IMPLANTAÇÃO DA FERRAMENTA IDS/IPS FAIL2BAN COMBINADA COM FIREWALL NETFILTER/IPTABLES NA MITIGAÇÃO DE ATAQUES COMBINADOS

Alex Marino Gonçalves de Almeida[1]; João Emiliano dos Santos Neto [2]; Thiago José Lucas [3]

Resumo
O presente artigo apresenta uma solução alternativa a problemas de segurança da informação aplicados a redes de computadores, em especial, servidores que executam distribuições Linux. Alguns importantes conceitos referentes as redes de computadores e sua evolução apontam para o surgimento de novas vulnerabilidades. O objetivo principal deste trabalho é provar que, por meio da utilização de software livre (Fail2ban, Linux e Netfilter/Iptables), é possível criar um cenário seguro contra ataques combinados, principalmente *brute-force* e *denial-of-service*. Por meio de testes em ambientes controlados utilizando-se de duas arquiteturas próximas do mundo real, uma com e outra sem a utilização dos mecanismos de segurança, foi possível demonstrar a eficiência das ferramentas estudadas na mitigação destes ataques.
Palavras-chave: Segurança da Informação; Intrusion Detection System; Intrusion Prevention System; Firewall.

Abstract
This paper presents an alternative solution to the information security problems applied to computer networks, in particular servers running Linux distributions. Some important concepts related to computer networks and their evolution point to the emergence of new vulnerabilities. The main objective of this work is to prove that, through the use of free software (Fail2ban, Linux and Netfilter / iptables), you can create a secure setting against blended attacks, mainly brute force and denial-of-service. Through testing in controlled environments using the next two architectures of the real world, one with and one without the use of security mechanisms, we could demonstrate the efficiency of the tools studied in mitigating these attacks..
Keywords: Information Security; Intrusion Detection System; Intrusion Prevention System; Firewall.

Introdução

Da criação até os dias atuais a Internet popularizou-se e expandiu muito, tornando-se um meio de comunicação muito utilizado. Um parâmetro desse crescimento é o número de máquinas conectadas em um período de dez anos. De acordo com Internet Systems Consortium (ISC, 2013) em Janeiro de 2003 foram computados 171.638.297 máquinas, já em Janeiro de 2013 esse número foi para 963.518.598.

Essa grande utilização deu origem a fluxos de dados maliciosos, como no caso

[1] Professor da Faculdade de Tecnologia de Ourinhos – FATEC. E-mail: alex.marino@gmail.com.
[2] Graduado em Gestão da Tecnologia da Informação pela Faculdade de Tecnologia de Ourinhos – FATEC. E-mail: joaoemiliano5@gmail.com.
[3] Professor da Faculdade de Tecnologia de Ourinhos – FATEC. E-mail: thiagojlucas@gmail.com.

dos ataques de negação de serviço originados por ataques de força bruta, que tem o intuito de afetar a disponibilidade de uma rede ou de um determinado serviço e aumenta a dificuldade de defesa pelo fato de estarem combinados.

Sabendo a importância da disponibilidade das informações e serviços oferecidos pelas organizações e das diferentes técnicas de ataques que ameaçam a disponibilidade, este trabalho tem como objetivo verificar se a utilização de mecanismos de proteção em conjunto é eficiente para minimizar a incidência de ataques combinados.

A seção 2 fornecerá ao leitor informações sobre a importância de mecanismos de proteção em redes de computadores. A seção 3 será destinada à apresentação das ferramentas utilizadas. A seção 4 esta destinada aos testes e resultados obtidos

2 Redes de computadores

Assim como as demais tecnologias presentes no âmbito da informática, as redes de computadores tiveram um longo processo de evolução até chegar aos padrões atuais (MORIMOTO, 2008). De acordo com Forouzan (2008, p. 17) ano de 1967 em um encontro da Association Computing Machinery, um grupo apresentou ideias para a criação de uma pequena rede de computadores, denominada ARPANET, a principal ideia desse projeto era realizar a conexão entre computadores de diferentes fabricantes.

Inicialmente desenvolvida para testes, em alguns anos a ARPANET já possuía diversos nós de comunicação e essa utilização originou em serviços que são utilizados até hoje. Outro padrão importante foi a *Ethernet*[4], desenvolvido pela Xerox, nos Estados Unidos, que permitia conectar máquinas e transmitir dados localmente. A ARPANET e o padrão *Ethernet* originaram respectivamente a Internet e às redes locais, duas inovações que revolucionaram a computação e tiveram uma popularização absurda (MORIMOTO, 2008).

De acordo com Tanembaum (2003, p. 3-6) as redes de computadores são de extrema importância para as organizações, pois com elas é possível realizar o compartilhamento de recursos físicos, troca de informações e atualmente as organizações apresentam uma enorme dependência de informações computadorizadas.

Pelo fato de realizar compartilhamento de recursos e de informações, é imprescindível adotar mecanismos de proteção para as redes de computadores, a fim de minimizar os riscos eminentes à que os bens da organização estão expostos.

[4] Arquitetura de interconexões para redes locais.

2.1 Requisitos de segurança

Guedes, Dueire e Oliveira (2006, p. 13-15) esclarecem que na literatura não há uma concordância sobre a classificação dos diversos termos utilizados na área de segurança da computação, sendo assim eles descrevem uma classificação que são mais utilizados e semelhantes às descritas por Donn Park, Stallings, Tanenbaum e Lino Sarlo Silva.

Confidencialidade: Serviço que disponibiliza o acesso à informação apenas para usuários autorizados. Outro ponto de destaque é a proteção à análise do fluxo do tráfego, impedindo que entidades não autorizadas visualizem informações presentes no canal de comunicação.**Integridade:** Este serviço garante que os dados não serão alterados durante uma transmissão sem o consentimento do emissor e receptor, o serviço de integridade pode ter mecanismos automáticos para detectar violações.

Disponibilidade: Serviço que busca manter os elementos de um sistema disponível para os usuários, mesmo em caso de ataques. Existem inúmeras técnicas de ataques que podem resultar na perda ou redução da disponibilidade.

Segundo Mayer e Paulino (2010) a gestão de segurança da informação classifica-se em três pontos: lógica, física e humana. Esses três pontos são constantemente atacados, com o intuito de identificar o ponto mais fraco.

2.3 Importância da informação nas organizações

Fala-se muito na importância da informação nas organizações, Gomes (2009, p. 4) esclarece que as organizações que não dão a devida importância para a informação pode apresentar perda de desempenho sem ao menos perceber.

Em praticamente todos os setores encontramos empresas que se sobressaem perante as outras. No setor automotivo, a Toyota tem um desempenho superior às demais. No varejo *on-line*[5] a Amazon é líder; já no *off-line*[6], considera a Wal-Mart, a maior varejista do planeta. Se observar busca na *web*[7], quem tem maior destaque é a Google.

[5] Termo que indica que alguma coisa está ligada ou conectada.
[6] Termo que indica que alguma coisa está desligada ou desconectada.
[7] Um Sistema de informações ligadas por meio de hipermídia, que permite ao usuário acessar uma infinidade de conteúdo pela Internet.

Essas empresas se sobressaem por serem capazes de utilizar os recursos disponíveis de maneira mais eficiente, normalmente devido a ativos de conhecimento e administração eficaz da informação (LAUDON; LAUDON, 2007, p. 71).

Por sua importância a informação torna-se muitas vezes alvo de ataques e atualmente existem inúmeras técnicas que visam afetar a confidencialidade, integridade e disponibilidade da informação.

2.4 Técnicas de ataques

Existe uma infinidade de ataques atualmente, o foco do presente artigo é nos ataques de negação de serviço originados por ataques de força bruta.

No ataque de negação de serviço o intuito é afetar a disponibilidade da informação ou serviço oferecido. Um exemplo de ataque utilizando-se desta técnica é um servidor *web* que recebe um grande volume de requisições provenientes de um mesmo endereço, o servidor irá responder a todas as requisições, ocasionando no congestionamento do *link*[8] ou exaustão de seus recursos. (MORIMOTO, 2008).

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR, 2012, p. 20) ataques de força bruta consistem em adivinhar, através de tentativa e erro uma credencial, a fim de executar processos ou acessar serviços com os privilégios do usuário obtido e que ataques de força bruta, dependendo de sua dimensão, pode resultar em um ataque de negação de serviço, devido à sobrecarga produzida.

3 Ferramentas utilizadas

3.1 NMAP – Network Mapper

É uma ferramenta muito poderosa, criada por Gordon Fyodor Lyon em 1997, é amplamente utilizada por profissionais de TI para realizar varredura de porta, descoberta de serviço e detecção de versões. A ferramenta possui uma série de funções específicas para a realização de diferentes varreduras de rede. (GIAVAROTO; SANTOS, 2013, p. 67).

[8] Canal de comunicação para a troca de dados entre máquinas.

3.2 Crunch

Os ataques de força bruta podem ser baseados em dicionários ou listas de palavras, esses arquivos podem estar disponíveis na Internet, porém na maioria das vezes infectados com algum tipo de código malicioso.

Uma saída interessante é utilizar ferramentas para a criação dessas listas de palavras, a ferramenta Crunch gera listas complexas para ser utilizadas em ataque de força bruta, com a opção de determinar os parâmetros de criação (GIAVAROTO, 2012).

3.3 Hydra

De acordo com The Hacker's Choice (THC, 2013) Hydra é uma ferramenta utilizada para quebra de senha, pode ser utilizada por consultores de segurança para verificar a complexidade das senhas utilizadas pelos usuários. O Hydra será utilizado para realizar o ataque de força bruta no servidor FTP[9].

3.4 BackTrack

É muito utilizado por auditores, analistas de segurança de redes e sistemas, entre outros profissionais. Voltada para testes de penetração o BackTrack possui cinco versões e mais de 300 ferramentas para testes de penetração e existem ainda algumas certificações que utilizam o BackTrack como ferramenta principal. (GIAVAROTO; SANTOS, 2013, p. 5).

As ferramentas descritas anteriormente como Hydra, Crunch e NMAP podem ser encontras no BackTrack e não necessita realizar a instalação.

3.5 Fail2ban

Os ataques de força bruta ocorrem com muita frequência nos serviços que utilizam autenticação por senha, muitas vezes não é possível trocar a porta padrão do serviço ou ficar analisando todos os arquivos de *log*[10] em busca de identificar tentativas de invasão.

Os arquivos de *log* possuem informações interessantes, principalmente quando se trata de tentativa de acessos falhos. O fail2ban trabalha com essas informações, ele

[9] File Transfer Protocol.
[10] Arquivo de registros de eventos relevantes em um sistema computacional.

realiza uma varredura nos arquivos de *log* e busca por padrões que correspondem a possíveis tentativas de invasões. Na maioria das vezes, o fail2ban insere uma regra no *firewall*[11] e/ou envia notificação por *e-mail*[12] para o administrador do sistema. Ele é inteiramente escrito em *Python*[13], funcionando na maioria das distribuições Unix, suporta uma série de serviços e ações (FAIL2BAN, 2014).

3.6 Firewall

Para Kurose (2010, p. 535-536) um *firewall* é a combinação de *software*[14] e *hardware*[15], que tem por objetivo isolar a rede interna do restante da Internet, controlando os pacotes que passam por ele. Com isso permite que o administrador gerencie o acesso entre o mundo externo e os recursos administrados, por meio do gerenciamento do tráfego.

O *firewall* utilizado será o Netfilter/Iptables, na página oficial do projeto Netfilter (2014 a), tem-se que o Netfilter é um *framework*[16] de filtragem de pacotes que permite ao *kernel*[17] do Linux registrar as funções de retorno dos pacotes de dados.

Segundo Netfilter (2014 b), o Iptables é uma estrutura utilizada para a definição de conjuntos de regras dentro de tabelas IP[18] podendo ser utilizado para listar todo o conteúdo presente no conjunto de regras de filtro de pacotes.

3.7 Zabbix

Zabbix é um *software* que monitora inúmeros parâmetros de uma rede, com intuito de manter o bom funcionamento dos servidores e serviços disponíveis (ZABBIX, 2014).

Sua arquitetura e a flexibilidade dos módulos faz com que a ferramenta possa ser utilizada para o monitoramento convencional, monitorar o desempenho de aplicações, analisar causa de problemas em ambientes complexos e verificar a experiência de

[11] Dispositivo cujo objetivo de aplicar uma política de segurança em determinado ponto da rede.
[12] Método que permite a troca de mensagens, por meio de sistemas eletrônicos.
[13] Linguagem de programação de alto nível.
[14] Sequência de instruções escritas para serem interpretadas por um computador.
[15] Parte física dos dispositivos eletrônicos.
[16] Conjunto de conceitos usados para resolver um problema de domínio específico.
[17] É o núcleo do sistema operacional, sua função é conectar o software ao hardware.
[18] Internet Protocol.

usuário. A ferramenta disponibiliza interface *web* para facilitar a administração e exibição dos dados. (4LINUX, 2014).

3.8 ProFTPD

De acordo com ProFTPD (2014), o projeto surgiu pela necessidade de maior segurança e facilidade de configuração para servidores FTP. No início do projeto o servidor mais utilizado era o Wu-ftpd, porém essa ferramenta possuía um histórico de segurança pobre, onde muitos desenvolvedores trabalharam por muito tempo realizando correções nas falhas de segurança da ferramenta, com isso surgiu à necessidade de reformulação completa.

4 Realização dos testes

Para comprovar a eficiência da combinação do *Firewall* Netfilter/Iptables e a ferramenta IDS[19]/IPS[20] Fail2ban, na mitigação de ataque de negação de serviço originado por ataque de força bruta, os testes serão realizados utilizando-se de duas arquiteturas próximas do mundo real, uma com os mecanismos de proteção em conjunto devidamente configurados e outra arquitetura sem os mecanismos de proteção e em um ambiente controlado, pela impossibilidade da utilização de um cenário real para a realização dos testes.

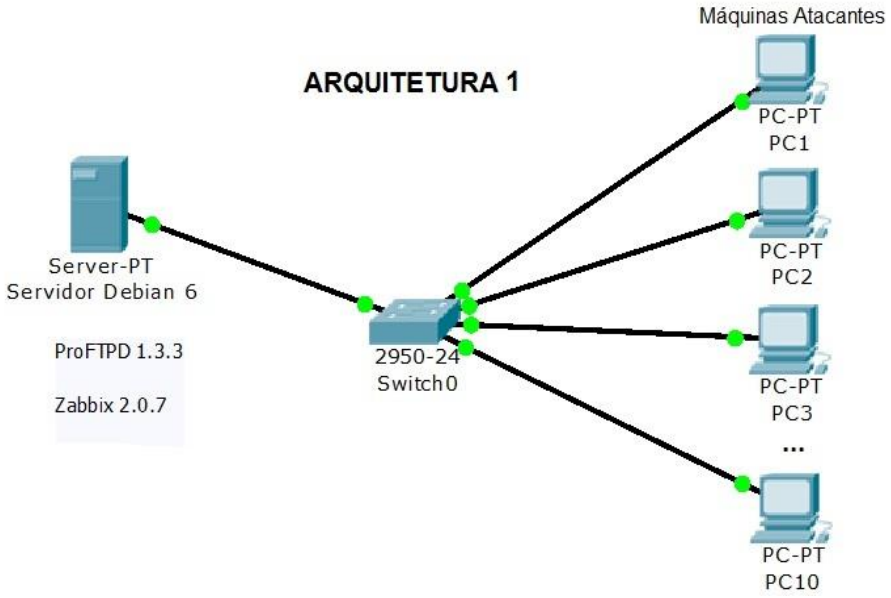
Arquitetura um: Será utilizado um servidor com a distribuição Debian na sua versão 6 com *kernel* Linux 2.6.32, onde será configurado o serviço FTP utilizando-se do *software* ProFTPD versão 1.3.3, disponibilizando dados, onde cada usuário utiliza-se do mecanismo de autenticação por senha para ter acesso ao servidor.

Serão conectados a esse servidor dez microcomputadores com sistema operacional BackTrack 5 r3 virtualizado pelo software Oracle VM VirtualBox versão 4.3.6.

Esses microcomputadores serão responsáveis pela realização dos ataques de força bruta no serviço FTP. A arquitetura está ilustrada na figura abaixo.

[19] Intrusion Detection System.
[20] Intrusion Prevention Systems.

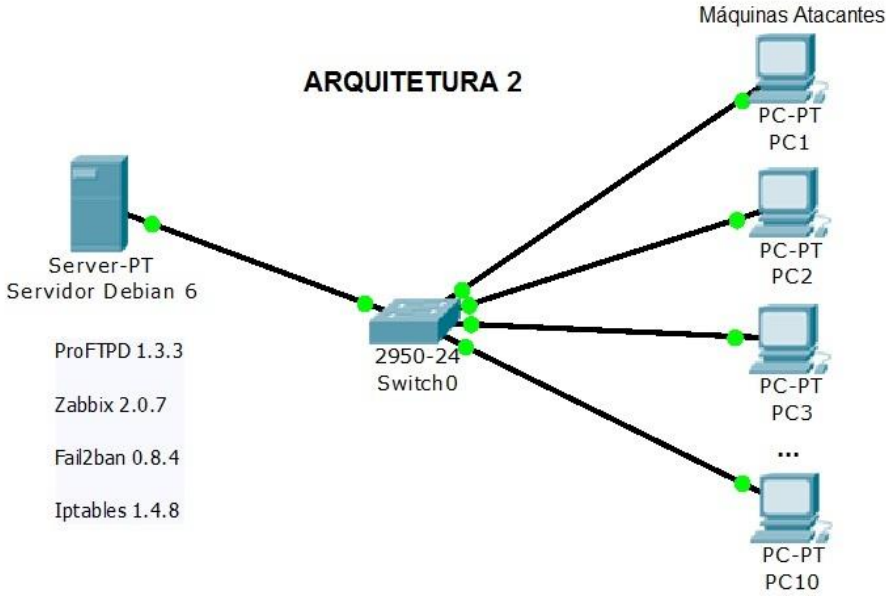
Figura 1 – Arquitetura de testes sem os mecanismos de segurança



Fonte: Elaborado pelos autores.

Arquitetura dois: Terá a mesma configuração de *hardware* e *layout*[21] da arquitetura um, o diferencial é a utilização do *software* Fail2ban versão 0.8.4 em conjunto com o *Firewall* Netfilter/Iptables versão 1.4.8. A arquitetura está ilustrada na figura abaixo.

Figura 2 – Arquitetura de testes com os mecanismos de segurança



Fonte: Elaborado pelos autores.

[21] Esboço que mostra a estrutura física ou determinada arquitetura.

Em ambas as arquiteturas o *software* Zabbix será instalado no servidor a fim de realizar o monitoramento de utilização de memória RAM[22], uso do CPU[23] e tráfego da rede.

4.1 Utilização das ferramentas

Para realizar um ataque de força bruta é necessário obter informações do servidor, como, portas, serviços e protocolos utilizados. O *software* NMAP será utilizado para realizar uma varredura na rede e levantar essas informações.

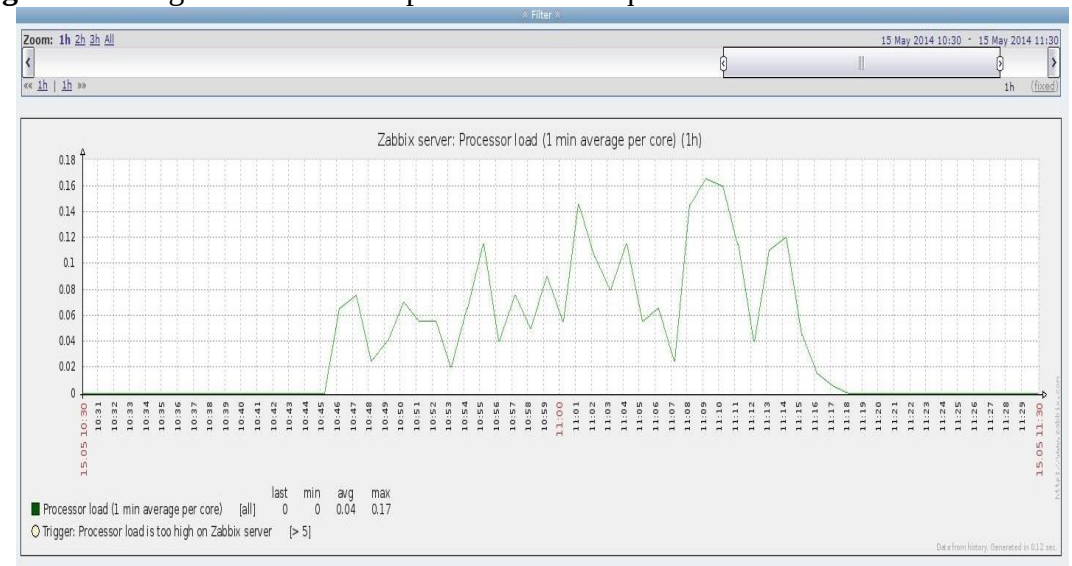
Após a coleta de dados do servidor, o ataque de força bruta será realizado com a ferramenta Hydra, e as listas de palavras utilizadas para gerar as combinações de credenciais, serão geradas pela ferramenta Crunch.

Sendo assim será realizado o ataque de força bruta a fim de criar um falso fluxo de dados na rede, com o intuito de sobrecarregar o canal de comunicação ou consumir recursos do servidor com as inúmeras requisições.

4.2 Resultados do teste

Os testes na arquitetura um, foram realizados no período ente 10h30min às 11h15min e os testes na arquitetura dois, foram realizados no período entre 10h25min às 11h00min.

Figura 3 – Carga de uso da CPU por minuto na arquitetura um.

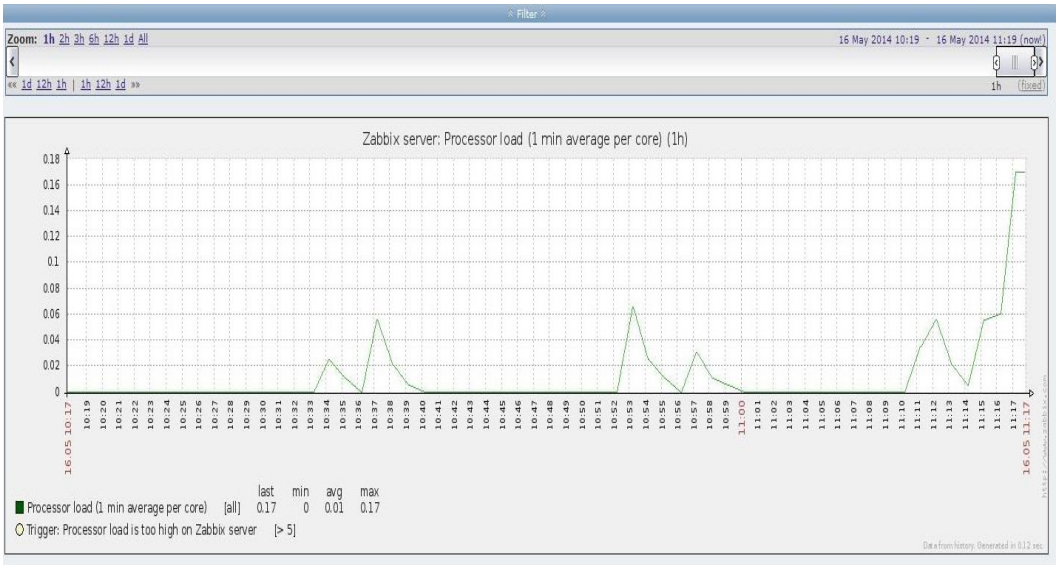


Fonte: Elaborado pelos autores.

[22] Random Access Memory.
[23] Central Processing Unit.

A carga de uso da CPU na arquitetura um foi maior do que na arquitetura dois. É possível observar ainda que na primeira arquitetura a utilização da CPU se manteve elevada desde o início até o fim do ataque, enquanto que na segunda arquitetura houve apenas duas pequenas elevações na utilização.

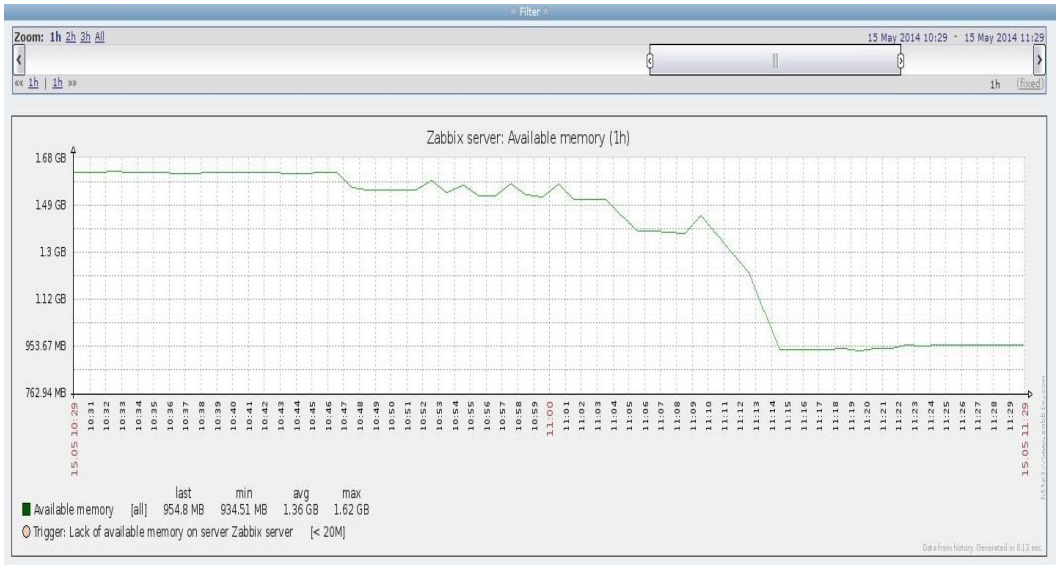
Figura 4 – Carga de uso da CPU por minuto na arquitetura dois.



Fonte: Elaborado pelos autores.

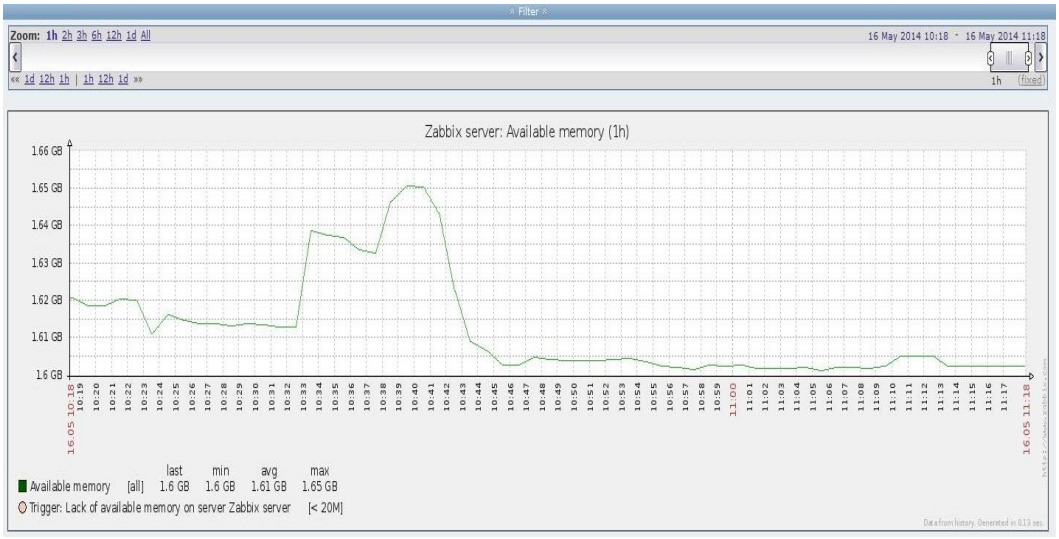
Os gráficos das figuras 5 e 6 apresentam a memória disponível para utilização, ao comparar as arquiteturas é possível verificar que a disponibilidade desse recurso na arquitetura um foi menor, ou seja, o ataque consumiu mais recurso na arquitetura que não possuía os mecanismos de proteção.

Figura 5 – Memória disponível na arquitetura um.



Fonte: Elaborado pelos autores.

Figura 6 – Memória disponível na arquitetura dois.

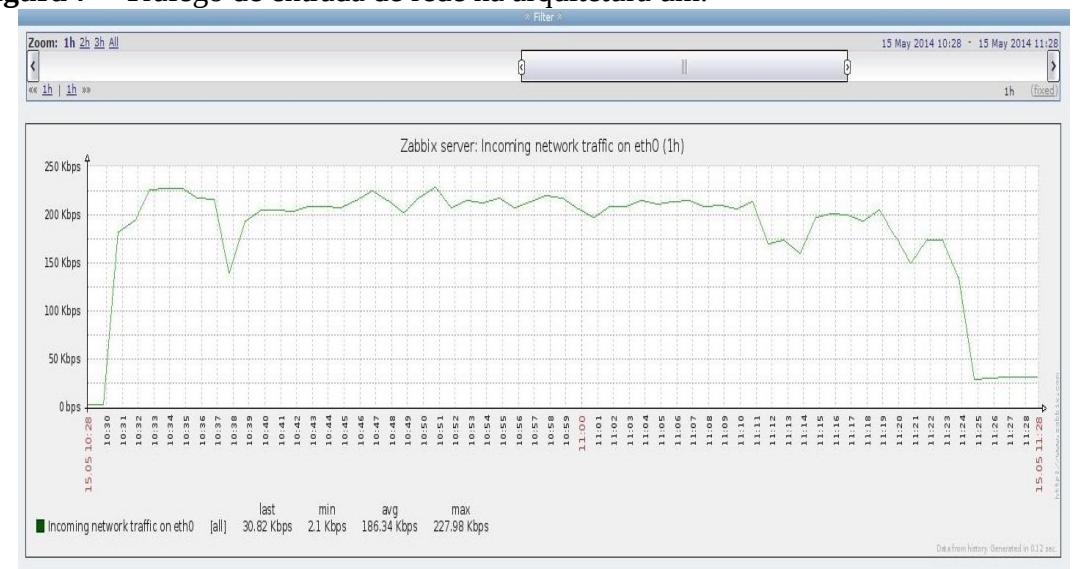


Fonte: Elaborado pelos autores.

O tráfego de entrada e saída de rede na arquitetura um foi bem superior e manteve-se elevado do início ao fim do ataque, pelo fato das máquinas atacantes gerarem muitas requisições e o servidor ter que responder essas requisições.

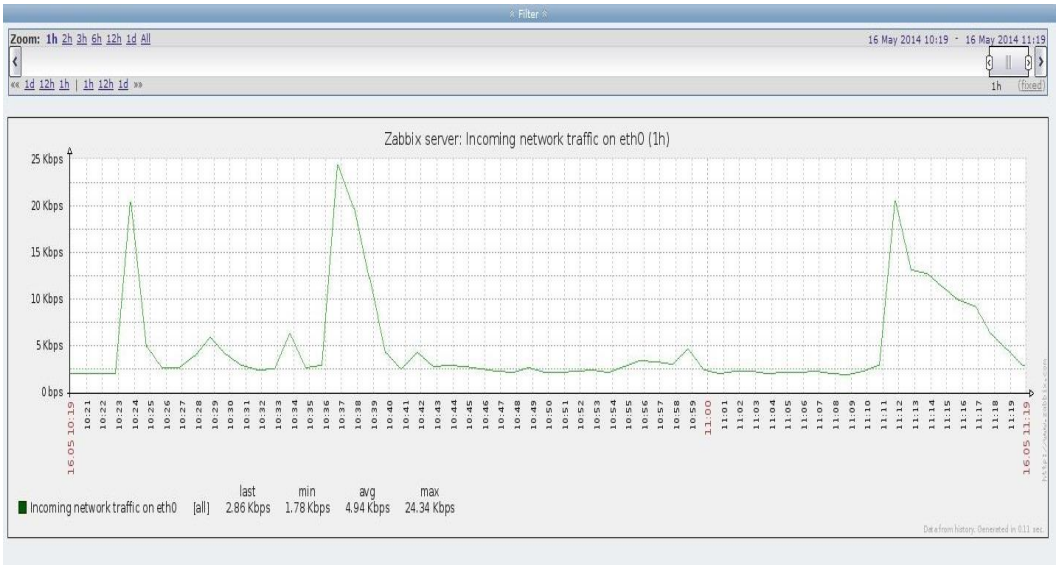
A grande ocupação da rede pode fazer com que requisições de usuários legítimos sejam descartadas.

Figura 7 – Tráfego de entrada de rede na arquitetura um.



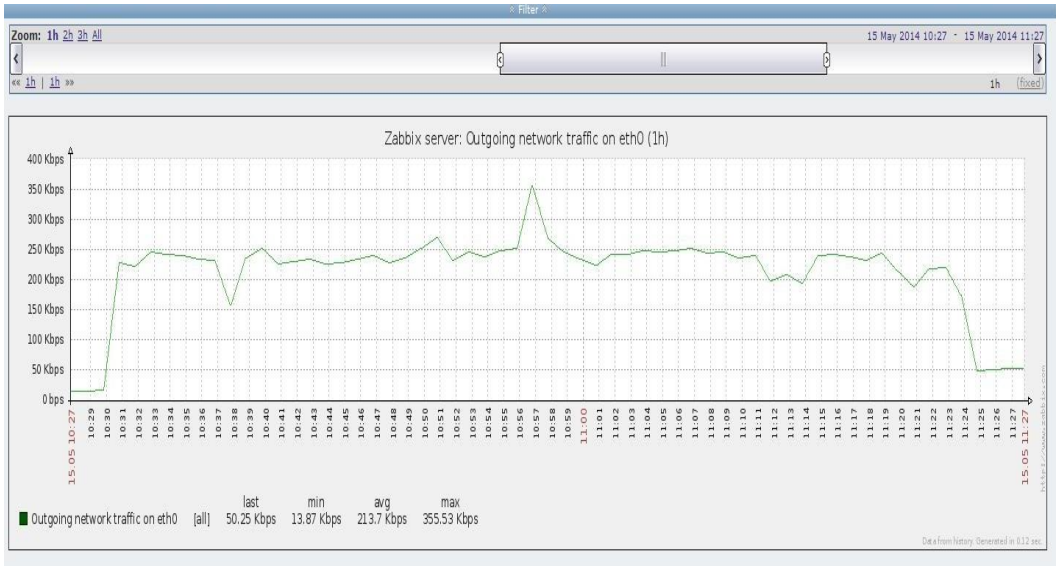
Fonte: Elaborado pelos autores.

Figura 8 – Tráfego de entrada de rede na arquitetura dois.



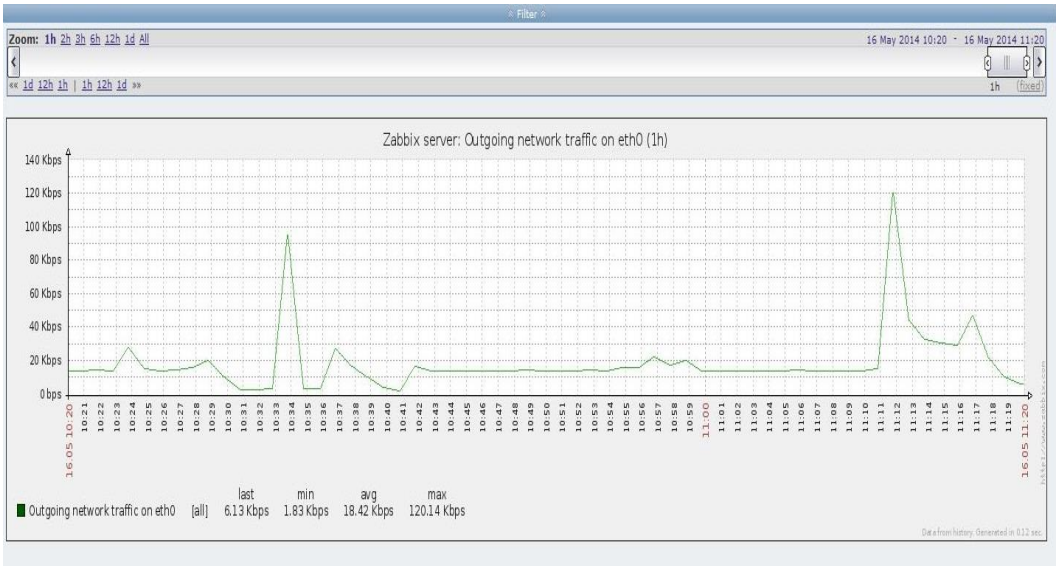
Fonte: Elaborado pelos autores.

Figura 9 – Tráfego de saída de rede na arquitetura um.



Fonte: Elaborado pelos autores.

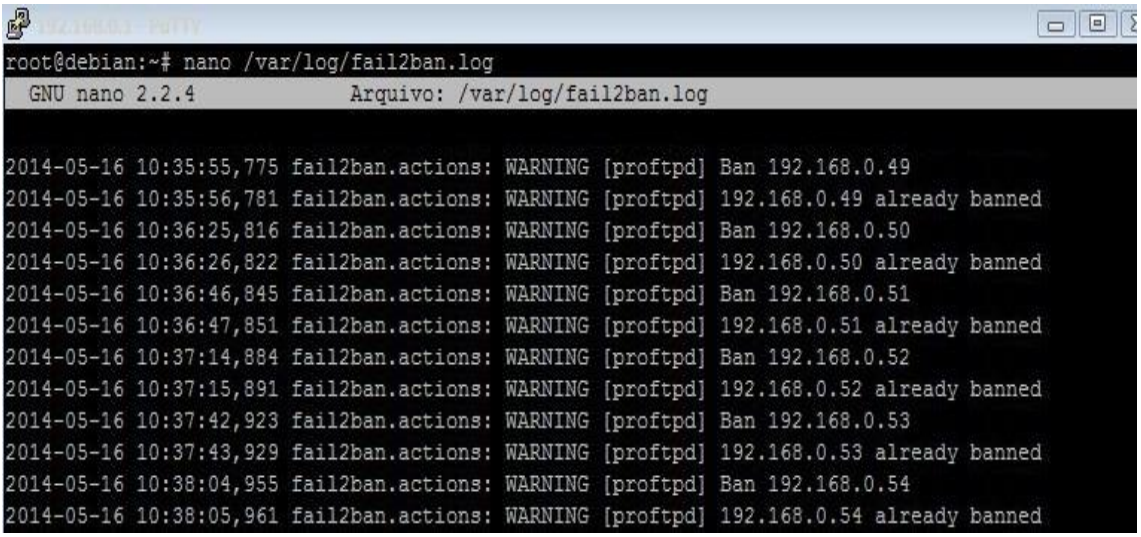
Figura 10 – Tráfego de saída de rede na arquitetura dois.



Fonte: Elaborado pelos autores.

No arquivo de *log* do Fail2ban pode-se observar o momento em que a ferramenta identifica os IP's atacantes e comunica ao *Firewall* Netfilter/Iptables solicitando o bloqueio dos IP's. A solicitação do bloqueio é indicada pelo texto final *'Ban'* seguido do IP da máquina e a execução da ação de bloqueio é indicada pelo texto final *'already banned'*.

Figura 11 – Log da ferramenta Fail2ban.

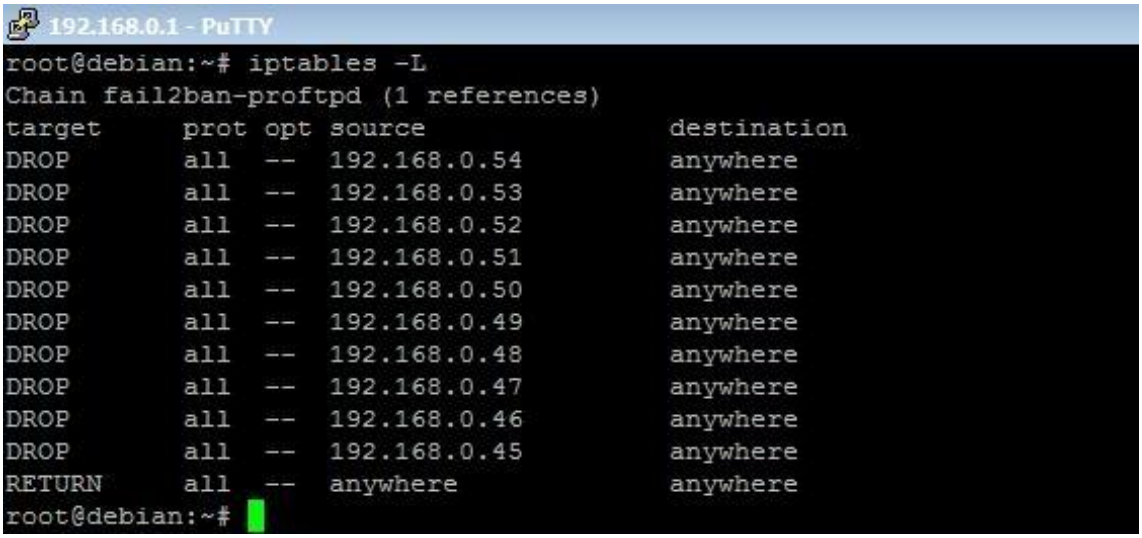


Fonte: Elaborado pelos autores.

Após a solicitação de bloqueio realizada pelo Fail2ban é possível observar que os IP's realmente foram bloqueados listando as *chains*[24] do *Firewall* Netfilter/Iptables.

[24] São cadeias e rotinas pré-definidas ou criadas pelo usuário que são executadas à medida que os pacotes chegam ao sistema operacional.

Figura 12 – Lista dos IP's bloqueados pelo Firewall.



Fonte: Elaborado pelos autores.

5 Conclusão

Durante o ataque foi possível observar que a arquitetura 01 teve maior consumo de recursos pelo fato de não possuir mecanismos de segurança. A utilização dos recursos analisados foi menor na arquitetura 02, pois em alguns minutos o ataque foi identificado e bloqueado.

Foi possível comprovar a eficiência das ferramentas IDS/IPS Fail2ban em conjunto com o *Firewall* Netfilter/Iptables na mitigação de ataque de negação de serviço por ataques força bruta. As ferramentas conseguiram evitar o consumo de recurso do servidor e congestionamento no *link* de dados bloqueando as máquinas atacantes.

Referências

4LINUX. **4Linux Open Software Specialists.** Disponível em: <www.4linux.com.br/zabbix/o-que-e-zabbix>. Acesso em Maio, 2014.

CERT. **Cartilha de Segurança para a Internet.** 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em Outubro, 2013.

FAIL2BAN. **Manual.** Disponível em: <http://www.fail2ban.org/wiki/index.php/MANUAL_0_8>. Acesso em Janeiro, 2014.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores.** São Paulo: McGraw-Hill, 2008.

GIAVAROTO, S. C. R. **Criando wordlists com o Crunch.** 2012. Disponível em: <http://www.backtrackbrasil.com.br/site/2012/08/criando-wordlists-com-o-crunch/>. Acesso em Janeiro, 2014.

GIAVAROTO, S. C. R.; SANTOS, G. R. **BackTrack Linux – Auditoria e teste de invasão em redes de computadores.** Rio de Janeiro: Editora Ciência Moderna, 2013.

GOMES, R. S. **A importância da informação.** 2009. Disponível em: <http://www.administradores.com.br/producao-academica/a-importancia-da-informacao/2820/>. Acesso em Julho, 2013.

GUDES, A. G.; DUEIRE, R. L.; OLIVEIRA, R. **Segurança com redes privadas virtuais VPNs.** Rio de Janeiro: Basport, 2006.

INTERNET SYSTEMS CONSORTIUM. **Number of Hosts advertised in the DNS.** 2013.

Disponível em: <http://ftp.isc.org/www/survey/reports/2013/01/>. Acesso em Outubro, 2013.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet:** uma abordagem top-down. São Paulo: Pearson, 2010.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais.** Editora São Paulo: Pearson Prentice Hall, 2007.

MAYER, J. R.; PAULINO, W. O. **Redes de Computadores I:** Estudo da Gestão de Segurança da Informação com Base no Framework ITIL V2. 2010. Disponível em: < http://www.teleco.com.br/tutoriais/tutorialitil/default.asp>. Acesso em Julho, 2013.

MORIMOTO, C. E. **Redes, Guia Prático 2ª Ed.** 2008. Disponível em: <http://www.hardware.com.br/livros/redes/>. Acesso em Setembro, 2013.

NETFILTER. **Netfilter Project Home-page.** Disponível em: <http://www.netfilter.org/>. Acesso em Fevereiro, 2014 a.

_____. **Netfilter Project Home-page.** Disponível em: <http://www.netfilter.org/projects/iptables/>. Acesso em Fevereiro, 2014 b.

PROFTPD. **ProFTPD Project Home-page.** Disponível em: <http://www.proftpd.org/goals.html>. Acesso em Fevereiro, 2014.

TANEMBAUM, A. S. **Redes de Computadores 4ª Ed.** Rio de Janeiro: Elsevier, 2003.

THE HACKER'S CHOICE. **TCH-Hydra.** Disponível em: <https://www.thc.org/thc-hydra/>. Acesso em Janeiro, 2014.

ZABBIX. **Zabbix Project Home-page.** Disponível em: <www.zabbix.com/documentation/2.0/manual/introduction/about>. Acesso em Maio, 2014.