ANOMALIAS E SEGURANÇA EM REDES COMPUTACIONAIS: Uma abordagem prática com ataque DOS

Renato Pereira Imaisumi[1], Henrique Pachioni Martins[1].

Departamento de Informática – Faculdade de Tecnologia de Bauru (FATEC)

Rua Manoel Bento Cruz, n° 30 Quadra 3, Centro, 17.015-171 – Bauru, SP - Brasil

{renato.imaisumi, henrique.pachioni01}@fatec.sp.gov.br

Abstract. *Regarding to the growing global demand for interconnectivity of network equipment, on-line devices and their operational systems, where services are provided in a decentralized manner, supporting numerous transactions that are realized through the internet. Therefore a demand for security in order to ensure the quality of services offered in the internet, was created based on some concepts as: Confidentiality preservation, integrity and information availability. This study suggests an analysis of anomalies in a computer network and their effects, proposing possible solutions for identifying and preventing security measures.*

Resumo. *Com a crescente demanda mundial por interconectividade de equipamentos, dispositivos em rede e seus sistemas, onde serviços entre redes são fornecidos de modo descentralizado dando suporte a inúmeros negócios consolidados através da rede, foi gerada uma necessidade grande por segurança, a fim de zelar e garantir a qualidade dos serviços ofertados. Que são baseadas em alguns pilares como: preservação da confidencialidade, integridade e disponibilidade da informação. O presente estudo sugere uma análise de anomalias em redes computacionais e seus efeitos, propondo possíveis soluções para identificação e prevenção com medidas de segurança.*

Palavras-Chave: Anomalias em redes, segurança em rede, DOS, T50, SLOW LORIS.

1. INTRODUÇÃO

A crescente demanda mundial por interconectividade de equipamentos, dispositivos e seus sistemas em redes, gerou uma necessidade grande por segurança, que deve ser baseada em alguns pilares como: preservação da confidencialidade, integridade e disponibilidade da informação (NBR-ISO-IEC-27001, ABNT, 2006). Esses equipamentos e dispositivos de comunicação trocam dados através de estruturas em redes interconectadas, resultando assim na convergência digital, onde negócios são realizados e até mesmo informações confidenciais são transmitidas o tempo todo em grades volumes.

Segundo Rangel (1999), essa proliferação de computadores e dispositivos é devida a confiabilidade e velocidade da transmissão, o poder computacional disponível e também o seu barateamento aquisitivo. Consequentemente, com essa convergência problemas e falhas surgiram, e o que era confiável e seguro passou a ser vulnerável e incerto, apresentando problemas que poderiam ser enumerados como: ameaças com a segurança por tentativas ou acessos não autorizados a uma rede ou sistema, proliferação de vírus e roubo de dados.

Esses problemas podem ou não gerar comportamentos observáveis no servidor, que fugindo do esperado, podem ser chamados de anômalos. Alguns tipos de ameaças ou ataques manifestam comportamentos diferentes.

Isso resultou na necessidade de práticas que visam solucionar ou atenuar danos ocasionados por ameaças ou ataques. Práticas como o monitoramento podem ajudar a analisar uma rede e seus sistemas, mas que por si só não resolvem o problema. Aplicar um sistema especialista baseado em assinaturas pode ser uma melhor resposta. A utilização de um *firewall* a fim de filtrar e evitar que ataques sejam realizados com sucesso, afetando um servidor ou comprometendo uma rede, visam garantir a qualidade dos serviços na rede, ou seja, assegurar que dados cheguem ao seu destino, preservando a disponibilidade da informação.

As anomalias existentes hoje são detectadas baseadas em assinatura de ataque ou desvio de comportamento, através dos programas antivírus ou sistemas especialistas. A análise através de monitoramento possibilita detectar eventos que ocorram fora do esperado ou permitido, podendo considera-los como anomalias. Assim, demonstrando a necessidade de propor possíveis soluções tanto para inibir como amenizar seus efeitos com medidas de segurança.

No decorrer do presente trabalho, pretende-se responder à seguinte questão: “Quais as medidas preventivas e corretivas mais importantes, observando as anomalias geradas em um servidor em um ambiente de rede, a serem considerados após a análise de dois tipos de ataques com comportamentos diferentes?”.

O objetivo desse trabalho é executar três ataques a um servidor e monitora-lo observando três parâmetros: o uso de processamento, memória física e tráfego. Os ataques têm como propósito deixar o serviço indisponível. Mostrar também como esses ataques se manifestam de maneiras diferentes, provocando anomalias no servidor e rede, demonstrando a necessidade da utilização de um sistema de detecção e prevenção de intrusão baseado em assinaturas e regras, para a segurança.

A motivação é aumentar as pesquisas relacionadas ao tema proposto criando assim um referencial prático que poderá ser usado em trabalhos futuros para definir um comportamento anômalo em redes de computadores, no caso de um ataque de negação de serviço.

Alguns estudos, baseados nessas práticas, fornecem bases de dados que são utilizadas posteriormente para a identificação de um padrão aplicando mineração de dados, como a base que foi construída durante o

KDD cup (Knowledge Discovery in Data Competitions). Com esse padrão encontrado, é possível compará-los com os resultados obtidos de outras bases de dados, criando bases e regras atualizadas.

2. REFERENCIAL TEÓRICO

Nessa seção serão discutidos os assuntos referentes a anomalias, segurança, entre outros, como histórico de ataques e incidentes reportados.

2.1 Anomalias

Buscar por anomalias em uma rede de computadores é também procurar por alterações em um padrão comportamental em se falando de tráfego em rede (PERLIN, 2011). A grande dificuldade em análise de anomalias esta na sua complexidade de apresentação de resultados, ora positivo, ora negativo, podendo assumir valores dúbios, ou seja, duvidosos, conhecidos como falsos positivos. Isso porque sistemas de detecção de intrusão podem acusar erroneamente algo anormal devido a vários fatores que podem ser provocados, até mesmo por uma alteração de energia.

De acordo com a IBM (2013) a anomalia de rede é vista como analítica do comportamento da rede, enquanto ameaças à segurança, comportamento hostil de usuários, problemas na infraestrutura, como violações a politicas de seguranças e alterações não permitidas.

2.2 Segurança da Informação

A segurança da informação visa proteger contra a divulgação indevida da informação, a preservação da informação em sua integralidade sem que sofra modificação por partes não autorizadas, que ela esteja disponível para o usuário autorizado sem sofrer rejeição e também garantir que os dados disponíveis estejam íntegros.

Segundo a norma NBR-ISO-IEC-27001, ABNT, 2006: Além da preservação da confidencialidade, integridade e disponibilidade da informação outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

2.3 Vulnerabilidades

De acordo com o CERT.br (2006), pode ser considerado uma vulnerabilidade, uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um hacker, resulta na violação da segurança de um computador ou rede de computadores.

2.4 Tipos de ameaças

Alguns tipos de ameaças podem ser responsáveis por provocar um comportamento indesejado tanto no lado do servidor ou do cliente, podendo comprometer uma rede.

2.4.1 Vírus

Segundo a Microsoft (2013), estes são programas maliciosos que de maneira geral danificam arquivos ou o Sistema Operacional do computador, pode ser transmitido por meio da troca de arquivo entre máquinas, em uma rede ou não.

2.4.2 Ataques

Existem diversos tipos de ataques, alguns com um mesmo objetivo embora tenham comportamentos diferentes na maneira de atuar. Segundo o Serpro (2013), o ataque DDoS (*distributed denial-of-service* -

ataque distribuído de negação de serviço) é um tipo que envolve uma saturação de tentativas de acesso a um servidor que hospeda um sítio, por exemplo como os servidores possuem um limite no número de pedidos de troca de informações que podem receber.

Algumas vezes esse tipo de negação de serviço pode ser resultado de um congestionamento temporário causado por um grande volume de solicitações legitimas de usuários que não tem a intenção em atacar o servidor, o que gera um falso positivo com relação a detecção de ataques.

2.5 T50

Segundo o site oficial do projeto T50, este é uma ferramenta para injeção de pacotes. Diferentemente do *slow loris*, funciona utilizando um único *socket*, com suporte a múltiplos protocolos. A ferramenta foi acoplada ao Back Track 5[1] como uma ferramenta para teste de saturação em redes.

De acordo com Brito (2012), um dos criadores da ferramenta, a sua verdadeira funcionalidade é testar redes TCP/IP (*Transfer control protocol/Internet protocol* – protocolo de controle de transferência/protocolo de internet) a fim de baratear o custo para testar o tráfego em uma rede, economizando assim em compra ou aluguel de equipamentos. O autor reconhece que seu uso pode ser aplicado para o DoS (ataque de negação de serviço) ou DDoS e se isenta da criação dessa ferramenta para esses fins, sendo indicado apenas para pesquisas.

2.6 Slow Loris

Uma técnica de ataque de negação de serviço desenvolvida pelo pesquisador em segurança conhecido como RSnake. O script é feito para abrir de maneira simples uma sessão HTTP (*HyperText Transfer Protocol* - Protocolo de Transferência de Hipertexto) e mantê-la aberta por muito mais tempo do que normalmente ficaria. De acordo com comentários feitos no próprio código, o script funciona como se pessoas estivessem na fila para o pagamento de suas compras em uma loja, onde cada um encontra com seu caixa, os sockets, e pagam suas compras em centavos, tomando muito tempo.

O *slow loris* utiliza os cabeçalhos HTTP (centavos) e mantém adicionando um novo cabeçalho a cada 5, 10 ou 299 segundos. Então o "caixa" do Apache não tem memória suficiente, pois quando cada novo cabeçalho é adicionado, o contador do timeout é resetado. Com essa técnica é possível bloquear cada tarefa do servidor ou *prefork process*, a trazer o servidor web para uma completa parada. Isso porque por padrão a configuração do timeout do Apache é de 300 segundos, assim, cada cabeçalho adicionado pode alargar o tempo de saída (RSNAKE 2013).

Em relação à auditoria, esse método de ataque não irá mostrar que o servidor está sofrendo um ataque. Assim como as mensagens no log de erros no servidor serão escassas. A CPU estará parada, sem operações de entrada e saída no disco e dificilmente será possível visualizar qualquer tráfego na rede. O que será possível observar será um enorme número de conexões de redes abertas como status de "estabelecidas", *stabilish state.*

2.7 Sistema de detecção de intrusão

Sistema de detecção de intrusão ou IDS (*Intrusion Detection System*) é uma ferramenta capaz de identificar tentativas de invasão em tempo real. Os IDS são classificados em dois tipos: NIDS (baseados em redes), cujo

[1] O Backtrack é um sistema operacional Linux baseado no Ubuntu, que tem como foco testes de segurança e de penetração (*pen tests*).

examinam o tráfego de rede e HIDS (baseado em host), que examinam o sistema. Ele tem o propósito de garantir a integridade do serviço prestado e seu perfeito funcionamento.

Um IDS analisa os pacotes que trafegam na rede comparando-os com assinaturas de ataques, caso seja positivo, de acordo com configurações definidas pelo administrador da rede, ele pode impedir o ataque. Segundo o Serpro (2013), um sistema de detecção ou prevenção de intrusão, conhecidos como IPS (*Intrusion Prevention System*) e IDS (*Intrusion Detection System*), tem como função verificar o tráfego na rede buscando trocas de dados atípicas, além das anomalias, e impedem a invasão.

Como exemplo, temos o Snort, que é uma ferramenta de detecção de intrusão usadas no mundo todo acoplada no Back Track 5, utilizada por administradores de redes em descobrir e prevenir ataques distribuídos de negação de serviço.

2.8 Histórico de ataques

Segundo o Serpro (2013), Serviço Federal de Processamento de Dados, órgão administrador da Infovia, estrutura de rede óptica metropolitana que é utilizada como canal de comunicação de dados pelos Ministérios, e que também administra sites do governo como www.presidencia.gov.br, www.brasil.gov.br e www.receita.fazenda.gov.br, quando um ataque é constatado, os logs de dados, que são registros de atividades nos sistemas e podem servir como evidencias e provas, são encaminhados para a polícia federal e para a ABIN (Agência Brasileira de Informação).

De acordo com seu site, de 22 a 26 de junho de 2011, o Serpro detectou cerca de 25 ataques a diversos sites hospedados em sua estrutura de rede, ações realizadas como tentativa de negação de serviço. No dia 22 de junho de 2011, o site da Receita Federal sofreu um ataque de negação de serviço com início às 12h30 e duração aproximada de 30 minutos. O ataque foi contido pela área de segurança do Serpro, não ocorrendo indisponibilidade do serviço.

Outro ataque registrado foi detectado às 0h30 do dia 22 de junho de 2011, proveniente de 1000 origens diferentes, com aproximadamente 300 mil simulações de acessos por segundo. Entre 0h30 e 3h, foram dois bilhões de acessos que afetaram os sites www.presidencia.gov.br e www.brasil.gov.br. Os sites ficaram indisponíveis por cerca de 40 minutos e apresentaram lentidão no breve período posterior.

2.9 Incidentes reportados

Segundo estudos do Centro de estudos, respostas e tratamentos de incidentes de segurança no Brasil (CERT.br), a definição de incidente pode ser considerada como qualquer evento adverso, sendo que esses eventos podem ser confirmados ou sob suspeita, e podem ser considerados também como um ato de violar uma política de segurança, explícita ou implícita.

Ainda segundo o CERT.br (2013), o número de ataques de diversas naturezas a redes de computadores tem aumentado continuamente, tendo se destacado o ataque de varredura de porta ou o *scan*.

Esses programas especialistas, conhecidos como *scan ports* são capazes de vasculhar através de uma rede uma vulnerabilidade para que posteriormente tentem algum tipo de invasão ou ação maliciosa, tendo como alvos computadores que estão com suas portas de comunicação acessíveis.

Analisando a Figura 1 é possível perceber que de janeiro a março de 2013 esses ataques aumentaram.

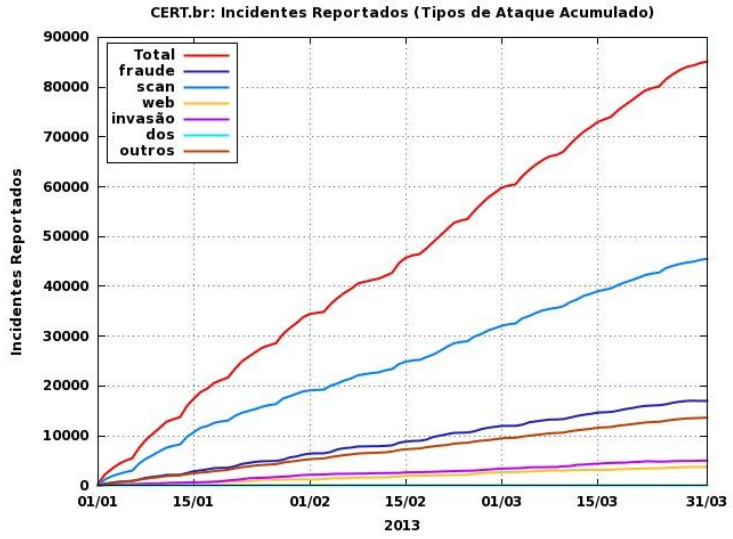

Figura 1 - Incidentes reportados ao CERT.br, no período de janeiro a março de 2013, relativo a tipos de ataques[2]. Fonte: CERT (2013).

3. MATERIAIS E MÉTODOS

No cenário proposto foram montadas duas redes locais com uma pequena estrutura utilizando dois computadores *notebooks* conectados a um *hub* físico. A partir disso, foram criados outros computadores de forma virtual utilizando o software *Virtual Box* para reproduzir o ambiente de rede. Ou seja, um notebook LG conectado a outro notebook, da marca TOSHIBA, por meio de uma rede interna.

Foi escolhido e instalado o Windows Server 2003, por ser utilizado por muitas empresas como o Sistema Operacional do servidor, e também o servidor e http Apache com php e mysql. Foi configurado no Windows Server o serviço SNMP (*Simple Network Management Protocol* - Protocolo Simples de Gerência de Rede) e nas configurações de segurança com o intuito de aceitar pacotes SNMP de qualquer host. Foi necessário desinstalar primeiramente o IIS (*Internet Information Services* - Internet Information Server) do Windows Server para posteriormente, instalar o Apache sem conflitos. Foi construída e hospedada no servidor uma página em php para que todos os hosts da rede pudessem assim acessá-la.

[2]Esta figura não inclui os dados referentes a *worms*. Os termos da figura são:
DOS (Denial of Service): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes nos quais ocorre uma tentativa de obter vantagem.
Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Também foi instalado uma ferramenta de monitoramento chamada Cacti para monitorar os eventos no servidor em amostras temporais, como o uso de CPU, memória física e tráfego em rede com o objetivo de observar o comportamento de dois tipos de ataques distintos em três momentos diferentes

O SNMP foi instalado, para que o monitoramento pelo Cacti fosse realizado, uma vez que o monitoramento é feito pelo protocolo escolhido, acessando assim as MIB´s (*Management Information Base* - Base de Informação de Gerenciamento).

No caso do presente trabalho, convém dizer que partimos do princípio que o ambiente laboratorial para esse experimento é considerado estável, pois todos os hosts e servidores envolvidos foram recém-instalados e sabemos quando e onde esses ataques irão atuar através de um monitoramento.

Para produzir os ataques ao servidor, foram instalados duas máquinas com o Back Track 5. Os ataques foram realizados com T50 e *Slow Loris*, ambos com objetivo de produzir a negação de serviço.

Para o sistema de detecção de intrusão, foi utilizado o Snort, ferramenta acoplada ao Back Track 5, que através de suas assinaturas consegue identificar e classificar um tipo de ataque. Sua função é barrar algo suspeito através de seu firewall. Ainda foi possível observar quais portas de comunicação estavam ativas, os tipos de protocolos em trânsito na rede com o wireshark e também classificar o tipo de ataque, sua origem e destino com o Snort, no caso do *slow loris*.

Tabela 1 - demonstrativo dos nomes dos computadores na rede, seus endereços e funções.

Computador	Sistema Operacional/versão	Endereço IP	Função na rede
TOSHIBA	Windows Server/2003	192.168.10.2	Servidor
TOSHIBA	Windows/XP	192.168.10.5	Host
LG	Linux Back Track/5	192.168.10.1	Atacante
LG	Linux Back Track/5	192.168.10.6	Atacante
LG	Linux Ubuntu/10.10	192.168.10.3	Monitoramento
LG	Windows/XP	192.168.10.9	Host

Tabela 1 – Funções na rede

Fonte: Elaborada pelo próprio autor (2013)

A topologia multiplataforma da rede desse laboratório é representada na Figura 2, especificando suas funções na tabela 1:

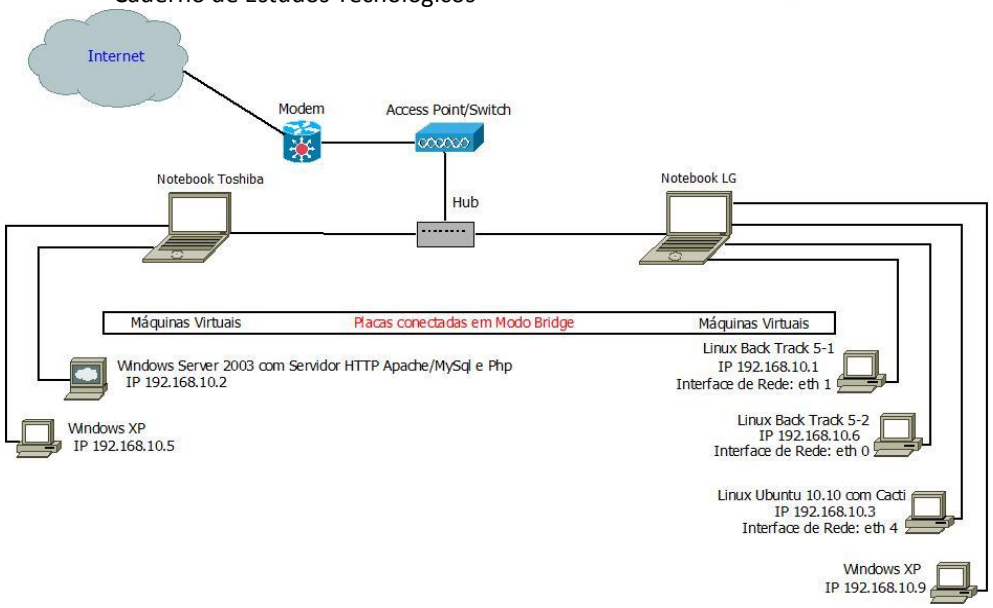

Figura 2 - Topologia

Fonte: Elaborada pelo próprio autor (2013)

7.1 Ataque realizado com o T50.

Estando no diretório /usr/sbin/t50 do computador LG, com a maquina virtual Linux Back Track 5-1, foram digitados os comandos com os seguintes parâmetros:

```
./t50 "IP" --flood -S --turbo --dport 80
```

Onde:

```
./t50: No diretório onde está o T50, parâmetro para execução do ataque

"IP": O IP do servidor que será atacado é digitado, no caso 192.168.0.2

--flood: Define o tipo do ataque a ser realizado

-S: Tipo do ataque(SYN flood)

--turbo: Acelera os pacotes enviados ao servidor

--dport 80: A porta onde o ataque irá atuar
```

7.2 Ataque realizado com Slow Loris

Para realização desse ataque foi necessário compilar o código do script em PERL, digitando pelo terminal do Linux Back Track 5 o seguinte comando no diretório onde se encontra o arquivo "slowloris.pl":

```
./slowloris.pl -dns "IP" -port 80 -timeout 2000 -num 500 -tcpto 5
```

Onde:

```
./slowloris.pl: script com o código do ataque

-dns "IP": IP do alvo a ser atacado, no caso 192.168.10.2

-port 80: Porta que será atacada no servidor

-timeout 2000: Número de segundos antes de enviar e receber o timeout

-num 500: Número de conexões criadas(sockets)

-tcpto 5: Aumenta o timeout do TCP para 5 segundos
```

4. RESULTADOS

Comparando os dois tipos de ataques, em três momentos diferentes, em conjunto com a análise dos seguintes parâmetros no Windows Server 2003: Utilização da CPU por parte do servidor, memória física em uso e tráfego em rede de tempo, pode-se notar valores distintos apresentados em cada um deles.

Onde:

A: Um único ataque "T50" como uma máquina com Back Track 5, chamada na rede de "Back Track 5-1", IP 192.168.10.1. De 9:55 até 10:15 do dia 22/05/2013, com duração de 15 minutos.

B: Dois ataques simultâneos com "T50", um vindo da máquina com Back Track 5, chamada na rede de "Back Track 5-1", IP 192.168.10.1 e outro com T50, um vindo da máquina com Back Track 5, chamada na rede de "Back Track 5-2", IP 192.168.10.6. De 10:25 até 10:55 do dia 22/05/2013, com duração de 30 minutos.

C: Ataque com "slow loris" vindo da máquina com Back Track 5, chamada na rede de "Back Track 5-1", IP 192.168.10.1. De 11:35 até 11:50, com duração de 15 minutos.

Observa-se na figura 3 que em "A" houve um aumento no processamento do servidor, no momento do ataque T50 com uma máquina na rede. Houve um intervalo de 5 minutos para que a rede se estabilizasse, e em "B" ocorreu o segundo ataque com o T50, agora com duas máquinas. Percebe-se um aumento no processamento do servidor.

Em "C" observa-se o processamento do servidor no momento do ataque com o "slow loris". Percebe-se que houve pouca alteração em relação aos outros ataques.

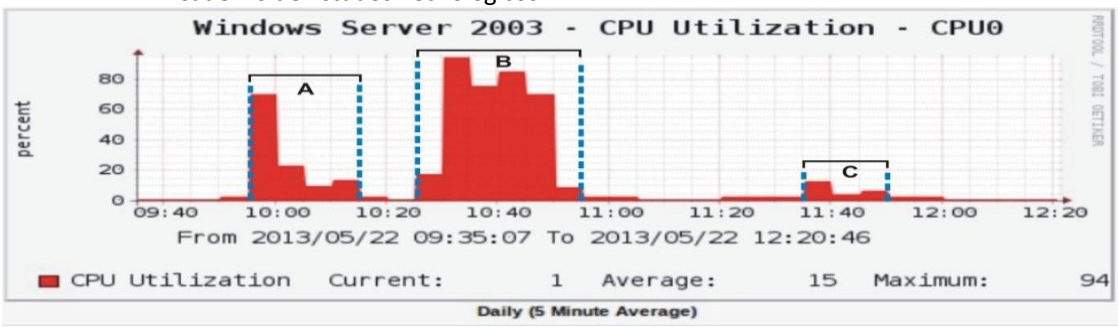

Figura 3 – Uso de processamento do servidor

Fonte: Elaborada pelo próprio autor (2013)

Na Figura 4, observando os intervalos dos ataques em "A", "B" e "C" notamos que os valores do uso de memória física se mantiveram em valores médios, sem discrepâncias consideráveis nos valores.

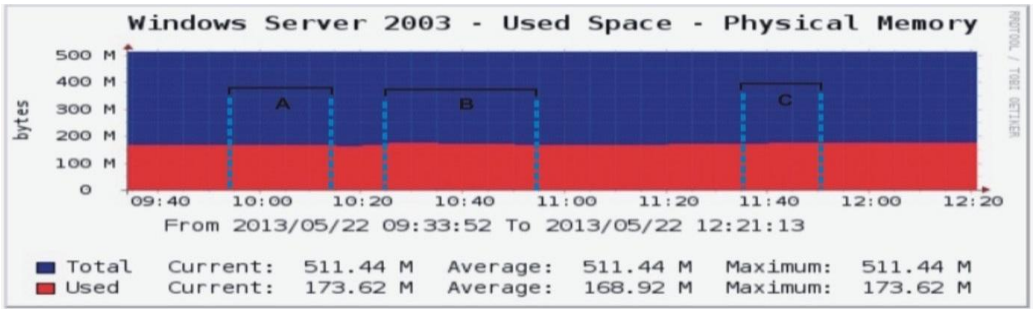

Figura 4 – Uso de memória física do servidor

Fonte: Elaborada pelo próprio autor (2013)

A Figura 5 apresenta o tráfego em rede no momento dos ataques "A", "B" e "C". Pode-se notar que em "A" os valores aumentam assim como em "B", porém em "C" os valores ficaram quase insignificantes.

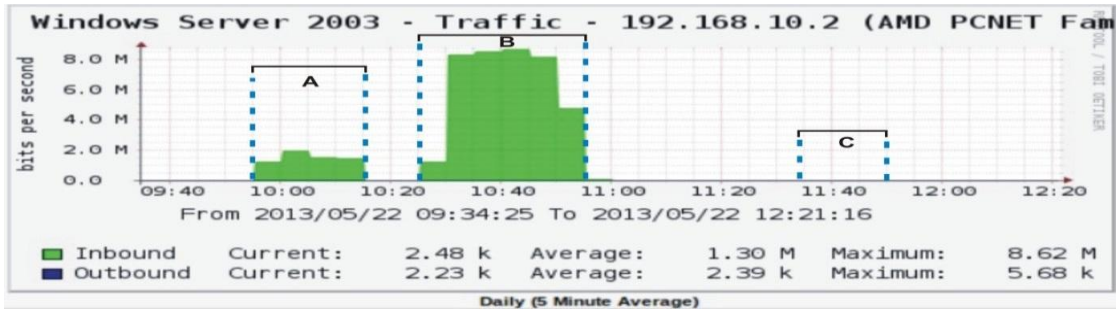

Figura 5 – Tráfego em rede

Fonte: Elaborada pelo próprio autor (2013)

No ataque A, o processamento e o volume do tráfego aumentaram no servidor, mantendo o uso de memória em valores médios.

Com o ataque B, o processamento e o tráfego foram maiores que no ataque A, mantendo o uso de memória em valores médios também. Em ambos nos ataques, A e B, foram utilizados o T50, porém em B com dois atacantes simultaneamente, que teriam como objetivo derrubar uma página no servidor Apache. Os ataques A e B não foram bem sucedidos, mesmo que em B a página apresentasse demora para ser carregada. Acreditamos que para que fosse bem sucedido seriam necessárias mais máquinas realizando o ataque ao alvo, configurando um ataque de negação de serviço distribuído, a fim de aumentar o tráfego e processamento a ponto de esgotar a capacidade do servidor para gerenciá-los.

O Ataque C utilizou uma técnica de ataque distinta chamada "Slow Loris". Foram analisados os mesmos parâmetros que no ataque anterior: processamento, uso de memória e tráfego em rede. Diferentemente, neste ataque, foi possível observar que o processamento aumentou pouco, o uso de memória se manteve em valores médios e o tráfego não se alterou.

Comparando os três ataques, ficou demonstrado que cada tipo de ataque tem um comportamento diferente e que para serem classificados e diagnosticados, necessitam de uma ferramenta com uma base de dados com assinaturas conhecidas de ataques e anomalias. Ou seja, é interessante notar que comparando o T50 e o *slow loris*, o T50 apresentou variações na medição de CPU e tráfego e o *slow loris* não.

O ataque C, com o "slow loris", foi bem sucedido comprometendo um dos três pilares que a segurança deve preservar, a acessibilidade. Com o ataque, a página do servidor se tornou indisponível, ou seja, a negação do serviço.

Os ataques atuam de forma diferente em seu comportamento, o T50 utiliza apenas um socket enquanto o *slow loris* cria vários sockets. Acreditamos que para o T50 ser bem sucedido, necessitaria de mais máquinas atacando, configurando assim, um ataque de negação de serviço distribuído (DDOS).

5. POSSÍVEIS SOLUÇÕES

A implantação de um firewall que atuará como filtro dos pacotes que chegam na rede por meio de um tráfego externo, podendo capturar o endereço de IP do atacante e bloqueá-lo e a utilização de um sistema de detecção de intrusão e prevenção. Esse sistema de detecção e prevenção de intrusão poderia ser dentro outros, o Snort, que para atuar de maneira eficiente deve estar com sua base de dados de regras atualizadas.

A figura 6 apresenta possíveis soluções para o problema com a utilização do Snort e firewall para conter as tentativas de ataque.

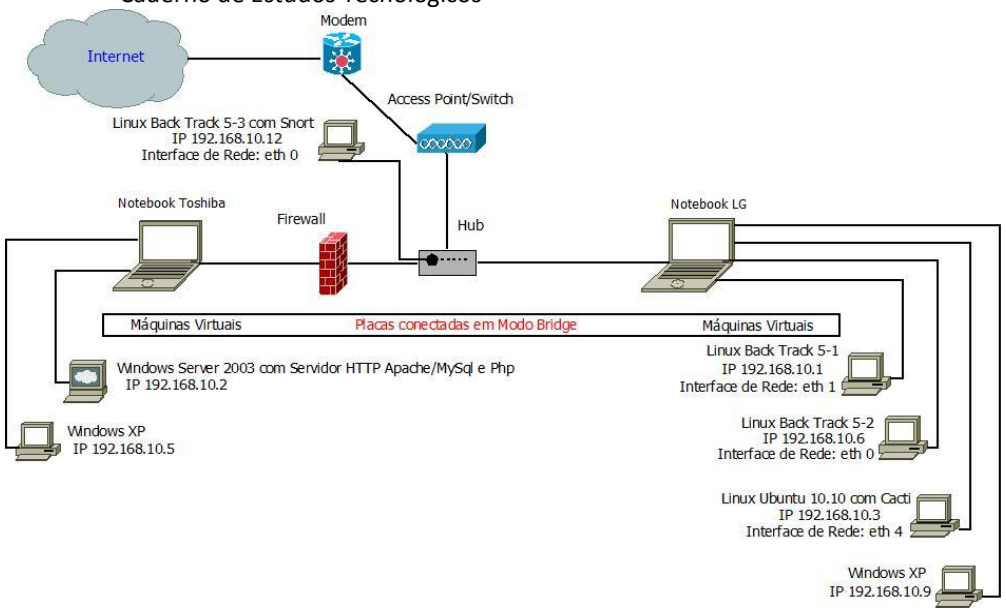

Figura 6 – Topologia com Snort como solução

Fonte: Elaborada pelo próprio autor (2013)

Na Figura 7 é possível observar que o Snort conseguiu classificar através de suas regras que sofreu um ataque de negação de serviço, vindo do IP 192.168.10.1 para o IP 192.168.10.12 na porta 80. A partir daí, seria possível barrar o tráfego partindo do IP atacante evitando a negação do serviço.

```
root@bt:/etc/snort# snort -q -A console -i eth0 -c /etc/snort/snort.conf
05/24-18:11:43.250842  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message floodin
g directed to SIP proxy [**] [Classification: Attempted Denial of Service] [Prio
rity: 2] {TCP} 192.168.10.1:48158 -> 192.168.10.12:80
05/24-18:11:43.250933  [**] [1:100000160:2] COMMUNITY SIP TCP/IP message floodin
```

Figura – 7 Ação do Snort classificando o ataque “C” como tentativa de negação de serviço

Fonte: Elaborada pelo próprio autor (2013)

No caso do Apache, alterar as configurações padrão para configurações que visam aumentar a segurança podem diminuir brechas. De acordo com a documentação no site oficial do servidor Apache (FOUNDATION, 2013), este afirma que o Servidor HTTP Apache tem uma grande documentação para segurança e conta com uma comunidade de desenvolvedores seriamente preocupados com questões de segurança, porém, afirma também que é inevitável que problemas diversos possam vir a ser descobertos após o lançamento do software. Dentre várias recomendações, cita:

Utilizar algum módulo do servidor Apache que limita o número de *sockets,* que é uma das pontas de duas vias de comunicação conectadas entre dois programas em execução que estão na rede ligados a uma porta de modo que a camada TCP(*transfer control protocol* – protocolo de transferência de controle) possa identificar a aplicação de dados a que se destina e origina (Oracle, 2013), permitidos por um único endereço IP (Exemplo: Mod_qos . Porém essa medida pode bloquear proxies ou roteadores NAT (*network address translation* – tradutor de endereços de rede) que despacham múltiplos clientes através de um único endereço IP. Em relação ao ataque de negação de serviço, o site diz que todos os servidores em rede estão sujeitos a

esse tipo de ataque, e que não seria possível prever esse tipo de ataque em sua totalidade, mas que seria possível atenuar problemas que eles podem causar.

Sugere também que a ferramenta mais efetiva contra um ataque DOS seria o *firewall* acompanhado de outras configurações do sistema operacional e servidor. Como firewalls podem ser configurados para restringir o número de conexões simultâneas de qualquer IP individual ou rede, é possível impedir assim uma série de ataques simples, porém, contra ataques distribuídos de negação de serviços, não é o suficiente. Para isso, é necessário medidas mais sofisticadas, como a utilização de sistemas inteligentes, como o Snort, para detecção de intrusão.

6. CONCLUSÃO

Foi possível demonstrar no presente trabalho três ataques a um servidor com o objetivo de provocar a negação de serviço e como se manifestam de formas diferentes. A negação de serviço com o ataque "C", *slow loris*, foi bem sucedida, e de acordo com os gráficos, mostrou nenhuma ou pouca alteração nos parâmetros monitorados.

Por fim, com a inclusão de um sistema de detecção e intrusão foi possível realizar essa classificação o que teria como consequência a filtragem, para não comprometer o servidor e a rede, barrando esses ataques.

Esse experimento mostrou a necessidade da utilização de um *software* para detecção e prevenção de intrusão, baseado em assinaturas e regras, como o Snort.

As implantações de políticas de segurança bem sucedidas se tornam possíveis através da consonância dos colaboradores que utilizam seus sistemas de informação e a gerência de tecnologia de informação. É importantíssimo que o usuário compreenda e atue de forma proativa zelando pela segurança, pois as ameaças surgem não apenas de fora de uma rede.

Sendo assim, em um ambiente real, onde a segurança é uma necessidade indispensável, procedimentos como os apresentados nesse estudo podem ajudar a amenizar ou resolver o problema de ataques de negação de serviço preservando a disponibilidade das informações.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR-ISO-IEC 27001: **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação** - Requisitos. Rio de Janeiro, 2006.

BRASIL, Snort. **O Snort.** Disponível em: <http://www.snort.com.br/snort.asp>. Acesso em: 31 maio 2013.

BRITO, Nelson et al. T50: Project Web Hosting - **Open Source Software**. Disponível em: <http://t50.sourceforge.net/>. Acesso em: 30 maio 2013.

BRITO, Nelson. **Uso irresponsável do T50**. Disponível em: <http://fnstenv.blogspot.com.br/2012/02/uso-irresponsavel-do-t50.html#more>. Acesso em: 26 maio 2012.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999. (A era da Informação: economia, sociedade e cultura, volume 1).

Centro de estudos, respostas e tratamentos de incidentes de segurança no Brasil (CERT.br). Disponível em: <http://www.cert.br/stats/incidentes/2013-jan-mar/tipos-ataque-acumulado.html> Acesso em: 11 de junho de 2013.

FOUNDATION, The Apache Software. **Security Tips**. Disponível em: <http://httpd.apache.org/docs/trunk/misc/security_tips.html#dos>. Acesso em: 30 maio 2013.

IBM (Estados Unidos). **Detecção de Anomalia de Rede**. Disponível em: <http://www.ibm.com/br/services/sps/iss/nad/>. Acesso em: 23 maio 2013.

MICROSOFT. **O que é vírus de computador?** Disponível em: <http://www.microsoft.com/pt-br/security/pc-security/virus-whatis.aspx>. Acesso em: 03 jun. 2013.

MORIMOTO, Carlos E. **Como criar um firewall e compartilhar conexão usando IPtables**. Disponível em: <http//www.hardware.com.br/artigos/firewall-iptables/> Acesso em: 9 de dezembro de 2012.

ORACLE. **What Is a Socket?** Disponível em: <http://docs.oracle.com/javase/tutorial/networking/sockets/definition.html>. Acesso em: 03 jun. 2013.

PERLIN, Tiago et al. **Detecção de Anomalias em Redes de Computadores através de Transformadas Wavelet**(artigo) Passo Fundo: Revista Brasileira de Computação Aplicada, 2011

RANGEL, Ricardo Pedreira. **Passado e futuro da era da informação**. Rio de Janeiro: Nova Fronteira Sa, 1999. 262 p.

RSNAKE. **Slowloris.pl.** Disponível em: <http://ha.ckers.org/slowloris/slowloris.pl>. Acesso em: 02 jun. 2013.

SERPRO. **Rio+20: segurança de TI garantida pelo Serpro**.Disponível em: <https://www.serpro.gov.br/noticias/rio-20-seguranca-de-ti-garantida-pelo-serpro/?searchterm=ataque%20ddos>. Acesso em: 27 maio 2013.

SERPRO. **Serpro faz balanço de medidas de segurança em resposta a ataques virtuais**. Disponível em: <https://www.serpro.gov.br/noticias/serpro-faz-balanco-de-medidas-de-seguranca-em-resposta-a-ataques-virtuais/?searchterm=ataque%20ddos>. Acesso em: 27 maio 2013.