CURSO: Tecnologo em Sistemas para Internet - 4º período – Noturno

UNIDADE CURRICULAR: Sistemas Operacionais l - TURMA:

PROFESSOR: Genair C. Viana

Prática 3:

- Instalar e configurar o CSF no Debian Debian 8.3

02/05/2023

Essa aula vai valer como trabalho, será dado 2 pontos do 2º bimestre

Configurando o CSF no firewall do servidor Debian Linux 8.3

Antes vamos resolver as dependências instalando o libwww-perl

#**apt install libwww-perl host**

libwww-perl (também conhecida como LWP) é uma coleção de módulos Perl que fornecem uma interface de programação (API) simples e coerente para a World-Wide Web.

Feito isso vamos para o CSF.

Instalando CFS

```
#cd /usr/src
#rm -fv csf.tgz
#wget https://download.configserver.com/csf.tgz
#tar -xzf csf.tgz
#cd csf
#sh install.sh
```

O CSF é um firewall que existe a bastante tempo e vem melhorado ao passar do tempo. Ele ajuda a filtrar ataques do tipo DoS e DDoS.

Primeiro instala o CSF em sua maquina administrativa, depois nos PCs clientes.

Agora que já está instalado vamos configurar.

Vamos até a pasta /etc/csf e abra o arquivo csf.conf com o editor de texto de sua preferencia, o meu é o editor vim.

#vim /etc/csf/csf.conf

Procurem no arquivo por:

TCP_IN =
TCP_OUT =
UDP_IN =
UDP_OUT =
TCP6_IN =
TCP6_OUT =
UDP6_IN =
UDP6_OUT =

Vamos aprender o editor vim

Comandos básicos:

:w -> salva o arquivo corrente.

ZZ -> salva o documento e sai do Vim. É conhecido como o comando “Zalva e Zai”. :)

:wq -> Salva o arquivo e sai do Vim

:w! -> O arquivo será salvo mesmo se aberto no modo somente leitura (readonly)

:q -> Sai do Vim. Se o arquivo não foi salvo, o programa emitirá um alerta.

:q! -> Força a saída, mesmo que o arquivo tenha sido modificado e não tenha sido salvo anteriormente

Comandos de busca:

/palavra - Busca pela palavra ou caractere em todo o texto

?palavra - Move o cursor para a ocorrência anterior da palavra

N - Repete o último comando / ou ?

Ctrl+g - Mostra o nome do arquivo, o número da linha corrente e o total de linhas

Comandos de substituição e deleção:

x - Deleta o caractere que esta sob o cursor

dw - Deleta a palavra, da posição atual do cursor ate o final

dd - Deleta a linha atual

D - Deleta a linha a partir da posição atual do cursor ate o final

Coloque as suas portas todos os que você quer ser aberto em seu servidor para o tráfego de entrada separadas por vírgula.

Exemplo:

TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"

Também abrir qualquer porta que você quer para o tráfego de saída

TCP_OUT = "20,21,22,25,53,80,110,113,443"

O mesmo vale para UDP_IN e UDP_OUT, lembrando que, estiver executando o serviço de DNS, então tem que abrir a porta 53 em UDP_IN como DNS porta 53 corridas em UDP em vez de TCP.

UDP_IN = "20,21,53"

Para permitir a saída traceroute 33434:33523 adiciona a lista

UDP_OUT = "20,21,53,113,123,33434:33523"

Adicione as portas que você precisará usar conforme necessário.
Procure por:

CT_LIMIT =

substitua por: **CT_LIMIT = "50"**

Procure por:

CT_PORTS =

Substitua o item acima pelas portas que você irá usar.

Exemplo:

CT_PORTS ="20,21,22,25,53,80,110,143,443,465,587,993,995"

Procure por:

SYNFLOOD =

Substitua por:

SYNFLOOD = "1“

Procure por:

SYNFLOOD_RATE =

Substitua por:

SYNFLOOD_RATE = "150/s"

Esta linha acima é para monitorar quando houver mais de 150 conexões por segundo por IP. Ela pode ser aumentada ou diminuída de acordo com seus critérios!

SYNFLOOD_BURST =

Substitua por:

SYNFLOOD_BURST = "200“

Nesta linha o IP é bloqueado temporariamente quando chegar a 200 conexões por segundo. Esta linha também pode ser aumentada ou diminuída de acordo com seus critérios!

Procure por:

UDPFLOOD = "0"

Substitua por:

UDPFLOOD = "1"

Procure por:

PORTFLOOD =

Substitua por:

PORTFLOOD = "22;tcp;20;5,80;tcp;150;5,2106;tcp;150;5,7777;tcp;150;5"

configuração acima é um exemplo, mas pode ser configurado com outros IPs também.

A configuração do **PORTFLOOD=** fará com que porta 22 tenha um limite de 20 conexões por IP a cada 5 segundos e as portas 80, 2106 e 7777 tenham um limite de 150 conexões a cada 5 segundos por IP. pode aumentar caso ache necessário!

Procure por:

PS_INTERVAL =

Substitua por:

PS_INTERVAL = "1500“

Procure por:

PS_LIMIT =

Substitua por:

PS_LIMIT = "20"

Finalizando as configurações, procure por:

TESTING = "1"

Substitua por:

TESTING = "0"

Agora salve o seu arquivo csf.conf e atualize-o em seu host.

Pronto, após ter feito toda a configuração iremos finalmente reiniciar o CSF.

Vá até o terminal root e execute o seguinte comando:

csf -u;csf –r

Deverá reiniciar o seu firewall e mostrar todas as configuraçoes ativadas por você!

Segue uma lista de comandos para gerenciar o firewall csf pelo SSH

csf -h / Mostra a ajuda

csf -l / Lista/ Mostra a configuração do iptables

csf -s / Inicia regras do firewall

csf -f / Limpa/Interrompe regras do firewall (Nota: lfd pode reiniciar o csf)

csf -r / Recarrega regras do firewall

csf -q / Reinicialização rápida (csf reiniciado pelo lfd)

csf -x / Desativa do firewall

csf -a <IP> / Libera um IP e adiciona-o em /etc/csf.allow

csf -ar <IP> / Remove um IP de /etc/csf.allow e deleta a regra

csf -d <IP> / Bloqueia um IP e adiciona-o em /etc/csf.deny

csf -dr <IP> / Desbloqueia um IP e remove-o de /etc/csf.deny

csf -df / Remove e libera todos os IPs em /etc/csf.deny

csf -g <IP> / Procura nas regras do iptables por um IP (incl. CIDR)

csf -t / Mostra a lista atual de IPs bloqueados temporariamente e o tempo até o desbloqueio

csf -tr <IP> / Remove um IP do bloqueio e liberação temporários