INSTITUTO
SUPERIOR
TÉCNICO

Instituto Superior Técnico
Relatório do Projecto
GRS-Gestão de Redes e Serviços

2ªEntrega-Monitorização e IDS

Bernardo Simões 63503
Guilherme Vale 64029

1.Finalização da 1ª Entrega

1.1 Servidor DNS slave

O servidor slave da empresa não estava devidamente configurado devido a problemas de permissões do servidor *master* que não o autorizava a passar informação para o *slave*. Para corrigir este problema teve mudou-se algumas permissões no servidor *DNS* primário (ver ficheiros: **dnsempresa1.startup** e **dnsempresa1/etc/default/bind9**)

Para testar que ambos os servidores estão a funcionar correctamente observou-se o *output* do comando **tail /var/log/daemon.log** e correram-se os comandos:

dig www.empresa.pt @190.12.131.1" e "dig www.empresa.pt @190.12.131.1
(190.12.131.1: dns primário empresa.pt e 190.12.131.2: dns secundário empresa.pt)
dig www.empresa.pt @190.12.192.1" e "dig www.empresa.pt @190.12.192.2
(190.12.192.1: dns pt e 190.12.192.2: dns root)

Em vários pontos dentro da empresa e também dentro do *ISP*, a tradução de nomes foi sempre possível.

1.2 Iptables no nó bastião

Na primeira entrega de projecto as *IpTables* do nó bastião a bloqueavam o tráfego na *chain input*, dado que todo o tráfego que passa no bastião apenas passa pela *chain forward,* nenhum tráfego era bloqueado. Esse erro foi corrigido e a *chain forward* está bloqueada por *white list*.

1.3 Servidor de email

Nesta segunda entrega de projecto corrigimos os problemas do servidor de e-mail. O mail está configurado no servidor *webmail* da *dmz*, com os servidores de *exim [Exim], pop3d* e *imapd*. Cada pc da

empresa tem uma conta de email associada. Cada utilizador tem de fazer *login* no *pine* para ter acesso á conta de *e-mail*.

Para testar o *webmail* internamente utilizamos o *pine* dentro da empresa enviando emails entre os clientes. Para testar o webmail externamente utilizamos *telnet* do *pcispconfig* da seguinte maneira:

telnet webmail.empresa.pt 25
MAIL FROM: <user>@empresa.pt
RCPT TO:<outro_user>@empresa.pt
DATA: Ola estou te a mandar um mail de fora da empresa
.

1.4 Outros Melhoramentos

O *webserver* e o router passaram a ter 64Mb de *RAM* em vez de 32 pois não conseguiam correr o *portmap*. Foram adicionados e autenticados *users* no *startup* dos pcs dos escritórios.

2. Monitorização da Rede

2.1.1 IDS: SNORT

O *SNORT* foi configurado no pc *bastião* e num segundo pc sem interface IP que monitoriza o tráfego entre o router e a *DMZ*.

Para configurar o *SNORT* basta editar o ficheiro **/etc/snort/snort.conf** onde se tem de dizer explicitamente a localização dos servidores *SNMP*, *WEB, email* e *SQL* entre outros. Como queriamos verificar ataques de injecção de *SQL* e não temos nenhuma base de dados *SQL* instalada, deixamos essa entrada como *any*.

Neste mesmo ficheiro de configuração pode-se adicionar e remover listas de possíveis ataques. Como não era pedido não foram alteradas as listas de ataques entre o nó bastião e o novo pc adicionado para monitorizar a *DMZ*. No entanto, caso o *SNORT* fosse utilizado em uma empresa real as regras teriam de ser escolhidas de forma ponderada pois os ataques feitos a uma *DMZ* são totalmente diferentes dos ataques feitos à zona dos funcionário, o que pode gerar um grande numero de falsos positivos. Quanto maior for a lista de "ataques" maior será a quantidade de *RAM* consumida pelo *SNORT*.

O *SNORT* tem de ser corrido à mão de forma a ser possível ver na consola os alarmes, em tempo real. No comando para correr o *snort* passa-se o argumento **-i br0** para correr na interface bridge onde passa o tráfego.

Devido ao *SNORT* consumir muita memória, alteramos a quantidade de *ram* dos pc's (que correm o *SNORT*) para 512 Mb.

2.1.2 Regras Para Identificar Ataques SQL

A regra para identificar ataques SQL foi adicionada ao ficheiro **/etc/snort/rules/grs.rules** e este ficheiro foi adicionado ao **/etc/snort/snort.conf**

2.2 Servidor SNMP

O servidor *SNMP* foi configurado para correr no servidor *web/mail* e no router da empresa. Ambos os servidores tem um utilizador '*MRTG*' que pode ler os valores das *MIBs*.

2.4 MRTG e PC de Monitorização

2.4.1 PC de Monitorização

Foi criado um novo pc, ligado ao *switch* do primeiro piso, com uma interface *tap* que atribui o **IP 192.168.1.2** ao pc monitor e **192.168.1.1** ao pc onde corremos o netkit de forma a ser possivel comunicar entre o *netkit* e a máquina que corre o *netkit*.

No entanto a interface *tap* adiciona o **IP 192.168.1.1** como *default gateway* ao PC monitor, esse *default gateway* terá de ser removido com o comando:

route del default gw 192.168.1.1

Caso contrário o pc monitor perde o router como *default gw* o que origina alguns problemas de encaminhamento.

Foi também instalado um servidor *Apache* e adicionada uma página *web* para facilitar o visionamento dos ficheiros gerados pelo *MRTG*.

2.4.2 MRTG

O *MRTG* foi configurado em ficheiros distintos:

router.cfg: tráfego das interfaces do router
webmail-info.cfg: informação do sistema do servidor *webmail*
webmail-mrtg.cfg: informação do tráfego do servidor *webmail*
todos.cfg: ficheiro que irá correr todos os anteriores de uma só vez.

Os ficheiros **router.cfg, webmail-info.cfg e wemail-mrtg.cfg** são configurados com as *MIBS* de maneira a satisfazer o pedido do enunciado de projecto. De notar que o *CPU* das *VMS* do *netkit* nunca passa de zero (mesmo que seja feito um *forkbomb*) portanto o gráfico não se altera, isto foi verificado correndo o comando *top*.

O ficheiro ***todos.cfg*** diz ao *MRTG* para correr como *daemon* em intervalos periódicos de 5 minutos. Desta forma não é necessário estar sempre a correr o *MRTG* à mão.

No ficheiro *startup* do pc de monitorização é corrido o *indexmaker* de forma gerar as paginas *HTML* para visualização a monotorização dos pc's. Para ver esta página basta ir ao browser e aceder ao **IP 192.168.1.2.**

O funcionamento das *MIBS* foi testado ao longo da configuração do *MRTG,* com a utilização das ferramentas *snmpwalk* e *snmpget*

2.5 Bloqueio do Porto Aberto pelo SNMP Não Usado Pelo MRTG

Foi utilizada a ferramenta *netstat* para encontrar o porto que era aberto pelo *snmp* para além do porto 161, é o porto 199, o comando foi o seguinte:

"netsat -anp --tcp"

Como o router funciona por *white lists* não foi preciso fechar especificamente o porto pois este já se encontra com o acesso negado. No servidor webmail foi adicionada uma regra de *iptables*, ao ficheiro *startup,* para bloquear a *chain* de *input* e *output* nesse mesmo porto.

3.Notas Finais

Nesta segunda entrega conseguimos cumprir não só os requisitos propostos da segunda entrega, mas também os objectivos da primeira entrega