Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

GIVANILDO ALMEIDA DE SOUSA

SISTEMA DE PREVENÇÃO E DETECÇÃO DE INTRUSÕES DE REDE UTILIZANDO A FERRAMENTA IPS-SNORT

Brasília
2016

GIVANILDO ALMEIDA DE SOUSA

SISTEMA DE PREVENÇÃO E DETECÇÃO DE INTRUSÕES DE REDE UTILIZANDO A FERRAMENTA IPS-SNORT

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Redes de Computadores com Ênfase em segurança

Orientador: Prof. Dr. José Eduardo Malta de Sá Brandão.

Brasília
2016

GIVANILDO ALMEIDA DE SOUSA

SISTEMA DE PREVENÇÃO E DETECÇÃO DE INTRUSÕES DE REDE UTILIZANDO A FERRAMENTA IPS-SNORT

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Redes de Computadores com Ênfase em segurança

Orientador: Prof. Dr. José Eduardo Malta de Sá Brandão.

Brasília, 06 de Setembro de 2016.

Banca Examinadora

_____

Prof. Me. Gilberto Oliveira Netto

_____

Prof. Dr. Gilson Ciarallo

Dedico este trabalho primeiramente a Deus, que me concedeu a oportunidade da vida, e a todas as pessoas que contribuíram para mais esta conquista.

AGRADECIMENTOS

A minha esposa Ivanudi, companheira para todas as horas, e quem me incentivou na realização desse curso de pós-graduação.

Aos meus pais, Geraldo e Maria do Socorro que com a permissão de Deus me deram a vida.

Aos meus avós maternos, Antônio e Celina *in memorian*, que sempre cuidaram de mim e me deram todo amor e carinho.

Aos meus avós paternos, Manoel e Lucinda, que sempre me aconselharam nos momentos difíceis.

Aos professores do Uniceub que ministraram esse curso de pós-graduação.

Ao professor José Eduardo que me ajudou muito nesse trabalho sendo meu orientador.

RESUMO

Com o avanço da tecnologia, passou-se a tratar a informação como um ativo de maior valor entre os demais, e por isso a sua proteção passou a ser um objetivo a ser alcançado diariamente. Desta forma, surgiram vários dispositivos e mecanismos de segurança que podem auxiliar na proteção da informação, tais como firewalls, antivírus e sistemas de detecção a intrusão.São vários os motivos que levam a um investimento em segurança, investimento este que pode ser justificado pelo valor que a informação tem para uma organização.O presente trabalho tem como objetivo principal, implementar e testar um sistema de detecção e bloqueio de intrusão em ambiente virtual, monitorar e prevenir o tráfego de dados que representem possíveis ameaças ao ambiente em estudo.Para isto, foram instaladas quatro máquinas virtuais para a realização dos testes.As máquinas virtuais tem como sistema operacional o Linux, essa escolha se justifica pela flexibilidade em ajustes e compilação em seu código fonte.A máquina que realiza a detecção e o bloqueio de tráfego está configurada com o IDS Snort, compilado para o modo inline, esta função é a que torna o Snort um IPS, responsável pelo o bloqueio. O ambiente de testes, foi desenvolvido em máquina virtual, com o software VMware Workstation Pro, onde as máquinas virtuais tiveram como sistema operacional o Linux na sua versão ubuntu e KaliLinux, esta última possui ferramentas para testes de intrusão à máquina alvo.Espera-se demonstrar com esse estudo a efetividade dos bloqueios feitos pela fermenta IPS Snort compilada no modo inline, frente a importância da proteção da informação em um ambiente de rede de computadores.

Palavras-chave: Segurança. Proteção.Intrusão.Bloqueio.IPS.

ABSTRACT

With the advancement of technology, it started to treat information as an asset of greater of the others, so their protection has become a goal to be achieved daily. Thus, there were various devices and security mechanisms that can help protect information, such as firewalls, antivirus and Intrusion detection systems .There are several reasons that lead to security investment, investment that can be justified by the value that information has for a organization. The present work aims, implement and test a detection system and intrusion block in a virtual environment, to monitor and prevent data traffic representing potential threats to the environment in this study.For this, four virtual machines will be installed to achieve the tests.As virtual machines has the operating system Linux, the choice is justified by the flexibility in adjustments and build on your source code. The machine that performs the detection and blocking traffic is configured with Snort, compiled for inline mode; this function is what makes the Snort an IPS, responsible for the blocking. The test environment will be developed in virtual machine with VMware Workstation Pro software, where virtual machines will have the operating system Linux, in your ubuntu version and Kali Linux, the latter has tools for intrusion tests to target machine. Expected demonstrated with this study, the effectiveness of locks made by IPS Snort tool compiled in inline mode, forward the importance of protection of information in a computer network environment.

Keywords: Security. Protection.Intrusion.Block.IPS.

SUMÁRIO

INTRODUÇÃO

As redes de computadores surgiram devido a necessidade de troca de informações, definindo uma nova realidade para o uso dos computadores, e nos sistemas computacionais. Com isso foi possível o acesso a determinado dado que está localizado fisicamente a centenas ou quilômetros de distância (TORRES, 2009).

A detecção e prevenção de Intrusão em redes de computadores e sistemas é uma área de grande expansão, pesquisas e investimentos em segurança em redes de computadores têm crescido de forma considerável. Para a maioria das aplicações atuais, desde redes corporativas simples até sistemas de e-commerce[1] ou aplicações bancárias, o uso de ferramentas adequadas de segurança da informação é indispensável na gestão de sistemas computacionais.

Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores universitários, com a finalidade de enviar mensagens de correio eletrônico, e também por funcionários de empresas, para compartilhar impressoras. Sob essas condições, a segurança nunca precisou de maiores cuidados. Porém, como milhões de cidadãos comuns atualmente estão usando as redes para executar operações bancárias, fazer compras e arquivar sua devolução de impostos, a segurança das redes está despontando no horizonte como um problema em potencial (TANENBAUM, 2003).

Motivação

Com o avanço tecnológico nas comunicações em rede por meio da interconexão de computadores à internet em todo o mundo, é verificado um

[1] Comércio eletrônico

conseqüente aumento nas tentativas de ataques de intrusão por programas mal intencionados nesse ambiente.

Diante dessas tentativas surgiu a necessidade de mais ferramentas de segurança em rede, como uma camada extra de proteção, que fossem capazes de fazer a detecção e o bloqueio de eventos de intrusão em uma rede de computadores, conhecidos, como sistemas de prevenção e detecção de intrusões IPS (*Intrusion Prevention System*).

Objetivos

Objetivo Geral

O presente estudo tem como objetivo geral implementar e testar um **sistema de prevenção e detecção de intrusões de rede utilizando a ferramenta *IPS-Snort***, em plataforma de software livre Linux e configurado em modo de contenção que seja capaz de fazer o bloqueio a certos tipos de intrusões.

Para alcançar esse objetivo, foram realizadas pesquisas, testes e análises de resultados obtidos por meio de ferramentas adequadas, foi adotado então o IPS *Snort*[2] como ferramenta de detecção e bloqueio muito difundido no contexto de software livre como sendo uma ferramenta que atende satisfatoriamente a proposta do estudo.

Objetivos Específicos

A partir do objetivo geral, foram identificados os seguintes objetivos específicos:

[2]http://www.snort.org.br/snort.php

- Definir e implementar um ambiente virtual para a realização de testes, utilizando o software VMware Workstation[3];
- Instalar e configurar as máquinas virtuais para a simulação dos testes;
- Configurar a máquina IPS *Snort* em modo de bloqueio com seu conjunto pré-definido de regras, que reporte as tentativas de intrusão e faça o bloqueio de pacotes de dados maliciosos;
- Instalar ferramentas auxiliares com funcionalidades adicionais ao IPS Snort como: biblioteca *libpcap*[4] e servidor Web Apache2[5] para atender ao objetivo proposto;
- Realizar a simulação de ataque do tipo força bruta utilizando a ferramenta *zenmap*[6], do pacote *Kali Linux*[7];
- Fazer as análises das tentativas de intrusão reportadas pelo *Snort* no modo passivo sob o ataque de força bruta e comparando com o mesmo cenário, agora com o modo de bloqueio ativado;
- Avaliar as informações colhidas na simulação.

Procedimentos metodológicos

---

[3]http://www.vmware.com/br/products/workstation

[4]Biblioteca desenvolvida e C++ para captura de tráfego em rede

[5]http://wiki.apache.org/httpd/FAQ#What_is_Apache.3F

[6]https://zenmap.org/zezenmap/

[7]Distribuição Linux especializada em testes de intrusão e auditoria de segurança

- A metodologia aplicada para o desenvolvimento deste trabalho foi composta por **pesquisas,técnicas aplicadas,testes e análise dos resultados obtidos;**
- No primeiro momento foram feitas **pesquisas de leitura** das diversas fontes da literatura,como livros,artigos e trabalhos acadêmico sobre **Segurança da Informação e Sistemas de Detecção de Intrusão;**
- As **ferramentas utilizadas** para o desenvolvimento do trabalho assim como o sistema operacional foram de **software livre para Linux**;
- Após proceder com as pesquisas,foram feitas análises das ferramentas e técnicas utilizadas na implementação de um IPS, optando-se pela ferramenta **Snort;**
- Em seguida foi desenvolvido um **ambiente de rede** em máquina virtual para a realização dos testes por ataque de força bruta;
- Após a realização dos testes,foi feita uma análise dos resultados obtidos e validação da efetividade dos bloqueios feitos pela ferramenta Snort.

Este documento está dividido como se segue:inicialmente é abordado o conceito de segurança, princípios, vulnerabilidades e ameaças em relação a proteção da informação e seu impacto em um sistema de informação segundo a definição de alguns autores e normas de segurança apresentados no primeiro capítulo.

No segundo capítulo é apresentado a finalidade de um sistema de detecção de intrusão, os métodos de detecção, os tipos de IDS(*Intrusion Detection System*) e o IPS(*Intrusion Detection System*) foco deste trabalho.

Já no terceiro capítulo é apresentado o Snort, sua definição e seu funcionamento.É explicado sua estrutura e o fluxo de pacotes em sua arquitetura.

Finalmente no quarto capítulo é apresentado a implementação, topologia do ambiente de desenvolvimento, testes, resultados obtidos e trabalhos futuros para a proposta de um sistema de detecção e prevenção de intrusão e a percepção de sua importância como uma camada a mais de segurança em um ambiente de rede.

1 CONCEITOS DE SEGURANÇA

Segurança da informação é uma área de conhecimento dedicada a proteger ativos de informação contra acessos não autorizados, alterações indevidas ou indisponibilidade (SÊMOLA, 2003).

Segundo a ISO/IEC17799(2005), segurança da informação é a proteção da informação contra vários tipos de ameaças, visando garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades de negócios.

De acordo com Donner e Oliveira (2008), a segurança da informação é definida como o processo de proteção das informações de ameaças para assegurar sua integridade, disponibilidade e confidencialidade.

Muito já foi feito no sentido de aprimorar a segurança da informação, apesar de não ser possível erradicar completamente o risco de seu uso indevido, como observam (SILVA; RANGHETTI; STEIN, 2007). Ao confirmar que a segurança da informação não deve ficar restrita aos aspectos tecnológicos, devendo proteger a informação em qualquer forma que se encontre. Afirmam ainda que a segurança da informação cobre também “toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros”, e a proteção deve ser correspondente ao seu valor para a organização e aos prejuízos que sua perda ou acesso indevido podem provocar. Isso é confirmado por Marciano e Lima-Marques(2006), que afirma que a TI não é suficiente para garantir a proteção das informações, e vai além ao afirmar que a tecnologia pode tanto ajudar quanto agravar os problemas relacionados à segurança da informação.

Assim, as organizações devem definir um nível de segurança de acordo com suas necessidades. O objetivo não é construir uma rede totalmente segura,mas sim um sistema confiável que seja capaz de identificar e anular os possíveis ataques que comprometam suas informações (NAKAMURA e GEUS,2007).

1.1 Princípios de Segurança

De acordo com Bishop (2003) e Russell e Gangemi (1991), a segurança da informação é caracterizada pelos seguintes princípios:

• Confidencialidade – assegura que um sistema computacional não deve permitir que informações sejam acessadas por pessoa não autorizada. A confidencialidade garante a privacidade das informações;

• Integridade – garante que a informação não será alterada ou destruída sem a autorização adequada.

• Disponibilidade – consiste na capacidade de manter acessível informação para os usuários autorizados quando solicitado.

1.2 Vulnerabilidades

Uma vulnerabilidade é um defeito ou uma falha no design ou na implementação de um sistema de informação, que inclui procedimentos de segurança e controles associados ao sistema, que pode ser intencionalmente ou acidentalmente exploradas, comprometendo a confidencialidade, integridade ou a disponibilidade (ROSS et al., 2005).

1.3 Ameaças Ataques e Intrusão

Segundo Nobre (2007), uma ameaça, consiste em uma possível violação de um sistema computacional, que pode ser acidental ou intencional. Uma ameaça acidental é aquela que não foi planejada, podendo ser, por exemplo, uma falha no hardware ou no software. Já uma ameaça intencional está associada à intencionalidade premeditada. Podendo ser desde um monitoramento não autorizado do sistema até ataques sofisticados, como os realizados por Hackers.

Ainda de acordo com Nobre (2007), algumas das principais ameaças aos sistemas nas redes de computadores envolvem destruição ou modificação de informações, roubo, remoção ou perda de informação, revelação de dados confidenciais ou não, e em casos extremos, chegando até a paralisação dos serviços de rede.

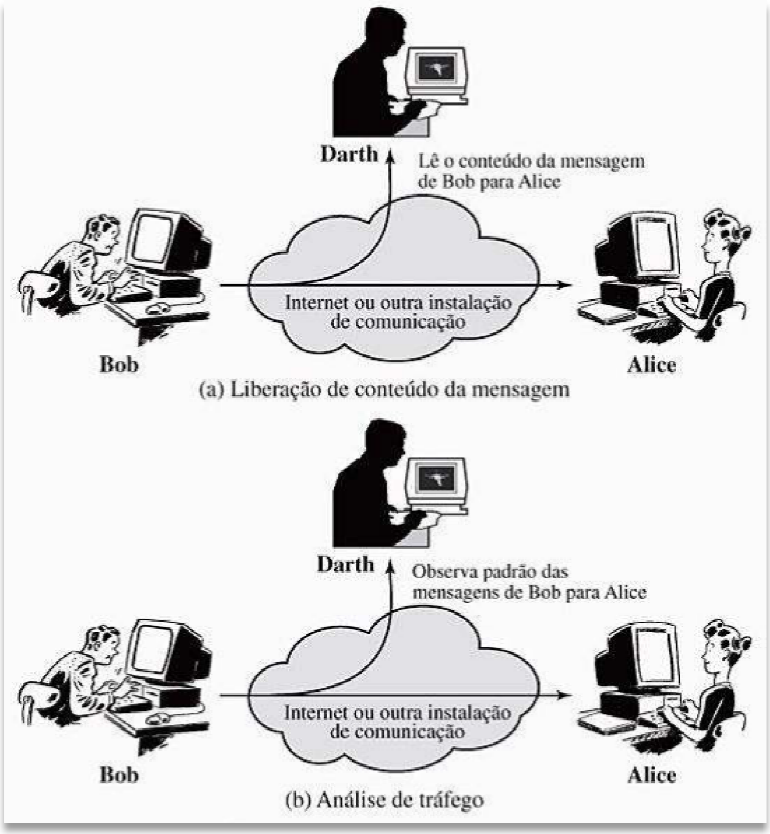
Um ataque acontece quando se efetiva uma ameaça intencional. Estes ocorrem por vários motivos. Variam desde a pura curiosidade, interesse em adquirir maior conhecimento sobre os sistemas, intenção em conseguir ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial ou venda de informações confidenciais. Outro tipo de interesse é o de ferir a imagem de um governo ou uma determinada empresa ou serviço, e quando isso acontece, a notícia da invasão é proporcional à fama de quem a sofreu e normalmente representa um desastre em termos de repercussão pública (NOBRE,2007).

Quando um ataque é bem sucedido, afirmamos que houve uma intrusão (BARKER and LEE 2004).

1.4 Técnicas de ataque

Existem dois tipos de ataques básicos: ataques passivos e ataques ativos. De acordo com (STALLINGS, 2008) os ataques passivos tem como objetivo investigar e tentar monitorar dados transmitidos. Esse tipo de ataque é difícil de ser detectado, pois como não envolve alteração de dados, fica na maioria das vezes imperceptível. Os ataques passivos são divididos em liberação de conteúdo da mensagem e análise de tráfego, como visto na figura1 abaixo:

Figura 1 - Ataques passivos

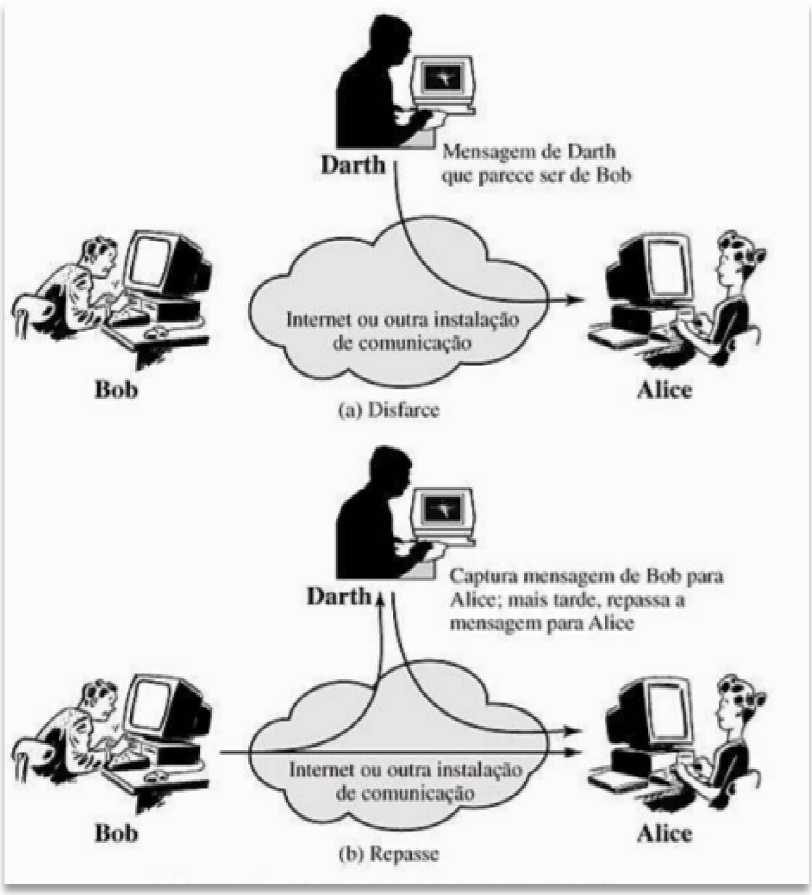


Fonte (STALLINGS, 2008)

De acordo com a figura1, pode-se perceber que quando Bob envia a mensagem para Alice, ela é interceptada por Darth, que lê o conteúdo da mensagem e observa o seu padrão, nesse caso dizemos que se trata de um ataque passivo, pois houve a liberação de conteúdo sem a alteração de dados.

Em contrapartida os ataques ativos ainda segundo (STALLINGS, 2008), ocorrem modificação ou criação de um determinado fluxo de dados, subdividindo-se em quatro categorias: disfarce, repetição, modificação de mensagens e negação de serviço, de acordo com as figuras seguintes:

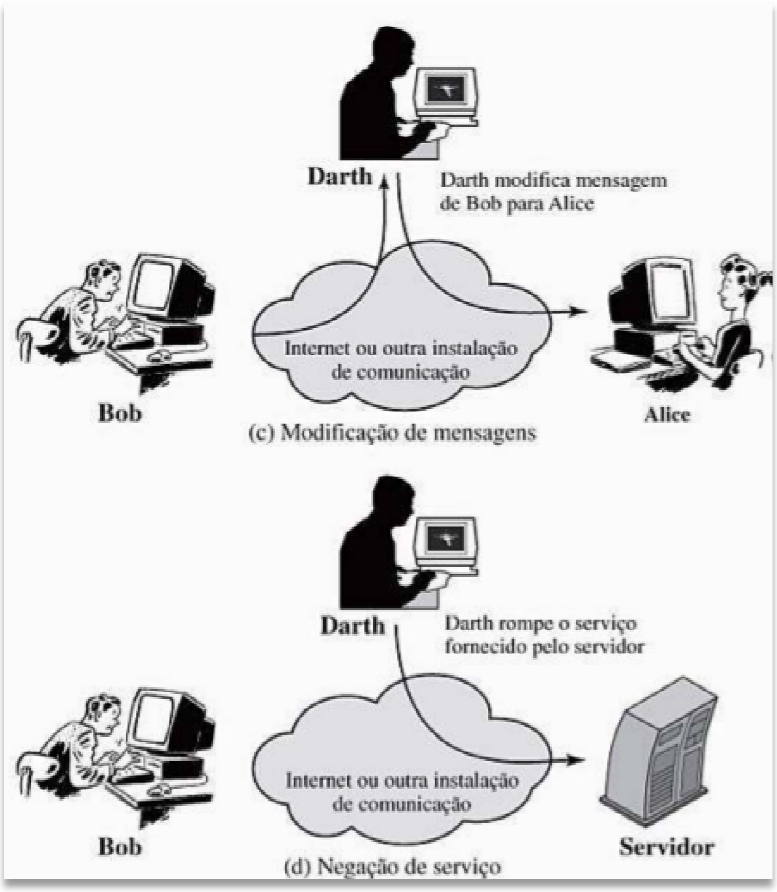
Figura -2 Ataque Ativos



Fonte - (STALLINGS, 2008)

Como pode ser observado na figura 2, a mensagem de Bob ao ser enviada para Alice, é interceptada por Darth, e repassada posteriormente parecendo ser de Bob, esse é um tipo de ataque ativo de disfarce.

Figura -3 Ataques ativos



Fonte - (STALLINGS, 2008)

Na figura 3, a mensagem de Bob ao ser enviada para Alice, é interceptada por Darth e modificada para envio a Alice, no segundo caso podemos perceber uma negação de serviço.

1.5 Técnicas de Defesa

Segundo Stallings(2008), um mecanismo de segurança consiste em qualquer processo (ou dispositivo incorporado a esse processo) implementado para detectar, impedir ou permitir a recuperação de um ataque à segurança. Para esse

objetivo existem diversas técnicas de defesas, tais como: criptografia, firewall, antivírus, detectores de intrusão, assinaturas digitais e outros.

2 DETECÇÃO E PREVENÇÃO A INTRUSÕES

A segurança é um processo complexo, que envolve processos tecnológicos e humanos, desta forma, uma estrutura de segurança mais simples, consiste em um firewall, que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados (NAKAMURA; GEUS, 2007).

Um sistema de detecção de intrusão, tem como objetivo detectar atividades suspeitas na rede, é um importante elemento de segurança, pois pode detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto não podem ser protegidas pelo firewall (NAKAMURA; GEUS, 2007).

2.1 Metodologia de Detecção

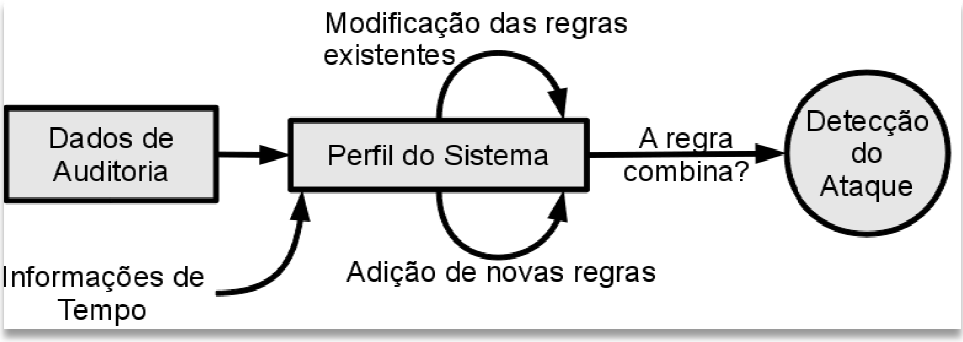
De acordo com Lari e Amaral(2004), as formas de detecção podem ser divididas sob dois aspectos: os que analisam as informações baseadas em conhecimento (eventos passados) e os que analisam o comportamento (estado corrente do sistema).

2.2 Métodos de Detecção Baseados em Assinatura

Esse método de detecção tem um baixo custo computacional e não causa muito comprometimento de desempenho (CANSIAN, 1977). Por ser um método

baseado em assinatura, utiliza técnicas de padrões, combinando os dados analisados da rede ou dos registros do sistema, com sua base de assinaturas de ataques já conhecidos, ao detectar um ataque emite um alarme ao administrador, como mostrado na figura 4 (PIETRO,2008; WANG,2009):

Figura 4-Métodos de Detecção Baseados em Assinatura



Fonte-(SUNDARAM, 1996)

Na figura 4, é mostrado o método de detecção baseado em assinatura, onde os dados analisados são submetidos aos padrões de regras já estabelecidas, caso combine com a base de assinaturas de regras, esse é identificado como um ataque.

Segundo Cansian(1997), os sistemas baseados em assinaturas podem ser:

- Sistemas especialistas: Tem a capacidade de fazer a analise dos atraque através de regras, propondo uma solução para o problema.
- Por modelamento: compara informações de registros de auditoria com modelos de comportamentos de ataques para gerar uma suspeita ou descartá-la.

Para Wang (2009), os diferentes tipos de assinaturas utilizados nestes sistemas podem ser:

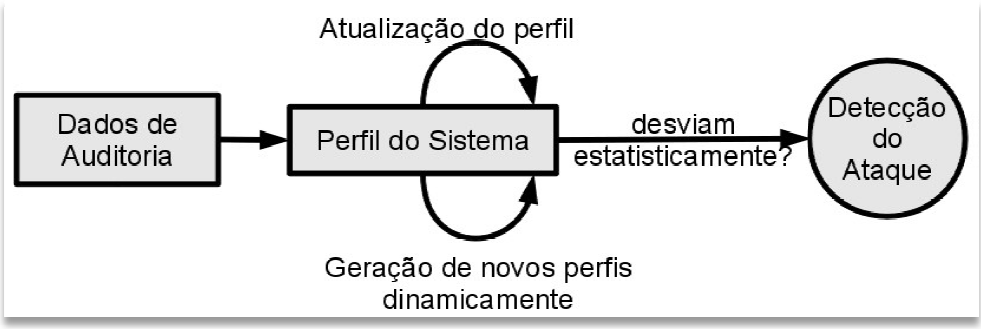
- Assinaturas de redes: Coleta informações dos pacotes que podem comprometer a execução normal do sistema. Esse método consiste em assinaturas de cabeçalho ou campo de dados(payload).As assinaturas de campo de dados monitoram as ações do usuário, enquanto as assinaturas de cabeçalho, verificam pacotes maliciosos.
- Assinaturas de hosts: Utilizam informações de comportamento que podem afetar o sistema, como tentativas de senhas erradas. Os IDS's deste modelo possuem três métodos para editar as assinaturas (WANG,2009):
- Sistemas Compilados (Built-in System):armazena um conjunto de regras de detecção predefinidas permitindo a edição de acordo com a necessidade desejada;
- Sistemas Programados *(Programim Systems*):possuem um conjunto de regras e uma linguagem de programação (ou script), permitindo selecionar as regras padrões e/ou escrever suas próprias regras;
- Sistemas Especialistas (*Expert Systems*):são o IDS's configurados para atender as necessidades específicas de uma organização, esse tipo requer uma qualificação profissional para definir as regras de detecção.

2.3 Métodos de Detecção Baseados em Anomalia

Sistemas baseados em anomalias realizam a supervisão de comportamentos anômalos do sistema, assumindo que comportamentos anormais

podem ser considerados invasões. A vantagem nesse tipo de detecção, é de detectar ataques recentes, o que exige um desenvolvimento mais complexo. (CANSIAN, 1997; DI PIETRO, 2008; SUNDARAM, 1996).

Figura 5-Métodos de Detecção Baseados em Anomalia



Fonte -. Adaptado de SUNDARAM, (1996)

Como ilustrado na figura5, os comportamentos anômalos do sistemas são submetidos aos novos perfis do sistema, caso estes se desviem das estatísticas, são considerados como um ataque.

Os Sistemas de Detecção de Intrusão(IDS)[8] desse tipo apresentam erros devido a identificação de atividades normais de um usuário como atividades anormais,(falso positivo) ou quando deixa de identificar atividades anormais como invasão (falso negativo) por parecerem muito com a atividade costumeira de um usuário.Podem-se encontrar os comportamentos (CANSIAN, 1997; KUMAR,1995):

- Intrusivo, mas não anômalo: também chamados de falso negativos. Neste caso, ocorre uma falha na detecção, pois a invasão não provoca atividade anormal, não sendo então detectada pelo sistema;

[8]Intrusion Detection System

- Não intrusivo, mas anômalo: também chamados de falso positivos. Neste caso, ocorre uma falha na detecção, que indica erroneamente a anormalidade como uma invasão;
- Não intrusivo e não anômalo: também chamados de verdadeiros negativos. Neste caso, ocorre um acerto, pois a atividade não e anômala e não e evidenciada como invasão;
- Intrusivo e anômalo: também chamados de verdadeiros positivos. Neste caso, ocorre um acerto, pois a atividade é anômala e é evidenciada como invasão.

2.4 Sistema de detecção de Intrusão

Um sistema de detecção de intrusão (*Intrusion Detections System* - IDS), é um componente essencial em um ambiente cooperativo, esse sistema tem como objetivo detectar atividades suspeitas, impróprias, incorretas ou anômalas em um ambiente de rede, funciona como um *sniffer*[9], opera de forma passiva, capturando e analisando a comunicação do seguimento de rede (NAKAMURA; GEUS, 2007).

2.5 Tipos de IDS

2.5.1 IDS baseado em host(HIDS)

[9] Farejador

Segundo Nakamura e Geus(2007), esse tipo de IDS faz o monitoramento do sistema, com base em informações de arquivos de log na máquina, ele é capaz de monitorar acessos e alterações em arquivos do sistema considerados importantes.

2.5.2 IDS baseado em rede(NIDS)

Esse tipo de IDS, monitora o tráfego do seguimento da rede onde ele é instalado. A detecção é realizada com a captura e análise dos cabeçalhos e conteúdos dos pacotes, que são comparados com padrões de assinaturas de ataques conhecidos (NAKAMURA; GEUS, 2007).

2.5.3 IDS híbrido

Combina as características do IDS baseado em Host(HIDS) e do IDS baseado em rede(NIDS), coletando o tráfego da rede, processando os pacotes e detectando e respondendo a ataques, oferece uma melhor capacidade de detecção (NAKAMURA;GEUS,2007).

2.6 Sistema de Prevenção de Intrusão-IPS

Diferentemente do IDS, que opera de forma passiva, somente capturando e analisando a comunicação do seguimento de rede, o (*Intrusion Prevention System*-IPS), Sistema de Prevenção de Intrusão, opera de forma reativa, pois ao capturar e

analisar os pacotes que trafegam pelo rede, tem a capacidade de e preveni-los.Esse tipo de IPS também é baseado em host ou em rede (NAKAMURA; GEUS,2007).

3 SNORT

Este capítulo tem como objetivo apresentar a estrutura do sistema de detecção de prevenção e detecção de intrusões (*Snort*), seu surgimento, funcionamento da estrutura de detecção e análise dos pacotes, o uso das regras como assinaturas pré-registradas e o pré-processador.

3.1 Definindo o Snort

Snort é uma moderna aplicação de segurança com três funções principais: ele pode servir como um *sniffer* de pacotes, um *logger* de pacotes ou um sistema de detecção de intrusão baseado em redes ou host.Foi desenvolvido em 1998 originalmente como um *sniffer* de pacotes. No final de 1999 foi implementado o recurso baseado em análise de assinaturas, podendo ser utilizado como um sistema de detecção de intrusão (BEALE, 2004).

Pode-se ainda definir o *Snort,* como sendo um sistema de detecção de código aberto, que tem a capacidade de realizar a análise de tráfego em tempo real nas redes IP (*internet Protocol*)[10], podendo ainda realizar a análise de protocolo, pesquisa/correspondência de conteúdo e ser usado para detectar vários tipos de ataques (CASWELL et al. 2003).

[10] Protocolo de comunicação usado nas máquinas em rede para o transporte de dados

O *Snort*[11] fornece aos administradores da rede informações importantes na tomada de decisões, através de análises de atividades de tráfegos suspeitos na rede (LARI; AMARAL, 2007)

3.2 Arquitetura e Funcionalidades do Snort

O *Snort* é considerado uma sistema de detecção de intrusão que não requer muito desempenho computacional para o seu funcionamento, além de oferecer configuração e suporte simples.A base do *Snort* é baseada na biblioteca *LibPcap*, que fornece funções de acesso a recurso de baixo nível, como o monitoramento de segurança (LARI; AMARAL, 2007).

Conforme Caswell et al.(2003), o *Snort* pode ser configurado em três principais modos, sendo estes:farejador (*sniffer*), registrador de pacotes (*packet logging*) e detecção de invasão.No modo farejador, os pacotes que trafegam na rede simplesmente são lidos e exibidos.O modo registrador de pacotes faz a leitura do tráfego e grava os pacotes em disco.Já no modo de detecção de invasão, o Snort analisa os pacotes da rede a procura de correspondências.

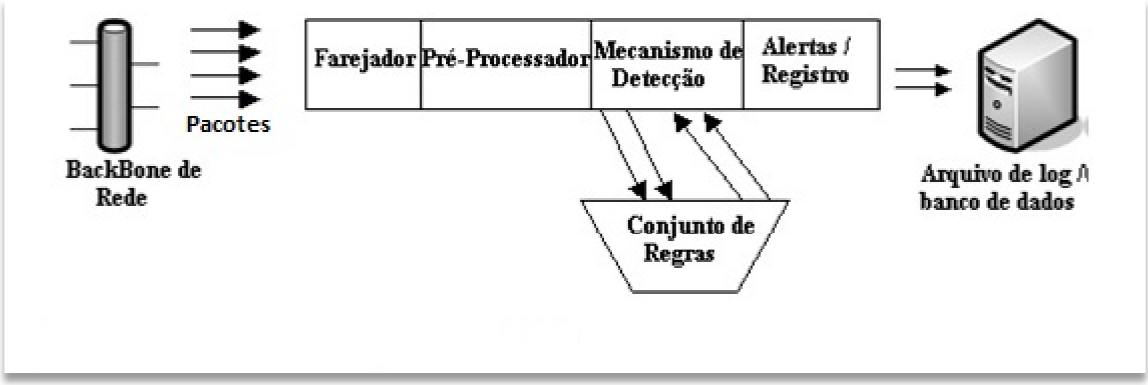
Segundo Caswell et al.(2003) o *Snort* possui quatro componentes básicos em sua arquitetura:

- O farejador;
- O pré-processador;
- O mecanismo de detecção;
- Alerta/registro

[11]https://www.snort.org

O pré-processador e o mecanismo de alerta são todos compostos por plug-ins que foram separados do código base para tornarem as modificações ao código fonte mais fáceis e confiáveis. A Figura 7 abaixo mostra uma visão geral da arquitetura do *Snort*.

Figura 6 -Arquitetura do Snort



Fonte- (CASWELL et al.,2003. p.26) modificado pelo autor

Conforme ilustrado na figura 6, o *Snort* é basicamente um farejador de pacotes. Porém, ele é projetado para processar os pacotes por meio do pré-processador e depois procurar uma correspondência desses pacotes com uma série de regras por meio do mecanismo de detecção Caswell et al. (2003).

Ainda segundo Caswell et al.(2003), farejadores de pacotes podem ser utilizados para:

- Analise de diagnostico e solução de problemas na rede;
- Analise e comparativo de desempenho;
- Intromissão para obter senhas em texto puro e outros dados interessantes.

4 IMPLEMENTAÇÃO E TESTES

Nesta sessão, serão demonstrados os testes realizados, as ferramentas utilizadas, a implementação do ambiente para simulação assim como os resultados esperados.

Os testes a serem realizados, serão testes de ataque de força bruta, que consiste na verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas, chegando a percorrer todo os espaço de busca.Esse ataque é disparado através da máquina atacante-*Kali-Linux,* essa máquina possui em sua distribuição, as ferramentas utilizadas em um teste de intrusão. Os testes de intrusão foram disparados usando a ferramenta *zenmap* na máquina Alvo-Webserver, máquina que possui instalado o servidor de internet. Esses testes foram realizados para demonstrar os bloqueios feitos pelo IPS *Snort*, habilitado no modo *inline*[12].

4.1 Implementação do Ambiente

O ambiente de testes implementado foi um ambiente virtual para a avaliação de desempenho do IPS *Snort*, desenvolvido com software de virtualização WMware Workstation Pro.

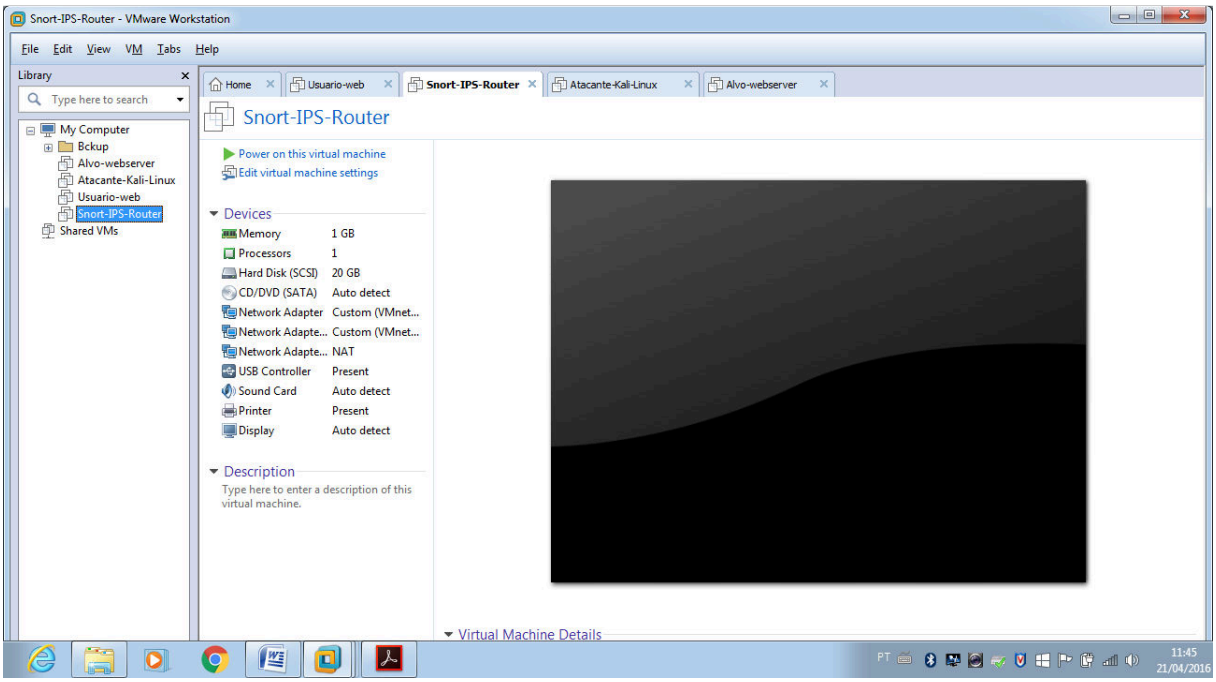
Nesse ambiente virtual, foram instaladas quatro máquinas virtuais para a simulação dos testes, por meio de uma máquina hospedeira com as seguintes

[12] Operação do Snort em modo de IPS, onde os pacotes são obtidos do iptables ao invés da biblioteca LibPcap.

configurações de hardware e Sistema Operacional(SO):Processador intel(R) Core(TM)i5-2430M CPU@ 2.40 GHz, memória RAM de 6,00 GB,500 GB de Hard Disk(HD) e o Sistema operacional Windows 7 Home Basic 64 bits[13]

Nas máquinas virtuais(VM) foram utilizadas as seguintes configurações de hardware e Sistema Operacional(SO):Memória Ram de 1GB, 30GB de Hard Disk(HD) e sistema operacional Linux Ubuntu[14] versão 14.04 LTS e KaliLinux 2.0.2,conforme figura 7 abaixo:

Figura 7– Ambiente de testes com as maquinas virtuais



Fonte – Produzido pelo autor do trabalho, 2016.

A figura 7 mostra o ambiente virtual implementado utilizando a ferramenta VMware Workstation com as máquinas virtuais(VM's) para a realização dos testes do Sistema de Prevenção de Intrusão *IPS-Snort.*

[13]https://www.microsoft.com/pt-br/windows

[14]http://www.ubuntu.com/

4.2 Ferramentas Utilizadas

As ferramentas utilizadas foram gratuitas, disponíveis para downloads e serviram para implementar as funcionalidades adicionais ao Snort ou trabalhar em conjunto com ele.

4.2.1 Apache

OApache2 é um serviço de HTTP que pode ser instalado em sistemas operacionais UNIX e em Windows.Neste trabalho, será utilizado para criar o servidor de internet a ser atacado, a máquina Alvo- webserver.

4.2.2 Linux Ubuntu

Sistema operacional utilizado para a criação das máquinas virtuais: máquina Alvo-webserver, máquina Usuário-Web e máquina Snort-IPS-Router.

4.2.3 Linux - KaliLinux

Sistema operacional utilizado para a máquina atacante-Kali-Linux, que possui ferramentas próprias para os testes de invasão, o qual será usado para o ataque de força bruta[15] contra o servidor Alvo-webserver, com a ferramenta zenmap.

---

[15] Consiste na verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas, chegando a percorrer todo os espaço de busca

4.2.4 Wireshark

O *wireshark*[16] é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades são parecidas com o *tcpdump* mas com interface *Grafic User Inferface*(GUI), com mais informações e com a possibilidade de uso de filtros.

4.2.5 Iptables

O *iptables*[17]é um sistema de controle de filtros para protocolos *ipv4*[18]utilizado nas regras de um firewall.Neste trabalho, o iptables será utilizado pelo Snort, onde os pacotes serão obtido através dele, em vez da biblioteca LibPcap.

4.3 Topologia do Ambiente

O ambiente de testes foi desenvolvido utilizando-se a ferramenta VMware Workstation, com a configuração de um ambiente virtual, com a criação de quatro máquinas, conforme a seguinte configuração ilustrada na figura 8.

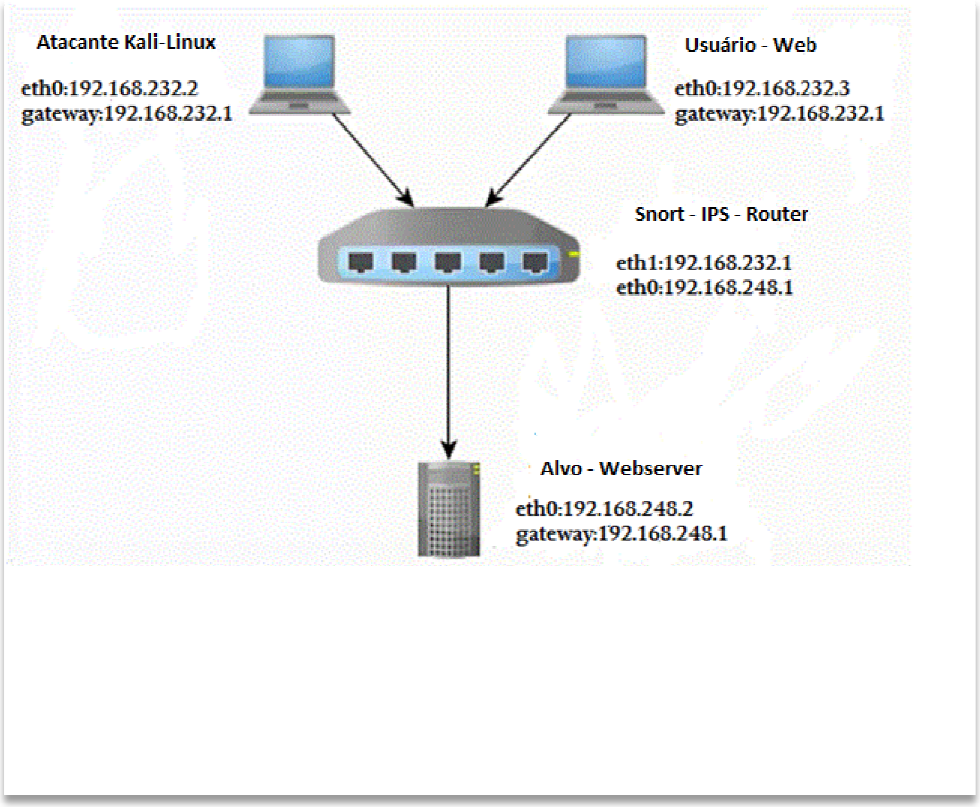
---

[16]https://www.wireshark.org/

[17]http://wiki.ubuntu-br.org/Iptables

[18]http://www.hardware.com.br/termos/ipv4

Figura 8-Topologia de rede



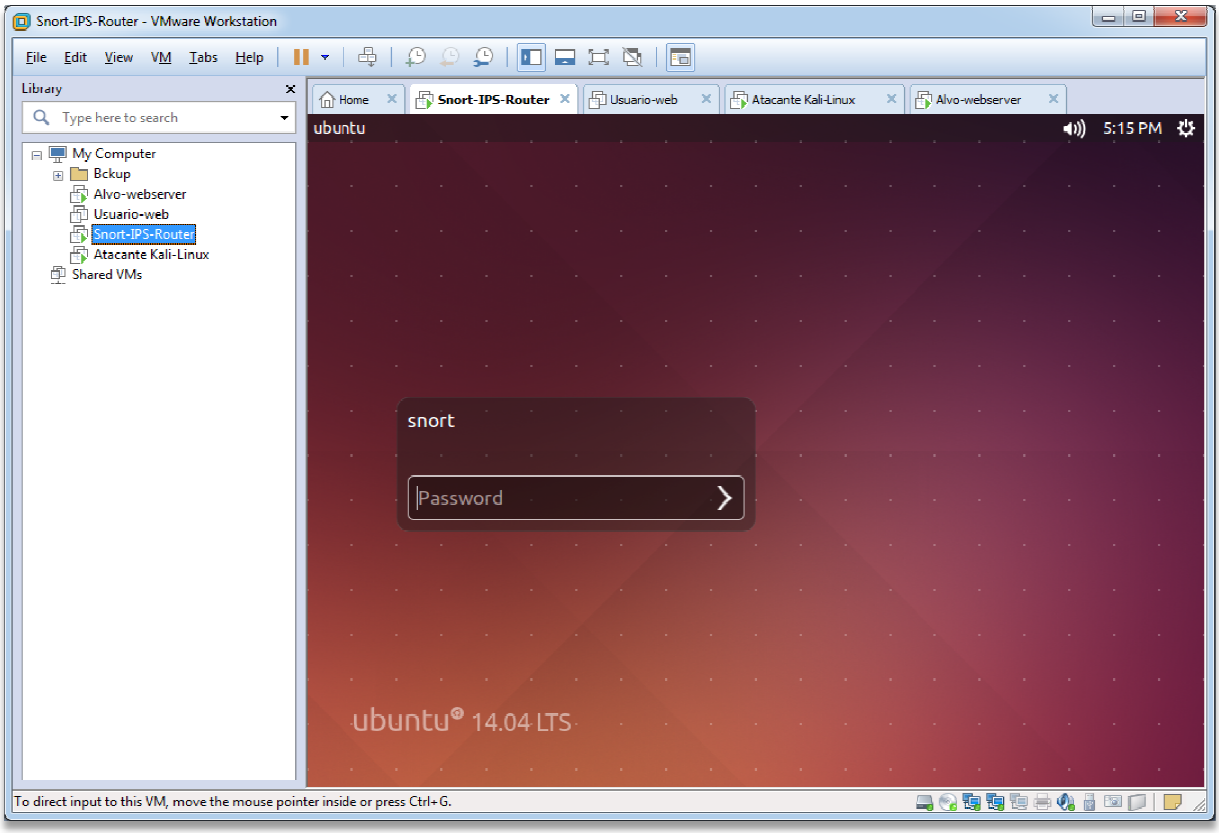
Fonte – Produzido pelo autor do trabalho, 2016.

De acordo com a figura 8, temos configuradas as seguintes máquinas virtuais:

- Snort -IPS-Router - configurada com o sistemas operacional Linux ubuntu, e funcionando como roteador na rede, todo o tráfego da rede passará por essa máquina, onde será monitorado.
- Alvo-webserver - configurada com o sistema operacional Linux ubuntu, e instalado o apache2, para a criação do servidor web, essa máquina é o nosso servidor de internet, que será o nosso alvo, onde será feita a tentativa de intrusão por força bruta.
- atacante-Kali-Linux - configurada com o sistema operacional Linux Kalilinux, usada para realizar os ataques na máquina Alvo-webserver.

- Usuário web - máquina de usuário comum, onde também será monitorado o tráfego proveniente dessa máquina ao nosso servidor Alvo-webserver.

Figura 9 - Máquina virtual Snort-IPS-Router



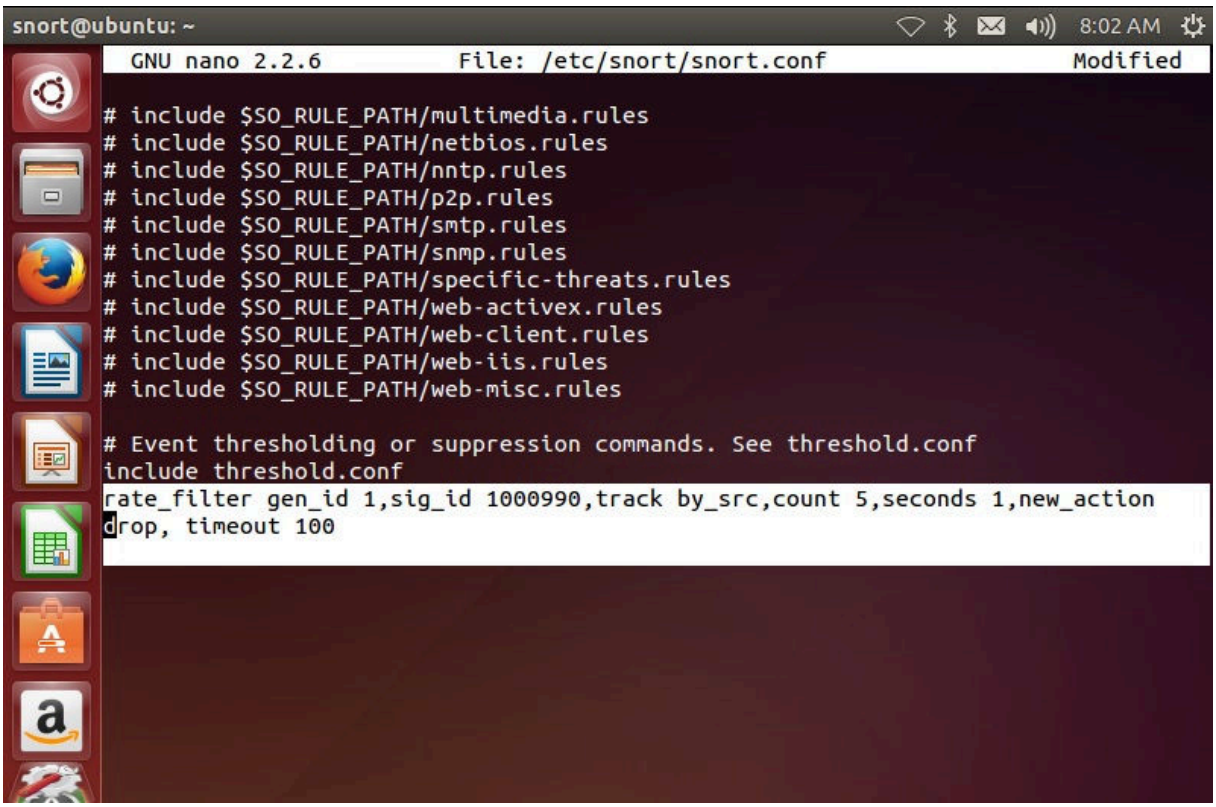
Fonte – Produzido pelo autor do trabalho,2016.

Na figura 9 é mostrado a máquina virtual onde foi instalada o IPS-Snort, essa é a máquina responsável por responder aos ataques de simulação realizados pelo atacante-Kali-Linux ao Alvo-webserver.

Para que o Snort funcione como um IPS, modo inline, foi configurado o arquivo snort.conf, localizado em /etc/snort/snort.conf, adicionado a linha ***rate_filtergen_id 1,sig_id 1000990,track by_src,count 5,seconds 1,new_action drop, timeout 100***, essa linha de comando faz o bloqueio dos pacotes suspeitos trafegados pela rede e filtrados pelo Snort a cada 5 segundos, sendo desta forma

bloqueados após o teste de invasão no nosso servidor Alvo-webserver, como mostrado na figura 10.

Figura 10 -Configuração de bloqueio ao ataques detectados pelo Snort

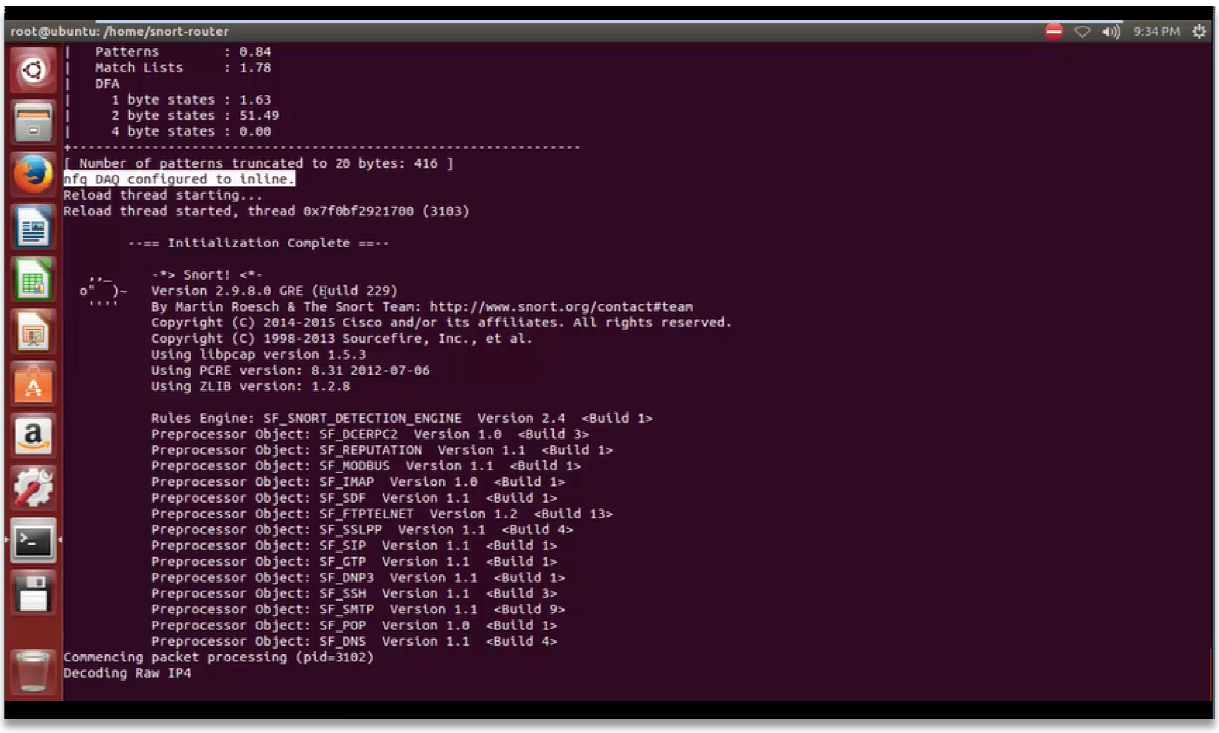


Fonte – Produzido pelo autor do trabalho,2016.

Como demonstrado na figura 10, a linha destacada (***rate_filtergen_id1,sig_id 1000990,track by_src,count 5,seconds 1,new_action droptimeout 100***)[19] é adicionada ao arquivo de configuração do snort(/etc/snort/snort.conf) para tornar o snort um IPS, configurado em modo inline, o que faz com que o snort realize os bloqueios aos ataques detectados.

[19] Essa linha de comando faz o bloqueio dos pacotes suspeitos trafegados pela rede e filtrados pelo Snort a cada 5 segundos.

Figura 11 - Snort configurado em modo inline



Fonte – Produzido pelo autor do trabalho,2016.

Na figura 11, é demonstrado o funcionamento do snort configurado em modo inline, IPS.e pronto para a detecção dos pacotes pelo conjunto de regras configuradas.

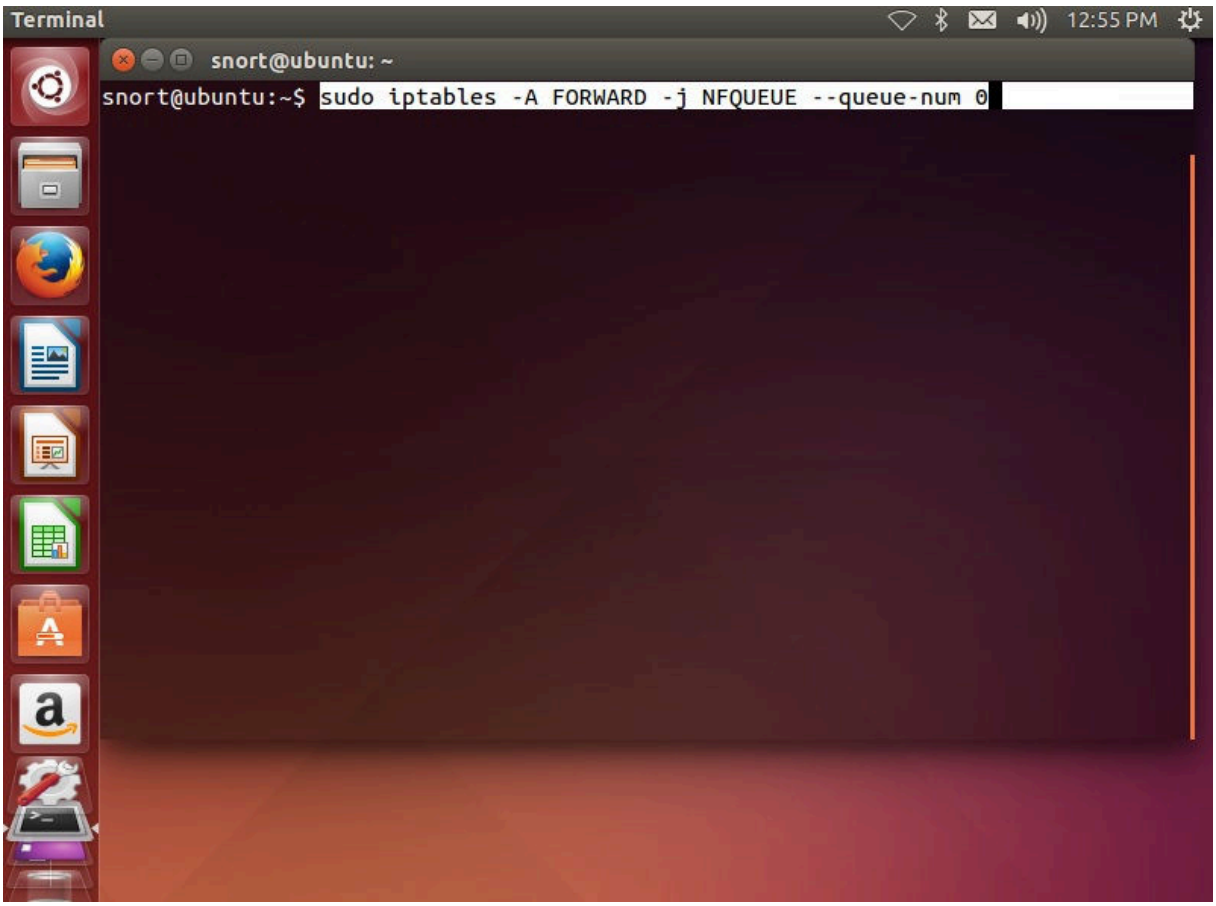
4.4 Testes

Nesse tópico, serão descritos os testes realizados, o primeiro teste com o snort somente no modo de detecção e o outro teste com o snort no modo de bloqueio, após esses testes, será feito a comparação entre os dois.

Todos os testes serão feitos da máquina atacante-Kali-Linux e da máquina usuário web, o teste da máquina atacante-Kali-Linux, será feito com o

comando de ataque de força bruta contra o servidor Alvo -webserver, e o outro teste somente de acesso ao servidor Alvo-webserver pela máquina do usuário web.

Figura 12- Linha de comando do Iptables



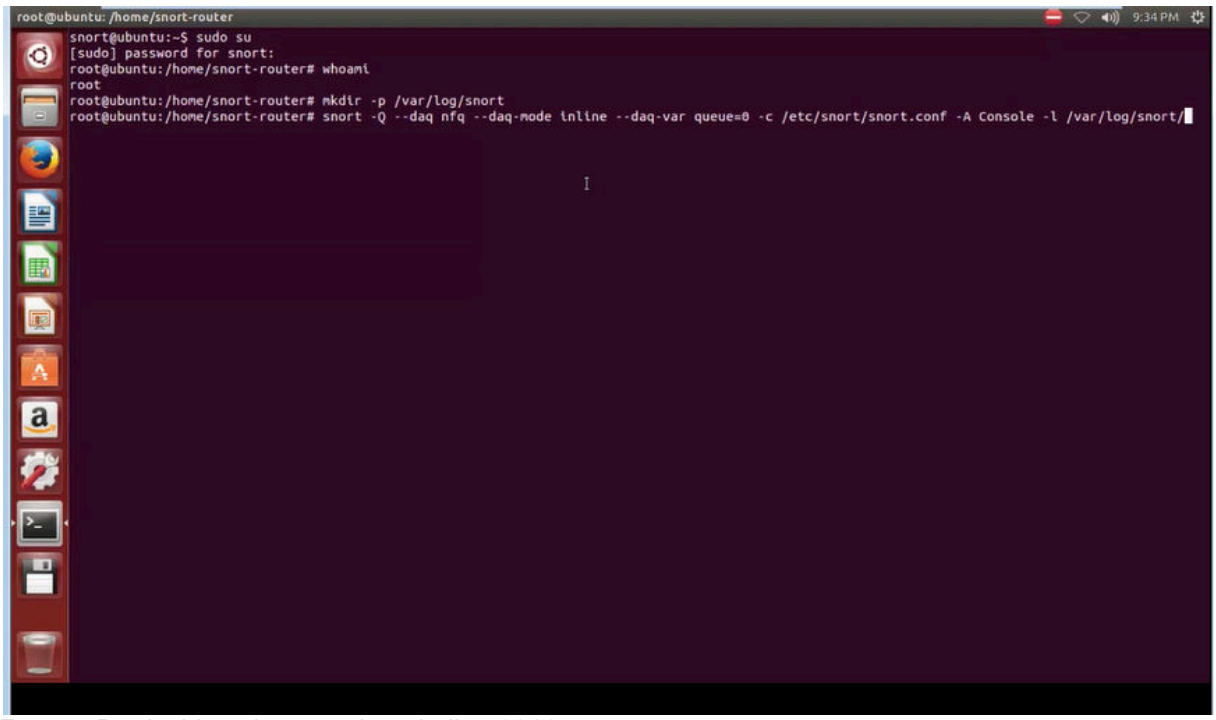
Fonte – Produzido pelo autor do trabalho,2016.

Na figura 12, é mostrado o comando ***sudo iptables -A FORWARD -j NFQUEUE --queue-num 0***[20]***,*** onde o snort no modo inline obtém os pacotes pelo iptables[21], bloqueando e permitindo pacotes baseados nas regras do Snort.

[20] Linha de comando que habilita o Snort a receber os pacotes pelo o iptables em vez da biblioteca Libpcap.

[21] Ferramenta que permite a criação de regras em um firewall.

Figura 13 - Habilitando o Snort em modo inline



Fonte – Produzido pelo autor do trabalho, 2016.

Na figura 13, é mostrado o comando ***snort -Q --daq nfq --daq-mode inline --daq-var queue=0 -c /etc/snort/snort.conf -A Console -l /var/log/snort/.***[22]

Esse comando habilita o modo de detecção do snort, que passará a monitorar os pacotes e fazer os bloqueios aos pacotes suspeitos, gravando os logs na pasta /var/log/snort/.

4.5 Teste de força bruta

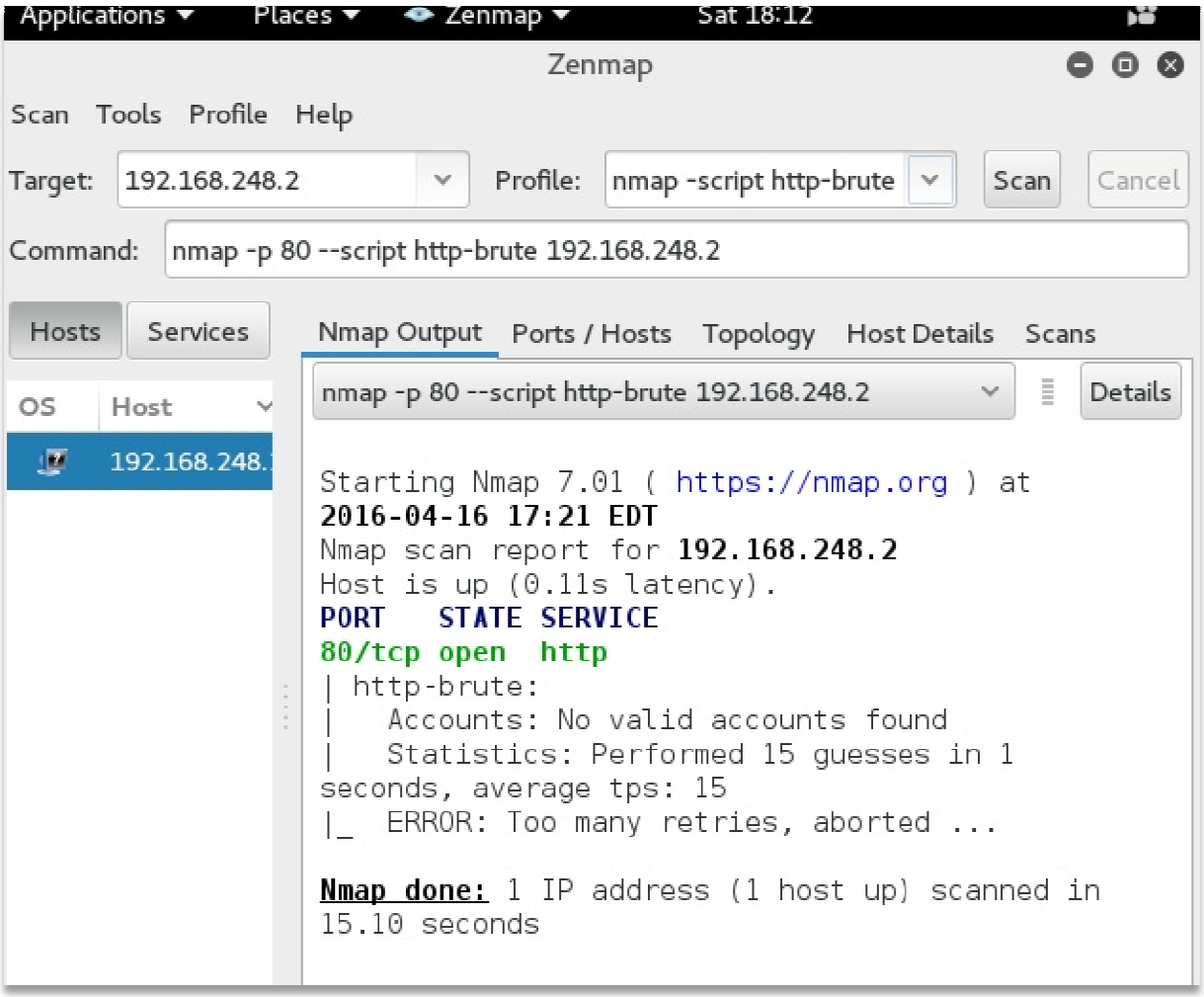
Após habilitar o *snort* em modo *inline*, será utilizado a ferramenta Zenmap,[23]que é uma versão gráfica do *nmap*, para o ataque de força bruta ao servidor Alvo-webserver.

---

[22] Comando que habilita o snort no modo inline, modo de detecção de bloqueio.

[23]https://nmap.org/zenmap

Figura 14 - Teste de força bruta com zenmap contra a máquina alvo-webserver



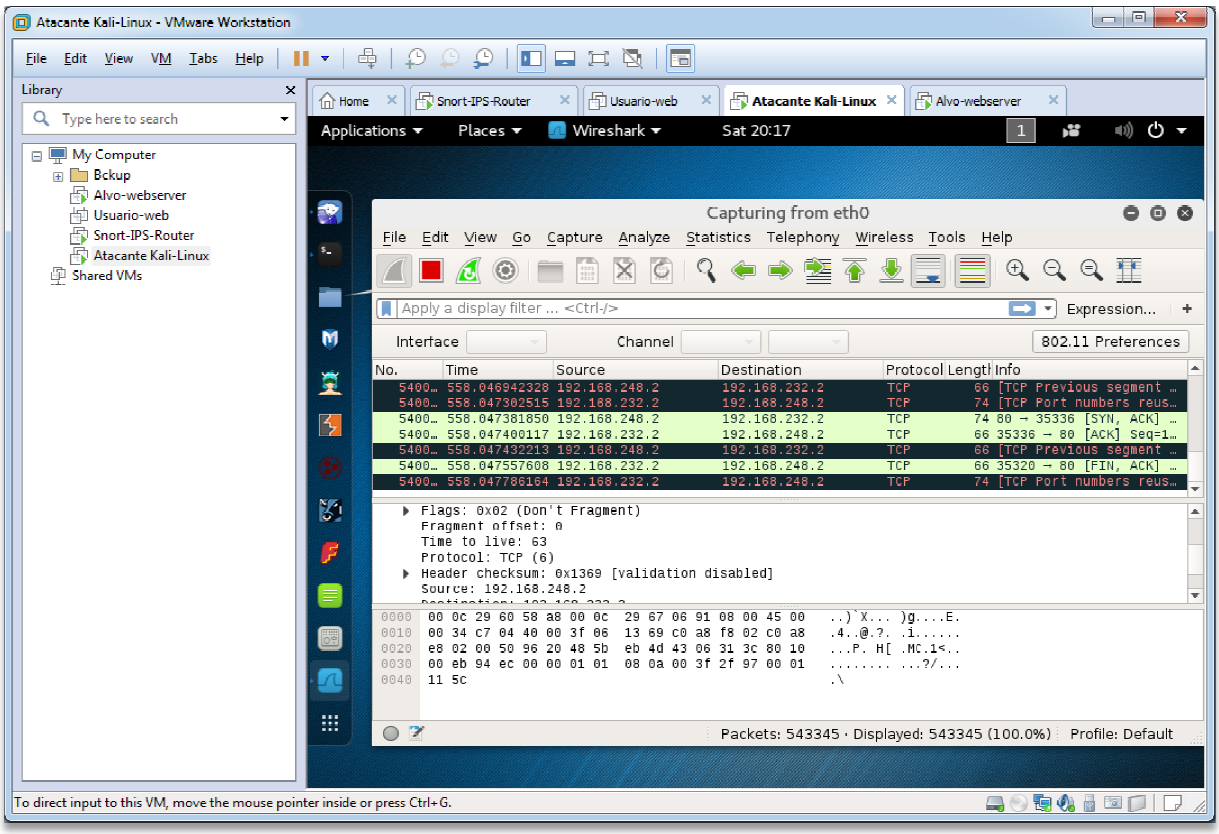
Fonte – Produzido pelo autor do trabalho,2016.

Como mostrado na figura 14, é disparado o seguinte comando de ataque de força bruta:***nmap -script http-brute -p 80 192.168.248.2***[24], por meio da ferramenta *Zenmap* ao servidor Alvo-webserver, onde o parâmetro 80 é a porta

[24] Comando de ataque de força bruta disparado pela ferramenta nmap ao endereço e porta especificados,esse comando consiste em fazer a varredura sistemática de chaves e senhas até encontrar a correta, percorrendo todo o espaço de busca.

utilizada para o tráfego em paginas web e 192.168.248.2 é o endereço IP do servidor Alvo-webserver.

Figura 15 Visualização do tráfego dos testes com o wireshark



Fonte – Produzido pelo autor do trabalho,2016.

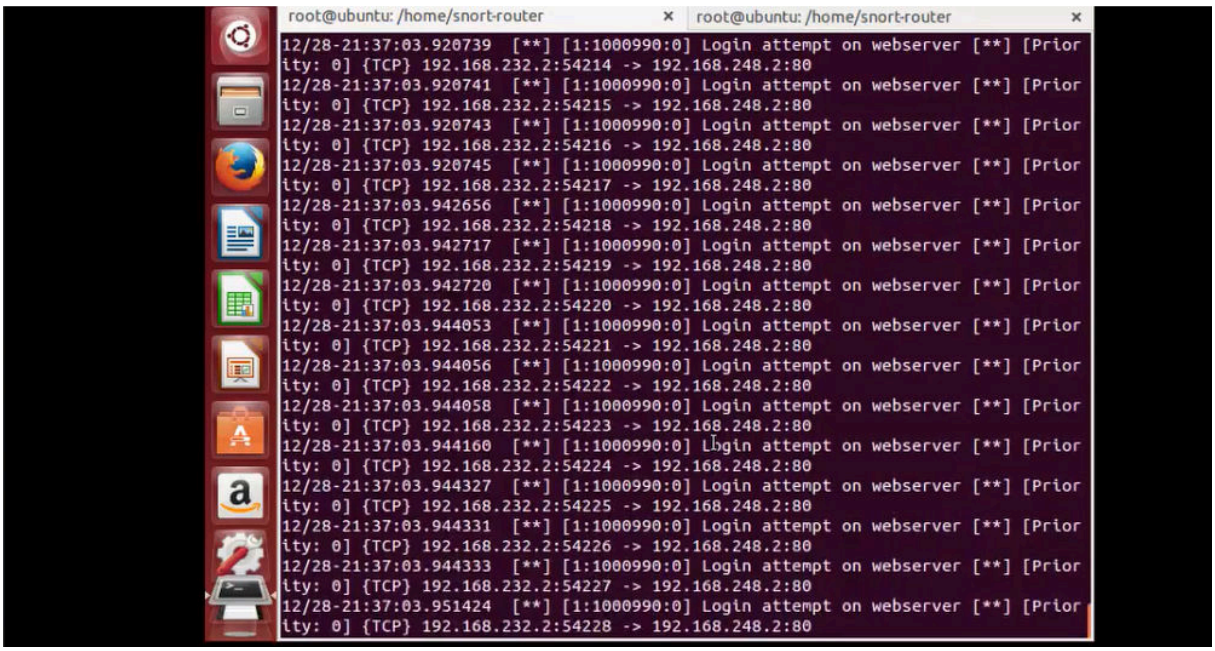
Observando a figura 15, pode ser visualizado por meio da ferramenta *wireshark*, após o comando de ataque de força bruta ao servido Alvo-webserver, o tráfego dos pacotes de origem da máquina atacante-kali-Linux (ip:192.168.248.2) ao destino servidor Alvo-webserver (ip:192.168.232.2).Fazendo a análise da tela, é verificado os tipos de protocolos presentes nesses pacotes.

4.6 Resultados Obtidos

Espera-se com os testes realizados, que o IPS Snort seja capaz de realizar o bloqueio proveniente de uma tentativa de ataque ao servidor Alvo-webserver.

Os resultados dos testes de bloqueio pelo Snort, são mostrados abaixo, onde, no primeiro teste, o snort encontra-se no modo passivo e no segundo teste no modo reativo ao ataque de força bruta pela máquina do atacante, ip 192.168.232.2 contra o servidor Alvo-webserver ip 192.168.248.2.

Figura 16 - Resultados gerados pelo Snort no modo passivo ao servidor Alvo-webserver

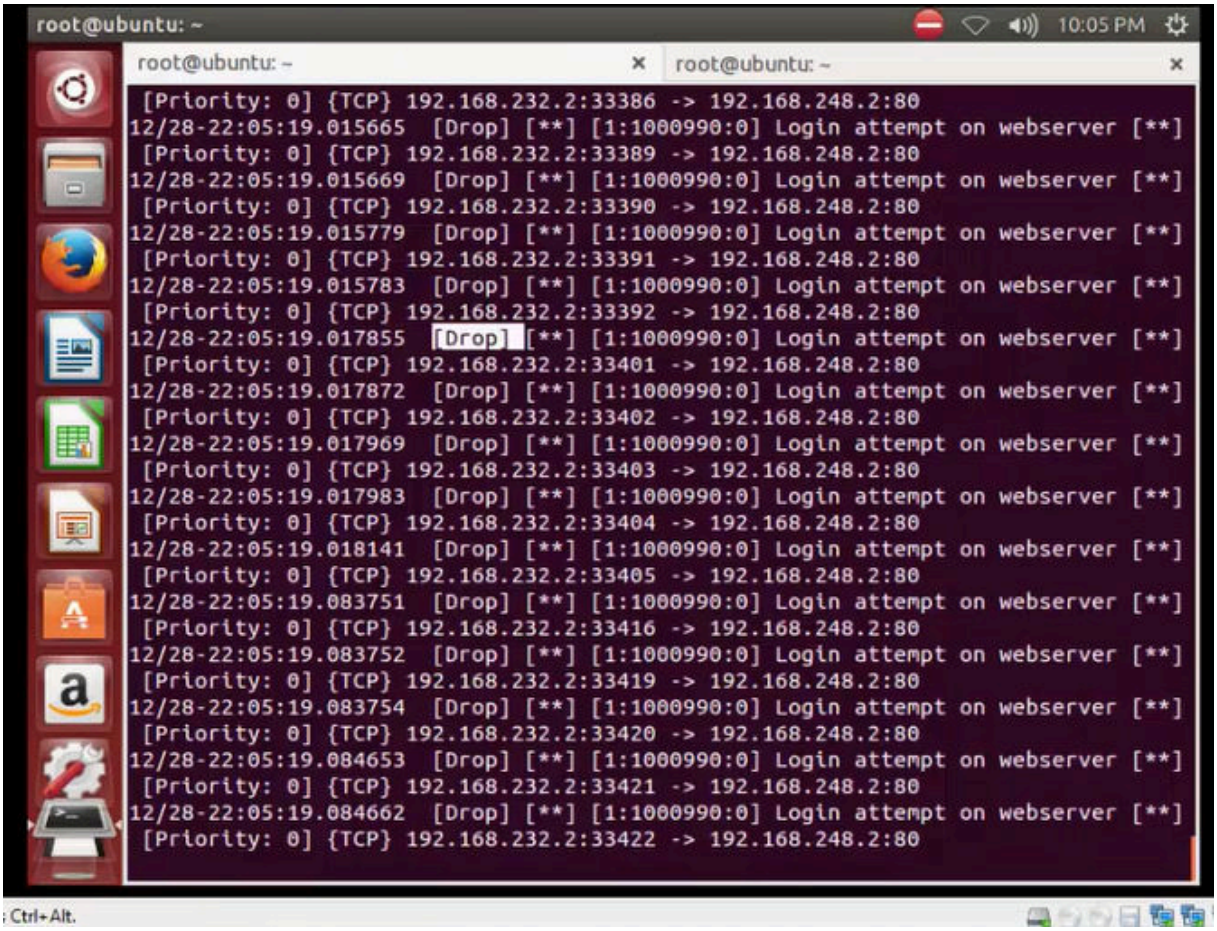


Fonte – Produzido pelo autor do trabalho,2016.

Pode-se notar na figura 16, que durante a detecção feita pelo snort no modo passivo, são gerados somente os alertas das tentativas de acesso ao servidor Alvo-webserver, disparados da máquina atacante-Kali-Linux(ip:

porta192.168.232.2:54223) para a máquina Alvo-webserver(ip: porta 192.168.248.2 :80), nessa verificação o servidor continua com o serviço de internet acessível.

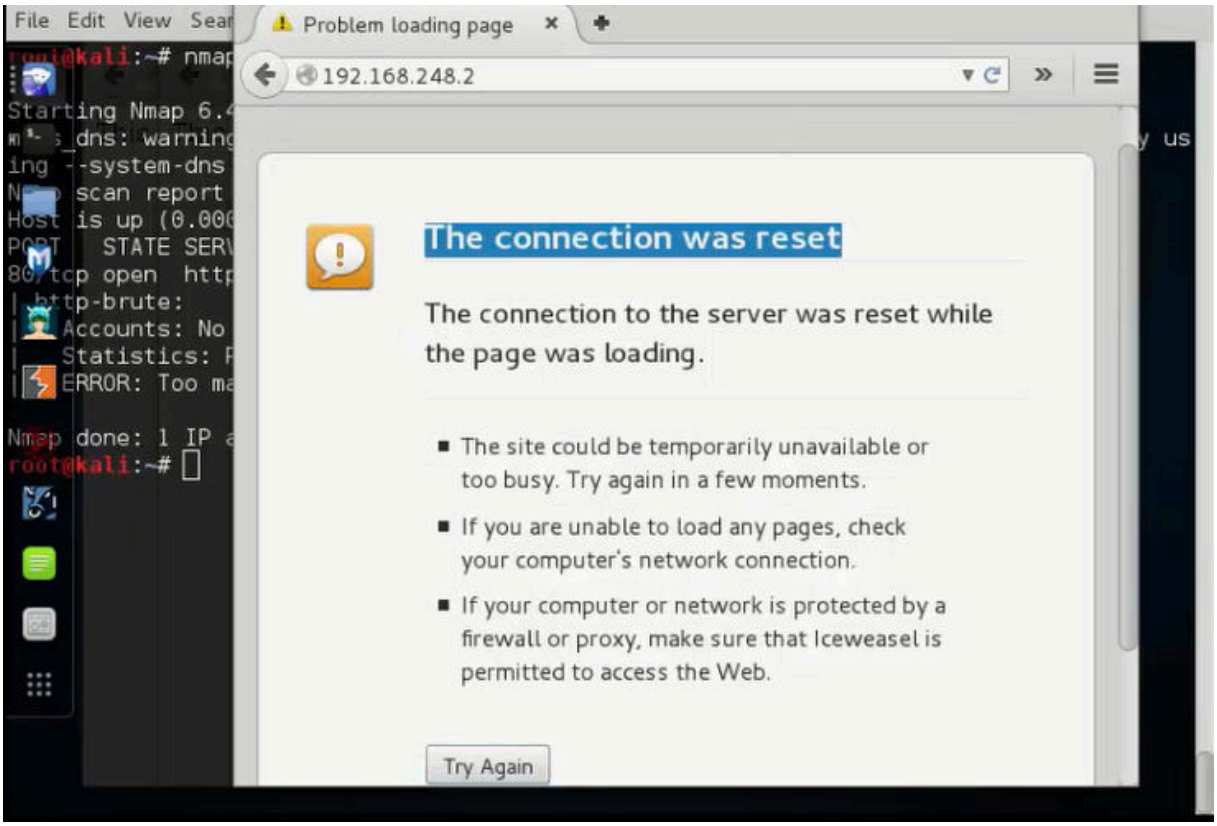
Figura 17 - Resultados gerados pelo Snort no modo reativo ao servidor Alvo-webserver



Fonte – Produzido pelo autor do trabalho,2016.

Diferentemente do que foi mostrado anteriormente, aqui na figura 17, durante a detecção feita pelo snort no modo de contenção, os pacotes além de serem detectados como tentativas de acesso ao servidor Alvo-webserver, eles são bloqueados, como destacado com o parâmetro Drop, nesse caso o serviço de internet é bloqueado para a máquina atacante.

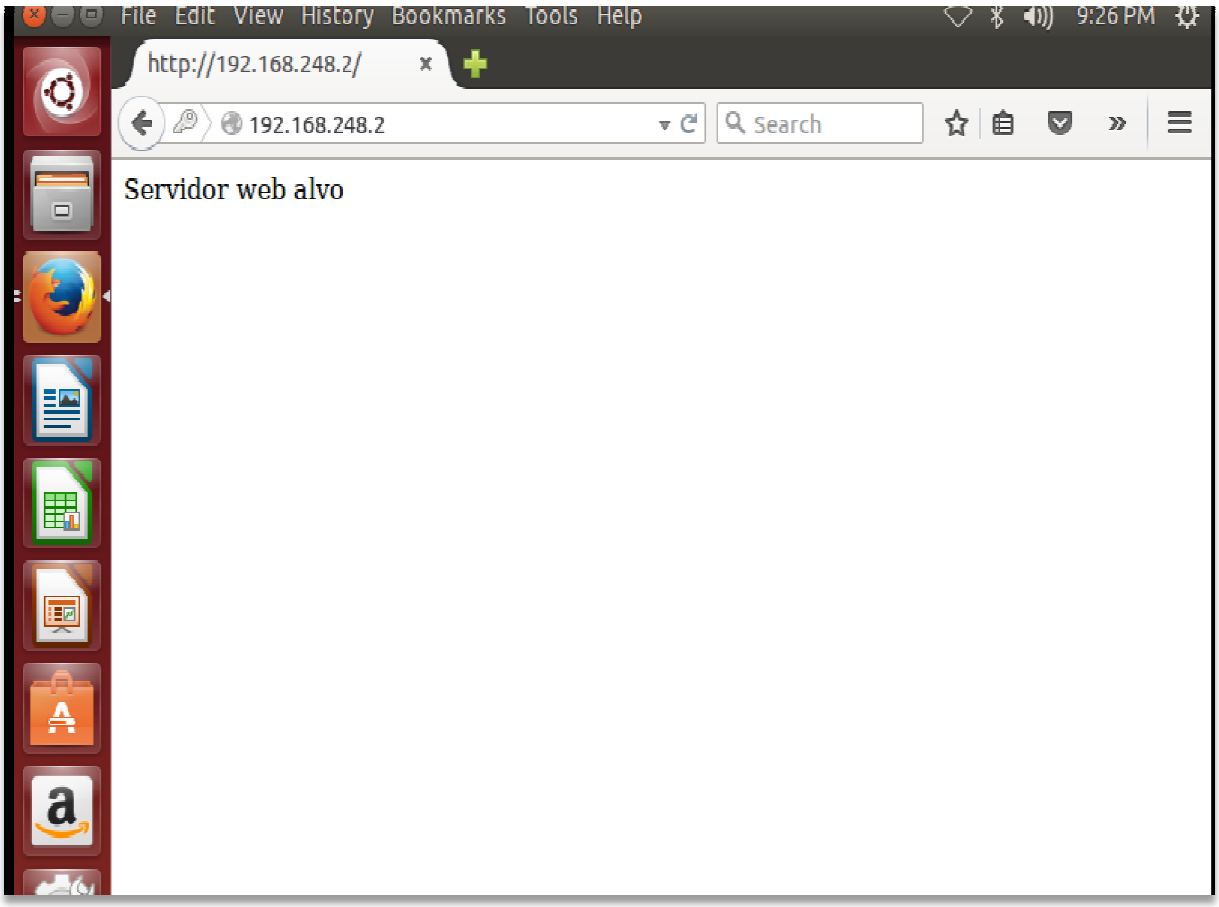
Figura 18-Reset na conexão para a máquina atacante-Kali-Linux ao servidor Alvo-webserver após o bloqueio feito pelo Snort.



Fonte – Produzido pelo autor do trabalho,2016.

Na figura 18, é visualizado o teste de conexão ao servidor Alvo-webserver da máquina atacante-Kali-Linux após o bloqueio feito pelo Snort, pode ser notado que a conexão sofre um reset, não permitindo mais acesso proveniente da máquina atacante.

Figura 19 - Teste de conexão ao servidor Alvo-webserver feito pela máquina usuario-web



Fonte – Produzido pelo autor do trabalho,2016.

Na figura 19, mesmo com o bloqueio feito pelo o Snort, a conexão ao servidor Alvo-webserver ficou liberada para a máquina usuario-web, diferentemente do reset na conexão para a máquina atacante-Kali-Linux, que foi bloqueada.

4.7 Dificuldades Encontradas

Algumas dificuldades foram encontradas no desenvolvimento deste trabalho:

- Atualização manual das regras de detecção do *Snor*t, pois neste trabalho não se optou pela atualização automática destas regras.
- Instalação de uma interface gráfica para visualização dos logs do *Snort*.
- Instalação de muitas dependências para a compilação do Snort inline.

4.8 Trabalhos Futuros

Por ser considerado um IPS muito utilizado em segurança de redes, e possuindo muitas ferramentas que podem ser adicionadas ao *Snort*, para a continuidade e melhoria de trabalhos futuros as seguintes implementações são recomendadas:

- A utilização do MySql para gravação dos logs do Snort;
- A opção por uma interface gráfica para visualização dos logs do Snort, como por exemplo o *BASE*[25](*Basic Analisy sand Security Engine*);
- Atualização de regras automáticas para o Snort;
- Criação de regras específicas para outros tipos de ataques.

[25]http://www.oracle.com/technetwork/systems/articles/snort-base-jsp-138895.html

CONCLUSÃO

A utilização de um IPS é uma importante ferramenta para a segurança de um ambiente de redes de computadores, pois além de realizar a detecção de tentativas de intrusões, faz também o bloqueio aos tráfegos suspeitos e envia os alertas aos administradores da rede, facilitando assim as tomadas de decisões para minimizar os impactos causados por incidentes de segurança.

Implementar e testar um sistema de detecção e bloqueio de intrusão em redes de computadores, teve uma grande contribuição para esta proposta de estudo, pois possibilitou a criação de uma camada extra de segurança com a utilização de ferramentas de software livre.

Nos testes realizados, foi verificado o funcionamento do IPS Snort como uma ferramenta que atendeu satisfatoriamente a proposta de estudo, pois foi capaz de realizar os bloqueios provenientes dos ataques de força bruta, ao qual foi submetido.

O estudo realizado teve como principal contribuição, a construção de conhecimentos acerca da importância de um sistema de detecção e bloqueio de intrusão frente as ameaças que comprometem a segurança em um sistema de informação.

REFERÊNCIAS

ABNT, NBRISO. IEC 27.002: 2005 (antiga NBR ISO/IEC 17799: 2005)-Código de Prática para a Gestão da Segurança da Informação.

BARKER, W. C. and LEE, A. (2004). Information security - volume ii: Appendices to guide for mapping types of information and information systems to security categories. NIST Special Publication 800-60

BEALE, J. Snort 2.1 Intrusion Detection, Second Edition. Syngress Publishing, 2004.

BISHOP, M. Computer Security: Art and Science. Addison Wesley, Bonston, MA, 2003.

CANSIAN, Adriano Mauro. Detecção de Intrusos em Redes de Computadores.Tese (Doutorado em Física Aplicada), Instituto de Física de São Carlos, São Carlos, 1997.

CASWELL, BRIAN at al. Snort 2 – Sistema de Detecção de Intruso - Open Source. Rio de Janeiro: Alta Books, 2003.

DA SILVA, Pilar; RANGHETTI, Denise; STEIN, Lilian Milnitsky. Segurança da Informação: uma reflexão sobre o componente humano. Ciências & Cognição, v. 10 2007

DONNER, Marcos Leandro; OLIVEIRA, L. R. Análise de satisfação com a segurança no uso de internet banking em relação aos atuais recursos disponíveis no canal eletrônico. XXXII Encontro da ANPAD–EnANPAD. Rio de Janeiro, 2008.

Education Press, Beijing and Springer-Verlag GmbH Berlin Heidelberg, 2009

KUMAR, Sandeep. Classification and Detection of Computer Intrusions. Tese (Doutorado), Department of Computer Sciences, Purdue University, Agosto, 1995.

LARI, PAULO AUGUSTO MODA; AMARAL, DINO MACEDO Snort, MySQL, Apache e ACID. Rio de Janeiro:Brasport, 2004.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. Ci. Inf., Brasília, v. 35,2006.

NAKAMURA, E. T. GEUS, PL de. Segurança de redes em ambientes cooperativos. São Paulo: Novatec, 2007.

NOBRE, JCA. Ameaças e Ataques aos Sistemas de Informação: Previnir e antecipar. Cadernos UniFOA, Volta Redonda, ano 2. n. 5, dez. 2007. 2013.

PIETRO, Roberto Di, MANCINI, Luigi V. Intrusion Detection Systems. Springer Publishing Company: Nova Iorque. 1st ed. 2008.

ROSS, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., ROGERS, G., e Lee, A. “Recommended Security Controls for Federal Information Systems”. NIST Special Publication 800- 53, February 2005.

RUSSELL, Deborah; GANGEMI, G. T. Computer security basics. " O'Reilly Media, Inc.", 1991.

SÊMOLA, Marcos. Gestão da segurança da informação. Vol. 1. Elsevier Basil, 2003.

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. Pearson Prentice Hall, 2008.

SUNDARAM, Aurobindo. An introduction to intrusion detection. Crossroads:The ACM Student Magazine, 2 ed. Abril, 1996.

TANENBAUM, Andrew S. "Computer networks, 4-th edition." ed: Prentice Hall (2003).

TORRES,Gabriel.Redes de computadores.1edição.Rio de Janeiro:Nova terra, 2009.

WANG, Jie. Computer Network Security: Theory and Practice. Higher

APÊNDICE

A Instalação e Configuração

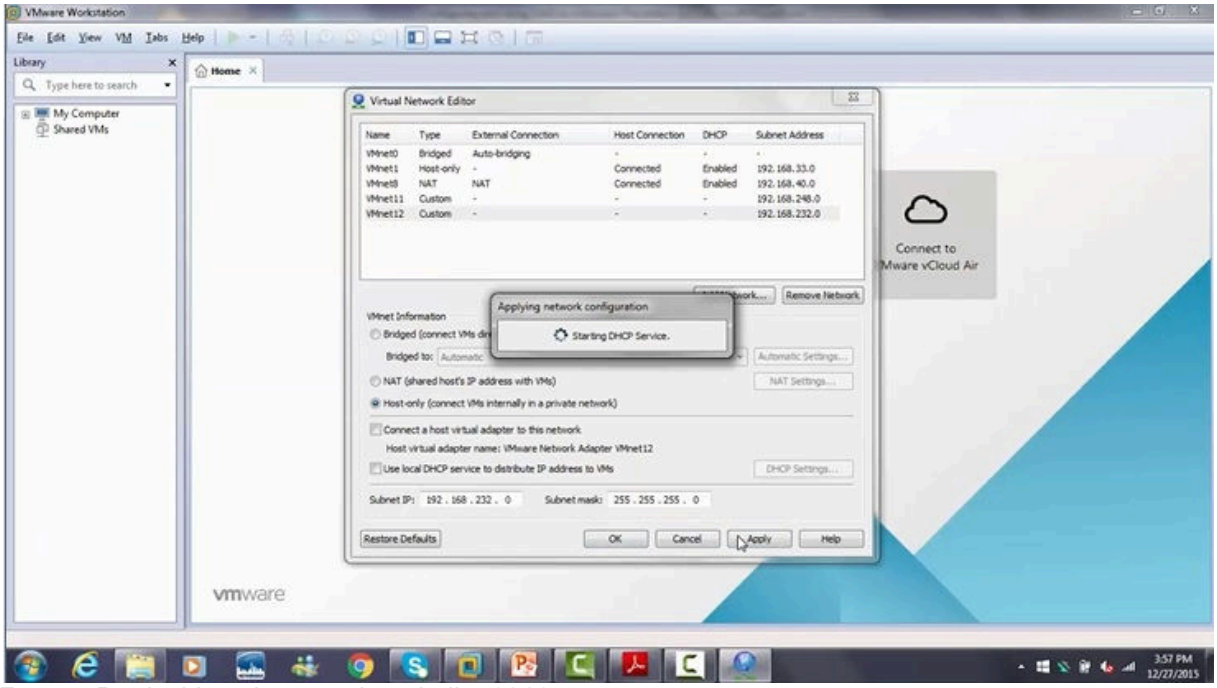
Será mostrado neste anexo, algumas telas de instalação e configuração das ferramentas utilizados para o desenvolvimento deste trabalho.

Criação das máquinas virtuais

As quatro máquinas virtuais instaladas tiveram as mesmas configurações de armazenamento e memória, todas utilizaram o sistema operacional de software livre Linux

.

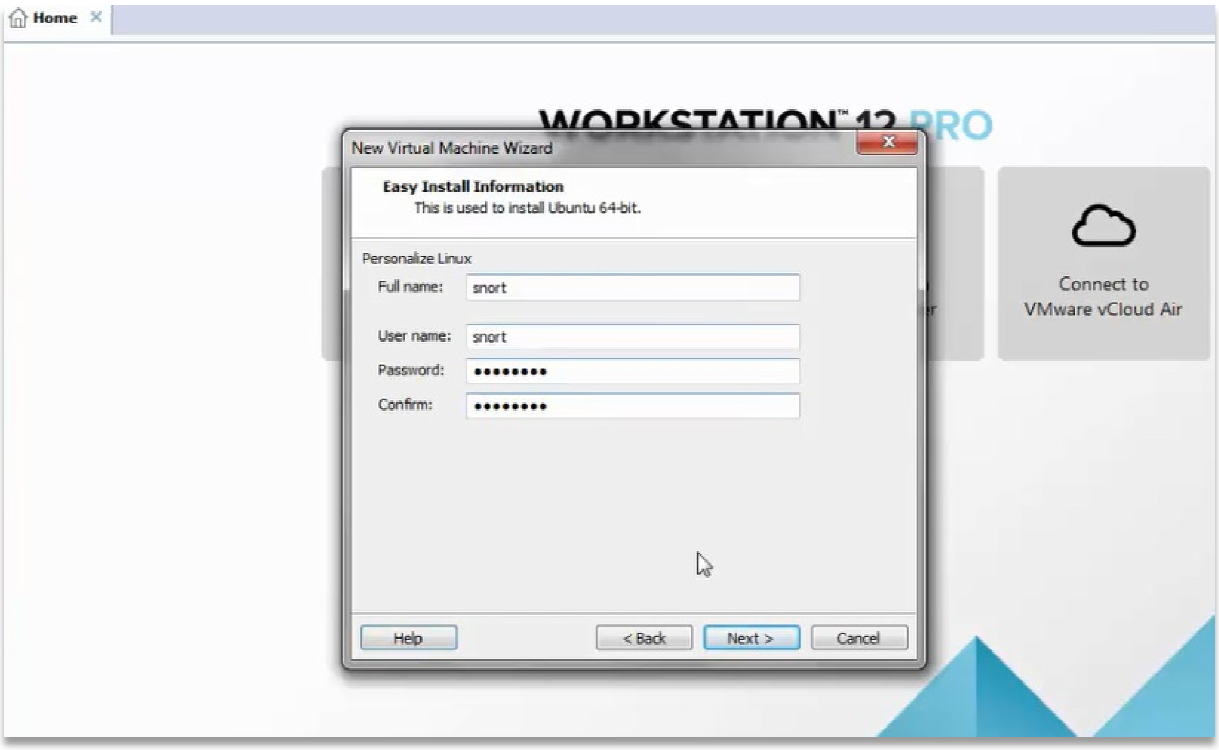
Figura A -1 Instalação do VmWare Workstation Pro



Fonte – Produzido pelo autor do trabalho,2016.

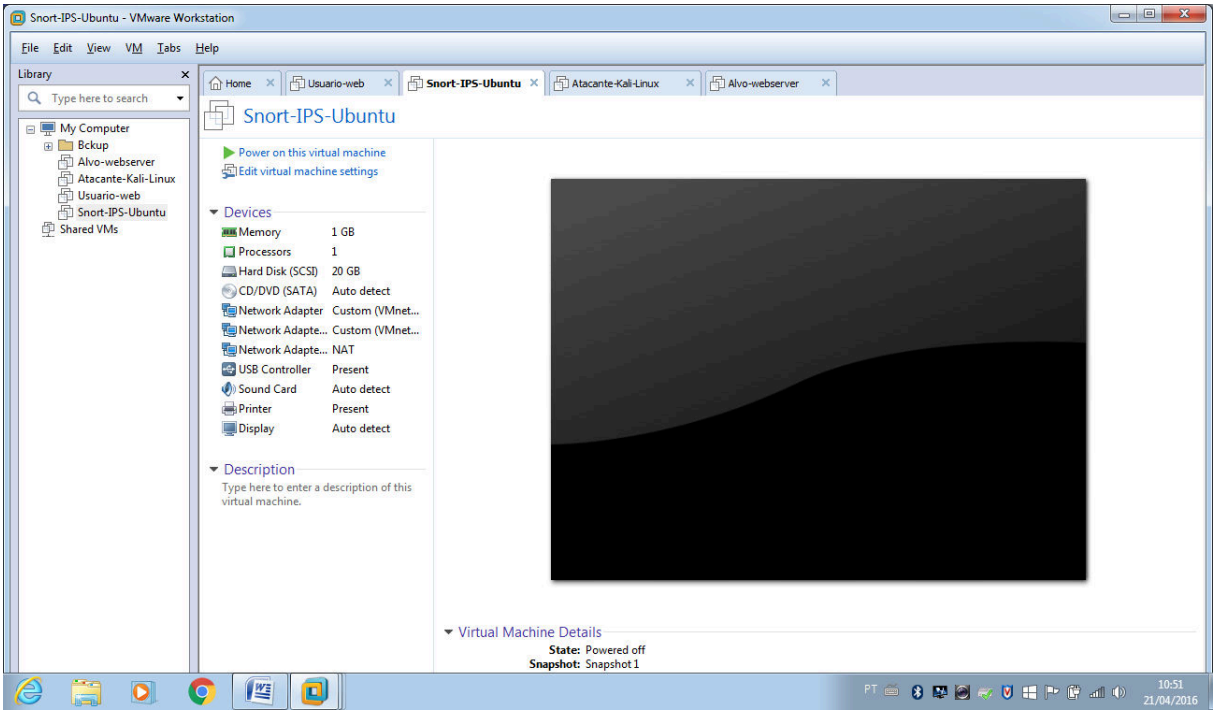
Na figura A-1, é mostrado a instalação da ferramenta de virtualização do ambiente de testes, o VMware Workstation, onde serão instaladas as máquinas virtuais alvo, atacante, snort e usuário web.

Figura A-2 Criação da máquina virtual Snort no VMware Workstation Pro



Fonte – Produzido pelo autor do trabalho, 2016.

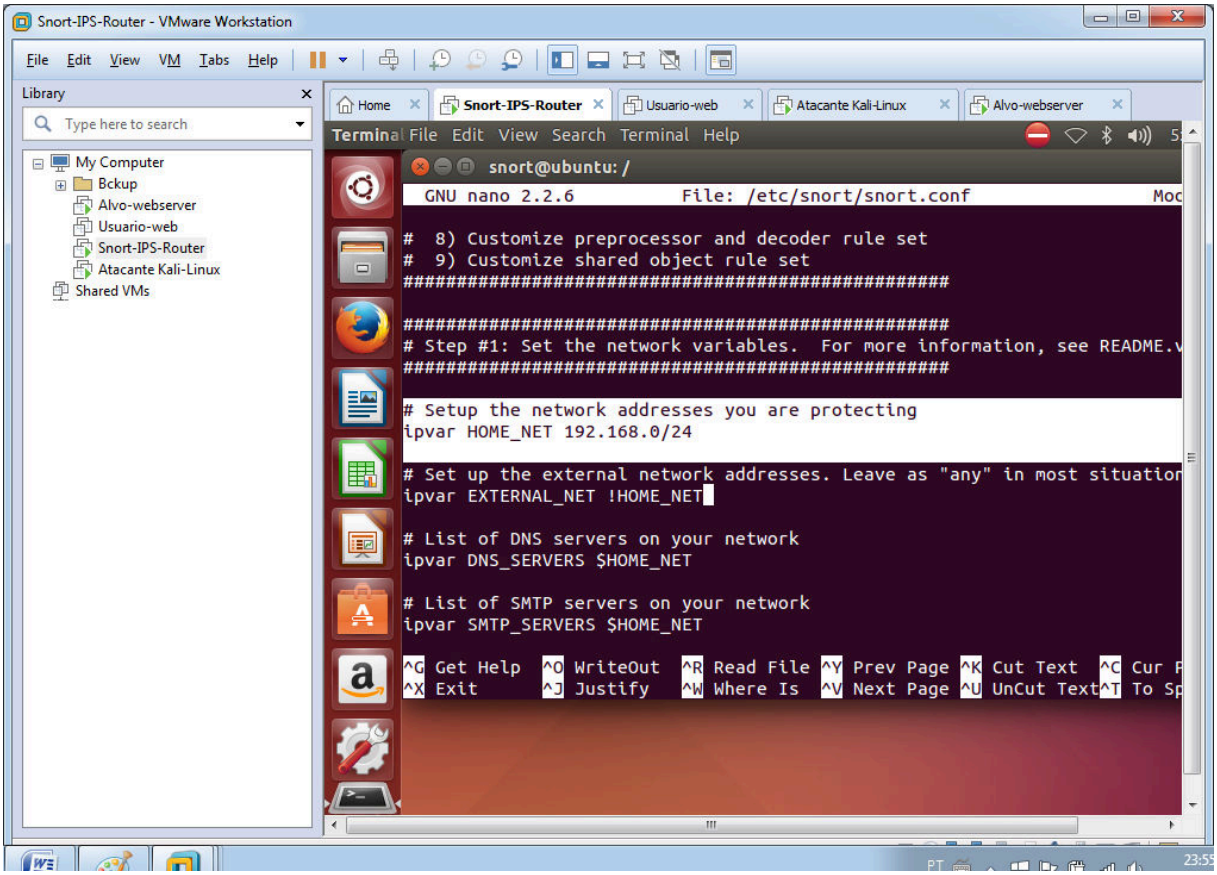
Figura A-3 Ambiente de testes VMWare Workstation



Fonte – Produzido pelo autor do trabalho, 2016.

Como demonstrado na figura A-3, o ambiente virtual de teste possui as máquinas Alvo-webserver, atacante-Kali-Linux, Usuário-web e Snort-IPS-Ubuntu.

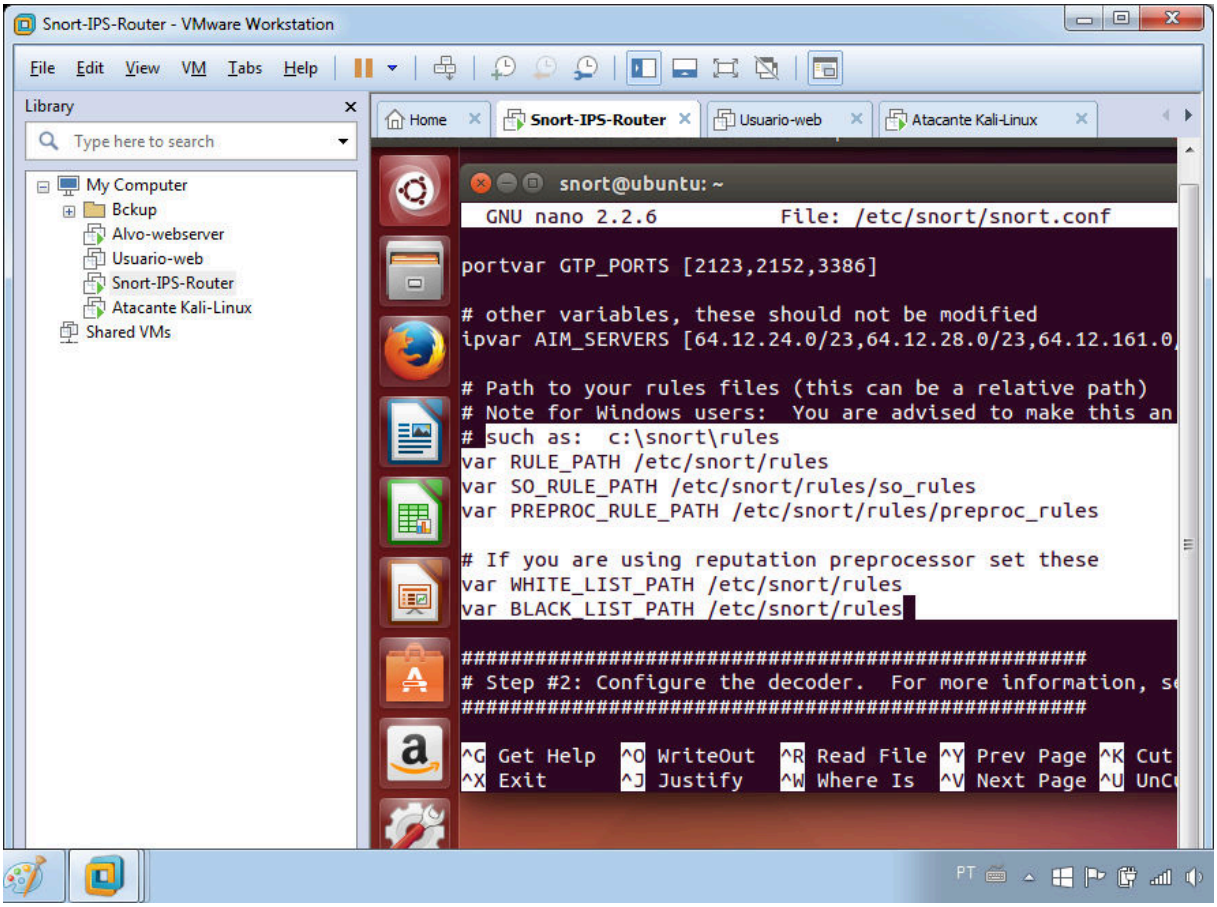
Figura A-4 Delimitação do range de rede a ser protegido pelo snort.



Fonte – Produzido pelo autor do trabalho,2016.

Na figura A-4, o trecho selecionado representa o range de ip da rede a ser protegido pelo IPS-Snort, essa configuração é feita no arquivo /etc/snort/snort.conf. As máquinas que estiverem nesse intervalo de rede serão protegidas.

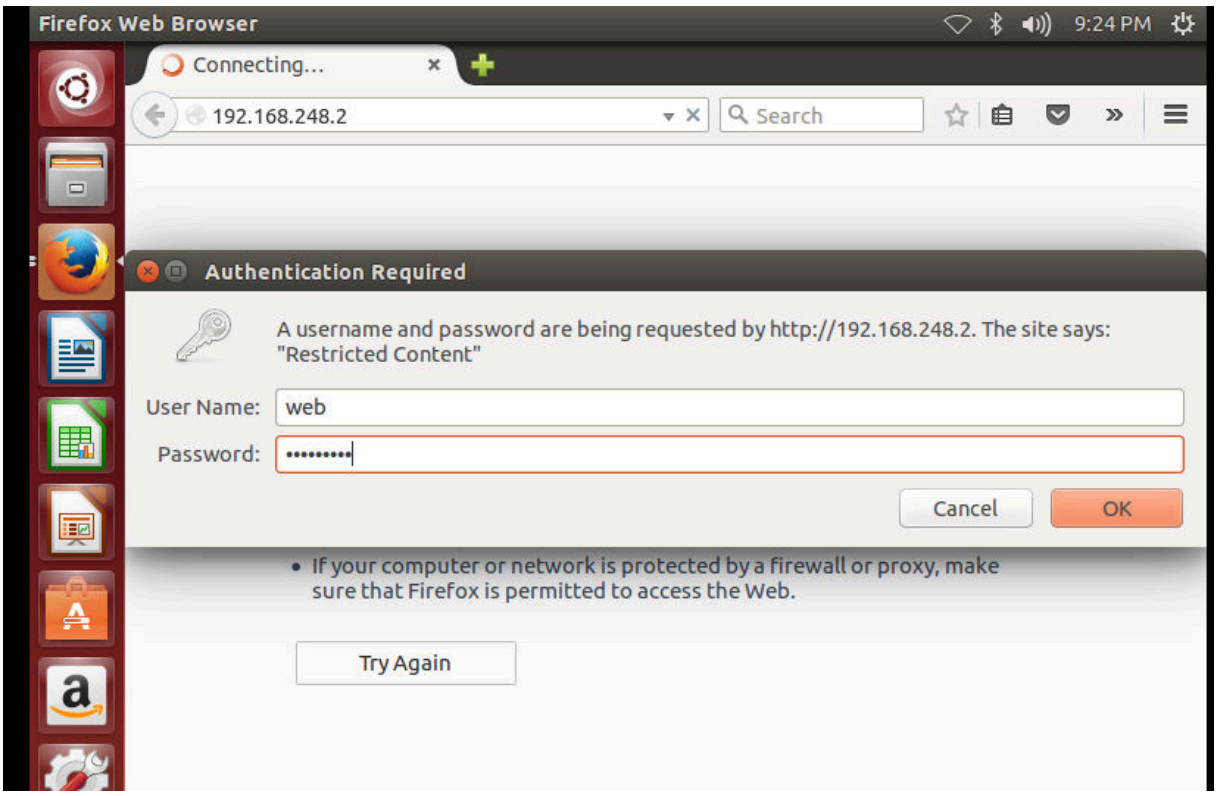
Figura A-5 Local de armazenamento das regras do Snort.



Fonte – Produzido pelo autor do trabalho,2016.

A tela A-5 mostra o local de armazenamento das regras do Snort,(arquivo /etc/snort/rules) que pode ser editado no arquivo de configuração do snort (/etc/snort/snort.conf).

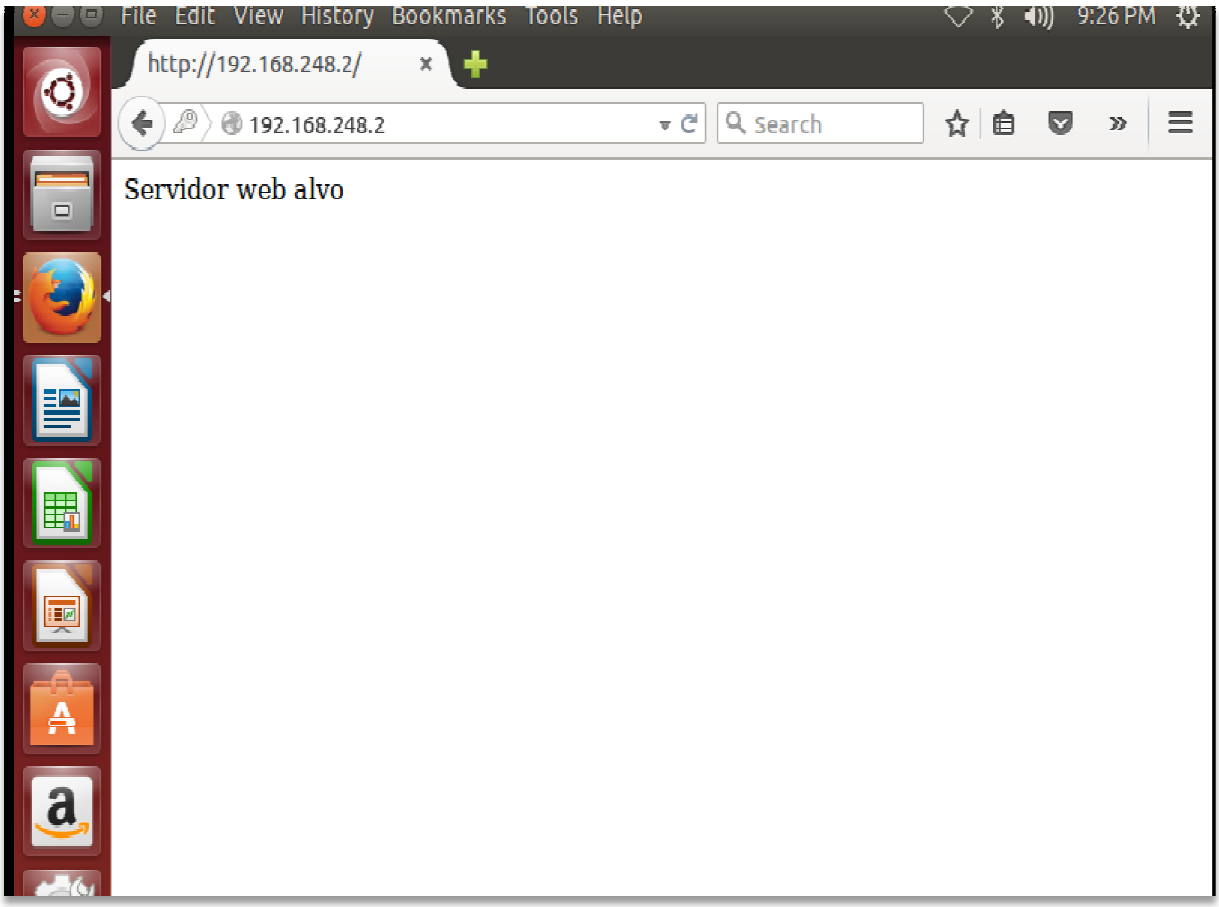
Figura A-6 Login na página web do servidor Alvo-webserverpara testar o apache



Fonte-Elaborado pelo autor,2016.

Na figura A-6, é mostrado a tela de acesso da página web do servidor Alvo-webserver.

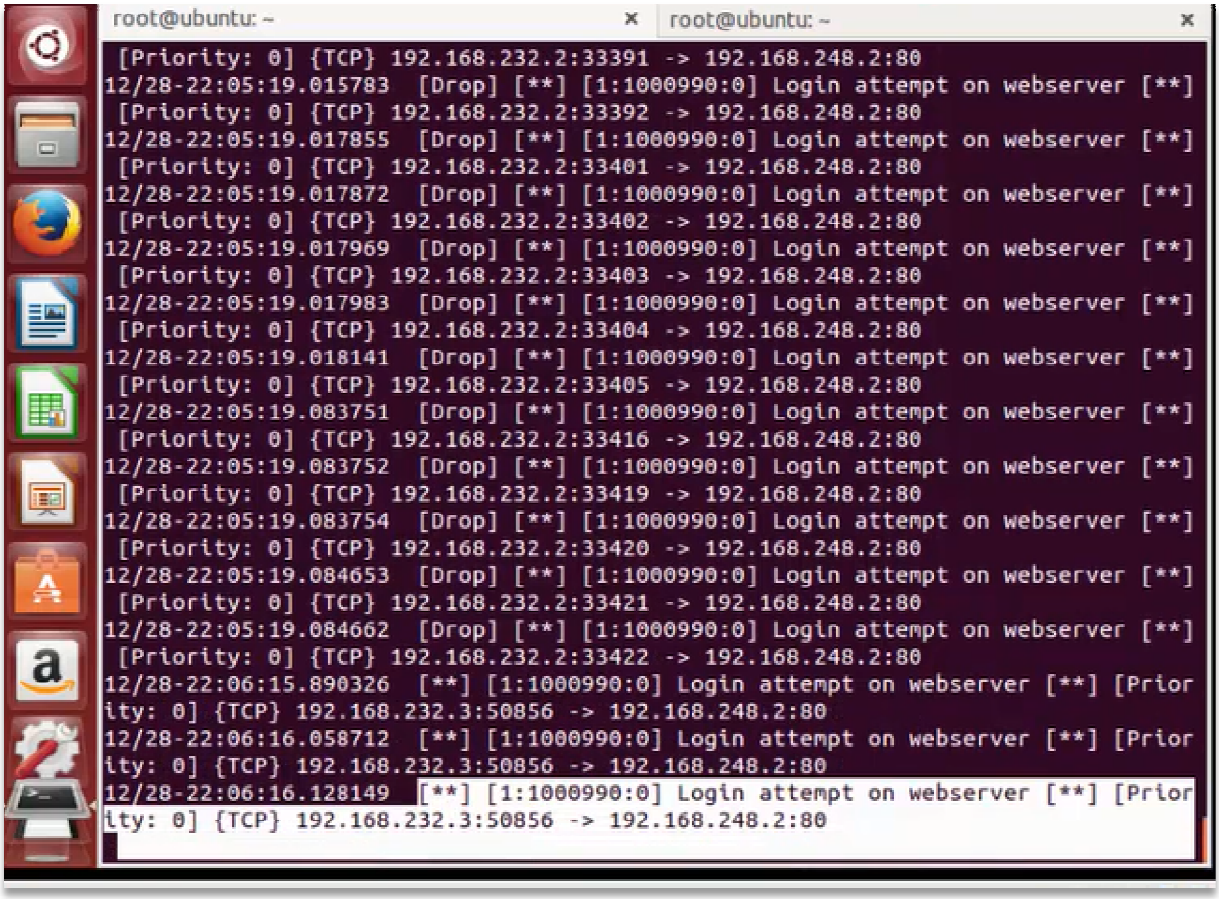
Figura A-7 Teste de conexão na página web do servidor Alvo-webserver



Fonte – Produzido pelo autor do trabalho, 2016.

De acordo com a figura A-7, é exibida a página web do servidor Alvo-webserver sendo acessada para testar a conexão.

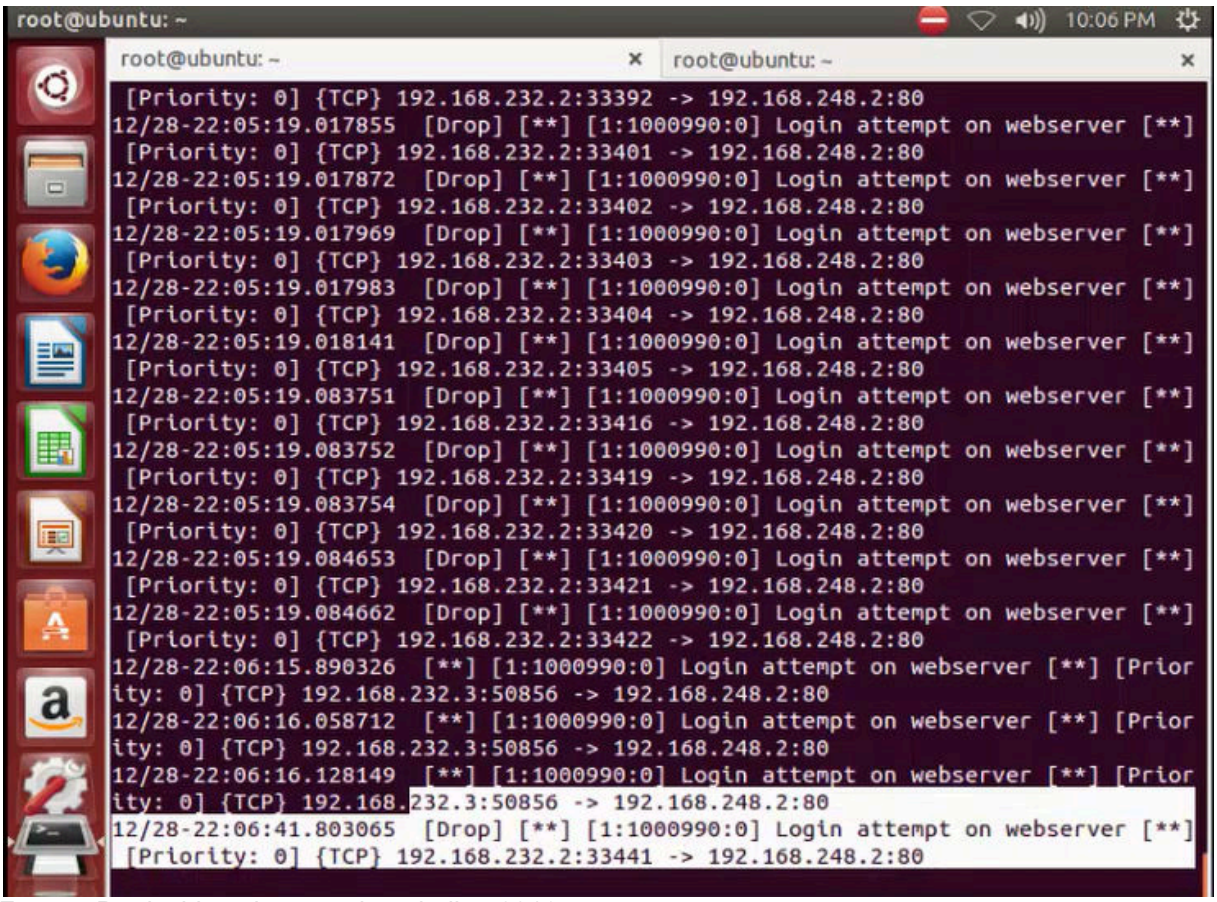
Figura A-8 Acesso liberado feito pelo usuário web ip 192.168.232.3 ao servidor alvo-webserver



Fonte – Produzido pelo autor do trabalho, 2016.

Após ser detectado pelo Snort a conexão da máquina usuário-web (ip 192.168.232.3) o acesso é liberado, conforme mostrado na figura A-8 na parte destacada.

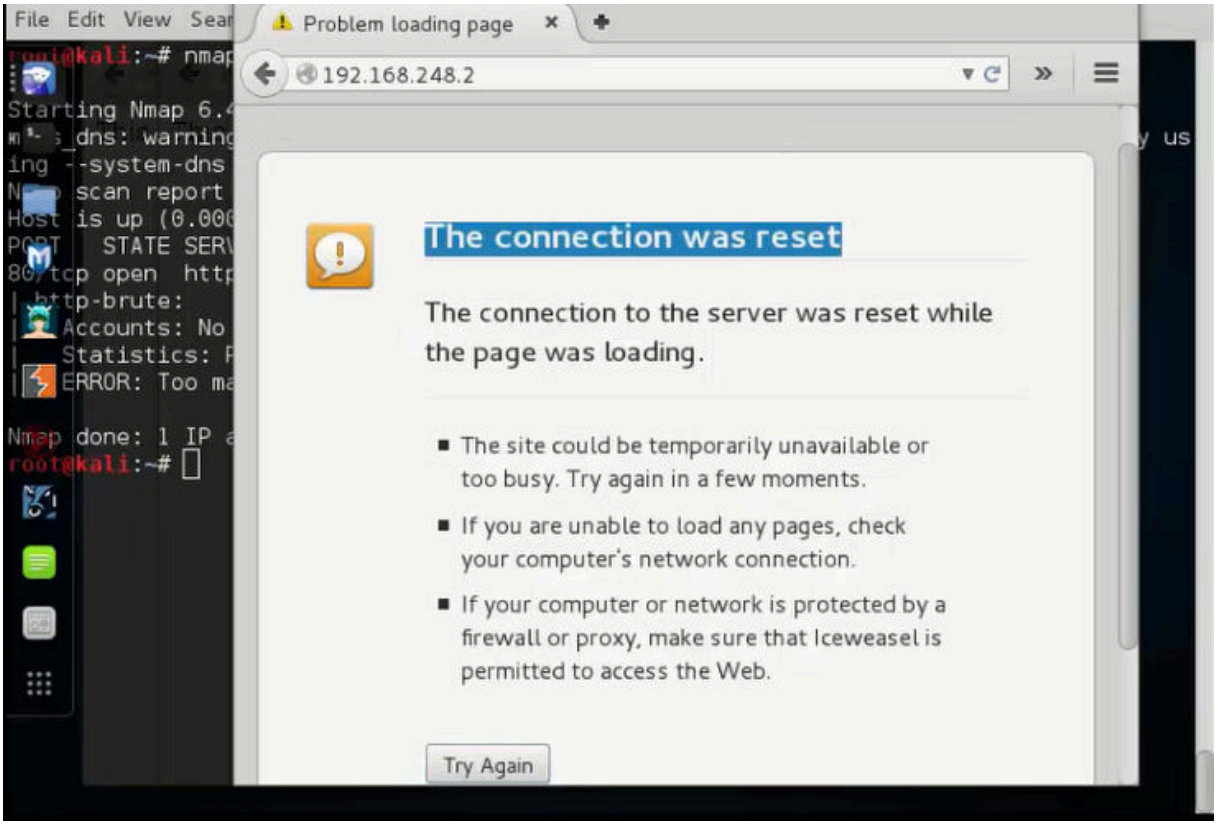
Figura A-9 Bloqueio feito pelo snort ao servidor alvo-webserver pelo atacante KaliLinux



Fonte – Produzido pelo autor do trabalho, 2016.

Na figura A-9, é mostrado na parte em destaque, o bloqueio feito pelo Snort à máquina atacante-Kali-Linux (ip 192.168.232.2:33441) ao servidor Alvo-webserver.na porta 80 (ip:192.168.248:80)

Figura A-10 Falha de conexão ao servidor Alvo-webserver após o bloqueio feito pelo Snort



Fonte – Produzido pelo autor do trabalho, 2016.

Na figura A-10, é mostrado o reset da página web do servidor Alvo-webserver feito para a máquina atacante-Kali-Linux, uma vez que teve o bloqueio pelo Snort. na figura anterior.