

1. Objetivos

Esta fase do trabalho pretende familiarizar os alunos com alguns dos problemas envolvidos na configuração de uma máquina segura, em particular, com a utilização e configuração de *firewalls* e de sistemas de deteção de intrusões.

O trabalho consiste na configuração de uma máquina segura onde será disponibilizado o servidor *myWhats*, utilizando as ferramentas *iptables* e *snort*.

2. Organização do trabalho

Este trabalho está dividido em duas partes:

Parte I: *iptables* – pretende-se que os alunos se familiarizem com a ferramenta *iptables* e que a utilizem de modo a configurarem a máquina segura.

Parte II: *snort* – de forma idêntica, pretende-se que os alunos se familiarizem com a ferramenta *snort* e que a utilizem de modo a configurarem a máquina segura.

De modo a cumprirem os seus objetivos, cada uma destas partes está subdividida nas seguintes etapas:

1. **Preparação prévia - a ser efetuada pelos alunos fora das aulas como preparação prévia para a aula de laboratório onde serão efetuadas as etapas seguintes;**
2. Exercícios na aula de laboratório (guião) - a serem efetuados pelos alunos durante uma aula teórico-prática (ver plano das aulas teórico-práticas na página da disciplina); e
3. Trabalho de grupo - a ser efetuado em grupo e cujo relatório será entregue na área de grupo da disciplina conforme descrito na secção 5 deste documento. Este trabalho pode ser efetuado durante a aula de laboratório.

3. Parte I: *iptables*

3.1. Preparação prévia

Antes de começar a realizar o projeto, estude a ferramenta *iptables* e efetue os exercícios do guião da aula TP.

3.2. Trabalho a realizar pelo grupo

Pretende-se que os alunos utilizem o comando *iptables* de modo a configurar a máquina segura onde será instalado o servidor *myWhats*.

A melhor maneira de garantir a segurança da máquina é reduzir os seus serviços ao mínimo indispensável e garantir a sua constante atualização. Neste contexto, a *firewall* deve ser configurada de modo a concretizar a seguinte política:

- Serviços suportados (aos quais a máquina responde): *ping*, *ssh* e serviços necessários para o servidor *myWhats*

Restrições: a máquina responde a *pings* apenas com origem nas máquinas da sua sub-rede local (com máscara 255.255.254.0), aceita ligações de clientes com qualquer origem para o servidor

myWhats e aceita ligações *ssh* apenas da máquina gcc. Os alunos devem assumir que a máquina corresponde a um dos PCs dos laboratórios do DI.

- Serviços utilizados: a máquina apenas pode fazer ping à máquina gcc.

Os alunos devem elaborar um relatório (iptables.pdf) com o seguinte conteúdo:

- Regras do comando *iptables* que permitem concretizar esta política; e
- explicação **do método de teste utilizado e observações realizadas**.

Observações:

- i) o normal funcionamento dos computadores dos laboratórios depende do seu acesso às seguintes máquinas:
DCs: 10.101.253.11, 10.101.253.12, 10.101.253.13, 10.121.53.14, 10.121.53.15, 10.101.53.16
Storage: 10.101.249.63
Iate/Falua: 10.101.85.6, 10.101.85.138
Nemo: 10.101.85.18
Gateway: 10.101.148.1
Proxy: 10.101.85.134
Deste modo, os alunos ao testarem as suas regras não devem impedir o acesso a estas máquinas.
- ii) a opção *-F* do *iptables* não altera a política definida por omissão. Assim, a seguinte sequência de comandos bloqueará o computador (ver justificação na observação anterior):
\$...
\$ sudo /sbin/iptables -P OUTPUT DROP
\$ sudo /sbin/iptables -F OUTPUT
- iii) O tráfego do dispositivo de loopback não deve ser filtrado:
\$ sudo /sbin/iptables -A INPUT -i lo -j ACCEPT
\$ sudo /sbin/iptables -A OUTPUT -o lo -j ACCEPT
- iv) O tráfego relacionado com uma ligação já estabelecida também deve ser aceite:
\$ sudo /sbin/iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
\$ sudo /sbin/iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

4. Parte II: *snort*

4.1. Preparação prévia

Antes de começar a realizar este trabalho, estude a ferramenta *snort* e efetue os exercícios da aula TP.

4.2. Trabalho de grupo

Pretende-se que os alunos utilizem o *snort* de modo a detetarem alguns ataques contra o servidor *myWhats*. Os alunos devem definir uma ou mais regras *snort* para as situações seguintes, potencialmente indicativas de um ataque:

- Deve ser gerado um alerta para a consola quando forem recebidas na máquina servidora 3 ou mais ligações TCP para portos inferiores a 2048 durante um intervalo de dois minutos (pode indicar um varrimento de portos) (NOTA: nesses dois minutos deve ser gerado **apenas** um alarme qualquer que seja a máquina que inicia as ligações, i.e., as ligações não têm de ter todas origem na mesma máquina).
- Deve ser gerado um alerta para a consola sempre que forem recebidas 3 ligações da mesma máquina emissora para o porto do servidor, durante um intervalo de 30 segundos (pode indicar que estão a tentar descobrir uma password de acesso ao serviço) (NOTA: deve haver um alerta **por cada** conjunto de 3 ligações observadas).

Os alunos devem elaborar um relatório (snort.pdf) com o seguinte conteúdo:

- regra(s) definida(s) para o comando *snort* com o comportamento descrito;
- forma de invocação do comando *snort*
- método de teste utilizado e observações realizadas

5. Entrega

- Dia **22 de Maio**, até às 23:59 horas.
 - Os grupos devem inscrever-se atempadamente de acordo com as regras afixadas para o efeito, na página da disciplina.
 - Na página da disciplina, submeter os ficheiros pdf dos 2 relatórios.
- Dia **23 de Maio**, até às 12:00 horas.
 - A entrega será em papel, no cacifo do professor das TPs.

Não serão aceites trabalhos por email nem por qualquer outro meio não definido nesta secção. Se não se verificar algum destes requisitos o trabalho é considerado não entregue.