Ciências ULisboa | Informática

di.ciencias.ulisboa.pt

/difcul

Segurança e Confiabilidade

2022/2023

Trabalho 2

1. Objetivos

Este trabalho pretende familiarizar os alunos com alguns dos problemas relacionados com a configuração de uma máquina segura, em particular com a utilização e configuração de *firewalls* e de Sistemas de Deteção de Intrusões (SDI).

O trabalho consiste na configuração de uma máquina segura, utilizando as ferramentas ***iptables*** e ***snort,*** onde terá de ser executado o servidor **TintolmarketServer** desenvolvido no Projeto 1.

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.

Para a realização do trabalho, os alunos irão utilizar uma máquina virtual (disponibilizada no Moodle) onde terão de executar o servidor e cliente **Tintolmarket** que foram desenvolvidos no Projeto 1, bem como as ferramentas ***iptables*** e ***snort***, num ambiente que simula a configuração dos computadores da rede dos laboratórios.

As instruções para execução da máquina virtual e do cliente e servidor **Tintolmarket** na mesma, e de como utilizar as ferramentas ***iptables*** e ***snort*** nesse contexto, serão dadas num ficheiro adicional disponibilizado no moodle.

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 **TintolmarketServer** que foi desenvolvido no Projeto 1.

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 segura responde): ***ping***, ***ssh*** e serviços necessários para aceder ao servidor **TintolmarketServer**

- Restrições: a máquina segura onde corre o servidor **TintolmarketServer**:

  (i) responde a *pings* apenas com origem na máquina **gcc** (10.101.151.5) e nas máquinas da sub-rede 10.101.85.0/24;

  (ii) aceita ligações de clientes **Tintolmarket** de qualquer origem para o servidor **TintolmarketServer**; e

  (iii) aceita ligações *ssh* apenas da máquina **gcc** e da sub-rede em que se encontram as máquinas DC1, DC2 e DC3 (com máscara 255.255.255.224).

- Serviços utilizados: a máquina segura onde corre o servidor **TintolmarketServer** apenas pode fazer:

  (i) *ping* às máquinas da sua sub-rede local. Contudo, a frequência dos *pings* deve ser limitada a um máximo de 3 *pings*/segundo;

  (ii) *ssh* 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 na rede dos laboratórios depende do seu acesso às seguintes máquinas:

   DCs: 10.121.52.14, 10.121.52.15, 10.101.52.16
   Storage: 10.121.72.23
   Falua: 10.101.85.138
   Luna: 10.101.85.24
   Gateway: 10.101.204.1
   Proxy: 10.101.85.137

   Deste modo, ao testarem as 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 **TintolmarketServer**. Um dos ataques a serem detetados é executado pela aplicação **NoTintol**, a ser disponibilizada aos alunos no Moodle. Esta aplicação lança um conjunto de *threads* que tentam insistentemente se ligar ao servidor **TintolmarketServer**, no seu respetivo porto.

Os alunos devem, portanto, definir uma ou mais regras ***snort*** para as situações descritas de seguida, potencialmente indicativas de um ataque:

- Deve ser gerado um alerta para a consola quando forem recebidas na máquina segura 5 ou mais ligações TCP para portos inferiores a 1024 durante um intervalo de um minuto (pode indicar um varrimento de portos) (NOTA: neste intervalo de um minuto deve ser gerado **apenas** um alarme, qualquer que seja a máquina que inicia as ligações, i.e., as ligações não têm todas de ter origem na mesma máquina).
- Deve ser gerado um alerta para a consola quando for detetado tráfego de rede que indique um possível ataque causado pela aplicação **NoTintol**. Esta situação deve ser diferenciada de um acesso considerado normal a partir de um cliente **Tintolmarket** (considera-se como acesso normal a ocorrência de até 3 ligações/tentativas de ligação num intervalo de 15 segundos) e que, portanto, não deve gerar alarme. Deve ocorrer **no máximo um alerta a cada 15 segundos**, caso a ação causada pela aplicação **NoTintol** persista. A aplicação **NoTintol** pode ser executada, por exemplo, na máquina *Outsider* e deve ser iniciada com os seguintes parâmetros: `java NoTintol <ip do TintolMarketServer> <porto do TintolMarketServer> <n_threads>`. Onde `n_threads` representa o número de *threads* lançadas e deve ser igual a `2000`.

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***;
- análise sobre a ação realizada pela aplicação **NoTintol** e o seu impacto no servidor **TintolmarketServer**. Devem comparar o consumo de recursos[1] pelas aplicações **NoTintol** e **TintolmarketServer**, relatar as eventuais consequências no servidor seguro e apresentar conclusões;
- método de teste utilizado e observações realizadas, para todas as regras criadas.

[1] Nota: embora as aplicações **NoTintol** e **TintolmarketServer** sejam executadas em diferentes máquinas do emulador de redes MininetX, na prática partilham os recursos da mesma máquina virtual em que o emulador é executado. Evidentemente, num sistema real, ao executar as referidas aplicações em máquinas diferentes, não haveria concorrência pelos mesmos recursos computacionais. No entanto, mesmo sendo um emulador, é possível fazer uma análise qualitativa sobre a variação e a proporção dos recursos consumidos pelas duas aplicações.

5. Entrega

Dia **26 de maio**, até as 23:59 horas. O relatório do trabalho deve ser entregue da seguinte forma:

- Criar um **ficheiro zip** com o nome **SegC-grupoXX-proj2.zip**, onde XX é o número do grupo, contendo os relatórios do ***iptables*** e do ***snort*** (2 ficheiros pdf). **Cada relatório deve ter no máximo 3 páginas**.
- Submeter o ficheiro zip através da atividade disponibilizada para esse efeito na página da disciplina no Moodle. Apenas um dos elementos do grupo deve submeter. Se existirem várias submissões do mesmo grupo, será considerada a mais recente.
- Preencher o formulário sobre contribuições para trabalho 2 que será disponibilizado no Moodle. **Alunos que não preencham o formulário sofrem uma penalização na nota de 10%**.

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.