O IMPACTO DA IMPLEMENTAÇÃO DA NORMA NBR ISO/IEC 17799 PARA DETECÇÃO DE FALHAS NA SEGURANÇA DA INFORMAÇÃO

BLIND REVIEW

Resumo **- A Tecnologia faz com que a tomada de decisão seja rápida, pois organiza processos, automatiza tarefas rotineiras, melhora o controle interno das operações, facilita o acesso e otimiza a tomada de decisões. A informação e os processos de apoio, sistemas e redes são importantes ativos para as organizações. Neste sentido, protegê-la de diversos tipos de ameaças minimiza danos, maximiza retornos dos investimentos, viabiliza novas oportunidades e garante a continuidade dos negócios. Este projeto propõe a análise da proposta de padronização da segurança da informação em empresas, de acordo com a norma NBR ISO/IEC 17799. Serão analisados como a norma está sendo adotada em empresas da região e qual o impacto da implantação da norma, no que compete à Segurança da Informação. Além disso, como trabalho futuro, é proposto um sistema para detecção de falhas na Segurança da Informação.**

Palavras-Chave **– segurança da informação, norma NBR ISO 17799, criptografia.**

THE IMPLEMENTATION THE IMPACT OF STANDARD ISO / IEC 17799 FOR DETECTION OF SAFETY INFORMATION FAILURES

Abstract **- The technology makes the decision-making is fast because it organizes processes , automate routine tasks , improve internal control of operations, facilitates access and optimizes decision-making. Information and the supporting processes , systems and networks are important assets for organizations. In this respect, protect it from various types of threats minimizes damage , maximizes investment returns , enables new opportunities and ensures business continuity . This project proposes the analysis of the proposed standardization of information security in companies , according to the standard ISO / IEC 17799. We will analyze how the standard is being adopted by companies in the region and the impact of the implementation of the standard , as it is for the Security of Information. Moreover, as future work , we propose a system for detecting faults in Information Security.**

Keywords - information security, ISO 17799 standard , encryption.

I. INTRODUÇÃO

Desde o surgimento dos computadores programáveis por volta de 1940 já havia a preocupação com a segurança da informação. Mesmo utilizando-se de cartões perfurados ou fitas perfuradas utilizadas nos telégrafos que não podiam ser copiadas, mas sim reproduzidas, já havia a preocupação da perda dos dados armazenados [1].

A invenção dos transistores por volta de 1948 pelos cientistas Walter H. Brattain, John Bardeen e John Bardeen, foi a revolução necessária para construir-se computadores cada vez menores e mais rápidos, e com isso a possibilidade de se criar programas cada vez mais eficientes e rápidos. Juntamente com os transistores apareceram, também, vários outros dispositivos como as impressoras, as fitas magnéticas que armazenavam o sistema operacional, os discos rígidos para armazenamento das informações: programas e linguagens de programação [1].

Os circuitos integrados, inventados por Jack Kilby por volta de 1958, possibilitaram a colocação de milhares e até milhões de componentes eletrônicos em um pequeno compartimento chamado de chip que diminuíram os computadores tornando-os portáteis, mais baratos e ao alcance da população.

Com o advento dos microcomputadores por volta de 1980 surgiram várias linguagens de programação como Basic, Cobol, C, Clipper, Pascal e várias outras. Diversos programas comerciais, jogos, editores de textos e planilhas; tudo gravado em discos de plásticos chamados de disquete e acoplados a um dispositivo chamado de disk drive – drive de disco [1].

Nesta etapa a preocupação com a informação já colocava-se bem acentuada devido ao armazenamento de dados da empresa como estoque e financeiro. Os disquetes serviam tanto para guardar o Sistema Operacional quanto programas e, também, o banco de dados pelo qual tinha-se tudo armazenado; produtos, vendas, clientes e a contabilização de compra e venda. As empresas agora se tornaram virtuais em termos de informações; tudo gravado em discos e fitas.

Cópias de segurança (Backups) se espalhavam pelas empresas em disquetes e fitas. Cópias diárias, semanais, mensais, trimestrais e de 6 em 6 meses. Tudo para garantir que a informação estivesse segura. Era prática levar cópias dos dados para a casa de algum funcionário de confiança. Em muitos casos disquetes e fitas falhavam tendo-se que recorrer a backups mais antigos e por muitas vezes perdia-se dados; e em outros casos que chamamos de Desastres, ou seja, a perda de todas as informações. A preocupação maior era com a falha da mídia de gravação, incêndio e roubo no

estabelecimento comercial e os já consagrados vírus de computador.

Com o surgimento da rede mundial de computadores – Internet, em 1990, para uso popular disseminou-se o conhecimento. As transações de informações entre as empresas passaram do papel para a forma eletrônica. Cada vez mais tinha-se computadores interligados em rede nas empresas e na internet. Os vírus continuavam a atacar neste período, não somente, em disquetes "infectados" que eram utilizados em vários computadores, mas "viajando" pela rede mundial, destruindo arquivos e deixando cada vez mais profissionais de tecnologia e donos de empresas preocupados com a segurança.

Surge atualmente mais um componente de destruição que é inteligente, de certa forma invisível e na maioria das vezes não deixa rastros por onde passa; é o famoso hacker. Indivíduo que apodera-se de senhas que estão gravadas ou que são capturadas através de softwares específicos para entrar em algum computador e realizar qualquer atividade como apagar informações, descobrir senhas de contas bancárias por onde pode-se fazer saques, desconfigurar sites, "derrubar" computadores e servidores, instalar programas por onde pode-se capturar informações necessárias para realizar atos ilícitos; como por exemplo o software ardamax .

Outra forma de invasão comum são através das caixas postais de e-mails que recebem dezenas, centenas de mensagens com textos falsos que tentam convencer o leitor a abrir e conferir seu conteúdo. Basta abrir a mensagem e um de seus anexos que o computador poderá ter recebido um ou mais programas maliciosos (vírus) que permitirá a captura de informações para o hacker apoderar-se de suas informações.

Cada vez mais empresas contratam serviços de profissionais para proteger suas informações e tentar minimizar as tentativas de invasão de computadores. Softwares antivírus tentam detectar a maioria das invasões provocadas por programas já conhecidos. Neste caso o antivírus precisa identificar as características comuns do programa invasor para poder identificá-lo e tratá-lo como um vírus, caso contrário o computador já está infectado.

O objetivo deste trabalho é pesquisar sobre aplicações de segurança da informação a fim de contribuir de maneira significativa com a melhoria dos níveis de segurança dentro das empresas. Além disso, neste trabalho propõe a criação de uma aplicação capaz de detectar falhas e evitar catástrofes.

II. FUNDAMENTAÇÃO TEÓRICA

A. Invasão

Muitas invasões são realizadas por falhas de sistemas operacionais ou de programas. Como por exemplo, a empresa IBM descobriu uma falha no sistema operacional Windows que persiste há 19 anos, desde a versão do Windows 95. Uma brecha que permite que o invasor entre no computador e através do Internet Explorer acesse uma URL que faça o download de algum conteúdo e através disso o controle do computador hospedeiro [3].

Até mesmo as novas tecnologias não estão a salvo. Uma vulnerabilidade nos Sistemas Operacionais iOS da Apple; falha identificada como "Masque Attack", são feitas através de instalação de programas que não fazem parte dos aplicativos da Loja da Apple. Com isso o invasor rouba o nome do usuário, senhas, captura seus dados e realiza acesso remoto.

Outra forma de invasão é através das portas de comunicação que dão entrada, saída ou entrada/saída de informações do computador. Estas portas devem ser "vigiadas" pelos profissionais de tecnologia da informação para verificar a ocorrência de invasões. Por exemplo a porta 80 é padrão para o protocolo HTTP (Hypertext Transfer Protocol – Protocolo de transferência de Hipertexto). Já para o serviço de FTP (File transfer Protocol – Protocolo de transferência de arquivos) é comum usar-se a porta 21. Pode-se usar outras portas para o mesmo serviço desde que especificadas para tal propósito.

Ataques digitais são feitos através de serviços DoS – Denial of Service. São comuns em servidores web que tem como propósito invalidar um serviço por sobrecarga. Outra forma é do tipo DDoS - Distributed Denial of Service, onde organizadores inserem vírus em computadores domésticos para enviar inúmeras requisições de serviços que possam "derrubar" um servidor.

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. Proteger a informação de diversos tipos de ameaças garante a continuidade do trabalho, minimizar os danos e maximizar o retorno dos investimentos e as oportunidades de negócio [2].

Quanto à importância, a informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado [2].

B. Criptografia

A criptografia é um conjunto de conceitos e técnicas que visa codificar (criptografar) uma informação de forma que somente pessoas autorizadas possam acessá-la, evitando que um intruso consiga interpretá-la. A criptografia é importante para que possamos proteger informações de cunho pessoal, senhas de banco, de redes sociais, cartões de crédito. Dados importantes para as empresas como as citadas anteriormente e sigilosas como uma pesquisa de mercado, um lançamento de produto, investimentos e muitos outros [4].

C. Assinatura Digital

A assinatura digital é uma tecnologia que permite dar garantia de integridade e autenticidade a arquivos eletrônicos. É um conjunto de operações criptográficas aplicadas a um determinado arquivo, tendo como resultado o que se convencionou chamar de assinatura digital. Permite comprovar que a mensagem ou arquivo não foi alterado e que foi assinado pela entidade ou pessoa que possui a chave criptográfica (chave privada) utilizada na assinatura.

*D. **Certificado Digital***

O Certificado digital é um documento digital, que comprova que uma chave privada pertence à determinada pessoa. Numa assinatura digital utiliza-se o certificado digital e a chave privada correspondente. É um documento eletrônico assinado digitalmente, contendo a identificação de uma pessoa, sua chave pública utilizada na verificação da validade da assinatura e assinado digitalmente por uma Autoridade Certificadora [4]

*E. **Vulnerabilidades***

Vulnerabilidades são falhas no software de computador que criam deficiências na segurança geral do computador ou da rede. As vulnerabilidades também podem ser criadas por configurações incorretas do computador ou de segurança. As ameaças exploram as vulnerabilidades, o que resulta em possíveis danos para o computador ou dados pessoais [5].

A análise de vulnerabilidade tem por objetivo identificar fragilidades de segurança no ambiente tecnológico de empresas, visando à implementação de controles que irão proteger suas informações e seus respectivos negócios. No processo de análise de vulnerabilidade são realizadas aferições visando à identificação de fragilidades técnicas de forma exaustiva sobre ambiente computacional de empresas. Esta análise possibilita evidenciar a exploração destas fragilidades através de um teste de penetração - penetration test - que utilizará ferramentas e técnicas para obter o acesso aos sistemas; complementado pela classificação de nível de risco, permitindo a priorização e o tratamento dos ativos mais expostos do ponto de vista de segurança e das respectivas operações de negócio [6].

III. NORMA NBR ISO/IEC 17799

De todos estes fatores e de outros que trazem muitos transtornos para o mundo globalizado da tecnologia é realizado um estudo detalhado da norma NBR ISO/IEC 17799. O objetivo da norma é: Fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações. Convém que as recomendações descritas nesta Norma sejam selecionadas e usadas de acordo com a legislação e as regulamentações vigentes [2].

A informação seja ela feita por qualquer tipo de mídia deve possuir como fundamentação básica: A sua integridade que consiste em garantir que os dados não foram alterados; a autenticidade que a informação transmitida e recebida é uma réplica da original; o não repúdio que visa a garantia de que o autor da informação não tenha como negar a criação e assinatura do documento e a irretroatividade que não permite que uma informação seja gerada com data anterior a atual.

Contudo, será feito um estudo detalhado da norma com ênfase em assinatura digital e criptografia onde são criadas chaves de segurança para encriptar e desencriptar uma informação. Através disto podem-se desenvolver políticas de segurança que visem estabelecer os requisitos, avaliar riscos e controles já existentes no intuito de utilizar as melhores práticas de segurança. A documentação, a definição de responsabilidades, o treinamento, os relatórios e a gestão certamente darão continuidade ao processo. Deste modo, com os controles já existentes, que estejam de acordo com a norma, como a criação de outros, diminuem-se riscos e pode-se chegar a níveis aceitáveis de segurança. A eficácia, por fim, dificulta ao máximo invasões que tanto prejudicam todo e qualquer processamento de informação.

IV. FERRAMENTAS PARA IMPLEMENTAÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

Apresenta-se a seguir ferramentas para verificação de vulnerabilidades em aplicações web, dispositivos móveis e banco de dados.

A ferramenta Burp Proxy gratuitamente encontrada no Kaly Linux captura solicitações e respostas entre o navegador e a aplicação web informando quais dados estão sendo transmitidos.

O Burp Proxy irá apresentar uma janela com os parâmetros da solicitação informando usuário e senha. Com estas informações pode-se alterar diretamente no proxy as solicitações antes de enviá-las ao servidor. O servidor jamais verá a solicitação original do navegador [7].

Na Figura 1 pode-se ver o resultado de uma solicitação HTTP get capturada informando usuário, senha e email de um site.

A ferramenta w3af(Web application attack and audit framework) é de código aberto; constituído de plugins para realizar vários tipos de testes em aplicações web à procura de vulnerabilidades inclusive de auditoria (audit). Este software utiliza 10 das principais categorias de vulnerabilidade do OWASP apresentadas na Tabela 1.

O software w3af é uma ferramenta para scanning e exploração de falhas de recursos web. O w3af oferece uma interface fácil de usar, que permite aos *pentesters* identificar rápida e facilmente quase todas as principais vulnerabilidades baseadas em web, conforme mostrado na Tabela 1, incluindo injeção de SQL, XSS, inclusão de arquivos, Cross-Site Request Forgery e várias outras [8].

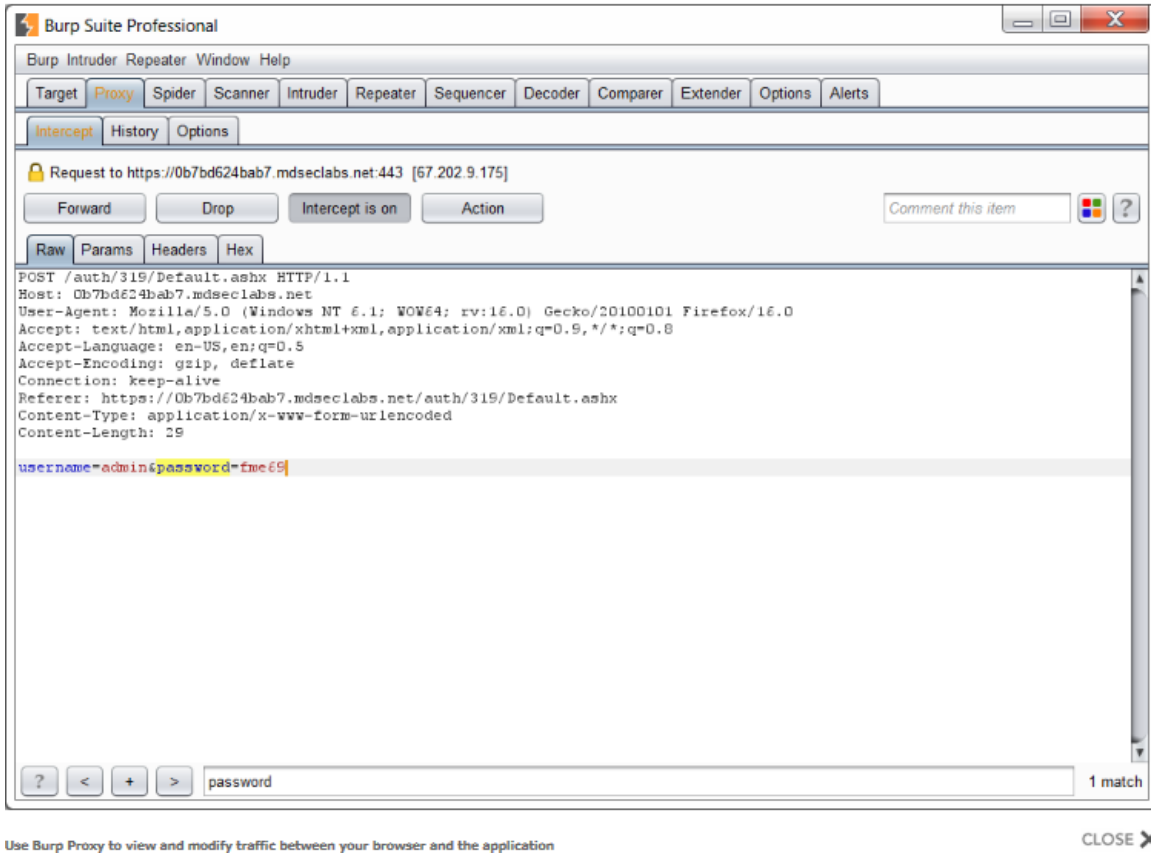

Fig. 1. Solicitação HTTP GET

Categoria	Descrição
1 – 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.
2 – 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.
3 – Cross-Site Scripting (XSS)	Falhas XSS ocorrem sempre que uma aplicação recebe dados não confiáveis e os envia ao navegador sem validação ou filtro adequados. 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.
4 – 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.

5 – 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.
6 – 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.
7 – 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.
8 – 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
9 – 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.
10 – 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.

Tabela 1 – Categorias de Vulnerabilidade do OWASP

Outra ferramenta para realizar-se testes de invasão é a Zed Attack Proxy (ZAP). O ZAP do OWASP é um toolkit completo para web hacking, que oferece três funcionalidades principais: Proxy de interceptação, spidering/ Web crawler (programa que navega pela internet à procura de informações) e scanning de vulnerabilidade [8].

Os dispositivos móveis estão cada vez mais presentes tanto na vida particular como nas organizações. Compartilhar é a palavra do momento. Os dispositivos compartilham informações através de mensagens, por comunicação por campo de proximidade (NFC) ou mesmo pela leitura de dados

de um QR code (Quick response code) que podem abrir códigos maliciosos.

A ferramenta Smartphone Pentest Framework (SPF), é uma ferramenta de segurança de código aberto, projetado para auxiliar na avaliação de segurança de smartphones. SPF contém ataques remotos, ataques de lado do cliente, ataques de engenharia social, e pós exploração.

Pode-se realizar ataques através do modem móvel tanto de telefones Android quanto nos iPhones. Através de SSH em telefones desbloqueados, atacar aplicativos de terceiros que possuem falhas, convencer o usuário a abrir uma página maliciosa e atacar o navegador com shell. Os ataques também podem ser feitos através de USSD (Unstructured Supplementary Service Data) que é uma maneira dos dispositivos móveis comunicarem-se com a rede móvel. Quando números específicos são discados, o dispositivo executa determinadas funções [7].

V. CONCLUSÕES E TRABALHOS FUTUROS

Em virtude do que foi mencionado, pode ser observado que a Segurança da Informação tem papel fundamental para proteger a informação de vários tipos de ameaças para garantir sua continuidade, minimizar o risco, maximizar o retorno sobre os investimentos e aumentar as oportunidades de negócios.

Como trabalhos futuros, pretende-se desenvolver um sistema para detecção de falhas na área de Segurança da Informação.

AGRADECIMENTOS

BLIND REVIEW.

REFERÊNCIAS

[1] MULLIN, RITA THIEVON (Org.). **Entenda o Computador – Input/Output**. 1ª Ed. São Paulo: Nova Cultural, 1988. 62 p.

[2] ABNT. NBR ISO/IEC 17799 - **Tecnologia da informação: código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2001.

[3] PORTAL G1, **Tecnologia e Games**. Disponível em: http://g1.globo.com/tecnologia/noticia/2014/11/governo-dos-eua-alerta-sobre-falha-no-sistema-operacional-da-apple-20141113183004012825.html. Acesso em 01 Março 2015.

[4] LOPEZ, FABIO DIAS; CAPARETO, LUIZ A. VIANA; e LIMA V. F. OLIVEIRA.. Disponível em: http://www.gta.ufrj.br/grad/10_1/quantica/quantica.html. Junho 2010. Acessado em Junho 2015.

[5] NORTON. **Como eles atacam**. Disponível em: http://br.norton.com/security_response/vulnerabilities.jsp. Acessado em Junho 2015.

[6] DATA SECURITY. Disponível em: http://www.datasecurity.com.br/index.php/seguranca/analise-de-vulnerabilidade-tecnica. Acessado em Junho 2015.

[7] WEIDMAN GEORGIA. Testes de Invasão. Uma introdução Prática ao Hacking. 1ª Ed. São Paulo: Novatec, 2014. 575 p.

[8] ENGEBRETSON, PATRICK. Introdução ao Hacking e aos testes de invasão. Facilitando o hacking ético e os testes de invasão. 1ª Ed. São Paulo: Novatec, 2014. 302 p.