UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

CIBERSEGURANÇA:
UM MODELO PARA ELABORAÇÃO DE EXERCÍCIOS DE ATAQUE E DEFESA EM APLICAÇÕES WEB

TRABALHO DE GRADUAÇÃO

Sandro Lemos Oliveira

Santa Maria, RS, Brasil
2013

CIBERSEGURANÇA: UM MODELO PARA ELABORAÇÃO DE EXERCÍCIOS DE ATAQUE E DEFESA EM APLICAÇÕES WEB

por

Sandro Lemos Oliveira

Trabalho de Graduação apresentado ao Curso de Ciência da Computação da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de
Bacharel em Ciência da Computação

Orientador: Prof. Dr. Raul Ceretta Nunes

Co-orientador: Me. Érico Marcelo Hoff do Amaral

Santa Maria, RS, Brasil

2013

Universidade Federal de Santa Maria
Centro de Tecnologia
Ciência da Computação

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Graduação

CIBERSEGURANÇA: UM MODELO PARA ELABORAÇÃO DE EXERCÍCIOS DE ATAQUE E DEFESA EM APLICAÇÕES WEB

elaborado por
Sandro Lemos Oliveira

como requisito parcial para obtenção do grau de
Bacharel em Ciência da Computação

COMISSÃO EXAMINADORA:

Prof. Dr. Raul Ceretta Nunes
(Presidente/Orientador)

Profª Drª. Roseclea Duarte Medina (UFSM)

Prof. Dr. Osmar Marchi dos Santos (UFSM)

Santa Maria, 22 de fevereiro de 2013.

Dedico a

minha avó materna Izoleta Azambuja Lemos, matriarca da família, a única dos meus avós que conheci, pelo carinho que me dedicou!

E aos heróis anônimos da tragédia da Kiss em especial ao Leonardo Lemos Karsburg (Dartagnan) que com carinho e alegria guardo na lembrança.

AGRADECIMENTOS

Agradeço aos membros da banca que, com suas contribuições, ajudaram-me a ver os diferenciais que o trabalho poderia ter. Ao orientador e ao co-orientador, pela amizade e pelas orientações. Às pessoas que convivi no INPE, durante todo tempo que estive por lá, em especial aos colegas do suporte, de estágio, do Gruma, da SMDH e ao grande amigo e orientador Koiti. Aos colegas de computação, com quem dividi tarefas, desilusões, trabalhos, estudos, truco, churrascos, alegrias, enfim, vida acadêmica. Aos que foram meus professores, pela paciência, dedicação e respeito, em especial aos da computação. Aos colegas do GTSeg, pela ajuda. À UFSM, pelas oportunidades, pela assistência, pelas bolsas, pela formação, pelas namoradas. À Lu, pelos bons momentos em que dividimos e pelo apoio que me deu. À Jê, que revisou o texto e fez o resumo em alemão. À C.E.U., pelos amigos, pela vivência, pelos ensinamentos. Aos bons amigos que fiz pelas cidades em que morei. Aos meus irmãos da União e do 4410, pela vida que dividimos, pela amizade que construímos, que vou levar para a eternidade. Aos meus familiares que, de uma forma ou de outra, durante a infância, souberam passar ensinamentos. Ao meu irmão, pelo apoio e por pagar meu cursinho pré-vestibular. Ao meu pai, pelo exemplo e à minha mãe, pela dedicação. A Deus, por ter colocado todas essas pessoas na minha vida.

A invencibilidade repousa na defesa,
A vulnerabilidade revela-se no ataque.
(TZU, 2006)

Nada de imposições, uma possibilidade entre outras; certamente que não mais verdadeira que as outras, mas talvez mais pertinente, mais eficaz, mais produtiva... E é isso que importa: não produzir algo de verdadeiro, no sentido de definitivo, absoluto, peremptório, mas dar 'peças' ou 'bocados', verdades modestas, novos relances, estranhos, que não implicam em silêncio de estupefação ou um burburinho de comentários, mas que sejam utilizáveis por outros como as chaves de uma caixa de ferramentas.
Foucault, a Norma e o Direito. François Ewald (1993, p.26)

RESUMO

Trabalho de Graduação
Curso de Ciência da Computação
Universidade Federal de Santa Maria

CIBERSEGURANÇA: UM MODELO PARA ELABORAÇÃO DE EXERCÍCIOS DE ATAQUE E DEFESA EM APLICAÇÕES WEB

AUTOR: SANDRO LEMOS OLIVEIRA
ORIENTADOR: RAUL CERETTA NUNES
Data e Local da Defesa: 22 de fevereiro de 2013, Santa Maria.

Há carência de capital humano em cibersegurança para tratar as vulnerabilidades web, frequentes e danosas. Nesse sentido, novas ferramentas e técnicas de ensino de segurança cibernética devem ser incorporadas aos cursos de tecnologia da informação sem que seja necessário aumentar o número e o tempo das disciplinas. Exercícios práticos que simulam a realidade têm demonstrado eficiência no ensino e no treinamento.

Este trabalho apresenta um modelo de como elaborar exercícios de cibersegurança para aplicações web. Utilizando o modelo, são propostos exercícios de ataque e de defesa para algumas vulnerabilidades web apresentadas no relatório da OWASP intitulado TOP 10 OWASP de 2010.

Palavras-chave: cibersegurança, vulnerabilidades web, segurança, OWASP, guia, exercícios práticos, modelo, elaboração.

ABSTRACT

Undergraduate Final Work
Undergraduate Program in Computer Science
Federal University of Santa Maria

CYBER SECURITY: A MODEL FOR DEVELOPING ATTACK AND DEFENSE EXERCISE IN WEB APPLICATIONS

AUTHOR: SANDRO LEMOS OLIVEIRA
ADVISOR TEACHER: RAUL CERETTA NUNES
Date and Place of Argumentation: Santa Maria, February 22rd, 2013.

There is a lack of skilled people to work with cyber security for frequent and danger web vulnerabilities. In this way, new tools and techniques for teaching cyber security should be incorporated into information technology courses, without the need to increase the number and duration of the disciplines. Practical exercises simulating the reality have demonstrated to be an efficiently tool in education and training.

This work presents a model to develop cyber security exercises for web applications. From the model, attack and defense exercises are proposed for web vulnerabilities presented on the OWASP report, entitled TOP 10 2010.

Keywords: cyber security, web vulnerabilities, security, information assurance, OWASP, guide, practical exercises, model, develop.

ZUSAMMENFASSUNG

Bachelor-Arbeit
Studiengang Informatik
Öffentliche Universität von Santa Maria

CYBER-SICHERHEIT: EIN MODELL FÜR DIE ENTWICKLUNG ÜBUNGEN VON ANGRIFF UND VERTEIDIGUNG IN WEB-ANWENDUNGEN

AUTOR: SANDRO LEMOS DE OLIVEIRA
LEITER: RAUL CERETTA NUNES
Datum und Ort der Argumentation: 22. Februar 2013, Santa Maria.

Es besteht ein Mangel an Humankapital in Cyber-Sicherheit für Schwachstellen web zu behandeln, die häufig und schädlich sind. Neue Werkzeuge und Lehrmethoden der Cyber-Sicherheit sollten in Kursen in der Informationstechnologie, Wissenschaftlichen und Beruflichen auf allen Ebenen, ohne die Notwendigkeit, die Anzahl und Dauer von Disziplinen zu erhöhen, integriert werden. Praktische Übungen die die Realität simulieren, bewiesen Effizienz in den Bereichen Bildung und Ausbildung.

Dieser Beitrag stellt ein Modell dafür, wie Cyber-Sicherheit Übungen für Web-Anwendungen zu entwickeln. Mit Hilfe des Modells werden Angriff und Verteidigungs Übungen vorgeschlagen für einige Web-Schwachstellen, die in dem Bericht OWASP unter dem Titel TOP 10 OWASP von 2010 vorgestellt sind.

Stichwörter: Cyber-Sicherheit, Schwachstellen Web, Sicherheit, OWASP, Leitfaden, Praktische Übungen, Modell, Vorbereitung.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Diversas nações já identificaram que há uma escassez de capital humano para atuar em cibersegurança e estão lançando estratégias de formação de profissionais. No Brasil, uma primeira iniciativa foi a criação da Escola Nacional de Defesa Cibernética (EsNaDCiber), a qual pretende fazer parcerias com universidades públicas para a formação em segurança cibernética.

Diante da falta de experiência e modelos de elaboração de exercícios, neste trabalho, propõe-se um modelo de elaboração de exercícios de cibersegurança em aplicações web, a fim de fornecer um guia para a criação de exercícios específicos de segurança web. Para tanto, tomou-se como referencial o artigo *Guide for Designing Cyber Security Exercises* e o ciclo de aprendizagem de David Kolb.

1.1 Objetivos

1.1.1 Objetivo Geral

Propor um modelo para a elaboração de exercícios de cibersegurança em aplicações web e aplicar o modelo em alguns exercícios sobre as vulnerabilidades que afetam aplicações web, segundo relatório da OWASP, Top 10 2010.

1.1.2 Objetivos Específicos

Destacam-se como objetivos específicos:

- Pesquisar sobre modelos guias para a elaboração de exercícios de cibersegurança;
- Pesquisar sobre metodologias de aprendizagem em exercícios práticos;
- Estudar as vulnerabilidades expostas no relatório da OWASP Top 10 2010;
- Propor um modelo, baseado no que foi aprendido nas pesquisas, para vulnerabilidades web.

1.2 Justificativa

As justificativas para o desenvolvimento deste projeto se apóiam no tripé: crescimento e importância da internet; aumento e diversidade das vulnerabilidades agravados pela sofisticação crescente dos ataques (Figura 1); e, principalmente, dificuldades de aprendizado sobre segurança cibernética em aplicações web.

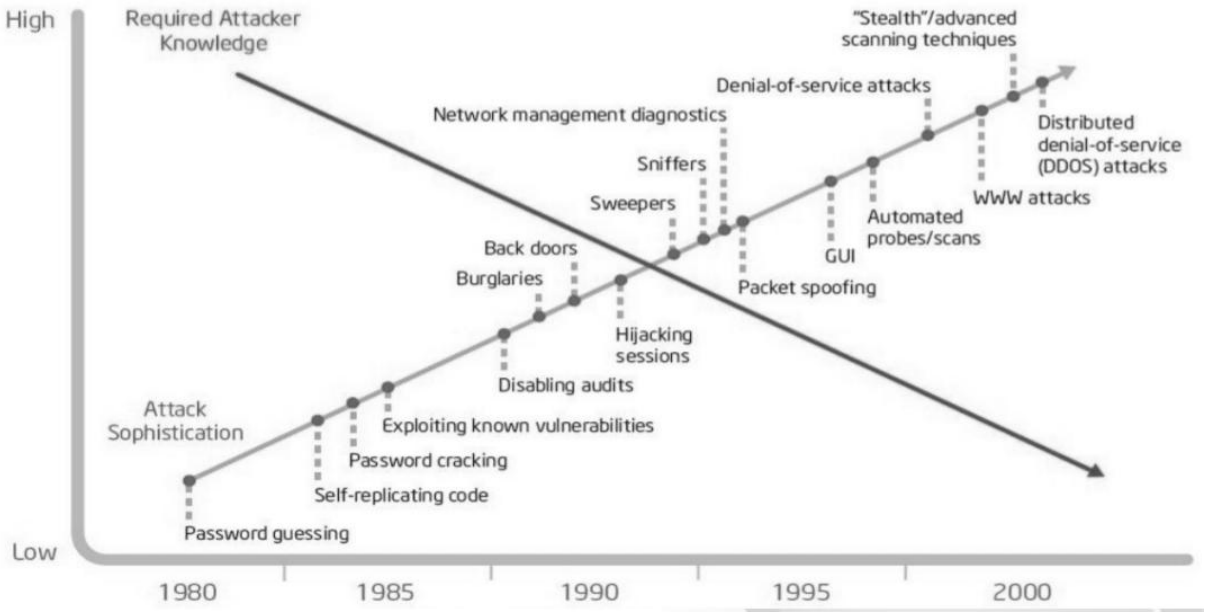

Figura 1 - Evolução dos ataques vs. conhecimento necessário

Das mais de 60 milhões de pessoas com acesso à internet em casa ou no local de trabalho, 46,3 milhões foram usuários ativos em setembro de 2011. Nota-se um crescimento de 14% sobre os 40,6 milhões constatados em setembro de 2010 (IBOPE; NIELSEN ONLINE, 2011). Em 2012, atingiu-se a marca de 70,9 milhões de pessoas que têm acesso à internet, dos quais, 50,9 milhões foram usuários ativos em setembro, totalizando um aumento de 10% em relação a 2011. Pode-se observar, na Figura 2, o importante crescimento de usuários com internet domiciliar e a divisão das três fases da internet brasileira. A quarta fase será de crescimento do uso de internet via *tablets* e *smartphones* (IBOPE; NIELSEN ONLINE, 2012).

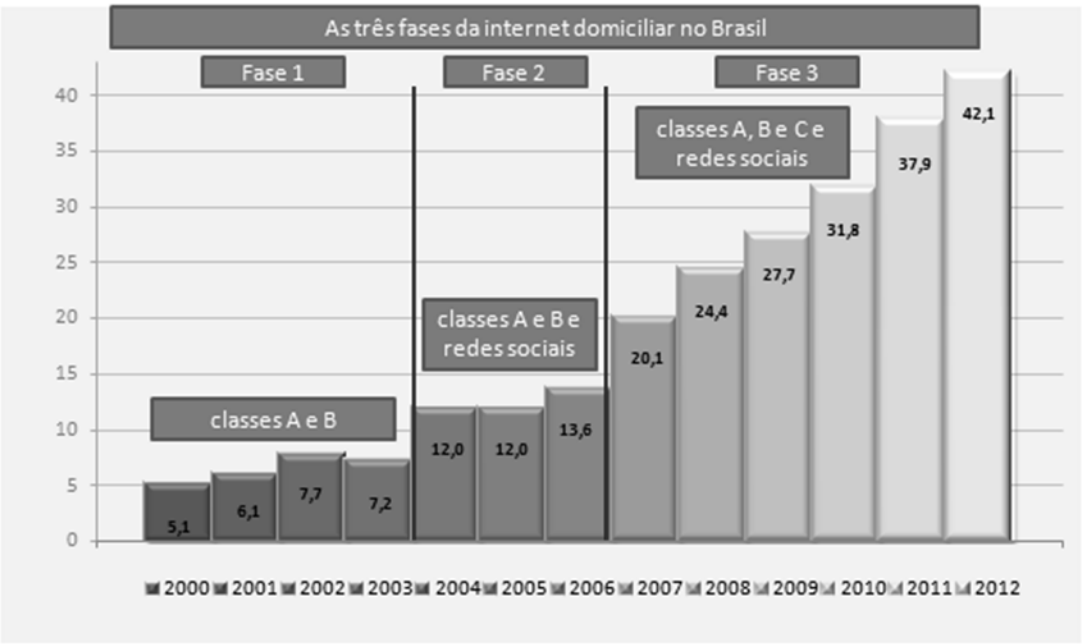

Figura 2 - Evolução dos usuários ativos domiciliares em milhões

Na Figura 3, pode-se constatar que as horas navegadas também vêm aumentando significativamente (CETIC.BR, 2012).

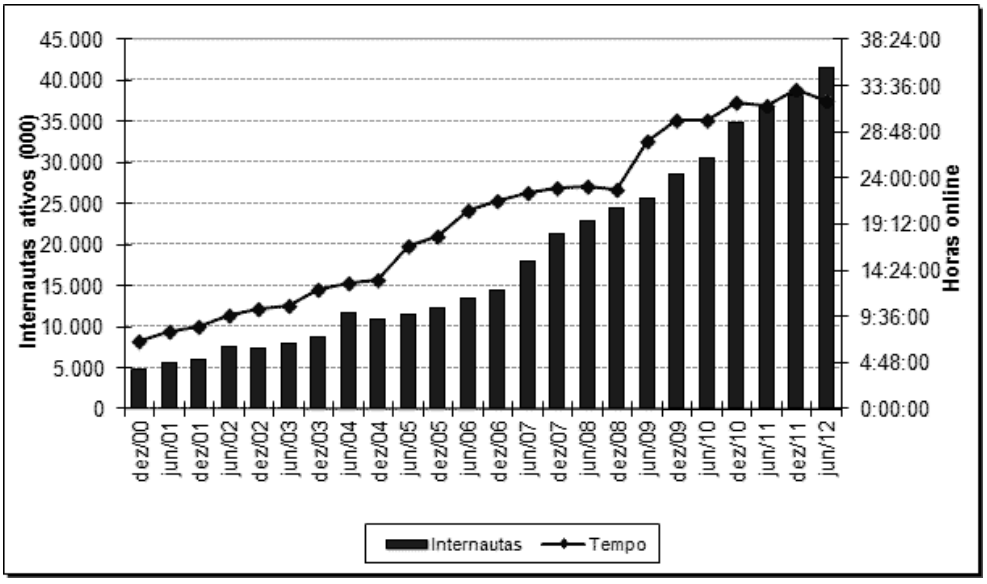

Figura 3 - Internautas domiciliares ativos[1] e horas navegadas[2]

Com a grande demanda por serviços de internet, a necessidade de aplicações web maiores e mais complexas, diante de equipes com pouca

[1] Pessoas com 2 anos ou mais que navegaram na internet por meio de computadores no domicílio no mês.

[2] Tempo médio de uso do computador pelos internautas brasileiros ativos no mês

experiência em cibersegurança, pode levar à desconsideração ou ao desconhecimento dos problemas de segurança agravados pelos prazos apertados de desenvolvimento (UTO; MELO, 2009).

Sabe-se que segurança cibernética é uma gestão de soberania, assim como as aplicações web aumentam em volume, importância, complexidade e interconexão. Assim, fazer software seguro, embora seja possível, não é tarefa fácil, pois é preciso qualificar profissionais capazes de compreender e de proteger os sistemas das vulnerabilidades. Porém, essa é uma tarefa onerosa e demanda um longo tempo. Para alcançar resultados efetivos, é necessário focar os esforços na obtenção de melhor resultado: capacitar profissionais para tratar as vulnerabilidades mais críticas e mais exploradas.

1.3 Organização deste trabalho

Este trabalho está organizado da seguinte forma: o capítulo 2 contextualiza a cibersegurança; o capítulo 3 apresenta o referencial teórico base deste trabalho; enquanto que no capítulo 4 propõe-se um modelo para a elaboração de exercícios de cibersegurança e sua aplicação sobre uma das vulnerabilidades do TOP 10 da OWASP. O capítulo 5 traz as conclusões, margeando trabalhos futuros e, por fim, o capítulo 6 identifica as referências.

2 CONTEXTUALIZAÇÃO

No decorrer da história das guerras, novos domínios foram sendo explorados, da terra ao ar, passando pelas águas e chegando ao espaço. Cada novo domínio exige uma força de defesa e novas estratégias. A guerra cibernética ou ciberguerra é um novo campo de batalha das nações, sendo a quinta dimensão do setor de defesa: a defesa do ciberespaço. Em 6 de setembro de 2007, Israel invadiu a rede de defesa antiaérea síria e tomou o controle de suas telas de radar, enquanto a força aérea israelense, com seus F-15 Eagles e F-16 Falcons, atacavam uma central nuclear em construção, deixando anos de trabalho secreto totalmente destruídos (CLARKE; KNAKE, 2010).

As nações, como não poderia ser diferente, estão se movimentando, a fim de criar e de consolidar mecanismos e órgãos de atuação na ciberguerra diretamente ligados aos altos escalões da administração.

> Economias desenvolvidas estão, exatamente neste momento, como por exemplo EUA e Reino Unido, revisando ou lançando, respectivamente, suas estratégias nacionais de segurança cibernética, com uma sinalização forte do quanto há por fazer, principalmente em termos de cooperação internacional, legislação, normalização, e capacitação de recursos humanos especializados.(CANONGIA; JUNIOR MANDARINO, 2009).

No Brasil, após estudos do Departamento de Segurança da Informação e Comunicações (DSIC), publicou-se no Diário Oficial da União em 9 de Setembro de 2009 a Portaria No. 45, do Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República (GSIPR), instituindo o Grupo Técnico de Segurança Cibernética (GT SEG CIBER). Esse grupo tem como objetivos propor diretrizes e estratégias para a Segurança Cibernética ou Cibersegurança, no âmbito da Administração Pública Federal (CANONGIA e MANDARINO, 2009, p. 37).

Mas, afinal, o que se deseja proteger? O intuito é preservar a informação, o conhecimento e a imagem das organizações. Do ponto de vista da Nação, é resguardar as suas infraestruturas críticas (CONONGIA e MANDARINO, 2009). Os bens intangíveis são reconhecidamente o principal ativo para muitas organizações. Tradicionalmente, protegem-se os ativos clássicos em cofres, grades, ou através de seguros, mas, de forma similar, necessita-se proteger a informação e os bens

intangíveis das ameaças e dos incidentes de segurança. Para tal proteção as organizações devem dedicar esforços para prevenir e monitorar os incidentes relacionados às Tecnologias da Informação e Comunicação (TICs) em uso, minimizando assim os riscos e, consequentemente, tomando decisões precisas e rápidas, para garantir a continuidade do negócio e preservar seu principal ativo. Quando se trata das nações, a preservação das infraestruturas críticas, tais como: defesa, energia, saúde, transporte e telecomunicações, é um caso de Defesa Nacional.

> Está lançado o grande desafio, harmonizar duas dimensões, a primeira dimensão diz respeito à cultura do compartilhamento, da socialização, da transparência, da criação de conhecimento, e a segunda dimensão refere-se às questões de proteção, segurança, confidencialidade, e privacidade. (CANONGIA e MANDARINO, 2009, p.23).

Embora a Internet ofereça uma série de facilidades agilizando o fluxo de informações, as transações bancárias, o comércio eletrônico, enfim, um conjunto de serviços que tornam nossas vidas mais fáceis, a disponibilização dessas informações ou serviços os expõe à exploração de vulnerabilidades, a fim de obter privilégios.

> A empresa britânica Ultra Electronics estimou que o mercado mundial de segurança cibernética movimente cerca de US$ 50 bilhões anuais.
> E este mercado cresce 10% ao ano, duas vezes mais rápido do que o setor de tecnologia da informação, afirmou Denis Gardin, diretor do Cassidian Cyber Solutions, uma unidade do gigante europeu da aeronáutica e da defesa.(L'AGENCE FRANCE-PRESSE(AFP), 2012).

A importância econômica da cibersegurança cresceu significativamente nos últimos cinco anos. Grandes empresas de defesa adquiriram parte, ou a totalidade, de empresas de segurança da informação, visando a agregar mais cibersegurança às suas soluções e de salvar-se da crescente queda de investimentos dos estados nas áreas de defesa tradicional. Em 2009, Robert Gates, então secretário de defesa dos Estados Unidos, anunciou investimentos em ciberdefesa e, em Maio de 2011, o ministro da defesa britânica, Nick Harvey, disse que o desenvolvimento de armas cibernéticas é parte integrante do armamento das Forças Armadas (HEIN; WANDSCHEER, 2011), o que acelerou o interesse das indústrias de equipamentos militares por ciberdefesa. Em 2010, a Cloudshield Technologies foi adquirida pela Sciences and Applications International Company (SAIC), que é um dos maiores

provedores de soluções para os segmentos militar, energia e saúde, com cerca de 40.000 funcionários ao redor do mundo (SAIC, 2011).

> Empresas de armamentos estão aproveitando essa onda. A norte-americana Lockheed Martin, líder no mercado, já abriu seu segundo centro de cibertecnologia, onde simula ataques cibernéticos. A Boeing adquiriu várias firmas especializadas no setor. E também o maior grupo aeroespacial e de armamentos da Europa, o EADS, quer lucrar com o negócio das armas digitais, planejando construir a própria empresa de segurança em TI, sob a égide de sua empresa de segurança, a Cassidian.(HEIN; WANDSCHEER, 2011).

As empresas brasileiras confirmam a importância econômica do setor, segundo pesquisa realizada anualmente pela consultoria PricewaterhouseCoopers (PwC) e pelas revistas CIO[3] e CSO[4]. Apesar do cenário de crise[5], pelo segundo ano consecutivo, executivos afirmaram que as empresas vão aumentar o investimento em segurança da informação no próximo ano, conforme elucida a Figura 4 ("Pesquisa Global de Segurança da Informação 2012," 2012).

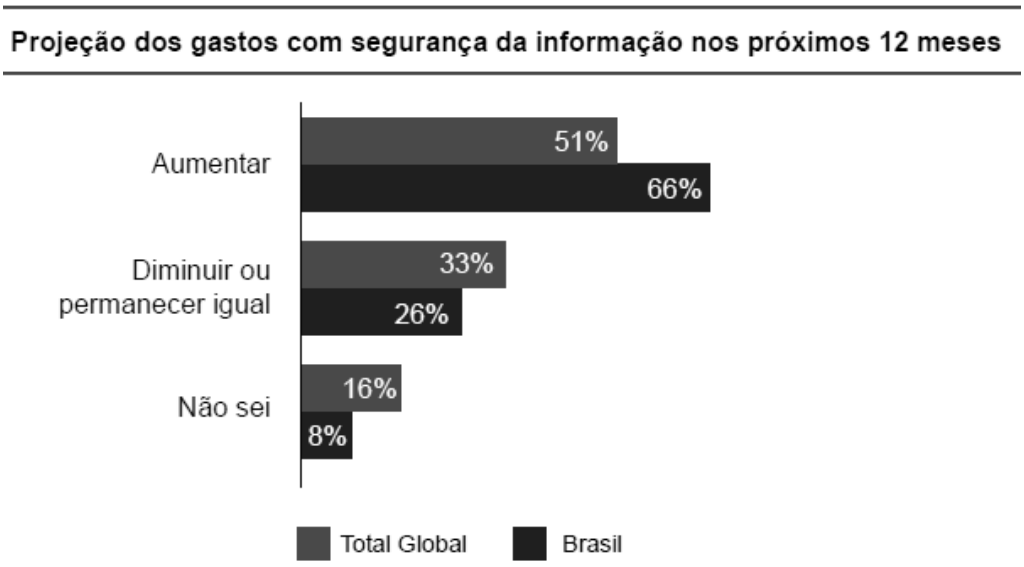

Figura 4 - Projeção de investimentos em segurança da informação

Com o crescimento da computação em nuvem (FURHT, 2010), mais dados e serviços são disponibilizados e acessados pela internet, mais recursos físicos são compartilhados por diferentes pessoas e organizações. Isso está mudando o modelo

[3] do inglês *Chief Information Officers* (http://www.cio.com/).

[4] Vem do inglês *Chief Security Officers (http://www.csoonline.com/).*

[5] Crise dos subprimes iniciada em 2008 nos EUA incluindo a crise do Euro em 2011.

computacional e tornando necessária a adaptação das políticas de segurança, já que a falta de confiança na segurança é o principal entrave na adoção do modelo de computação em nuvem (ALMORSY; GRUNDY; MÜLLER, 2010). Outro fator que estimula o investimento em segurança são as vulnerabilidades inerentes dos softwares, que continuam sendo desenvolvidos sem o uso de práticas de minimização de falhas de segurança.

O item abaixo traz aprofundamentos sobre os problemas de mão de obra, e a possível alternativa brasileira para minimizá-los ou resolvê-los.

2.1 Definição do problema

No intento de disciplinar e de agregar segurança em sistemas computacionais, há diversas iniciativas que culminaram na criação de vários documentos normativos. Esses documentos foram disponibilizados principalmente na forma de orientações, metodologias e *frameworks*, criados em sua maioria por instituições públicas ou entidades privadas sem fins lucrativos.

A *Open Web Aplication Security Project* (OWASP) é uma comunidade aberta dedicada a promover o desenvolvimento de aplicações Web seguras. Entre outros projetos, a OWASP mantém o TOP 10, o qual visa a criar uma consciência sobre a segurança das aplicações mediante a identificação dos riscos mais críticos. O projeto é referenciado por diversos padrões e organizações, como MITRE, PCI DSS, DISA, FTC. O último OWASP TOP 10 foi lançado em 2010 e apresentou modificação em relação aos anteriores, como estimar o risco associado, em lugar de somente se basear na frequência da vulnerabilidade (WILLIAMS; WICHERS, 2010).

A fim de qualificar pessoas em cibersegurança, instituições públicas como academias militares e universidades, principalmente as estadunidenses, promovem competições e exercícios periodicamente, em que os alunos desempenham os papéis de atacantes e/ou defensores em um ambiente controlado e bem definido (PATRICIU e FURTUNA, 2009). Essa abordagem prática tem sido bastante aceita e utilizada para o ensino de defesa cibernética.

O principal desafio da cibersegurança e, consequentemente, da segurança na web é a formação de recursos humanos. Em um estudo realizado pelo Center for

Strategic & International Studies (CSIS), ligado à presidência dos Estados Unidos, intitulado *A Human Capital Crisis in CyberSecurity* dá uma panorama da falta de profissionais no país. Uma das conclusões do estudo revela que o problema é tanto de quantidade como de qualidade, especialmente quando se trata de profissionais altamente qualificados tecnicamente. Verifica-se não só uma escassez de pessoas necessárias para operar e suportar sistemas já implantados, mas também uma escassez ainda mais desesperada de pessoas que possam projetar sistemas seguros, escrever código seguro e criar as ferramentas - cada vez mais sofisticadas e necessárias - para prevenir, detectar, mitigar e reconstituir danos devido a falhas no sistema ou atos maliciosos (EVANS, 2010).

> According to interviews conducted with Jim Gosler, NSA Visiting Scientist and founding director of the CIA's Clandestine Information Technology Office, there are only about 1,000 security specialists in the United States who have the specialized skills to operate effectively in cyberspace; however, the United States needs about 10,000 to 30,000 such individuals. (EVANS, 2010)

Na estratégia brasileira de consolidação do setor cibernético na Defesa, a capacitação de recursos humanos constitui a atividade prioritária (Figura 5), uma vez que ela é indispensável para mobiliar os quatro vetores que integram o setor: a inteligência; a doutrina; a ciência, a tecnologia e a inovação; e as operações. Entre suas ações estratégicas, a capacitação prevê a parceria entre a Escola (EsNaDCiber) e as instituições públicas de ensino, junto ao MEC e ao MCT, sugerindo ao MEC ações de fomento na área de segurança e defesa cibernética (BARROS; GOMES; FREITAS, 2011).

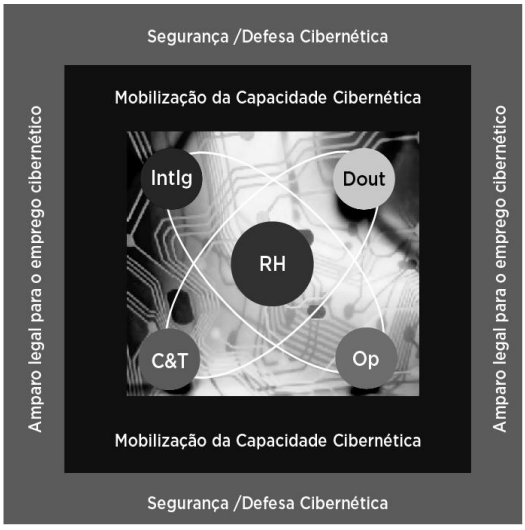

Figura 5 - Consolidação do Setor Cibernético na Defesa Nacional

3 REFERENCIAL TEÓRICO

3.1 Segurança da informação

A segurança da informação pode ser definida como a área do conhecimento responsável pela proteção contra as ameaças à informação, como bem intangível de pessoas físicas e jurídicas, com a finalidade de assegurar a continuidade do negócio e minimizar os riscos. Um exemplo de segurança da informação é evitar o acesso, a divulgação ou a alteração de informações por pessoas não autorizadas.

A segurança da informação segue alguns princípios, conforme estabelecidos na (“ABNT NBR ISO/IEC 27001:2005,” 2006):

- **Confidencialidade** - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- **Disponibilidade** - propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
- **Integridade** - propriedade de salvaguarda da exatidão e completeza de ativos.

Quando há a quebra de algum dos princípios de segurança, há uma violação de segurança.

3.2 Vulnerabilidade

Uma vulnerabilidade é um defeito ou fraqueza no projeto, na implementação ou na configuração de um sistema de informações, que pode ser intencionalmente ou acidentalmente explorada, violando a segurança da informação.

3.3 Risco

O risco à segurança da informação é o possível impacto negativo gerado pela exploração de uma vulnerabilidade, considerando a probabilidade do ataque e o impacto do ataque.

> O risco pode ser expresso matematicamente como uma função da probabilidade de uma origem de ameaça (ou atacante) explorar uma vulnerabilidade potencial e do impacto resultante deste evento adverso no sistema e, consequentemente, na empresa ou organização. (BRANDÃO; FRAGA, 2008).

Para contê-los há atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos (GUIDE, 2009).

3.4 Ameaças, Ataques e Intrusão

A **ameaça** cibernética é qualquer circunstância ou evento com potencial para afetar negativamente as operações ou ativos de uma organização ou indivíduo (incluindo missão, funções, imagem ou reputação), através de um sistema de informação via acesso não autorizado, destruição, modificação, divulgando informações e/ou negando serviços. (NIST e STONEBURNER, 2002)

Considerando que a vulnerabilidade é a falha que não necessariamente apresenta risco, a ameaça é a circunstância potencial de exploração intencional ou acidental da vulnerabilidade.

Nesse sentido, atos intencionais que podem produzir violações de segurança são chamados de **ataques**. Finalmente, quando um ataque é bem sucedido, afirma-se que houve uma **intrusão**. (BRANDÃO e FRAGA, 2008)

A Figura 6, a seguir, demonstra as diferentes rotas possíveis de exploração das vulnerabilidades em aplicações web (WILLIAMS; WICHERS, 2010).

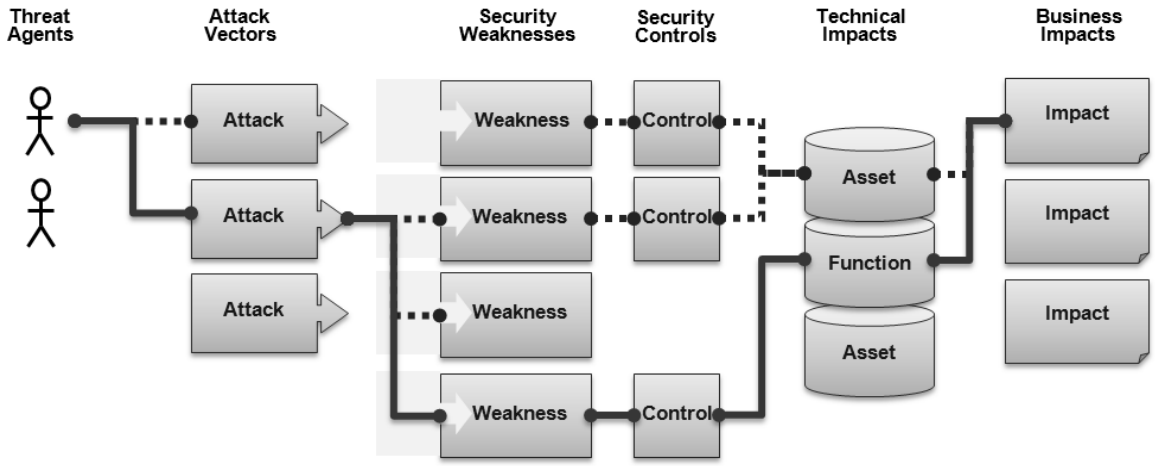

Figura 6 - Rotas de Ataque

Para determinar os riscos a cibersegurança, deve-se avaliar a probabilidade associada com cada agente da ameaça, vetor de ataque e a vulnerabilidade. Em seguida, é preciso combiná-la com as estimativas de impacto tecnológico e de impacto ao negócio.

3.5 Criação de Exercícios de Cibersegurança

Exercícios de cibersegurança são eficientes para se aprender de maneira prática aspectos da segurança. Entretanto, projetar esses exercícios não é trivial, pois demanda tempo e exige bastante trabalho. É necessário seguir metodicamente algumas diretrizes, modelos e formatos para elaboração, principalmente no caso de projetistas pouco experimentados, nutrindo-se de experiências e de resultados vivenciados por outras equipes.

Exercícios são usados há vários anos como atividade final de alunos de graduação em universidades Estadunidenses (HOFFMAN et al., 2005). Entre e dentro das universidades dos Estados Unidos são organizadas competições, a fim de avaliar os conhecimentos em segurança dos alunos, os quais desempenham os papéis de atacante e de defensores.

Um guia para a criação de exercícios de cibersegurança para universidades é apresentado por Victor-Valerio Patriciu e Adrian Constantin Furtuna (2009). Os passos para a elaboração foram sintetizados a partir de diferentes trabalhos acadêmicos, relatando exercícios educacionais de cibersegurança. A principal

contribuição que o artigo, intitulado *Guide for Designing Cyber Security Exercises,* oferece é um método geral para organizar novos exercícios, podendo ser personalizado de acordo com as necessidades do organizador. Embora seja grande a diversidade nas estruturas, objetivos e abordagens dos distintos tipos de competições, os autores estabeleceram as características básicas, comuns à maioria, utilizadas na construção do guia.

> To address this diversity, this guide can be used as a starting point for any university that wishes to organize its own cyber security exercise / competition. In this case, the exercise would best fit as a capstone project for last year students, which already have an Information Assurance background.(PATRICIU; FURTUNA, 2009).

3.5.1 Etapas de elaboração

O guia elaborado por Patriciu e Furtuna (2009) elenca os passos para a criação de exercícios e estabelece que o exercício tenha objetivos bem definidos. De acordo com os objetivos, define-se a abordagem específica na concepção do exercício, o hardware e o software que serão utilizados e qual será a sua topologia. Com a topologia e os objetivos, constrói-se o cenário e o contexto. Enquanto as regras são definidas a partir do cenário e dos objetivos. Já as métricas medem a eficiência no exercício e são baseadas nos objetivos. Para finalizar, coletam-se as lições aprendidas pelos participantes e organizadores. A sequência de passos pode ser observada na Figura 7.

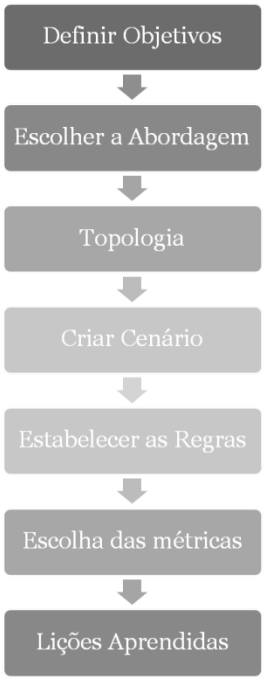

Figura 7 - Etapas de Criação

Segundo Patriciu e Furtuna (2009), em geral, os exercícios de segurança cibernética têm dois lados: os atacantes e os defensores. Em cada lado, há sistemas computacionais gerenciados pelas equipes para atacar ou serem defendidos. Tipicamente, os componentes dos exercícios são cinco:

- Equipe de defensores;
- Sistema alvo;
- Infraestrutura;
- Equipe atacante;
- Sistema de Ataque.

3.5.2 Definição dos objetivos dos exercícios

Os objetivos dos exercícios de cibersegurança podem ser divididos em duas categorias: segurança ofensiva e defensiva, como é proposto no citado guia. Segurança defensiva prepara genericamente para gerenciar a segurança. Patriciu e Furtuna (2009) mencionam como um bom exemplo de segurança defensiva a competição anual *Ciber Defense Exercise* conhecida por CDX.

> The defensive security training prepares the participants for the generic job of security administrator. Their main goal is to be experts in configuring and managing various security equipments.(PATRICIU e FURTUNA, 2009).

Por sua vez, a segurança ofensiva prepara genericamente os participantes para fazer teste de penetração[6] ou teste de invasão (UTO e MELO, 2009). A grande vantagem da segurança ofensiva é treinar o pensamento como se fosse um invasor.

> This type of training prepares the participants for the generic job of penetration tester and helps them "think like the enemy", in a proactive manner.(PATRICIU; FURTUNA, 2009).

Essas categorias não são disjuntas e sim complementares, porque um gerente de segurança precisa conhecer quais e como são os ataques utilizados, a fim de preparar as defesas, e um *pentester* deve saber quais os métodos utilizados para defender um sistema, a fim de tentar transpô-los ou evitá-los.

3.5.3 Escolha da abordagem

A abordagem é consequência dos objetivos definidos anteriormente. Para capacitar administradores de segurança, adota-se uma abordagem defensiva e, para formar testadores de invasão, adota-se uma abordagem de ataque. Porém, os exercícios mais completos adotam as duas, ou seja, ataca-se e defende-se no mesmo exercício.

Na abordagem defensiva, treina-se e pratica-se os métodos que devem ser utilizados antes, durante e depois de um ataque. Esses métodos estão intimamente relacionados com as tarefas de administração de sistemas e atividades forenses. A segurança é um processo contínuo. Conforme Patriciu e Furtuna (2009), pode-se dividir o processo de defesa nas ações:

- Criar uma política de segurança;
- Implementar medidas de segurança;
- Monitorar o estado da segurança;
- Testar a segurança;
- Aumentar a segurança.

[6] Vem do inglês **penetration test**, ou **pentest**

Essas são as ações do Ciclo da Segurança usadas com o propósito de garantir o ativo defendido e de monitorar sua atividade, a fim de perceber ataques e evitar (ou diminuir) suas consequências, aumentando a segurança.

Na abordagem dos exercícios orientados à defesa[7], há pelo menos três formas de organização:

- Fornecer os requisitos e serviços a serem providos pelos participantes através de ferramentas desenvolvidas por eles;
- Ofertar instalações padrão a serem configuradas e protegidas; e
- Disponibilizar sistemas configurados para serem defendidos.

Na abordagem ofensiva, os participantes aprendem como são feitos os ataques e consequentemente a melhor forma de defender-se deles. O Ataque real é simulado geralmente contra vários alvos, colocando os participantes na posição de atacante e fazendo-os pensar como um. Essa abordagem de ataque ajuda principalmente a localizar posteriormente falhas em seus sistemas, testando técnicas de ataques aprendidas. As ações de ataque típicas são (PATRICIU; FURTUNA, 2009):

- Executar o reconhecimento;
- Procurar e enumerar;
- Ganhar acesso ou executar DoS[8];
- Escalar privilégios;
- Manter o acesso;
- Cobrir rastros e criar blackdoors.

O sistema alvo pode ser previamente configurado com vulnerabilidades, podendo, mas não necessariamente, ser administrado por alguém durante o ataque.

A abordagem Mista combina a defensiva e a ofensiva, sendo a mais abrangente para ciberexercícios. Os participantes são divididos em duas equipes: a dos defensores e a dos atacantes.

[7] Nestes exercícios, o atacante pode ser o instrutor.

[8] denial-of-service attack (DoS attack) ataque de negação de serviço

3.5.4 Definir topologia de rede

Nesta etapa, define-se a infraestrutura, a forma de conexão, os computadores e os sistemas que serão utilizados no exercício. A topologia de rede deve condizer com os objetivos aos quais se quer treinar. No caso de aplicações web, é pouco relevante já que os ataques e defesas concentram-se nas aplicações, nos sistemas e não em possíveis falhas de redes, do meio. Em geral, considera-se que a rede é insegura, portanto, toda informação sigilosa que trafegar em claro é uma vulnerabilidade.

3.5.5 Criação de cenário

A apresentação aos participantes dos exercícios de cibersegurança é o próximo passo. O centro desse passo é uma intrigante e entusiasmante história, que simula uma situação real em que se tenha que atacar ou defender. O cenário descreve o ambiente que está sendo simulado e a sequência lógica dos fatos. Podendo conter ou simular um ambiente de trabalho, segundo os autores, em:

> As part of the scenario, the participants could be asked to perform business related tasks during the exercise, in order to simulate a real working environment.(PATRICIU; FURTUNA, 2009).

Objetivos realistas de ataque tornam o cenário mais real. Em geral, os objetivos de ciberataques foram categorizados da seguinte forma (PATRICIU; FURTUNA, 2009):

- Acesso a dados confidenciais;
- Negação de serviço;
- Controle de máquinas.

Esses, consequentemente, também são os ataques que os defensores não devem permitir que aconteçam. E os alvos? Do ponto de vista lógico, são:

- Os serviços;
- As redes de computadores;
- As pessoas;
- As relações de confiança.

3.5.6 Conjunto de regras

O conjunto de regras estabelece as diretrizes de execução dos exercícios. Patriciu e Furtuna (2009) defendem uma divisão das regras em:

- As regras gerais – explicitam a forma de execução do exercício, bem como as ferramentas que serão utilizadas, o tempo da competição, o papel das equipes ou participantes, as formas de comunicação durante o exercício e as penalidades, caso as regras sejam quebradas;
- Mecanismo de pontuação – deve ser transparente, ou seja, as regras devem incluir a forma de ganho de pontos, ações que valem pontos, que perdem pontos ou sem valor. Os mecanismos de pontuação devem incluir as condições de finalização e de determinação do vencedor;
- Elegibilidade – quem pode ou não participar do exercício é determinado pelas regras de elegibilidade, ou seja,os requisitos para participar da competição;
- Questões Legais – a legalidade do treinamento passa pela observação das leis e normativas das instituições, nas quais o exercício está sendo realizado, física ou virtualmente. Alguns tipos de testes são proibidos em determinados países, independente de que a motivação seja ou não educacional;
- Limitações - por fim, as regras de limitações impõem aos participantes o escopo do exercício, o que pode ser realizado; e aos coordenadores, a forma de interação com os participantes. As limitações podem ser por restrições ou por exclusões. Por exemplo, uma restrição pode forçar a usar determinado tipo de defesa com finalidade de que sejam treinados os conhecimentos nesse tipo específico.

3.5.7 Métricas

As métricas são as medidas realizadas para saber se os objetivos foram alcançados. Quanto mais adequadas forem as métricas em relação aos objetivos, mais precisos serão os indicativos de sucesso. Por exemplo, para um ataque distribuído de negação de serviço, do inglês *Distributed Denial of Service* (DDoS), uma métrica interessante seria o tempo que o serviço ficou fora do ar em relação ao

tempo de ataque. Escolher as métricas exige bastante conhecimento, certamente uma das fases mais difíceis da elaboração.

3.5.8 Lições Aprendidas

Para finalizar, realiza-se uma discussão sobre as lições aprendidas com a realização do exercício. Em uma atividade de aprendizagem, é natural observar que essa finalização é extremamente importante para a eficácia da mesma.

> The organizers should find an appropriate mechanism for gathering feedback from the participants (e.g. evaluation forms at the end of the exercise)(PATRICIU; FURTUNA, 2009).

Essa discussão sobre as técnicas e ferramentas que cada participante usou maximiza a experiência de cada participante com as contribuições dos demais, registrando o resultado em um relatório a ser divulgado posteriormente, para que os participantes tenham a visão geral do que aconteceu no exercício, assim como isso sirva para consultas posteriores.

3.5.9 Conclusões sobre o guia

O Guia de elaboração é de uso geral e ajuda a definir cada uma das etapas necessárias para a elaboração de exercícios educativos de cibersegurança. Pode ser adaptado ao tipo de exercício a ser realizado, encurtando ou prolongando uma etapa ou outra do desenvolvimento. Patriciu e Furtuna (2009) conseguiram transmitir experiência vivenciada e absorvida de outros artigos nesse guia, tornando-o leitura fundamental na criação de exercícios de segurança da informação.

3.6 Competições de Cibersegurança

As competições de cibersegurança são o exercício mais próximo da realidade a ser enfrentada por um profissional de segurança. Elas envolvem diversos conhecimentos referentes à segurança da informação em um único exercício.

A Academia Militar de West Point lançou um desafio às outras cinco academias militares estadunidenses para participar de um exercício, interacadêmicas, de defesa cibernética apresentado no artigo *The cyber defense exercise: an evaluation of the effectiveness of information assurance education*.

O Centro de Operações e Tecnologia da Informação (ITOC) criou o Centro de Análises e Pesquisa na Segurança da Informação (IWAR), o qual foi desenhado para dar suporte a graduandos e pesquisadores da academia militar, tendo em mente que no futuro todas as academias poderiam ter pesquisas nessa área, podendo, assim, compartilhar informações e descobertas.

A proposta do curso de IA[9] é dar aos alunos (cadetes) uma amostra das ferramentas dos adversários, assim como das vulnerabilidades atuais dos sistemas de informação e como elas podem ser exploradas. Isso levou à criação de um espaço específico para testes e aprendizado. Este espaço, batizado de "sandbox" é um local seguro e isolado, onde é permitida a utilização dos testes para estudo e para os professores verificarem o desempenho de seus alunos (SCHEPENS, 2002).

O IWAR foi dividido em 4 redes:

- Gray Network: é o lado atacante do laboratório. Os cadetes usavam máquinas virtuais para executar diferentes sistemas operacionais;
- Gold Network: é o lado dos servidores alvos. Nesse lado da rede, os cadetes usavam suas ferramentas para analisar e pôr em pratica seus conhecimentos, bem como verificar os resultados;
- Black Network: pode ser utilizada tanto para ataque, como para a defesa. Ela também permitia aos professores desenvolver pesquisas de forma isolada;
- Green Netkwork: permitia aos cadetes explorar as vulnerabilidades nos sistemas táticos do exército.

Também havia dois computadores desconectados da rede de ataques, esses computadores eram usados para a procura na internet de novas ferramentas que poderiam ser úteis nas outras máquinas.

A construção de toda a estrutura demandou tempo e recursos, mas o curso respondeu a todo esforço, oportunizando aprendizado prático aos estudantes, os quais gratificaram a organização do curso, útil em suas carreiras. A competição não permitia aos cadetes se ramificarem em muitas áreas, entretanto, ela proporcionou

[9] information assurance

aos cadetes a experiência em segurança da informação que pode ser utilizada na proteção e na defesa das informações do exército (SCHEPENS, 2002).

3.6.1 Implementação do laboratório

O local deve ser isolado e ter um cenário que dê maior realismo aos estudantes, isso é importante na preparação dos integrantes para situações reais de defesa cibernética. Além disso, a infraestrutura de rede deve ser pensada, a fim de que não haja nenhum tipo de conexão física com outras redes fora do laboratório, com o objetivo de evitar acidentes. Nesse ponto, deve-se recorrer aos objetivos para determinar o sistema alvo e o hardware necessário para a prática. E o hardware deve ser o mais homogêneo possível, para dar as mesmas condições de comunicação entre as máquinas. (SCHEPENS, 2002)

Os principais sistemas operacionais utilizados foram as distribuições do Unix (RedHat, Solaris), Linux (BackTrack), Windows e Macintosh, os quais são empregados de uma forma heterogênea para simular a rede real de computadores. Pode-se implementar também uma máquina central, que acompanha as anomalias causadas pelos ataques, a efetividade da defesa e a minimização dos impactos na rede.

3.7 Aprendizagem experiencial

Sob a perspectiva de Kolb, o homem é um ser integrado ao meio natural e cultural, capaz de aprender a partir de suas experiências. Porém, não significa que qualquer vivência resulte em aprendizagem. A aprendizagem é um processo cognitivo, sendo assim, tornar próprios os saberes procedentes da experiência demanda processos contínuos de ação e reflexão. Pelo olhar de Kolb, a experiência é o caminho para o desenvolvimento. Nesse sentido, as experiências de aprendizagem levam ao desenvolvimento porque dirigem a uma meta, a um propósito especifico de aprendizado (PIMENTEL, 2007). Kolb define aprendizagem experiencial como:

> o processo por onde o conhecimento é criado através da transformação da experiência. Esta definição enfatiza que o conhecimento é um processo de transformação, sendo continuamente criado e recriado... A aprendizagem

> transforma a experiência tanto no seu caráter objetivo como no subjetivo... Para compreendermos aprendizagem, é necessário compreendermos a natureza do desenvolvimento, e vice-versa.(KOLB, 1984)

A teoria Kolbiana sustenta-se no conceito de zona de desenvolvimento proximal de Vygotsky. De forma simplista, esse conceito diz respeito à formulação de novos conhecimentos pelo contexto histórico-cultural, ou seja, a construção do desenvolvimento profissional a partir dos conhecimentos pré-existentes.

> A aprendizagem experiencial coloca a ênfase na interação entre o sujeito e a ação e sustenta as novas aprendizagens na experiência, ao mesmo tempo em que valoriza o contexto e a reflexão. Mas, ao valorizar também o lado funcional da aprendizagem, sua exteriorização social, adquire uma dimensão pragmática que ... é essencial porque promove a resolução de problemas pelos atores envolvidos, mas também por conceder a estes o poder de os resolver e a consciência de que detêm esse poder.(ALARCÃO, 2002)

Parafraseando Pimentel (2007), aprender é um processo permanente e incremental, impulsionado pela experiência. No entendimento de Kolb, o desenvolvimento é representado por três níveis sucessivos e multilineares:

- **Aquisitivo** – identificação, reconhecimento e registro dos objetos envolvidos na ação;
- **Especializado** – consciência interpretativa, organização em redes de significação;
- **Integrado** – estágio mais complexo do desenvolvimento, manifestado pela segurança e autoafirmação quanto pela necessidade de novas mudanças. Identificado pela confrontação existencial podendo ser um processo lento ou repentino desencadeado por forte carga afetivo-emocional.

Segundo Pimentel (2007), da relação entre aprender, conhecer e desenvolver, o ciclo de aprendizagem experiencial é constituído de quatro modelos adaptativos de aprendizagem, no qual se combinam preensão e transformação. Os modelos:

- **Experiência concreta (CE)** – contato direto com problemas a serem resolvidos. Enfática nas experiências pessoais e nos sentimentos envolvidos na aprendizagem;

- **Observação reflexiva (RO)** – reflexão sobre os fatos concretos da experiência tais como: identificação de elementos, associações, agrupamentos e caracterização. Segundo Trevelin (2011), com paciência, o aprendiz utiliza a habilidade de entender ideias de diversos pontos de vista;
- **Conceituação abstrata (AC)** – generalização dos elementos e características da experiência, comparação com realidades semelhantes. O entendimento é baseado na compreensão intelectual da situação, exigindo elevado nível de abstração;
- **Experiência ativa (AE)** – aplicação prática dos conhecimentos tornados refletidos, explicados e generalizados. Centrados na socialização do conhecimento e do trabalho em equipe. As pessoas deste modelo gastam bastante tempo experimentando situações, mudando as variáveis e formulando hipóteses.

Enquanto a **preensão** liga o concreto ao abstrato, a **transformação** liga a ação à reflexão. A aprendizagem por **preensão** combina a experiência concreta à conceituação abstrata, implicando dois processos opostos:

- **Apreensão** – aprendizagem diretamente ligada à experiência concreta, intuitiva e instantânea;
- **Compreensão** – processo mental, interpretativo, abstrato e conceitual da experiência.

Por sua vez, a aprendizagem por **transformação** dá-se através da combinação entre observação reflexiva e experiência ativa. A representação simbólica se baseia nos processos opostos intenção e extensão:

- **Intensão** – interiorização do aprendizado, reflexão intencional, consciente e voluntária.
- **Extensão** – exteriorização da experiência, socialização do conhecimento. Colocar a prova o que se apropriou, observou e conceituou anteriormente.

Na Figura 8, a seguir, é apresentado o ciclo de aprendizagem de Kolb, no qual as setas entrecruzadas indicam as duas dimensões que unem a ação prática e a teorização. Nos retângulos, os quatro modelos de desenvolvimento; já os textos curvos referem-se aos sistemas de pensamento e, finalmente, nas elipses, as modalidades de aprendizagem (PIMENTEL, 2007).

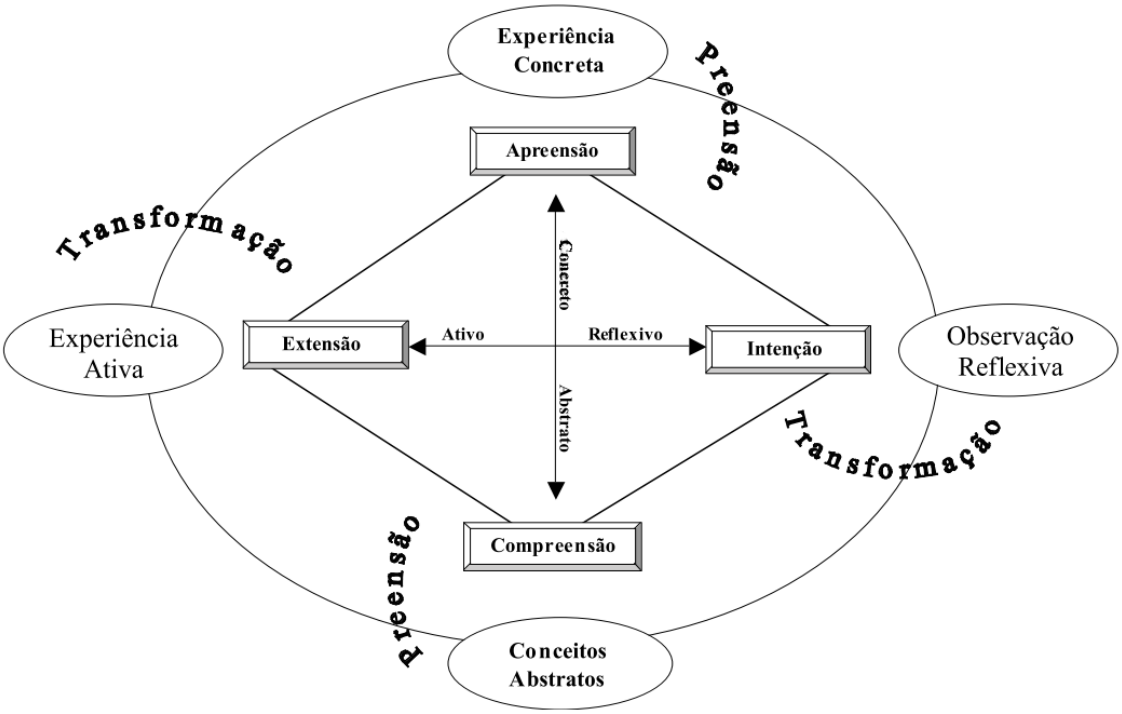

Figura 8 - Ciclo de aprendizagem de Kolb

Pimetel (2007) explica o ciclo de aprendizagem de Kolb:

> Esse ciclo quadrifásico de aprendizagem experiencial pode iniciar a partir de quaisquer das modalidades, resultando em formas distintas de intervir na realidade e aprender com a experiência. Supondo-se o início pela experiência concreta, segue-se a observação sobre as condições da experiência, sua meta e as ações erigidas. Nessa etapa, o exemplo advindo da experiência imediata é compreendido, propiciando o exame e a seleção de ações que possam ser aplicadas a circunstâncias semelhantes, a fim de antecipar novas experiências e projetar ações plausíveis. Em seguida, o foco se dirige à descoberta de princípios gerais, são erigidas hipóteses explicativas, não apenas cabíveis ao exemplo particular, mas de caráter mais conclusivo, úteis para novas situações de aprendizagem. Finalmente, os conhecimentos e desenvolvimento resultantes podem ser testados, na experiência ativa, a partir da qual o ciclo se renova de modo ascendente e contínuo. (PIMENTEL, 2007)

Quando a disciplina é teórica, o ensino por conceituação abstrata não chega a ser um problema. No entanto, quando o conhecimento exige prática, a

aprendizagem é dificultada. Os alunos têm dificuldades de sair das abstrações e chegar à prática. Ensina-se o conceito “o que” e exige-se aplicação prática “e se” (TREVELIN, 2011).

> ... o professor articula bem o raciocínio em nível abstrato, consegue visualizar a solução, mas não a transforma em uma sequência de passos estruturados, dificultando a transposição da teoria (abstração) para a prática (experiência concreta) por parte dos alunos. (TREVELIN, 2011)

Além dos quatro tipos de estágios do ciclo de aprendizagem, é preciso entender os quatro tipos de estilos de aprendizagem. O estilo de aprendizagem de cada indivíduo combina dois dos quatro estilos de aprendizagem como descreve Trevelin (2011):

- **Divergente** (observador) – **Por quê?** – Integra experiência com seus valores; prefere ouvir e partilhar ideias; é criativo; tem facilidade para propor alternativas e reconhecer problemas; gosta de saber o valor do que irá aprender;
- **Assimilador** (pensador) – **O quê?** – Integra experiência com o conhecimento existente; utiliza a dedução para resolver problemas; trabalha bem com detalhes e dados; procura assimilar novas ideias e pensamentos; é mais interessado pela lógica de uma ideia do que pelo seu valor prático;
- **Convergente** (examinador) – **Como?** – Integra teoria e prática; utiliza tanto a abstração quanto o senso comum na aplicação prática das ideias e teorias; procura sempre a melhor solução para um problema prático; gosta de resolver problemas práticos. É melhor com tarefas técnicas e resolução de problemas do que com eventos sociais e interpessoais;
- **Acomodador** (atuador) – **E se?** – Integra a experiência com sua aplicação e faz imediata aplicação de nova experiência. É altamente ativo e criativo. Aprende por tentativa e erro e desenvolve novos conhecimentos;

Observa-se que a teoria de Kolb (1984) fornece subsídios para minimizar as dificuldades de aprendizado em segurança cibernética. Para alcançar maior eficiência e alcançar os aprendizes de maneira significativa, deve-se passar pelos quatro quadrantes trabalhados (Figura 9), experiência concreta (CE), observação reflexiva (RO), a conceituação abstrata (AC) até experiência ativa (AE).

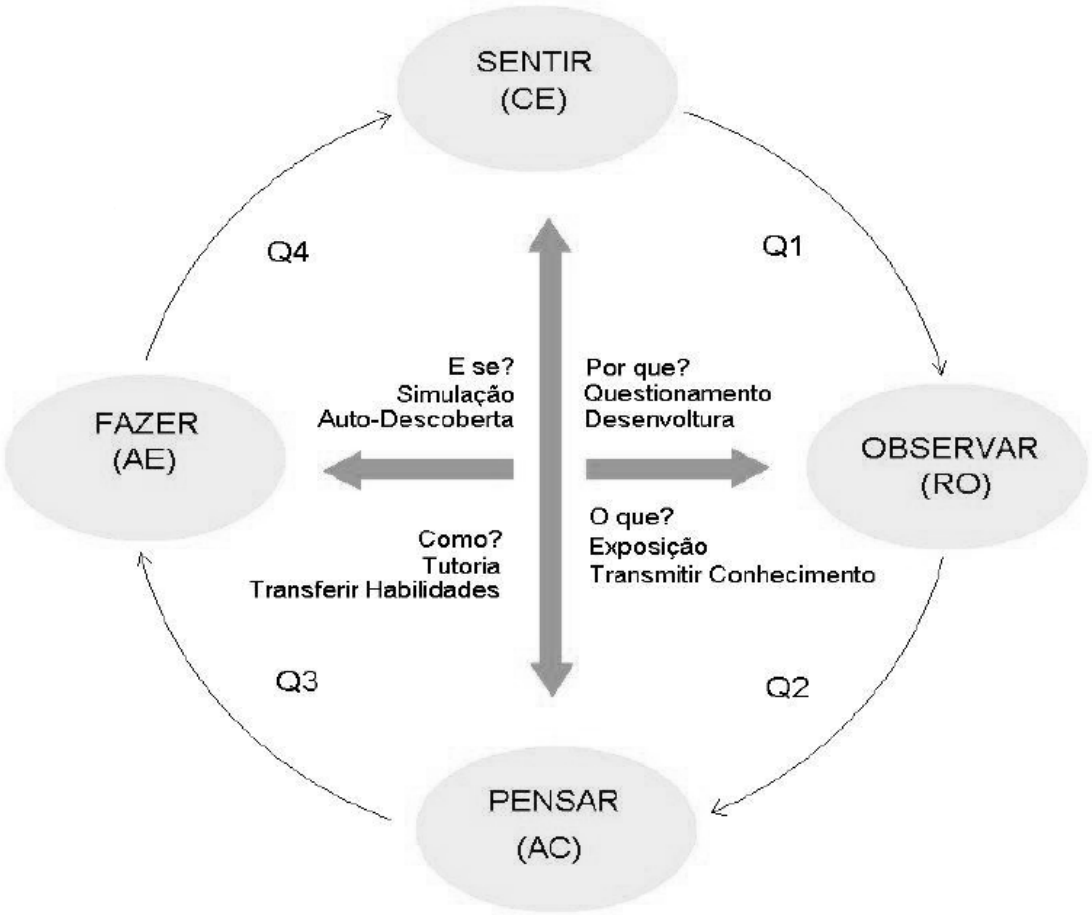

Figura 9 - Ciclo de aprendizagem (Trevelin, 2011)

> ... se o aluno tiver contato com apenas o quadrante AC, haverá apenas 20% de retenção da aprendizagem, se este mesmo aluno tiver contato com os quadrantes RO e AC, a retenção ficará em 50%, se forem usados os quadrantes CE, RO e AC em conjunto a retenção da aprendizagem passará a 70% e utilizando-se todos os quadrantes a retenção será de 90%. Assim, quanto mais quadrantes forem utilizados, maior será a retenção de conhecimento dos alunos. (KOLB; BAKER; DIXON, 1985).

O Artigo *A Comparison of Preferred Learning Styles, Approaches and Methods between Information Science and Computing Science Undergraduates* demostra outras diferenças menos óbvias - do que ciência da computação tem menos mulheres que sistema da informação - por meio de uma pesquisa online com

graduandos do primeiro ano utilizando o inventario de Kolb. Ele relata a diferença entre os estilos de aprendizagem, abordagens para estudar e ambientes de aprendizagem. (WISHART, 2005)

Outras metodologias podem ser utilizadas para ensino de tecnologia e, consequentemente, de segurança da informação, além da experimental de Kolb (1984), a teoria construtivista de Jean Piaget, ou do construcionismo de Seymour Papert. MACHADO e MAIA (2004) utilizaram o construtivismo para propor melhorias no aprendizado de sistemas operacionais. Papert (1987) trabalha o ensino intermediado por computador, mais especificamente através da linguagem LOGO[10], sendo referência para diversos trabalhos envolvendo tecnologia e educação.

[10] Linguagem de programação interpretada, voltada principalmente para crianças.

4 MODELO PARA A CRIAÇÃO DE EXERCÍCIOS DE ATAQUE E DE DEFESA EM APLICAÇÕES WEB

Este capítulo apresenta um modelo para a elaboração de exercícios de cibersegurança para as vulnerabilidades web. O modelo toma por base o guia de elaboração proposto por Patriciu e Furtuna (2009) e se fundamenta na aprendizagem experiencial elaborada por David Kolb (1984). A teoria dos estilos de aprendizagem de Kolb sugere que o tutor trabalhe o processo de ensino/aprendizagem passando pelos quatro quadrantes do ciclo (Figura 9) “Por quê?”, “O quê?”, “Como?”, “E se?”, atingindo os diferentes estilos de aprendizagem.

O projetista do exercício inicialmente escolherá a vulnerabilidade e os **objetivos** educacionais, que são as formulações explícitas das mudanças que se espera que ocorram nos aprendizes durante o processo educacional (BLOOM; ENGELHART; FURST, 1973). Definidos os objetivos, escolhe-se a **abordagem** a ser tomada: defensiva, ofensiva ou ambas.

A topologia típica dos exercícios com vulnerabilidade web é uma ou mais máquinas virtuais cliente e uma ou mais máquinas virtuais para servidores (web, banco de dados, autenticação, firewall de aplicação). Mas pode-se usar máquinas físicas diferentes para cliente e servidor, com o uso ou não de switchs, porém sempre isoladas do resto da rede.

A utilização dos documentos oferecidos pela OWASP nesse momento se torna imprescindível. Tais documentos ajudam a identificar as vulnerabilidades a serem trabalhadas, além de reconhecer a identidade dos agentes; dos vetores de ataque; as deficiências de segurança: a frequência e a detecção; bem como o nível de impacto: técnicos e para o negócio.

4.1 Por quê?

Nesse quadrante do círculo, o aprendiz gosta de saber o porquê de estar aprendendo sobre determinada vulnerabilidade. Então, o tutor deve mostrar a

importância de conhecer a vulnerabilidade e tornar a ligação com a realidade facilmente assimilável. Além disso, deve afastar a ideia de que tal conhecimento não será utilizado. Fazendo, portanto, a apresentação dos problemas relacionados à vulnerabilidade e a relevância de mitigar os riscos relacionados a ela, nesta fase, não se usa terminologia técnicas em demasia, optando-se por um vocabulário mais informal. Dessa forma, é possível utilizar: uma exposição simples, fotos, vídeos, seminários. Então, nesse quadrante apresentam-se as seções:

- Apresentação da vulnerabilidade;
- Agentes de ameaça – quem pode explorar essa vulnerabilidade: administradores, usuários; forma de exploração: via navegador, injeção, cabeçalho; quais os objetivos do atacante; qual o nível de dificuldade para explorar a vulnerabilidade;
- Impactos – quais os impactos de um possível ataque, tanto impactos técnicos quanto para o negócio, ou seja, os riscos associados à ameaça.

4.2 O quê?

Neste quadrante, a comunicação é fundamental já que o tutor emite informações, e uma recepção por parte do aprendiz deve se converter em conhecimento. Três são os tipos de comunicação: Unilateral, Bilateral e Multilateral. (TREVELIN, 2011).

Nessa etapa, expõem-se os conceitos ligados à defesa da ameaça e/ou necessários ao ataque utilizando conceituação formal, típico de uma aula expositiva. A apresentação deve ser direcionada pelos objetivos educacionais, o que se deve saber sobre a vulnerabilidade. É importante promover além da comunicação unilateral tutor/aprendiz, a comunicação bilateral tutor/aprendiz; aprendiz/tutor e a multilateral tutor/aprendiz, aprendiz/tutor e aprendiz/aprendiz, promovendo uma postura questionadora e curiosa. As seções:

- A abordagem – ataque, defesa e/ou ambos;

- Os objetivos – apresentam-se os objetivos de aprendizagem, os objetivos educacionais, os objetivos do exercício;
- Vetores de ataque;
- Deficiências na Segurança;
- Dificuldade de exploração;
- Cenário – simula-se uma situação real, através de uma história cativante, intrigante; um enredo; uma trama; para motivar o aprendiz, para colocá-lo dentro da história, deve-se mexer com seus valores e sentimentos;
- Regras – explicitam a forma de execução do exercício, bem como as ferramentas que serão utilizadas; o tempo da competição; o papel das equipes ou participantes; as formas de comunicação durante o exercício; as penalidades, caso as regras sejam quebradas; os mecanismos de pontuação; a elegibilidade; os requisitos para participar; as questões legais; as limitações, determinando o escopo do exercício.

4.3 Como?

Aqui o aprendiz vai usar os conhecimentos adquiridos no quadrante anterior, a fim de realizar um ataque e/ou defesa em uma vulnerabilidade específica, com o conteúdo aprendido deve chegar à solução. Este quadrante deve exigir somente a aplicação dos conceitos e das técnicas apresentadas. Além disso, é aqui que deve ocorrer a sedimentação do conhecimento teórico. Utiliza-se, portanto, a aprendizagem baseada em problemas, método de instruções caracterizado pelo uso de situações reais como cenário, com a finalidade de criar uma postura crítica e as habilidades para solucionar problemas.

> A Aprendizagem Baseada em Problemas pode ocorrer tanto de maneira individual como em pequenos grupos, porém, é no grupo de tutoria que o pensamento crítico pode ser encorajado e argumentos levantados, ideias podem ser construídas de maneira criativa, novos caminhos podem ser

> estabelecidos, permitindo a análise coletiva de problemas que espelhem a prática profissional futura. (TREVELIN, 2011).

Neste quadrante, apresenta-se **uma proposta de resolução** para o exercício exposto no passo anterior. Ela permite que o aprendiz possa seguir a resolução do exercício juntamente com a topologia, o software e o hardware.

4.4 E se?

No quadrante anterior, há certa previsibilidade e confiança no que se vai encontrar e fazer sobre determinada vulnerabilidade. Aqui, no quarto quadrante, o aprendiz deve utilizar o que já aprendeu em novas situações nas quais não se tem o domínio completo dos dados fornecidos.

A técnica de aprendizagem por descoberta mostra-se adequada para trabalhar neste quadrante, pois

> ... a descoberta é uma condição necessária para a aprendizagem das diversas técnicas para a solução de problemas. A prática na descoberta ensina a adquirir informação de uma forma tal que a mesma se torne mais viável na solução de problemas. (TREVELIN, 2011) apud (RONCA, 1985).

Nesse sentido, solicita-se uma resolução dos aprendizes, oferecendo-lhes o cenário a partir do qual poderão testar estratégias de resolução para a vulnerabilidade. Tal cenário pode ser o mesmo do passo anterior, com novas regras, com restrições diferentes, enfim, trabalhando a aprendizagem por descoberta através dos conhecimentos já adquiridos.

Sugere-se como metodologia trabalhar diversas vulnerabilidades até o ponto “O que?” e, em uma competição entre grupos, exigir o “E se?”, a exemplo do item 3.6 - Competições de Cibersegurança.

5 EXERCÍCIOS

Este capítulo utiliza o modelo proposto para a elaboração de exercícios de cibersegurança para as vulnerabilidades web indicadas no TOP 10 2010. Cabe salientar a importância de verificar se os participantes dos exercícios têm os requisitos exigidos e se conhecem a metodologia utilizada. Caso contrário, em momentos anteriores à realização, deve - se elucidar os conceitos essenciais. É necessário que os participantes compreendam o que é um agente de ameaça, o que são vetores de ataque e etc, para o correto entendimento das propostas dos exercícios.

Os Exercícios de segurança geralmente são aplicados a alunos dos últimos anos de cursos universitários, como já mencionado, porém acredita-se que esse modelo pode ser adaptado como metodologia de ensino já nos primeiros ensinamentos em segurança web.

5.1 A10 – Redirecionamentos e reenvios não validados - Ataque.

Abaixo, transita-se pelos quatro quadrantes, conforme modelo proposto neste trabalho.

5.1.1 “Por quê?”

Redirecionamento inválido é a décima vulnerabilidade do relatório TOP 10 2010 da OWASP. Essa vulnerabilidade é relativamente desconhecida, ou melhor, há pouco conhecimento sobre ela. Isso é uma das justificativas da sua escolha. Tal vulnerabilidade entrou nesse último relatório, como se pode observar na Figura 10, já que sua ocorrência tem crescido e por causar danos significativos (WILLIAMS; WICHERS, 2010).

Redirecionamentos[11] (*Redirect*) em aplicações web são bastante comuns e geralmente incluem parâmetros fornecidos pelos usuários na *Uniform Resource*

[11] em .NET são chamados Transferências.

Locator (URL)[12] de destino. Os reenvios (*Forward*) ou encaminhamentos são as mudanças a outras páginas da mesma aplicação. Neste caso, também ocorre o uso dos parâmetros para construção das URLs.

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Figura 10 - comparativo entre o TOP 10 de 2007 e o de 2010

5.1.1.1 Agentes de Ameaça

Atacante que queira enviar o usuário do site atacado, utilizando o reconhecimento deste, para outro site malicioso ou, no caso do reenvios inválidos, queira ganhar acesso a partes da aplicação que normalmente não teria.

5.1.1.2 Impactos

Atacantes, ao redirecionar os usuários às páginas hostis, usam códigos maliciosos que podem ser instalados, podendo obter senhas ou informações importantes. Além disso, por meio de reenvio inválido, acessam páginas e serviços sem autorização, conseguindo burlar o controle de acesso da aplicação. Seu nível de impacto foi considerado moderado (WILLIAMS; WICHERS, 2010).

[12] o termo correto seria *uniform resource identifier* (URI) que é a URN + URL porém URL é mas utilizado

5.1.2 “O quê?”

Pode-se promover a discussão sobre cada item, recuperar os conceitos e relacionar conceitos já dominados ou apresentados no passo anterior e aprofundá-los.

5.1.2.1 Abordagem

A abordagem será ofensiva.

5.1.2.2 Objetivos

Desenvolver a percepção de como as aplicações suscetíveis a redirecionamentos maliciosos podem ser atacadas, revelando as ameaças. Deve-se repensar o uso de redirecionamentos e encaminhamentos e, se possível, evitá-los com a finalidade de mitigar os riscos relacionados.

5.1.2.3 Vetores de Ataque

Embora os ataques sejam feitos basicamente por alteração de URL, dividem-se em dois tipos:

- Uso de **URL inválida** de redirecionamento levando o usuário a clicar no link. Com um domínio conhecido, a propensão ao clique é maior, direcionando os usuários a destinos externos inseguros, por exemplo, com phishing ou malware;
- Uso de **parâmetros não validados**, em que o atacante pode pular as verificações de autenticação dentro da aplicação e escalar privilégios.

5.1.2.4 Deficiência de Segurança

Falta de verificação do destino e da autorização do usuário ao fazer redirecionamentos e reenvios para novas páginas. Ao redirecionar os usuários, a página de destino, os argumentos não são validados, assim, é possível que a página de destino seja substituída por outra. Embora o nível de impacto seja moderado, essa vulnerabilidade tem um nível de ocorrência pouco comum e é de fácil detecção.

5.1.2.5 Cenário

Uma empresa que faz tráfico de animais selvagens nativos do Brasil tem o site www.wildanimals.com armazenado em um servidor no exterior e em inglês. É preciso obter acesso à aplicação, como administradores, para coletar provas com a devida autorização judicial! Descobre-se que a empresa utiliza um Sistema de Gestão de Conteúdo (SGC) do inglês *Content Management Systems* (CMS).

5.1.2.6 Regras

O atacante deve redirecionar o administrador da página a outra semelhante, a fim de obter o usuário e a senha. No entanto, a captura deve ser imperceptível para evitar que o administrador troque a senha. Tempo estimado para o exercício 50 min.

5.1.3 "Como?"

A proposta de resolução não é única, uma vez que é possível adotar outras, o importante é obter sucesso na resolução.

5.1.3.1 Topologia, Software e Hardware

Em um computador isolado, configura-se uma máquina virtual (VM)[13] como servidor web (Apache configuração padrão) e se instala a versão 2.2.1 do CMS Wordpress. Em outra máquina virtual, a do atacante, instala-se o BlackTrack ou qualquer outra distribuição Linux com Wireshark[14].

5.1.3.2 Estratégia de resolução

Estruturar um ataque tipo redirecionamento a um site com *phishing*. Verificar se utiliza e qual versão do CMS. Para isso, pode se visualizar o código fonte da página através do navegador e pode-se buscar pela meta tag *generator*, então, guardam-se as informações. Cabe salientar que a organização é importante para obter um mapa do sistema a ser atacado.

```
<meta name="generator" content="WordPress 2.2.1" />
```

Utilizando o Wireshark, é possível monitorar os pacotes trocados entre a máquina em que se está posicionado e o servidor da página, à procura de pacotes tipo POST que enviam o usuário, a senha e a URL de destino, caso o *login* seja efetivado com sucesso.

Nesse exemplo, ao acessar a página de administração de uma aplicação local onde o usuário é *usuário* e a senha é *senha*, redirecionamento foi feito para a página http://localhost/wordpress/wp-admin/. Conforme se pode observar na Figura 11.

[13] do inglês virtual machine

[14] http://www.wireshark.org/

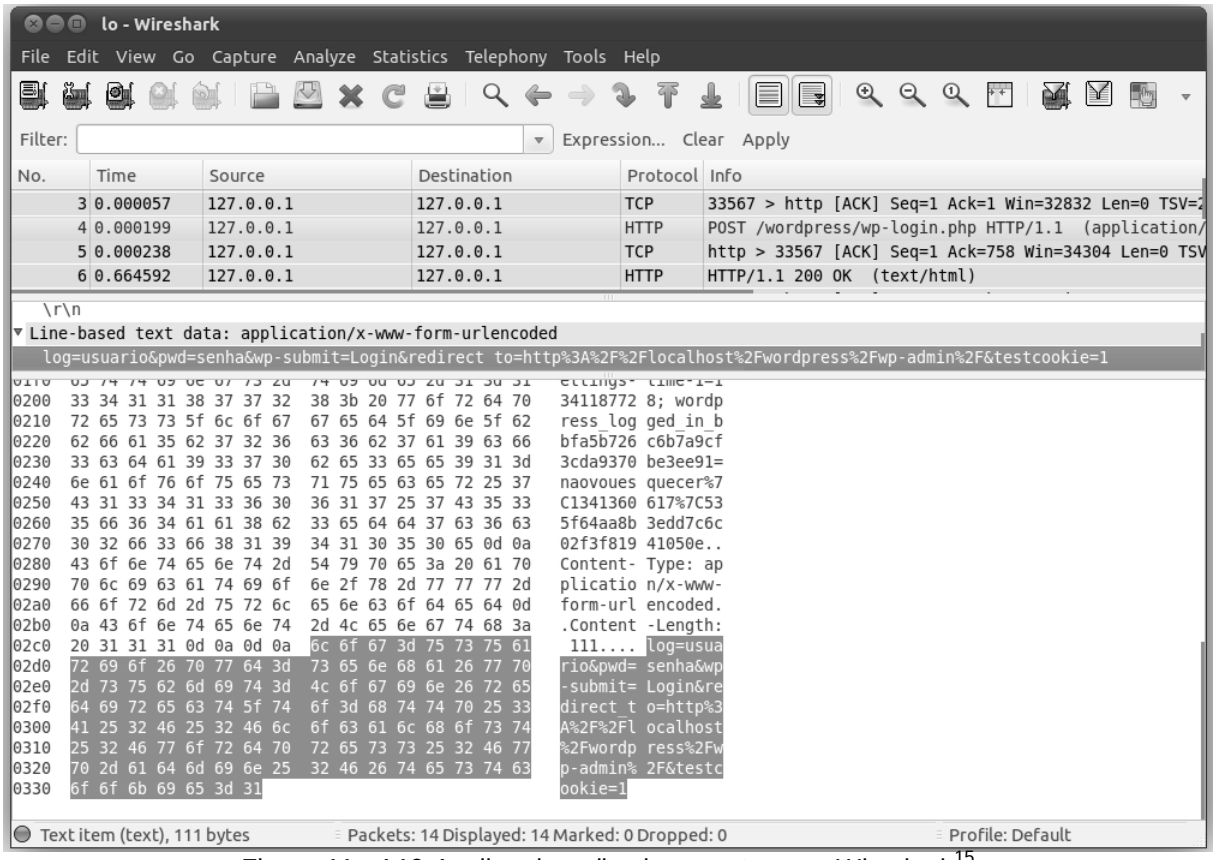

Figura 11 - A10 Analise do redirecionamento com Wireshark[15]

Essa abordagem pode ser generalizada para outras aplicações nas quais a comunicação não seja criptografada, basta compreender como cada linguagem faz o redirecionamento. Sendo assim, como se pode redirecionar o administrador à outra página para capturar seu usuário e senha? Supõe-se que a página alvo seja www.salvaselvagem.net, onde se espera que o administrador se autentique na armadilha. Faz-se uma página erro.php e se redireciona o usuário com a seguinte url usando xencodeURI()[16]:

```
www.wildanimals.com/wp-
login.php?redirec_to=http%3A%2F%2Fwww%2Esalvaselvagem%2Enet%2Ferro%2Ephp
```

Ao se autenticar com sucesso na página correta, o usuário será transferido para a página com a armadilha.

[15] http://www.wireshark.org/

[16] http://www.design215.com/toolbox/urlencode.php

Figura 12 - A10 erro.php

Para enviar ao administrador o endereço com o redirecionamento, pode-se usar a área de contato. Ao se autenticar na armadilha, guardam-se as informações e reencaminha-se o administrador à sua página verdadeira, através de outro redirecionamento, incluindo os parâmetros fornecidos.

```
log=usuarioveradeiro&pwd=senhacorreta&wp-
submit=Login&redirect_to=http%3A%2F%2Fwww.wildanimals.com%2Fwordpress%2Fwp-
admin%2F&testcookie=1
```

Essa vulnerabilidade já foi corrigida nas versões mais atuais do CMS Wordpress, mas, como teste, mesmo nas aplicações mais novas (3.4.1), experimente localmente redirecionar.

```
www.teusite.com.br/wp-login.php?redirect_to=http%3a%2f%2flocalhost%2f
```

Muitos sites baseados em Wordpress usam uma extensão, um *plugin* para solicitar a idade dos visitantes, para conteúdos adultos como indústrias de bebidas, cigarro, danceterias e etc. Esses *plugins* possuem uma vulnerabilidade de redirecionamento, conforme reportado por http://www.exploit-db.com/exploits/18350/. Os sites que usam esse *plugin* podem ser redirecionados a outros sites como, por exemplo:

Via GET:

```
http://www.dominio.com.br/wp-content/plugins/age-verification/age-
verification.php?redirect_to=http%3A%2F%2Fwww.ameaca.com.br
```

Via POST:

```
http://server/wp-content/plugins/age-verification/age-verification.php

redirect_to:    http://www.ameaca.com.br

age_day:        1

age_month:      1

age_year:       1991
```

Buscar por aplicações que utilizem esse *plugin* é simples, basta buscar no Google por:

```
inurl:wp-content/plugins/age-verification/age-verification.php
```

5.1.4 "E se?"

O aprendiz deve utilizar o que já aprendeu em novas situações, estendendo esses conhecimentos a novos exercícios.

5.1.4.1 Cenário

A aplicação utiliza reenvios para redirecionar os pedidos, pós-autenticação, as páginas da aplicação. Para facilitar, algumas páginas utilizam um parâmetro para indicar para onde será encaminhado o usuário se a transação for correta. Neste caso, o atacante edita uma URL que pula as verificações de autenticação e chegará a uma função de administração em que normalmente não teria acesso. Deve-se procurar na aplicação PHP fornecida e tentar explorar a vulnerabilidade.

5.2 A10 – Redirecionamentos e reenvios não validados - Defesa.

Exercícios de defesa para redirecionamentos e encaminhamentos devem ensinar como evitar ataques através de validação dos parâmetros e de teste de autorização.

5.2.1 "Por quê?"

Idêntica a do exercício anterior.

5.2.2 "O quê?"

5.2.2.1 Abordagem

A abordagem será defensiva.

5.2.2.2 Objetivos

Conscientizar os defensores de que é preciso tratar os redirecionamentos e os encaminhamentos, assim como os parâmetros e de que as entradas podem ter os mais diversos formatos.

5.2.2.3 Vetores de Ataque

Idênticos aos do exercício anterior.

5.2.2.4 Deficiência de Segurança

Idênticos aos do exercício anterior.

5.2.2.5 Cenário

A página do seu curso de graduação está sofrendo ataques de redirecionamento, redirecionando os colegas a outras páginas maliciosas. Foi percebido que o código atual da página não tem nenhuma proteção contra redirecionamentos.

5.2.2.6 Regras

Oferecer uma solução simples e rápida, para que não seja necessário refazer todo o código da página. Tempo estimado para o exercício 125 min.

5.2.3 "Como?"

5.2.3.1 Topologia, Software e Hardware

Utilizar uma máquina virtual com OWASP Mantra OS e criar um código simples, o qual dependendo do parâmetro e da autenticação, redireciona a uma página ou a outra;

5.2.3.2 Estratégia de Resolução

Há várias formas de minimizar as chances de ataques por redirecionamentos indevidos:

- Evitando ao máximo os redirecionamentos;
- Não utilizando parâmetros dos usuários para compor a URI;
- Se houver a necessidade de usar parâmetros, então optar por um dos seguintes:
    - Validar cada parâmetro para garantir que é válido e autorizado

- Se o redirecionamento é para outra página do curso, basta verificar se o redirecionamento realmente pertence ao domínio do site do curso;
- Considerar o uso de whitelist para sites confiáveis;
- Avisar os usuários quando eles forem redirecionados a uma página externa.

Neste caso, é recomendado verificar se realmente são necessários os redirecionamentos e depois utilizar a API ESAPI do OWASP para fazer os redirecionamentos, mais especificamente, a classe SecurityWrapperResponse. Essa classe oferece um método chamado sendRedirect(java.lang.String location), que valida os redirecionamentos após a configuração da API para o domínio do curso.

5.2.4 “E se?”

Utilizar a ferramenta CAL9000, para testar sua implementação com novos tipos de entradas como caracteres em hexadecimal por exemplo.

5.3 Discussão

Observa-se que o modelo é compatível com a elaboração de exercícios de cibersegurança. É possível, ainda, utilizá-lo para o ensino de segurança web, satisfazendo o modelo proposto por Kold e orientado pelo guia de Patriciu e Furtuna.

6 CONCLUSÃO

Sabe-se que a segurança cibernética é uma necessidade das nações e das organizações e também é um desafio, considerando que há uma escassez de mão de obra qualificada. Diante disso, modelos eficientes de elaboração de exercícios de cibersegurança são necessários, a fim de atingir os diferentes estilos de aprendizagem existentes, como propõe Kolb (1984). Orientado pelo guia de Patriciu e Furtuna (2009), pela aprendizagem experiencial e alimentando-se das informações do relatório TOP 10 da OWASP, elaborou-se um modelo para a criação de exercícios de ataque e de defesa para segurança web.

Propor uma modelo/metodologia de ensino de cibersegurança exige fortes esforços para unir duas áreas diferentes do conhecimento que são educação e computação.

Outras discussões/propostas de modelo/metodologia envolvendo ensino de segurança web e modelos de aprendizagem não foram encontradas na literatura. Isso aponta para a probabilidade de que este trabalho seja o único até o presente momento.

Trabalhos futuros poderão ser desenvolvidos aplicando o modelo em sala de aula e desenvolvendo mais exercícios com essa metodologia. É possível, ainda, criar um software/jogo baseado no modelo para a elaboração de exercícios de ataque e de defesa em aplicações web para a educação a distância.

7 REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2005. , 2006. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/biblioteca_tcu/ABNT NBR ISOIEC 27001.pdf>

ALARCÃO, I. Escola reflexiva e desenvolvimento institucional: que novas funções supervisivas. **A supervisão na formação de professores**, 2002.

ALMORSY, M.; GRUNDY, J.; MÜLLER, I. An analysis of the cloud computing security problem. **the proc. of the 2010 Asia Pacific Cloud …**, 2010.

BARROS, O.; GOMES, U.; FREITAS, W. Desafios estratégicos para segurança e defesa cibernética. 2011.

BLOOM, B.; ENGELHART, M.; FURST, E. Taxionomia de objetivos educacionais. 1973.

BRANDÃO, J. DE S.; FRAGA, J. DA S. Gestão de Riscos. **dainf.ct.utfpr.edu.br**, 2008.

CANONGIA, C. (INMETRO); JUNIOR MANDARINO, R. (GSIPR). Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, n. 29, p. 21-46, 2009.

CETIC.BR. **CETIC.br - Painel IBOPE/NetRatings**. Disponível em: <http://www.cetic.br/usuarios/ibope/tab02-01-cons.htm>. Acesso em: 9 fev. 2013.

CLARKE, R.; KNAKE, R. Cyber War: The next threat to national security and what to do about it. 2010.

EVANS, K. A Human Capital Crisis in Cybersecurity. 2010.

FURHT, B. Cloud computing fundamentals. **Handbook of Cloud Computing**, 2010.

GUIDE, I. S. O. 73: 2009. **Risk management—Vocabulary**, 2009.

HEIN, M. VON H.; WANDSCHEER, R. **Empresas e governos fazem investimentos bilionários em ciberdefesa | Ciência e Tecnologia | DW.DE | 29.07.2011**. Disponível em: <http://www.dw.de/empresas-e-governos-fazem-investimentos-bilionários-em-ciberdefesa/a-15273943>. Acesso em: 8 fev. 2013.

HOFFMAN, L. J. et al. Exploring a national cybersecurity exercise for universities. **Security & Privacy, …**, v. 3, n. 5, p. 27-33, 2005.

IBOPE; NIELSEN ONLINE. **Internet no Brasil cresceu 14% em um ano**. Disponível em: <http://www.ibope.com.br/pt-br/noticias/Paginas/Internet no Brasil cresceu 14_ em um ano.aspx>. Acesso em: 9 fev. 2013.

IBOPE; NIELSEN ONLINE. **Internet em domicílios continua a crescer no Brasil**. Disponível em: <http://www.ibope.com/pt-br/relacionamento/imprensa/releases/Paginas/Internet-em-domicilios-continua-a-crescer-no-Brasil.aspx>. Acesso em: 9 fev. 2013.

KOLB, D. Experiential learning: Experience as the source of learning and development. 1984.

KOLB, D.; BAKER, R.; DIXON, N. Personal learning guide: Self study booklet. **A Personal Guide for Setting Learning Goals and …**, 1985.

L'AGENCE FRANCE-PRESSE(AFP). **Setor de segurança cibernética cresce 2 vezes mais que TI - Terra Brasil**. Disponível em: <http://tecnologia.terra.com.br/negocios-e-ti/setor-de-seguranca-cibernetica-cresce-2-vezes-mais-que-ti,43c9fe32cdbda310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 8 fev. 2013.

MACHADO, F.; MAIA, L. Um Framework Construtivista no Aprendizado de Sistemas Operacionais-Uma Proposta Pedagógica com o uso do Simulador SOsim. **XII Workshop de Educação em Computação …**, 2004.

NIST, S.; STONEBURNER, G. 800-30 Risk Management Guide for Information Technology Systems. **Nist special …**, 2002.

PAPERT, S. Information technology and education: Computer criticism vs. technocentric thinking. **Educational Researcher**, 1987.

PATRICIU, V.; FURTUNA, A. Guide for designing cyber security exercises. **… E-Activities and information security and privacy**, 2009.

Pesquisa Global de Segurança da Informação 2012. . [S.l: s.n.]. Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pwc-pesquisa-global-de-seguranca-da-informacao-2012.pdf>. Acesso em: 8 fev. 2013.

PIMENTEL, A. A teoria da aprendizagem experiencial como alicerce de estudos sobre desenvolvimento profissional. **Estudos de Psicologia**, 2007.

RONCA, A. Desmistificação e Comprometimento: os dois maiores desafios que se apresentam ao educador. **Cadernos Cedes**, 1985.

SAIC. **SAIC To Acquire Cybersecurity Solutions Provider CloudShield Technologies, Inc.** Disponível em: <http://investors.saic.com/phoenix.zhtml?c=193857&p=irol-newsArticle&ID=1438860&highlight=>. Acesso em: 8 fev. 2013.

SCHEPENS, W. The Cyber Defense Exercise: An evaluation of the effectiveness of information assurance education. **… of Information …**, 2002.

TREVELIN, A. ESTILOS DE APRENDIZAGEM DE KOLB: ESTRATÉGIAS PARA A MELHORIA DO ENSINO-APRENDIZAGEM. **Revista de Estilos de Aprendizagem**, v. 7, n. 7, 2011.

TZU, S. A arte da guerra–os treze capítulos originais. 2006.

UTO, N.; MELO, S. DE. Vulnerabilidades em Aplicaçoes Web e Mecanismos de Proteçao. **IX Simpósio Brasileiro de Segurança da …**, 2009.

WILLIAMS, J.; WICHERS, D. OWASP top 10–2010. **OWASP Foundation, April**, 2010.

WISHART, J. A comparison of preferred learning styles, approaches and methods between information science and computer science undergraduates. **ITALICS**, 2005.