E-fólio B | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

NOME: Ricardo Ferreira da Conceição Dias Marques

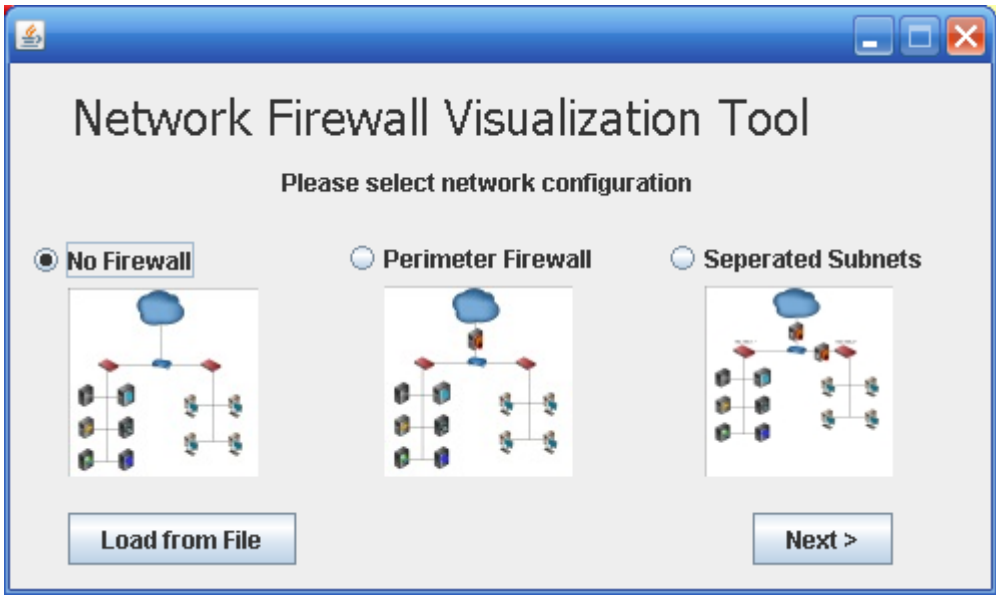
N.º DE ESTUDANTE: 1100281

CURSO: Licenciatura em Engenharia Informática

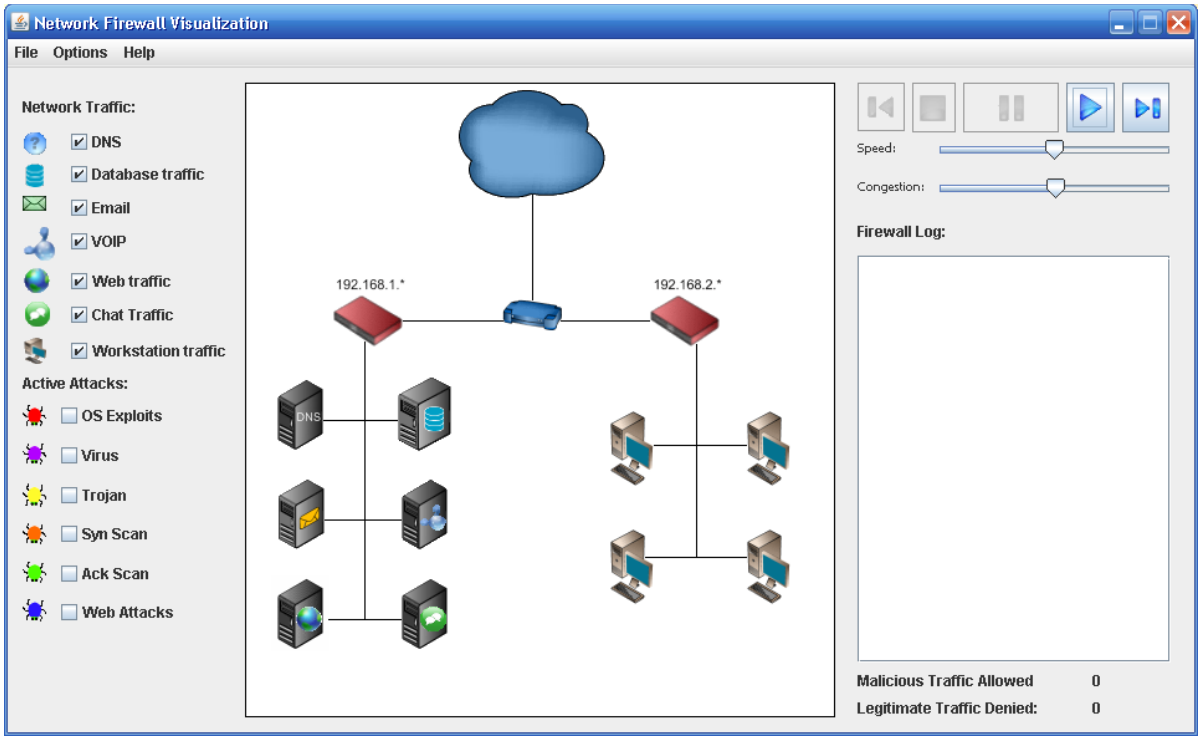
DATA DE ENTREGA: 4 de janeiro de 2019

Firewall Exercise
BACKGROUND:

1. Start the Firewall program from the Tools menu of the class web site. You should see a screen similar to the one below:



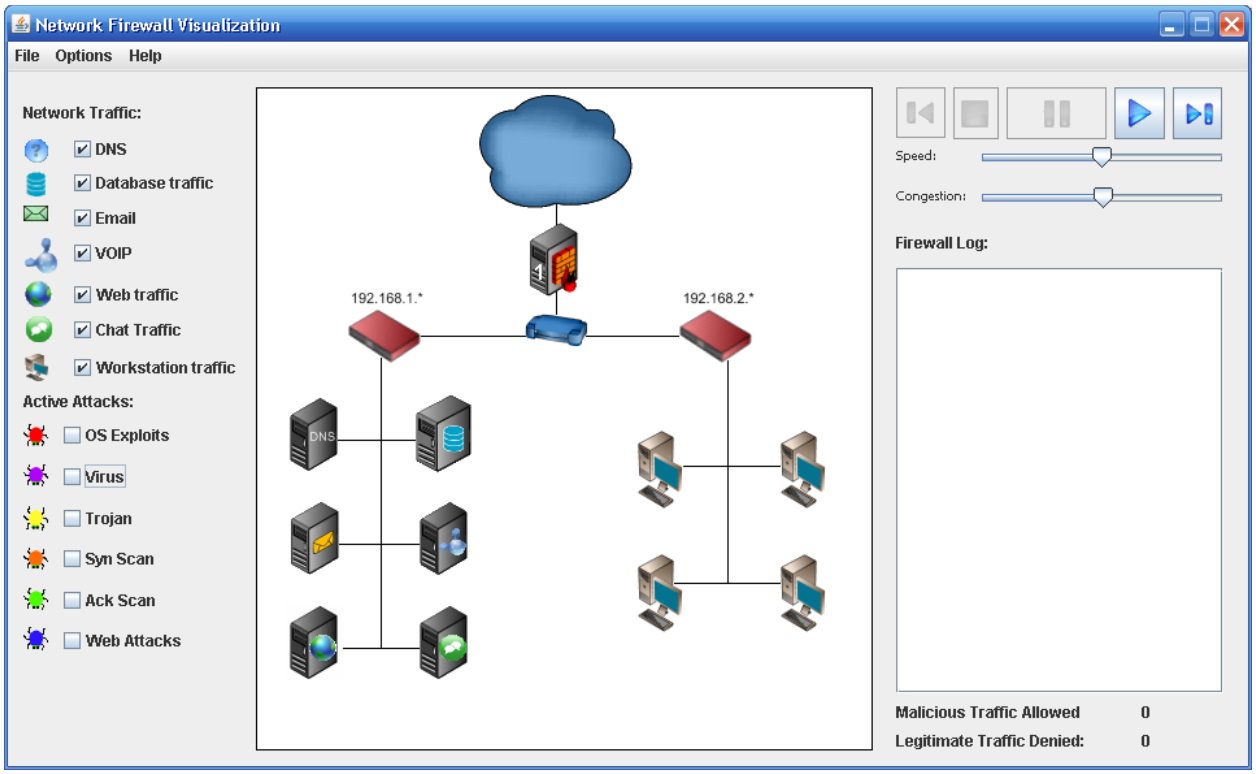
Choose “no firewall” and click next. The following screen will appear:



Click the  button. Note that the traffic flows both from the "cloud" or internet to the client machines. By default, there is no malicious traffic flowing to the machines. Click on the *OS Exploit* option. Eventually, you'll see a similar red colored bug flow from the internet into the local area network and land on a machine, infecting the machine. Once a machine is infected, it is marked as such with the "international No" emblem or  . Let's see how configuring a firewall will help prevent such infections.

FIREWALL Configuration.

1. Start a new session by clicking File -> New in the upper window of the tool. This time, choose the Parameter firewall. The window that comes up will look like this:



You now have a firewall between the internet (represented by a cloud) and your network router. Click the play button and watch what happens. **Do you see traffic flowing from the internet into your system or from your network to the internet? Explain why or why not:**

> *1. Do you see traffic flowing from the internet into your system or from your network to the internet? Explain why or why not:*

Resposta: Não existe tráfego a fluir da Internet para a rede interna, nem da rede interna para a Internet, dado que a *firewall* provavelmente terá definida uma política implícita de não permitir tráfego que não esteja explicitamente autorizado. Esta política é descrita, por exemplo em Stallings (2007, Cap. 21, pág.9) como sendo uma política do tipo "***Default = discard***", segundo a qual tudo o que não estiver explicitamente permitido, encontra-se proibido (no texto original "*That which is not expressly permitted is prohibited")*.

2. Add some active attacks by clicking on several different options. **Are these attacks able to get to your network? Do you feel your system is secure? What's wrong with this scenario?**

> *2.1. Are these attacks able to get to your network?*

Resposta:

Os ataques **não** são capazes de entrar na nossa rede porque, tal como vimos na pergunta anterior, a configuração atual da *firewall* bloqueia todo o tráfego da Internet para a rede interna e vice-versa.

> *2.2. Do you feel your system is secure?*

Resposta:

O nosso sistema está "seguro", na medida em que, estando bloqueado **todo** o tráfego, então o tráfego que seja **malicioso** não entrará na rede interna (assumindo o aparente pressuposto do simulador em que os ataques apenas vêm da Internet e nunca têm origem na própria rede interna).

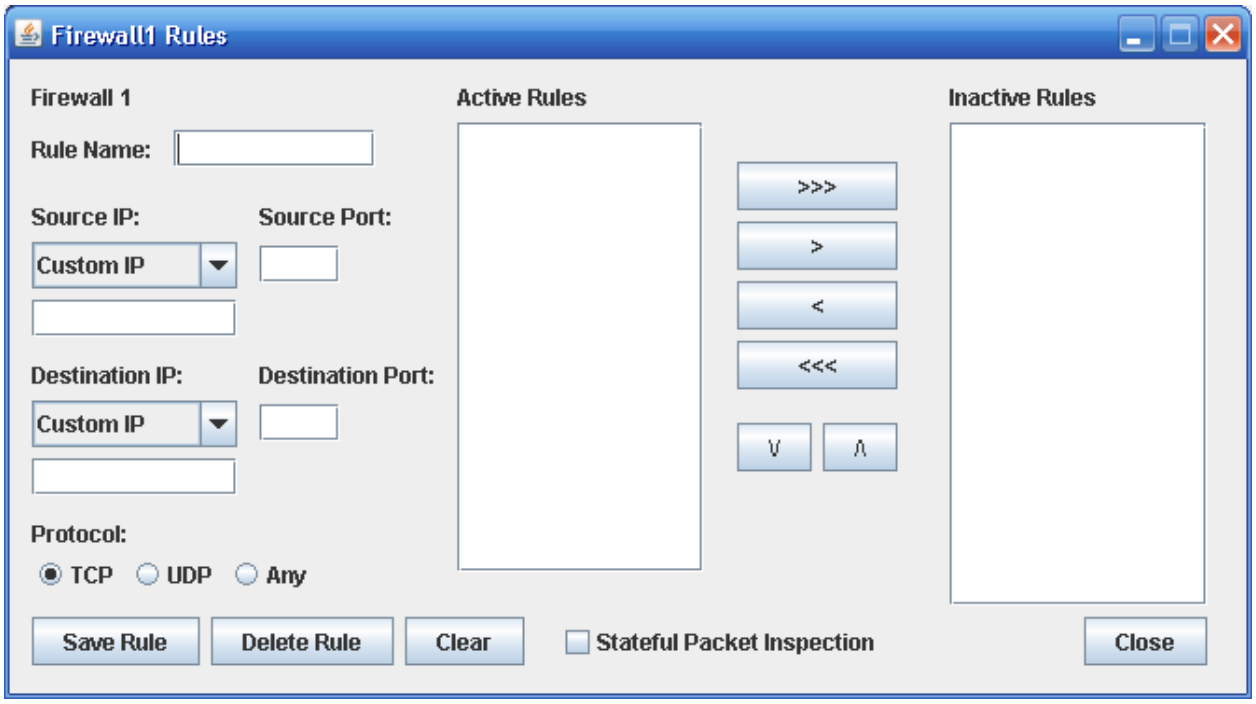
> *2.3. What's wrong with this scenario?*

Resposta:

O que está "errado" neste cenário é que, conforme vimos, **nenhum** tráfego (seja ele **malicioso** ou **legítimo**) vindo da Internet consegue entrar na rede interna e nenhum tráfego vindo da rede interna consegue aceder à Internet. Ora, na grande maioria dos cenários, é necessário e pretendido que tráfego da Internet que seja considerado **legítimo** (seguindo políticas em vigor) possa aceder a partes definidas da rede interna **-E-** é também necessário e pretendido que determinados tipos de

tráfego (definidos também em políticas como sendo legítimos) que tenham origem na rede interna possam aceder à Internet.

3. Configure your firewall to allow traffic to flow in and out of your network. Do this by choosing the 'options' tab at the top of the tool and define firewall rules. You should see a screen similar to the one below:



Name your firewall rule (typically with a name that focuses on a given subject or attack). The "Source IP" option and port refer to how you want the firewall to recognize a given source IP/Port combination and respond. The Destination is similar but focusing on a destination rule. The goal of any good firewall configuration is to identify legitimate traffic while restricting malicious traffic. Try setting the following firewall rule:

Rule Name: DNS Rule
Source IP: DNS, Source Port: 53
Destination IP: Any, Destination port *
Protocol: Any.

Click "Save Rule". You should now see the rule in your Active Rules box. Click "close" and you should be back to your Network Firewall Visualization Tool window. Click the play button and watch what happens. You may need to move the speed bar to the right for a higher speed of traffic. **What traffic now flows through the firewall?** Add some active attacks and watch if they flow through the firewall. **Would you claim your rule is now sufficient to allow traffic to flow for a typical network? Why or why**

not? Do any of the active attacks now work against machines behind the firewall?

> *3.1. What traffic now flows through the firewall?*

Resposta:

O tráfego que atravessa a *firewall* é o tráfego de DNS (resolução de nomes para os respetivos endereços IP) que tenha, como origem (na perspetiva da *firewall*), o servidor de DNS da organização. Tipicamente, estaremos a falar de resolução de nomes para os quais o servidor de DNS esteja configurado como sendo um *DNS forwarder.*

> *3.2. Would you claim your rule is now sufficient to allow traffic to flow for a typical network? Why or why not?*

Resposta:

A regra que criei continua a **não** ser suficiente, na medida em que todo o tráfego legítimo originário da Internet (com destino à rede interna) continua a ser bloqueado e que o único tráfego legítimo originário da rede interna com destino à Internet que a *firewall* deixa passar é o tráfego de DNS.

> *3.3. Do any of the active attacks now work against machines behind the firewall?*

Resposta:

Os ataques ativos continuam a **não** funcionar contra as máquinas atrás da *firewall*, dado que continua a ser bloqueado todo o tráfego com origem na Internet e com destino na rede interna.

4. Come up with a series of rules which seems to protect the network from all attacks. Be sure to watch the legitimate traffic denied and malicious traffic permitted in the lower right hand portion of the screen. That should tell you how well your rules are working. **How many rules did you have to write**

to secure your network? Were you able to completely secure the network? What types of rules did you create?

> *4.1. How many rules did you have to write to secure your network?*

Resposta:

Criei 13 regras, que passarei a indicar e a descrever, de forma breve, mais adiante, na resposta à pergunta "***What types of rules did you create?***".

> *4.2. Were you able to completely secure the network?*

Resposta:

Não, não consegui segurar completamente a rede, na medida em que os "*OS Exploits*" (contra o servidor Web) e "Scans" continuam a atravessar a *firewall* e a chegar os servidores. Dado que estes tipos de ataques usam os portos corretos dos servidores, não é possível bloqueá-los apenas com uma *firewall* do tipo "filtro de pacotes" (*packet filtering firewall*), como aparenta ser a *firewall* usada no simulador.

Assim, é normal que tenham conseguido passar, na *firewall,* "OS Exploits" ao Servidor Web e *scans* aos vários servidores, dado que esses *exploits* usam os portos permitidos (associados aos serviços correspondentes) e a *firewall* em causa é uma *firewall* do tipo "filtro de pacotes" (*packet filtering firewall*). Ora, conforme é indicado, por exemplo em Stallings (2007, Cap. 21, pág. 12), este tipo de *firewalls* tem algumas limitações, como sejam as seguintes (aplicáveis à situação do presente e-fólio):

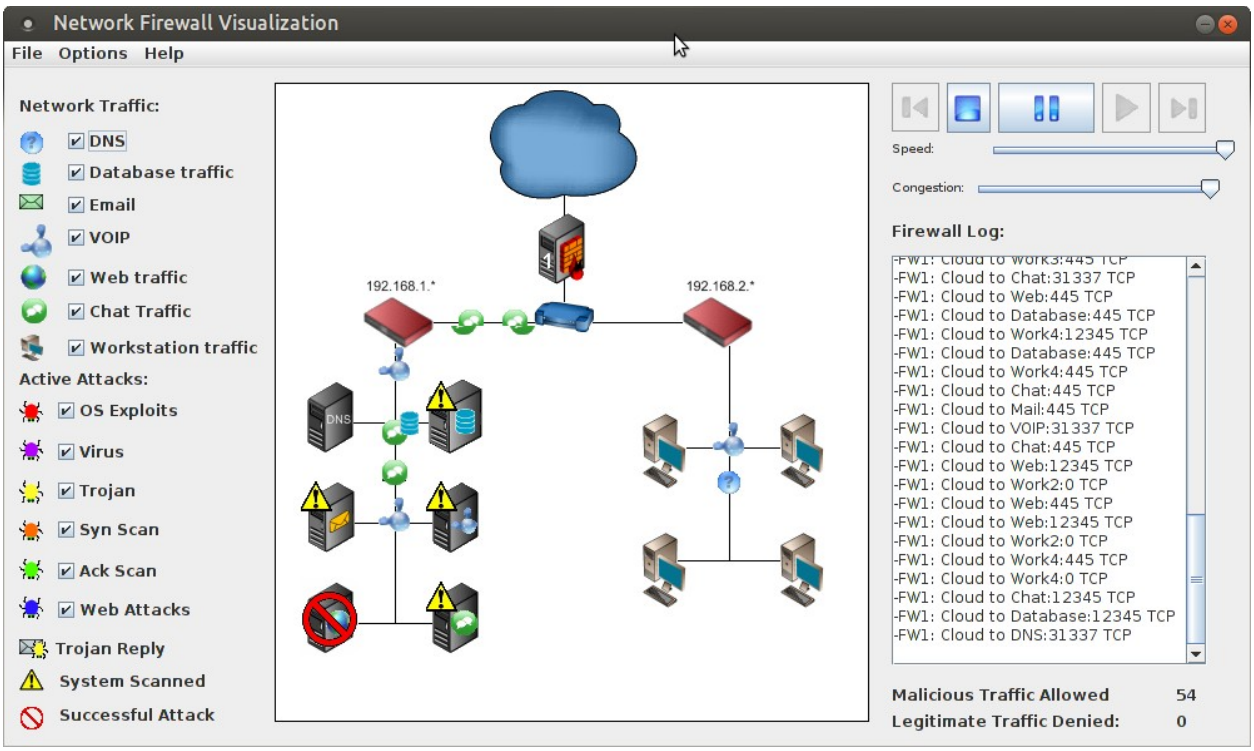
"*Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.(...) Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing.*"

Mais abaixo, incluo uma *screenshot* que revela que, com as regras que criei:

1 - **não foi bloqueado tráfego legítimo**

2 - o **tráfego malicioso** que conseguiu passar consistiu em "*OS Exploits"* ao Servidor Web e Scans aos vários servidores (o servidor de DNS, pelos vistos não foi *scanned*, talvez por eu ter restringido o tráfego, na regra correspondente, ao protocolo UDP, não autorizando o protocolo TCP).

Segue abaixo a *screenshot* da simulação, usando as regras que criei:



> *4.3. What types of rules did you create?*

Resposta:

Criei regras para :

1 – Permitir acesso *inbound* aos servidores nos portos associados dos serviços que prestam (ex: permitir acesso ao porto 80 do Servidor Web).

2 – Permitir acesso *outbound* da gama de endereços IP das estações de trabalho ao porto 80 (web) da Internet.

3 – Permitir acesso *outbound* dos vários servidores à Internet, que tenham destino no porto do mesmo tipo de serviço (ex: permitir que o servidor de DNS da organização aceda ao porto UDP 53 – de DNS – de outros endereços IP).

Nos nomes das várias regras que criei:

- Usei o indicador "**O**" para indicar que uma regra é uma regra "***O**utbound*" (no sentido de ser uma regra com **ORIGEM** nalgum dispositivo da rede interna).

- Usei o indicador “**I**” para indicar que uma regra é uma regra “***I****nbound*” (no sentido de ser uma regra com **DESTINO** nalgum dispositivo da rede interna).
- Usei o indicador “**R**” em todas as regras, apenas para indicar que uma regra é, precisamente, uma “**R**egra”.

Abaixo, estão as 13 regras de *firewall* que criei:

Nome da regra	**Endereços IP de Origem**	**Porto de Origem**	**Protocolo**	**Endereços IP de Destino**	**Porto de Destino**
VOIP I R	*.*.*.*	*	TCP	192.168.1.74	38287
Chat I R	*.*.*.*	*	TCP	192.168.1.68	5222
WK O Web R	192.168.2.*	*	TCP	*.*.*.*	80
Web I R	*.*.*.*	*	TCP	192.168.1.114	80
DB I R	*.*.*.*	*	TCP	192.168.1.233	3306
Mail I R	*.*.*.*	*	TCP	192.168.1.136	25
DNS I R	*.*.*.*	*	UDP	192.168.1.5	53
DNS O R	192.168.1.5	*	UDP	*.*.*.*	53
Mail O R	192.168.1.136	*	TCP	*.*.*.*	25
DB O R	192.168.1.233	*	TCP	*.*.*.*	3306
Chat O R	192.168.1.68	*	TCP	*.*.*.*	5222
VOIP O R	192.168.1.74	*	TCP	*.*.*.*	38287
Web O R	192.168.1.114	*	TCP	*.*.*.*	80

5. Download the “FicheiroRedeTrabalho” scenario from the eFolio page and save it to your desktop. Choose File -> new to restart the program and click “load from file” button, pointing the program to the file you downloaded.

This scenario was configured so that workstations can pass through *firewall2* and gain access to the database. *Firewall1* has an ***allow all*** traffic rule set so all information is passed through to the network and from the network to the servers. Write rules to prevent active attacks from passing through *firewall 1* and attacking the database. **Which active attacks are you able to prevent by restricting access on the firewall?**

> *5.1. Which active attacks are you able to prevent by restricting access on the firewall?*

Resposta:

Apesar de eu ter adicionado uma regra específica, na "Firewall1", que permita o acesso ao servidor de Base de Dados (conforme indicado no enunciado), **não** consigo bloquear quaisquer ataques, dado que existe uma regra pré-configurada chamada "***All In***" que permite todos os acessos *inbound, com* origem em qualquer endereço IP e com destino em qualquer endereço IP.

Para se poder bloquear ataques seria necessário remover a regra pré-configurada "***All In***"; **regra essa que, aliás, nem faz sentido existir numa *firewall*,** ainda para mais, numa "*firewall* de perímetro", como é o caso (que lida com tráfego oriundo de uma rede externa, como seja a Internet). Faria muito mais sentido que a configuração permitisse **apenas** o tráfego explicitamente considerado como sendo legítimo e que bloqueasse todo o restante tráfego.

Think back to the class discussion on malicious software attacks and distributed denial of service attacks. **Using the information from that class, why do you think that these types of attacks are not able to be prevented through the firewall? How might you prevent these attacks from taking place?**

> *5.2. Using the information from that class, why do you think that these types of attacks are not able to be prevented through the firewall? How might you prevent these attacks from taking place?*

Resposta:

Quanto aos ataques do tipo *distributed denial of service* (*distributed denial of service attack*) – abreviamente "***DDoS attacks***" - os mesmos estão descritos, por

exemplo, em Stallings (2007, Cap. 21, págs. 48 e seguintes) como sendo ataques que têm origem em múltiplos hosts e que impedem / visam impedir que utilizadores legítimos de um serviço possam usar esse serviço. Dado que um ataque deste tipo, por definição, surge num dado momento do tempo, com múltiplas origens em simultâneo e, várias vezes, usando tipos de tráfego que têm de ser permitidos (de forma a prestar os serviços), torna-se então difícil filtrá-los usando uma *firewall* convencional.

Quanto aos ataques do tipo de *software* malicioso (***malware***), existem vários mecanismos de **prevenção** que são descritos, por exemplo, na secção "*Malware Countermeasure Approaches*" de Stallings (2007, Cap. 21, pág 37) que cita um trabalho de outros 2 autores (Souppaya e Scarfone, 2012) em que se descreve **4 elementos principais de prevenção: política; consciência (*awareness*); mitigação de vulnerabilidades (*vulnerability mitigation*) e mitigação de ameaças (*threat mitigation*)**. Stallings detalha que uma das primeiras formas de prevenção é assegurar que **os sistemas sejam tão atualizados quanto possível, com todos os *patches* aplicados**, de forma a reduzir o número de vulnerabilidades que possam ser exploradas no sistema (se tal tivesse sido feito no caso apresentado no nosso simulador, talvez os ataques do tipo "*OS Exploits*" não tivessem resultado).

Stallings (2007, Cap. 21, pág 37) refere ainda outras formas de prevenção de *malware*, como sejam definir **controlos de acesso** em aplicações e dados armazenados no sistema (de forma a diminuir a "superfície de ataque") e **educar os utilizadores** para que sejam menos suscetíveis a ataques de engenharia social (*social engineering attacks*) como sejam os ataques de *phishing*.

Além disso, podemos considerar, como outras formas de prevenção de *malware*, o **uso de *software* antivirus e *antispyware* nos servidores**, tal como é descrito, por exemplo, em Stallings (2007, Cap. 21, págs. 39-42, na secção "*Host-Based Scanners*" e o uso de ***IPS*** (***Intrusion Prevention Systems***), em particular, no "perímetro" da rede (fronteira entre a rede interna e a rede externa), conforme descrito, por exemplo, na secção "*Perimeter Scannings Approaches*" de Stallings (2007, Cap. 21, págs. 43-46).

Referências Bibliográficas

Stallings, William (2007) *Cryptography and Network Security: Principles and Practice.* 7th Edition (Global Edition), Prentice Hall.

Souppaya, M., e Scarfone,K (2012) *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication 800-83 (Draft).