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

ANDRÉ FERREIRA ALVES MACHADO

SIMULADOR DE OPERAÇÕES DE GUERRA CIBERNÉTICA: FERRAMENTA DE TREINAMENTO E PREPARO DE RECURSOS HUMANOS PARA ATUAREM NO CIBERESPAÇO.

Brasília
2016

ANDRÉ FERREIRA ALVES MACHADO

SIMULADOR DE OPERAÇÕES DE GUERRA CIBERNÉTICA: FERRAMENTA DE TREINAMENTO E PREPARO DE RECURSOS HUMANOS PARA ATUAREM NO CIBERESPAÇO.

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

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

Brasília
2016

ANDRÉ FERREIRA ALVES MACHADO

SIMULADOR DE OPERAÇÕES DE GUERRA CIBERNÉTICA: FERRAMENTA DE TREINAMENTO E PREPARO DE RECURSOS HUMANOS PARA ATUAREM NO CIBERESPAÇO.

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

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

Brasília, ___ de _____ de 2016.

Banca Examinadora

_____

Prof. Dr. Gilberto de Oliveira Netto

_____

Prof. Dr. Gilson Ciarallo

RESUMO

A revolução tecnológica transformou e ainda transforma, cada dia mais, a vida de pessoas, estados e nações. Dentro deste cenário, a cibernética ganha espaço em reportagens de revistas e jornais, programas de televisão, nas mídias sociais e até mesmo em filmes de Hollywood. Os acontecimentos no ciberespaço envolvem e atingem a todos, pois estamos conectados em uma grande rede virtual. Neste contexto, a preocupação de defender as fronteiras virtuais e formar soldados digitais, ganha foco nos governos de todo o mundo. A preocupação brasileira de formar recursos humanos aptos a combater no espaço cibernético está registrada em diversos documentos nacionais. Desta forma, este trabalho buscou apresentar uma ferramenta de simulação voltada para o treinamento de militares brasileiros que atuarão no espaço cibernético. Com este objetivo geral, realizamos pesquisas bibliográficas em diversas fontes militares (manuais ostensivos), artigos acadêmicos (nacionais e internacionais), materiais didáticos utilizados em cursos específicos da área cibernética e livros da ciência da computação. Um estudo de caso foi apresentado, assim como o desenvolvimento de um exercício de ataque cibernético realizado com um simulador cibernético. Por meio deste estudo, foi possível identificar vantagens e desvantagens da ferramenta em questão, bem como salientar a importância do assunto e a dificuldade da formação de recursos humanos aptos a operarem em ambientes virtuais, com segurança e eficiência.

Palavras-chave: Cibernética. Simulador. Capacitação.

ABSTRACT

The technological revolution has transformed and still turns, each day more, the life of people, states and nations. Within this scenario, cybernetics is highlighted in reports from newspapers and magazines, television programs, social media and even in Hollywood movies. The events in cyberspace involve everyone, because we are connected in a big virtual network. In this context, the concern of defending the vertical borders and form digital soldiers, gains focus in governments around the world. The Brazilian concern to train human resources capable of combat in cyberspace is registered in several national documents. Thus, this study aimed to present a simulation tool dedicated to the training of Brazilian soldiers who will act in cyberspace. With this overall objective, we conducted literature searches in several military sources (ostensible manuals), academic articles (national and international), teaching materials used in specific courses of cyber area and books of computer science. A case study was presented, as well as the development of a cyber attack exercise conducted with a cyber simulator. Through this study, it was possible to identify advantages and disadvantages of the tool in question, as well as stress the importance of the subject and the difficulty of the formation of human resources capable of operating in a virtual environment, safely and efficiently.

Key words: Cybernetics. Simulator. Qualification.

LISTA DE FIGURAS

Sumário

INTRODUÇÃO

A partir dos avanços tecnológicos, transformações vividas pela humanidade são facilmente constatadas nas mais distintas áreas. Na saúde, por exemplo, equipamentos modernos auxiliam na prevenção e tratamento das mais diversas doenças. Na área das ciências exatas, o horizonte do saber cresce a cada dia e teorias formuladas a séculos atrás ganham provas científicas modernas. Na educação, a tecnologia apresenta-se como grande aliada de professores que buscam aumentar e aprimorar o conhecimento de seus alunos.

Dentro deste processo tecnológico, surgem avanços variados, contudo, pessoas mal intencionadas podem utilizar esta tecnologia para tirar proveito, obter informações reservadas, auferir dinheiro e poder. Dentro deste escopo tecnológico, mais especificamente na área da computação, abordaremos as vulnerabilidades que a rede mundial de computadores (Internet) pode possuir afetando a vida dos cidadãos, estados e governos.

Nosso estudo terá como contexto a situação das Forças Armadas e mais especificamente a do Exército Brasileiro. Assim como muitas instituições civis, o Exército mantém na Internet, disponível para o público, dezenas de sites da instituição. Páginas divulgando suas Unidades e Grandes Unidades, operações militares, escolas de formação e demais sites que são acessadas diariamente por militares e civis, brasileiros ou não.

Ciente dos problemas ocorridos ao redor do mundo digital, o Gabinete de Segurança Institucional, da Presidência da República (GSIPR), por meio do documento intitulado O Livro Verde - Segurança Cibernética no Brasil (MANDARINO; CANONGIA, 2010) destaca a carência da cultura em segurança cibernética e ainda ressalta a urgência do País em desenvolver esta potencialidade.

Desta forma, este trabalho pretende responder a seguinte problemática: Como preparar profissionais militares para atuarem na área cibernética?

Para responder a questão de pesquisa, destacamos como objetivo geral deste trabalho a análise de ferramentas computacionais que viabilizem o preparo educacional de pessoas para atuarem, de forma segura, no ambiente cibernético. Ainda, como objetivos específicos, destacamos a necessidade do estudo a respeito da cibernética; análises das ferramentas educacionais existentes; e da identificação das possíveis soluções.

Para alcançar esses objetivos, este trabalho apresentará uma pesquisa bibliográfica extensa, envolvendo manuais militares (de conhecimento ostensivo), legislações, artigos científicos nacionais e internacionais, manuais técnicos e livros específicos da área. Na sequência, realizaremos um estudo de caso envolvendo uma organização militar particular que possui a responsabilidade de realizar a formação de militares das diversas forças armadas para atuarem no espaço cibernético.

Espera-se demonstrar com este estudo a importância da utilização de ferramentas específicas para a formação de "guerreiros cibernéticos", destacando também a importância do assunto para a segurança militar e, consequentemente, para a nação brasileira.

Para alcançar todos estes objetivos, responder a questão problema e justificar a importância da pesquisa, estruturamos este trabalho em 4 capítulos. No primeiro capítulo, apresentaremos considerações a respeito da cibernética, apresentando um breve histórico, comentando sobre a importância e relevância do assunto, apresentando alguns conceitos necessários para o desenvolvimento do trabalho e concluindo com a apresentação da organização militar que servirá de estudo de caso.

O segundo capítulo proporciona uma análise sobre simulação. Este capítulo está subdividido em mais três: apresentação sobre simuladores e suas características principais; análise de simuladores com propósito de atuar no ambiente cibernético; e, por fim, um breve estudo sobre simuladores cibernéticos de uso militar.

O terceiro capítulo irá apresentar um estudo de caso envolvendo uma ferramenta específica utilizada por uma escola militar. E o último capítulo irá realizar a simulação de um exercício cibernético, demonstrando as potencialidades e facilidades da ferramenta.

1. Cibernética

A palavra cibernética deriva do termo grego *kybernetidé*, que significava a arte de pilotar uma embarcação, entretanto o significado moderno da palavra relaciona-se ao uso do termo *governator* (do inglês) em Mecânica. Em 1868, o físico escocês James Clerk Maxwell descreveu um certo tipo de mecanismo de controle no ensaio *The Theory of Governors*. Foi nesse ensaio de Maxwell, que o matemático Norbert Wiener diz ter-se inspirado para, em 1948, escrever a obra *Cybernetics, or Control and Communcation in the Animal and the Machine*. O interesse de Wiener por esse tema parece ter origem em um projeto de pesquisa iniciado nos primeiros anos da década de 1940, quando, como parte do esforço de guerra norte-americano, ele recebeu a incumbência de desenvolver um "sistema de controle de baterias antiaéreas que fosse capaz de acompanhar a trajetória em que se movia um avião, predizer sua posição futura e disparar fogo levando em conta, senão só os hiatos humanos do canhão e do avião envolvidos." (MOREIRA, 1980, p. 32). Segundo o próprio Wiener, a cibernética envolveria "o estudo do que em contexto humano é às vezes descrito genericamente como o ato de pensar e o que em engenharia é conhecido como controle e comunicação" (MOREIRA, 1980, p. 33).

Assim os primeiros projetos "cibernéticos" tratavam do desenvolvimento de mecanismos destinados a regular automaticamente determinados artefatos industriais e bélicos, capazes de substituir o homem na tarefa de corrigir desvios dos sistemas projetados, por dispositivos reguladores programados especificamente para esta finalidade (WIENER apud EPSTEIN, 1986, p. 13-14). De forma geral, o termo cibernética no século XX passou a sugerir "o estudo das funções humanas de controle e dos sistemas mecânicos e eletrônicos que se destinam a substituí-los" (THEOPHILO, 2011).

No entanto, com o advento das redes de computadores (especialmente a internet), a conotação da cibernética se aproxima cada vez mais da ideia de sistemas interligados de informação. Nesse sentido, o controle dos sistemas de comunicação passa a dominar a "agenda cibernética". Temas como pirataria, espionagem e ataques cibernéticos surgem na mídia mundial.

Quadro 1 – Ações Cibernéticas

Ano	Envolvidos	Tipo de ação	Obs
1990	EUA	Pirataria Cibernética	-
2003	China x EUA	Ciberespionagem	Titan Rain
2007	Estônia x Rússia	Ataque cibernético	DDOS
2008	Geórgia x Rússia	Ataque cibernético	DDOS
2009	China x Tibet	Ciberespionagem	GhostNet
2010	EUA e Israel x Irã	Ataque Cibernético	Stuxnet *(malware)*
2010	Suécia, EUA	Ciberespionagem	*WikiLeaks*
2011	Canada x China	Ciberespionagem	-
2012	Iran	Ciberespionagem	*Flame (malware)*
2013	Coreia do Sul x Coreia do Norte	Ataque Cibernético	*DarkSeoul (malware)*

Fonte: o Autor

No Quadro 1, verificamos a evolução das ações cibernética ao redor do mundo. Embora seja um resumo bastante ínfimo, podemos constatar a importância do assunto que aborda questões de espionagem, pirataria e ataque cibernético. A coluna mais à direita, apresenta algumas informações complementares relacionada aos eventos em tela.

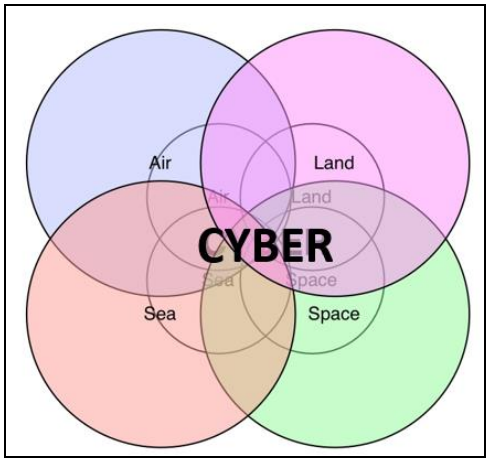
Ainda como evolução destas ações cibernéticas, novos conceitos foram adicionados ao "dicionário cibernético". Segundo o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, do Departamento de Segurança da Informação e Comunicação, Segurança Cibernética é: "arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (GSIPR, 2009d)".

O manual de Doutrina Militar do Ministério da Defesa Brasileiro (BRASIL, 2014), apresenta mais algumas definições importantes ao tema.

> Espaço Cibernético - espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas. (BRASIL, 2014)
> Defesa Cibernética - conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (BRASIL, 2014).
> Guerra Cibernética - corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. (BRASIL, 2014)

O fato é que a guerra cibernética impõe uma nova realidade para os teatros de operações militares na medida em que o espaço cibernético constitui-se como um novo tipo de “território” (espaço de poder).

Figura 1 – Espaço de Poder



Fonte: MACHADO; BARRETO; YANO (2013)

A Figura 1 ilustra as 4 áreas de atuação militar tradicionais (ar, mar, terra e espacial) e no centro da figura um quinto elemento do combate é identificado pela palavra “CYBER”. Destaca-se que este quinto elemento encontra-se intencionalmente no meio da figura, pois possui influência em todos as demais áreas de atuação.

Esta influência da cibernética ocorre porque atualmente a maioria dos sistemas de informação, necessários para o funcionamento da sociedade moderna, encontram-se interligados por meio de redes de computadores. Nesse contexto, Dutra (2011) salienta:

> Os alvos não são mais somente pessoal e instalações militares. Agora, bancos, usinas elétricas, empresas de telefonia e de telecomunicações, sistemas de transporte e logística, serviços de emergência e segurança pública, entre outros são alvos em potencial, uma vez que a indisponibilidade continuada de quaisquer destes serviços certamente levaria uma nação ao colapso (DUTRA, 2011).

Cientes do poder de combate proporcionado pelo controle do espaço cibernético, forças militares dos diversos países iniciaram a exploração deste ambiente. Como exemplo, desde 2013, a Coreia do Norte tem reportado possuir times qualificados em cibernética para atuarem no espaço cibernético adversário (Figura 2 - a).

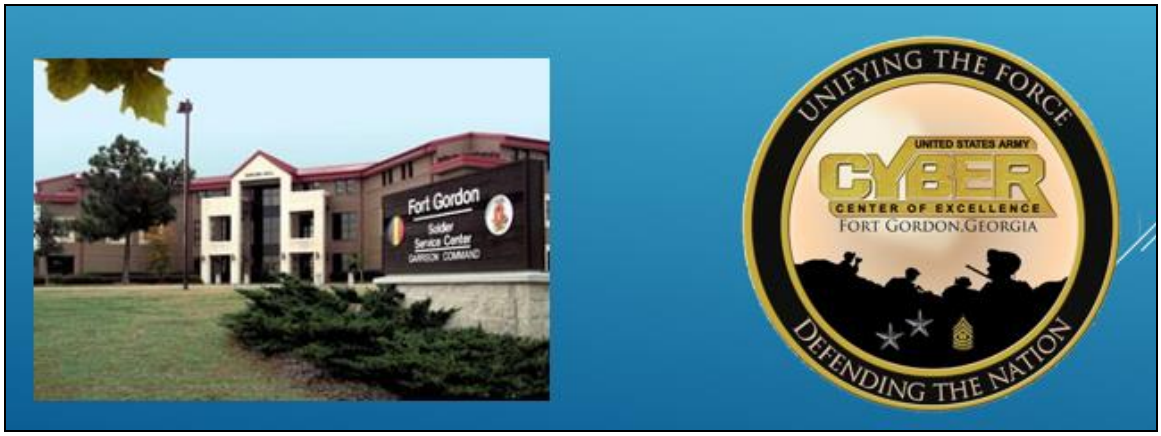
Figura 2 – Forças militares cibernéticas

(a) **(b)**

Fonte: MACHADO (2015)

Da mesma forma, o exército de Israel tem treinado militares para protegerem o seu espaço cibernético contra prováveis ataques (Figura 2 – b). O mesmo ocorreu no exército americano que, em 2010, criou o *U.S. Army Cyber Command*; em 2013 publicou a *Joint Publication Cyberspace Operations*; e em 2014 ativou a Brigada de Proteção Cibernética e alterou o nome do Centro de Excelência de Comunicações (Fort Gordon) para Centro de Excelência Cibernética (Figura 3).

Figura 3 – Centro de Excelência Cibernética dos EUA



Fonte: MACHADO (2015)

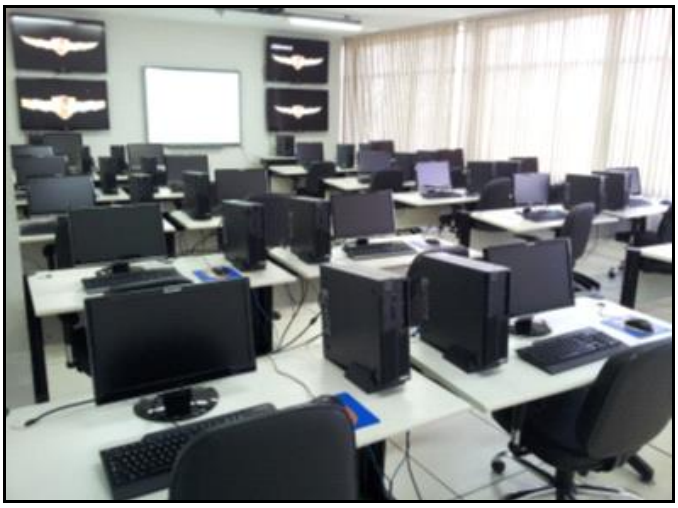
No Brasil, em 2008 o Ministério da Defesa (MD), por meio da Estratégia Nacional de Defesa – END (BRASIL, 2008), reconheceu o setor cibernético como de grande interesse, cabendo ao Exército desenvolvê-lo. Neste sentido, o Centro de Defesa Cibernético (CDCiber) é criado no Comando do Exército e inicia suas atividades com o lançamento de diversos projetos estratégicos (Figura 4)

Figura 4 – Projeto Estratégico de Defesa Cibernética

Fonte: CDCIBER (2014)

O primeiro projeto, denominado Capacitação, Preparo e Emprego Operacional, foi entregue ao Centro de Instrução de Guerra Eletrônica (CIGE) que, em 2010, criou a Seção de Instrução de Guerra Cibernética e, em 2011, iniciou em suas instalações (Figura 5) o Curso de Guerra Cibernética para oficiais e sargentos da Marinha, Exército e Aeronáutica.

Figura 5 – Laboratório de Cibernética do CIGE



Fonte: DIEDRICH; MACHADO (2015)

Para a formação dos guerreiros cibernéticos, a Seção de Instrução de Guerra Cibernética do CIGE identificou a necessidade de possuir uma ferramenta automatizada que pudesse auxiliar, de forma segura e controlada, na formação dos futuros combatentes digitais. Neste sentido, foi identificado a possibilidade de se utilizar simuladores para este objetivo.

2. Simulação

Simulação é a manipulação de um modelo que busca representar o comportamento de um sistema. É uma ferramenta para explora sistemas e processos sem ter que construí-los (ICEMAET, 2014).

De acordo com Shannon (1975) simulação é:

> Processo de projetar modelos de um sistema (ou processo), e conduzir experimentos com esses modelos com o propósito de entender o comportamento do sistema ou avaliar várias estratégias para a operação do sistema (SHANNON, 1975).

Independente do conceito utilizado, a simulação torna-se viável a partir da utilização de computadores, que carregam o simulador com propriedades e características de sistemas reais, criando um ambiente "virtual", que é usado para testar as teorias desejadas. O computador efetua os cálculos necessários para a interação do ambiente virtual com o objeto em estudo e apresenta os resultados do experimento no formato desejado pelo analista.

Atualmente muitos simuladores são empregados em diversos ambientes de trabalhos, por inúmeras diferentes razoes. Por exemplo, a realização de testes em equipamentos físicos, e em dimensões reais, podem custar muito caro tornando a simulação uma opção interessante. Além do mais, o uso de simuladores pode realizar análises mais rápidas (economizando recursos e tempo) e em diferentes escalas, o que favorece o realismo das análises (LEEUWEN, et al., 2010). Assim como, em situações reais, a quantidade de problemas (vulnerabilidades) de um sistema, cresce proporcional a sua complexidade, o que motiva o uso de simuladores ao invés de testes exaustivos em sistemas complexos (LICOL, 2005).

Como exemplo de utilização de simuladores, encontramos as áreas de: Administração (planejamento da produção de fábricas); Economia (modelos macroeconômicos); Engenharia elétrica (geração e teste de circuitos eletrônicos); Engenharia de transportes (controle de tráfego); Biologia e medicina (propagação de doenças endêmicas, crescimento populacional das espécies); Ciências sociais (crescimento demográfico); Engenharia Aeroespacial (simuladores de aeronaves, lançadores). E, naturalmente que na Computação e áreas afins este recurso pode ser muito utilizado na organização de computadores, criação de circuitos lógicos, simulação de redes de computadores, criação de sistemas de bancos de dados, etc.

Segundo Licol (2005) e Pastor (2010), a simulação tem sido fundamental para a Ciência da Computação, particularmente nas áreas de segurança, sendo utilizada por indústrias e agências de governos preocupados com a segurança de infraestruturas críticas, como centrais de energia e centros financeiros.

Neste sentido, os simuladores são, cada vez mais empregados para análises de sistema computadorizados, pelo fato do seu alto grau de complexidade, o que favorece o surgimento de problemas (vulnerabilidades) que pode prejudicar o funcionamento normal dos sistemas.

A técnica de simulação também pode ser combinada com a técnica de virtualização, viabilizando análises mais realísticas.

Segundo Singh (2004), virtualização é um framework ou metodologia para dividir os recursos de um computador em múltiplos ambientes de execução. Esta técnica permite, por exemplo, particionar um único sistema computacional em vários outros denominados de máquinas virtuais. Cada máquina virtual oferece um ambiente completo muito similar a uma máquina física. Com isso, cada máquina virtual pode ter seu próprio sistema operacional, aplicativos e serviços de rede. (CARISSIMI, 2008).

O uso de máquinas virtuais, proporcionam muitas vantagens. Por exemplo, a virtualização de uma significante porção de hardwares modernos (complexos) viabilizando os estudos necessários referentes a equipamentos e serviços prestados por estes hardwares. Também, é possível a criação de fluxos de dados que seriam gerados por dezenas de sistemas, sem no entanto possuir os equipamentos reais para a produção destes fluxos. Finalmente, como último exemplo, a virtualização pode ser utilizada para a emulação de equipamentos que são normalmente encontrados em redes típicas de produção (LEEUWEN, et al., 2010).

Emulação, segundo o dicionário Houaiss, é o esforço para imitar ou tentar seguir o exemplo de alguém. Em termos computacionais, é a capacidade de um programa de computador, ou de um dispositivo eletrônico, de “imitar” outro programa ou dispositivo. (CARISSIMI, 2008).

Na área específica de educação, Roger Schank (SRIKUMAR, 1995) professor emérito de Filosofia, Educação e Ciência da Computação, recomenda a técnica de simulação para diversas áreas.

> The best educational software ever written is the flight simulator … A 747 pilot can try different strategies, even crash the plane repeatedly with no consequences. (SRIKUMAR, 1995, p.56)

Neste mesmo sentido, Delooze, Mckean e Mostow (2004) salienta que a técnica de simulação voltada para o ensino já foi estudada pela Academia da Marinha Americana para facilitar a compreensão dos estudantes na área específica de segurança da computação

> The United States Naval Academy will incorporate simulation into the senior-level Information Assurance course for the Information Technology Majors… (DELOOZE, MCKEAN e MOSTOW, 2004)

Ainda como exemplo, profissionais do Departamento de Defesa Americano, conduzem treinamentos e exercícios operacionais com o suporte de simuladores para controlar possíveis ameaças em redes de computadores (DELOOZE, MCKEAN e MOSTOW, 2004).

Segundo Delooze, Mckean e Mostow (2004), para conduzir uma boa simulação faz-se necessário: possuir conhecimentos sobre metodologias de simulação; formular o problema corretamente; obter informações consistentes sobre os procedimentos operacionais do sistema; modelar adequadamente os fenômenos aleatórios do sistema em estudo; escolher o software mais adequado e utilizá-lo de forma correta; estabelecer a validade e credibilidade do modelo; e utilizar procedimentos estatísticos adequados para analisar os resultados.

Todos estes itens devem ser explorados para se obter uma boa simulação do sistema em estudo. Assim podemos verificar que a simulação auxilia a análise de sistemas complexos, no entanto, requer um planejamento e recursos adequados, para que produza resultados realísticos. Caso contrário, estaremos perdendo tempo, dinheiro e correndo risco de implantar algum produto que não foi adequadamente testado e avaliado pela simulação.

Além de um bom planejamento, o recurso da simulação exige precisão, tamanho adequado e correção dos dados de entrada. Dados incorretos irão gerar uma simulação imprecisa e consequentemente incorreta.

2.1 Simuladores

Um simulador é um programa que implementa um modelo de sistema recebendo parâmetros de entrada e condições iniciais de contorno e serve para auxiliar na predição e análise de comportamento do sistema simulado. (CARISSIMI, 2008)

Com a crescente utilização da simulação, linguagens de programação específicas, de maior desempenho, foram desenvolvidas e outras ferramentas foram adicionadas às

linguagens anteriores. Dentre elas destacamos: *General Purpose Simulation System* (GPSS)[1], Simscript[2], Siman (PEGDEN, 1983), Simula[3] e GASP (ALAN, PRITSKER, 1977). Estas linguagens possuem estruturas pré-existentes para modelagem e, por este motivo, diminuem o tempo de programação.

Os ambientes de simulação englobam a descrição do modelo, o controle da simulação e a coleta e visualização de estatísticas. Como exemplo de ambientes de propósito geral (que atende a diversas áreas), temos: MicroSaint[4], PowerSim[5], Simul8[6] e Visual Simulation Environment (VSE) (BALCI, et. al., 1998). E como exemplo de ambientes de propósito específico (que atende a uma área de estudo particular) podemos citar: Taylor Manufacturing Simulation (KING, 1996), ProModel[7] e Farming Simulatior[8].

Desta forma, temos uma quantidade grande de simuladores disponíveis no mercado. Como exemplo, o software Arena[9] é um ambiente gráfico integrado de simulação. O seu diferencial está na ausência de linhas de código, pois todo o processo de criação do modelo de simulação é gráfico, visual e de maneira integrada. A linguagem incorporada é o SIMAN (DAVIS; PEGDEN, 1988).

O GloMoSim (ZENG; GERLA, 1998) é um simulador moderno e de alto desempenho, com enfoque em redes *wireless* e móveis. O Opnet é altamente utilizado no ambiente corporativo para simulação de redes de telecomunicações. Já o NCTUns[10] é didático, de fácil utilização e moderno. Porém é limitado em sua escalabilidade, pois o número máximo de nós na simulação é baixo.

O *IMUNES*[11] é um sistema de emulação/simulação realístico de redes baseados no sistema operacional *freeBSD*. Foi projetado para se integrar com o *kernel* do *freeBSD* e, através disso, cria nós virtuais utilizando-se de várias instâncias, o que permite gerar uma emulação realística de uma rede. Desta forma, aplicativos geradores de tráfego, analisadores de rede, servidores de Web entre outras ferramentas, podem rodar nos nós virtuais como se

[1] http://www.csd.uwo.ca/staff/dave/gpss.html
[2] http://www.simscript.com/
[3] http://staff.um.edu.mt/jskl1/talk.html
[4] http://www.microsaintsharp.com/
[5] http://www.powersim.com/
[6] http://www.simul8.com/
[7] https://www.promodel.com/
[8] http://www.farming2015mods.com/
[9] https://www.arenasimulation.com/
[10] http://www.techrepublic.com/resource-library/whitepapers/nctuns-6-0-a-simulator-for-advanced-wireless-vehicular-network-research/
[11] http://www.brianlinkletter.com/imunes-network-simulator-test-drive/

fossem máquinas reais. Além disso, o *IMUNES* possui um ambiente gráfico para a criação e gestão de cenários de simulação. Embora a interface gráfica possa rodar nos principais sistemas operacionais, a emulação só pode ser executada em ambientes *freeBSD*. Pelo fato deste simulador possuir uma grande utilização na área acadêmica, encontra-se com uma base relativamente consolidada e, por este motivo, é utilizado para validar outros simuladores.

Existem também simuladores gratuitos como o Delta3D[12] que possui ampla variedade de aplicações de modelagem e simulação. E os simuladores voltados a área militar. Por exemplo, o VR-Forces[13] que é um poderoso e flexível simulador de cenários (Figura 6). Possui muitas características para o uso de treinamento tático, gerador de ameaças e teste de modelo de comportamento.

Figura 6 - Simulador VR-Forces

Fonte: Barreto; et al. (2012)

2.2 Simuladores Cibernéticos

Para este trabalho, definiremos Simulador Cibernético como sendo soluções computadorizadas, constituídas de hardware e software, destinadas a implementar um modelo de um ambiente cibernético, recebendo parâmetros de entrada e condições iniciais, com os propósitos de: representar o comportamento de um ambiente computacional, realizar predições, demostrar consequências de uma falha (ou ataque), viabilizar pesquisas, realizar testes ou analisar o ciberespaço (sistema simulado).

2.2.1 Network Simulator (NS3)

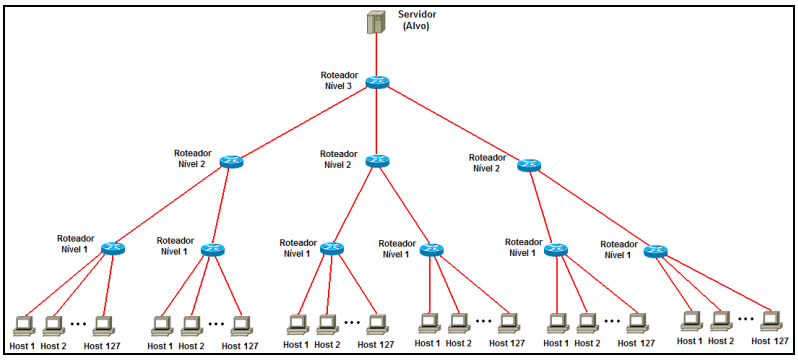
O Network Simulator (NS3)[14] é um sistema de simulação de eventos discretos para ambientes *unix-like* com foco, principalmente, em simulações de sistemas baseados na arquitetura Internet e voltado para pesquisa e educação. Quanto às atuais funcionalidades implementadas, o NS3 possui:

[12] http://delta3d.org/
[13] http://www.mak.com/products/simulate/vr-forces
[14] https://www.nsnam.org/

- Construção de redes virtuais e suporte a diversos itens de auxílio a simulações de redes;
- Suporte a emulação de rede, permitindo interação com redes reais;
- Simulação distribuída, possibilitando simulações de grande porte; e
- Suporte *a tracing, logs* e estatísticas de componentes da simulação.

Os alunos Luiz Júnior e Souza (2011), do Instituto Militar de Engenharia (IME), realizaram uma implementação de um ataque de negação de serviço (DoS - *Denial of Service*) no ambiente do NS3. Com o objetivo de simular um ataque DoS os alunos construíram uma topologia composta de três níveis de roteadores, no qual o servidor alvo estava ligado ao roteador de nível três. Os hosts atacantes estavam separados em seis sub redes nas quais cada uma continha 127 *hosts* (Figura 7).

Figura 7 - Topologia de ataque DDoS utilizando o NS3.



Fonte: Luiz Júnior e Souza (2011)

De acordo com os alunos, em cada sub rede, 40% dos *hosts* foram selecionados aleatoriamente para participarem do ataque. Além disso, as conexões (*host*-roteador nível 1) dentro de cada sub rede continuaram sendo distribuídas entre ADSL, Dial-Up e fibra ótica. As conexões entre os roteadores nível 1 e nível 2 foram de 100Mbps e entre os de nível 2 e nível 3 de 1Gbps, ambas de fibra ótica. A conexão entre o roteador nível 3 e o servidor alvo possuía largura de banda de 100Mbps, sendo também de fibra ótica. Além disso, as latências foram configuradas de acordo com o tipo de cada *link*. Com isso, os alunos procuraram reproduzir redes reais, inclusive com a implementação de trafego de fundo. A partir das configurações heterogêneas, realizaram ataques ao servidor com pacotes TCP, UDP e ICMP.

Com essa topologia, os alunos realizaram diversas simulações alterando parâmetros básicos como tempo de execução, distribuição dos endereços IP nos *hosts* e número de pacotes máximos enviados.

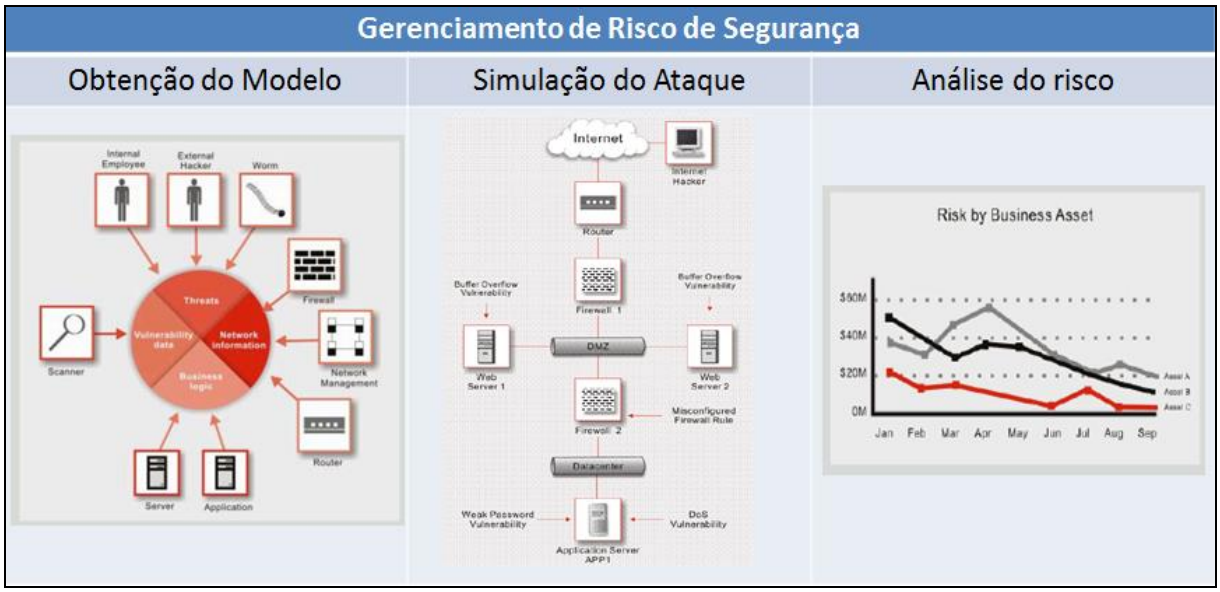
De acordo com as conclusões dos alunos, o uso de variáveis aleatórias para a criação de atributos não determinísticos (latência de enlaces, intervalo de resposta de aplicações, falhas de comunicação) tornam as simulações mais realísticas. No entanto, a conclusão apresentou uma limitação do NS3 no tocante a segurança, pois não prevê um *framework específico* para esta área.

2.2.2 Skybox

Um outro exemplo de simulador que pode ser citado nesta seção, é o Skybox. Por definição da própria empresa, o Skybox é uma plataforma automatizada de gestão de riscos que auxilia empresas de tecnologia da informação na busca e soluções (SKYBOX SECURITY, 2010).

De forma geral, o gerenciamento de risco é realizado em fases (Figura 8). Primeiro ocorre a obtenção de um modelo. Neste modelo existem as ameaças (funcionários, hackers, vírus, etc), informações sobre a rede de dados (*firewall*, roteador, gerenciamento da rede, etc), lógicas de negócio (requerimentos, serviços, etc.) e demais vulnerabilidades identificadas na rede. Depois, o Skybox realiza uma simulação de ataques e, por último, analisa os riscos, com base nos perigos identificados e nas regras de negócio (SKYBOX RISK CONTROL 2010, p. 9 – 11).

Figura 8 - Gerenciamento de Risco de Segurança Realizado pelo Skybox



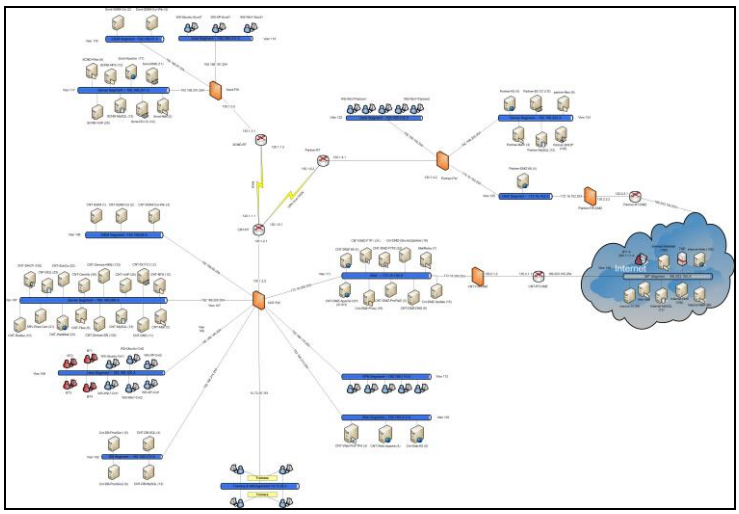
Fonte: Machado e Yano (2013)

Assim, o Skybox não se caracteriza simplesmente como um simulador, no entanto, em uma fase importante de sua análise, utiliza este recurso (simulação de ataque aos ativos vulneráveis) para identificar as vulnerabilidades que podem afetar a empresa sob análise e emite os relatórios e alertas de saída.

2.2.3 *CyberShield*

O *CyberShield*[15] é um simulador da empresa ELBIT SYSTEMS que consiste em uma aplicação baseada em virtualização VMware[16]. O coração do sistema é uma máquina virtual que realiza ataques de alta complexidade em uma rede corporativa, com 19 cenários distintos (Figura 9).

Figura 9 – Exemplo de Cenário do *CyberShield*



Fonte: Guide (2012)

Como funcionalidades especiais o sistema permite: a gravação em vídeo de todos os passos dos alunos, a utilização de marcos temporais para identificação de eventos de interesse, controle remoto dos computadores dos alunos, dentre outras funcionalidades.

O simulador possui os seguintes componentes principais: servidores; *storage*; gerador de tráfego; switches; 01 máquina gerente; máquinas do time azul (defesa); e máquinas do time vermelho (atacantes).

O sistema é controlado por uma máquina gerente através do programa TMS-Client, onde o gerente da simulação (professor / instrutor) deve selecionar os alunos que participarão do treinamento e deve inclui-los em uma turma de treinamento. Após escolher o cenário, o gerente da simulação deve selecionar, carregar a rede corporativa e iniciar os eventos de

[15] https://www.elbitsystems.com/elbitmain/area-in.asp?parent=455&num=456
[16] http://www.vmware.com/br

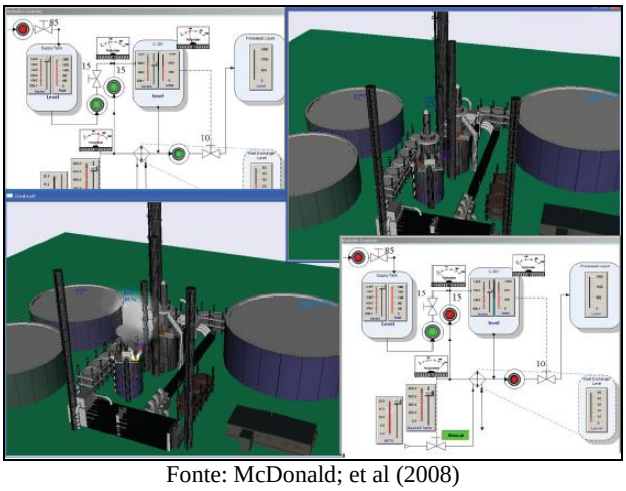
ataque. O instrutor pode acompanhar todo o treinamento através de uma linha de tempo, onde se pode lançar observações que serão úteis ao final do exercício. Os alunos devem acessar as máquinas físicas e conectar ao servidor via rede privada virtualizada (Virtual Private Network – VPN). Após acessar a rede do simulador os alunos devem utilizar as ferramentas de administração de rede e o manual da rede para identificar e sanar possíveis incidentes de segurança. Em todo momento do exercício o aluno pode acessar qualquer máquina da rede, na condição de gerente da mesma, para configurar serviços, ler registros de *log* e reparar serviços indisponíveis (GUIDE b, 2012).

2.2.4 *Virtual Control System Environments* (VCSE)

O VCSE é um modelo hibrido de simulação que atua na segurança cibernética de sistemas industriais (MCDONALD; et. al, 2008). Baseia-se no framework Umbra que foi desenvolvido para modelar sistemas de controle e tem sido usado para desenvolver e analisar uma grande variedade de sistemas automatizados, incluindo robótica, automação industrial, sistemas militares, e tecnologias de segurança. Segundo McDonald et. Al. (2008), o VCSE é uma ferramenta ideal para a modelagem de sistemas físicos e controle de interface com equipamentos reais e elementos do sistema SCADA[17].

Como exemplo de utilização do VCSE, a Figura 10 apresenta modelos de controle de uma refinaria antes de um ataque cibernético e, na parte inferior da mesma figura, os controles após o ataque.

Figura 10 - Ambiente VCSE de uma refinaria



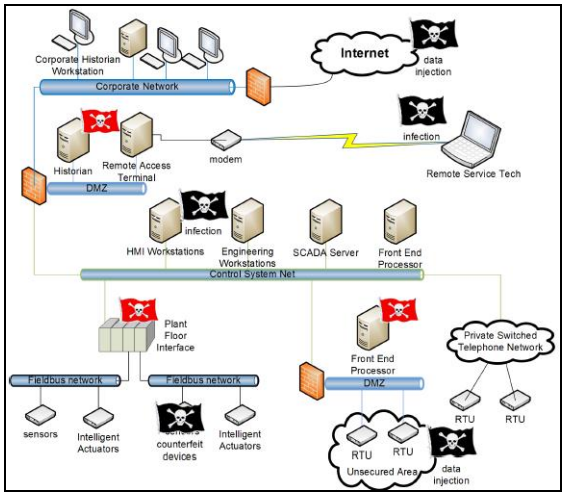
Fonte: McDonald; et al (2008)

[17] *Supervisory Control and Data Acquisition* (SCADA) é um sistemas de supervisão e aquisição de dados que utiliza *software* para monitorar e supervisionar dispositivos de sistemas de controle (POCKET GUIDE, 2003).

O simulador pode ser utilizado para representar controladores, interfaces de chão de fábrica, sensores, inteligentes, atuadores e unidades terminais remotas (UTRs) e outros componentes comuns em um sistema industrial (MCDONALD; et. al, 2008).

A Figura 11 apresenta, de forma esquemática, algumas ameaças em uma rede industrial típica analisada pelo VCSE. Neste caso, existe uma variedade de ameaças cibernéticas, identificadas por bandeiras pretas (ponto de injeção), que os adversários podem usar para entrar nessas redes. Uma vez injetado o ataque, essas ameaças podem mover-se para outros pontos (bandeiras vermelhas) para assumir o controle das funções da indústria. No exemplo abaixo, identificamos como um adversário poderia usar um *exploit*, do *Metasploit framework*[18], para injetar códigos em um alvo que estava usando o Microsoft Server 2000, sem atualização de segurança. A partir deste ponto, verificamos como um adversário poderia reconectar com o site de injeção e assumir completamente as funções da planta. Em outro experimento, foi demonstrado como um ataque específico (*man-in-the-middle*), baseado na ferramenta Ettercap[19], poderia ser usado para induzir estes mesmos operadores a acreditar que a fábrica estava funcionando normalmente.

Figura 11 - Ameaças em uma rede industrial



Fonte: McDonald et. al. (2008)

McDonald; et. al. (2008) salientam, que a comunidade de segurança tem de ampliar a utilização de abordagens de ambientes virtuais para projetar soluções para problemas cibernéticos de segurança em indústrias. Isto irá permitir que: organizações melhorem os seus sistemas de proteção e preparem-se para sobreviver a futuros ataques cibernéticos; formular políticas governamentais para determinar quais aspectos de proteção de segurança cibernética

[18] https://www.metasploit.com/
[19] https://ettercap.github.io/ettercap/

devem ser regulamentadas e padronizada; e para que desenvolvedores de tecnologia possam melhorar as tecnologias e padrões existentes.

2.3 Simuladores Cibernéticos de Emprego Militar

Ainda como exemplo de simuladores cibernéticos, mas agora focado ao treinamento de recursos humanos, principalmente de militares americanos, apresentamos os seguintes simuladores citados por Pastor (2010):

– CyberProtect, desenvolvido pelo Departamento de Defesa Americano. Foi criado para auxiliar o treinamento dos profissionais de segurança de rede e familiarizá-los com as novas terminologias dos sistemas de informação, concepções e políticas. Possibilita a realização de exercícios onde os usuários terão a oportunidade de configurar redes seguras e submete-las a ataques.

– *Military Academy Attack/Defense Network* (MAADNET), foi criado para auxiliar a formação dos cadetes da Academia Militar Norte Americana. O MAADNET é uma arquitetura cliente servidor que utiliza simuladores de eventos discretos. Os usuários iniciam suas atividades construindo uma rede específica de acordo com um cenário apresentado. A rede pode ser construída com diferentes ativos (switches, roteadores, estações de trabalho, pontos de acesso wireless, etc). Cada um destes, pode ter um ou vários tráfegos de rede associados. O ataque criado pode vir da Internet (fora da rede), de um usuário interno a rede ou de ambos os lados.

– *CyberOps: NetWarrior*, desenvolvido pela Agência de Defesa de Sistemas da Informação, do Departamento de Defesa Norte Americano. O CyberOps destaca-se pela interatividade que o simulador propicia e por sua capacidade gráfica. A ferramenta é um ambiente virtual em 3D, com equipamentos de rede realísticos. Neste simulador, os recursos financeiros são limitados e os alunos devem avaliar os custos no momento em que montam as redes. O equipamento permite, em uma mesma simulação, a formação de diversos “times” que podem ser atacantes, defensores ou juízes.

- *The cyber Defense Technology Experimental Research laboratory* (DETERlab*)*, foi desenvolvido pela Universidade de Utah e é utilizado como um laboratório nas aulas de segurança cibernética. Suporta experimentos complexos para propiciar pesquisas a respeito do planejamento, criação e interação de cenários. Algumas ferramentas incluem a geração de tráfego de rede, ataques, configuração de rede e coleta de dados.

– *CyberCIEGE*, do Centro de Estudos de Segurança de Sistemas de Informação e Pesquisas, da Universidade de Pós-graduação dos EUA. O simulador possui o objetivo de proteger o sistema de TI utilizando apropriadas medidas de segurança envolvendo procedimentos, segurança física e técnica. Inclui cenários desenvolvidos para criar novas situações e um vídeo-enciclopédia que educa os alunos durante os exercícios.

– *Real-Time Immersive Network Simulation Enviromment* (RINSE), é um simulador desenhado para realizar treinamento e exercício de segurança cibernética em tempo real. Consiste em cinco componentes: o simulador de rede iSSFNet; um gerenciador de banco-de-dados; um banco-de-dados, um servidor de banco-de-dados, e um cliente da rede. Os comandos do simulador incluem as ações de: ataque; defesa; diagnostico da rede; controle de dispositivos; e simulação de dados.

- *Reconfigurable Cyber-Exercise Laboratory (RCEL)*, é o resultado da Tese de Mestrado do aluno R. J. Guild, apresentada na Universidade de Pós-graduação Norte Americana, em 2004. O laboratório é composto por várias estações as quais são responsáveis por funções específicas, tais como: autenticação; controle de domínio; servidores de DNS, DHCP, FTP, syslog, e-mail, banco-de-dados, imagem de disco; certificação PKI; autoridades de registro; ponto de acesso sem fio; honeynet; vulnerabilidades de acesso; *switches*; roteadores; *firewall*; sistemas de detecção de intruso; e dispositivos com redes privadas.

Concluindo este capítulo 2 - Simulação, verificamos que a utilização de simuladores pode auxiliar na formação e preparação de recursos humanos para atuarem no ciberespaço. Mas, dentre os diversos tipos de simuladores existentes, qual podemos adotar para tratar da defesa cibernética no Brasil? Quais as características mais importantes que devemos procurar em um simulador de Defesa Cibernética?

3 Simulador de Operações de Guerra Cibernética (SIMOC)

Os simuladores cibernéticos apresentados na seção anterior foram projetados e construídos para atender a necessidades específicas de seus patrocinadores, desenvolvedores, grupos de trabalho, unidades militares e/ou países. Por estes motivos, apresentam características, funcionalidades e limitações específicas.

A Seção de Ensino de Cibernética do CIGE analisou grande parte dos simuladores apresentados e identificou muitas funcionalidades interessantes, no entanto existem outras características particulares da escola (CIGE) que não eram atendidas.

Como exemplo de requisito considerado importante pelo CIGE, podemos citar: necessidade de possuir o controle total do hardware e software, incluindo as linhas de código; capacidade de desenvolver os seus próprios cenários de simulação ou de modificar os já existentes, sem contudo necessitar integralmente do apoio dos desenvolvedores do simulador; falta de conformidade entre os produtos apresentados e as necessidades técnicas e comerciais; custo inicial e de sustentação dos simuladores apresentados (MACHADO; REGUEIRA; REZENDE, 2015).

Cabe acrescentar a esta discussão, a determinação da Estratégia Nacional de Defesa brasileira de desenvolver a Indústria Nacional de Defesa (BRASIL, 2008). Além do mais, cabe ressaltar a criticidade do assunto em pauta. A possibilidade de adquirir um simulador cibernético de outra nacionalidade, poderia impactar na segurança cibernética do país.

Desta forma, foi decidido pelo desenvolvimento nacional de um simulador cibernético que atendesse as necessidades do CIGE, na formação dos futuros combatentes cibernéticos.

Por definição da empresa, o SIMOC é:

> ... software que permite, através da virtualização das inúmeras possibilidades de montagens no mundo das redes de computadores, configurar ambientes simulados, destinados à ampliação da didática utilizada pelo Centro de Instrução de Guerra Eletrônica do Exército (CIGE) em instruções da capacitação e preparo operacional dos militares do Exército Brasileiro, voltadas para as atividades de segurança e defesa na área de Guerra Cibernética. (SIMOC, 2014b)

3.1 Desenvolvimento do SIMOC

Para a preparação de recursos humanos aptos a lidarem com as ameaças digitais, o Exército Brasileiro decidiu usar armas nacionais. De acordo com o Jornal Valor Econômico,

de 23 de Janeiro de 2012, a empresa do Rio de Janeiro, DECATRON[20], venceu a licitação de R$ 5,1 milhões para desenvolver um simulador de guerra cibernética. No mesmo artigo, o General Antonino Santos Guerra, comandante do Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx)[21], informa que o investimento faz parte das ações para reforçar as defesas e se preparar para contra-atacar as ameaças cibernéticas (BRIGATTO, 2012).

Do acordo com Carlos Rust, sócio-diretor da DECATRON, em reportagem intitulada: Brasil se prepara para possível guerra cibernética, acessada no site da UOL, Olhar Digital (RUST, 2012).

> O país está em posição de destaque no mundo e essa evidência pode ser bastante perigosa neste aspecto. Temos ativos e patrimônios para proteger. Se algum país quiser nos atacar não precisa soltar bombas, basta atacar nossa rede. (RUST, 2012)

Rust (2012), comenta que o simulador adquirido pelo Exército, e em fase de desenvolvimento, poderá criar diversos cenários, criar redes virtuais e fazer experiências de proteção e ataque. O software deverá gravar todas as ações dos alunos para que o instrutor analise o ataque ou defesa do aluno e faça as devidas observações.

> Existe um módulo de criação de cenários que permite dizer quantos roteadores, servidores ou impressoras tem aquele local e um outro módulo que elabora a missão a ser cumprida. (RUST, 2012)

Por intermédio do edital número 28 / 2011, a Base Administrativa do CComGEx explicitou os detalhes a respeito do SIMOC (BRASIL, 2011). Segundo o documento, o simulador possui fins didáticos para atender as necessidades de especialização dos recursos humanos. Devendo, para este fim, executar ações de proteção cibernética e defesa ativa. No anexo I, deste edital, encontramos o projeto básico para o desenvolvimento do simulador. Em uma descrição detalhada, o documento regula que o simulador deve:

- permitir o treinamento do tipo ação reação, onde atacantes e defensores se enfrentam, enquadrados em um cenário didático pré-estabelecido e que permita ajustes constantes por parte do instrutor;

- além de permitir a capacitação dos recursos humanos, deverá também permitir a identificação de vulnerabilidades em redes de computadores, por meio de virtualização de ambientes computacionais;

[20] http://www.decatron.com.br/
[21] http://www.ccomgex.eb.mil.br/

- ser capaz de implementar um ambiente estanque (sem conexões externas) para que os alunos possam praticar, de forma segura, todas as ações ofensivas e defensivas que estão aprendendo. No entanto, para surtir o efeito esperado, o ambiente deve se aproximar ao máximo da realidade, ou seja, de um espaço cibernético hostil;

- permitir a existência de um ou dois oponentes. Caso existam os dois, estes poderão realizar ataques ou defesas (simultaneamente). Caso contrário, o sistema deverá simular a presença de um dos adversários;

- emular o comportamento de uma rede de produção típica (roteadores, *switches*, *firewalls*, estações de trabalho, servidores, etc.), além de disponibilizar serviços de rede típicos (e-mail, servidor de páginas, servidor de arquivos, etc.) com os seus respectivos tráfegos de dados. Assim, as ações desencadeadas pelos alunos devem ter reflexo direto no funcionamento da rede e no comportamento do ambiente virtual;

- possuir uma interface de controle, composto de: painel de configuração, onde os cenários são manipulados; e de monitoramento, capaz de acompanhar o desenvolvimento da simulação (em tempo real); e

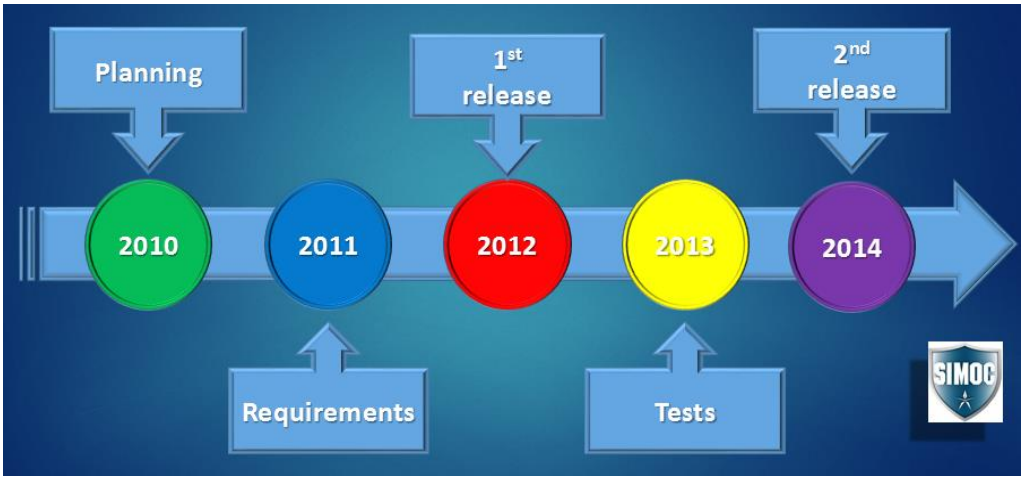
- possuir características de dinamismo e interatividade (determinados pelo instrutor).

3.2 Entregas do SIMOC

Para atender aos requisitos básicos apresentados sucintamente no item anterior, a empresa desenvolvedora optou em realizar um desenvolvimento de software utilizando uma metodologia ágil. Em consequência, o desenvolvimento foi acompanhado de uma série de testes e uma sequência de reuniões com os integrantes da seção de ensino de cibernética do CIGE.

O quadro de trabalho geral, pode ser resumido pela Figura 12. Os planejamentos e análise dos simuladores existentes no mercado (comentados na seção anterior – ***2.2 Simuladores Cibernéticos***) ocorreu no ano de 2010 e os requisitos foram identificados e publicados em 2011.

Figura 12 – Quadro de desenvolvimento do SIMOC

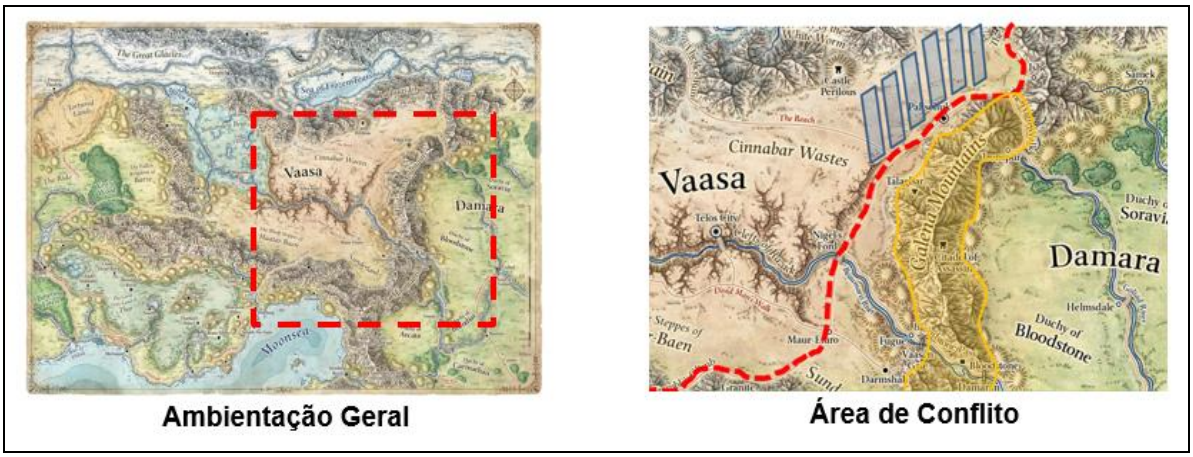


Fonte: o Autor

Como resultado do trabalho, foram realizadas duas grandes entregas, sendo a primeira em 2012 e a última, seguida de um ano de testes (2013), no final do ano de 2014 (Figura 12).

A primeira versão do simulador foi oficialmente utilizada no curso do CIGE no final de 2012. A simulação foi realizada para uma turma de 20 alunos, que receberam um conjunto de atividades, dentre elas, a realização de ações cibernéticas a uma infraestrutura crítica de um país fictício (Figura 13).

Figura 13 – Ambiente de Simulação



Fonte: o Autor

Foram definidas duas equipes (Alfa e Bravo) onde cada uma foi alocada em uma sala de treinamento. Em cada sala foi instalada uma máquina contendo uma maquete da usina que era alvo do treinamento. Essa máquina foi acoplada à rede virtual do SIMOC. Foi criado um treinamento no SIMOC para cada equipe, com objetivos, instruções, tarefa e métricas de avaliação.

Para viabilizar o exercício, foi elaborado pelos instrutores um projeto de rede contendo as configurações necessárias para que os alunos pudessem explorar vulnerabilidades aprendidas durante o curso, e também novos desafios. A rede criada possuía em torno de 45 elementos de rede, organizados de forma a se assemelhar à uma rede corporativa.

O treinamento durou 3 dias, sendo considerado satisfatório para as necessidades do CIGE. A infraestrutura inicial teve como objetivo viabilizar o uso experimental do simulador. No entanto, por ser a primeira experiência de uso em produção, alguns problemas foram identificados (MACHADO; REGUEIRA; REZENDE, 2015):

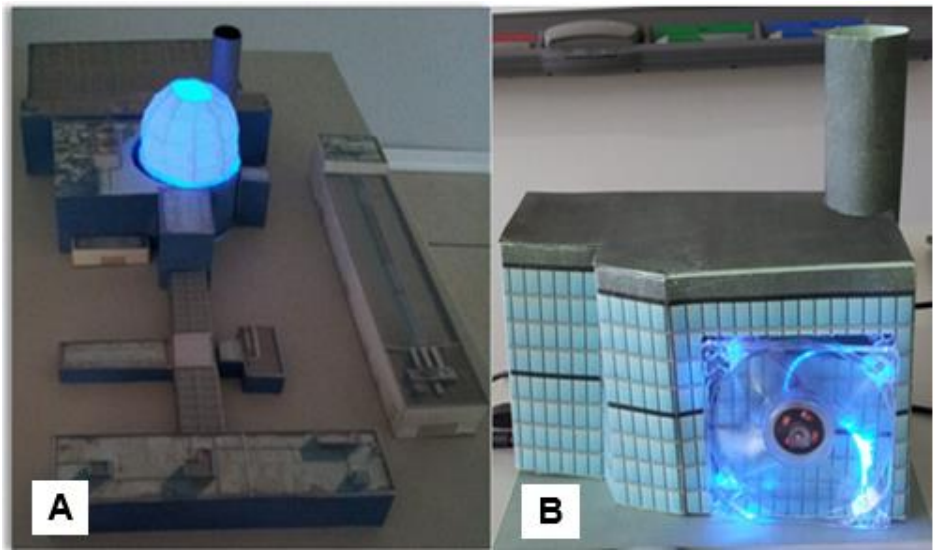
1. Servidor de aplicação do simulador indisponível por alguns instantes (menos de 3 minutos):
    - Infraestrutura inicial muito requisitada pela rede virtual dos alunos, fazendo com que os recursos disponíveis para o servidor de aplicação do simulador ficassem escassos;
    - A solução adotada pelo analista técnico foi limitar os recursos destinados à máquina virtual do servidor (necessidade de reinicialização da máquina virtual);
    - Apesar da situação ocorrida, o treinamento seguiu normalmente e os alunos não foram prejudicados, pois os mesmos estavam trabalhando em suas redes virtualizadas;

2. O Link dos alunos, às suas respectivas máquinas, ficou lento em alguns momentos do treinamento:
    - Infraestrutura inicial muito requisitada pela rede virtual dos alunos, fazendo com que os recursos disponíveis para o *Vsphere Web Client* (componente do *VCenter*[22] responsável pelo acesso dos alunos) ficassem escassos.
    - Por não ser uma situação impeditiva, o treinamento continuou sendo realizado.

Essa mesma versão do simulador foi utilizada no exercício de 2013. Nesta ocasião, foi criado um treinamento no SIMOC para cada equipe a partir do exercício do ano anterior. Os dados gerais do treinamento também se mantiveram. O sistema foi configurado para que fossem acopladas duas máquinas físicas à rede virtual do treinamento, como no ano anterior, para possibilitar o uso de uma maquete, montada pelos instrutores do curso, representando uma usina termelétrica (Figura 14-A).

[22] http://www.vmware.com/br/products/vcenter-server

Figura 14 - **Maquete da Usina**



Fonte: o Autor

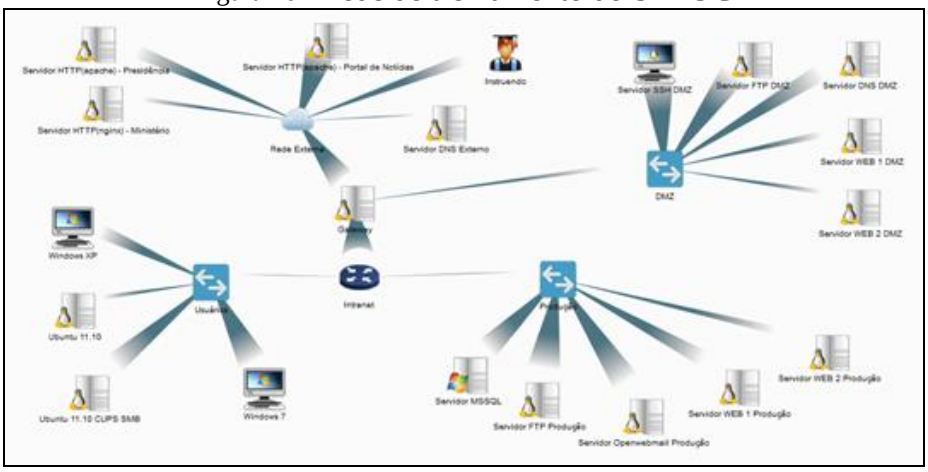
Por meio de uma ação de guerra cibernética, os alunos deveriam controlar e neutralizar as turbinas das usinas termelétricas (Figura 14-B). Para isso, o planejamento da ação cibernética continha os seguintes passos: reconhecimento (*reconnaissance)* em páginas de redes sociais (Figura 15-A); varredura (*scanning)*, utilizando ferramentas estudadas no curso (Figura 15-B); explorar (*exploit)* o sistema de controle (Figura 15-C); criar um *backdoor*; e cobrir os rastros do ataque.

Figura 15 – Passos do Ataque

Fonte: o Autor

Com o intuito de simular um ambiente real, a rede corporativa foi configurada com uma faixa de endereços totalmente diferente, possuindo quatro segmentos: a rede DMZ, rede de produção, rede de clientes e uma rede secreta. Inicialmente os alunos teriam acesso ao servidor FTP, tendo obtido as credenciais em fases anteriores do treinamento ministrado fora do SIMOC. A Figura 16 apresenta um esboço da rede elaborada para o treinamento.

Figura 16 - Rede de treinamento do SIMOC



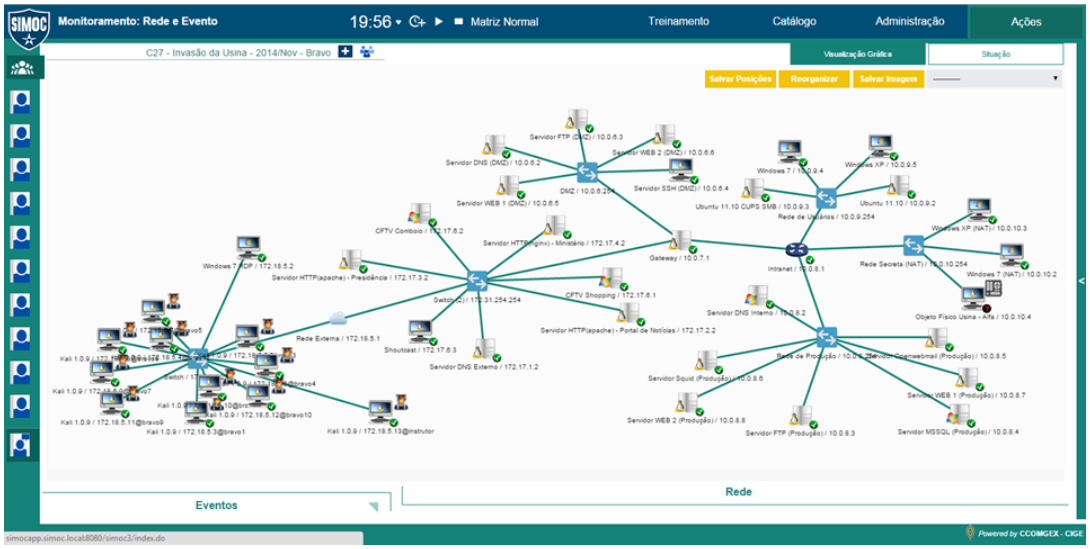
Fonte: o autor

É importante ressaltar que os problemas detectados no primeiro treinamento (2013) não se repetiram durante o segundo treinamento, agora com a infraestrutura de hardware mais adequada ao simulador.

O próximo treinamento monitorado foi realizado em 2014, já na segunda versão do simulador. Algumas questões favoreceram este exercício. Em primeiro lugar, a maior familiaridade da equipe de instrutores com as potencialidades do simulador e suas funcionalidades. Em segundo, a experiência adquirida desde a primeira fase do simulador, seja dos instrutores, e também da equipe de desenvolvimento.

O exercício foi uma evolução do cenário da usina, já apresentado no curso de anos anteriores. Fazendo uso dos novos recursos do simulador, os instrutores evoluíram o projeto da rede, e também as atividades que deveriam ser realizadas pelos alunos. A Figura 17 mostra o esboço da rede virtualizada, sobre a qual os alunos realizaram as suas atividades.

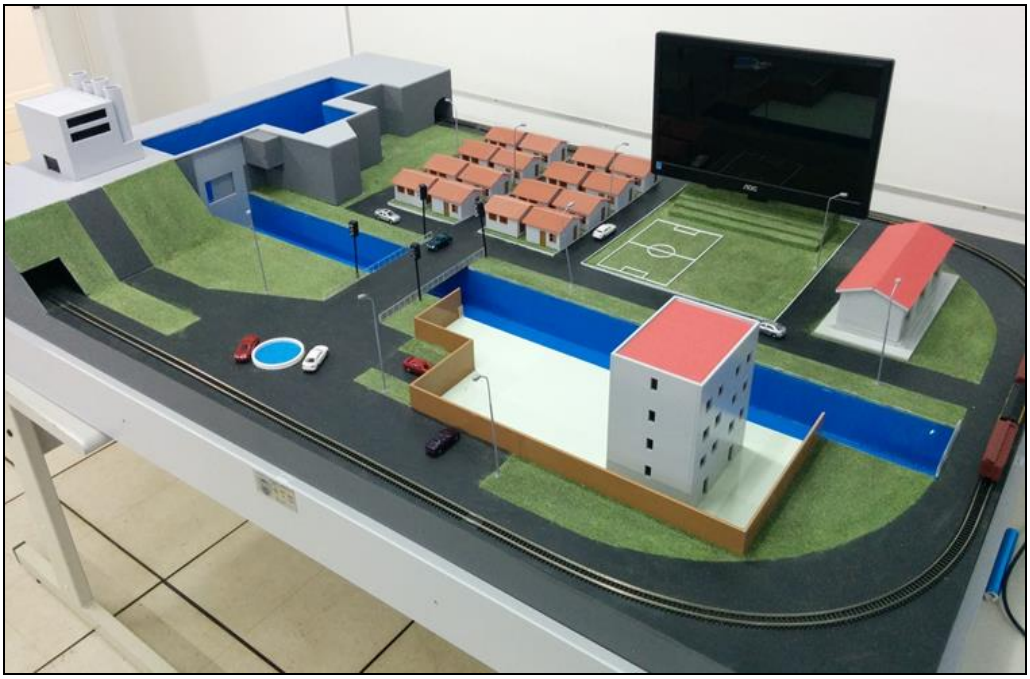
Figura 17 - Esboço da rede virtualizada



Fonte: o Autor

A maquete do treinamento também evoluiu para uma cidade (e não mais apenas uma usina), permitindo aos alunos uma maior interação com o cenário, podendo interferir na rede de iluminação, nas comportas da represa, na linha de trem, no placar do campo de futebol, dentre outras atividades. Utilizando a funcionalidade do simulador de integração com objetos reais, a equipe do CIGE integrou a rede virtual criada no SIMOC com a referida maquete (Figura 18).

Figura 18 – Maqueta da Cidade



Fonte: o Autor

No modelo utilizado, estavam presentes algumas infraestruturas críticas que poderiam ser comprometidas por meio de ações cibernéticas. Foram utilizados protocolos similares ao SCADA para controlar instalações como: usina hidrelétrica, sistema de controle de tráfego, comportas da usina, placar do estádio de futebol, etc. A utilização da maquete se mostrou proveitosa, uma vez que o aluno do curso pode identificar os efeitos de suas ações cibernéticas no campo cinético.

3.3 Aspectos técnicos

Para realizar as simulações comentadas anteriormente, o SIMOC possui alguns aspectos técnicos que passaremos a comentar neste subcapítulo.

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. Neste caso, todos os elementos usados na criação da rede são modulares, possibilitando a reutilização e facilitando a expansão do conteúdo disponível.

Neste 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 através 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. Estes alunos, podem possuir redes individualizadas (uma rede por aluno) ou podem estar todos conectados em uma mesma rede.

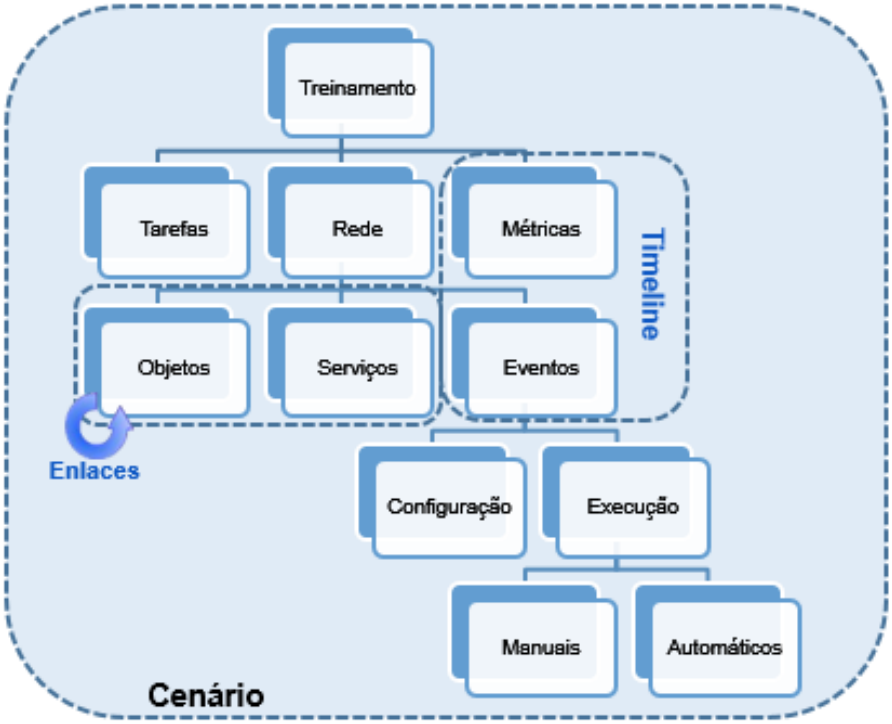
O projeto foi desenvolvido em Java para Web Server, utilizando o VMware como plataforma de virtualização de máquinas e redes. Para dar dinamismo ao treinamento, foi desenvolvido o conceito do Motor de Simulação, que é a parte do código responsável pela execução de scripts no decorrer dos treinamentos.

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).

Como terminologia e conceitos básicos utilizados pelo SIMOC, destacamos: Treinamentos, Tarefas, Rede, Métricas, Objetos, Serviços, Eventos, Configuração, Execução, Manuais e Automáticos.

Estes conceitos podem ser relacionados de forma hierárquica conforme a Figura 19.

Figura 19 – terminologias e conceitos



Fonte: Gomes (2014)

O Treinamento é a simulação do exercício que envolve todos os outros conceitos. Abaixo do treinamento possuímos as Tarefas, que são as atividades que os alunos deverão executar, ou que a simulação deverá executar. As Métricas, que são as diversas formas de medir o desempenho do Treinamento dos alunos.

A Rede é peça chave da simulação e possui, subordinado a ela: os Objetos, os Serviços, e os Eventos. Os Objetos são todos os ativos de rede que podem existir na simulação. Os Objetos podem ser agrupados em Classes e se interligam por meio de Enlaces. Os Serviços são todos os serviços (DNS, FTP, mensagens, etc.) de rede que podem existir no Treinamento. E, por fim, os Eventos que são todos os eventos (fluxos de mensagens, ataques, atrasos na rede, perturbações, etc.) previstos em uma matriz que podem ocorrer na Rede. Esta matriz de eventos será utilizada pelo instrutor para descrever as condições necessárias para que eventos sejam disparados. Com isso, algumas condições iniciais da simulação são preparadas com base no comportamento esperado da rede e dos instruendos.

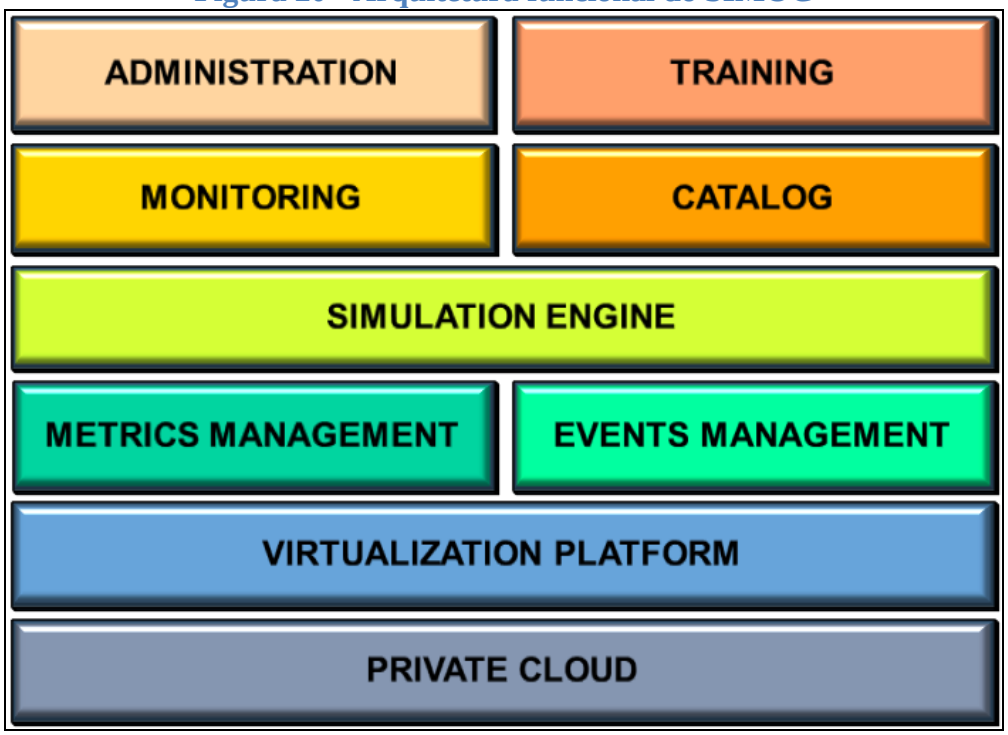
Os Eventos ainda podem ser relacionados com a Configuração (configuração do evento) e Execução, que pode ser de forma Manual (ação do instrutor) ou Automática (execução automática do evento na rede de treinamento). (SIMOC, 2014b)

Por último, englobando todos os conceitos vistos na Figura 19, temos o Cenário. O Cenário pode ser comparado, de forma ilustrativa, a um cartucho ou jogo de vídeo game.

Dependendo do Cenário escolhido pelo instrutor, os alunos receberão um Treinamento diferente, o que impacta em uma simulação diferente, com Tarefas, Redes, Métricas e todos os demais conceitos vistos, diferentes.

A Figura 20 apresenta a arquitetura funcional resumida do SIMOC.

Figura 20 - Arquitetura funcional do SIMOC



Fonte: Gomes (2014)

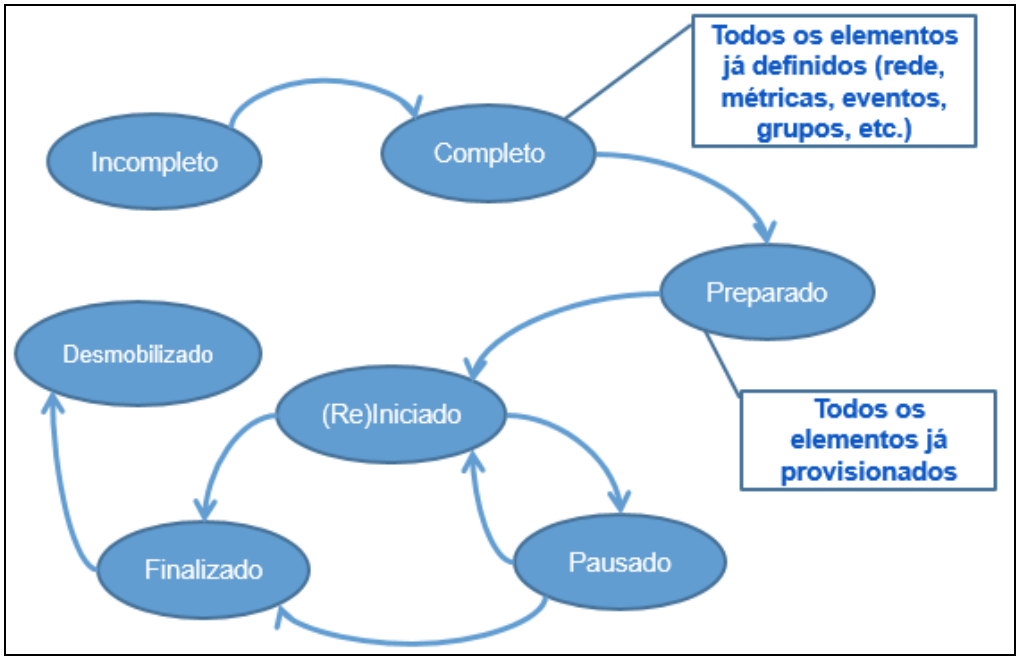
A arquitetura funcional do SIMOC possui 9 módulos:

- *Private Cloud*: módulo responsável pela administração e controle das redes virtuais criadas para cada treinamento;
- *Virtualization Platform*: plataforma responsável por intermediar a comunicação entre o Motor de Simulação e as redes virtuais. As operações básicas desta plataforma são: criar objetos, executar eventos (scripts) em um objeto e realizar métricas em objetos;
- *Events Management*: módulo responsável por gerir a configuração de eventos das redes e treinamentos executados.
- *Metrics Management*: módulo responsável por gerenciar as métricas que irão ser usadas durante o treinamento;

- *Engine Simulation*: motor de simulação responsável por prover dinamismo ao treinamento e interagir com as redes durante a execução do treinamento;
- *Catalog*: módulo responsável por gerenciar o catálogo de características do sistema. Os principais catálogos são: objetos, redes, eventos e métricas. Todos os elementos podem ser configurados pelo instrutor e podem ser utilizados para futuros treinamentos;
- *Monitoring*: módulo responsável por prover o monitoramento dos treinamentos. Por intermédio deste módulo, o instrutor pode monitorar a execução da simulação em tempo real, assim como pode gerar relatórios junto com o exercício;
- *Training*: Módulo responsável pela gestão do treinamento; e
- *Administration*: módulo responsável pela administração do sistema, usuários e classes.

O SIMOC pode possuir estados do Treinamento diferentes (Figura 21)

Figura 21 – Estados do Treinamento



Fonte: Gomes (2014)

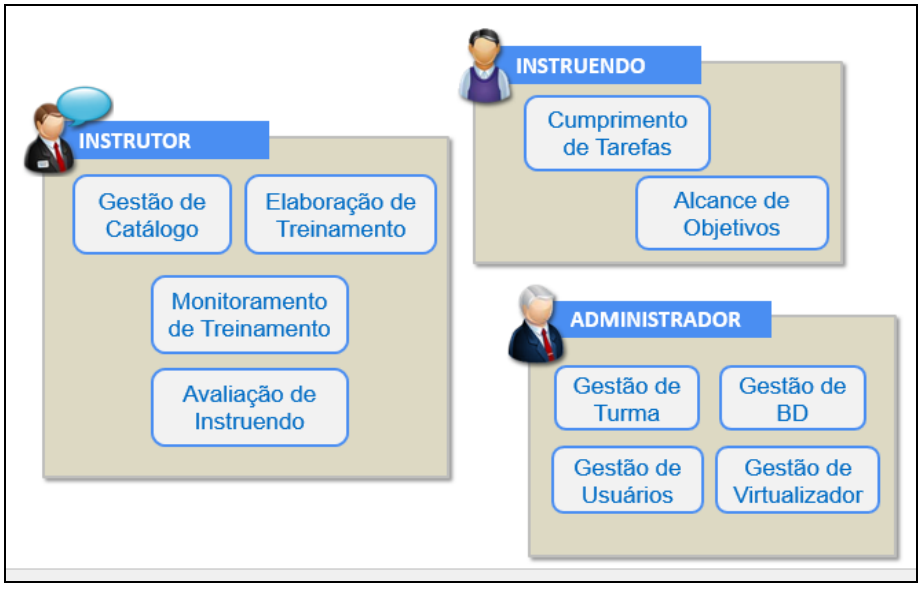
O Treinamento pode estar Incompleto, ou seja, já foi cadastrado alguns elementos da simulação, mas ainda não está terminado. O estado Completo ocorre justamente quando todos

os elementos (Rede, métricas, etc) já estão definidos para o Treinamento. O estado Preparado é alcançado quando todos os elementos estão provisionados para a simulação. Após esta fase o Treinamentos pode ser Iniciado ou Reiniciado, pois o Treinamento pode ser pausado (entra no estado de Pausado) pelo instrutor, a qualquer momento do Treinamento, para realizar algum ajuste, orientação, etc.

Na sequência, o Treinamento pode ser Finalizado, quando os alunos alcançarem seus objetivos no Treinamento, ou quando o tempo (de acordo com as Métricas discriminadas) acabar. E por último, o Treinamento alcança o estado de Desmobilizado, quando os elementos da simulação deixam de ser definidos para o Treinamento em questão.

Quanto aos perfis e papéis existentes, o SIMOC possui: o Instrutor, Instruendo e o Administrador (Figura 22).

Figura 22 – Perfis e papéis no SIMOC



Fonte: Gomes (2014)

O Instrutor possui a responsabilidades de configurar novas simulações e/ou utilizar as configurações já existentes para aplicá-las em suas simulações, iniciar objetos virtualizados; elaborar o treinamento; cadastrar o manual de apoio; criar o cenário, contendo táticas de ataque e defesas comuns de mercado (previamente cadastrada); aditar cenário (alterar, apagar, consultar); acompanhar a simulação, pelo painel de monitoramento; editar objetos (consultar, remover, configurar); gerir eventos e serviços de rede; configurar métricas; gerir usuário (criar, modificar, consultar, remover); gerar relatórios e logs do sistema; e lançar

as notas para cada participante, de acordo com a análise das métricas e repostas dos Instruendos. (SIMOC, 2014b)

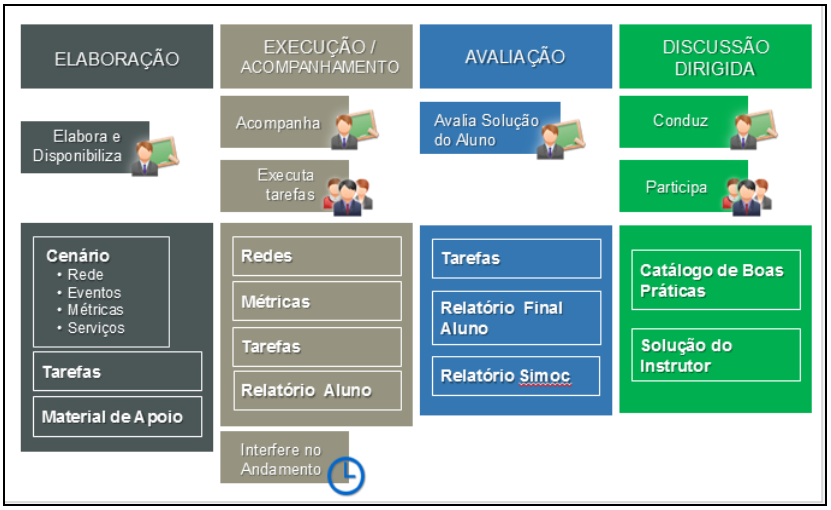
Por sua vez, o Instruendo deve cumprir as tarefas passadas pelo instrutor e tentar alcançar os objetivos traçados, dentro das Métricas formuladas pelo instrutor.

> É aquele que, diante de um determinado cenário disponibilizado pelo Instrutor, deverá realizar as tarefas que normalmente seriam encontradas em um contexto cibernético hostil, tanto em operações defensivas quanto ofensivas, apoiando-se em seu conhecimento prévio e no manual de apoio que o Instrutor disponibilizar. (SIMOC, 2014b)

Por fim, o Administrador possui o perfil de gerenciamento e controle do sistema, podendo criar novos usuários, administrar a utilização do VMWare, bem como acessar todas as funcionalidades do Instrutor, realizando configurações e monitoramento dos treinamentos (SIMOC, 2014b). Possui as seguintes responsabilidades: realizar a gestão de turma (criar, modificar, encerrar uma turma), fazer a gestão do banco de dados do SIMOC, realizar a gestão de usuários (incluir, excluir, modificar), e realizar a gestão de virtualizados.

Como resumo de uma dinâmica geral de um exercício, apresentamos a seguinte imagem (Figura 23).

Figura 23 – Dinâmica Geral de um exercício



Fonte: SIMOC (2014)

A fase da Elaboração é realizada pelo Instrutor. Inicia pela elaboração do exercício (montagem dos cenários, tarefas e material de apoio) e termina com a disponibilização do exercício para os instruendos.

A fase seguinte da Figura 23 (execução / acompanhamento) é realizada pelo instrutor e pelos instruendos. O instrutor acompanha e exercício e os instruendos devem executar as tarefas e preencher os relatórios (registrar detalhadamente os passos realizados durante o treinamento e as possíveis dúvidas existentes). Ainda nesta fase, o instrutor pode realizar interferências no exercício (pausar, retroceder, modificar o material de apoio, modificar o nível de dificuldade do exercício, etc) com o objetivo de melhorar o aprendizado dos instruendos.

A fase da avaliação é realizada pelo instrutor e precede a fase da discussão dirigida. Nesta última fase da Figura 23, o instrutor apresenta a solução padrão das tarefas feitas no exercício, pode citar as boas práticas constantes do catálogo e comenta a atuação dos alunos. Caso alguma solução diferente seja apresentada por um instruendo, esta poderá ser adicionada ao catálogo de soluções possíveis do SIMOC para aquele exercício em particular.

Quanto à manutenção do simulador, existem funcionalidades que permitem realizar a atualização do software de simulação, inserir novos itens nos respectivos bancos de dados, realizar uma reversão completa do sistema para estado no qual o mesmo saiu da fábrica e permitir, ou não, a manutenção remota por parte dos desenvolvedores do software.

Concluindo este subcapítulo, disponibilizamos em anexo algumas especificações técnicas do SIMOC presentes no edital número 28 / 2011, da Base Administrativa do CComGEx.

3.4 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; REGUEIRA; REZENDE, 2015):

1) Criar cenários similares aos da organização em que o simulador se presta;
2) 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 em estudo;
3) Possibilidade de reusar elementos (objetos, eventos, métricas, etc) pré-registrados no catálogo do simulador com o objetivo de adequar a uma nova situação problema ou de criar uma nova;

4) Importar máquinas virtuais para o catálogo do simulador;
5) Criar redes mistas, contendo segmentos virtuais e segmentos de rede reais;
6) Variedade de funcionalidades que apoiam o instrutor durante as simulações (exercícios). Como por exemplo: gerador de tráfego randômico, defesa automatizada, ataque automatizado, recurso de gravação, material de apoio, e aplicação das diversas métricas existentes;
7) Monitoramento em tempo real com a possibilidade de interferência do instrutor durante a execução dos exercícios. Como exemplo, o instrutor pode: pausar a simulação (exercício), adiantar, repetir uma situação, mudar parte do cenário e modificar o nível de dificuldade do exercício;
8) A implementação do simulador conta com uma relativa segurança na sua infraestrutura, seja para o acesso interno (administrador, instrutor, alunos) ou para acessos externos;
9) A utilização de maquetes, conectadas ao simulador, propicia ao instruendo a possibilidade de identificar a consequência "real" de um ataque cibernético, realizado pelo instruendo, sobre a infraestrutura de uma localidade (fábrica, cidade, etc).

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

1) Inviabilidade de simular ligações de fibra ótica. No entanto, esta 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, como 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 este 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 esta 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 neste caso os APTs não executam seus códigos maliciosos;
5) Atualmente não é possível conectar no SIMOC as máquinas pessoais dos instruendos para realizar os exercícios. Este fato acaba-se torando um óbice, pois é comum que estes instruendos já possuam, em suas máquinas, suas ferramentas instaladas e customizadas para as atividades no ciberespaço.

Além destas limitações, o SIMOC ainda possui algumas necessidades que precisam ser atendidas, como 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; REGUEIRA; REZENDE, 2015).

4 Resolução de cenário

Com o intuito de exemplificar a utilização do SIMOC e disponibilizar mais algumas informações técnicas sobre o simulador, passaremos a resolver um cenário específico pré-existente no catálogo de cenários.

O catálogo do SIMOC possui 43 cenários prontos que podem ser utilizados nas mais diferentes simulações. Os primeiros cenários são menores (poucos ativos de rede), simples e de resolução imediata (poucas operações). Na sequência, temos cenários mais completos, com grandes redes, muitos eventos e que exigem maior atenção e trabalho dos alunos. Cabe ressaltar, que o simulador possui cenários para participantes individuais, equipes e exercícios de "dupla ação". Ou seja, dois "times" adversários realizando ações de ataque e defesa cibernética.

Dentre os cenários existentes, iremos resolver o cenário 3A. A letra "A" que aparece após o número do cenário indica apenas a existência de outros cenários similares, com apenas pequenas modificações, o que pode tornar a simulação um pouco mais complexa.

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).

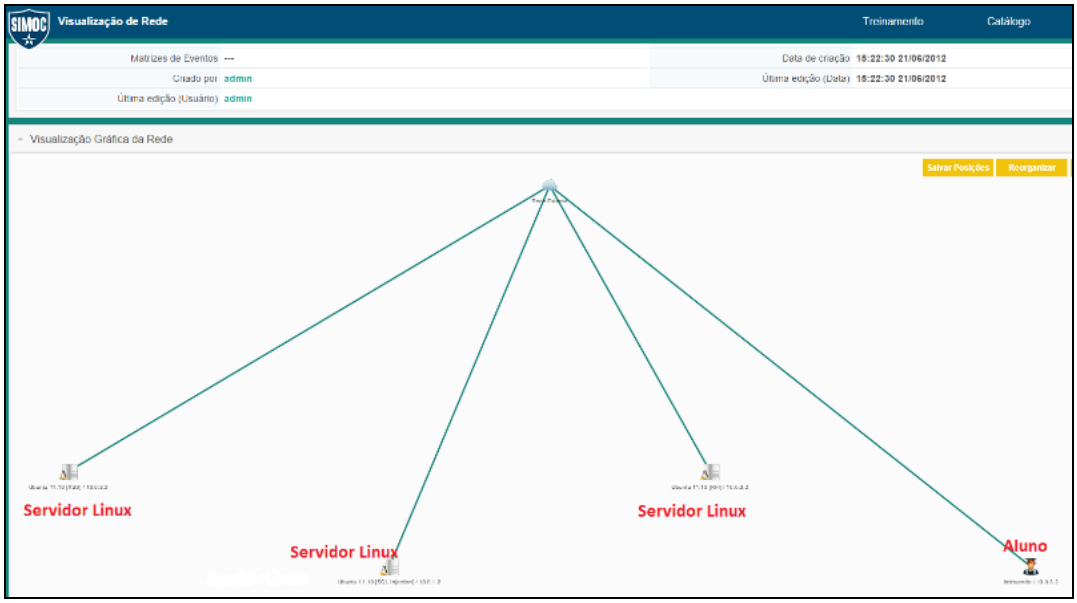
De forma resumida, a vulnerabilidade XSS ocorre pela falha de segurança de uma página web possibilitando a inserção e processamento de dados realizadas por pessoa não autorizada (atacante). Estes, utilizam JavaSrcipt, VBScript, ActiveX, HTML ou Flash para esconder os códigos maliciosos que são injetados nos sistemas dos usuários. O usuário confia nestas aplicações e o atacante aproveita esta situação de confiança para realizar ações que, em situações normais, não seriam permitidas. Neste caso o atacante poderá roubar cookies de sessão, redirecionar usuário para outro site, roubar dados pessoais, dentre outras fraudes e roubos (CEH, 2014).

O *SQL Injection* é um tipo de ameaça de segurança que aproveita falhas em páginas Web (não validação de entrada de dados em formulários Web) que interagem com bases de dados via *Structured Query Language* (SQL). O ataque ocorre quando o atacante consegue injetar uma série de comandos SQL maliciosos através da manipulação das entradas de dados de uma aplicação Web, realizando pesquisas não autorizadas em bancos de dados. A injeção dos comandos SQL pode expor dados reservados, sobrescrever ou ainda executar comandos no servidor atacado (CEH, 2014).

Por fim, o RFI é um tipo de ataque em que o hacker inclui remotamente arquivos maliciosos nas páginas Web vulneráveis (sem controle de acesso). Como consequência, o usuário irá receber arquivos disponibilizados pelo atacante, o que pode resultar nos mais diversos problemas de segurança.

Retornando ao Cenário 3A, a rede da simulação possuirá 3 servidores Linux, na função de servidores Web. Cada um com vulnerabilidades específicas (XSS, SQL e RFI) que deverão ser exploradas pelo instruendo que se encontra na mesma rede de simulação dos servidores (Figura 24 e Figura 25).

Figura 24 - Rede do Cenário 3A (captura de tela do instrutor)



Fonte: o Autor

Figura 25 - Lista de objetos (captura de tela do instrutor)

Lista de Objetos

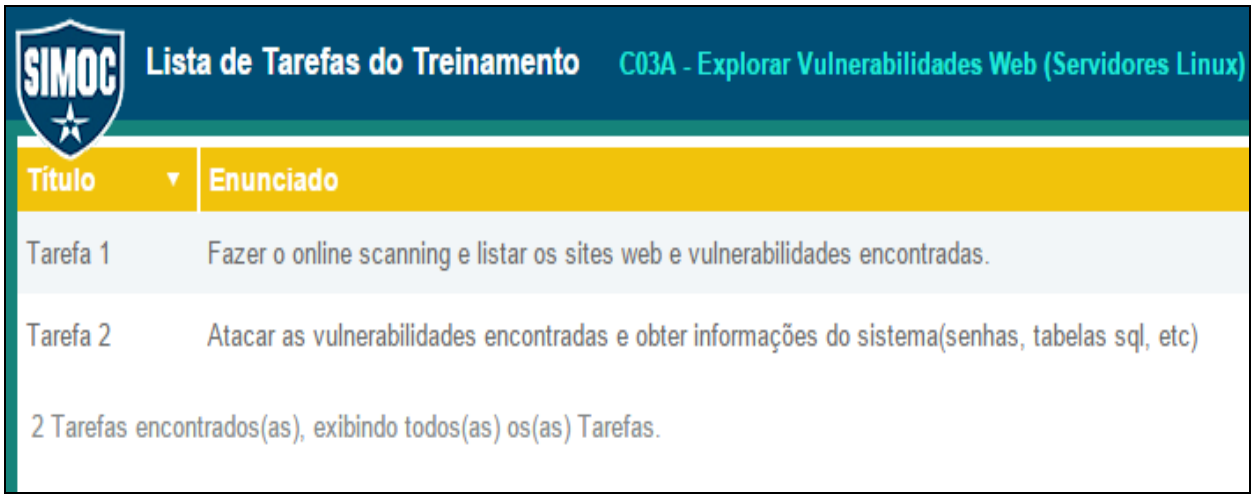
Nome	IP	Objeto Template	HD (GB)	RAM (GB)	Classificação
Instruendo	10.0.3.2	Instruendo	0.0	0.0	USUARIO
Rede Externa	---	Rede Externa	4.63	0.5	REDE
Ubuntu 11.10 [RFI]	10.0.0.2	Ubuntu 11.10 [RFI]	33.23	1.0	SO
Ubuntu 11.10 [SQL Injection]	10.0.1.2	Ubuntu 11.10 [SQL Injection]	33.56	1.0	SO
Ubuntu 11.10 [XSS]	10.0.2.2	Ubuntu 11.10 [XSS]	33.57	1.0	SO

Fonte: o Autor

Como atividade, o instruendo deverá:

✓ Executar, de forma online, 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.

Figura 26 - Atividades do Cenário 3A (captura de tela do Instruendo)



Fonte: o Autor

Como métricas de controle e de acompanhamento, o cenário possui:
✓ Tempo em que o aluno levou para listar as vulnerabilidades; e
✓ Tempo em que o aluno necessitou para descobrir as informações do website, tais como: senhas, tabelas SQL, consultas SQL, etc.

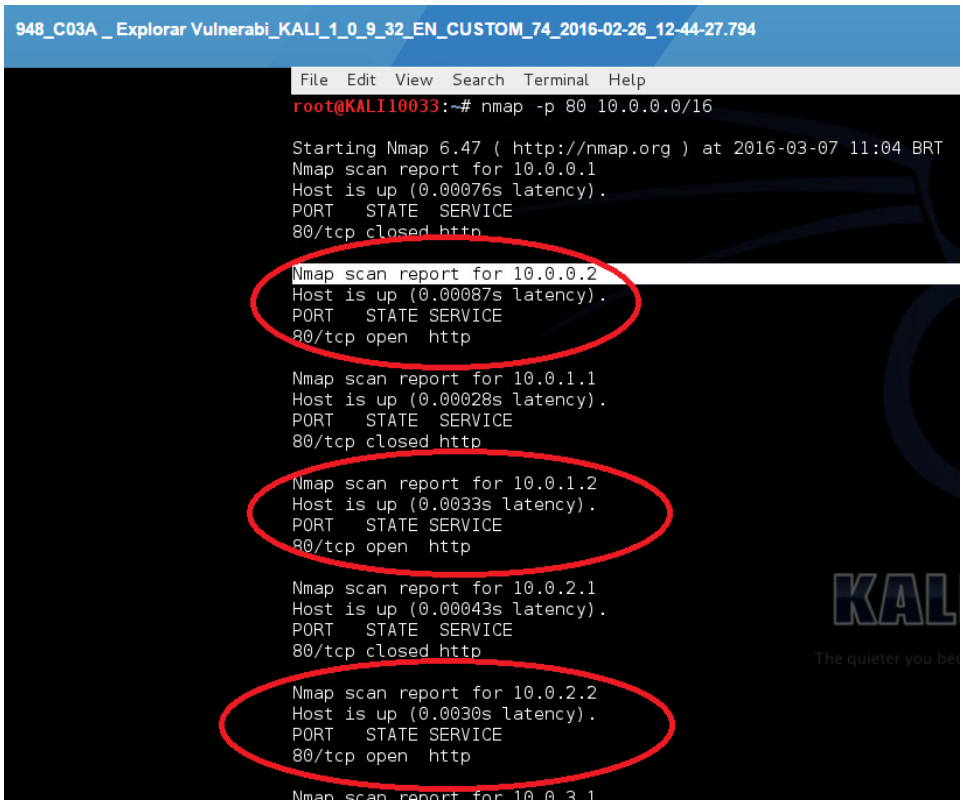
4.2 Roteiro de Resolução do Cenário 3A

Para realizar a primeira atividade (*scanning* de rede) o instruendo poderá realizar o comando "NMAP" para tentar identificar os IPs dos servidores que estão ativos na rede do instruendo. O comando completo pode ser (SIMOC, 2014c):

nmap –p 80 10.0.0.0/16

Com este comando iremos varrer todo a sub-rede 10.0.0/16 a procura de portas 80 abertas. Como resultado do comando, obtemos a seguinte tela (Figura 27):

Figura 27 - Comando nmap (captura de tela do instruendo)



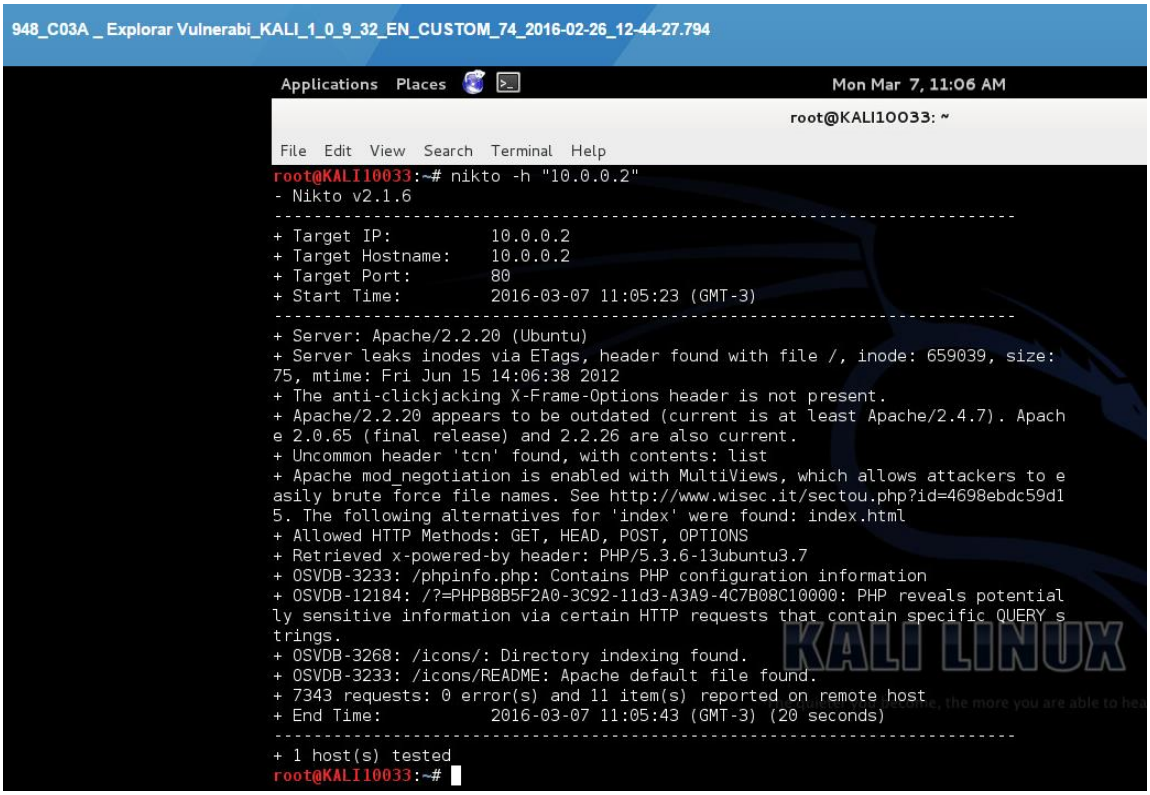
Fonte: o Autor

Nesta tela de relatório do nmap (Figura 27) 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, tentaremos identificar as vulnerabilidades para cada servidor. Para isso, podemos utilizar as diversas ferramentas disponibilizadas na simulação (Nessus, Nikto, OWASP, DirBuster). Por exemplo, utilizando “nikto” o instruendo deverá escolher um IP e executar o comando de varredura.

Figura 28 - **Scanning IP 10.0.0.2 (captura de tela do instruendo)**



Fonte: o Autor

Do resultado obtido com o scanning no IP 10.0.0.2 (Figura 28), podemos identificar as seguintes vulnerabilidades:

- o servidor é um Apache, versão 2.2.20 (sem atualização);

- Anti-clickjacking[23] não presente (vulnerabilidade)

- MultiViews[24] habilitado (vulnerável a ataques de força bruta);

- *Headers* incomuns encontrados (possível problema);

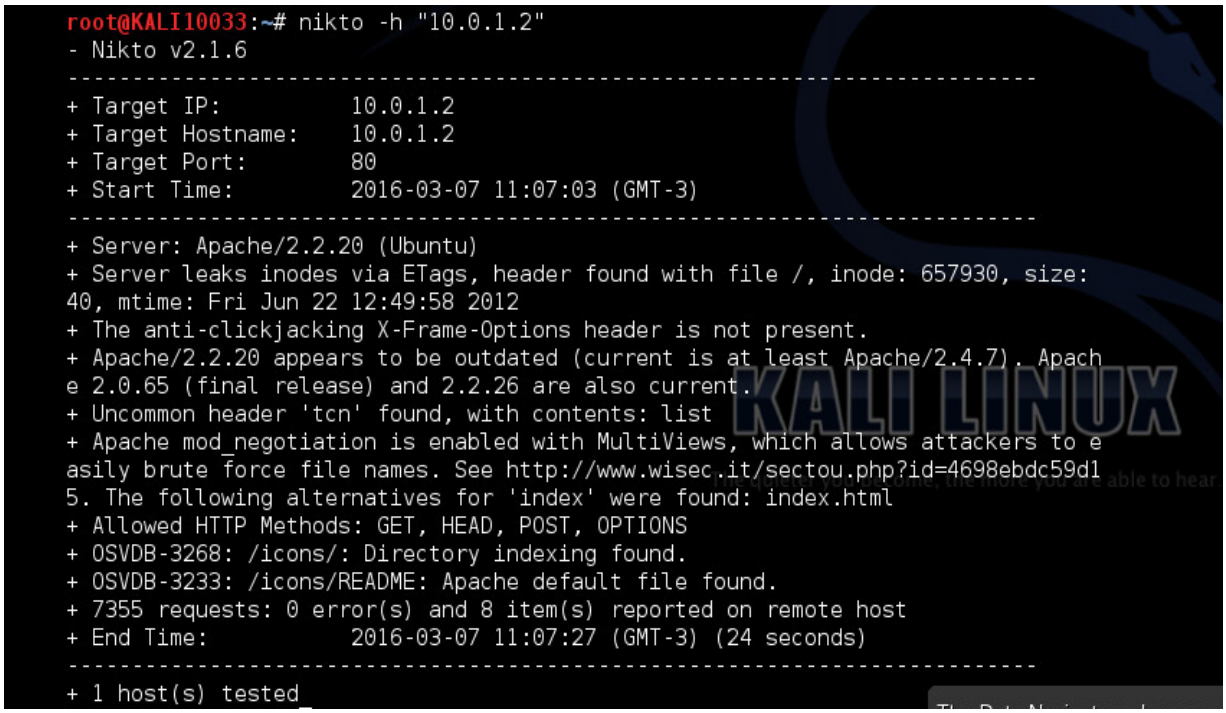
- possibilidade de obter, via consulta HTTP, informações sensíveis sobre o servidor;

- OSVDB[25] 3268[26]: vulnerabilidade registrada em que o servidor não verifica de forma adequada a autoria de arquivos, o que possibilita que os usuários abram arquivos de fontes desconhecidas. Por este motivo este servidor pode ser vulnerável ao RFI.

Repetindo o procedimento para o IP 10.0.1.2, temos:

[23] Clickjacking ("furto de *click*") é uma técnica fraudulenta. O roubo de click é uma armadilha preparada para que o usuário pense que está fazendo uma ação em um determinado site, mas na verdade os cliques executados nessa ação estejam sendo usados pelo atacante, para executar operações maliciosas.
[24] Multiviews é uma opção da diretiva Options do Apache utilizada para habilitar/desabilitar acesso aos arquivos sem informar a sua extensão.
[25] https://blog.osvdb.org/
[26] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3268

Figura 29 - Scanning IP 10.0.1.2 (captura de tela do instruendo)



Fonte: o Autor

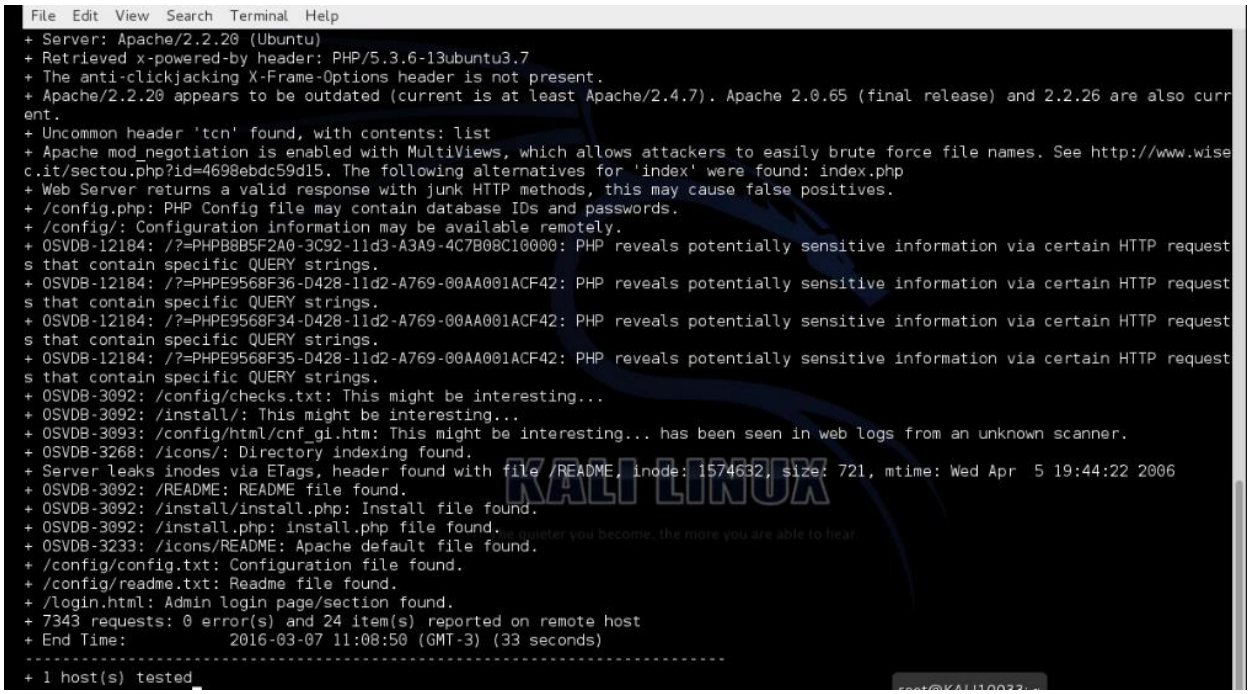
Do resultado obtido com o scanning no IP 10.0.1.2 (Figura 29), podemos identificar as seguintes informações / vulnerabilidades:

- Servidor Apache 2.2.20 – Ubuntu (não atualizado - vulnerabilidade);
- Anti-clickjacking não presente (vulnerabilidade);
- *Headers* incomuns encontrados (possível problema);
- MultiViews habilitado (vulnerável a ataques de força bruta);
- permitida as ações (HTTP Methods) de: GET, HEAD, POST, OPTIONS
- OSVDB – 3233[27]: relata possibilidade de ataque SQL Injection.

Concluindo a varredura, realizamos a operação para o IP 10.0.2.2, como pode ser visto na Figura 30.

[27] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3233

Figura 30 - Scanning IP 10.0.2.2 (captura de tela do instruendo)



Fonte: o Autor

Do resultado obtido com o scanning no IP 10.0.2.2 (Figura 30), podemos identificar as seguintes informações / vulnerabilidades:

- Servidor Apache, 2.2.20 – Ubuntu (não atualizado);

- Anti-clickjacking não presente (vulnerabilidade);

- *Headers* incomuns encontrados (possível problema);

- MultiViews habilitado (vulnerável a ataques de força bruta);

- Servidor retorna resposta positiva quando alimentado de forma errada, o que pode causar falsos positivos (vulnerabilidade);

- Arquivo PHP config[28] pode conter dados de usuários e senhas (vulnerabilidade);

- possibilidade de obter, via consulta HTTP, informações sensíveis sobre o servidor;

- Arquivos *readme, configuration* e *intall* encontrados;

- Página *admin login* encontrada.

- OSVDB – 3233: Além de relatar a possibilidade do ataque SQL Injection (como identificado na análise do IP 10.0.1.2) também relata a vulnerabilidade a ataques XSS.

Após varrer a rede, o instruendo deverá apresentar os resultados obtidos, destacando as vulnerabilidades encontradas nos três servidores.

[28] O php-config é um script shell para obter informações sobre as configurações do PHP instalado.

Figura 31 - **Resposta ao pedido 1 e 2 (captura de tela do instruendo)**

Fonte: o Autor

Para a realização da terceira atividade (ataques), dividiremos este subcapítulo nos três tipos de ataques solicitados para o exercício (*Cross-site scripting*, *SQL Injection* e *Remote File Inclusion*).

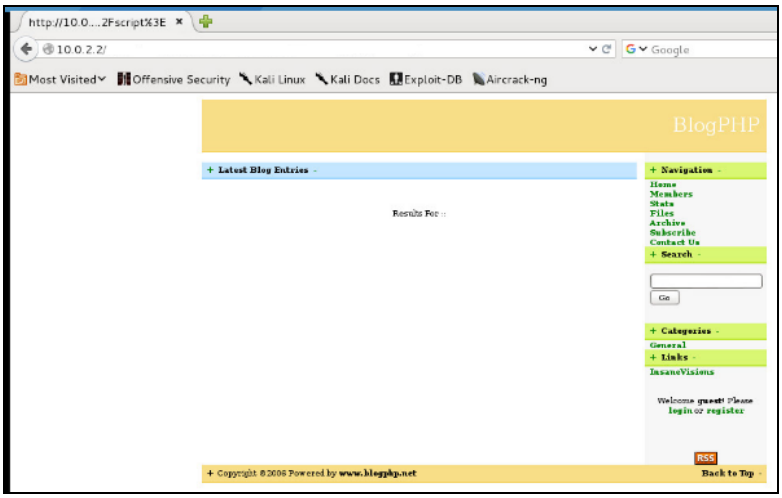
4.2.1 *Cross-site scripting* (XSS)

O roteiro para o instruendo realizar este ataque consiste em 9 passos.

1) Alterar a configuração de proxy HTTP do Firefox para localhost:8080;
2) Abrir o owasp-zap presente em /pentest/web/owasp-zap/zap.sh
   Este passo sugere a utilização do *Zed Attack Proxy* (ZAP)[29] que é uma ferramenta de distribuição gratuita e que pode auxiliar na identificação de vulnerabilidades. Pelo fato de termos utilizado anteriormente o *nikto* para identificar as vulnerabilidades, este procedimento pode ser opcional.
3) Acessar a página web do blogphp em http://10.0.2.2 e verificar se o owasp-zap está listando as chamadas feitas ao site acessado;

[29] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Figura 32 - Página web do blog php (captura de tela do instruendo)



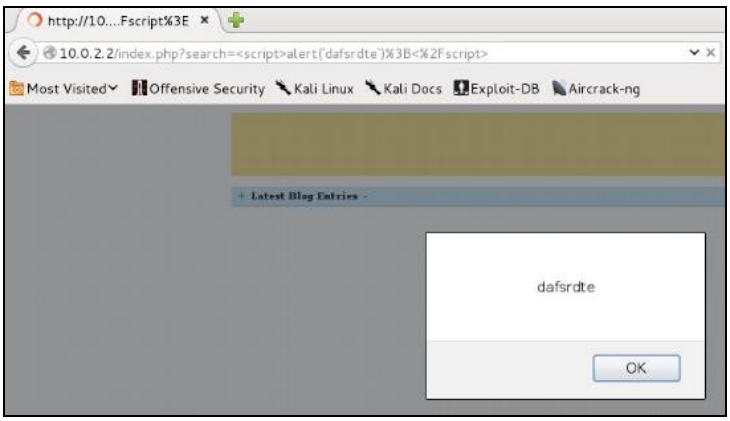
Fonte: o Autor

4) Mandar o blogphp buscar por algo, como a *string* teste e clicar em "Go";
5) Voltar no owasp-zap e clicar com o botão direito no nó GET:index.php(search)->Attack->Active scan node;

   Neste passo, o ZAP enviou e recebeu a requisição realizada no passo 4 e pode realizar análises do alvo.
6) Ir na aba Alerts (oculta no canto inferior direito) e expandir;
7) Selecionar a aba "*Alerts*" e clicar sobre o item "cross-site scripts";

   Neste passo, uma análise específica sobre XSS foi realizada pelo ZAP.
8) Abra a URL no Firefox http://10.0.2.2/index.php?search=</title><script>alert('dafsrdte');</script><title> pelo exemplo do owasp; e
9) Uma caixa de alerta será mostrada como especificado na Figura 33.

Figura 33 - Ataque XSS realizado na página blog php (captura de tela do instruendo)



Fonte: o Autor

Concluído estes 9 passos, identificamos que o servidor é vulnerável a um ataque XSS. Cabe ressaltar que a partir deste momento o atacante pode copiar toda a URL do passo 09, incluir a mensagem de interesse e enviar via e-mail, por exemplo, para os alvos (pessoas que irão clicar no link e abrir a página que contém a mensagem do atacante).

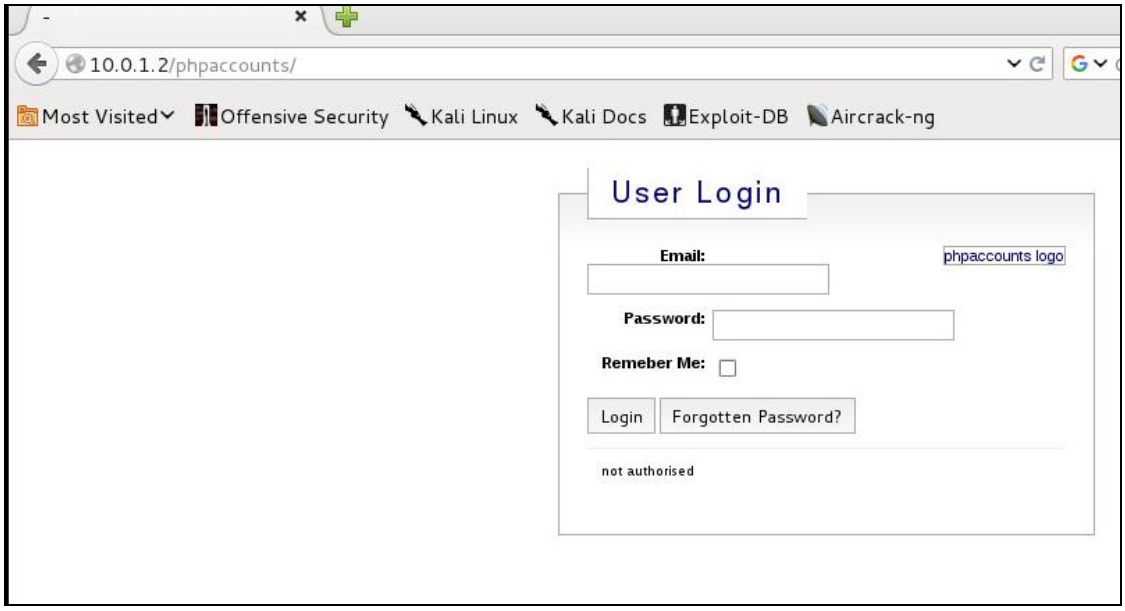
4.2.2 *SQL Injection*

1) Acessar a máquina do instruendo;

2) Rodar o comando startx para iniciar a interface gráfica;

3) Abrir o Firefox e acessar a URL http://10.0.1.2/phpaccounts/ (Figura 34)

Figura 34 – Página phpaccounts (captura de tela do instruendo)



Fonte: o Autor

4) Abrir o código fonte do formulário web de login (Figura 35) e encontrar os nomes dos campos de login, senha e ação do formulário;

Figura 35 – Código fonte do formulário Web (captura de tela do instruendo)

```
File  Edit  View  Help
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title> - </title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">

<link rel="stylesheet" href="style.css" type="text/css">
</head>
<body class="bgbody">
<div id="loginForm">
<form name="loginForm" action="index.php?frameset=true" method="POST" target="_top">
<input type="hidden" name="" value="" />

    <fieldset>
<div id="logolarge">
<a target="_blank" href="http://www.phpaccounts.com" title="php accounts project website"><img src="http://www.phpaccounts.com/offsite/images/logo0.5.gif" alt="ph
</div>
        <legend>User Login</legend>
                <p><label for="Email">Email:</label>
                <input type="text" name="Login_Username" value="" /></p>
                <p><label for="Login_Password">Password:</label>
                <input type="password" name="Login_Password" value="" /></p>
                <p><label for="remeber_me">Remeber Me:</label>
                <input type="checkbox" name="remember_me" value="true"  /></p>

        <input type="submit" class="submit" name="login" value="Login" />
        <input type="submit" class="submit" name="forgotten_password" value="Forgotten Password?" />
<p class="message">not authorised</p>
    </fieldset>
</form>
</div>

</body>
</html>
```

Fonte: o Autor

5) Acessar o diretório /pentest/database/sqlmap

Sqlmap[30] é uma ferramenta de teste de penetração gratuita que automatiza os processos de detecção e exploração do ataque SQL Injection.

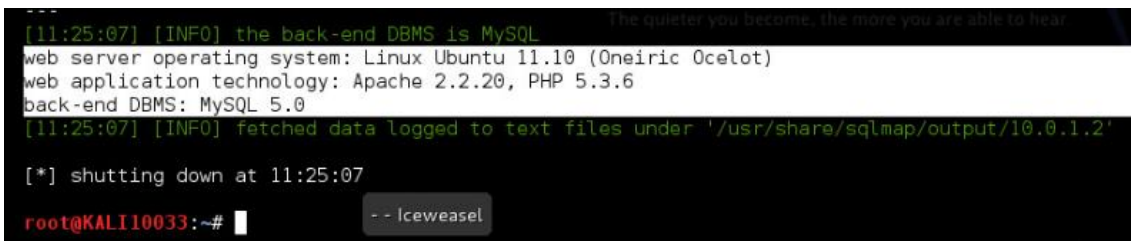
6) Executar o comando ./sqlmap.py –u

7) 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)

8) Como resultado é impresso o sistema operacional, versão do Apache, Mysql e PHP;

Figura 36 – Resultado do Ataque de SQL Injection (captura de tela do instruendo)



```
[11:25:07] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 11.10 (Oneiric Ocelot)
web application technology: Apache 2.2.20, PHP 5.3.6
back-end DBMS: MySQL 5.0
[11:25:07] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/10.0.1.2'

[*] shutting down at 11:25:07

root@KALI10033:~#
```

Fonte: o Autor

[30] http://sqlmap.org/

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

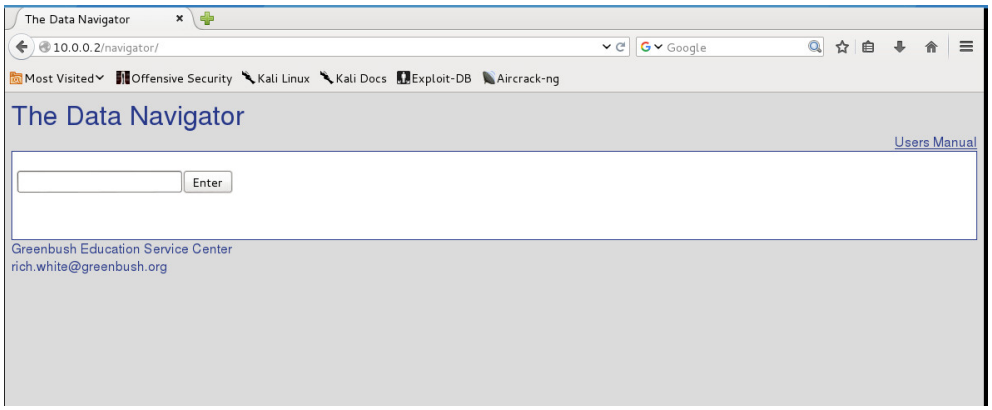
9) Faça login no formulário web usando o usuário <x' or '1' = '1'#> sem os sinais de < e > e qualquer senha.

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.

4.2.3 *Remote File Inclusion* (RFI).

1) Reconfigure o proxy do Firefox para usar as configurações de proxy do sistema;
2) Abrir url http://10.0.2.2/navigator/ e notar que ao clicar em "*login*" ele redireciona para http://10.0.2.2/navigator/index.php?page=login.php;

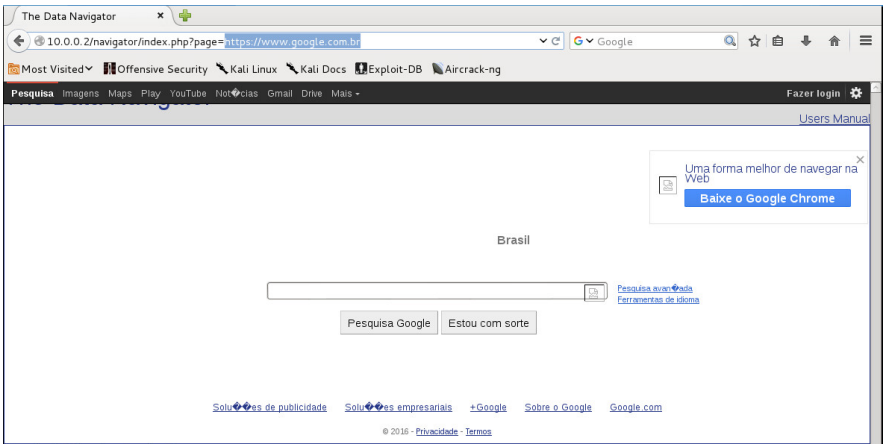
Figura 37 – Página que será atacada (captura de tela do instruendo)



Fonte: o Autor

3) Executar o nikto em /pentest/web/nikto/ através da linha de comando ./nikto.pl -host "http://servidor/navigator/index.php?page=login.php
4) Verificar na saída do comando nikto que RFI foi detectado, indicando que conseguiu inserir um arquivo remoto. Também é possível reproduzir com http://servidor/navigator/index.php?page=https://www.google.com.br

Figura 38 – Site sob ataque RFI (captura de tela do instruendo)



Fonte: o Autor

Em resumo, com este procedimento o atacante pode inserir remotamente um arquivo que poderá causar danos aos servidores vulneráveis a RFI. No exemplo acima, o site *navigator* foi redirecionado indevidamente para a página do *google*. Neste caso, não identificamos maiores problemas, mas na situação de um ataque a um site de banco, o atacado (correntista do banco) poderia estar sendo redirecionado para uma página clonada do banco e seria iludido a digitar os seus dados bancários, senhas e demais informações. Neste caso, o atacante, de posse dos dados bancários, poderia entrar na conta e realizar o roubo.

CONCLUSÃO

Este trabalho teve como problemática a questão envolvendo a preparação de profissionais militares para atuarem na área cibernética; e como objetivo geral, a análise de ferramentas computacionais que viabilizassem o preparo de militares para atuarem no ambiente cibernético.

Com este foco, utilizamos uma extensa pesquisa bibliográfica envolvendo manuais militares, legislações, artigos científicos, manuais técnicos e livros específicos da área. E por fim, um estudo de caso envolvendo o Simulador de Operações de Guerra Cibernética (SIMOC) na formação de militares para atuarem no espaço cibernético.

A utilização de simuladores não é novidade no meio civil e tão pouco na área militar. Simuladores de combate são utilizados para treinar pilotos de caças, posicionar embarcações, conduzir carros de combate, empregar efetivos militares em teatros de operações distintos, conduzir tiros e prever trajetórias.

As vantagens de utilizar recursos simulados são amplas. O simulador viabiliza segurança pessoal (operadores, pilotos, engenheiros), economia de recursos materiais e financeiros, velocidade de processamento, realização de testes exaustivos (o que garante segurança e confiabilidade), e utilização de recursos não disponíveis (que são virtualizados). Enfim, uma infinidade de possibilidades fica disponível quando trabalhamos em um ambiente virtual.

Desta maneira, este trabalho apresentou algumas características do SIMOC que o Exército está utilizando nos cursos do Centro de Instrução de Guerra Eletrônica (CIGE). O intuito é utilizar a ferramenta para formar militares aptos a combaterem no ambiente cibernético.

O software basicamente proporciona 2 modos de operação. O primeiro, contendo “times” participantes, que realizam ataque e defesa em um ambiente controlado e monitorado pelo simulador. Na ausência de um dos partidos, o software deverá simular a presença do inimigo e executar ações de ataque e/ou defesa. O segundo modo tem por objetivo analisar e determinar vulnerabilidades em uma rede de computação.

Para estes fins o simulador possui os módulos de virtualização, módulo de gestão de cenários e módulo de monitoramento. Assim, o SIMOC é capaz de implementar um ambiente estanque, permitindo a existência de um ou dois agentes (oponentes), emula o comportamento de uma rede de produção típica, possui interface de controle e tem características de dinamismo e interatividade.

Para maiores detalhes, uma sequência de requisitos técnicos é apresentada em anexo a este trabalho, com base no Edital Nr 28, realizado em 2011, pela da Base Administrativa do Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEX). Nestes requisitos, podemos ter uma noção das funcionalidades que o SIMOC possui.

Como vantagem da utilização do simulador, podemos destacar: a possibilidade de criar cenários similares ao emprego real da tropa militar; possibilidade de criar diversos tipos de simulações; reuso de elementos de simulação (objetos, eventos, métricas, etc) pré-registrados no catálogo do simulador; possibilidade de importar máquinas virtuais para o catálogo do simulador; criar redes mistas, contendo segmentos virtuais e segmentos de rede reais; variedade de funcionalidades que apoiam o instrutor durante as simulações; monitoramento em tempo real; segurança na sua infraestrutura; utilização de maquetes conectadas ao simulador; e o desenvolvimento nacional da ferramenta.

No entanto, algumas limitações existem: inviabilidade de simular ligações de fibra ótica; falta de cenários que contemplem ativos e situações militares; alguns produtos de TI não possuem versões virtualizadas; o simulador não possui um ambiente adequado para a análise de *malwares;* e não é possível conectar no SIMOC as máquinas pessoais dos instruendos para realizar os exercícios.

Cabe ressaltar, que durante o trabalho apresentamos sugestões de como contornar parcialmente, em situações peculiares, grande parte destas limitações.

Como limitação deste trabalho, não foi possível identificar, por exemplo, a capacidade do software em “aprender” formas de ataques e defesas diferentes. Já que o simulador proporciona ambientes virtualizados para que agentes realizem ações ofensivas e defensivas, o programa poderia aproveitar estas situações para estudar como realizar estas ações e, se fosse o caso, atualizar a sua matriz de eventos.

Basicamente a sugestão seria de, por intermédio da inteligência artificial, possibilitar que o simulador filtre as ações dos agentes, que ele (simulador) ainda não possui na sua biblioteca, e disponibilize estas ações de ataque / defesa para que o instrutor tome conhecimento e insira, ou não, estas novas modalidades de combate em simulações futuras. Esta funcionalidade sugerida 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

ALAN, A; PRITSKER,B. Introduction to GASP IV. **Proceedings** of 9th Winter Simulation Conference. Pages 28-30. IEEE Press Piscataway, NJ, USA, 1977.

BALCI, O; et. al. Visual Simulation Environment. Proceeding of the Winter Simulation Conference, 1998.

BARRETO, A, B; et. al. Entendimento do impacto dos aspectos cibernéticos em missões: um novo desafio para as forças Armadas. Spectrum, Setembro, 2012.

BRASIL. Edital do Pregão Eletrônico N 28. SALC, Base Administrativa do Centro de Comunicações e Guerra Eletrônica do Exército. Brasília – DF, 2011.

BRASIL. **Estratégia Nacional de Defesa**. Ministério da Defesa. 2ª Ed. Brasília, Distrito Federal, 2008.

BRASIL. MINISTÉRIO DA DEFESA. MD31-M-07. Doutrina militar de defesa cibernética, Brasilia, 1 Edição, 2014.

BRIGATTO, G. Exército quer arma Nacional para travar guerra on-line. - São Paulo : Jornal Valor Econômico, Janeiro 23, 2012.

CARISSIMI, A. Virtualização: da teoria a soluções. 26º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Rio de Janeiro, 2008.

CEH. Certified Ethical Hacker V. 8. Ethical Hacking and Countermeasures. Module 13 - Hacking Web Applications. EC-Council. 2014.

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

DAVIS, D, A; PEGDEN, C, D. Introduction to SIMAN. Proceeding of the Winter Simulation Conference, 1988.

DELOOZE, L.; MCKEAN, P.; MOSTOW, J. R. Incorporating Simulation into the Computer Security Classroom, Savannah, 2004. ISSN 0-7803-8552-7/04.

SANTOS, J. C. Podemos recrutar hackers [Interview]. - [s.l.] : Revista Epoca, Edição 687, julho 18, 2011.

DIEDRICH, T, J; MACHADO, A, F, A. Capacitação de Pessoal em Defesa Cibernética no Âmbito do Comando-Geral de Operações Aéreas. Spectrum [Journal]. 2015.

DUTRA, A, M, C. Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto. Simpósio de Aplicações Operacionais em Área de Defesa. Instituto Tecnológico de Aeronáutica. São José dos Campos – SP. 2011.

GOMES, R. Simulador de Operações de Guerra Cibernética [Palestra]. Centro de Instrução de Guerra Eletrônica. Brasília-DF, 2014.

GUIDE. Technical Operator. Elbit System. PAIZ. 2012a.

GUIDE. Training Scenario. Elbit System. PAIZ. 2012b.

LUIZ F. J.; SOUZA V. H. B. Implementação de um ataque de negação de serviço no ambiente network simulator. - Rio de Janeiro : [s.n.], 2011.

MANDARINO, R. J.; CANONGIA, C. Livro Verde - Segurança Cibernética no Brasil [Book]. - Brasília : [s.n.], 2010.

GONÇALVES, A. J.; CANONGIA, C.; MANDARINO, R. J. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. - Brasília : Presidência da República - Gabinete de Segurança Institucional, 2010.

KING, C,B. Taylor II Manufacturing Simulation Software. Proceeding of the Winter Simulation Conference, 1996.

LEEUWEN, V. et al. Cyber security analysis testbed: combining real, emulation, and simulation, Albuquerque, 2010. ISSN 978-1-4244-7402-8/10.

LICOL, D. M. Modeling and Simulation in Security Evaluation, Urbana-Champaign, 2005. ISSN 15407993/05.

MACHADO, A. F. A; BARRETO,A, B; YANO, E., T. Architecture for Cyber Defense Simulator in Military Applications [Presentation]. 18 International Command and Control Research Symposium. Alexandria, EUA, 2013.

MACHADO, A. F. A; YANO, E., T. Arquitetura conceitual de um simulador para consciência situacional cibernética [Tese de Mestrado]. Instituto Tecnológico de Aeronáutica, São José dos Campos- SP, 2013.

MACHADO, A, F, A. Security: new information society challenge. [Presentation]. 2 International Seminar on Safety Critical Systems. São José dos Campos – SP. Brasil. 2015.

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

MCDONALD, M, J.; et. al. Cyber Effects Analysis Using VCSE: Promoting Control System Reliability, Sandia Report SAND2008-5954, printed September 2008.

MOREIRA, M. M.; KARL, D. A Política e a Cibernética. In: Deutsch na UNB: conferência, comentários e debates de um simpósio internacional realizado de 11 a 15 de agosto de 1980. Brasília: Editora da UNB, 1980.

PASTOR. State-of-the-art simulation systems for information security education, training and awareness, 2010.

PEGDEN, C,D. Introduction to SIMAN. Proceedings of 16th Winter Simulation Conference. Pages 34-41. IEEE Press Piscataway, NJ, USA, 1984.

POCKET GUIDE, IDC Engineers. Power Systems Protection Power Quality and Substation Automation. Published by IDC Technologies 1031 Wellington Street West Perth 6005 Australia. ISBN 1 875955 09 7. Fifth Edition. 2003.

RUST, C. Brasil se prepara para possível guerra cibernética [Interview]. - [s.l.] : Olhar digital, janeiro 19, 2012.

SHANNON R.E. System Simulation: the art and science [Book]. - Englewood Cliffs, N.J: Prentice : [s.n.], 1975.

SIMOC. Simulador de Operações de Guerra Cibernética. Manual do Usuário. Perfil do Instruendo. RustCon 2014 a.

SIMOC. Simulador de Operações de Guerra Cibernética. Manual do Usuário. Perfil do Administrador. RustCon 2014b.

SIMOC. Simulador de Operações de Guerra Cibernética. Documentação de Resolução de Cenário. RustCon 2014c.

SINGH, A. An introduction to virtualization. Jan 2004. Disponível em: <http://www.kernelthread.com/publications/virtualization/>. Acesso em 10 jul. 2016.

SKYBOX RISK CONTROL. Manual. Getting Started Guide. Skybox Security. Versão 11. 2010.

SRIKUMAR, S. The Simulator Classroom: Why Corporations are Betting Heavily on Sophisticated New Simulation Software, v. Vol. 164 (3), p. 56. 1995.

THEOPHILO, R. A História da Cibernética**.** Disponível em: <http://www.psicologia.org.br/internacional/ap10.htm>. Acesso em: 03 out. 2015

WIENER, N. *Cybernetics, or control and communication in the animal and the machine.* Cambridge, Massachusetts: The Technology Press; New York: John Wiley & Sons, Inc., 1948.

ZENG, X; GERLA, M. GloMoSim: a library for parallel simulation of large-scale wireless networks. Twelfth Workshop on Parallel and Distributed Simulation, 1998. PADS 98. Proceedings. Banff, Alfa. 1998.

ANEXO I – Especificação Técnica do SIMOC

Quanto à especificação técnica, segundo o edital número 28/2011, a Base Administrativa do CComGEx, o simulador de defesa cibernética deve, dentre outras possibilidades:

- gerenciar as máquinas virtuais (ligar, desligar, clonar, salvar estado, tomar um instantâneo e instanciar máquina em um determinado ponto da rede);
- implementar os seguintes itens: cliente de rede Windows XP, cliente de rede Windows Vista, cliente de rede Windows 7, cliente de rede Ubuntu, servidor de arquivos Linux Debian, servidor de arquivos Windows Server 2003, servidor de impressão Windows Server 2008, servidor de páginas Linux Debian com Apache, servidor de páginas Linux Debian com Nginx, servidor FTP Linux Debian, servidor de email Exchange, servidor de email Sendmail, servidor de email Postfix e firewall;
- criar enlace entre entidades virtualmente conectadas;
- possibilitar a modelagem de qualquer tipo de enlace (interrupção do enlace, interrupção em somente um dos sentidos, aumento e diminuição da largura de banda, aumento e diminuição da taxa de erro de bits, inserção de pacotes duplicados e degradação do enlace);
- implementar os seguintes itens como objetos no catálogo das classe: Ethernet 10/100/1000 base T, WiFi a/b/g/n, ADSL, modem discado e enlace satelital.
- para o serviço de rede: tornar a ação do agente mais rápida ou mais lenta, restringir ou proibir a ação do agente sobre uma porção específica da rede e inserir ações erráticas no comportamento do agente;
- para o serviço de rede, implantar: usuário web, usuário da intranet, usuário baixando conteúdo de software P2P, usuário acessando sua caixa postal, usuário tunelando tráfego, varredura do perímetro externo de uma rede e ataque de força bruta em sistemas de autenticação remota;
- medir: a quantidade de tráfego que passa por determinado nó da rede em relação à quantidade total de tráfego da rede, quantidade de tráfego que a rede é responsável em relação à quantidade total de tráfego no simulador, e nós da rede para o qual convergem a maioria do tráfego de rede;

- quanto ao cenário, deve permitir: extração de dados por parte de um atacante, realização de ataque DDoS e degradação do canal de comunicação entre duas redes.

- Licença de software de virtualização para, pelo menos, 03 servidores com 2 processadores contendo, no mínimo, as seguintes funcionalidades:

- ✓ suportar a quantidade de núcleos do processador do servidor físico, independente de sua quantidade;
- ✓ suportar até 2TB de memória RAM por servidor físico;
- ✓ suportar por servidor físico: 2,0 TB de disco podendo atingir até 64 TB localizados em uma SAN (“StorageArea Network); 32 portas Gigabit Ethernet; 4 portas 10 Gigabit Ethernet; 8 HBA’s (Host BustAdapter); 20 CPU’s Virtuais por core não excedendo quantidade máxima de 256 CPU virtuais por servidor; e até 256 máquinas virtuais.

- Possuir sistema operacional próprio executando diretamente no hardware para execução do software de virtualização;

- Permitir a criação de máquinas virtuais multiprocessadas, com até 32 processadores em todos os sistemas operacionais suportados;

- Viabilizar a criação de máquinas virtuais com até 1 TB de memória;

- Possibilitar a criação de máquinas virtuais com até 10 placas de rede;

- Ser compatível com as seguintes tecnologias: “x86_64”; “dual core”; “quad core”; “hexa core”; “hyperthreading”; e Intel EPT.

- Permitir a criação de máquinas virtuais coexistindo no mesmo hardware físico com, no mínimo, os seguintes sistemas operacionais:

- ✓ Windows Server 2008 (Standard, Enterprise, and Datacenter editions);
- ✓ Windows Server 2003 Standard, Enterprise, Web, ou Small Business Server;
- ✓ Windows Server 2003 Standard, Enterprise, Web, or Small Business Server R2;
- ✓ Windows 2000 Advanced Server e Server (SP3 ou SP4);
- ✓ Windows NT Server;
- ✓ Windows XP Professional SP2 e SP3;
- ✓ Windows Vista Enterprise 32 e 64 bits;
- ✓ Windows Vista Home Basic 32 e 64 bits;

- ✓ Windows Vista Home Premium 32 e 64 bits;
- ✓ Windows Vista Business 32 e 64 bits;
- ✓ Windows Vista Ultimate 32 e 64 bits;
- ✓ RedHat Enterprise Linux 5;
- ✓ RedHat Enterprise Linux 4;
- ✓ RedHat Enterprise Linux 3;
- ✓ RedHat Enterprise Linux 2.1;
- ✓ Suse Linux Enterprise Server 11;
- ✓ Suse Linux Enterprise Server 10;
- ✓ Suse Linux Enterprise Server 09;
- ✓ Suse Linux Enterprise Server 08;
- ✓ Ubuntu 8.04 LTS;
- ✓ Ubuntu Linux 7.10;
- ✓ Ubuntu Linux 7.04;
- ✓ CentOS 4;
- ✓ CentOS 5;
- ✓ Debian 4;
- ✓ Debian 5;
- ✓ FreeBSD 6.3;
- ✓ FreeBSD 6.4;
- ✓ FreeBSD 7.0;
- ✓ FreeBSD 7.1;
- ✓ Netware 6.5 Server ;
- ✓ Netware 6.0 Server;
- ✓ Netware 5.1 Server;
- ✓ Solaris 8 for x86;
- ✓ Solaris 9 for x86;
- ✓ Solaris 10 for x86;
- ✓ SCO Openserver 5.0;
- ✓ SCO Unixware 7;
- ✓ Asianux 3.0; e
- ✓ OSX Server 10.6 (SnowLeopard).

- Suportar tecnologias para melhoria de performance de rede;

- Deverá suportar a criação de VLANS nas redes virtuais;

- Permitir o isolamento das máquinas virtuais (a não ser pelo ambiente de rede), evitando assim que o uso de uma máquina virtual interfira na segurança de outra;

- Viabilizar o acesso por mais de um caminho (*multipath*) e tolerante a falha ao SAN (*Storage Area Network*);

- Possuir sistema de arquivo que permita ser configurado em *storage* compartilhado e que mais de um servidor físico consiga acessar o mesmo compartilhamento simultaneamente;

- Realizar conexões com tecnologias de *storage* SAN FC, iSCSi e NAS;

- Permitir a instalação em um servidor físico sem disco físico local, podendo ser iniciado através de uma SAN FiberChannel ou iSCSI, utilizando o conceito de diskless;

- Permitir que cada máquina virtual tenha endereço IP e MAC próprio;

- Aceitar a conversão ilimitada de um sistema físico existente com sistema operacional Windows para uma máquina virtual;

- Suportar a extensão do tamanho do disco virtual enquanto a máquina virtual permanecer ligada;

- Suportar o clone de máquinas virtuais sem a interrupção da máquina virtual a ser clonada;

- Possuir recurso de compartilhamento de páginas de memória entre múltiplas máquinas virtuais;

- Realizar balanceamento automático dos discos virtuais no nível do *storage*; e

- Admitir alocação do disco da máquina virtual de acordo com o perfil de utilização.

Na funcionalidade de Gerenciamento e Administração o sistema deverá, dentre outras, possuir no mínimo:

- possuir funcionalidade de gerenciamento dos recursos de hardware (consumo de processadores, memória RAM, dispositivos de rede, discos rígidos, controladoras de disco/storage);

- gerenciar a performance das máquinas virtuais instaladas no Servidor de Virtualização;

- permitir a gerência centralizada de todo o parque virtualizado, a partir de uma única console;

- permitir a criação de workflows para automação e orquestração dos processos de virtualização;

- possibilidade de definir a quantidade mínima e máxima de CPU e memória para cada máquina virtual;

- definir a saída de banda de rede para cada máquina virtual;

- Permitir a criação de ambiente de alta disponibilidade (cluster ou tecnologia equivalente ou superior) entre as máquinas virtuais;

- Tolerar a migração de uma máquina virtual para outra máquina física, sem necessidade de interrupção dos serviços da máquina virtual;

- Permitira migração de máquinas virtuais entre diferentes servidores físicos para fins de manutenção, balanceamento de carga e ou upgrades;

- Possuir funcionalidades de detecção de falha de uma máquina física, migrando automaticamente as máquinas virtuais afetadas para controle de outra máquina física e procedendo, sua ativação automaticamente. Para esta funcionalidade, deverá suportar um grupo de até 32 servidores simultaneamente;

- Possuir funcionalidades de detecção de falha do sistema operacional Windows de uma máquina virtual;

- permitir que a configuração de rede do ambiente virtual possa ser feita uma única vez e replicada para todo o ambiente;

- Permitir que ferramentas de backup, tais como, Tivoli, Netbackup realizem backup e recuperação incrementais, diferenciais e de imagem completa de máquinas virtuais bem como em nível de arquivo para os sistemas operacionais;

- Permitir a visualização gráfica da topologia da infra-estrutura virtual;

- Admitir o monitoramento em tempo real e otimizar a utilização dos recursos não utilizados pelos hardwares;

- Permitir configurar faixas de alarme para monitoração de CPU, memória, rede e disco que alertem após um período de tempo pré-definido no estado de alerta;

- Permitir a monitoração e notificação de alertas parametrizados através de e-mail, traps SNMP e scripts;

- Consentir armazenar dados e estatísticas de monitoração por até dois anos;

- Permitir a redução da complexidade de gerenciamento, combinando servidores físicos em clusters para maior disponibilidade, e controle de recursos mais flexível;

- Permitir a criação de recursos de alta disponibilidade para toda infra-estrutura virtual. A perda de um servidor físico não, necessariamente, interrompe o sistema;

No tocante a Segurança, o anexo I prevê que o sistema deverá possuir no mínimo:

- integração com o sistema de diretório MICROSOFT ACTIVE DIRECTORY, possibilitando integrar a estrutura de usuários com a hierarquia de segurança dos grupos de servidores e máquinas virtuais sem precisar alterar o esquema do serviço de diretório;

- Possuir funcionalidade para automatização da aplicação de atualizações no sistema operacional utilizado para virtualização;

- Permitir gerenciar o acesso a console de administração de forma granular (cada usuário ou grupo terá uma quantidade de ações que ele pode executar);

- A console de gerenciamento deverá permitir no mínimo a granularidade de acesso para as seguintes ações:

- ✓ Ligar uma ou mais máquinas virtuais;
- ✓ Desligar uma ou mais máquinas virtuais;
- ✓ Criar máquinas virtuais;
- ✓ Remover máquinas virtuais;
- ✓ Criar templates de máquinas virtuais;
- ✓ Criação de cluster de máquinas virtuais;
- ✓ Adicionar e remover um servidor físico à console de gerenciamento;
- ✓ Criar grupos de permissão e associar a usuários;
- ✓ Criar e apagar alarmes de monitoração.