ESTGF | POLITÉCNICO DO PORTO

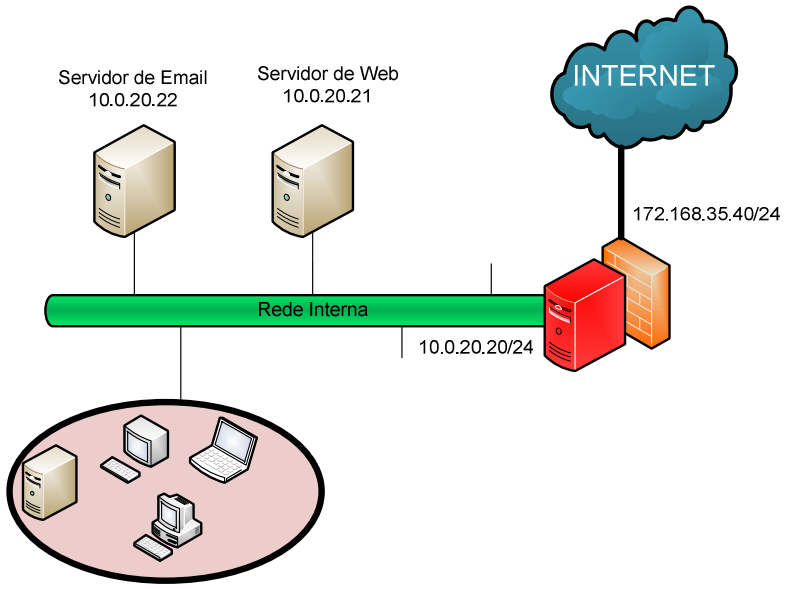
Licenciatura em Segurança Informática em Redes de Computadores

SEGURANÇA DE REDES

ANO LECTIVO 2019/2020

Trabalho Prático II

Case Study I



Neste exemplo, temos apenas uma máquina a fazer de firewall com duas interfaces. Uma interface (eth0) ligada á Internet, e a outra (eth1) ligada á rede interna.

Antes de mais é necessário definir os objetivos gerais da firewall. Isto deve ser feito durante a criação da política de segurança, e sendo mais exacto deve ser feito durante a criação da política de firewall.

Objetivos da Firewall

1. Permitir ICMP pings (“echo requests” e “echo replies”) através da firewall.
2. Permitir que os nossos clientes externos acedam ao servidor de email.
3. Clientes internos não podem usar servidores de email na internet.
4. Vamos permitir que clientes externos acedam ao nosso servidor web.
5. Vamos bloquear tentativas de “spoof” de endereços internos.
6. Máquinas internas acedem á Web.
7. As máquinas internas podem pingar hosts na internet.

8. As máquina internas não podem permitir outro tipo de trafego para a internet que não os permitidos acima.

1. Criação de cenário

a. Preparar o cenário com recurso a máquina virtuais, usando o virtual Box, e com software disponível no LAB P5.
b. O módulo de firewall deve ser o iptables. Podem usar qualquer versão de Linux para o efeito. As restantes máquinas podem ser Linux ou Windows. Façam um desenho pormenorizado da vossa implementação.

2. Configuração

a. Implementar as politicas de firewall descritas na introdução do case study.
    i. Descrever todos os passos da configuração das regras.
    ii. Indicar com comentários elucidativos toda a configuração efetuada.
    iii. Usar sempre que possível “user-defined chains” para melhor leitura e compreensão das regras.

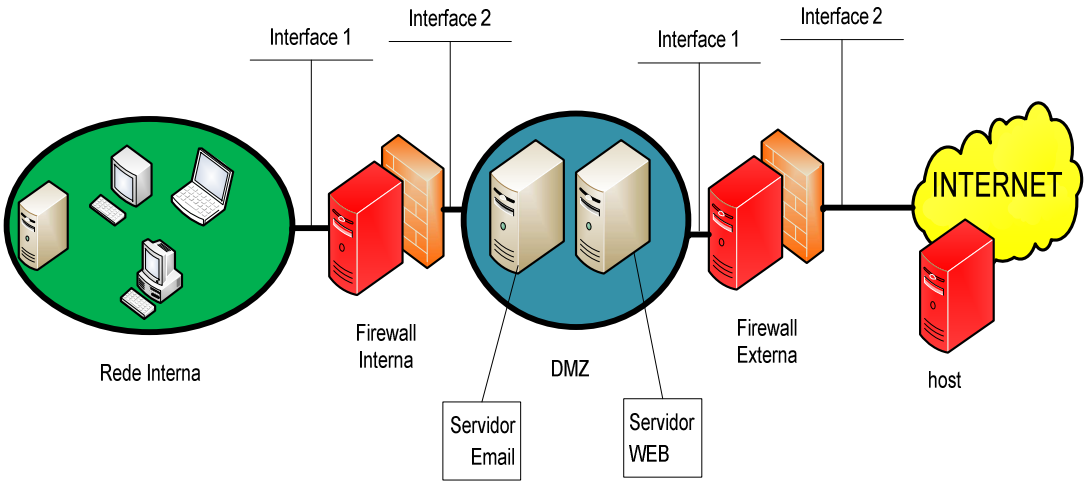
3. Demonstração

a. Listar todas as chains. Indicar comando necessário.
b. Demonstrar que as políticas implementadas estão de facto a funcionar.
c. Comentar o objetivo 1 na perspetiva de segurança.

4. Firewall Builder

a. Criar as mesmas regras usando o firewallbuilder. Demonstrar a configuração em printscreen da janela de configuração.
b. Anexar a script gerada pela ferramenta.
c. Comentem a utilidade deste tipo de ferramenta.

Case Study II



- **Regras para Firewall Interna**

	Interface 1		Interface 2	
Protocolo	**Inbound**	**Outbound**	**Inbound**	**Outbound**
Telnet	Sim(security)	Sim(security)	Não(all)	Sim(security)
FTP	Sim(Subnet)	Não(all)	Não(all)	Sim(Subnet)
Ping	Sim(all)	Sim(all)	Sim(all)	Sim(all)
Web	Sim(all)	Não(all)	Não(all)	Sim(all)
Email	Sim(all)	Não(all)	Não(all)	Sim(all)

- **Regras para Firewall Externa**

	Interface 1		Interface 2	
Protocolo	**Inbound**	**Outbound**	**Inbound**	**Outbound**
Telnet	Sim(security)	Não(all)	Não(all)	Sim(security)
FTP	Sim(Subnet)	Não(all)	Não(all)	Sim(Subnet)
Ping	Sim(security)	Não(all)	Não(all)	Sim(security)
Web	Sim(all)	Sim(all)	Sim(all)	Sim(all)
Email	Não(all)	Sim(all)	Sim(all)	Não(all)

- **Configuração da firewall**

O endereçamento a usar está listado na tabela seguinte.

IP a usar	Endereço	Subnet Mask
Subnet Interna	172.16.10.0	255.255.255.0
Security Host	172.16.10.10	255.255.255.0
Servidor Web Interno	172.16.100.100	255.255.0.0
Int. 1 Firewall interna	172.16.100.1	255.255.0.0
Int. 2 Firewall interna	192.168.10.1	255.255.255.0
DMZ - Servidor email	192.168.10.100	255.255.255.0
DMZ - Servidor Web	192.168.10.101	255.255.255.0
Int. 1 Firewall Externa	192.168.10.2	255.255.255.0
Int. 2 Firewall Externa	10.10.10.10	255.255.0.0

Antes de mais é necessário planear as “chains” e “rules” que vão ser usadas. É necessário decidir se são criadas novas “chains”, ou usar as “default chains”. Planeie primeiro, em papel por exemplo, todo o processo antes de avançar para a implementação. De seguida indico uma lista de alguns passos genéricos que podem usar para esta atividade.

- Decida se vai modificar as políticas default, e anote como as mudava.
- Decida se quer criar novas rules/chains para gestão, e registe a decisão.
- Em Linux, se criar novas chains, defina os saltos para essas chains.
- Defina o objetivo geral da firewall.
- Registe as regras que vai configurar.
- Descreva como vai verificar que essas rules e chains estão correctas.

Assim que tenha tudo planeado é tempo para configuração.

1. Cenário

a. Preparar o cenário com recurso a máquina virtuais, usando o virtual Box, e com software disponível no LAB P5.
b. O módulo de firewall a usar deve ser o iptables. Podem usar qualquer versão de Linux para o efeito. As restantes máquinas podem ser Linux ou Windows. Façam um desenho pormenorizado da vossa implementação

2. Configuração

a. Implementar as politicas de firewall descritas na introdução do case study II.
    i. Descrever todos os passos da configuração das regras. Siga as guidelines indicadas na introdução.
    ii. Indicar com comentários elucidativos toda a configuração efetuada.
    iii. Usar sempre que possível “user-defined chains” para melhor leitura e compreensão das regras.

3. Demonstração

a. Listar todas as chains.
b. Demonstrar que as políticas implementadas estão de facto a funcionar.
c. Identificar os protocolos inseguros e propor alterações ás tabelas de regras de firewall listadas na introdução.

4. IPS/IDS

a. Baseando-se no desenho apresentado, e no case study II, onde colocava um Network IPS/IDS com o objetivo de deteção e ação sobre o tráfego proveniente da Internet? Justifique.
b. Vamos aproveitar o cenário para analisarmos o funcionamento dos IPSs. Vamos Considerar que o Host

representa o mundo exterior, os servidores WEB e Mail são máquinas da empresa (internas), e a firewall externa será o IDS/IPS, e estará inline com todo o trafego proveniente do exterior e para o exterior.

i. Retirar as regras de firewall colocadas na máquina firewall externa/Host.
ii. Instalar na ex-Firewall/Host externa o software snort e todos os softwares de apoio.
iii. Analisar as assinaturas existentes. Mostrar evidencia.
iv. Configurar alerta para trafego ICMP (pings) do exterior (host).
v. Verificar nos logs o registo do alerta do ponto anterior.
vi. Configurar para barrar o trafego anterior.
vii. Demonstração da configuração de IDS até ao ponto vi.
viii. Configurar alerta para acesso a uma página com referência á palavra “Adult”. Origem nas máquinas internas. Demonstração dessa configuração.
ix. Configurar alerta para detectar login de um utilizador root em ftp (serviço a instalar num dos servidores do cenário). Demonstrar.
x. Configurar alerta e log para deteção de pacotes com origem da Internet com flags de controle FIN, SYN e Reset a 1. Demonstrar.
xi. Configurar alerta e log de passwords de paginas em http. Origem do interior da empresa para a internet. Demonstrar.

Conclusão

1. Entre os dois case studies, indique qual o que garante melhor proteção da rede interna e serviços disponibilizados para a WEB? Justifique.