E-fólio B | Folha de resolução para E-fólio

UNIDADE CURRICULAR: SEGURANÇA EM REDES E COMPUTADORES

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

A preencher pelo estudante

NOME: Hélio Emanuel Soares de Sousa

N.º DE ESTUDANTE: 2000027

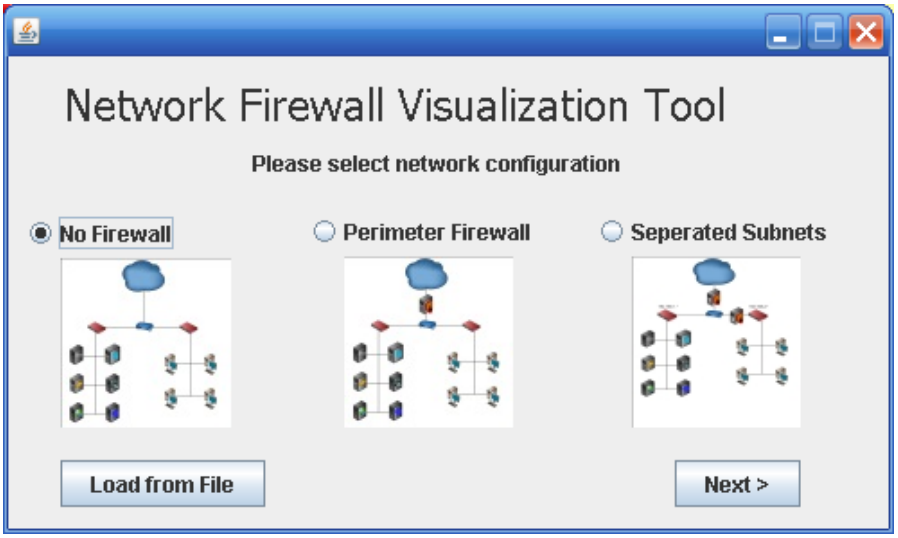
CURSO: Engenharia Informática

DATA DE ENTREGA: 2020-12-08

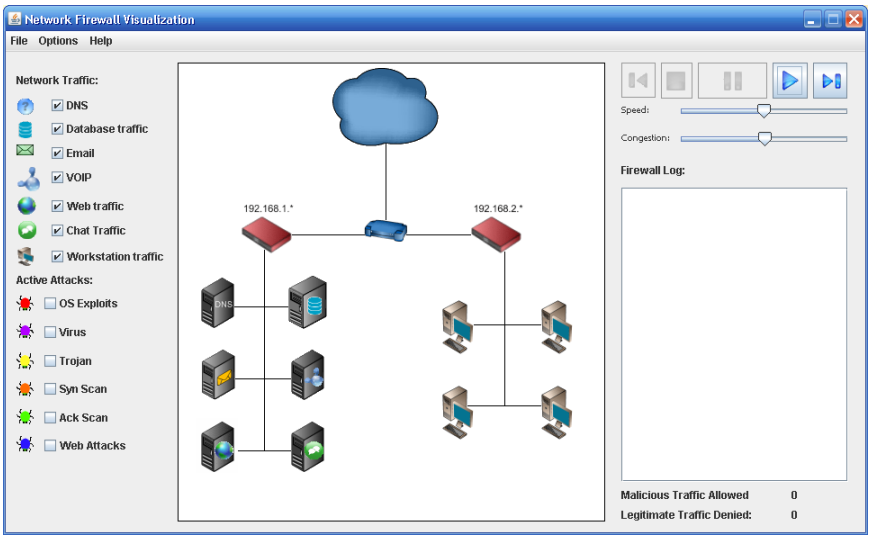
TRABALHO / RESOLUÇÃO:

Preparação do Ambiente

Execute o programa da “Network Firewall Visualization Tool” que foi disponibilizado. Deve obter o seguinte ecrã:

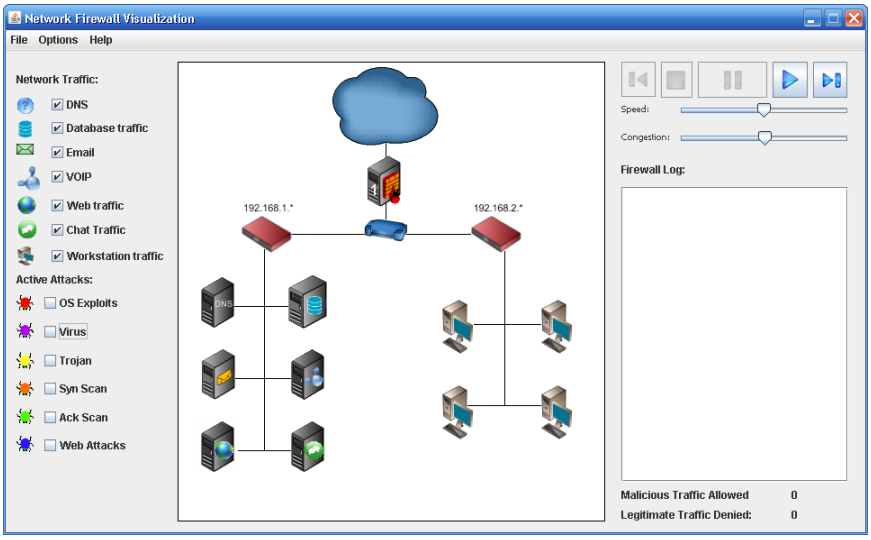


Selecione “No Firewall” e de seguida prima o botão “Next”. Aparecerá o seguinte ecrã:



Prima o botão  . Observe que o tráfego flui da “nuvem” ou da Internet para as máquinas clientes. Por defeito, não há tráfego malicioso fluindo para as máquinas. Clique na opção “OS Exploit”. Eventualmente, você verá um *bug* de cor vermelha fluir da Internet para a rede local e pousar em uma máquina, infetando a mesma. Depois de uma máquina ser infetada, ela é marcada como tal com o emblema "Não internacional" ou  . Vejamos como configurar uma *firewall* ajudará a prevenir tais infeções.

Iniciar uma nova sessão fazendo “File” -> “New” nas opções da ferramenta. Desta vez, escolher o “Perimeter Firewall”. O ecrã que se obtém deve ser semelhante ao seguinte:



Agora temos uma *firewall* entre a Internet (representada por uma nuvem) e seu roteador (*router*) de rede. Clique no botão play e veja o que acontece.

<u>Questão Nº 1</u> - Você vê o tráfego fluindo da Internet para o seu sistema ou da rede para a Internet? Explique porque ou porque não:

R:. Não consigo verificar tráfego fluindo da Internet (*cloud*) para o sistema, nem da rede interna para a Internet. A razão para esta ocorrência é a Firewall que está a bloquear toda e qualquer comunicação entre a rede interna e a rede externa, no teste que realizei deixei o programa correr durante 15 minutos para ver até onde iria e obtive cerca de 208 comunicações legítimas bloqueadas e zero comunicações maliciosas que conseguiram entrar na rede.

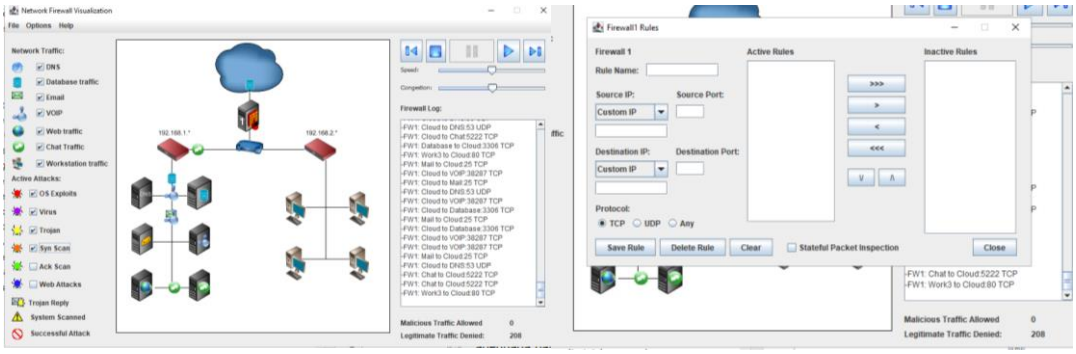


Imagem - 1 - Teste e regras da firewall

Para perceber melhor fui verificar as regras da firewall e constatei que não estão definidas nenhumas regras na firewall, assim sendo, e de acordo com a página 9 do dos apontamentos teoricos Cap 23-Firewalls a firewall deverá estar definida por defeito para a opção: *Default = discard: That wich is not expressly permitted is prohibited*.

Logo o que não é permitido é proibido, assim sendo, se não temos regras para permitir a entrada de tráfego então nenhum tráfego pode passar pela *firewall*.

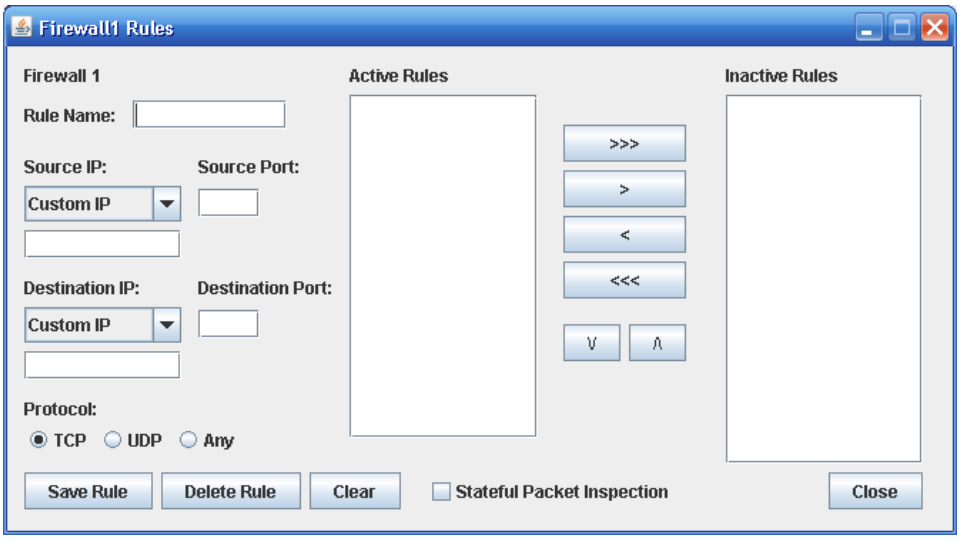
<u>Questão Nº 2</u> - Adicione alguns ataques ativos clicando em várias opções diferentes. Esses ataques são capazes de atingir sua rede? Você acha que seu sistema está seguro? O que há de errado com este cenário?

Usando a mesma configuração que na questão 1, nenhum ataque externo conseguiu entrar na rede, como seria expetável dado que nada pode entrar nem sair.

O sistema está seguro tal como está, para ataques externos. No caso, de um ataque a partir da rede interna, aparentemente, não existe controlo do tráfego na rede interna.

Este sistema tem de errado que não permite que comunicações legítimas possam chegar ao seu destinatário, o que invalida o propósito da existência das redes de comunicação, os objetivos da firewall apenas são atingidos quando ocorre a passagem de tráfego pela *firewall*, caso contrário a mesma não cumpre o seu objetivo de permitir a passagem de tráfego autorizado, e legitimo

<u>Questão Nº 3</u> - Configure seu *firewall* para permitir que o tráfego entre e saia da rede. Faça isso escolhendo "Options" na parte superior da ferramenta e defina as regras de *firewall*. Você deverá ver um ecrã semelhante ao seguinte:



Nomeie sua regra de firewall (normalmente com um nome que refere um determinado assunto ou ataque). A opção e porta “IP de origem” referem-se a como você deseja que o *firewall* reconheça uma determinada combinação de IP / porta de origem e responda. O destino é semelhante, mas com foco numa regra de destino. O objetivo de qualquer boa configuração de firewall é identificar o tráfego legítimo enquanto restringe o tráfego malicioso. Tente definir a seguinte regra de firewall:

Rule Name: DNS Rule

Source IP: DNS, Source Port: 53

Destination IP: Any, Destination port *

Protocol: Any.

Clique em “Save Rule”. Agora você deve ver a regra na caixa de regras ativas (“Active Rules”). Clique em “Close”, o que o levará de volta à janela da ferramenta de visualização do *firewall* de rede. Clique no botão “play” e veja o que acontece. Pode ser necessário mover a barra de velocidade para a direita para aumentar a velocidade do tráfego.

3.1 Qual tráfego agora flui pela *firewall*?

O único tráfego que atravessa a *firewall*, na direcção rede interna para a rede externa, é o tráfego DNS (resolução de nomes para os endereços IP) que tem origem na comunicação feita pelas workstations ao servidor da organização DNS que por sua vez emite pedidos de resolução de nomes para a rede de internet.

O contrário, já não ocorre, isto é, quando externamente existe um pedido de resolução de nome, a firewall bloqueia esse pedido. Para o efeito teria de ser criada uma segunda regra, em que unicamente se trocava o destinatário pelo emissor.

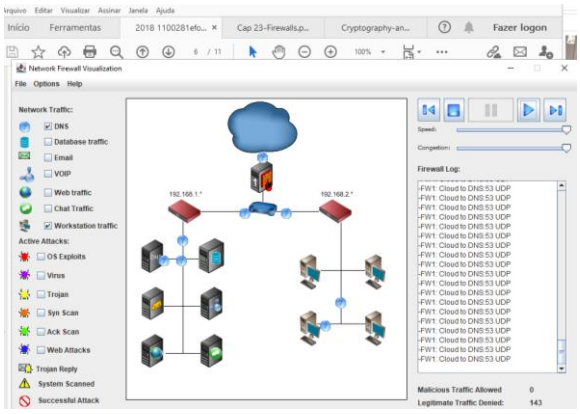


Imagem - 2 Teste ao trafego DNS que é aceite

3.2 Adicione alguns ataques ativos e observe se eles passam pelo *firewall*.

Como seria de esperar, não passam, pois nem sequer passa a resolução de nomes.

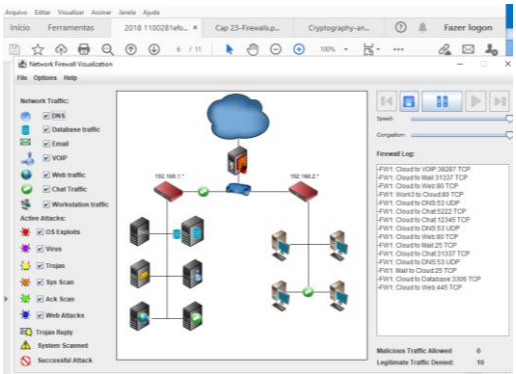


Imagem - 3 Teste de ataques após implementação da DNS Rule

3.3 Você diria que sua regra agora é suficiente para permitir que o tráfego flua para uma rede típica?

A regra criada não é suficiente para o tráfego fluir. Porque falta, resolução de nomes (DNS) na direção internet para a rede interna, tráfego em ambas as direções de e para a base de dados, email, VOIP, web e *chat traffic*. Em suma, falta praticamente tudo.

3.4 Porque ou porque não?

Porque apenas permite que os pedidos de resolução de nomes passem para a internet. Para resolver o problema, teremos de criar regras para permitir que todos os tipos de tráfego legitimo possam fluir através da *firewall*.

3.5 Algum dos ataques ativos agora funciona contra as máquinas atrás do *firewall*?

Não, todos os ataques neste momento estão a ser bloqueados, como é expetável.

Questão Nº 4 - Crie uma série de regras que pareçam proteger a rede de todos os ataques. Certifique-se de observar o tráfego legítimo negado e o tráfego malicioso permitido na parte inferior direita do ecrã. Isso deve mostrar o quão bem suas regras estão funcionando.

4.1 Quantas regras você teve que escrever para proteger sua rede?

Primeiro temos de definir o que é tráfego legitimo, e tendo por base (Fulton, et al., Help Documentation, 2020) encontramos a definição dos tipos de tráfego legitimo para esta aplicação: DNS, Database, Email, VOIP, Web, Chat.

Pela análise dos conteúdos dados em (Mamede, 2020) e em (Stallings, 2017) a definição destes tipos de tráfego legítimos está correta, e é expetável que os utilizadores desta rede possam comunicar sem interferências por parte da *firewall* recorrendo a este tipo de tráfego. Com base nesta informação, teremos de permitir que passem pela firewall de e para a internet, dado que são legítimos e pretendemos que a nossa rede cumpra a sua função de comunicação.

Assim sendo, teremos de ter 6 regras para cada tipo de tráfego legitimo na direção intranet -> internet e depois outras 6 na direcção internet -> intranet.

Por fim, é necessário adicionar mais uma regra que permita a ligação entre Workstations e a internet, isto é aceder à internet, porto 80, já o oposto é interdito dado que não faz sentido que alguém pretenda aceder diretamente aos IP´s das Workstations em contexto empresarial, em questões particulares poderá fazer sentido para aplicações de remote desktop, para aceder diretamente a uma workstation teremos de ter uma solução como por exemplo uma Watchguard, que tendo em conta o aumento brutal do trabalho remoto passaram a ser ainda mais importantes.

4.2 Você conseguiu proteger a rede completamente?

Não foi possível proteger completamente a rede. Fiz uma análise por tipologia de tráfego malicioso, deixei o programa correr durante 5 minutos para cada tipo de ataque individual, e depois uma simulação com todos os ataques definidos. Em baixo, apresento os resultados da simulação:

OS Exploits – na simulação executada com as regras definidas nenhum tráfego malicioso desta tipologia consegui passar a firewall, dado que nenhum tráfego é permitido através do porto 445/TCP com o conjunto de regras criadas (Fulton, et al., Help Documentation, 2020).

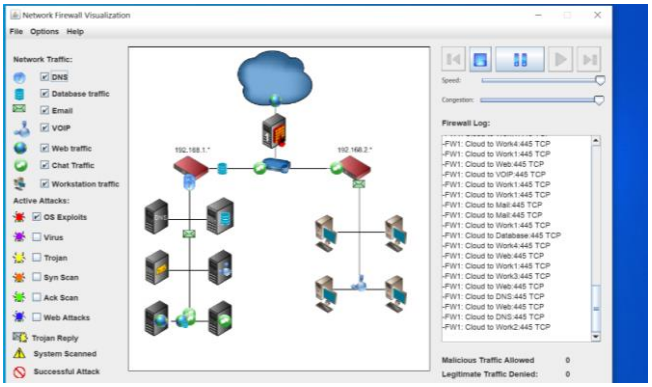


Imagem - 4 Simulação OS Exploits

Virus - na simulação executada com as regras definidas nenhum tráfego malicioso desta tipologia consegui passar a firewall, o vírus sistematicamente tentou utilizar o porto 12345/TCP, mas dado não ser um porto autorizado o tráfego é impedido pela firewall (Fulton, et al., Help Documentation, 2020).

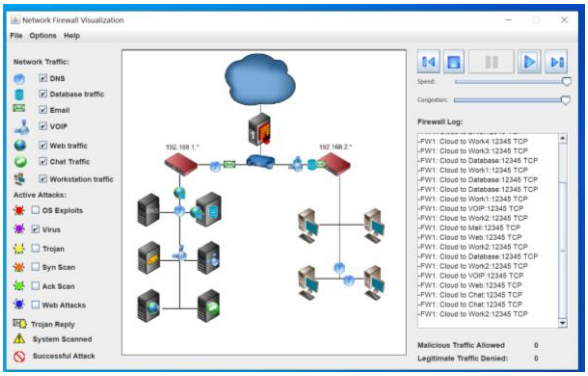


Imagem - 5 Simulação Virus

Trojan - na simulação executada com as regras definidas nenhum tráfego malicioso desta tipologia conseguiu passar a firewall, o vírus sistematicamente tentou utilizar o porto 31337/TCP, o tráfego é impedido pela firewall, tal como no caso do vírus, pois o mesmo é não autorizado (Fulton, et al., Help Documentation, 2020).

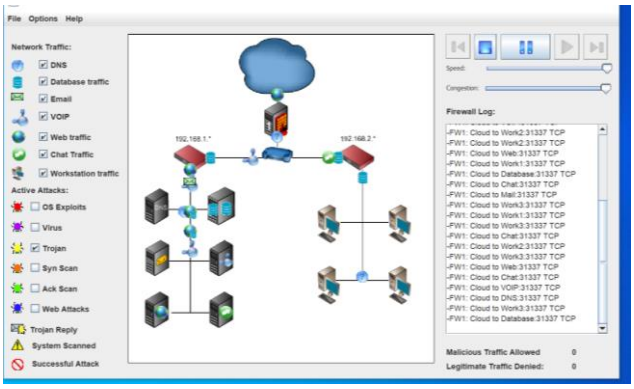


Imagem - 6 Simulação Trojan

Syn Scan – este tipo de ataque nesta simulação seleciona de forma aleatória um host da rede como sendo a sua morada de destino (ip de destino) e depois tenta passar pela firewall. Como defini regras para deixar passar tráfego legitimo eventualmente o Syn scan conseguirá passar e irá obter a confirmação dos dados de IP e o respetivo Porto do host, porque a regra assim o permite. Neste momento, não existe forma de verificar se um dado packet é ou não legitimo, pois o mesmo para a firewall é legitimo dado que a firewall apenas está a controlar números de ip e portos, não faz o controlo do conteúdo do packet. Eventualmente, acabará por obter todos os ip´s e portos dos hosts que estejam a comunicar através do protocolo TCP, pelo que o servidor DNS não será infetado pois está a comunicar unicamente através do protocolo UDP. Os IP´s que comunicam com a internet ficaram comprometidos e o intruso pode começar a explorar o porto que se encontra aberto (Fulton, et al., Help Documentation, 2020).

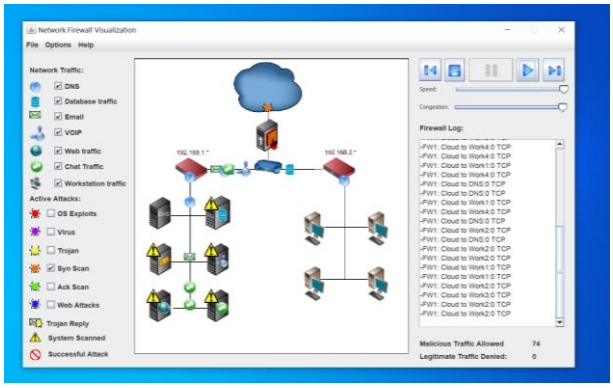


Imagem - 7 Simulação Syn Scan

Ack Scan – este tipo de ataque tira partido da vulnerabilidade das clássicas *packet filtering firewall* que não guardam o estado de pacotes prévios e como tal assume que quando um pacote ack é enviado para a rede assume que alguém dentro da rede enviou um pacote syn para tentar criar uma conexão fora da firewall. É exatamente, para estas situações que a tipologia *Stateful Packet Inspection Firewall* foi desenvolvida, pois mantém uma lista das conexões atualmente ativas e os respetivos

portos, colocando a firewall em *Stateful* previne estes ataques (Fulton, et al., Help Documentation, 2020) e (Fulton, et al., Firewall visualization project, 2010).

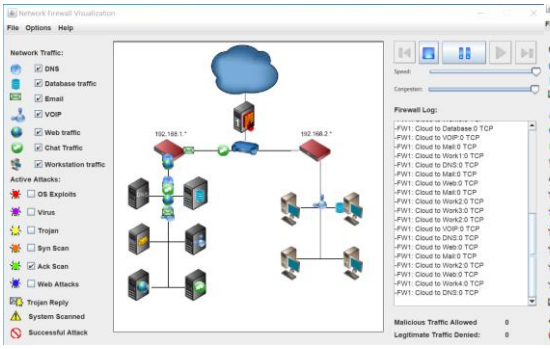


Imagem - 8 Simulação Ack Scan sem Stateful

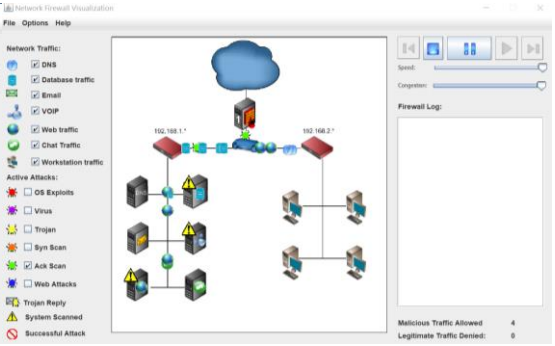


Imagem - 9 Simulação Ack Scan com Stateful

Web Attacks – São ataques direcionados a um servidor ou recurso web, pelo que são enviados os pacotes através do porto 80, pelo que a firewall não tem possibilidade de os controlar dado que não tem a capacidade de realizar investigação ao conteúdo de um dado pacote como por exemplo possui um sistema de prevenção de intrusos. Consequência, todos os ataques que são realizados para serviços web não serão parados pela firewall (Fulton, et al., Help Documentation, 2020).

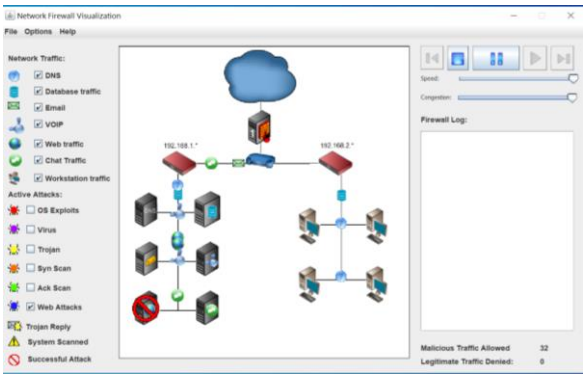


Imagem - 10 Simulação Web Attacks

Todos os ataques ativos – Analise feita para saber se o Syn Scan tem efeito nos restantes ataques. Nota-se que nesta simulação não, mas é provável que o intruso que realize o Syn Scan utilize a informação que o mesmo devolveu para enviar tráfego malicioso através dos portos e IP´s que descobriu estão abertos ao tráfego.

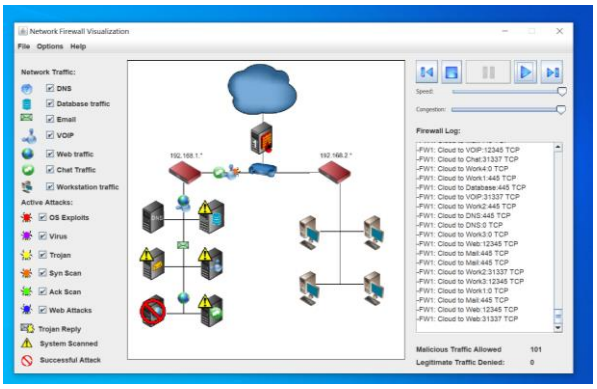


Imagem - 11 Simulação todos ataques ativos

Nota Final: Prova-se que a firewall não irá impedir todos os ataques, mas melhora significativamente a segurança, que tem de ser complementada com sistemas de prevenção de intrusões, como por exemplo: Honeypots.

4.3 Que tipo de regras você criou?

Apenas criei regras de *Allow*, isto é, regras que permitem que um dado tipo de tráfego possa fluir pela firewall, dado que todo o restante tráfego é automaticamente bloqueado e a aplicação não permite criar regras mais complexas como alguns dos exemplos dados na página 10 de Cap 23-Firewalls.

Como nota, um simples *packet filtering firewall* tem de permitir tráfego de entrada para a rede em portos de número muito altos (>1024 e < 65535) e isto cria uma vulnerabilidade que pode ser explorada por utilizadores não autorizados. Por esse motivo, selecionei a opção *Stateful Packet Inspection Firewall*, dado que este tipo de *firewall* melhora as regras relativas aos tráfegos de TCP criando um directório de conexões TCP de saída (*outbound*), sendo esse diretório (tabela) usado pelo *packet filter* para filtrar o tráfego de entrada (*inbound)*. Não é bem uma regra de firewall, enquadra-se mais numa tipologia de firewall diferente, mas dado que melhora a segurança da rede optei por a implementar, e esta pergunta aparenta ser o local mais apropriado para o referir (Fulton, et al., Help Documentation, 2020).

4.4 Liste-as todas e indique a finalidade de cada uma.

Em baixo, listo todas as regras criadas para esta rede. A letra E para entrada de trafego e a letra S para Saída de trafego:

Rule Name	Source IP	Source Port	Destination IP	Destination Port	Protocol
E DNS Rule	Any *.*.*.*	*	DNS 192.168.1.5	53	UDP
S DNS Rule	DNS 192.168.1.5	53	Any *.*.*.*	*	UDP
E DB Rule	Any *.*.*.*	*	Database 192.168.1.233	3306	TCP
S DB Rule	Database 192.168.1.233	3306	Any *.*.*.*	*	TCP
E Mail Rule	Any *.*.*.*	*	Mail 192.168.1.136	25	TCP
S Mail Rule	Mail 192.168.1.136	25	Any *.*.*.*	*	TCP
E VOIP Rule	Any *.*.*.*	*	VOIP 192.168.1.136	38287	TCP
S VOIP Rule	VOIP 192.168.1.136	38287	Any *.*.*.*	*	TCP
E Chat Rule	Any *.*.*.*	*	Chat 192.168.1.68	5222	TCP
S Chat Rule	Chat 192.168.1.68	5222	Any *.*.*.*	*	TCP
E Web Rule	Any *.*.*.*	*	Web 192.168.1.114	80	TCP
S Web Rule	Web 192.168.1.114	80	Any *.*.*.*	*	TCP
S WK1-4	Custom IP 192.168.2.*	80	Any *.*.*.*	*	TCP

Finalidade de cada regra:

E DNS Rule – permite a entrada de tráfego DNS através da firewall.

S DNS Rule – permite a saída de tráfego DNS através da firewall.

E DB Rule – permite a entrada de tráfego Database através da firewall.

S DB Rule – permite a saída de tráfego Database através da firewall.

E Mail Rule – permite a entrada de tráfego Mail através da firewall.

S Mail Rule – permite a saída de tráfego Mail através da firewall.

E VOIP Rule – permite a entrada de tráfego VOIP através da firewall.

S VOIP Rule – permite a saída de tráfego VOIP através da firewall.

E Chat Rule – permite a entrada de tráfego Chat através da firewall.

S Chat Rule – permite a saída de tráfego Chat através da firewall.

E Web Rule– permite a entrada de tráfego Web através da firewall.

S Web Rule – permite a saída de tráfego Web através da firewall.

S WK1-4 – permite a saída de tráfego das estações de trabalho através da firewall para a internet através do porto 80 (aceder diretamente à internet).

Questão Nº 5 - Descarregue o cenário WorkstationBD (fornecido com o enunciado) e grave-o na sua área de trabalho. Escolha "File" -> "New" para reiniciar o programa e clique no botão "Load From File", apontando o programa para o arquivo que você descarregou.

Este cenário foi configurado para que as estações de trabalho possam passar pelo *firewall2* e obter acesso à base de dados. O *firewall1* tem um conjunto de regras de permissão para todo o tráfego, de forma que todas as informações sejam passadas para a rede e da rede para os servidores.

Escreva regras para evitar que ataques ativos passem pelo *firewall1* e ataquem o banco de dados.

Que ataques ativos você pode evitar restringindo o acesso no *firewall*?

Primeiro fiz uma simulação para verificar o que iria ocorrer caso nada fosse feito.

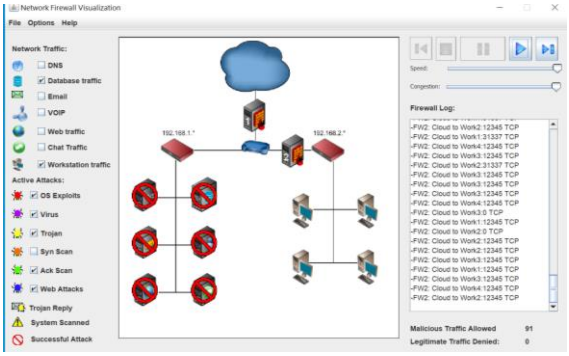


Imagem - 12 Simular Ficheiro Rede Trabalho sem regras

Como seria expetável, as regras All In e All Out (que são essencialmente as mesmas) permitem que todo o tráfego flua pela firewall sem nenhuma restrição o que origina contaminação de todos os hosts que comunicam de e para a internet, ou seja, os servidores.

Criar regras na firewall1 não irá resolver o problema, pois os ataques continuarão a passar porque as regras anteriores assim o permitem.

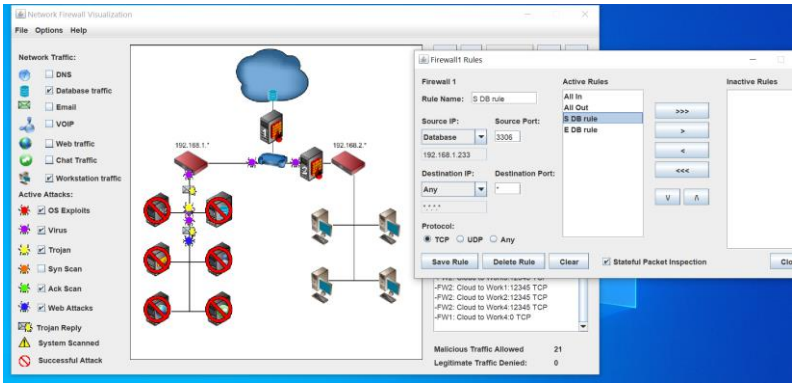


Imagem - 13 Simular com regras

Para melhorar a segurança, teremos de apagar/inativar as regras *All in* e *All out* e substituí-las pelas regras criadas na pergunta 4 e listadas em 4.4, para permitir que todo o trafego legitimo passe, embora apenas seja requerido que flua trafego para a DB. Quanto à firewall2 não existe necessidade no âmbito desta pergunta de alterar as regras desta firewall dado que todo o tráfego legitimo está a fluir corretamente.
Para comprovar a afirmação anterior realizei um teste com as novas regras e verifiquei o seu resultado:

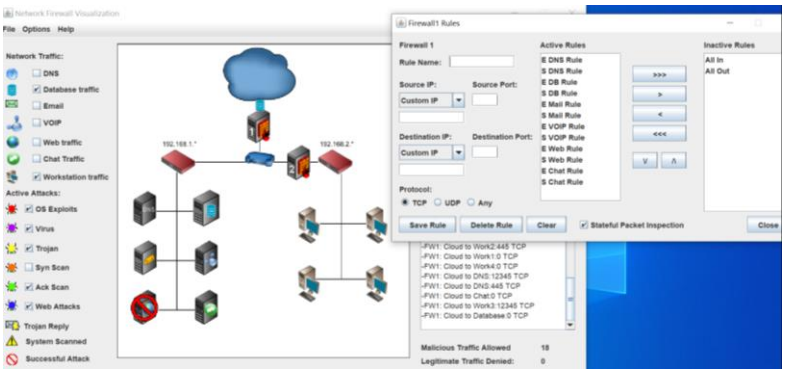


Imagem - 14 Simulação com regras mas sem All In e All Out

Como seria expetável, ocorre melhoria significativa da segurança da rede, permanecendo neste momento apenas os ataques web, de notar que nesta simulação os ataques Syn Scan estão inativos, mas os mesmos se fossem ativados também passariam pela firewall como verificado anteriormente na questão 4.
Agora o administrador da rede poderá se concentrar nos ataques web e syn scan para que exista uma melhoria ainda mais significativa nesta rede.

Por fim, respondendo à pergunta em si consigo evitar todos os ataques à base de dados, exceto o Syn Scan, aplicando as regras E DB rule e S DB Rule, enquanto que garanto que todo o tráfego legitimo flua para a base de dados sem interferência por parte da firewall.

ANEXO:

Definição de tráfego legitimo para esta aplicação

Legitimate Traffic

You have the ability to define which traffic options you would like active on your network. To define traffic, use the checkboxes along the left side of the main window. To turn traffic on simply check the box or uncheck it to turn it off. Below you will find all information on each legitimate service.

----------**DNS**----------

IP Address: 192.168.1.5

Port: 53

Protocol: UDP

----------**Database**---------

IP Address: 192.168.1.233

Port: 3306

Protocol: TCP

----------**Email**----------

IP Address: 192.168.1.136

Port: 25

Protocol: TCP

----------**VOIP**----------

IP Address: 192.168.1.74

Port: 38287

Protocol: TCP

----------**Web**----------

IP Address: 192.168.1.114

Port: 80

Protocol: TCP

----------**Chat**----------

IP Address: 192.168.1.68

Port: 5222

Protocol: TCP

BIBLIOGRAFIA

Fulton, S., Warner, J., Musielewicz, D., Masters, G., Verett, T., & Winchester, R. (2010). *Network firewall visualization in the classroom.* United States Air Force Academy, Colorado: Journal of Computing Sciences in Colleges.

Fulton, S., Warner, J., Musielewicz, D., Masters, G., Verett, T., & Winchester, R. (2020). *Firewall Visualization Project - Help Documentation.* United States Air Force Academy, Colorado: Version 1.0.

Mamede, H. S. (2020). *Unidade Curricular: Segurança em Redes de Computadores - AF3 - Apontamentos Teoricos.* Lisboa: UAb.

Stallings, W. (2017). *Cryptography and Network Security* (7 (Global Edition) ed.). Harlow, England: Pearson Education Limited.