Uso de teste de invasão para avaliar a segurança dos serviços Web da Universidade Estadual de Maringá

Marcelo Yuri Benesciutti (PIC/CNPq/UEM), Luciana Andréia Fondazzi Martimiano (Orientadora), e-mail: lafmartimiano@uem.br

Universidade Estadual de Maringá / Centro de Tecnologia/Maringá, PR

Ciências Exatas e da Terra. Ciência da Computação.

Palavras-chave: segurança da informação, vulnerabilidades, teste de invasão

Resumo: Com mais de 20 mil pessoas envolvidas em sua rotina diária, a UEM possui sistemas importantes que precisam funcionar com segurança e eficiência, e dentre os mais críticos estão os sistemas Web. É importante que esses sistemas não tenham vulnerabilidades, pois em uma situação de exploração de uma falha de segurança, as consequências poderiam ser graves, permitindo acesso indevido às informações acadêmicas e pessoais da comunidade, ou causando indisponibilidade dos sistemas. Neste contexto, a ideia de realizar testes de invasão nos sistemas Web da UEM com a intenção de detectar possíveis vulnerabilidades surge como uma opção, visto que este tipo de teste é eficiente por abordar métodos que seriam utilizados por um atacante em potencial. A partir do uso do teste de invasão, espera-se prover material para a equipe de desenvolvimento e manutenção dos sistemas da UEM possa corrigir as vulnerabilidades existentes e mitigar outras, melhorando a segurança desses sistemas tão importantes para a comunidade acadêmica.

Introdução

Com o *boom* da internet nos últimos 30 anos, muita coisa mudou com relação aos computadores pessoais. O que antes era impensável, como por exemplo, realizar procedimentos bancários direto de casa, virou possível com os serviços de Internet Banking. Diante desse cenário, a informação virou o mais importante produto comercializável, visto que quem detém informação é quem detém dinheiro. Sem perder tempo, surgiram os “criminosos virtuais”, que descobriram meios de realizar golpes por meio da Internet, comprometendo e ameaçando os pilares básicos da segurança da informação, que são confidencialidade, integridade e disponibilidade. De acordo com Kumar (1995), para que um sistema seja considerado seguro, é necessário que esses pilares sejam respeitados como regras da seguinte forma: confidencialidade requer que as informações sejam acessadas somente por entidades autorizadas a fazê-lo; integridade requer que as

informações não sejam alteradas por acidentes ou tentativas maliciosas; e disponibilidade requer que o sistema funcione sem degradação, e que proporcione recursos aos usuários autorizados quando estes forem necessários. Um dos meios de descobrir potenciais vulnerabilidades que afetem os três pilares de segurança da informação são os testes de invasão. Teste de invasão (*pentest ou pentesting*), segundo Whitaker e Newman (2005), é a tentativa de comprometer uma rede de computadores ou sistemas de determinada organização com o objetivo de avaliar a segurança. O teste de invasão tem como princípio explorar o ambiente computacional, só que de uma maneira ética, com o objetivo de identificar vulnerabilidades e meios de explorá-las, do mesmo jeito que um *cracker*, porém, com a diferença de não se aproveitar das vulnerabilidades para benefício próprio, mas sim para corrigi-las.

Materiais e métodos

Existem diferentes tipos de teste de invasão, todos relativos à quantidade de conhecimento sobre o ambiente do escopo que o testador (*pentester*) possui, e ao conhecimento que os administradores dos sistemas possuem sobre os testes que serão realizados. Podem-se definir três tipos de testes de acordo com Whitaker e Newman (2005):

• *Black-box*;
• *White-box*;
• *Gray-box*.

O *Black-box* e o *White-box* são completamente opostos, com o testador (*pentester*) não tendo conhecimento algum sobre o alvo no caso do *Black-box*, e tendo conhecimento total sobre o alvo no caso do *White-box*. O terceiro tipo, *Gray-box*, é destinado à simulação de um ataque interno, no qual o testador possui uma conta na rede interna do sistema e acesso padrão às funcionalidades. Os testes realizados neste trabalho seguiram o modelo *Black-box*, tendo somente conhecimento dos endereços que deveriam ser testados, construindo o resto do teste com base apenas nessa informação.

Um teste de invasão é constituído normalmente por sete fases, de acordo com OWASP (2016):

• Pré-engajamento;
• Coleta de informações;
• Avaliação de possíveis ameaças;
• Análise de Vulnerabilidades;
• Exploração;
• Pós-exploração;
• Relatório.

Na fase de **Pré-engajamento** acontece o encontro entre o *pentester* e os responsáveis pelos sistemas que serão testados, para definição de escopo, quais os limites dos testes, e quais testes poderão ser realizados, engenharia social e ataques de negação de serviço. A **Coleta de Informações** é a fase de descoberta de qualquer tipo de informação que seja de domínio público, como pesquisas sobre a organização alvo, seus colaboradores, qual sistema operacional, serviços, e versão de sistemas são utilizados, dentre outras. As fases de **Avaliação de possíveis ameaças** e **Análise de Vulnerabilidades** são de descoberta das vulnerabilidades em si, analisando quais são as mais críticas, nível de dificuldade de exploração, etc. **Exploração** é a fase na qual de fato as vulnerabilidades encontradas são exploradas, com o objetivo de comprometer as aplicações alvo e conseguir acesso. Na fase de **Pós-exploração** o objetivo é manter o acesso conseguido, para que seja possível voltar ao sistema com mais facilidade, sem necessitar explorar as vulnerabilidades novamente. A escrita do **Relatório** diz respeito à documentação de tudo que foi encontrado durante o *pentest* e que precisa ser corrigido, para que os administradores das aplicações alvo saibam o que necessita ser feito.

Este trabalho englobou as fases de pré-engajamento, coleta de informações, avaliação de possíveis ameaças, análise de vulnerabilidades, exploração e escrita do relatório.

Existem sistemas operacionais desenvolvidos especificamente para auxiliar em testes de invasão, sendo o mais utilizado o Kali Linux (https://www.kali.org/), que foi o escolhido para a realização dos testes deste trabalho. O Kali contém diversas ferramentas destinadas à análise de vulnerabilidades em aplicações Web, mapeamento de redes, ataques de força bruta, dentre outras. Dentre as ferramentas disponíveis, as seguintes foram utilizadas:

- BURP Suite;
- OWASP Zap;
- Nikto;
- SQLMap.

As ferramentas BURP Suite, OWASP Zap e Nikto são *scanners* automatizados de vulnerabilidades que foram utilizados na fase de descoberta de vulnerabilidades. Já o SQLMap é uma ferramenta para automatização de ataques do tipo *SQL Injection*, e foi utilizada durante a fase de exploração para avaliar se vulnerabilidades do tipo *SQL Injection* encontradas eram de fato válidas.

Resultados e Discussão

Com a realização dos testes de invasão nas aplicações Web da UEM, foi possível verificar que as aplicações de fato possuem vulnerabilidades, sendo algumas delas críticas, e que, se exploradas por algum atacante com más intenções, poderiam resultar em prejuízos de diferentes tipos, tanto para a universidade quanto para a comunidade acadêmica em si. Detalhes sobre as vulnerabilidades encontradas não são descritas neste artigo para resguardar os sistemas analisados. Evidências a respeito das vulnerabilidades encontradas foram documentadas e servirão de insumo para a equipe mantenedora dos sistemas realizarem a análise e tomarem as providências cabíveis visando à correção das vulnerabilidades.

Conclusões

Neste trabalho foi discutida a importância da segurança de aplicações Web, da informação, além de apresentar uma forma de descobrir vulnerabilidades, o teste de invasão, que se baseia nas mesmas técnicas que *crackers* utilizam, porém visando à correção dessas vulnerabilidades.
Tendo em vista que de fato foram encontradas vulnerabilidades nas aplicações da UEM, e sendo estas trazidas ao conhecimento dos administradores destes sistemas, chega-se à conclusão de que este trabalho foi útil para a comunidade acadêmica, contribuindo para melhorar a segurança das aplicações Web que são vitais para o funcionamento da UEM.
O próximo passo, além da continuidade da execução dos testes de invasão, é criar um guia para apoiar o desenvolvimento de aplicações Web mais seguras, com ênfase na mitigação de vulnerabilidades ainda na fase de desenvolvimento dos sistemas, pois é mais fácil realizar a solução de falhas em um sistema quando este ainda está em desenvolvimento do que após vários anos de uso.

Agradecimentos

Os autores agradecem o apoio dos analistas do NPD (Núcleo de Processamento de Dados) da UEM para realização deste trabalho.

Referências

KUMAR, S. **Classification and detection of computer intrusions**. 1995. Tese (Doutorado) — Computer Sciences Department, Purdue University, 1995.

WHITAKER, A.; NEWMAN, D. P. **Penetration testing and network defense**. 2005. Indianapolis, US: Cisco Press, 2005.

OWASP. **Penetration testing methodologies**. 2016. OWASP. Disponível em: https://www.owasp.org/index.php/Penetration_testing_methodologies. Acesso em: 26 jul. 2018.