotamente, a oportunidade de abuso e exploração existirá sempre. Este, foi um dos princípios no qual o desenvolvimento do SpotLight se baseou.

Actualmente, e no decorrer do constante aparecimento de novas ameaças, as organizações apresentam uma abordagem de segurança estruturada em três áreas distintas: prevenção, detecção e resposta. A prevenção é a base defensiva que previne a intrusão ou acesso não autorizado aos recursos corporativos; a detecção consiste na identificação de falhas no processo de prevenção e na gestão de alarmística; finalmente, a resposta é o modo como a organização reage a qualquer eventualidade ou incidente de segurança.

A segurança é baseada em pessoas, e as pessoas cometem erros. Nesse contexto, e independentemente das medidas preventivas, tecnológicas ou processos implementados na organização, é garantido que existirá uma falha de segurança algures no tempo. Assim, é fundamental uma rápida detecção e resposta ao eventual incidente, valorizando a componente de detecção numa abordagem de segurança corporativa.
Uma detecção eficaz é preponderante para a manutenção do nível de segurança de uma organização, garantindo a disponibilidade e competitividade do negócio em causa. Primeiro, ao identificar rapidamente actividade não-autorizada, poderá ainda ser possível deter o ataque. Segundo, a rapidez da detecção poderá ser fundamental para mitigar o impacto de uma intrusão bem sucedida.

O princípio fundamental da segurança informática baseia-se no seguinte conceito: "*nenhuma infra-estrutura de rede é completamente segura*". A segurança informática está completamente dependente e relacionada com a gestão de risco. Ou seja, quanto maior for o valor real do imóvel e quanto maior for a exposição a ameaças de segurança, maior terá que ser o esforço envolvido na implementação da segurança a esse mesmo imóvel. Deste modo, é fundamental ser capaz de avaliar correctamente o valor do imóvel, o grau de exposição a ameaças de segurança e as medidas de segurança apropriadas para o caso [RISK MANAGEMENT].

Tradicionalmente a segurança informática tem sido unicamente defensiva. Os processos de implementação de segurança nas organizações, baseiam o seu âmbito em mecanismos singularmente defensivos, tais como *firewalls*, sistemas de detecção a intrusão (IDS), antivírus e encriptação. A estratégia utilizada prende-se com a implementação da CIA *Triad* (Confidencialidade, Integridade e Disponibilidade) onde as medidas correctivas são a prevenção, detecção e resposta [CIA TRIAD]. Ou seja, é necessário defender a organização de uma forma eficaz, ter capacidade de detectar todas as vulnerabilidades no sistema de defesa, assim como ter capacidade de reagir rapidamente a qualquer ameaça ou intrusão dos sistemas.

Os sistemas de HoneyPot ou *HoneyNet* podem ser considerado como ferramentas de aprendizagem e recolha de informação sobre as tecnologias e metodologias da comunidade *hacker*. O método utilizado baseia-se no desenvolvimento e implementação de uma armadilha conceptual integrada num ambiente devidamente estruturado e bem definido, e com o único objectivo de caçar *hackers* em plena acção.

Lance Spitzner, membro e fundador do grupo de investigação *HoneyNet Project*, apresenta a sua definição do termo *"HoneyPot"* do seguinte modo:

"*A security resource who's value lies in being probed, attacked or compromised.*" [SPITZNER2003MAY].

Pode-se considerar uma definição bastante genérica e simplista, que é associado ao quase integral consenso dentro da comunidade *HoneyPot*. Esse seria um dos objectivos da abordagem de Spitzner, sendo capaz de englobar a totalidade dos sistemas *HoneyPot* actualmente existentes e do mesmo modo, disponibilizando uma futura integração de novos dados, fruto do progresso na investigação do tema *HoneyPot*.

Apesar do *HoneyPot*, como solução conceptual, ser um sistema com uma arquitectura simples de fácil implementação e integração, ainda combina algumas "virtudes" adicionais para a maioria dos cenários empresariais: volumes de informação reduzidos, capacidade de aprendizagem, indiferente a protocolos de comunicação, processamento pouco exigente, simplicidade e flexibilidade [SPITZNER2003MAY].

O presente trabalho, SpotLight, propõe uma plataforma tecnológica e aplicacional, baseada nos conceitos funcionais de uma *HoneyNet Generation II* [SPITZNER2005MAYGENII], acrescido de algumas das principais funcionalidades de uma *Virtual HoneyNet* [SPITZNER2003JAN]. Apresenta ainda, algumas funcionalidades referentes à sua capacidade de resposta e disponibilidade perante ataques externos, tendo sido implementada uma arquitectura aplicacional com elevada capacidade de aprendizagem e angariação de informação sobre as mais diversas metodologias comportamentais da comunidade *hacker* actual.

O objecto do trabalho, iniciou com a investigação e análise dos conceitos académicos, e das várias soluções/implementações existentes na comunidade HoneyNet. A noção, entretanto adquirida, das potencialidades da tecnologia em causa, relacionado directamente com o conhecimento do mercado actual e estado de arte da Segurança Informática, permitiu desenvolver uma "ideia" concreta, suportada através de uma definição clara das necessidades específicas a implementar ao abrigo deste projecto. De seguida, após a definição e formalização da estrutura aplicacional do projecto - SpotLight, foi iniciado o processo de implementação baseado nos conceitos adquiridos previamente. A estrutura conceptual do SpotLight foi desenvolvida e implementada assentando sobre um conjunto de requisitos e objectivos bastante concretos: disponibilidade de serviço, capacidade de aprendizagem, conhecer as fragilidades do sistema de produção e a capacidade de recolha de evidências.

Resumindo, o SpotLight para além de respeitar os conceitos básicos do modelo inerente à *CIA Triad*, tem como principais objectivos: manter a disponibilidade de um qualquer serviço crítico para a organização; "desviar" as atenções de sistemas realmente vitais para a organização, para sistemas secundários ou meramente redundantes; capacidade de desenvolver evidências legais de qualquer tentativa de intrusão e principalmente, a capacidade de aprendizagem de vulnerabilidades do sistema defen-

sivo actual da organização, tais como a aprendizagem de novas tecnologias ou metodologias de ataque. Assim é, possível manter os conceitos da CIA *Triad*, activar mecanismos de resposta e aquisição de informação que possibilite optimizar todo o processo de aprendizagem interno e externo à organização, e ainda recolher o máximo de evidências de ataques e tentativas de intrusão.

O artigo está estruturado da seguinte forma. Na Secção 2 são discutidos os requisitos subjacentes à concepção e desenvolvimento da plataforma SpotLight. Na Secção 3 é discutida a concepção e implementação do sistema. Na Secção 4 é feita uma primeira validação do sistema sendo apresentados e discutidos resultados de testes laboratoriais efectuados. Finalmente, na Secção 5, são apresentadas as principais conclusões do trabalho e indicadas algumas direcções para trabalho futuro.

2 Requisitos para o SpotLight

Nesta secção são analisados os requisitos subjacentes aos desenvolvimento da ferramenta SpotLight. Para além dos requisitos decorrentes da CIA *Triad* foram ainda considerados requisitos adicionais com vista à construção de uma solução mais robusta e versátil, adequada a ambientes empresarias.

2.1 Disponibilidade de Serviço

Manter a disponibilidade de serviço é um dos principais objectivos do SpotLight. Os ataques de *Denial of Service* (DoS) são cada vez mais vulgares e comuns na Internet, pela sua facilidade de execução e inúmeras maneiras de os realizar sem ser detectado. As organizações, com principal destaque para as que baseiam o seu negócio na prestação de serviços online, tendem a concentrar o seu sistema de defesa em torno de apenas esse serviço crítico. No entanto, devido ao crescimento do número de ataques externos a serviços online e à enorme variedade de métodos (em crescendo) para o concretizar, a tarefa defensiva não tem sido de fácil concretização para as equipas de segurança da organização.

2.2 Aprendizagem

O crescimento ascensional do número de ataques realizados na Internet prende-se com a mudança de mentalidade dentro da comunidade *hacker*. Actualmente, esta privilegia a partilha e discussão do conhecimento informático de um modo malicioso e leviano. Assim, o processo de descobrir e explorar vulnerabilidades é bastante mais rápido e eficaz, mesmo quando desenvolvido e executado por um principiante. Tal como na comunidade *hacker*, as equipas de segurança informática também se juntaram em comunidades cooperantes de modo a maximizar a sua capacidade de defesa, na partilha de conhecimento e de experiências passadas. Assim, estas equipas de segurança conseguem, quase em tempo real, ter conhecimento do que se passa em

várias organizações mundiais, protegendo-se atempadamente contra os respectivos ataques.

A aquisição de conhecimento e capacidade de aprendizagem de novas técnicas e métodos de ataque oriundos da comunidade *hacker* é um dos objectivos do SpotLight. Só assim, poderá existir uma capacidade de defesa semi-instantânea contra ataques ainda desconhecidos. O SpotLight terá que estar capacitado para adquirir todo o tipo de conhecimento possível, nomeadamente vulnerabilidades desconhecidas e novos métodos de ataque, de modo a esse mesmo conhecimento ser disponibilizado ás restantes comunidades de segurança informática, espalhadas pelo mundo inteiro, dando-lhes a oportunidade de se prepararem atempadamente.

2.3 Conhecimento das Fragilidades da Organização

A maior dificuldade das equipas de segurança na defesa das organizações é conhecer as reais vulnerabilidades do sistema que se prestam defender. Geralmente, têm apenas como principal objectivo a implementação de sistemas defensivos genéricos sem, na maioria das ocasiões, validar a sua real necessidade para o contexto em causa. Existem vários cenários negativos numa implementação deste tipo. Da mesma forma, é necessário estar completamente alerta perante o aparecimento, quase constante, de novas vulnerabilidades no mundo da informática. Ou seja, não basta conhecer detalhadamente as vulnerabilidades existentes na organização, é igualmente necessário, estar alerta e disposto a implementar um processo concreto de gestão de alertas sobre o aparecimento de novas vulnerabilidades no mundo da informática.

O SpotLight tem como objectivo coordenar e complementar um processo existente de gestão de vulnerabilidades na organização, no sentido de facilitar o conhecimento das existentes, tal como de alertar para o aparecimento de novas, na infra-estrutura. O SpotLight em coordenação com um processo interno de gestão de vulnerabilidades, irá aumentar a capacidade de alerta para novas vulnerabilidades tal como irá detalhar as vulnerabilidades existentes na organização, auxiliando e completando a análise interna de vulnerabilidades.

2.4 Recolha de Evidências

Actualmente, o processo de incriminação judicial de um *hacker* é extremamente complexo e demorado, acabando por vulgarmente serem abandonados por falta de provas. Na maioria das ocasiões não é possível recolher as evidências necessárias sobre a intrusão nem identificar a entidade responsável. O SpotLight tem como objectivo contrariar esta conjuntura actual, de certa forma impune, no processo de detecção, acusação e incriminação judicial. Propõe-se efectuar em primeiro um historial detalhado sobre qualquer tipo de evidência de intrusão ou tráfego malicioso sobre uma determinada organização. Terá de ser capaz de proteger eficazmente a “recolha de

evidências", dado que naturalmente esta passará a ser o alvo principal do *hacker* após a intrusão [VANGIE2005]. Em último terá de identificar formalmente, a identidade do autor directo da tentativa de intrusão ou tráfego malicioso.

O contributo do SpotLight, traduz-se na possibilidade de, para além de criar um historial sobre intrusões e os seus percursos numa dada organização para registo futuro, como também de justificar e validar uma acção judicial sobre o responsável ,mesmo que moralmente indirecto. Tal como na contexto militar, é fundamental saber quem é o inimigo, qual o tipo de estratégia de ataque, quais as ferramentas utilizadas e qual o seu objectivo. A recolha desta informação reveste-se de uma certa complexidade, mas de extrema importância. O conhecimento das estratégias de ataque possibilita o desenvolvimento e aperfeiçoamento das medidas preventivas, tal como da correcção das vulnerabilidades. A recolha do máximo de informação sobre o inimigo é um dos principais objectivos do *HoneyPot*.

3 Arquitectura do SpotLight

O SpotLight foi encarado desde inicio, e tal como nas tradicionais *HoneyNets*, como uma arquitectura conceptual (em prol) de um eventual produto ou solução tecnológica. Os seus objectivos baseiam-se numa suave integração entre os ideais e conceitos académicos de uma *HoneyNet*, onde a aprendizagem é um factor preponderante, com as exigências operacionais de negócio numa dada organização. Nesta, é preponderante e prioritário manter o negócio disponível de forma incondicional. Nesses termos, e de acordo com os objectivos propostos, o SpotLight apresenta duas abordagens distintas para a vertente externa:

- Componente de Aprendizagem: Terá que implementar as variáveis académicas de uma HoneyNet, aplicando as suas ferramentas internas para aprender e adquirir o máximo de conhecimento sobre as metodologias e ferramentas/técnicas da comunidade *hacker*;
- Componente de Negócio: Será responsável por garantir a integridade e continuidade de negócio na organização. Neste caso concreto, e como exemplo conceptual, terá que proteger a disponibilidade e integridade de um servidor WEB corporativo, assegurando a estabilidade e continuidade do modelo de negócio existente.

A estrutura idealizada para o SpotLight garante uma grau de flexibilidade bastante razoável, permitindo analisar, compreender e integrar as necessidades de negócio da organização na sua estrutura aplicacional. Do mesmo modo, e como objectivo de relevo, cumpre os requisitos académicos do conceito de *HoneyNet*, ao implementar mecanismos eficazes de monitorização e recolha de informação sobre o comportamento operacional (técnicas, ferramentas, abordagens, procedimentos de engenharia, etc.) da comunidade *hacker* actual.

3.1 Arquitectura

A arquitectura e estrutura aplicacional do SpotLight (ilustrada na Figura 1) foi desenvolvida com o intuito de ser suficientemente simples, dinâmica e extremamente versátil, de acordo com o ambiente que a rodeia, são estas as suas principais virtudes, na perspectiva de uma solução eficaz, na óptica de segurança versus aprendizagem. A ideia estrutural baseia-se em criar um ambiente simples, mas eficaz, onde seja possível reproduzir uma estrutura de rede corporativa, que disponibilize um servidor WEB para o exterior, como uma eventual forma de negócio para uma dada organização. Nesse sentido, cabe ao SpotLight proteger e retirar o máximo de informação de qualquer tipo de actividade maliciosa sobre o referido servidor corporativo [SUNDARAM1996]. Assim, e respeitando sempre os conceitos e ideais de uma *HoneyNet*, foi desenvolvida e implementada uma "camada adicional" que garante a integridade desses mesmo conceitos cumprindo as necessidades de negócio da organização, protegendo adequadamente a estrutura tecnológica que suporta o referido negócio, o servidor WEB corporativo.

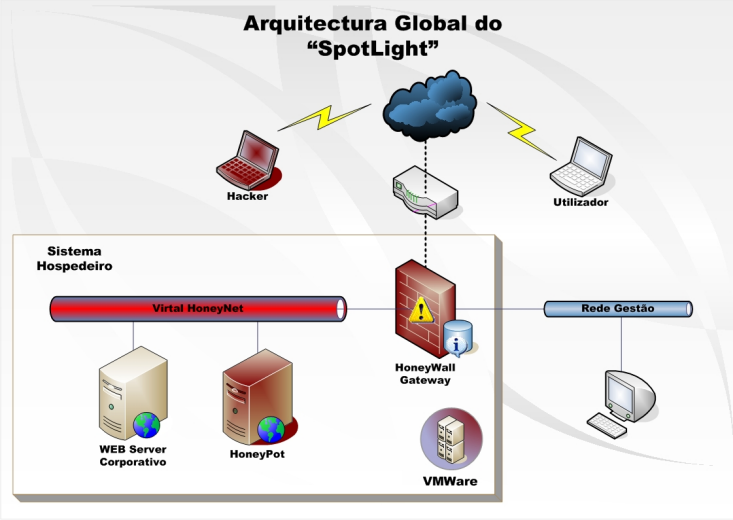

Figura 1. Arquitectura do SpotLight

Como suporte para uma estrutura dinâmica e versátil, o SpotLight baseia a sua estrutura aplicacional e tecnológica numa ferramenta de virtualização aplicacional de servidores – VMWare [VMWARE], a qual permite criar e gerir vários sistemas virtuais sobre um único sistema físico. Desse modo, e fazendo uso dos recursos físicos (espaço em disco, memória, processador, etc.) do sistema hospedeiro, partilha-os adequada e quantitativamente com os seus sistemas virtuais, implementando uma estrutura de processamento paralelo com vários sistemas operativos (o *HoneyPot*, servidor WEB e a *HoneyWall*), de uma forma completamente invisível para o utilizador final.

Como descrito anteriormente, o SpotLight terá a função de disponibilizar um servidor WEB corporativo, a fonte de negócio da organização para a Internet; tal como será igualmente responsável, por garantir a sua segurança e integridade em tempo real, no decorrer da sua "exposição natural" ao mundo inseguro da Internet. Na realidade, e em termos práticos, a *HoneyWall* terá que detectar e identificar actividade maliciosa destinada ao servidor WEB corporativo, redireccionando todo o tráfego suspeito directamente, e de um modo transparente, para o *HoneyPot*. Deste modo, ao retirar o sistema corporativo do "campo de visão" do *hacker*, e expondo apenas o *HoneyPot*, garante-se a integridade e disponibilidade do modelo de negócio assente sobre esse mesmo servidor corporativo. Da mesma forma, é viabilizado um modelo de aprendizagem sobre as eventuais fragilidades do sistema que suporta o negócio da organização, assim como, sobre o comportamento e metodologias (técnicas, ferramentas, conhecimentos, etc.) da comunidade *hacker* sem comprometer a segurança da organização.

3.1.1 Controlo e Captura de Dados

Tal como no modelo funcional das tradicionais *HoneyNets* Generation II [SPITZNER2005MAYGENII], os mecanismos de controlo e captura de dados do SpotLight encontram-se sediados no seu centro nevrálgico, a *HoneyWall*. A componente operacional do SpotLight responsável por controlar a actividade e o campo de acção do *hacker* está implementado, e integrado, internamente na *HoneyWall*. De acordo com a arquitectura proposta para o SpotLight, o mecanismo que garante a recolha, armazenamento e monitorização de informação referente à actividade maliciosa sobre o servidor WEB corporativo, está sediada no mesmo sistema que implementa o módulo funcional de controlo de acessos, a *HoneyWall*.

3.1.2 Virtualização de Servidores

A arquitectura do SpotLight está assente numa tecnologia de virtualização aplicacional de servidores - VMWare [VMWARE]. Foi baseado nessa mesma tecnologia que foi desenvolvida uma plataforma virtual de rede e servidores aplicacionais que definem o modelo organizacional definido por SpotLight. Como tal, passamos de um conceito genérico de *HoneyNet Generation II* para uma arquitectura aplicacional *Virtual HoneyNet* [SPITZNER2003JAN].

A Figura 2 ilustra a virtualização de servidores utilizada no sistema SpotLight. A ferramenta de virtualização aplicacional de servidores está inserida fisicamente num sistema hospedeiro, que irá disponibilizar recursos físicos para os sistemas virtuais integrados na arquitectura aplicacional do SpotLight. Ou seja, as três "máquinas virtuais", servidor WEB Corporativo, *HoneyPot* e *HoneyWall*, irão reservar um conjunto específico de recursos físicos do sistema hospedeiro, disponibilizando um desempenho considerável e completamente transparente para o mundo exterior. Não existe qualquer comunicação interna, sendo garantida uma segregação quase física do tráfego de dados (ao nível de rede) entre os sistemas virtuais e hospedeiro.

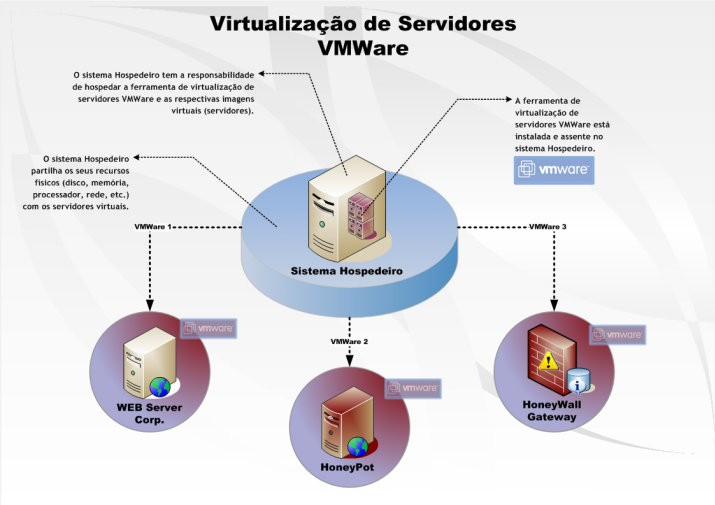

Figura 2. Tecnologia de Virtualização de Servidores (VMWare)

Em termos práticos, apenas existe uma partilha heterogénea e individualizada dos recursos físicos do sistema hospedeiro, onde os sistemas virtuais apenas conseguem, de uma forma abstracta, visualizar a sua percentagem de recursos como sendo intrinsecamente sua. Para além das vantagens inerentes à tecnologia de virtualização de servidores, o SpotLight associa a sua componente operacional à flexibilidade disponibiliza por este tipo de arquitectura aplicacional. Ou seja, é previsível que durante a actividade do SpotLight, o *HoneyPot* seja comprometido com alguma regularidade, sendo necessário garantir simplicidade, dinâmica e flexibilidade na operação/reposição desse mesmo sistema. Ao utilizar imagens virtuais (disponibilizadas pelo software VMWare), o HoneyPot ao ser comprometido, e no intuito de restabelecer rapidamente a actividade do SpotLight, basta "trocar" a imagem do sistema e reiniciar a solução como se nada tivesse acontecido, sendo a operação realizada com um *down-time* de poucos minutos [SPITZNER2003APRIL].

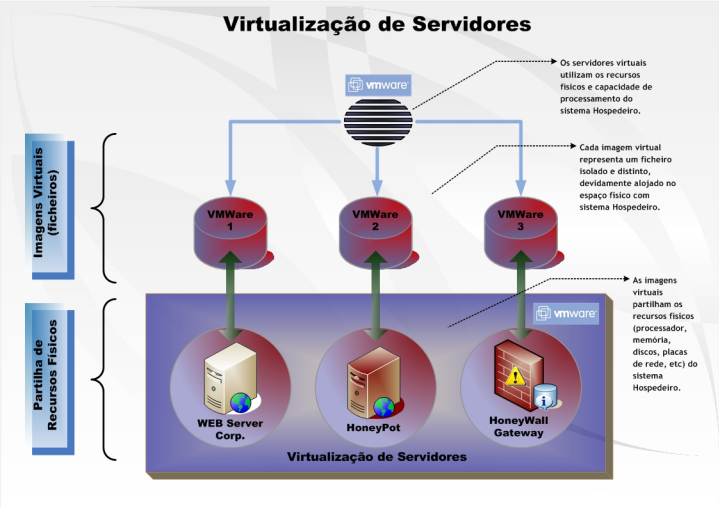

Figura 3. Virtualização dos servidores no SpotLight

O processo de atribuição de recursos do VMWare é considerado como sendo seguro, rigoroso e flexível, permitindo reservar previa e personalizadamente os recursos necessários para cada sistema virtual, assegurando o controlo sobre qualquer tentativa de alteração do modelo, inicialmente definido. Na realidade, e em termos operacionais, os sistemas virtuais não identificam, nem conseguem visualizar o sistema hospedeiro, apenas reservam e utilizam os seus recursos físicos "pensando-os" sendo como originalmente seus [SEIFRIED2002].

3.2 HoneyWall

A *HoneyWall* é o centro nevrálgico do SpotLight. Podemos considerá-la como o "cérebro" da arquitectura desenvolvida no âmbito deste projecto. A totalidade de processamento e análise de tráfego é da sua inteira responsabilidade. Na Figura 4 é ilustrada a *HoneyWall* utilizada no SpotLight.

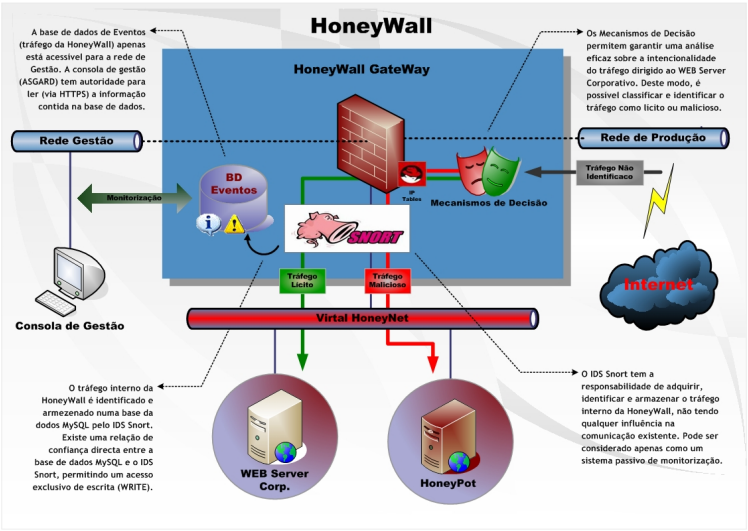

Figura 4. Subsistema HoneyWall

Numa primeira fase, foi necessário desenvolver mecanismos de análise e decisão sobre o tráfego direccionado ao SpotLight, focando especialmente a componente de dados destinada ao servidor WEB institucional. Numa segunda fase, e já com o conhecimento do objectivo real da comunicação (lícito ou ilícito/malicioso) sobre o sistema, foi necessário direccionar de uma forma coerente esse mesmo canal de comunicação para o sistema directamente associado: tráfego lícito para o servidor WEB institucional e tráfego malicioso para o *HoneyPot*. Finalmente, e após estabelecer os canais de comunicação apropriados, a *HoneyWall*, fazendo uso dos seus sistemas de detecção a Intrusão (IDS) passivos e reactivos, terá que identificar (via assinaturas e algoritmos comportamentais) quais os pacotes de tráfego existentes na rede, e qual a sua origem e destino atribuída internamente na infra-estrutura do SpotLight [SPITZNER2003APRIL]. Do mesmo modo, e para uma posterior análise e investigação a partir da rede de gestão, terá que armazenar e disponibilizar (via WEB) toda a informação recolhida durante os processos de análise, identificação e controlo de tráfego de dados.

3.2.1 Mecanismos de Decisão

A HoneyWall tem a responsabilidade de analisar, identificar e classificar o tráfego direccionado ao servidor WEB institucional consoante as intenções inerentes à comunicação oriunda do exterior. Ou seja, antes de permitir qualquer comunicação entre a Internet e o servidor institucional, a *HoneyWall* identifica e orienta o túnel de comunicação para o sistema directamente associado à categoria de tráfego existente, não permitindo qualquer tráfego malicioso ou ilícito para o servidor corporativo. Assim sendo, a implementação de mecanismos capazes de analisar detalhada e correctamente todo o tráfego existente no SpotLight, tornou-se o objectivo fundamental no decorrer da implementação deste projecto.

A *HoneyWall*, devido a um conjunto de mecanismos de detecção a intrusão e análise de tráfego, tem capacidade de "compreender" as reais intenções de um eventual *hacker* no decorrer da comunicação com o SpotLight, permitindo, de uma forma dinâmica, responder reactivamente aos eventuais ataques do exterior. Do mesmo modo, e para garantir a integridade e disponibilidade do sistema corporativo, a *HoneyWall* ainda implementa mecanismos internos (activos e passivos) de resposta a eventuais quebras de segurança no próprio SpotLight [BRAIN2000].

3.2.2 Encaminhamento de Pacotes

Após a correcta identificação das reais intenções do "utilizador externo", é necessário orientar o tráfego directamente para o servidor associado consoante os objectivos pretendidos, lícitos ou maliciosos. O tráfego identificado como malicioso é enviado para o HoneyPot, enquanto o tráfego lícito será entregue normalmente ao servidor corporativo. Foi assim, desenvolvido um mecanismo "inteligente", baseado no módulo original de controlo de acessos da plataforma Linux – IPTables com capacidade para controlar e coordenar tráfego (pacotes TCP/IP) consoante as regras de processamento pré-definidas nesse mesmo módulo aplicacional [RUSSEL1999]. Fazendo uso das funcionalidades de controlo de acessos e encaminhamento de pacotes do módulo de IPTables e após a correcta identificação de legitimidade do tráfego existente, é possível direccionar o tráfego para o sistema associado consoante as intenções, *HoneyPot* ou servidor WEB institucional.

3.2.3 Análise e Identificação de Tráfego

Na componente funcional, referente aos Mecanismos de Decisão do SpotLight, apenas é abordado a legitimidade do tráfego existente no decorrer da comunicação, onde serão processados alguns mecanismos operacionais de identificação dos objectivos da comunicação previamente estabelecida. A componente de Análise e Identificação de tráfego é precedida de uma análise bastante mais detalhada, onde o principal objectivo é classificar e correlacionar a estrutura do tráfego com eventuais ataques conhecidos, utilizando os modelos de identificação baseados em assinaturas e/ou algoritmos comportamentais [PTACEK1998]. No caso concreto do SpotLight, foi integrado o "conhecido" sistema de Detecção a Intrusão - Snort [SNORT], dada a sua elevada capacidade de identificar e classificar pacotes de tráfego baseados em assinaturas de padrões de ataques conhecidos, no decorrer da comunicação com o servidor corporativo.

3.2.4 Armazenamento e Historial

Um dos seus principais objectivos do SpotLight é adquirir e armazenar o máximo de informação referente às actividades e metodologias utilizadas actualmente pela comunidade *hacker*. Como tal, a componente funcional responsável por adquirir (*logging*) e armazenar a informação referente ao tráfego existente no SpotLight, está directamente associada à *HoneyWall*. Utilizando as capacidade de *sniffing*, identificação de assinaturas e flexibilidade aplicacional do Snort, é possível armazenar a informação recolhida numa base de dados local. Ou seja, a HoneyWall utiliza o Snort como ferramenta da aquisição e classificação de tráfego, e de um modo automatizado, armazena essa mesma informação numa base de dados de eventos - MySQL. O poste-

rior estudo e análise sobre a informação referente às metodologias utilizadas pela comunidade *hacker*, devidamente armazenada na HoneyWall, é realizado sobre um acesso HTTP personalizado, com credenciais de acesso específicas sobre essa mesma base de dados de informação. Da mesma forma, e no intuito de aumentar a segurança no controlo de acessos à informação e à própria *HoneyWall*, apenas é permitido o acesso autorizado a partir de um único sistema da arquitectura do SpotLight – a Consola de Gestão.

4 Avaliação

O SpotLight foi desenvolvido na perspectiva de, numa fase experimental, simular e avaliar as capacidades e performance da arquitectura aplicacional e funcional desenvolvida para o efeito num suposto "mundo real". Nesse sentido, foi implementado um laboratório capaz, de num primeiro período de análise, simular as necessidades corporativas de uma qualquer organização, e numa perspectiva de análise e avaliação da própria solução, fosse capaz de reproduzir as ameaças aplicacionais e tecnológicas existentes no mundo da Internet actual. O piloto (ou laboratório) disponibilizou um servidor corporativo WEB "fictício" sobre um ambiente aplicacional abrangente no intuito de testar e avaliar as capacidades de defesa e reacção do SpotLight evidenciadas no decorrer deste projecto. Os objectivos passavam por garantir uma exposição declarada e inequívoca de um conjunto de serviços aplicacionais, vulgarmente reconhecidos e identificados pelas suas vulnerabilidades aplicacionais, na expectativa de ser imediatamente reconhecido, proporcionando uma atenção adicional sobre a comunidade *hacker*, permitindo analisar e validar a totalidade das capacidades do SpotLight.

Para garantir uma análise detalhada e credível da capacidade de reacção do SpotLight, o piloto desenvolvido e implementado ao abrigo deste projecto, apresentou duas vertentes distintas de investigação: uma abordagem de ataque orientada para um contexto controlado, e numa vertente mais realística, uma abordagem onde não existe qualquer tipo de orientação técnica ou controlo no decorrer das iniciativas maliciosas. A investigação realizada sobre a abordagem controlada teve como objectivo analisar efectivamente a resposta reactiva por parte do SpotLight perante um conjunto específico de ataques conhecidos na Internet. Por outro lado, a exposição do SpotLight ao mundo "real" da Internet deveu-se essencialmente a testar as suas capacidades de resposta perante a realidade existente actualmente em termos de iniciativas maliciosas das comunidades *hacker*.

Apesar do SpotLight ter sido devidamente testado e avaliado num ambiente de laboratório que, reflectia um contexto aplicacional e tecnológico bastante próximo do real, foi necessário validar o seu comportamento em ambientes com maior índices de exigência e realismo. Nesse sentido, e promovendo um piloto que garantisse um acesso directo às ameaças e metodologias da comunidade *hacker* actual, o SpotLight foi exposto directamente na Internet. No decorrer de ambas as fases de piloto, laboratório e em real, foram registados inúmeros ataques direccionados ao sistema corporativo, permitindo uma análise detalhada da realidade actual da Internet, e da performance e

viabilidade da própria solução desenvolvida no âmbito deste projecto - SpotLight. O entendimento do contexto operacional implementado no decorrer da fase de piloto, foi definido em duas vertentes distintas: ataques controlados, e ataques não-controlados, onde a variável de controlo está associada directamente aos testes realizados em ambiente de laboratório. Em contrapartida, e no decorrer da exposição do SpotLight à Internet, os ataques não-controlados foram classificados como o conjunto de actividades maliciosas com origem na Internet. Numa perspectiva operacional, ambas as vertentes têm igual significado para a arquitectura do SpotLight, sendo os ataques processados de igual forma, como se tratassem de ataques maliciosos com o mesmo nível de gravidade ou ameaça para a infra-estrutura tecnológica em causa. No entanto, e numa óptica de investigação e desenvolvimento, o ambiente de laboratório foi bastante útil na concepção e aperfeiçoamento das funcionalidades do SpotLight, permitindo testar um conjunto de ataques previamente definidos e estabelecidos perante uma determinada sequência e pressupostos aplicacionais.

4.1 Disponibilidade de Serviço

A garantia da disponibilidade de serviço foi, desde a sua concepção, considerado como um dos principais objectivos do SpotLight. Os ataques de *Denial of Service* (DoS) são considerados como dos ataques com maior índice de impacto na disponibilidade de serviço nas plataformas tecnológicas. Este género de ataques, devido à ameaça que representam sobre a disponibilidade de serviços das organizações, e pela vulgaridade e facilidade com que são executados na Internet, torna preponderante desenvolver mecanismos que consigam, numa fase prévia, detectá-los em tempo útil, e como reacção imediata, serem capazes de implementar "barreiras" eficazes que garantam a integridade e disponibilidade da organização.

Como seria de esperar, e de acordo com o estado actual dos ISPs nacionais, foi de realçar a dimensão exagerada do número de ataques automatizados e sistematizados por gamas de endereçamento IP na rede interna do fornecedor. Este tipo de ataques devem-se na sua maioria, ao número elevado de sistemas vulneráveis e infectados com *worms*, que por serem aplicacionalmente auto-replicáveis, tentam de forma automatizada e aleatória pela rede, replicarem-se por outros sistemas vulneráveis na Internet. Da mesma forma, e apesar de se tratar de uma fase prévia ao ataque directo, foi também detectado um conjunto bastante alargado de ferramentas de *scanning*, que de uma forma automatizada, pesquisam por sistemas vulneráveis a determinadas falhas de segurança (vulnerabilidades), no intuito de posteriormente avançarem com ataques e tentativas de intrusão baseados nesse conjunto de vulnerabilidades específicas.

Após analisar os resultados práticos do SpotLight perante uma exposição directa sobre a Internet, sujeito a uma enorme variedade e dimensão de ataques sucessivos no decorrer do piloto, foi possível concluir que o objectivo da garantia da disponibilidade de serviço, devidamente suportada sobre os módulos funcionais de identificação de tráfego e respectivos mecanismos de decisão, foi cumprido na sua totalidade, com

uma prestação extremamente positiva considerando as soluções alternativas do mercado actual. Este resultado, deve-se essencialmente, à capacidade e performance associada ao modelo funcional de Mecanismos de Decisão no processo de recepção de pedidos de comunicação da Internet. Este módulo, estabelece a decisão "estratégica" de qual será a intenção objectiva da comunicação estabelecida, e qual o destino final do tráfego dirigido ao SpotLight. A sua prestação é devida essencialmente à simplicidade aplicada sobre o modelo funcional, permitindo estabelecer um tempo de resposta no processamento de dados razoável, com um índice de falsos positivos bastante reduzido no decorrer do processo de identificação da legitimidade do tráfego.

4.2 Aprendizagem

Tal como estabelecido inicialmente, e de acordo com o conjunto de objectivos propostos, o SpotLight tem como um dos seus maiores objectivos a implementação de mecanismos e procedimentos funcionais que garantam uma capacidade eficaz de aprendizagem sobre, numa primeira fase, as metodologias em vigor na comunidade *hacker* actual, e posteriormente, sobre o aparecimento e modo de exploração de novas vulnerabilidades nos sistemas críticos das organizações.

O SpotLight, aplicando o seu módulo de captação de pacotes de tráfego (sniffing), devidamente correlacionado com assinaturas de ataques conhecidos foi, no decorrer deste piloto, capaz de reconhecer e identificar inúmeras tentativas de intrusão oriundas directamente da Internet. A informação recolhida pelo módulo de *sniffing*, e à medida que foram sendo publicadas novas vulnerabilidades, na sua grande maioria pelo fabricante Microsoft, foi notório que no espaço de dias houve uma alteração substancial no comportamento da Internet com o SpotLight, tendo sido evidenciado e reportado várias tentativas de *scanning* e/ou exploração sobre portos específicos e associados às novas vulnerabilidades. Na realidade, para além de ter sido possível analisar e conhecer o método de exploração, e respectiva tentativa de intrusão, sobre um determinado conjunto de novas vulnerabilidades, o SpotLight acabou por funcionar como um barómetro comportamental da comunidade *hacker*, detectando as alterações comportamentais da comunidade à medida que as novas vulnerabilidades iam sendo tornadas públicas na Internet.

De uma forma resumida, o SpotLight apresentou duas vertentes de aprendizagem distintas: numa perspectiva mais técnica foi capaz de garantir a aquisição de informação relativa aos métodos e técnicas utilizadas pela comunidade *hacker* para explorar vulnerabilidades específicas, e numa perspectiva mais abrangente e comunitária, possibilitou a integração de uma funcionalidade de alerta e análise comportamental sobre a comunidade *hacker*, permitindo perceber antecipadamente qual a orientação estratégica da grande maioria dos ataques oriundos da Internet, estando directamente relacionados com a publicação de novas vulnerabilidades. Com a concretização deste objectivo, e de uma forma potencialmente comunitária, é de esperar e recomendável que num futuro próximo, que o SpotLight partilhe toda a informação angariada no

decorrer da sua actividade pelas restantes comunidades de segurança informática espalhadas pela Internet, possibilitando-lhes uma oportunidade adicional de se prepararem antecipadamente para o esperado ataque "*day zero*".

4.3 Conhecimento das Fragilidades do Sistema Corporativo

Na perspectiva da organização, o sistema corporativo é, sem margem de dúvida, o seu bem mais valioso, e sobre o qual é necessário aplicar o maior esforço na implementação das medidas de segurança que correspondam à garantia da integridade e estabilidade dos serviços e recursos corporativos associados ao referido sistema. Para tal, é fundamental analisar detalhadamente a especificidade e características técnicas dos serviços corporativos expostos para a Internet, evitando uma vertente mais genérica e demasiado abrangente na perspectiva de proteger toda a infra-estrutura tecnológica de igual forma sem considerar as funcionalidades e criticidade dos recursos envolvidos. O SpotLight tem como objectivo operacional permitir às equipas de segurança um nível superior de conhecimento sobre o estado geral da organização que se pretende defender, nomeadamente na informação relativa às vulnerabilidades existentes, na sua plataforma corporativa, facilitando e complementando o processo de implementação de segurança na organização. Paralelamente, e tal como referido anteriormente, o SpotLight ao estar "atento" ao aparecimento de novas vulnerabilidades no mundo da segurança informática, permite analisar quais destas vulnerabilidades poderão afectar os sistemas corporativos em vigor na organização, promovendo medidas preventivas e, eventualmente reactivas na correcção dessas mesmas vulnerabilidades.

No decorrer do piloto realizado com o SpotLight, e fazendo uso das funcionalidades de aprendizagem da solução desenvolvida, foi possível compreender de uma forma quase imediata, quais as vulnerabilidades existentes no sistema corporativo utilizado consideradas como mais emergentes e "apetecíveis" para a comunidade *hacker*. O facto do *HoneyPot* ser uma réplica exacta do servidor WEB corporativo, permitiu analisar ao detalhe quais as vulnerabilidades que foram sendo pesquisadas e posteriormente exploradas pelos *hackers*, e qual o impacto traduzido a nível interno sobre a infra-estrutura e, respectivo negócio da organização. O SpotLight, ao direccionar todo tráfego identificado como malicioso para o *HoneyPot*, garantiu em primeiro lugar a integridade do sistema corporativo, e simultaneamente, permitiu analisar e investigar em tempo real as variadas interacções da comunidade *hacker* sobre os serviços corporativos disponibilizados pelo HoneyPot (réplica do servidor WEB institucional). No decorrer do piloto, e consoante as várias tentativas de exploração e intrusão a partir da Internet, foi possível detectar o conjunto de falhas de segurança existentes no HoneyPot, e por associação, no próprio sistema corporativo. Ou seja, durante o piloto, o HoneyPot foi comprometido por várias ocasiões e de diversas formas, tendo sido explorado um conjunto bastante alargado de vulnerabilidades de segurança. No decorrer deste processo, apesar de terem sido detectadas algumas vulnerabilidades amplamente conhecidas no mundo da segurança informática, foram descobertas algumas possíveis e eventuais falhas de segurança, que para além de não serem ainda reconhecidas, poderão vir tornar-se ameaças graves num futuro próximo. Sendo o HoneyPot

uma réplica do sistema corporativo, foi possível adquirir o conhecimento detalhado de quais as falhas de segurança a que o sistema estaria sujeito, possibilitando implementar de forma urgente e, se possível, imediata, as devidas correcções ou medidas de segurança de modo a manter a integridade do sistema e dos serviços corporativos associados.

No intuito de expor o SpotLight directamente a uma exposição o mais intensa possível na Internet, foi considerado como prioritário para o projecto, aproximar a solução, ainda em versão académica, a um ambiente supostamente próximo do real. Para tal, e aumentado o "realismo" pretendido para o piloto, foi utilizado um sistema corporativo com falhas de segurança graves e extremamente "apetecíveis" para a grande maioria dos *hackers* (incluindo iniciantes). Como prova dessa abordagem, foi impressionante a rapidez na qual todas as vulnerabilidades foram reconhecidas, identificadas, e imediatamente exploradas, comprometendo a integridade do sistema em causa, o HoneyPot. Tendo o piloto durado alguns meses, bastou um espaço temporal de dias, para que o conjunto de vulnerabilidades disponibilizadas no SpotLight, desde logo identificadas, fossem exploradas e comprometidas na sua totalidade. Este facto, e numa perspectiva mais realística ou operacional com uma análise sobre a intrusão do HoneyPot, teria permitido, em caso de desconhecimento, estabelecer procedimentos imediatos e reactivos de correcção do sistema corporativo numa eventual organização.

4.4 Recolha de Evidências

Actualmente, e de acordo com a publicidade existente sobre os vários incidentes de segurança exercidos pelo mundo fora sem qualquer punição, tem sido notório a dificuldade em consolidar efectivamente uma acusação sólida e devidamente fundamentada sobre a comunidade *hacker*. Tipicamente, e devido a cenários tecnológicos extremamente voláteis e de enorme complexidade para a maioria das entidades reguladoras e/ou policiais, o processo judicial acaba por ser abandonado por falta de evidências ou provas concretas que consolidem uma acusação formal sobre um determinado indivíduo.

No decorrer do piloto e respectiva exposição à Internet, a base de dados de informação do SpotLight foi crescendo exponencialmente, permitindo analisar ao detalhe todo o percurso de um determinado *hacker* durante e após a tentativa de intrusão, adquirindo um conhecimento extremamente válido para uma posterior investigação técnica e/ou judicial do respectivo ataque. Tendo como base de suporte este conjunto de dados de informação, e o valor atribuído à vertente académica, é possível desencadear um processo de acusação formal com registos sólidos e comprovados das iniciativas maliciosas da comunidade *hacker* sobre uma determinada organização. Na realidade, e mais uma vez durante a experiência desenvolvida, houve oportunidade de enumerar e identificar um conjunto bastante extenso, e de grande dimensão, de eventuais *hackers*, com registos evidentes e detalhados dos ataques destinados e concretizados sobre o HoneyPot.

No entanto, e como tem sido comum no decorrer das iniciativas da comunidade *hacker*, muitos dos eventuais atacantes, foram identificados como possíveis "terceiras entidades" ou *zombies*, que estariam infectados com algum *worm* ou vírus que estaria a originar autónoma e massivamente ataques aleatórios sobre determinadas gamas de endereçamento na rede pública. Tal como definido inicialmente nos objectivos propostos para o SpotLight, apenas era suposto identificar o primeiro nível da cadeia de ataque, excluindo por inerência situações deste género, onde apenas estamos a identificar entidades adicionais que podem ser consideradas igualmente vítimas de ataques anteriores, e de responsabilidade, de *hackers*. Ainda que se encontrem na situação de vítimas estão, ainda que involuntariamente, a desenvolver ataques perigosos e com impacto pela Internet, sendo legitimo para qualquer organização, identificá-los como "agressores", activando de imediato os seus mecanismos de defesa e identificação (para promover posteriormente uma análise técnica e judicial) dos responsáveis originais dessa iniciativa. Eventualmente, após uma análise detalhada e exaustiva sobre a terceira entidade, identificada como a origem do ataque à organização, é possível detectar qual o *hacker* que o terá utilizado como fonte de ataque. No caso de existir um ataque directo de um *hacker*, sem a participação de uma terceira entidade, será possível identificar directa e exclusivamente o prevaricador em questão, permitindo estabelecer um processo formal de acusação judicial sobre o verdadeiro atacante.

No decorrer do piloto, foi evidente o contributo do SpotLight para a identificação de muitos dos elementos da comunidade *hacker* actual. Tornou-se possível criar um historial exaustivo sobre as intrusões e os seus percursos técnicos até ao comprometimento de uma dada organização. Tendo como suporte o conjunto de informação recolhida no decorrer da sua actividade, foi comprovado a sua capacidade em justificar e validar uma acção judicial concertada com registos adicionais de outras entidades, sobre os responsáveis por ataques directos sobre uma dada organização, mesmo que moralmente involuntários.

4.5 Resultados

O entendimento do contexto operacional implementado no decorrer da fase de piloto, foi definido em duas vertentes distintas: ataques controlados, e ataques não-controlados, onde a variável de controlo está associada directamente aos testes realizados em ambiente de laboratório. Em contrapartida, e no decorrer da exposição do SpotLight à Internet, os ataques não-controlados foram classificados como o conjunto de actividades maliciosas com origem na Internet. Numa perspectiva operacional, ambas as vertentes têm igual significado para a arquitectura do SpotLight, sendo os ataques processados de igual forma, como se tratassem de ataques maliciosos com o mesmo nível de gravidade ou ameaça para a infra-estrutura tecnológica em causa. No entanto, e numa óptica de investigação e desenvolvimento, o ambiente de laboratório foi bastante útil na concepção e aperfeiçoamento das funcionalidades do SpotLight,

permitindo testar um conjunto de ataques previamente definidos e estabelecidos perante uma determinada sequência e pressupostos aplicacionais.

A análise e classificação das actividades maliciosas detectadas no decorrer do piloto do SpotLight, foram categorizados em três categorias distintas de ataques informáticos:

- Ataques de Reconhecimento: *Hacker*s tentam descobrir os sistemas e recolher o máximo de informação disponível sobre uma dada organização. Geralmente, este tipo de ataques são utilizados para adquirir o máximo de conhecimento possível sobre a infra-estrutura, de modo a suportar um ataque posterior de acesso ou Denial of Service - DoS (exemplo: *portscan*, *fingerprint*).
- Ataques de Acesso: Este tipo de ataques tenta ganhar acesso não-autorizado a um dado sistema de modo a obter informação específica (exemplo: ganhar acesso às *passwords* do sistema, escalar privilégios, executar um *exploit*).
- Ataques DoS: *Hacker*s utilizam este tipo de ataques com o objectivo de corromper o acesso ou disponibilidade de serviços, sistemas ou redes. Ou seja, o intuito é unicamente de negar o acesso a utilizadores devidamente credenciados a estes recursos.

Em resumo, e na intenção de analisar o estado actual do mundo da Internet, o SpotLight funcionou como barómetro comportamental da comunidade *hacker*. No decorrer do piloto, com exposição directa do SpotLight na Internet, foi possível enumerar e analisar o conjunto de actividades maliciosas ocorridas no período de exposição (cerca de três meses) do SpotLight à realidade da mundo virtual da Internet (Figura 5).

Figura 5. Análise dos Ataques ocorridos durante o Piloto

4.5.1 Ataques de Reconhecimento

Como seria expectável, durante o período de exposição à Internet, o SpotLight foi alvo de uma quantidade enorme de ataques de reconhecimento, onde uma percentagem acentuada se devia a ataques automatizados espalhados pela Internet.

ATAQUES DE RECONHECIMENTO				
Ataque	**Período**	**Tentativas**	**Origens**	**Tipo de Ataque**
PortScan	3 meses	439	214	Não-Controlado
	N/A	78	1	Controlado
FingerPrint	3 meses	321	211	Não-Controlado
	N/A	78	1	Controlado
PortTool - Microsoft Windows NT 4.0 / 2000 Predictable LPC Message Identifier Multiple Vulnerabilities	N/A	1	1	Controlado

4.5.2 Ataques de Acesso

No decorrer do piloto, foi possível comprovar esta teoria, tendo sido detectados um número substancial de execução de "*buffer overflows*" na tentativa de acesso malicioso sobre o sistema corporativo. Da mesma forma, foi notório a relação directa entre a frequência de ataques e a publicação periódica das vulnerabilidades associadas às aplicações activas no servidor corporativo, nomeadamente o servidor WEB – Microsoft IIS, e o serviço RPC.

ATAQUES DE ACESSO (*buffer overflow*)				
Vulnerabilidade	**Período**	**Tentativas**	**Origens**	**Tipo de Ataque**
MS Windows RPCSS Multi-thread Race Condition Vulnerability	N/A	1	1	Controlado
MS RPCSS DCOM Interface Long Filename Heap Corruption Vulnerability	N/A	3	1	Controlado
MS Windows Workstation Service Remote Buffer Overflow Vulnerability	N/A	1	1	Controlado
Microsoft Windows Locator Service Buffer Overflow Vulnerability	3 meses	24	10	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows Server Message Block Handlers Remote Buffer Overflow Vulnerability	N/A	1	1	Controlado
Microsoft IIS Executable File Parsing Vulnerability	3 meses	45	19	Não-Controlado
	N/A	1	1	Controlado
Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability	N/A	1	1	Controlado
Microsoft Internet Explorer Content Advisor File Handling Buffer Overflow Vulnerability	N/A	1	1	Controlado
Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability	N/A	1	1	Controlado
Microsoft Windows Media Services NSIISlog.DLL Remote Buffer Overflow Vulnerability	N/A	1	1	Controlado

4.5.3 Ataques de *Denial-of-Service*

No decorrer do piloto, foi uma vez mais notório, a relação directa entre a publicação de novas vulnerabilidades, e respectivos *worms*, com o número de incidências de ataques *DoS* sobre o sistema corporativo. A maioria dos ataques direccionados ao SpotLight referem-se, na sua grande maioria, a ataques de worms, nomeadamente o Blaster e Sasser que continuam a "imperar" na Internet.

ATAQUES DE DENIAL of SERVICE (*buffer overflow*)				
Vulnerabilidade	**Período**	**Tentativas**	**Origens**	**Tipo de Ataque**
Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability	3 meses	21	8	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows RPC Service Denial of Service Vulnerability	3 meses	21	8	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows Messenger Service Buffer Overrun Vulnerability	N/A	1	1	Controlado
Microsoft Windows ASN.1 Library Bit String Processing Integer Handling Vulnerability	N/A	1	1	Controlado
Microsoft Windows RPC Service Denial of Service Vulnerability	3 meses	12	8	Não-Controlado
	N/A	1	1	Controlado
Microsoft IIS Unspecified Remote Denial Of Service Vulnerability	N/A	1	1	Controlado
Microsoft IIS WebDAV Denial of Service Vulnerability	N/A	1	1	Controlado
Microsoft XML Parser Remote Denial of Service Vulnerability	N/A	1	1	Controlado

ATAQUES DE DENIAL OF SERVICE (*worms*)				
Vulnerabilidade	**Período**	**Tentativas**	**Origens**	**Tipo de Ataque**
W32.Blaster.Worm - Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	3 meses	361	210	Não-Controlado
	N/A	6	1	Controlado
W32.Sasser.Worm - Microsoft Windows LSASS Buffer Overrun Vulnerability	3 meses	172	39	Não-Controlado
	N/A	1	1	Controlado
Microsoft Windows RPC Service Denial of Service Vulnerability	3 meses	72	34	Não-Controlado
	N/A	1	1	Controlado
W32.CodeBlue.Worm - Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability	3 meses	23	12	Não-Controlado
	N/A	1	1	Controlado

4.6 Avaliação geral

Em termos de objectivos propostos, o SpotLight está associado a quatro desafios tecnológicos: garantia da disponibilidade de serviço dos recursos críticos da organização, promover a aprendizagem sobre as novas metodologias da comunidade *hacker*, descobrir as vulnerabilidades e falhas de segurança do sistema corporativo, e finalmente, a capacidade de angariar e armazenar evidências de eventuais incidentes de segurança. Na Figura 6 é ilustrada o cumprimento dos objectivos inicialmente definidos pelo SpotLight.

Numa análise superficial, foi evidente que o SpotLight cumpriu, e para além das expectativas iniciais, os objectivos originalmente estabelecidos no âmbito deste projecto. Adicionalmente, é notório como a abordagem apresentada pelo SpotLight, com destaque à sua capacidade de garantia de disponibilidade de serviço e dinâmica na

resposta a ataques externos, veio modificar alguns dos conceitos mais tradicionais do mundo dos sistemas de informação na componente de segurança informática.

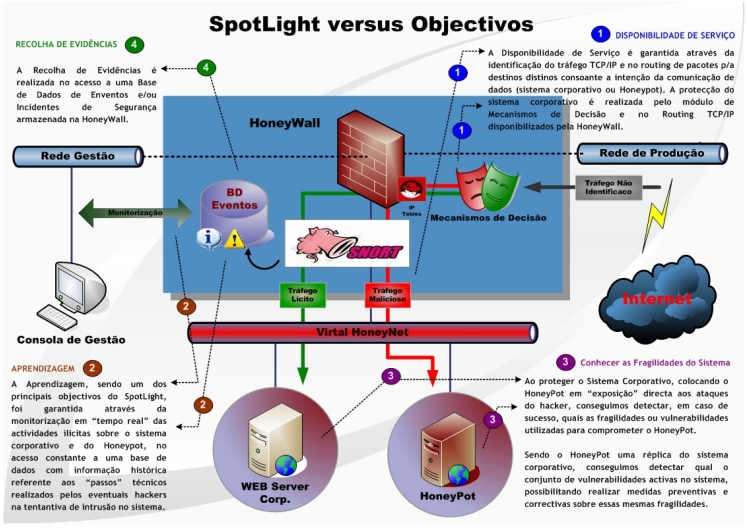

Figura 6. Cumprimento dos objectivos pelo SpotLight

5 Conclusões

As conclusões sobre os resultados obtidos, e a respectiva análise da performance funcional e operacional do próprio SpotLight, foram baseados nas interacções existentes no decorrer do piloto numa janela temporal de dois meses. O projecto SpotLight, apesar de se tratar de um desafio de âmbito bem definido, e conceptualmente estruturado de acordo com o conjunto de objectivos propostos inicialmente, foi particularmente ambicioso ao desenvolver mecanismos que garantissem as necessidades corporativas, e pacificamente, conseguissem manter as métricas académicas. Da mesma forma, e numa perspectiva de futuro, foi igualmente desafiador estabelecer procedimentos operacionais e funcionais que garantissem a estabilidade e integridade da própria solução sem, obviamente, defraudar ou condicionar o cumprimento dos objectivos originalmente propostos.

Desde logo, e numa óptica de inovação sobre o estado actual do mundo da segurança informática, o SpotLight pretendeu adicionar e integrar conceitos tecnológicos e organizacionais completamente distintos, orientados numa abordagem inovadora perante um cenário hostil considerado ainda como "desconhecido". Esta abordagem foi, desde logo, idealizada com o objectivo de se tornar inovadora para a comunidade, mas que fosse um registo bastante válido da sua eficácia perante uma interacção com ambientes hostis, evitando tender para as vertentes mais tradicionais e, simplistas, de criar estruturas de defesa rígidas e pouco "inteligentes" obcecadas exclusivamente

com a componente defensiva na resposta a um comportamento malicioso ainda "desconhecido". Ao ser capaz de responder eficazmente a um conjunto bastante abrangente de ameaças ainda "desconhecidas" baseando-se em conceitos académicos consolidados (nomeadamente os da CIA Triad e *HoneyNet*), e estando em completa sintonia com as exigências e necessidades das organizações actuais, o SpotLight veio trazer alguma inovação na comunidade de segurança dos nossos dias. Adicionalmente, a sua capacidade de integração pacifica com uma infra-estrutura tecnológica já em completa fase de produção, e sua disponibilidade de abranger variadas tecnologias ou serviços corporativos foi, desde logo, um factor crítico de sucesso para o *road-map* de evolução da solução, ainda em fase de investigação e consolidação, SpotLight.

Em termos conceptuais, e tal como referido, a estratégia de evolução do SpotLight passa por implementar e garantir as métricas de segurança lógica descritas anteriormente (confidencialidade, integridade e disponibilidade) através de mecanismos funcionais baseados num modelo de segurança reconhecido na área; Prevenção, Detecção e Resposta. Para além da sua fácil e flexível capacidade de integração em qualquer infra-estrutura tecnológica, é também responsável por estabelecer e implementar procedimentos preventivos de manutenção da segurança, correlacionados com mecanismos eficazes de detecção e resposta a incidentes de segurança, permitindo estruturar um sistema global seguro e eficaz perante ambientes hostis, sujeitos a ameaças conhecidas e/ou desconhecidas.

Durante o período de actividade do SpotLight, com destaque na experiência obtida a partir do piloto, e apesar de ter em consideração os resultados satisfatórios obtidos, foi notória a necessidade emergente em evoluir conceptual e funcionalmente a arquitectura inicialmente concebida para esta solução. Nesse sentido, e tendo como base esta análise experimental, podemos concluir que o processo de evolução do SpotLight passa, numa primeira fase, por optimizar o módulo referente aos Mecanismos de Decisão que têm sobre si a responsabilidade de identificar e classificar o tráfego direccionado ao sistema corporativo. É prioritário garantir a diminuição, e se possível, a eliminação dos falsos-positivos ainda existentes. Paralelamente, e para conseguir uma integração completa do SpotLight com a rede interna da organização, será adicionado e integrado dinamicamente todo o endereçamento interno disponível na arquitectura do SpotLight, garantindo um controlo e monitorização da totalidade da rede interna.

Outra questão a ser analisada num futuro próximo, prende-se com a salvaguarda do bem mais valioso do SpotLight e das organizações que se pretendem proteger, a informação recolhida no decorrer das iniciativas maliciosas da comunidade *hacker* sobre a organização. Nesse sentido, é importante adicionar um sistema dedicado exclusivamente ao armazenamento de informação, garantindo a integridade e redundância de informação no decorrer da actividade do SpotLight.

Referências

[RISK MNAGEMENT] Wikipedia, “Risk Management”,
http://en.wikipedia.org/wiki/Risk_management

[CIA TRIAD] Wikipedia, “CIA Triad refers to the mnemonic CIA; Confidentiality, Integrity and Availability”,
http://en.wikipedia.org/wiki/CIA_triad

[SPITZNER2003MAY] Lance Spitzner, "Honeypots - Definitions and Value of Honeypots”,
http://www.honeynet.org/papers/honeypot/

[SEIFRIED2002] Kurt Seifried, "Honeypotting with VMware - basics”,
http://www.seifried.org/security/ids/20020107-honeypot-vmware-basics.html

[RUSSEL1999] Rusty Russell, "Linux iptables HOWTO”,
http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html

[BRAIN2000] Brain Laing, "HowTo Guide-Implementing a Network Based Intrusion Detection System",
http://www.snort.org/docs/iss-placement.pdf

[PTACEK1998] Thomas H. Ptacek, Timothy N. Newsham , "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection",
http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html

[SNORT] http://www.snort.org/

[SPITZNER2005]
Lance Spitzner, "Honeynets - What a honeynet is, its value, and risk/issues involved."
http://www.honeynet.org/papers/honeynet/

[VANGIE2005]
Vangie Beal, "Intrusion Detection and Prevention - All About IPS & IDS"
http://www.webopedia.com/DidYouKnow/Computer_Science/2005/intrusion_detection_prevention.asp

[BOBBITT2002]
Mike Bobbitt, "Inhospitable Hosts"
http://infosecuritymag.techtarget.com/2002/oct/cover.shtml

[SUNDARAM1996]
Aurobindo Sundaram, "An Introduction to Intrusion Detection"
http://www.acm.org/crossroads/xrds2-4/intrus.html

[SPITZNER2003APRIL]
Lance Spitzner, "Honeypots: Simple, Cost-Effective Detection"
http://www.securityfocus.com/infocus/1690

[SPITZNER2005MAYGENI]
Lance Spitzner, "Know Your Enemy: Honeynets"
http://www.honeynet.org/papers/honeynet/index.html

[SPITZNER2005MAYGENII]
Lance Spitzner, "Know Your Enemy: GenII Honeynets"
http://www.honeynet.org/papers/gen2/index.html

[SPITZNER2003JAN]
Lance Spitzner, "Know Your Enemy: Defining Virtual Honeynets"
http://www.honeynet.org/papers/virtual/index.html

[VMWARE]
http://www.vmware.com/