FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE

PÓS-GRADUAÇÃO MBA EM REDES DE COMPUTADORES E SEGURANÇA DA INFORMAÇÃO

CLAUDIVAN DA SILVA SANTANA

PRINCIPAIS MODOS DE ATAQUE NO AMBIENTE VIRTUAL MOODLE

Aracaju
2016/01

CLAUDIVAN DA SILVA SANTANA

PRINCIPAIS MODOS DE ATAQUE NO AMBIENTE VIRTUAL MOODLE

Projeto de pesquisa científica apresentado como requisito de avaliação do TCC – Trabalho de Conclusão do Curso.

Aracaju
2016/01

SUMÁRIO

PRINCIPAIS MODOS DE ATAQUE NO AMBIENTE VIRTUAL MOODLE

Claudivan da Silva Santana
MBA em Redes de Computadores e Segurança da Informação
Faculdade de Administração e Negócios de Sergipe - FANESE
Aracaju, Sergipe, Brasil
contato@claudivan.com.br

RESUMO

Em uma busca constante pelo conhecimento, instituições do mundo todo disponibilizam plataformas para estudos a distância, o Moodle é uma dessas ferramentas. Um software livre que auxilia na aprendizagem, utilizado como ferramenta na Educação a Distância. O presente trabalho tem como objetivo apresentar formas de vulnerabilidade de ataque ao Ambiente Virtual de Aprendizagem.

Palavras-chave: Moodle; AVA; Vunerabilidade; Segurança.

ABSTRACT

In a constant search for knowledge, institutions worldwide provide platforms for distance studies, Moodle is one such tool. A free software that helps in learning, used as a tool in Distance Education. This study aims to present forms of attack vulnerability to the Virtual Learning Environment.

Keywords: Moodle; AVA; Vulnerability; Security.

1. INTRODUÇÃO

Com a constante evolução da tecnologia, estudar ficou mais fácil na atualidade, pois muitos têm acesso à informação e aos dispositivos que auxiliam na educação. Um bom exemplo com relação aos estudos nos dias atuais são as grandes quantidades de cursos e capacitações através da Web, promovendo formação contínua do ser humano. O crescimento em larga escala da Internet também proporciona um avanço na educação, mas esse aumento de dados e informações entre usuários e servidores é a deixa que pessoas maliciosas precisam para invadir, derrubar e até colher informações.

A grande rede está disponível para cada um fazer uso como queira, uns acabam estudando, outros trabalhando e alguns maldosos denominados *hackers* se realizam com invasão em sites e sistemas. Mas *hacker* é um termo que representa pessoas que são extraordinárias no que fazem e nem sempre fizeram invasões, pegadinhas e truques. Os acadêmicos na década de 70, por exemplo, desenvolviam suas soluções tecnológicas com base nesses truques que hoje são usados para o mal.

A segurança da informação é questionada por vários quesitos e uma política de segurança tem várias estratégias para uma defesa segura e no Ambiente Virtual de Aprendizagem não seria diferente. Existem várias formas de ataques *hackers* e este trabalho visa mostrar alguns deles. A ética *hacker* é baseada em Steven Levy (1984), que descreve alguns valores para caracterizar as similaridades das culturas hacker que são seguidos até hoje:

1 - A informação deve ser livre;

2 - Desconfie das autoridades e promova descentralização;

3 - Julgue as pessoas pelo que elas criam e não por suas credenciais;

4 - O acesso aos computadores deve ser ilimitado;

5 - As pessoas podem criar arte e beleza com os computadores;

6 - Os computadores podem mudar a vida e o mundo para melhor.

Na grande maioria, AVA utiliza software livre em sua aplicação web para seus alunos e administradores. As atualizações não são realizadas e/ou não mais disponíveis, com isso a aplicação fica sem correção, encontrando assim brechas na plataforma.

1.1 Objetivos

Este trabalho tem como objetivo mostrar alguns tipos de ataques a aplicações Web e suas definições, apresentar a importância do Moodle (*Modular Object-OrientedDynamic Learning Environment*) como Ambiente Virtual de Aprendizagem – AVA, tomando como base a plataforma instalada no servidor do IFS – Instituto Federal de Sergipe que utiliza para seus alunos. Esta pesquisa visa apresentar o perigo a ataques maliciosos que estamos sujeitos a receber, em particular no Moodle, no qual sou administrador da Instituição citada acima.

2. DESENVOLVIMENTO

Os anos passam e os noticiários não deixam de apresentar a atuação de criminosos digitais no mundo todo, em 2015 não foi diferente, dentre os ataques alguns que mostram a ousadia são:

- **Ashley Madison**: Site famoso por simular uma rede social para pessoas que procuram trair seus parceiros. Ano passado o site recebeu um roubo de dados e uma lista d contendo informações de usuários vazou na Internet.
- **Estado Islâmico**: O grupo Anonymous deu início a vários ataques aos grupos que usavam a rede para recrutar novos soldados para o Estado Islâmico. Tudo indica que em 2016 teremos mais ataques iguais, hackeando sites da organização terrorista.
- **App Store**: o que o mundo pensava que nunca iria acontecer, vimos no ano passado. A loja virtual da Apple teve o seu primeiro ataque registrado e um malware foi encontrado, mas logo removido.

Em um mundo tecnológico e altamente globalizado sugar as potencialidades dos recursos disponíveis é uma forma correta de viver. Não tem como abordar a temática Internet e Educação, sem focar em um dos ambientes virtuais que mais vem sendo acessado nos dias de hoje, o Moodle. É uma plataforma com fins educativos escrita na linguagem PHP, que permite educadores e alunos interajam em salas, criando e gerenciando usuários em cursos.

2.1 Moodle

Criado em 2001, o software livre tem como objetivo estudar em qualquer lugar que tenha acesso a Internet, é uma plataforma de aprendizagem que visa a realização de cursos com várias atividades e recursos: páginas, wiki, vídeos, fóruns, apresentação, avaliação online, entre outros. De acordo com o site https://moodle.org/, o Brasil fica em terceiro lugar numa lista de países que se registram para ter o software livre e pelo fato de ser livre existem ainda ataques à plataforma que apresentaremos mais a frente.

Confira a lista na integra de países que registram na plataforma Moodle:

Lista 01

Lista de registro no Moodle

Country	Registrations
Estados Unidos da América	8,336
Espanha	5,617
Brasil	3,827
Reino Unido da Grã-Bretanha e da Irlanda do Norte	2,855
Mexico	2,339
Alemanha, República Federal da	2,091
Colômbia	1,752
Itália	1,572
Austrália	1,453

Top 10 from registered sites in 221 countries

Fonte: www.moodle.org

Data: 30 de agosto de 2015

2.2 Como funciona?

Como qualquer plataforma de ensino a distância, é obrigatória a disponibilidade de funcionalidade que permita o usuário a colaboração e interação via Internet, sendo essas 100% on-line ou presencial. No Instituto Federal de Sergipe, local que tiramos como base para o nosso estudo, o modo de ensino é semi-presencial, onde o aluno tem aula uma vez por semana, realizando as atividades e recursos disponíveis no Ambiente Virtual de Aprendizagem - AVA.

Cada instituição de ensino tem a sua metodologia e particularidade de ensino, podemos dizer que atualmente só usamos 50% do que a plataforma disponibiliza:

- Fórum;
- Banco de Questões;
- Atividade Autoinstrutiva;
- Glossário;
- Chat;
- Compartilhamento de arquivos, vídeos e páginas Web;
- Avaliações.

O Moodle é considerado uma “caixa de ferramentas”, onde o aluno fica responsável em “construir” seus conhecimentos. Já que o estudante é responsável dos seus próprios passos após um encontro semanal do seu curso. O IFS disponibiliza duas modalidades de cursos – Cursos Técnicos e o Profuncionário. A primeira opção é acessível para o público em geram, já a segunda apenas para quem faz parte do quadro efetivo municipal ou estadual. Os cursos são distribuídos da seguinte forma:

• CURSOS TÉCNICOS o Administração o Reabilitação de Dependentes Químicos o Transações Imobiliárias o Secretariado	• PROFUNCIONÁRIO o Alimentação Escolar o Infraestrutura Escolar o Multimeios Didáticos o Secretaria Escolar

2.3 A ferramenta

Inicialmente o Moodle foi criado para programadores e acabou sendo auxilio como material de estudo para centros acadêmicos. O tempo passa e hoje acaba sendo uma forte ferramenta, proporcionando interação em todos os pontos abordados.

Atualmente a plataforma está alocada em uma VM no servidor Blade, esta foi a única informação que o Departamento de Tecnologia do Instituto Federal disponibilizou, afirmando não poder entrar em mais detalhes. A mudança de servidor foi realizada no ano de 2014, anteriormente a plataforma não suportava um chat com alunos de um curso por exemplo. Abaixo a figura exemplifica a arquitetura do Moodle, ainda sendo possível instalar em diversos ambientes (Unix, Linux, Windows, Mac OS):

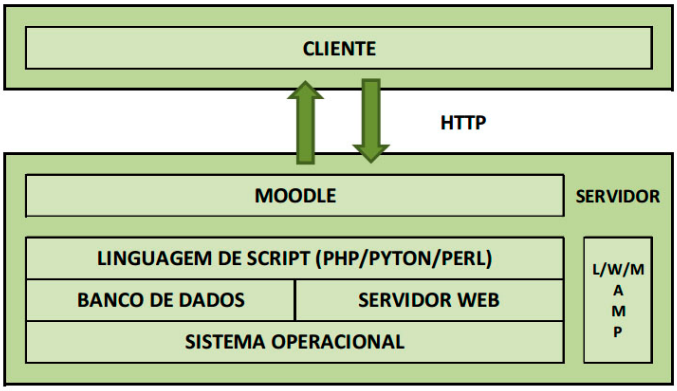


Figura 01. Arquitetura Moodle

Data: 19 de maio de 2016

O sistema de gestão de aprendizagem possui mais de 79 milhões de alunos em 220 países, com um sistema extremamente robusto, suporta milhares de alunos em uma única instalação, no IFS por exemplo antes dos problemas em 2014 tínhamos 2500 alunos ativos, atualmente temos 4282 usuários na aplicação.

Com o código aberto e disponível para todo mundo, a plataforma Moodle vira alvo de ataques *hackrs* em todo o mundo. Muitos desses ataques são DDoS (*DistributedDenial-of-Service ATTACK*), que são considerados os mais comuns e *Cross-Site Scripting* (XSS).

Não se fala em segurança da informação de empresas ou instituições apenas para fins lucrativos, é um item de extrema importância em todos os sentidos. Em cursos ofertados gratuitamente como no IFS, por exemplo, ser humanos maliciosos podem tirar um servidor do ar por protesto, ego, disputa entre grupos e/ou pessoas na Internet.

Figura 02. Moodle no mundo

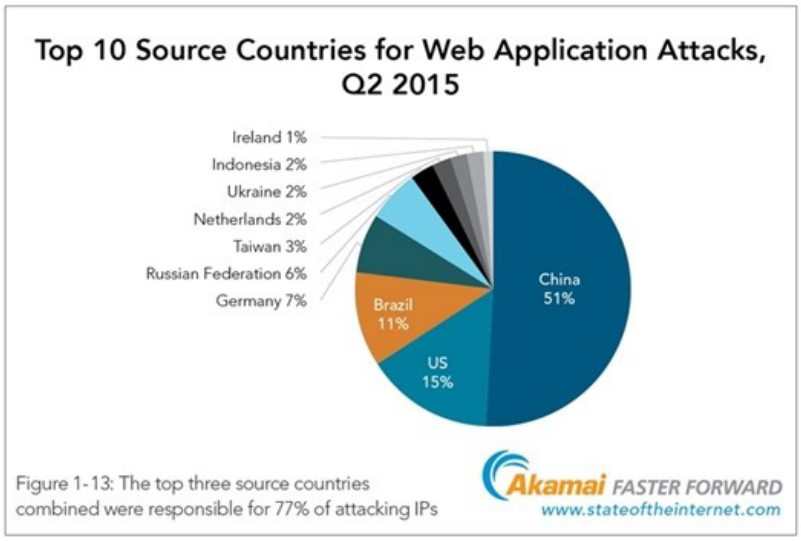
Fonte: www.moodle.org
Data: 30 de agosto de 2015

3. ATAQUES

Em uma publicação realizada pela empresa Akamai[1], quando o assunto é ataque a aplicações Web, comprova que o Brasil fica atrás de duas potencias, China e Estados Unidos. Conforme a ilustração a seguir:

Gravura 03

Países de origem para ataques a aplicações Web



Fonte: Akamai

Data: 31 de agosto de 2015

Ainda existem algumas vulnerabilidades que segundo *Open Web Application Security Project* – OWASP são as mais críticas quando se referem a aplicações web. OWASP é uma comunidade aberta que não visa lucros, dedicada capacitar as organizações a desenvolver, adquirir e manter aplicações confiáveis, visando a segurança na rede.

Em 2013 a OWASP disponibilizou uma relação contendo os dez riscos de aplicações vulneráveis na Internet. Confira na tabela a seguir:

[1]Akamai Technologies é uma empresa de Internet, fundada em 1998, responsável por segurança, que utiliza diversos computadores para conter a ataques

Tabela 1 – Vulnerabilidade em aplicações WEB.

Injeção	As falhas de Injeção, tais como injeção de SQL, de SO (Sistema Operacional) e de LDAP, ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados manipulados pelo atacante podem iludir o interpretador para que este execute comandos indesejados ou permita o acesso a dados não autorizados.
Quebra de Autenticação e Gerenciamento de Sessão	As funções da aplicação relacionadas com autenticação e gerenciamento de sessão geralmente são implementadas de forma incorreta, permitindo que os atacantes comprometam senhas, chaves e tokens de sessão ou, ainda, explorem outra falha da implementação para assumir a identidade de outros usuários.
Cross-Site Scripting (XSS)	Falhas XSS ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequado. XSS permite aos atacantes executarem scripts no navegador da vítima que podem "sequestrar" sessões do usuário, desfigurar sites, ou redirecionar o usuário para sites maliciosos.
Referência Insegura e Direta a Objetos	Uma referência insegura e direta a um objeto ocorre quando um programador expõe uma referência à implementação interna de um objeto, como um arquivo, diretório, ou registro da base de dados. Sem a verificação do controle de acesso ou outra proteção, os atacantes podem manipular estas referências para acessar dados não-autorizados.
Configuração Incorreta de Segurança	Uma boa segurança exige a definição de uma configuração segura e implementada na aplicação, frameworks, servidor de aplicação, servidor web, banco de dados e plataforma. Todas essas configurações devem ser definidas, implementadas e mantidas, já que geralmente a configuração padrão é insegura. Adicionalmente, o software deve ser mantido atualizado.

Exposição de Dados Sensíveis	Muitas aplicações web não protegem devidamente os dados sensíveis, tais como cartões de crédito, IDs fiscais e credenciais de autenticação. Os atacantes podem roubar ou modificar esses dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes. Os dados sensíveis merecem proteção extra como criptografia no armazenamento ou em trânsito, bem como precauções especiais quando trafegadas pelo navegador.
Falta de Função para Controle do Nível de Acesso	A maioria das aplicações web verificam os direitos de acesso em nível de função antes de tornar essa funcionalidade visível na interface do usuário. No entanto, as aplicações precisam executar as mesmas verificações de controle de acesso no servidor quando cada função é invocada. Se estas requisições não forem verificadas, os atacantes serão capazes de forjar as requisições, com o propósito de acessar a funcionalidade sem autorização adequada
Cross-Site Request Forgery (CSRF)	Um ataque CSRF força a vítima que possui uma sessão ativa em um navegador a enviar uma requisição HTTP forjada, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão, a uma aplicação web vulnerável. Esta falha permite ao atacante forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima.
Utilização de Componentes Vulneráveis Conhecidos	Componentes, tais como bibliotecas, frameworks, e outros módulos de software quase sempre são executados com privilégios elevados. Se um componente vulnerável é explorado, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor. As aplicações que utilizam componentes com vulnerabilidades conhecidas podem minar as suas defesas e permitir uma gama de possíveis ataques e impactos.

Redirecionamentos e Encaminhamentos Inválidos	Aplicações web frequentemente redirecionam e encaminham usuários para outras páginas e sites, e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de phishing ou malware, ou usar encaminhamentos para acessar páginas não autorizadas.

Fonte: OWASP, 2013

O site espanhol HISPASEC, em outubro de 2011 publicou uma nota, auxiliando os administradores do Moodle sobre as vulnerabilidades de algumas versões – 1.9.x, 2.0.x e 2.1.x – que apresentam na aplicação Web. No IFS, local que estamos tomando como base para o nosso trabalho está com a versão 2.3.3 e preparando servidor para a instalação da versão 2.8.x, onde temos na versão em questão estabilidade e com ícones atualizados/novos. Podemos verificar abaixo as falhas, erros, falta de permissão e outros erros apresentados pelo site espanhol:

Tabela 2 – Vulnerabilidade plataforma Moodle.

MSA-11-0027	há um erro de falta de validação dos pedidos de HTTP feitas por usuários que poderiam ser utilizados para a realização de referência falsificação cross site "(CSRF), com links para o wiki.
MSA-11-0028	há uma falta de erro de validação em certas entradas relacionadas aos comentários wiki que poderiam ser usados para levar a cabo cross-site scripting "ataques (XSS).
MSA-11-0029	revela uma falta de permissões de verificação de erros no servidor de arquivos que poderiam ser usados para revelar informações sobre categorias e cursos para os usuários que não têm acesso a eles.
MSA-11-0030	expõe uma falha na implementação do plug-in 'Box.net' por não incluir a funcionalidade de autenticação OAuth do aplicativo para solicitar as credenciais do usuário.

MSA-11-0031	erro na função 'setConstant' que leva os valores das formas que pode ser explorada para modificar os valores enviados via essas formas.
MSA-11-0032	revela um erro durante a manipulação dos dados fornecidos pela função 'openssl_verify' 'MNet' que poderia ser utilizado para prevenir a validação dos certificados de SSL.
MSA-11-0033	há um erro durante o processo de instalação, causando não definir corretamente o valor 'registration_hubs.secret "segredo relacionado com centros comunitários.
MSA-11-0034	há uma falha na funcionalidade de chat que faz com que a divulgação de informações confidenciais, como nomes completos de todos os usuários da plataforma, incluindo aqueles que foram eliminados.
MSA-11-0035	uma falha relacionada com a variável 'CFG-> usesid' nas sessões sem cookies podem ser exploradas para dar um salto de restrições.
MSA-11-0036	a falta de verificação de erros "mensagem / refresh.php 'faz pedidos ilimitados para alterar o valor do parâmetro' espera 'para zero e poderia causar uma negação de serviço.
MSA-11-0037	há uma falta de verificação de erros de dados introduzidos por usuários 'editsection.html' e poderia ser usado para executar código arbitrário (HTML e JavaScript) através de dados de entrada especialmente criados.
MSA-11-0038	vários erros de filtragem funções do banco de dados pode ser usado para realizar ataques de injeção SQL.
MSA-11-0039	um erro de falta de validação de 'secção' parâmetro de entrada seria usado para scripting cross site ataques (XSS).
MSA-11-0040	erro não especificado "mod / forum / user.php" que poderia ser usado para revelar informações sensíveis sobre os usuários da plataforma para pessoas não autorizadas.
MSA-11-0041	há uma verificação de permissão falha na funcionalidade do motor de pesquisa global que poderia permitir que um usuário convidado a revelar informações sensíveis através de pesquisas desse tipo diretamente de uma URL.

Fonte: HISPASEC, 2011

Com a informação e a divulgação da lista, contendo brechas na aplicação, o Moodle já disponibilizou imediatamente correções para os erros citados para as versões 1.9.14, 2.0.5 e 2.1.2. Podendo baixar no site oficial da comunidade ou direto do ambiente instalado no seu servidor.

3.1. Entendendo o DDoS

Muito se fala em invasão por parte de *hackrs*, mas em um ataque DDoS não é bem uma invasão. O ataque de negação de serviço distribuído por mais que seja comum e não tenha entrado na relação do OWASP, acontece quando uma pessoa tem o controle de vários micros e utiliza esses vários dispositivos para fazer um ataque DoS (*Denial-of-Service*). Relativamente simples, esses ataques tem o objetivo de derrubar o serviço para o usuário final, sobrecarregando o servidor ou fazendo uso dos seus recursos até que estes se esgotem, como mostra a ilustração a seguir.

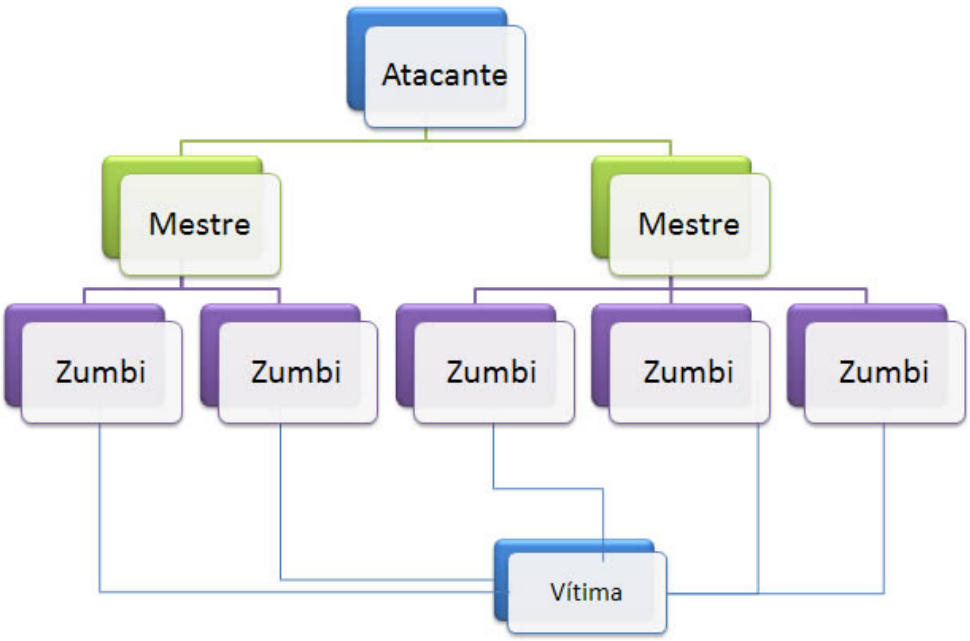


Figura 03. Ataque DDoS

Fonte: www.moodle.org

Data: 31 de agosto de 2015

Esse ataque é baseado no DoS, onde os indivíduos fazem tentativas para computadores ou servidores, forçando serviço e impedido a máquina de realizar tarefa. Trazendo para o nosso cotidiano seria como uma caminhoneta com uma carga quatro vezes mais que ela possa suportar, assim ela não sai ao menos do local para realizar o serviço de condução.

4. SEGURANÇA DA INFORMAÇÃO

Não podemos afirmar com precisão como prevenir o defender tal tipo de ataque, nenhuma arma dá total garantia de proteção. Para prevenção de ataques, os servidores e aplicações devem contar com uma equipe bem preparada, contendo ataques e antenado nas novidades e atualizações de cada sistema.

Se sua aplicação Moodle tem algumas das três versões citada anteriormente aqui nesse trabalho, a atualização deverá ser feita imediatamente, corrigindo as 15 vulnerabilidades da plataforma e deixando seu ambiente mais seguro. O software livre ainda afirma no seu próprio site que leva segurança a sério e que sempre melhora a aplicação Web, fechando os buracos encontrados e aconselha as recomendações abaixo:

- Atualização regularmente em cada liberação;
- Desativar registros globais;
- Use senhas fortes para admin e professores;
- Somente professor/admin dar contas a usuários confiáveis.

A falha na segurança também acaba sendo responsabilidade dos administradores, optando por senhas de fácil aplicação, pensando que nunca serão quebradas. A desativação de serviços não utilizados é muito eficaz, firewall com diferentes programas e combinações, cópias de segurança pronta – tanto de cursos (coisa que podemos fazer forma sistemática na plataforma) quanto dos dados no servidor, entre outras seguranças que podemos realizar no ambiente. Veremos pontos cruciais para a segurança e defesa do ambiente de estudo:

a) **Engenharia social** – considerado um dos pontos mais críticos quando falamos de segurança, os engenheiros sociais acabam atuando em manipulação psicológica, independente de sistemas computacionais. Não adianta ter várias ferramentas de verificação de vulnerabilidade e o administrador do sistema anotar sua senha e colocar do lado do computador por exemplo, o homem acaba sendo a maior falha nesse quesito. Segundo Giavaroto e Santos (2013, p.36): "[...] é possível diminuir a ação de engenheiros sociais através de treinamentos constantes de conscientização de todo o pessoal envolvido nos processos".

b) **Backups** – Com relação as cópias de segurança, o Moodle não trabalha com a opção de backup na plataforma, é sugerido fazer cópias dos seguintes itens:

   - Aplicação do Moodle;
   - Base de dados;
   - Pasta moodledata.

   Ainda pode estipular, de forma sistematizada a cópia dos cursos, já a backup da aplicação fica a critério, porém, podemos restaurar o estado do Moodle em todos os sentidos. Já base de dados aconselho fazer um *dump* da base inteira. A pasta *moodledata* contém todos os dados dos usuários e dos cursos.

c) **Permissões de acesso** – Por mais que o aluno tenha sua senha no acadêmico e outras instituições fazem a comunicação entre sistemas, o IFS não trabalha desta forma. Já na plataforma podemos estipular os administradores e designar as funções que cada usuário (aluno, tutor, coordenador, professor, etc) possa fazer.

d) **Antivírus** – A plataforma Moodle tem a disponibilidade de utilização de programa para prevenir ataques, adicionando no bloco de configurações administrativas. O ClamAV é o antivírus para fazer esse trabalho, varrendo o servidor, verificando arquivos, e-mails, raiz do site, home de

cada usuário, entre outros serviços. Mantendo sempre sua plataforma segura e confiável.

e) **IPs** – O ambiente ainda trabalha com um bloqueador de IP na segurança da plataforma. Inserindo uma lista de IP permitido e outra de bloqueado. Por padrão, as entradas na lista de IPs bloqueados são processadas primeiro. Caso essa opção seja vaga, o administrador Moodle pode solicitar junto ao responsável de rede uma solução RTBH – Remotely Triggered Black Holes, também conhecida como “Filtragem via Buraco Negro”. RTBH é a base para uma série de técnicas de rastreamentos a ataque de negação de serviço. Essa técnica manipula a rota já na borda ou em qualquer outro lugar, bloqueando o atacante e não o alvo atacado, o que garante a disponibilidade do serviço atacado, economizando processamento e a banda.

f) **Criptografia** – no Moodle a senha só entra criptografada por MD5. Sites afirmam que da versão 2.5 em diante não usa mais hash MD5 simples, utilizando agora a função crypt do PHP.

Já com relação a ataques DDoS que costumam “visitar” nossa aplicação por exemplo, sistematicamente podemos ver um aumento no fluxo de serviço e optar em derrubar essa solicitação, como foi citado anteriormente com o RTBH. Uma analogia com relação a essa afirmação: um chinês com um link de Internet cinco vezes maior do que temos aqui no Brasil, inicia um ataque de solicitação de serviço, o sistema ver que não há normalidade nessas requisições e tem certeza que são “zumbis”, derrubando a solicitação feita. Claro que uma técnica de tamanha grandeza como é a "Filtragem via Buraco Negro" (Remotely Triggered Black Holes) não poderia atuar sozinha, a mesma trabalha junto com outras potencialidades:

- **BGP:** uso de atributos do protocolo de roteamento dinâmico Border Gateway Protocol;
- **uRPF:** Unicast Reverse Path Forwarding que é o diferencial da solução, combinando as técnicas de Black Role para realizar o bloqueio de tráfego.

CONSIDERAÇÕES FINAIS

No geral, o assunto de segurança da informação em ambiente virtual de aprendizagem é bastante complexo, portanto, o objetivo foi passar noções dos ataques distribuídos por negação de serviço, os profissionais que trabalham contra o ataque precisam efetuar configurações nos equipamentos que levam até o site desejado. Muitas vezes são utilizados filtros que vão determinar quais IPs podem acessar o site e quais são perigosos para o servidor.

O Moodle é um software livre e comunidades se ajudam, apresentando as falhas nos fóruns para partilharem da informação e chegarem logo a uma correção. Cadastre-se no site da comunidade – https://moodle.org/ – e interaja com os demais desenvolvedores.

Não podemos atualizar de imediato uma versão da aplicação quando sair, mesmo a comunidade e administradores estipulando essa ação. Ideal que pesquise antes para ver se a versão desejada para a atualização esteja estável, se rodará perfeita nas especificações do seu servidor e depois dessa pesquisa poder atualizar.

Outra solução é recorrer a empresas especializadas, como a Akamai. Essa técnica é efetiva porque as máquinas estão em diferentes locais do planeta e combatem os zumbis dividindo a tarefa, de modo que cada computador de defesa combata um número reduzido de máquinas.

REFERÊNCIAS

GIAVAROTO, S. C. R.; SANTOS, G.R. dos. “Backtrack Linux: Auditoria e Teste de Invasão em Redes de Computadores”. São Paulo, Ciência Moderna Ltda, 2013.

HISPASEC. **Múltiples vulnerabilidades en la plataforma educativa Moodle**. Disponível em http://unaaldia.hispasec.com/2011/10/multiples-vulnerabilidades-en-la.html. Acesso em: 25/02/2016.

LEVY, Steven. **Hackers, heroes of the computer revolutions**. New York: Penguin Books, 1984.

MOODLE. **Open-source learning platform |** Moodle.org. Disponível em https://moodle.org. Acesso em: 30/08/2015.

OWASP, OWASP Top Ten – 2013. **The Ten Most Critical Web Application Security Risks**. Disponível em https://www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf. Acesso em: 05/02/2016.

Sites Visitados:

http://www.tecmundo.com.br/ataque-hacker

https://blogs.akamai.com/2015/08/q2-2015-state-of-the-internet-security-report-released.html

http://nitehack.blogspot.com.br/2012/11/ataques-ddos-moodle.html

https://www.ovh.pt/anti-ddos/principio-anti-ddos.xml