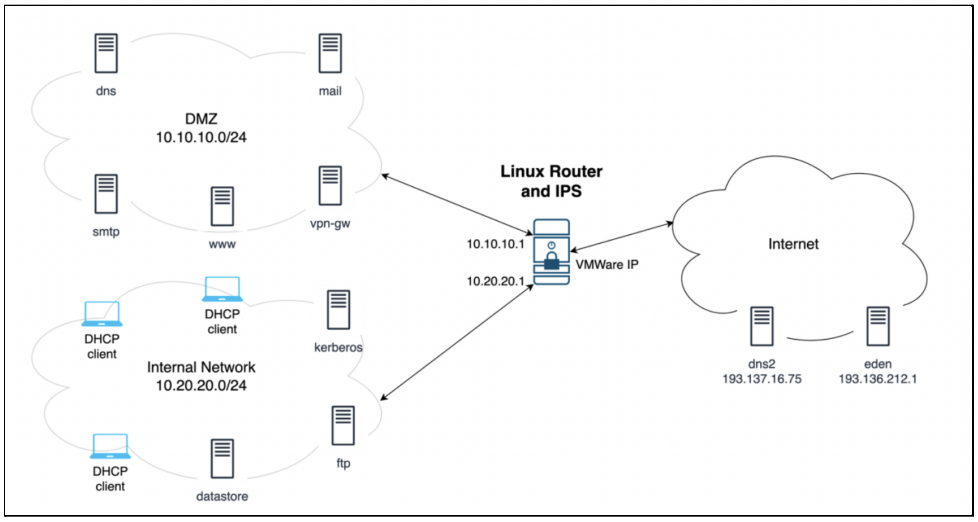
1 2 9 0

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D COIMBRA

Segurança em Tecnologias da Informação

Relatório do Trabalho Prático 2



Mestrado em Engenharia Informática

Sistemas Inteligentes

2021/2022

PL2	Gabriel Fernandes	2018288117	gabrielf@student.dei.uc.pt
PL2	Miguel Rabuge	2018293728	rabuge@student.dei.uc.pt

Índice

1. Cenário Experimental

O cenário experimental é composto por 3 máquinas virtuais e a *host*.

As máquinas virtuais **IN_VM** e **DMZ_VM**, simulam as redes *Internal Network* (10.20.20.0/24) e *DMZ* (10.10.10.0/24) e os serviços presentes nestas, respectivamente.

A última máquina virtual, **Router**, funciona como router e IDS/IPS, permitindo a ligação entre *internal network*, *DMZ* e *internet*, bem como protegendo de possíveis ataques SQLi / XSS.

A *Internet* é simulada pela máquina *host* das 3 máquinas virtuais.

2. Configurações

Neste capítulo descrevemos a forma como configuramos os demais requisitos deste trabalho prático.

2.1. Router VM

Nesta secção abordamos os requisitos configurados do router. Estes podem ser encontrados nos ficheiros src/router/firewall/configure.bash para as regras de IPTables e src/router/snort/configure.bash para o snort. Estes scripts encontram-se bem documentados e são, por natureza, um complemento de peso a este relatório.

Nota: Para o funcionamento do ftp em modo passivo, adicionamos o módulo **ip_conntrack_ftp**.

2.1.1. Interfaces

O **Router** está equipado com 3 interfaces de rede, uma para cada rede que vai ligar (*DMZ, internal network* e *internet*). O endereço de IP atribuído às interfaces das redes privadas é o 3º da respetiva rede (x.x.x.2), enquanto que o da interface que ligada à *internet* é atribuído automaticamente pelo vmware e pode variar de *host* para *host*.

2.1.2. Forwarding

Para que uma máquina linux possa operar como *router*, é necessário permitir o *forward* de ligações, utilizando, por exemplo, o comando

```
sudo sysctl -w net.ipv4.ip_forward=1
```

2.1.3. IPTables FILTER

As *chains* INPUT e FORWARD são configuradas com a política DROP. As várias regras necessárias ao *input* e *forward* das ligações pedidas foram colocadas regras nas *chains* INPUT e FORWARD, respetivamente.

Para permitir as ligações de retorno, colocámos uma regra que permite o *forwarding* de todas as ligações ESTABLISHED e RELATED (por via do módulo state do iptables).

De maneira a permitir o funcionamento do snort inline, adicionamos em como primeira regra na *chain* FORWARD a seguinte regra:

```
sudo iptables -A FORWARD -j NFQUEUE --queue-num 0
```

fazendo com que todos os packets recebidos (com destino a outra máquina) sejam colocados numa *queue* para serem analisados pelo snort.

2.1.4. IPTables NAT

Para as ligações entre a *Internet* e redes privadas, *DMZ* e *Internal network*, é necessário efetuar a tradução dos endereços de destino ou fonte. Caso seja uma ligação de umas das redes privadas para a internet, é preciso adicionar a regra que altera a *source* para o ip da interface do *router* que está na *internet* à *chain* POSTROUTING. Se a ligação for da *internet* para uma das redes privadas, é necessário adicionar uma regra que mude a *destination* para um ip da rede privada em questão à *chain* PREROUTING.

2.1.5. SNORT

Como mencionado acima, o ficheiro de configuração do snort contém a instalação de todas as dependências necessárias ao normal funcionamento do mesmo, bem como a definição de regras e o comando para executar o IDS/IPS inline, em conjunto com o IPTables.

2.2. DMZ VM

Nesta encontram-se os serviços *www*, *smtp*, *dns*, *mail*, *vpn-gw* e tem apenas uma interface de rede com o endereço ip 10.10.10.3 e *default gateway* 10.10.10.2 (IP da interface do **Router** na rede *DMZ*).

2.3. Internal Network VM

Na **Internal Network VM** estão presentes os serviços *ftp*, *datastore*, *kerberos* e *dhcp clients*. Esta é composta por uma interface de rede, à qual é atribuído o endereço IP 10.20.20.3. O *default gateway* é o endereço 10.20.20.2 (ip da interface do **Router** na rede *internal network*).

3. Descrição dos Ataques

Neste capítulo descrevemos os ataques que detectámos e prevenimos.

3.1. SQL Injection

Nesta secção exemplificamos os dois ataques que protegemos, recorrendo à sua descrição (formulário) bem como ao comando do snort respetivo.

3.1.1. OR SQLi Detection and Prevention

Formulario: Um user, através de uma rest api conectada ao vpn-gw, coloca no campo de pesquisa, em vez de apenas o seu nome, "Nome or 1 = 1", conseguindo todos os registos da tabela em vez dos que lhe dizem respeito.

```
drop tcp any any -> 10.20.20.3 5432
(
      msg: "OR SQLI Detected";
      content: "or";
      nocase;
      sid:100000008;
)
```

3.1.2. Comma SQLi Detection and Prevention

Formulario: Um user, através de uma rest api conectada ao vpn-gw, coloca no campo de pesquisa, em vez de apenas o seu nome, "Nome; Drop table users", levando a que a tabela users seja apagada.

```
drop tcp any any -> 10.20.20.3 5432
(
      msg: "COMMA SQLI Detected";
      content: ";";
      Nocase;
      sid:100000009;
```

```
)
```

3.2. Cross Site Scripting

De forma semelhante à secção anterior, exemplificamos os dois ataques que protegemos, recorrendo à sua descrição (formulário) bem como ao comando do snort respetivo.

3.2.1. Image Tag XSS Detection and Prevention

Formulario: Um user, através de um *form http* de uma página *web*, coloca no campo de pesquisa, em vez do seu nome, "<img src=", levando a que um script malicioso contido num .svg seja executado.

```
drop tcp any any -> 10.10.10.3 80
(
      msg: "XSS <img src= tag Detected";
      pcre: "/< *img +src *=/i";
      sid:100000010;
)
```

3.2.2. Script Tag XSS Detection and Prevention

Formulario: Um user, através de um *form http* de uma página *web*, coloca no campo de pesquisa, em vez do seu nome, "<script>", levando a que um script malicioso seja executado.

```
drop tcp any any -> 10.10.10.3 80
(
      msg: "XSS <script> Detected";
      pcre: "/< *script *>/i";
      sid:100000011;
)
```

4. Testes

Relativamente aos testes realizados a tabela seguinte sintetiza os resultados obtidos:

Tasks	From	To	Tested
Firewall configuration to protect the router			
Drop all communications entering the router system except:	Anyone	Anyone	TRUE
DNS (TCP + UDP)	Internal into Router Internet IP	Internet	TRUE
	DMZ into Router Internet IP	Internet	TRUE
SSH	Internal	Router Internal IP	TRUE
	vpn-gw server	Router DMZ IP	TRUE
Firewall configuration to authorize direct communications (without NAT):			
Drop all communications between networks except:	Anyone	Anyone	TRUE
DNS (TCP + UDP)	Internal	*dns server*	TRUE
	Internet	*Router Internet IP into dns* server	TRUE
	dns server into Router Internet IP	*dns2* & Other servers (internet)	TRUE
Synchronize the contents of DNS zones (TCP)	*dns* server into Router Internet IP	*dns2* server	TRUE
	dns2 server	*Router Internet IP into dns* server	TRUE
SMTP	Internal	*smtp* server	TRUE
	Internet	*Router Internet IP into smtp* server	TRUE
POP	Internal	*mail* server	TRUE
	Internet	*Router Internet IP into mail* server	TRUE
IMAP	Internal	*mail* server	TRUE
	Internet	*Router Internet IP into www* server	TRUE
HTTP	Internal	*www* server	TRUE
	Internet	*Router Internet IP into www* server	TRUE
HTTPS	Internal	*www* server	TRUE

	Internet	*Router Internet IP into www* server	TRUE
OpenVPN	Internal	*vpn-gw* server	TRUE
	Internet	*Router Internet IP into vpn-gw server*	TRUE
PostgreSQL	VPN Clients	*datastore* server	TRUE
Kerberos v5 (max: 10 connections)	VPN Clients	*kerberos* server	TRUE
Firewall configuration for connections to the external IP address of the firewall (using DNAT):			
FTP (active)	Internet	Router Internet IP into *ftp* server	TRUE
FTP (passive)	Internet	Router Internet IP into *ftp* server	O serviço teria de existir
SSH	*eden*	Router Internet IP into *datastore* server	Não nos é possível
	dns2	Router Internet IP into *datastore* server	
Firewall configuration for communications from the internal network to the outside (using SNAT)			
DNS	Internal into Router Internet IP	Internet	TRUE
HTTP	Internal into Router Internet IP	Internet	TRUE
HTTPS	Internal into Router Internet IP	Internet	TRUE
SSH	Internal into Router Internet IP	Internet	TRUE
FTP (active)	Internal into Router Internet IP	Internet	TRUE
FTP (passive)	Internal into Router Internet IP	Internet	O serviço teria de existir

Recorremos ao `netcat`, `wget` e `nslookup`, para testar as várias ligações entre as redes. Dado que os serviços não foram implementados, o teste para a verificação de conexão a esses portos, foi feito através da flag `-l` do mesmo comando.

5. Referências

OpenVPN Ports
Advanced Option Settings On The Command Line | OpenVPN

PostgreSQL Ports
Port 5432 (tcp/udp) :: SpeedGuide

Kerberos v5 Ports
2.2 Active Directory Authentication

SSH ports
Are SSH destination and source ports identical (symmetric ports)? - Stack Overflow

XSS Attacks
Detect SQL Injection and Cross Site Scripting attacks

XSS img Attack
What could an "<img src=" XSS do? - Information Security Stack Exchange

SNORT Users Manual
Snort Manual

Material das Aulas Teóricas e Práticas STI@2022

Granjal, J. (2017). Segurança Prática em Sistemas e Redes com Linux (02–2017th ed.). FCA.