DOI: 10.5102/un.gti.v7i1.4322

Utilização de simuladores para a formação de guerreiros cibernéticos*

Use of simulators for the training of cyber warriors

André Farreira Alves Machado[1]

Resumo

O presente artigo apresenta o emprego de simulador como ferramenta para treinar os militares combatentes do espaço digital. Como estudo de caso, apresentamos o Simulador de Operações de Guerra Cibernética (SIMOC) empregado pela Seção de Guerra Cibernética, do Centro de Instrução de Guerra Eletrônica (CIGE), na formação dos alunos do Curso de Guerra Cibernética do Exército Brasileiro. No artigo, um exemplo de exercício cibernético é apresentado, assim como: aspectos técnicos a respeito da arquitetura do SIMOC e uma análise crítica abordando os aspectos positivos e negativos do simulador.

Palavras-chave: Simulador. Cibernética. Treinamento.

Abstract

This article presents the use of simulator as a tool to train the digital space military warriors. As a study case, we present the Cybernetics War Operations Simulator employed by Cyber War Section, from Electronic Warfare Training Centre, in training of Brazilian military students in Cybernetics War Course. In the article, a cyber exercise example is presented, as well as technical aspects regarding of architecture and a critical analysis covering the positive and negative aspects of the simulator.

Keywords: Simulator. Cybernetic. Training.

* Recebido em: 10/10/2016.
Aprovado em: 23/03/2017.

[1] Possui graduação em Comunicações, pela Academia Militar das Agulhas Negras (1997); graduação em Matemática, pela Universidade Regional Integrada do Alto Uruguai e das Missões (2007); especialização em Matemática, pela Universidade de Gama Filho (2010); especialização em TI pela FAE/CDE (2002); mestrado em Comunicações, pela Escola de Aperfeiçoamento de Oficiais (2005); e Mestrado em Engenharia da Computação, pelo ITA (2013). Tem experiência na área de Educação, com ênfase em Educação matemática e segurança cibernética.

1 Introdução

Em 2008, por meio do Decreto Nº 6.703 de 18 de dezembro, a Presidência da República torna púbica a Estratégia Nacional de Defesa (END), reconhecendo o setor cibernético como de grande interesse para o Brasil e para a Defesa Nacional (BRASIL, 2008).

Ciente das atribuições previstas na END, o Ministério da Defesa (MD), mediante a Diretriz Nº 14, de 2009, atribuiu ao Exército Brasileiro (EB) a responsabilidade de coordenação e integração do Setor Cibernético no âmbito da Defesa e, em agosto de 2010, o Comandante do Exército criou o Centro de Defesa Cibernético (CDCiber).

Dentre os dez primeiros projetos estruturados pelo CDCiber, destacamos o projeto Capacitação, Preparo e Emprego do Setor Cibernético, que visa desenvolver as capacidades operativas, preparando os militares para atuarem no ciberespaço.

O projeto de capacitação foi atribuído ao Centro de Instrução de Guerra Eletrônica (CIGE). O CIGE é uma escola do EB criada em 1984 com foco na capacitação de militares na área de Guerra Eletrônica e, a partir de 2010, com a criação do Núcleo de Defesa Cibernético e, posteriormente, a Seção de Ensino de Guerra Cibernética, passou, também, a atuar no espaço cibernético.

Segundo (BARFORD et. al., 2009), o espaço cibernético é, profundamente, distinto e, por esse motivo, as ferramentas e processos utilizados em outros espaços (físico, eletromagnético, dentre outros) podem não funcionar, adequadamente, com o ambiente cibernético.

Por esse motivo, o CIGE identificou a necessidade de possuir uma ferramenta específica, que pudesse atuar no ciberespaço de forma segura e controlada, auxiliando e viabilizando a formação dos guerreiros cibernéticos.

Dessa forma, a utilização de simuladores foi identificada como sendo a ferramenta mais adequada para a escola preparar os futuros combatentes.

A utilização do simulador pelo CIGE, para treinar e formar seus guerreiros cibernéticos, é o foco deste artigo. Com esse objetivo, o presente trabalho apresenta considerações básicas sobre o simulador, apresenta alguns aspectos técnicos básicos sobre a arquitetura do SIMOC e demonstra o emprego do simulador em exercícios cibernéticos. Antes das considerações finais, apresentamos uma análise crítica do SIMOC, destacando aspectos positivos e negativos do seu uso. Como conclusão, apresentamos algumas observações e sugestões a respeito do simulador de operações cibernéticas.

2 Simulador de operações cibernéticas

A existência de um ambiente simulado para o ensino das técnicas de segurança e defesa, em cibernética, foi considerado primordial pelos instrutores do CIGE, tendo em vista que não seria viável a utilização de redes em produção, por se tratarem de técnicas que, por vezes, podem comprometer a segurança da informação e das comunicações, quando aplicadas em uma situação real.

Ressalta-se, ainda, que a implantação de um simulador proporcionaria economia para o CIGE, uma vez que não seria necessário instalar redes físicas nas instalações da escola, visto que a simulação proporcionaria o emprego de todas as técnicas necessárias para o processo de ensino-aprendizagem. Nesse contexto, entende-se por simulador uma ferramenta (hardware / software) que viabiliza a virtualização de redes de computadores com o intuito de auxiliar no treinamento dos alunos.

Após a decisão de adquirir um simulador para atender às necessidades da Seção de Cibernética, passou-se a analisar os simuladores que poderiam ser adquiridos no mercado e que atendessem às necessidades do CIGE.

Apesar de existirem soluções, extremamente, elaboradas e interessantes (*Cyber training* da empresa ELBIT, *Cyber-Range-In-A-Box (CRIAB)* (BOEING, 2016) e *Cyber Protect* (PASTOR, 2010), nenhuma delas atendia, plenamente, todas as necessidades do CIGE. Dentre as deficiências principais, podemos citar:

"Proibição" política e estratégica, das nações detentoras da solução, de não permitir a comercialização de alguns módulos e cenários;

Soluções contendo cenários fixos, o que tornaria o CIGE totalmente dependente do fornecedor na evolução dos cenários de treinamento; e

Falta de aderência à rotina de atividades realizadas pelo CIGE.

Tendo em vista as limitações dos simuladores analisados, julgou-se necessário o desenvolvimento de um simulador próprio, que atendesse às necessidades nacionais.

Como resultado da avaliação, foram elaboradas especificações de requisitos voltada à experiência de pesquisa aplicada, que foi publicada em Edital (BRASIL, 2011). A empresa vencedora da licitação trabalhou em

um modelo de parceria com o CIGE, por meio do qual os requisitos e as formas de soluções eram discutidos e as metas definidas para o projeto. A primeira versão do simulador foi entregue em 2012. O objetivo dessa primeira fase foi a construção de um software simulador baseado em ambiente virtual, destinado à didática, que atendesse às necessidades de especialização de recursos humanos para executar ações de proteção cibernética e defesa ativa. Após o emprego de um ano do simulador, a Seção de Cibernética estabeleceu novas funções de automatização e apoio ao instrutor, que foram entregues no final de 2014.

O simulador do CIGE, denominado Simulador de Operações de Guerra Cibernética (SIMOC), é um software que permite, por meio de tecnologia de virtualização, a configuração e administração de redes de computadores e oferece um ambiente educacional para treinamento de: configuração e administração de redes; e operações cibernéticas de ataque e defesa às redes TCP/IP, sistemas operacionais e/ou aplicações instaladas nas máquinas e/ou demais dispositivos existentes na rede (GOMES, 2013).

3 Aspectos técnicos

O SIMOC foi desenvolvido para prover simulações virtualizadas e para isso faz uso de máquinas virtuais. As máquinas virtuais desejadas para uma simulação devem ser selecionadas para montar uma rede específica de simulação. Para a criação da rede, é possível especificar configurações em forma de scripts, que serão executados nas máquinas virtuais. Nesse caso, todos os elementos usados na criação da rede são modulares, possibilitando a reutilização e facilitando a expansão do conteúdo disponível.

Nesse contexto, o objetivo do SIMOC é de prover uma ferramenta para geração automática de redes virtualizadas, devendo ser viável a configuração das redes com suas máquinas e serviços de forma flexível e modular, permitindo reuso de conteúdo.

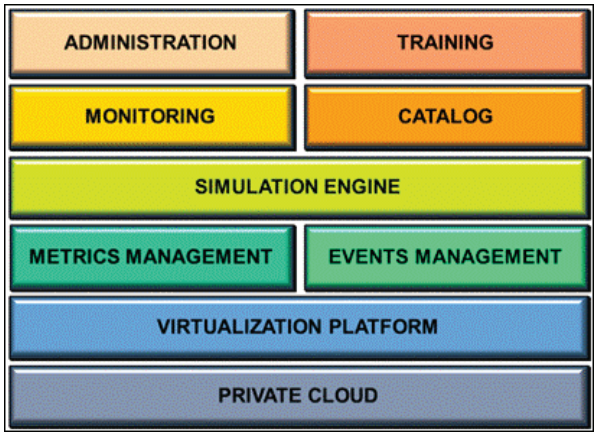
Toda criação de redes virtuais é feita, exclusivamente, por meio da interface Web do sistema, não sendo necessário a intervenção manual na sua preparação. Após especificar a rede no simulador, é possível a sua criação de forma repetida e automatizada, de acordo com a necessidade e a quantidade de alunos que estão sendo treinados. Esses alunos podem possuir redes individualizadas (uma rede por aluno) ou podem estar todos conectados em uma mesma rede.

O projeto foi desenvolvido em Java para Web Server, utilizando o VMware como plataforma de virtualização de máquinas e redes. Para dar dinamismo ao treinamento, foi desenvolvido o conceito do Motor de Simulação, que é a parte do código responsável pela execução de scripts no decorrer dos treinamentos.

Por questões de eficiência, os comandos enviados aos sistemas operacionais virtualizados podem ter tempos de processamentos distintos, de modo a gerenciar os comandos de forma independentemente e concorrentes (implementação em threads).

A Figura 1 apresenta a arquitetura do SIMOC.

Figura -1- Arquitetura do SIMOC



Fonte: Gomes (2013).

A arquitetura (Fig.1) possui 9 módulos:

1. *Private Cloud*: módulo responsável pela administração e controle das redes virtuais criadas para cada treinamento;
2. *Virtualization Platform*: responsável por intermediar a comunicação entre o Motor de Simulação e as redes virtuais;
3. *Events Management*: módulo responsável por gerir a configuração de eventos das redes e treinamentos executados;
4. *Metrics Management*: módulo responsável por gerenciar as métricas que irão ser usadas durante o treinamento;
5. *Engine Simulation*: responsável por prover dinamismo ao treinamento e interagir com as redes durante a execução do treinamento;
6. *Catalog*: gerencia o catálogo de características do sistema;
7. *Monitoring*: responsável por prover o monitoramento dos treinamentos;

8. *Training*: responsável pela gestão do treinamento; e
9. *Administration*: módulo responsável pela administração do sistema, usuários e classes.

4 Emprego do simulador

Para exemplificar a utilização do SIMOC, passaremos a resolver um cenário específico, preexistente no catálogo de cenários.

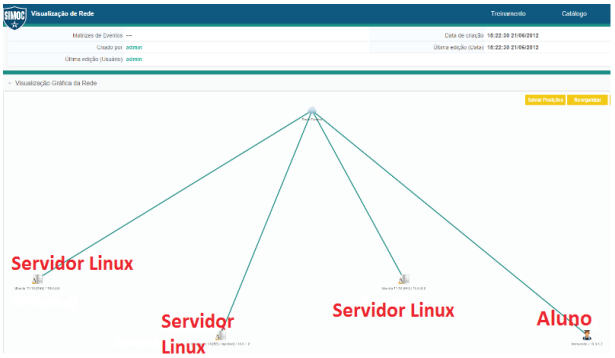
Dentre os 43 cenários existentes, resolveremos o cenário 3A.

4.1 Conhecendo o Cenário 3A

O objetivo deste exercício é de que o aluno explore vulnerabilidades Web, tais como *Cross-site scripting* (XSS), *SQL Injection* e *Remote File Inclusion* (RFI) (EC-COUNCIL, 2014).

No cenário 3A, a rede da simulação possui 3 servidores Linux, na função de servidores Web. Cada um com vulnerabilidades específicas (XSS, SQL e RFI) que deverão ser exploradas pelo instruendo. Nesse cenário, o aluno encontra-se na mesma rede de simulação dos servidores (Fig. 2)

Figura 2 - Rede do Cenário 3A



Fonte: o Autor

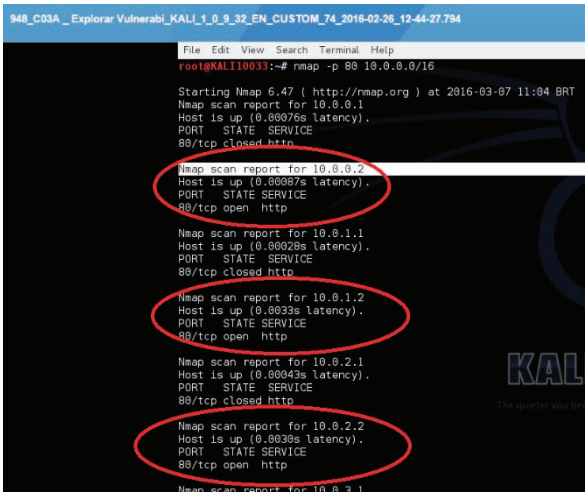
Como atividade, o aluno deverá:

- Executar o *scanning* da rede utilizando as ferramentas disponibilizadas no cenário (Nessus, Nikto, OWASP ou DirBuster);
- Listar as vulnerabilidades encontradas; e
- Realizar ataques às vulnerabilidades encontradas no site web através de técnicas de *SQL Injection*, XSS e RFI.

4.2 Roteiro de Resolução do Cenário 3A

Para realizar a primeira atividade (*scanning* de rede), o aluno poderá realizar o comando "NMAP" para tentar identificar os IPs dos servidores que estão ativos na rede (RUSTCON, 2014). Como resultado do comando, obtemos o seguinte resultado (fig. 3):

Figura 3 – Comando nmap



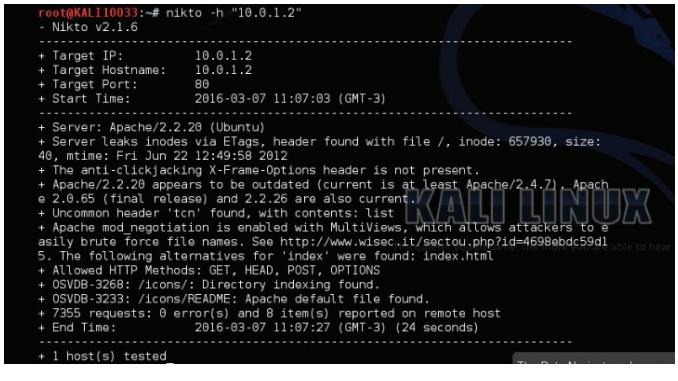
Fonte: o Autor

Na tela de relatório do nmap (Fig. 3), podemos identificar, dentre os vários resultados apresentados, três IPs específicos com as portas 80 abertas. São eles:

- 10.0.0.2
- 10.0.1.2
- 10.0.2.2

Após a identificação dos IPs, os alunos tentarão identificar as vulnerabilidades para cada servidor. Para isso, poderão utilizar as diversas ferramentas disponibilizadas na simulação (Nessus, Nikto, OWASP, DirBuster). Por exemplo, utilizando "nikto", o aluno deverá escolher um IP e executar o comando de varredura.

Figura 4 – Scanning do IP 10.0.0.2



Fonte: o Autor.

Em relação ao resultado obtido com o *scanning* no IP 10.0.1.2 (Fig. 4), podemos identificar as seguintes informações / vulnerabilidades:

- Servidor Apache 2.2.20 – Ubuntu (não atualiza-

do – vulnerabilidade);

- Anti-clickjacking não presente (vulnerabilidade);
- *Headers* incomuns encontrados (possível problema);
- MultiViews habilitado (vulnerável a ataques de força bruta);
- OSVDB – 3233: vulnerabilidade registrada que relata possibilidade de ataque SQL *Injection* em servidor Web.

O mesmo procedimento de varredura deverá ser realizado com os demais servidores.

Após varrer a rede, os alunos deverão apresentar os resultados obtidos, destacando as vulnerabilidades encontradas nos três servidores.

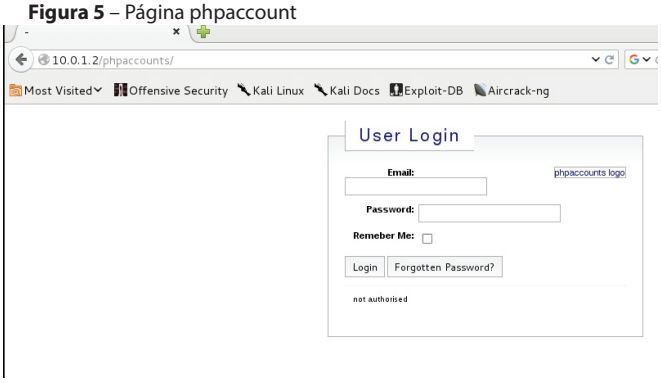
4.3 Ataque ao servidor

O roteiro para o aluno realizar o ataque SQL *Injection* consiste em 9 passos (RUSTCON, 2014).

1. Acessar a máquina do aluno;
2. Rodar o comando startx para iniciar a interface gráfica;

Abrir o Firefox e acessar a URL <

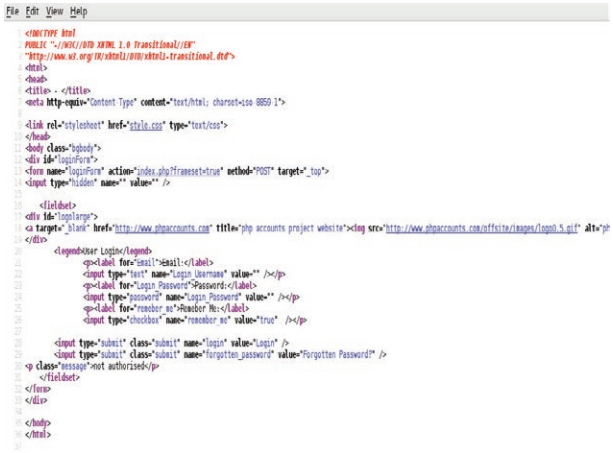
Figura 5 – Página phpaccount



Fonte: o Autor.

1. Abrir o código fonte do formulário web de login (Fig. 6) e encontrar os nomes dos campos de login, senha e ação do formulário;

Figura 6 – Código fonte do formulário Web



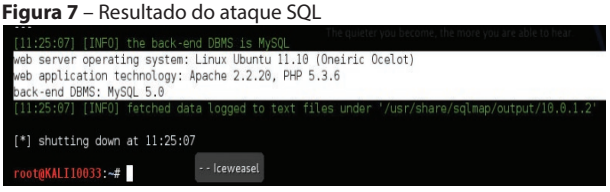
Fonte: o Autor

1. Acessar o diretório /pentest/database/sqlmap
2. Sqlmap é uma ferramenta de teste de penetração gratuita que automatiza os processos de detecção e exploração do ataque SQL *Injection*.
3. Executar o comando./sqlmap.py –u
4. Digitar http://10.0.1.2/phpaccounts/index.php?frameset=true --data='Login_Username=teste&Login_Password=teste&login=-Login'

Os parâmetros "'Login_Username" e "Login_Password" digitados no sqlmap foram retirados do código fonte (passo 4)

Como resultado é impresso o sistema operacional, versão do Apache, Mysql e PHP (Fig. 7);

Figura 7 – Resultado do ataque SQL



Fonte: o Autor.

Neste ataque os alunos obtiveram alguns metadados a respeito do servidor. A partir dessas informações, um atacante poderia tentar obter outras informações como: nomes, senhas etc.

Faça login no formulário web usando:

Usuário: x' or '1' = '1'; /*

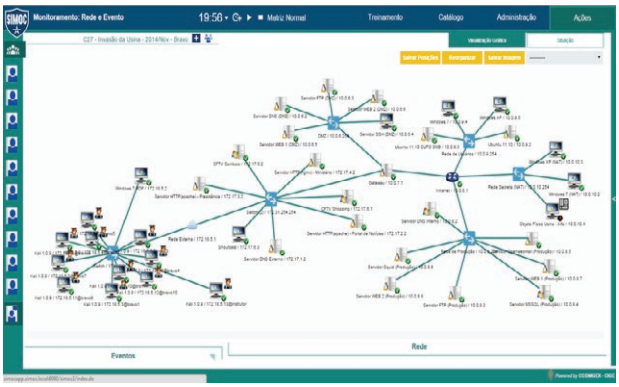
Senha: */

Uma vez identificado que o servidor é vulnerável a ataques de SQL *Injection*, o atacante pode tentar acessar o banco de dados utilizando diversos tipos de *payload* no campo usuário e senha.

4.4 Cenários complexos

Diferentemente do senário apresentado anteriormente, o cenário 27 apresenta uma complexidade maior, com diversos passos intermediários para realizar o ataque ao alvo específico (usina). A rede do cenário 27 pode ser observada na figura 8.

Figura 8 – Rede virtualizada do Cenário 27



Fonte: o Autor

Em complemento, uma maquete de treinamento é utilizada para facilitar a compreensão dos alunos. Nessa pequena cidade (Fig. 9), os alunos podem interagir com o cenário, podendo interferir na rede de iluminação, nas comportas da represa, na linha do trem, no placar do campo de futebol e nos semáforos.

Figura 9 – Maquete utilizada pelo SIMOC

Fonte: o Autor

A utilização da maquete permite a identificação do impacto de um ataque cibernético no ambiente cinético, o que motiva e aprimora o ensino.

5 Análise Crítica

A utilização de simuladores para o treinamento no ambiente cibernético tem se mostrado muito interessante. Em particular, a utilização do SIMOC apresentou as seguintes vantagens (MACHADO et al., 2015):

1. Possibilidade de criar diversos tipos de simulações (exercícios) tais como: exercícios de dupla ação (envolvendo dois partidos), criação de redes de computadores (a partir de uma situação-problema) e a gerência de uma rede de dados;
2. Reuso de elementos (objetos, eventos, métricas etc.) pré-registrados no catálogo do simulador, com o objetivo de adequar o cenário a uma nova situação-problema ou de criar uma nova;
3. Criar redes mistas, contendo segmentos virtuais e segmentos de rede reais;
4. Variedade de funcionalidades que apoiam o instrutor durante as simulações (exercícios). Como: gerador de tráfego randômico, defesa automatizada, ataque automatizado, recurso de gravação, material de apoio e aplicação das diversas métricas existentes;
5. Monitoramento em tempo real com a possibilidade de interferência do instrutor durante a execução dos exercícios. Como exemplo, o instrutor pode: pausar a simulação, adiantar, repetir uma situação, mudar parte do cenário e modificar o nível de dificuldade do exercício;
6. A implementação do simulador conta com uma relativa segurança na sua infraestrutura, seja para o acesso interno (administrador, instrutor, alunos) ou para acessos externos;
7. A utilização de maquetes, conectadas ao simulador, propicia ao instruendo a possibilidade de identificar a consequência "real" de um ataque cibernético, realizado pelo aluno, sobre a infraestrutura de uma localidade (fábrica, cidade etc.);
8. O simulador pode ser acessado, remotamente, permitindo a realização de treinamento de militares em diferentes localidades.

Contudo, algumas limitações da abordagem foram identificadas. As principais limitações atuais do SIMOC são (MACHADO et al., 2015):

1. Inviabilidade de simular ligações de fibra ótica. No entanto, essa limitação pode ser, parcialmente, contornada com a integração de redes de fibra óticas reais ao SIMOC;
2. Ainda não existem cenários que contemplem

ativos e situações militarizados, por exemplo: rádios militares, sistemas de radar, sistemas de Guerra Eletrônica, satélite de comunicações militares, dentre outros.

3. Os principais mercados de TI não disponibilizam as versões virtualizadas de seus produtos. Uma possibilidade de contornar esse problema seria de fazer parcerias com as empresas principais para obter os produtos de interesse na forma virtualizada. Por exemplo, atualmente, existe a possibilidade de virtualizar roteadores da empresa CISCO (CISCO, 2015). Contudo, para realizar essa virtualização, dependemos de autorização da empresa;
4. O simulador não é um ambiente adequado para a análise de vírus de computador porque *malwares* avançados e os *Advanced Persistent Threats* (APT) são capazes de identificar a existência de máquinas virtuais e nesse caso os APTs não executam seus códigos maliciosos;
5. Atualmente, não é possível conectar no SIMOC as máquinas pessoais dos alunos para realizar os exercícios. Esse fato acaba-se tornando um óbice, pois é comum que esses instruendos já possuam, em suas máquinas, suas ferramentas instaladas e customizadas para as atividades no ciberespaço.

Além dessas limitações, o SIMOC, ainda, possui algumas necessidades que precisam ser atendidas, por exemplo: Infraestrutura de *Cloud* Privada (dispositivos de rede virtualizados, servidores virtualizados, plataforma de virtualização VMWare); Instrutores capacitados para elaborar cenários complexos; e Licenças para máquinas virtuais não gratuitas (MACHADO et al., 2015).

6 Conclusões

O presente artigo apresentou o emprego do Simulador de Operações de Guerra Cibernética (SIMOC) do Exército Brasileiro na capacitação de militares do setor cibernético.

O SIMOC é um projeto em andamento, que está em constante evolução, seja em relação a novos desenvolvimentos, como na construção de novos conteúdos ou no desenvolvimento de novas funcionalidades, com o objetivo de aprimorar a capacitação dos militares. Consequentemente, novos requisitos continuam sendo levantados e novas ideias implantadas.

O simulador foi desenvolvido, inicialmente, para atender às demandas do CIGE, tendo o seu emprego focado no curso de Guerra Cibernética. No entanto, atualmente, o simulador, também, está sendo empregado em outros adestramentos.

Desse modo, com a experiência de uso do SIMOC, temos condição de afirmar que as vantagens teóricas tradicionalmente citadas, como o aumento da escalabilidade, redução de custo e redução de tempo, foram constatadas na prática (MACHADO et al., 2015).

Assim como foram identificadas muitas vantagens do uso do simulador neste artigo, limitações, também, foram mapeadas e os seus respectivos tratamentos estão sendo endereçados pela equipe responsável pelo projeto.

Uma limitação relevante do uso de um simulador baseado em uma solução de virtualização de rede é o fato de que os principais ativos de rede do mercado não permitirem a virtualização de seus sistemas operacionais. Assim, os cenários criados podem se tornar, excessivamente, acadêmicos e teóricos, divergindo do objetivo do treinamento, que é fazer uso de redes corporativas com ativos de rede de mercado.

Para tentar contornar essa limitação, o SIMOC possui um recurso chamado de rede mista contendo ativos virtuais e físicos, mas essa é uma solução paliativa pois o fato de fazer uso de um ativo físico traz consigo as desvantagens de não fazer uso de uma rede virtual.

Para as futuras utilizações do simulador, pretende-se acoplar o SIMOC ao LAB VOLT (simulador de radar utilizado pelo CIGE) para realizar a identificação de impacto causado por um ataque cibernético sobre radares.

Como estudo futuro, sugerimos o uso da inteligência artificial para que o simulador filtre as ações dos alunos, que ele (simulador), ainda, não possui na sua biblioteca e disponibilize essas ações de ataque / defesa para que o instrutor tome conhecimento e insira, ou não, essas novas ações no banco de dados do simulador. Essa funcionalidade poderia manter o simulador atualizado, com formas de ataque e defesa atuais, o que, possivelmente, elevaria o nível de treinamento e preparação dos recursos humanos, submetidos ao simulador.

Referências

BARFORD, P. et al. *Cyber situational awareness:* issues and research. New York: Springer, 2009.

BOEING. *Cyber-Range-in-a-Box.* Disponível em: <http://www.boeing.com/defense/cybersecurity-information-management/#/cyber-range-in-a-box>. Acesso em: 20 jun. 2016.

BRASIL. Ministério da Defesa. *Edital do pregão eletrônico n. 28.* Brasília: SALC, base administrativa do Centro de Comunicações e Guerra Eletrônica do Exército, 2011.

BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa.* 2. ed. Brasília: Ministério da Defesa, 2008.

CISCO. Disponível em: <http://www.cisco.com>. Acesso em: 15 jan. 2015.

EC-Council. ETHICAL HACKING AND COUNTER-MEASURES. *Hacking web applications:* module 13. v. 8. 2014. Disponível em: <http://www.arthur-training.com/Downloads/CEH/CEH%20v8%20Labs%20Module%2013%20Hacking%20Web%20Applications.pdf>.

GOMES, R. *Simulador de operações de guerra cibernética*. Palestra, 2013.

MACHADO, A. F. A.; REGUEIRA, F. A. C.; REZENDE, J. Use of simulation to achieve better results in cyber military training. In: *MILCOM:* Military Communications Conference, 2015, Tampa, IEEE Communications Society, p. 1270.

PASTOR, V.; DÍAZ, G.; CASTRO, M. *State-of-the-art simulation systems for information Security Education*. Madri: Training and Awareness, 2010.

RUSTCON. *Simulador de operações de guerra cibernética:* documento de resolução de cenários. Escritório de Projetos, 2014.