Segurança em Redes de Computadores: Ameaças, Vulnerabilidades e Ataques.

William Sousa, Manuel Maciel, and Rui Santos

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a61029,a68410,a67656}@alunos.uminho.pt

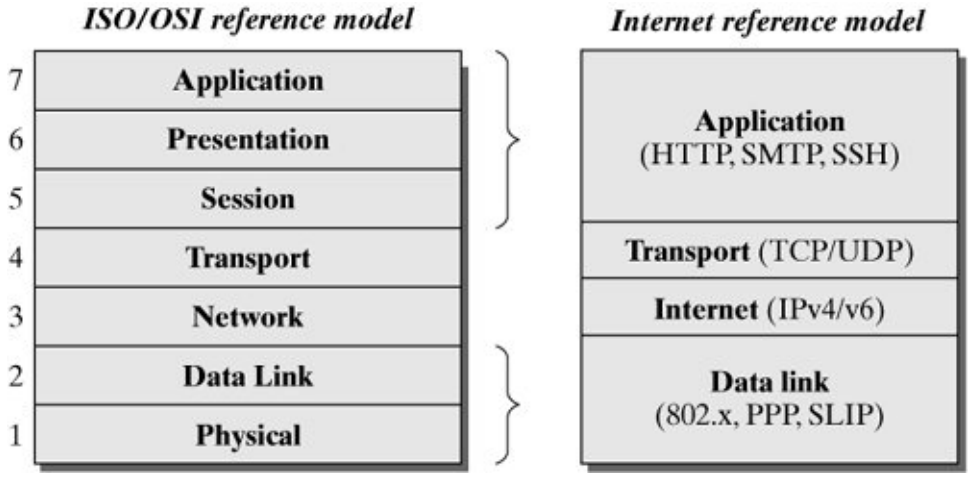
Resumo Em plena era da informação e com sistemas e serviços, que cada vez mais, dependem da fiabilidade e segurança das redes de computadores, e dada a as vulnerabilidades e preucupação, ou falta dela, por parte de quem implementa e desenvolve as aplicações e protocolos, não é nenhum eufemismo dizer quer "uma rede verdadeiramente segura é uma rede isolada". Neste relatório iremos descrever, em que medida, as redes de computadores estão vulneráveis a ataques e que mecanismos de segurança existem para as proteger, e. g. *firewalls* e protocolos de segurança, e apesar de identificarmos e utilizarmos como objeto de estudo alguns ataques *(IP Spoofing, Sniffing e DOS)*, o intuito deste relatório não é descrever ou explicar como podem ser implementados, mas sim compreender, em que nível da rede atuam e quais vulnerabilidades tiram partido. Portanto é expectável, que a leitura deste artigo possa sensibilizar o leitor para alguns aspetos relacionados com a segurança em rede de computadores, tanto ao nível das medidas de prevenção como das possíveis vulnerabilidades presentes nas redes de computadores.

1 Rede de Computadores

Uma possível definição para uma rede de computadores é um qualquer conjunto de linhas de comunicação que formem uma rede e/ou conjunto de sub-redes e sistemas interconectados, tais que num limite inferior dois computadores, conectados, formam uma rede. Com base nessa definição é possível inferir, que a forma como a rede está conectada é irrelevante, i.e. não há apenas uma forma de rede mas varias, esta abstração é importante para o estudo e analise dos tópicos abordados a seguir.

1.1 Conceitos Básicos: modelo ISO, Internet e o protocolo TCP/IP

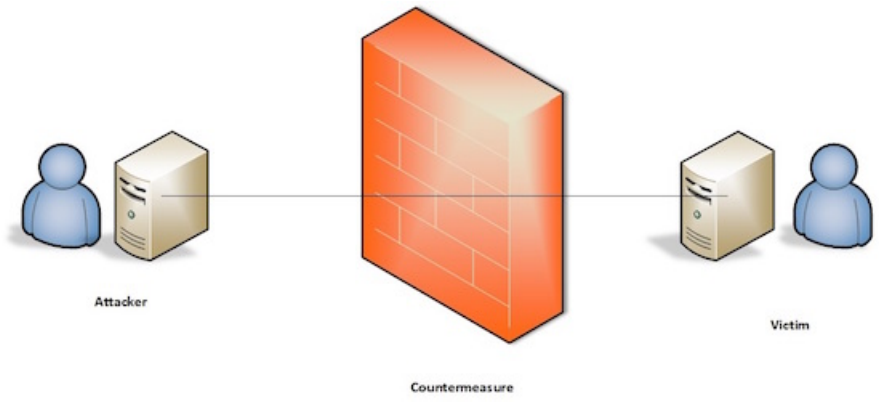
Neste relatório as redes de computadores iram ter como base o modelo de referencia *ISO (International Standards Organization)* onde uma rede de computadores está divida por camadas e que, de uma maneira simples, cada camada tem como objetivo fornecer um serviço para a camada inferior, as camadas constituintes de uma rede estão presentes na seguinte imagem:



Outro conceito fundamental é a *Internet*, que pode ser vista como uma rede de redes de computadores, a maior de todas, e que acreditasse ser impossível de interromper, ou destruir, totalmente em um só evento dado a complexidade da sua infraestrutura e implementação. Temos ainda o protocolo *TCP/IP (Transport Control Protocol/Internet Protocol)* que pode ser visto, como a "linguagem da *Internet*" [1]. Tudo que possa aprender a "falar em *TCP/IP*" pode comunicar com a Internet. Esta funcionalidade ocorre ao nível da camada de rede *(IP)* e da camada de transporte *(TPC)* do modelo de referência *ISO*, e consequentemente, um *host* que implemente a funcionalidade *TCP/IP (e.g. Unix, MacOS ou Windows NT)* pode facilmente suportar aplicações que utilize a *Internet*.

1.2 Ataques e Ameaças na Rede

Para que possamos compreender em que medida as redes de computadores estão seguras ou vulneráveis a ataques, primeiramente, temos que analisar o que define um ataque em rede de computadores.



De uma maneira geral, qualquer ataque em rede de computadores, tem um objetivo e um alvo predefinidos, independente do grau de sofisticação, e todos os *exploits* e vulnerabilidades utilizados durante o ataque tem sempre esses pontos presentes. Mesmo que não seja evidente, numa primeira analise, esses são os dois pontos mais importantes na compreensão, e possível implementação, de medidas de segurança. Vamos por exemplo analisar, de forma breve, um dos principais ataques e responsáveis por inúmeras fraudes eletrónicas o *phishing*, que tem origem no termo inglês *fishing*, que consiste em tentar adquirir informações pessoais (contas, palavras-chave, número de cartões de credito e etc.) a fazer-se passar por entidades confiáveis, há varias formas de *phishing*, vamos nos focar

no *phishing* por *e-mail* que tira proveito da falta de segurança relacionada com o protocolo *SMTP (Simple Mail Transfer Protocol)* e a verificação do remetente, de facto, o *SMTP* não permite uma autenticação por parte do remetente das mensagens. Tornando assim um alvo, fácil, para aqueles que desejam cometer *phishing*, basta apenas, alterar o cabeçalho protocolar do *SMTP* no envio das mensagems para o correio electrónico. Mas, então, porque não há medidas de segurança implementas, para evitar esse tipo de ataque através do protocolo *SMTP*? A resposta para essa questão, não é simples, e vem de encontro ao segundo ponto importante da noção de segurança e medidas a serem implementadas na rede de computadores, que é abordado a seguir.

2 Segurança

Uma primeira afirmação que está presente nesse relatório é a de que "uma rede verdadeiramente segura é uma rede isolada", mas será essa rede útil para o que eu pretendo? Voltando a análise do *SMTP*, é importante notar que o este protocolo foi desenvolvido pelo *IETF (Internet Engineering Task Force)* em 1982 (documentado no RFC 821) com o intuíto de facilitar e criar uma norma *standard* para o envio e troca de *e-mails* entre universidades e/ou istituições, não havendo a necessidade de se fazer um controle extensivo de autenticação para evitar *spam* ou *phishing*, que não eram preocupações "relevantes" na altura. Contundo é difícil responder, o quão seguro é um sistema, depende daquilo que é considerando como aceitável por parte dos utilizadores e até que ponto os mesmos estão dispostos a ser "incomodados" por essas medidas de segurança. E um compromisso complicado de se manter, por parte de quem implementa ou fornece o serviço de segurança, pois para além de ser "obrigado a dar respostas a ataques conhecidos" tem de implementar e prever possíveis novos ataques, mas está limitado a implementações de medidas de segurança que vão de encontro a disponibilidade e paciência dos utilizadores da rede, por isso, segurança é mais que uma medida de prevenção é uma medida do compromisso que o sistema, ou protocolo, fornece face a possíveis ataques e ameaças. Passemos agora a análise mais aprofundado de três tipos de ataques, que são bastante comuns e ajudam a compreender algumas vulnerabilidades das redes de computadores.

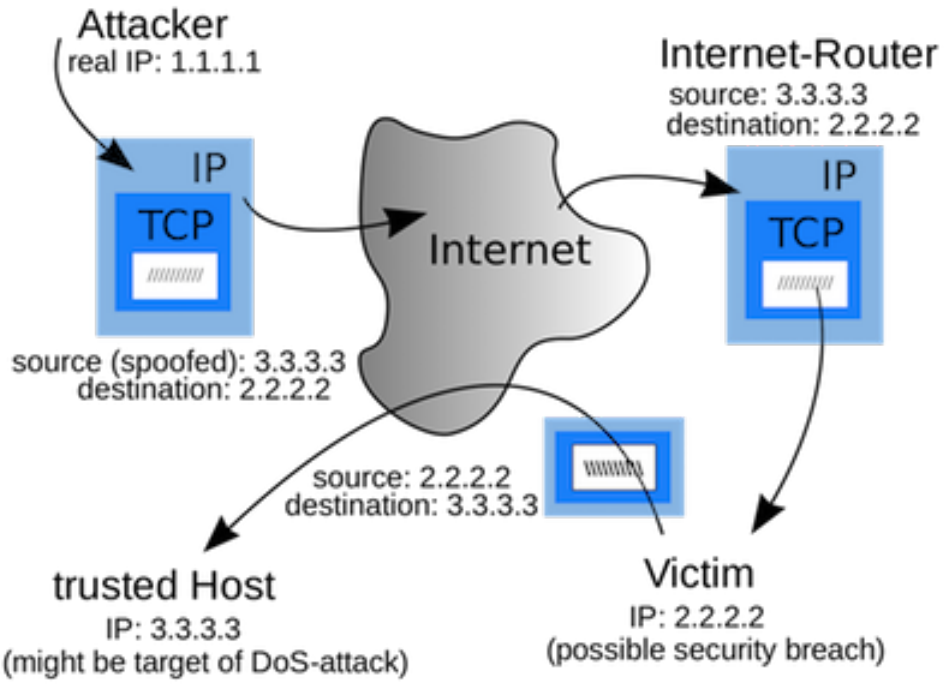
2.1 Sniffing

O *packet sniffing* é o processo de interceptar pacotes enviados, entre duas máquinas, tipicamente seguido duma descodificação para obter acesso à informação contida nos pacotes. Existem usos legítimos, nomeadamente a monitorização ou investigação policial, mas na sua grande maioria os usos são maliciosos. Cada pacote tem duas partes essências, o *header* e a *payload*. Por vezes apenas os *headers* são guardados para poupar memória, no entanto estes já fornecem bastante informação tal como a origem e destino do pacote, protocolo, tamanho entre outros. Caso a data esteja a ser armazenada e possivel que tudo esteja a ser descodificado, o atacante tem acesso aos sites que foram visitados, *e-mails* enviados e recebidos, *passwords*, etc. As redes por fio estão mais protegidas a este tipo de ataque, visto que podem cortar o acesso através de switches ou routers, já as ligações wireless estão mais vulneráveis, uma vez que qualquer pessoa com um recetor pode eventualmente cometer este tipo de ataque. Não é fácil impedir *packet sniffing*, mas a encriptação é uma boa medida de segurança, já que mesmo que alguém tenha acesso ao *payload* de dados, dificilmente terá acesso à informação.

2.2 IP Spoofing

Este tipo de ataque consiste em disfarçar *(spoof)* os pacotes *IP* enviados, mais especificamente, modificando o campo do remetente no *header* de cada pacote *IP*. Este ataque tem como objetivo esconder a identidade de um remetente. Existem protocolos que combatem

este tipo de ataque, como por exemplo o *TCP*, e tentam garantir uma conexão segura através de uma técnica conhecida como *3-way handshake* e/ou gerando sequências de números que são seguidos de confirmações sempre que um dos intervenientes recebe um pacote.

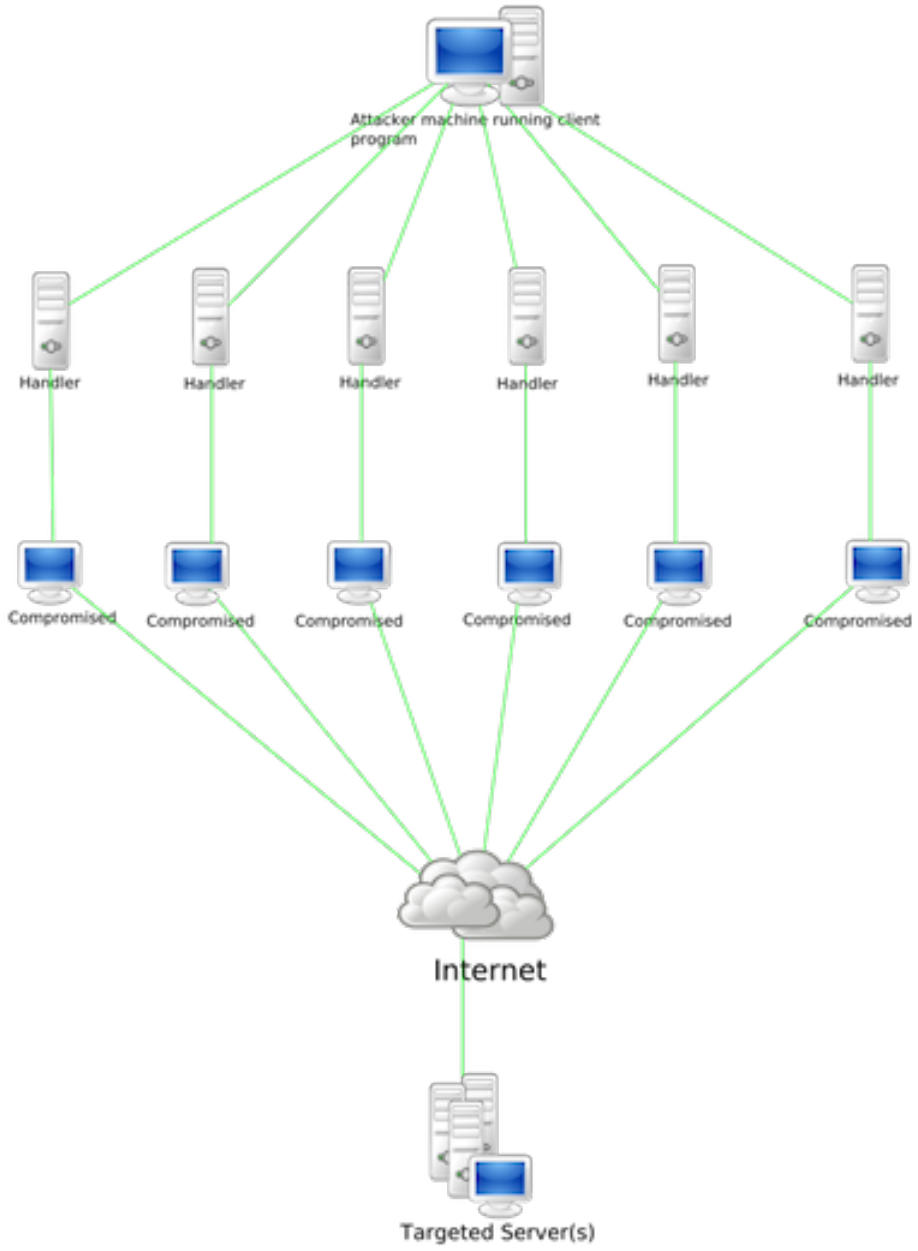


É possível categorizar o *IP Spoofing* em dois tipos [4]; caso a vítima esteja na mesma *subnet* que o atacante, esta encontra-se vulnerável a um *Non-Blind Spoffing*, que é especialmente perigoso porque o atacante pode fazer *sniff* aos pacotes da vítima, e consequentemente tem acesso à sequência de números que identifica o computador da vítima na sua conexão atual. De tal forma que o atacante consegue contornar as medidas de segurança impostas pelo protocolo e passa a ter a possibilidade de se fazer passar pela vítima ou até de entrar em sessões que a mesma tenha aberta, ação esta denominado de *Session Hijacking*; mas caso não tenha acesso à mesma *subnet* que a vítima a sequência de números terá que ser adivinhada, *Blind Spoofing*, um método que é mais difícil, visto serem bastantes extensas e aleatórias as informações geradas, mas que chegou a ser um método eficaz em sistemas mais antigos. Uma terceira possibilidade, é o um metódo conhecido como *Man in the Middle*, em que o atacante recebe todo o tráfego enviado entre duas máquinas e o redireciona, tal como se não estivesse lá, deste modo não alerta as vítimas e tem acesso a informação durante longos períodos de tempo. *IP spoofing* pode ainda ser usado em ataques *DDOS* a partir de uma só máquina, pois permite identificar cada pacote com uma origem única, tornando mais difícil distinguir os utilizadores legítimos dos pacotes de spam. De modo a combater I*P spoofing* existem várias táticas, aumentar o nível de encriptação e torna o processo muito mais demorado para qualquer atacante, usar uma autentificação por chaves entre máquinas da mesma rede *(IPsec)* para uma ligação segura ou filtrar todo o tráfego, de entrada e saída, bloqueando, por exemplo, todo o trafégo que se identifique com um *IP* interno, mas venha de fora.

2.3 DOS

O *DOS*, ou *denial of service attack*, é um ataque com o objetivo de tornar um serviço online inutilizável normalmente através de *flooding*, ou seja, do esgotamento da banda. Este tipo

de ataque é muito comum atualmente, é usado por razões monetárias, como rivalidades comerciais ou extorsão, por puro vandalismo ou até mesmo por razões sociais, como por exemplo bloquear um site político.



A variação mais comum deste ataque é o *DDOS, distributed denial of service*, em que a única diferença é que o ataque tem vários pontos de origem, resultando num volume maior de mensagens e numa maior dificuldade em ser parado. Este método, utiliza normalmente um *botnet*, uma rede de computadores normalmente infetados por *malware* que fica escondido até receber um sinal, que ativa todos os computadores infetados ao mesmo tempo. Um dos tipos mais simples, e que pode ser praticado por qualquer utilizador com conhecimentos mínimos, é o *ping flood*, no qual o computador envia *pings*, o mais rápido possível, sem

esperar pela resposta, basta que o *upload* do atacante seja superior ao *download* da vítima.O *SYN flood* é um tipo de *DOS* que explora o funcionamento do *TCP*; são enviados sucessivos pacotes *TCP/SYN*, com o *IP* de origem modificado *(IP spoofing)*, que levam a que o servidor abra uma conexão e espere pela resposta que nunca chegará, atingindo rapidamente, o número máximo de ligações abertas, tornando o serviço inútil. Um tipo mais recente de *DOS*, neste caso a nível de aplicação, consiste em enviar *headers* legítimos, seguidos da informação a um ritmo muito reduzido, tentando assim ter o máximo de ligações abertas, em vez de tentar esgotar a banda. Existem ainda *DOS* acidentais, como por exemplo, no dia da morte do Michael Jackson muitos sites de redes socias caíram e até a Google, pensou que estava a ser atacada. O método de proteção, mais simples, é utilizar uma *firewall* a fazer bloqueios baseados no *IP* de origem, ou mesmo fechando portas, se bem, que a última poderá levar a que serviços legítimos sejam afetados. Existem também routers e switches, aos quais podem ser adicionadas regras ou limites, mas todos estes métodos partilham o problema, de que muitas vezes é difícil separar o tráfego legítimo do ilegítimo, e bloquear tudo, não resulta, pois, esse é o objetivo do ataque. Uma solução possível, é deixar o servidor a ser atacado ligado, de modo a servir de distração, enquanto que todos os pedidos novos são encaminhados para um novo.

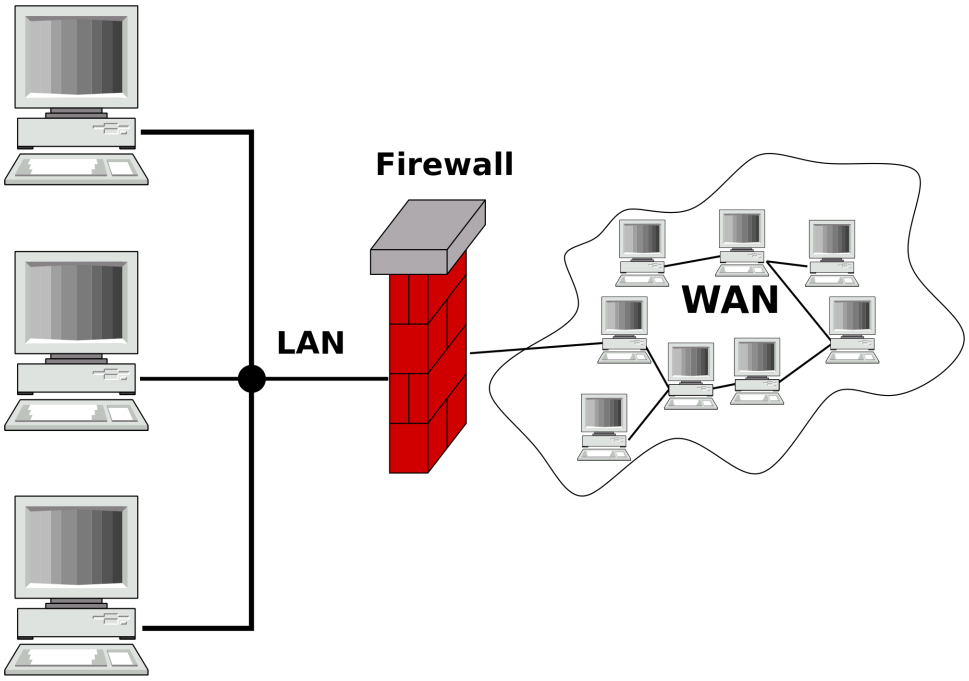
2.4 Firewall

A *Firewall* é uma solução de segurança que pode ser baseada tanto em *software*, normalmente o mais utilizado, como em hardware. Tem como objetivo controlar os pacotes que entram e saem de uma determinada rede. Uma *firewall* decide quais pacotes deixa entrar numa rede consoante as regras implementadas na mesma. Por exemplo, uma *firewall* pode ser configurada de modo a bloquear qualquer pacote que tente entrar na rede, porem a rede fica totalmente isolada. Pode também ser configurada de maneira a deixar um tipo de pacotes entrar na rede, mas a bloquear outro. Existem vários tipos de *softwares* de *firewall*, sendo estes comparados através da sua capacidade de examinar os acontecimentos em cada camada do *TCP/IP*.

Camada de Aplicação	Estabelece ligação com uma determinada aplicação.
Camada de Transporte	Transformar os dados recebidos e enviá-los como pacotes entre redes.
Camada de Internet	Adiciona informação aos pacotes sobre o sítio para onde têm de ir.
Camada de Interface de Rede	Tem como objetivo enviar os pacotes pelos elementos ”físicos”da rede.

Figura 1. Camadas organizadas desde a mais alta até à mais baixa (TCP/IP) [2]

Tipos de Firewall Apesar de existirem vários tipos de *firewall* as seguintes são algumas das mais conhecidas. Uma das primeiras medidas de seguranças, implementadas numa *firewall*, que apesar de ser bastante básica, está, ainda hoje presente na maior parte dos sistemas de *firewall*, e é a *firewall* presente na maioria dos routers. Tal como o nome indica, este tipo de *software*, deixa passar ou bloqueia um pacote consoante as regras definidas pelo utilizador. Um pacote traz consigo diversas informações como a origem, o destino, as portas por onde tem de passar, entre outras, ou seja, informação básica. A *Firewall* analisa essa informação, e depois verifica no conjunto de regras, se bloqueia, ou não, o pacote. Existem dois tipos de filtragem de pacotes, a filtragem estática e a filtragem dinâmica.



Filtragem de Pacotes Estática Esta filtragem aprova ou não pacotes, com base na informação básica do pacote. E como tal há um problema, pois certos serviços podem ser aprovados, e, no entanto, os requisitos que estes necessitam para funcionar, podiam ser rejeitados, o que leva ao não funcionamento de serviços que tinham sido aprovados pela *firewall*. Para corrigir, isto os utilizadores da firewall são obrigados a diminuir a ”rigidez”das regras do filtro.

Filtragem de Pacotes Dinâmicos É capaz de criar regras, que se adaptam às informações básicas de serviços, que dependem de trafego continuo para funcionar. Permitindo assim, que pacotes necessários ao funcionamento das aplicações, possam sair e entrar da rede, reduzindo o risco de serem rejeitados.

Proxy Este tipo de *firewall*, funciona como um intermédio, entre o computador e a rede externa, normalmente instalados em servidores, devido à necessidade de suportar com elevados números de pedidos. E como funciona, como um intermediário, impede que haja uma comunicação direta entre a rede interna e externa. Qualquer pedido, feito pelo utilizador na rede interna é enviado para o *proxy*, e este é que entra em contacto com a rede externa, mas apenas se o pedido do utilizador for aprovado pelas regras da *firewall*. Quando um pacote é enviado para a rede interna, este é enviado primeiro para a *firewall*, que analisa o pedido e só depois envia para a rede interna, caso este passe no conjunto de regras. No entanto, o *proxy* é ”invisível”a ambas as redes, fazendo-as pensar que há uma conexão direta entre elas.

Inspeção de Estados Este tipo de *firewall* trabalha ao nível da camada de transporte do *TCP/IP*, seguindo os estados de conexão de um pacote e bloqueando o seu acesso, caso este se desvie do seu destino espectável. Neste tipo de *firewall* todo o tráfego é analisado, e toda a informação analisada é armazenada, isto acontece para que todo o tráfego, que se passe pela *firewall*, seja comparado com as informações armazenadas, de forma a encontrar um padrão de tráfego, de tal modo que a f*firewall* consiga prever o seu destino, e saber, portanto se a informação do pactote é válida.

3 Conclusão

Este trabalho no âmbito da unidade curricular de Redes de Computadores, permitiu a todos os elementos do grupo, aprofundar e estudar tópicos relacionados com Segurança, Protocolos e Normas tanto da IETF como do IEEE que se mostraram uma mais valia, para o estudo e analise do tema proposto neste relatório. Conseguimos tirar lições importantes, tanto ao mais baixo nível, de implementação das redes de computadores como, ao mais alto nível, de programação em que conseguimos apurar que face aos diferentes tipos de ataques e ameaças é sempre importante manter-se atualizado, das vulnerabilidades presentes não só ao nível do Sistema Operativo mas ainda dos protocolos utilizados para comunicação de dados. Acreditamos ter abordado o tema da segurança de forma coesa e precisa, e apesar de termos muito mais a dizer, dado a limitação imposta pelo trabalho e de forma a manter o tema dentro do âmbito da unidade curricular, decidimos fazer uma abordagem horizontal ao tema, e avaliamos o trabalho positivamente em relação ao tema e tópicos aqui abordados.

Referências

1. Matt Curtin: Introduction to Network Security (1997) http://www.interhack.net/pubs/network-security/
2. Fan Yan, Yang Jian-wen, Cheng Lin: Computer Network Security and Technology Research (2015) http://ieeexplore.ieee.org
3. Liu Chunli, Liu DongHui: Computer Network Security Issues and Countermeasure (2012) http://ieeexplore.ieee.org
4. Victor Velasco: Introduction to IP Spoofing (2000) http://ieeexplore.ieee.org
5. Wentao Liu: Research on DoS Attack and Detection Programming (2009) https://en.wikipedia.org/
6. Sabeel Ansari, Rajeev S.G., Chandrashekar H.S.: Packet sniffing: a brief introduction (2003) http://www.symantec.com/
7. Karen A. Scarfone, Paul Hoffman: Guidelines on Firewalls and Firewall Policy - SP 800-41 (2009) http://dl.acm.org
8. Emerson Alecrim: O que é firewall? (2013) http://www.infowester.com/firewall.php