Desenvolvimento prático de projetos de segurança da informação no Instituto Federal de Educação de Rondônia – Campus Ariquemes

Practical development of information security projects at the Federal Institute of Education of Rondônia – Campus Ariquemes

DOI:10.34117/bjdv8n2-225

Recebimento dos originais: 07/01/2022
Aceitação para publicação: 15/02/2022

Luciano Topolniak
Mestrando do Programa de Pós-Graduação em Ciência da Computação da Universidade Federal do Acre - UFAC
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – Campus Ariquemes
Rodovia 01, KM 13, S/N, Zona Rural, Ariquemes, Rondônia, 78.932-000
E-mail: luciano.topolniak@ifro.edu.br

Anderson Federice
Especialista em Cyber Security pela DARYUS Consultoria
Telefônica Tech
Av. Marcos Penteado de Ulhôa Rodrigues, nº 1690, Tamboré, 06543-001, Santana de Parnaíba/SP
E-mail: andfederice@gmail.com

Ricardo Ribeiro Tavares
Especialista em Cyber Security
DARYUS Consultoria / Gemina Threat Intelligence
Av. Yojiro Takaoka, 4384, Alphaville, SP
E-mail: ricardo@tavares.io

Sandra Regina da Luz Inácio
Pós-doutorado em negócios internacionais pela Flórida Christian University - Flórida - EUA
Instituto Daryus de tecnologia de São Paulo
Av. Paulista, 2001 - 620 – 3º Andar - Bela Vista, São Paulo - SP, 01311-300
E-mail: sandra@empresafamiliar.com.br

RESUMO
O presente artigo relata como foram criados e executados projetos de extensão sobre temas relacionados à segurança da informação, no curso técnico em manutenção e suporte em informática, do Campus Ariquemes, do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia. O objetivo foi verificar se os discentes do ensino médio técnico seriam capazes de, sobre orientação de um professor da área, elaborar e executar um projeto prático, sobre os temas, criptografia, engenharia social, SQL Injection WannaCry, dentre outros, apresentando-os e demonstrando a sua prática em uma palestra aberta à comunidade em geral. Os discentes foram alocados em grupos, onde receberam um tema específico, escreveram o projeto, aprenderam a utilizar as tecnologias pertinentes aos

temas, criaram apresentações de slides e apresentaram o tema em evento do Campus, demonstrando de forma prática a sua execução, obtendo sucesso nas suas atividades.

Palavras-chave: Segurança da Informação, Criptografia, Engenharia Social, SQL Injection, WannaCry.

ABSTRACT
This article reports how extension projects were created and executed on information security related topics, in the technical course in computer maintenance and support, Campus Ariquemes, Federal Institute of Education, Science and Technology of Rondônia. The objective was to verify if the students of the technical high school would be able, under the guidance of a teacher of the area, to elaborate and to execute a practical project, on the subjects, cryptography, social engineering, SQL Injection WannaCry, among others, presenting them and demonstrating their practice in a lecture open to the wider community. Students were assigned to groups, where they received a specific theme, wrote the project, learned to use the technologies relevant to the themes, created slideshows and presented the theme at a Campus event, practically demonstrating its execution, being successful in their activities

Keywords: Information Security, Cryptography, Social Engineering, SQL Injection. WannaCry.

1 INTRODUÇÃO

O presente trabalho discorre sobre um relato de caso a respeito da elaboração e execução de projetos de extensão executados no âmbito do Campus Ariquemes, do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia. Os projetos foram realizados pelos alunos do terceiro ano do ensino médio técnico, do curso de manutenção e suporte em informática, cursando a disciplina de segurança da informação.

O problema consistia em verificar se, "os alunos do referido curso, conseguiam, sob orientação de um professor da área, elaborar, executar e apresentar projetos específicos sobre temas relacionados à segurança da informação". O trabalho completo a ser desenvolvido pelos alunos consistia em escrever um projeto, registrá-lo no departamento de extensão do Campus, fazer um pequeno referencial teórico sobre o tema a ser abordado em cada projeto, treinar a execução da parte prática, elaborar slides para a apresentação ao público presente na palestra no evento "*O dia do Orgulho Nerd"*, desenvolver a parte prática frente ao público, escrever o relatório final para o fechamento do projeto no Departamento de Extensão.

A motivação para o desenvolvimento dos projetos se deu devido ao fato do tema segurança da informação ter se tornado mais conhecido nos dias atuais, devido aos inúmeros ataques que têm sido veiculados nos meios de comunicação em massa,

praticamente todos os dias. Mesmo assim, muitas pessoas não têm conhecimento específico sobre o tema e não fazem ideia de como elas e seus dados estão expostas na grande rede de computadores chamada Internet, e, por isso, não tomam nem as medidas mais simples para a própria proteção.

Com o aumento de consumo de telefones inteligentes com acesso à Internet e a redução dos custos de conexão à mesma, o número de usuários aumentou consideravelmente. Contudo, com o aumento do número de usuários, vem também o aumento de dados e pessoas expostas, pois a maioria, não está comprometida com a segurança digital e online, e, muitos usuários não acreditam que possam ser alvos de um ataque, e que se forem, não tem nada de importante para ser exposto que possa vir a se tornar um possível prejuízo financeiro ou para a sua imagem.

Nesse sentido, sabendo-se que mesmo profissionais de tecnologia muitas vezes não se preocupam com a segurança digital, faz-se necessário que cada vez mais cedo, os alunos de escolas do ensino médio passem a ter esse conhecimento, para que possam saber como a tecnologia e os ataques funcionam e como podem se proteger deles. Dessa forma, formando mais cidadãos comprometidos com a segurança digital e que, futuramente, irão disseminar esse conhecimento a outros, tornando assim o mundo digital mais seguro e as pessoas menos propensas à exposição online.

A relevância do projeto fica por conta da própria necessidade de se conhecer os temas intrínsecos à segurança da informação por parte de todos os cidadãos. Nesse ínterim, levar os alunos do ensino médio a trabalhar com tais temas, não só os prepara para atuar no mercado de trabalho, como também faz com que os assuntos sejam conhecidos destes, e também promovem a propagação do tema aos demais, que assistiram as palestras e seus contatos futuros. Nesse contexto, acredita-se que a principal diferença do presente trabalho em ralação aos já realizados e publicados, se dá exatamente por trabalhar com pessoas que estão em idade escolar do ensino médio, ou seja, que ainda não ingressaram na faculdade e com isso, o tema segurança da informação poderá também ser fator considerado na escolha de sua futura profissão.

2 REFERENCIAL TEÓRICO

A cada dia, a corrida para levar os negócios para a Internet se torna mais frenética, grandes empresas já se estabelecerem no mercado online e agora é a vez das pequenas começarem a trilhar esse caminho. Todavia, nessa corrida, é necessário ficar atento ao quesito segurança da informação. É imprescindível contratar serviços que protejam e

garantam a integridade e disponibilidade dos dados expostos na Internet contra roubos e alterações.

Para tornar as aplicações *webs* seguras contra ataques maliciosos é preciso investir em servidores e redes seguras, pois:

> À medida que serviços de Tecnologia da Informação surgem nas diversas áreas e ficam disponíveis para melhorar a vida das pessoas, também ficam vulneráveis a ataques cibernéticos das mais diferentes formas, estes ataques visam causar a indisponibilidade de sistemas e serviços, obter acesso não autorizado, roubo de dados, propagação de códigos maliciosos em rede de computadores (CRUZ, 2017)

Segundo (BERTOGLIO; ZORZO, 2016) "Os riscos relacionados com a segurança de informações em empresas, organizações e entidades que trabalham com dados sensíveis, sejam eles públicos ou não, têm obtido certa expressividade nas preocupações de tais instituições", assim, com os ataques cibernéticos cada vez mais presentes no cotidiano das pessoas, as empresas têm empenhado esforços para se proteger no mundo cibernético.

Desta feita, melhor é se antecipar aos indivíduos mal intencionados e realizar um *pentest* - teste de invasão, que segundo (WEIDMAN, 2014), é a simulação de ataques reais para avaliar os riscos e potenciais brechas de segurança. Uma vez que o teste foi realizado, será possível conhecer as falhas expostas e proceder com suas correções, evitando assim um ataque real e o comprometimento dos serviços, dados e a imagem da empresa.

Para a realização de um teste de invasão se faz necessário a contratação de pessoa ou empresa especialista no assunto, pois o mundo da segurança da informação é vasto e profundo. Sistemas já nascem com *bugs* e centenas ou milhares de pessoas no mundo estão em busca desses *bugs* para explorá-los, seja para o bem, seja para o mal.

Um *Pentester – Profissional que realiza o teste de penetração*, é um profundo conhecedor de redes, sistemas operacionais e ferramentas de exploração de falhas de segurança, a diferença entre um *pentester* e uma pessoa mal intencionada é que o *pentester* decidiu usar os seus conhecimentos para o bem, enquanto o outro, para o mal.

Para se tornar um *Pentester* é preciso estudar bastante, pois os assuntos relacionados à segurança da informação são vastos. Por isso, quanto mais cedo o contato, melhor. Dentre os assuntos estudados, estão os elencados nos projetos desenvolvidos, a seguir.

2.1 CRIPTOGRAFIA

A criptografia é a tecnologia que garante as transações seguras na Internet, ela provê mecanismos para o tráfego de informações de forma que, se tais informações forem interceptadas por um terceiro, este não conseguirá obter acesso inteligível à mesma em tempo hábil para que possa tomar alguma decisão.

Foi a criptografia que possibilitou a comunicação entre emissor e receptor de forma segura em canais públicos, bem como, alavancou as transações financeiras na Internet e a popularização dos *Internet Bankings* e o comércio eletrônico.

No entanto, a criptografia pode ser usada para fazer o mal e extorquir alguém, é o caso dos *ransomwares*, que usam a criptografia de discos para sequestrar os dados dos usuários, exigindo pagamento para voltá-los ao seu estado original.

A criptografia também é usada para o armazenamento seguro de dados nos bancos de dados das empresas, visando assegurar que, caso haja algum vazamento, tais dados não serão facilmente descriptografado.

De forma simples, de acordo com (CERT.BR, 2012), a criptografia é definida como a ciência de escrever em códigos de forma que os dados criptografados não sejam inteligíveis sem o processo inverso que torna o texto cifrado em texto claro novamente.

Apesar de ser um dos pilares da transformação digital no que diz respeito ao tráfego seguro de dados, a criptografia começou de forma simples, quase sempre relacionado à comunicação segura em tempos de guerra. Conta a história que um dos primeiros algoritmos conhecidos foi a Cifra de César, criada pelo então Imperador Júlio César para se comunicar com suas tropas. (SILVA, 2019)

A cifra de césar é um algoritmo bastante simples para os dias atuais, servindo apenas para fins didáticos, uma vez que conhecido o seu funcionamento, é fácil quebrá-lo por força bruta. Ele consiste em alterar as posições das letras do alfabeto determinadas posições para frente para cifrar e para decifrar faz-se o processo inverso. (COUTINHO, 1997)

Com o tempo os algoritmos criptográficos evoluíram e passaram a ser classificados como criptografia simétrica e assimétrica. Os algoritmos simétricos são aqueles em que a mesma chave criptográfica usada para cifrar a mensagem, é usada para decifrá-la. Fazendo com que a segurança esteja na proteção da chave, que precisa ser compartilhada entre o emissor e o receptor.

Atualmente esses algoritmos ainda são bastante usados, por serem rápidos para cifrar e decifrar. Contudo apresentam grande problema, que é o gerenciamento das

chaves, pois, como já dito, necessitam ser compartilhada entre o emissor e o receptor, fazendo com que a distribuição da chave de forma segura, seja um problema. Os algoritmos de chave simétricas mais citados na literatura são, *AES*, *Blowfish*, *DES* e o *3DES*, sendo esse último uma melhoria do DES.

Já a criptografia de chave assimétrica representou um grande avanço na comunicação segura, fazendo com que o seu algoritmo além de ser aberto, ou seja, de conhecimento de todos, funcione com um par de chaves, denominadas de chave pública e chave privada. Desta forma, o algoritmo de criptografia assimétrica é programado de tal forma que a chave que cifra o texto, não serve para decifrá-lo. Numa analogia simples, é como se um cadeado possuísse duas chaves, a chave que o fecha, não o abre.

O algoritmo de chaves assimétricas melhorou o problema de distribuição das chaves, uma vez que o emissor mantém segura somente a chave privada e distribui abertamente em servidores na internet a sua chave pública. Desta forma, quando o portador da chave privada cifra uma mensagem, os detentores da sua chave pública conseguem decifrá-la para a leitura. Esse processo dá ao receptor a garantia da origem da mensagem.

O processo inverso também é bastante interessante, pois qualquer pessoa pode acessar a chave pública de um par de chaves e cifrar uma mensagem, tendo plena certeza de que somente o detentor da chave privada poderá decifrá-la.

Contudo, os algoritmos de chave assimétricas são lentos se comparados aos algoritmos de chaves simétricas. O que fez nascer a criptografia híbrida, que faz uso das duas técnicas. Usa-se as chaves públicas e privadas para estabelecer uma comunicação inicial segura, a partir de então, as chaves simétricas são geradas e enviadas pelo canal seguro, então, a cifragem e decifragem são realizadas pelo algoritmo de chave simétrica.

O algoritmo de chave assimétrica mais famoso e mais usado atualmente é o *RSA* - que leva as iniciais dos nomes dos seus criadores, *Ron Rivest*, *Adi Shamir* e *Leonard Adleman* - e funciona através da técnica matemática de fatoração de números primos gigantes (SILVA, 2019), processo lento para ser realizado com o poder computacional atual, o que faz com que, mesmo se a mensagem seja interceptada, o interceptador levaria anos para conseguir decifrá-la e usá-la, o que desencoraja tal ato.

2.2 ENGENHARIA SOCIAL

A Engenharia Social é um tipo de ataque que surgiu muito antes da propagação da internet. Ela faz uso da manipulação psicológica das pessoas, usando da inocência,

medo, senso de urgência, responsabilidade, curiosidade ou até mesmo da sua ganância. A maioria das pessoas estão susceptíveis a algumas dessas características. (WEIDMAN, 2014)

2.2.1 Engenharia social antes da internet

A inocência faz com que determinadas pessoas caiam em golpes por acreditarem em outras pessoas, com isso, acabam fazendo o que elas pedem, sem imaginar que podem estar sendo manipuladas.

Já o medo é um fator que está presente em quase todas as pessoas do universo, todas têm algum tipo de medo. A Engenharia Social faz uso dessa característica para manipular as pessoas persuadindo-as a clicar em um link para resolver um problema no sistema de proteção de crédito por exemplo, por medo de ficarem com o nome sujo. Até mesmo em um falso sequestro esse método é utilizado, pois por medo, a pessoa alvo acaba por fazer o que o atacante solicita.

Do mesmo modo, a ganância é inerente a quase todos os seres humanos, de alguma forma, todos querem se dar bem, tirar proveito para si de alguma situação que se lhe apresenta, uma promoção irrecusável, um erro no valor de um produto em uma loja virtual. Por fim, todos esses mecanismos acabam sendo usados para persuadir o alvo a fazer algo de interesse do atacante.

Portanto, a engenharia social não é algo exclusivo da internet, pois muito antes desta, ela já existia com várias técnicas, que são usadas até os dias de hoje, mesmo em tempos de alta conectividade e *fake news* diárias. Olhar sobre o ombro de alguém quando ela digita uma senha, ligar para uma empresa se passando por um superior, manipular alguém através de conversa para conseguir informações confidenciais, vasculhar o lixo do alvo, etc, são técnicas usadas para auferir algo de outrem, sem que o mesmo perceba que está sendo manipulado para tal. (MAGNO; ROSAL, 2017), (UTO, 2013)

Desta forma, segundo (SILVA, 2015), a essência da engenharia social está em usar a fragilidade das pessoas contra elas mesmas, pois como se sabe, o fator humano é o elo mais fraco da segurança da informação;

2.2.2 Engenharia social na internet

Com a popularização da Internet e o considerável aumento de usuários leigos quanto a segurança da informação, a engenharia social evoluiu com fins de alcançar o

maior número possível de pessoas. Dentre as técnicas mais utilizadas na Internet estão o *Phishing*, o *Spear Phishing* e o *Pharming*.

O *Phishing* é a técnica conhecida como pescaria, pois através dela o atacante elabora e-mails que se passam por e-mails de empresas idôneas oferecendo serviços aos usuários, buscando levá-los a clicar em links que os levam para sites falsos ou baixam programas maliciosos em seus computadores. Na maioria das vezes visam capturar dados pessoais e financeiros dos usuários desatentos.

Já o *Spear Phishing* é similar ao *Phishing*, contudo é mais direcionado a uma empresa específica, a determinado departamento. Nessa técnica o atacante elabora e-mails concernentes a assuntos ligados ao alvo, fazendo com que o mesmo seja interessante ao alvo, levando-o a cair no golpe.

Por fim, o *Pharming* tenta se passar por um endereço *url* válido, fazendo com que o mesmo seja muito parecido com o original, o que dá confiança e segurança para a vítima, que na maioria das vezes não percebe a sutil diferença e acaba clicando na *url* e preenchendo cadastros, informando dados reais em um formulário de site falso.

2.2.3 Engenharia social e a propagação das ferramentas

A engenharia social evoluiu de tal modo que o número de ferramentas para a sua prática tem crescido consideravelmente, fazendo com que qualquer pessoa com conhecimentos básicos e um pouco de estudos possa criar um site falso que se pareça com o original, levando as pessoas a informarem seus dados, credenciais de acesso, e-mails e dados financeiros.

Como exemplo dessas ferramentas, tem-se algumas bastante conhecidas e utilizadas, como o *setoolkit* (TRUSTEDSEC, 2019) presente no kali linux, e *blackeye* (THELINUXCHOICE, 2019), que são ferramentas poderosíssimas, por apresentarem diversas opções aos seus usuários e serem de fácil uso. Tais ferramentas permitem que com um servidor web simples, páginas possam ser copiadas para se passarem pelas originais, visando a captura de credenciais de acesso e dados pessoais.

2.3 SQL INJECTION

Dentre as falhas mais conhecidas e exploradas na Internet se encontra o *SQL Injection*, que é uma falha causada pelo fator humano, ou seja, não é uma falha de software, mas sim um erro de lógica cometido pelos programadores ao escreverem as sentenças SQL que retornam dados dos bancos de dados para as aplicações web.

Segundo a (SFAKIANAKIS et al., 2018) e (OWASP, 2018) as falhas de injeções de comandos estão entre as mais exploradas nos últimos três anos, e a injeção de SQL figura em primeiro lugar dentre essas falhas, concentrando 51% dos ataques em aplicativos web.

A falha de injeção de SQL pode ser explorada manualmente através da passagem de comandos na *url* das aplicações web, no entanto, essa técnica varia bastante de um Sistema Gerenciador de Banco de Dados (SGDB) para outro, o que faz com que o atacante precise ter muito conhecimento sobre os diversos SGDBs existentes. No site da *Open Web Application Security Project* (OWASP) (OWASP, 2019), pode ser encontrado um guia completo sobre as técnicas de exploração de vulnerabilidades de aplicações para a internet.

No entanto, o processo pode ser automatizado com as diversas ferramentas criadas para tal. Pode-se usar ferramentas de varredura de falhas para identificar se determinada aplicação web apresenta falha de injeção de SQL e após isso, usar ferramentas que automatizem o processo de exploração para a obtenção dos dados ou até mesmo levar a uma invasão do sistema operacional do servidor que armazena o banco de dados.

A ferramenta mais conhecida para automatizar o processo de exploração de injeção de SQL é o *SQLMap*, que já vem instalada dentre as muitas ferramentas encontradas no *Kali Linux*. Através dessa ferramenta e de posse de uma *url* de aplicativo web com a vulnerabilidade é possível obter o banco de dados inteiro do aplicativo, ou obter as credenciais de acesso para se apossar da aplicação. Outras duas ferramentas conhecidas para automatizar o processo de injeção de sql são *Havij* e *JSQL*, que também realizam o processo sem muitas interações com o usuário, tornando o trabalho bastante simplista.

2.4 SEGURANÇA DE SENHAS

Para a garantia de privacidade e autenticação nos mais variados serviços, o uso de credenciais de acesso é o recurso utilizado. Ela garante que a pessoa é quem ela diz ser. Por credenciais de acesso, entende-se o uso de nome de usuário e senha. O nome de usuário não é tão relevante, pois pode ser conhecido de terceiros, tal como nas redes sociais, onde as pessoas são conhecidas pelo seu acrônimo, seu login de acesso.

Já a senha é o que determina a privacidade, o acesso restrito e legítimo pelo seu dono portador. Para a autenticação, basicamente tem-se três formas, a saber, aquilo que você é, digital, íris, aquilo que você possui, *token*, e aquilo que você tem, senha.

Nas senhas encontram-se a segurança e a legitimidade de um acesso a um serviço, seja ele online, acesso físico, etc. Portanto, ter uma senha segura é extremamente necessário. Credenciais de acesso são o alvo da maioria dos ataques na Internet, pois de posse das credencias de uma pessoa, o atacante se passa por ela, acessando todos os serviços nos quais ela faz uso com a mesma senha.

No entanto, a segurança de senhas é um problema recorrente, pois as pessoas cometem diversos erros ao criar as suas senhas. Dentre os principais erros estão: Senhas pequenas demais, contendo apenas letras, apenas números, sem unir letras e números a caracteres especiais, envolvendo nomes dos filhos, datas de nascimentos de pessoas próximas, nomes de animais de estimação, que são de uso comum, estando listadas entre as mais utilizadas no mundo com base em relatórios de dados vazados.

Na maioria das vezes, as pessoas definem senhas que lhes são fáceis de memorizar, e com isso acabam por definir uma senha simples e usando a mesma senha em vários serviços, o que acarreta em grande risco, pois se um determinado serviço ocorrer o vazamento de dados, a senha estará comprometida.

Para uma senha ser considerada segura, ela deve pelo menos: Conter no mínimo oito caracteres, letras Minúsculas: (a, b, c), letras Maiúsculas (A, B, C), dígitos numéricos (0..9), símbolos: (#, , _,), e caracteres Unicode, enfim, criar uma senha conforme preconiza a norma brasileira 27002 ISO/IEC 27002 que é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação para as empresas.

Muitas vezes, quando um determinado serviço exige uma senha mais complexa para o usuário, este incorre em um erro básico, que é anotar a senha em uma agenda ou em lugar de fácil acesso por terceiros.

Por outro lado, muitos serviços, por erro de desenvolvimento e inexperiência dos desenvolvedores ou até mesmo de forma intencional, armazenam as senhas dos usuários em texto claro, ao invés de armazenar um *hash* da mesma. Uma função hash é um algoritmo que transforma uma entrada em um texto diferente do mesmo, contudo, correlacionado a ele, sendo assim, ao ser armazenado, a senha seria ininteligível para quem a visualizasse.

O problema das senhas curtas demais ou as que fazem uso de somente dígitos numéricos é que elas são facilmente quebradas por softwares específicos de força bruta, que consiste em testar todas as possibilidades até encontrar a senha. Outro método bastante utilizado são as chamadas *rainbow tables*, tabelas arco íris, que nada mais são que tabelas de equivalências de senhas em texto claro com suas versões em *hashes*. Assim, se uma senha, mesmo que esteja *cifrada*, cair nas mãos erradas, ela poderá voltar a ser um texto claro, se for uma senha simples que já esteja presente nas tabelas de equivalências.

Um dos mecanismos atuais para tentar mitigar o problema dos vazamentos de senhas e senhas fracas é o método de autenticação em dois fatores, que exige que o usuário ao acessar um serviço e informar a sua credencial de acesso, tenha que confirmar esse acesso através de outro dispositivo em sua posse. Mesmo assim, já há notícias de que a autenticação em dois fatores tenha sido burlada em alguns serviços por pessoas mal intencionadas.

As empresas devem criar uma política de senhas seguras e forçar os seus usuários a isso, bem como o seu armazenamento em local seguro, fazendo uso de cofres de senhas, onde uma senha mestra dá acesso às demais. Assim, o usuário só precisaria memorizar uma senha complexa e segura, para acessar o seu cofre e então teria acesso às demais.

Outro mecanismo de segurança de senhas é fazer com que o usuário seja forçado a trocá-la periodicamente e não permitir que ele use a mesma senha para mais de um serviço na empresa.

2.5 VULNERABILIDADES DO WORDPRESS

O WordPress é um gerenciador de conteúdo, desenvolvido na linguagem *PHP*, que usa do *MySQL* para armazenar os dados. Sua facilidade de uso e instalação fez com que imediatamente tivesse um estrondoso sucesso, que o acompanha até os dias atuais. O WordPress é perfeito para quem necessita colocar um site no ar em poucas horas, sem se preocupar com a programação da estrutura do mesmo, mas sim, somente com o seu conteúdo e aparência da página web.

Segundo (LEWIS, 2019), o WordPress abocanha 59% do *market share* de gerenciadores de conteúdo do mundo, mais do que os também famosos *Drupal* e *Joomla* combinados.

(LEWIS, 2019) afirma também que aproximadamente 75% dos 40.000 sites populares desenvolvidos sobre o WordPress estão vulneráveis. A maioria dos problemas

de vulnerabilidades estão relacionadas ao fato de que somente 25% destes sites estão executando a última versão lançada. Ou seja, seus administradores não se preocupam com a atualização do mesmo, fazendo com que vulnerabilidades conhecidas não sejam corrigidas.

Outro fator preponderante ao se falar no WordPress é a quantidade enorme de plugins disponíveis para o mesmo, no repositório oficial há mais de 50.000 plugins disponíveis para download. Esse número enorme de plugins, desenvolvidos por diferentes programadores, faz com que o número de vulnerabilidades aumente consideravelmente, pois muitos desses plugins ficam abandonados, sem atualizações pelo desenvolvedor e pelos administradores dos sites que os usam.

A grande popularidade do WordPress também faz com que ele seja alvo constante de ataques visando a sua invasão. Várias ferramentas foram desenvolvidas para automatizar o processo de escaneamento de vulnerabilidades. Nem todas as ferramentas foram criadas com o fim de destruir, mas o que determina o bom e o mau uso é a pessoa que a usa.

Uma das ferramentas mais conhecida é o *WPScan*, criada pela empresa de segurança voltada para a Web, Sucuri.

O *WPScan* mantém uma base de dados de vulnerabilidades conhecidas do WordPress e dos seus plugins. Ao fazer uma varredura, ele consegue elencar as vulnerabilidades que estão presentes no web site escaneado. Esta ferramente é capaz de listar as vulnerabilidades do *core* do WordPress baseado na versão instalada, enumerar os plugins, temas e suas vulnerabilidades, enumerar também os usuários presentes no mesmo, bem como tentar força bruta contra a senha dos usuários listados, fazendo uso de uma *wordlist*.

Para manter o WordPress seguro, deve-se mantê-lo sempre atualizado, usar somente os plugins e temas realmente necessários, excluindo tudo o que não está em uso. O próprio WordPress oferece pacotes de plugins voltados à sua segurança, que implementam diversas características, tais como, *captcha*, tentativas de login limitadas, dentre outras. Uma lista completa de como manter o WordPress seguro pode ser encontrada em (SUCURI, 2018).

2.6 RANSOMWARE WANNACRY

Segundo o (CERT.BR, 2012), existem dois tipos de *Ransomwares*, o que impede que o usuário acesse o seu equipamento, que é o denominado *Locker*, e o *Crypto*, que

impede que os dados do equipamento infectado sejam acessados. Esse último geralmente faz uso da criptografia. Desta forma, o método de ataque do *Locker* é basicamente criptografar os dados do disco do usuário e exigir um pagamento, que geralmente é em moeda digital (criptomoeda), para que os arquivos sejam descriptografados.

A periculosidade do Ransomware é tamanha, pois além de infectar o equipamento da vítima ele é capaz de se espalhar pela rede de computadores, buscando novos alvos que também estejam vulneráveis.

No entanto, para se proteger desse tipo de ataque, não é necessário fazer nada especial, além do que já deve ser feito normalmente para estar seguro, que é, manter sempre o sistema operacional do computador atualizado, ter software de segurança, tal como um antivírus instalado e atualizado, e, consciência de não clicar em links em e-mails cujo os quais não solicitou, tampouco executar arquivos desconhecidos.

Em se tratando de segurança da informação, o mundo se divide em, antes e depois do WannaCry, pois esse *ransomware* infectou computadores em 150 países no mundo, inclusive no Brasil. As notícias saíram dos jornais e blogs que circulam na internet e foram parar nos jornais de destaques em rede nacional nas grandes emissoras de televisão.

Muitos foram os prejuízos causados pelo WannaCry e sua popularidade foi tamanha, contudo, muitas pessoas continuam não aprendendo a lição ou por descrença, não tomam as medidas necessárias para mitigar o problema. O fato é que até os dias atuais, tal ransomware continua fazendo novas vítimas. (MACKENZIE, 2019)

3 METODOLOGIA

A metodologia utilizada neste trabalho foi a revisão bibliográfica, de natureza pura, exploratória e descritiva, seguida de intervenção. Foi realizada pesquisa e revisão bibliográfica que, segundo (GIL, 2002), é desenvolvida principalmente sobre livros e artigos científicos a respeito dos temas abordados, que neste caso foram: *Criptografia*, *engenharia social*, *SQL Injection*, *segurança de senhas*, *vulnerabilidades do WordPress* e o *Ransomware WannaCry*.

Para (CRUZ, 2017), a segurança da informação visa a proteção dos dados e informações de indivíduos ou organizações. No entanto, na segurança digital há um consenso que diz que, para proteger os ativos de um possível ataque é preciso saber como o criminoso atua, em outras palavras, não podemos nos defender sem saber como o ataque funciona.

Desta forma, os projetos exploraram como os ataques são realizados e como devem ser os procedimentos para mitigar seus efeitos, ou mesmo, impedir que eles aconteçam.

Sendo assim, tão logo definidos os temas para cada equipe, foi realizada a revisão bibliográfica para que os alunos pudessem se inteirar sobre o tema e conseguir realizar os procedimentos de forma prática.

Uma vez registrados os projetos, cada equipe preparou o ambiente de execução dos mesmos, alguns temas necessitaram de ambiente controlado para sua execução, que foram preparados e testados previamente. A execução em ambientes controlados deu-se devido a segurança da infraestrutura do Campus, bem como, problemas legislativos, ou seja, não podem ser executados sem o prévio consentimento do alvo, sobre pena de infringir a lei e sofrer as possíveis consequências deste ato.

4 RELATO DE CASO

Em praticamente todos os anos, o Campus Ariquemes, do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, através do Curso Técnico de Informática Integrado ao Ensino Médio, organiza o evento denominado de "*O dia do Orgulho Nerd*". Nesse evento são criadas diversas atividades para os alunos, servidores do Campus e também para a comunidade externa, numa tentativa de integrar o Instituto à comunidade ariquemense.

Um dos objetivos do evento é que os alunos produzam atividades, tais como, protótipos, palestras, cursos, dentre outros. Neste ano, 2019, o evento tomou uma proporção maior, envolvendo outros dois cursos, Alimentos e Agropecuária, ambos, integrados ao Ensino Médio.

Nesse ínterim, vários alunos me procuraram para orientá-los em alguns projetos. Eu disse a eles que tinha interesse em projetos relacionados ao tema segurança da informação, e lancei algumas ideias. Por estarem cursando uma disciplina relacionada ao assunto, inclusive de mesmo nome, vários alunos aceitaram a ideia e partimos para a definição dos temas.

Foram formados seis grupos dentre os alunos que decidiram fazer sobre segurança da informação, os temas escolhidos para trabalharem foram: Criptografia, Engenharia Social, SQL Injection, Segurança de senhas, Vulnerabilidades do WordPress e Ransomware WannaCry.

Para cada equipe, foi necessário escrever um projeto de extensão e registrá-lo no departamento de extensão da instituição. Todos os projetos seguiram os padrões solicitados pelo departamento. Após escritos, revisados e aprovados pelo orientador, todos os projetos foram submetidos ao departamento de extensão e aprovados.

Cada projeto contemplava uma revisão bibliográfica sobre o tema, a realização prática de exploração do tema selecionado, a elaboração de uma palestra para apresentar ao público presente no dia do evento, a demonstração prática do projeto e a escrita do relatório final para a apresentação no departamento de extensão e conclusão dos mesmos.

4.1 DESENVOLVIMENTO DOS PROJETOS

Nesta seção será apresentada pequena descrição de como cada projeto foi implementado na prática.

4.1.1 Criptografia

Para o projeto de criptografia, para que o mesmo fosse o mais simples possível e interessante para os participantes, que na sua maioria eram leigos e não pertencentes à área de informática, os alunos decidiram abordar o algoritmo cifra de césar, que é um dos algoritmos mais simples, usado atualmente como material didático sobre o tema. Contudo, foi abordado sobre os algoritmos atuais durante a palestra apresentando os conceitos gerais de criptografia, além da sua importância para o mundo atual.

Em suma, o que foi realizado pelos alunos foi construir um texto cifrado com o algoritmo cifra de césar e explicar aos presentes o funcionamento do mesmo, colaborando para que todos fizessem o processo de descriptografia. Voltando o texto cifrado em texto claro, e vice e versa.

Após a primeira dinâmica, realizada no papel e o entendimento do algoritmo pelos presentes, foi utilizado um site que cifra e decifra usando o algoritmo em questão. Todos puderam praticar e usar o algoritmo através do site <https://rot13.com/>, uma vez que a palestra foi ministrada no laboratório de informática.

4.1.2 Engenharia social

Para o trabalho de engenharia social foi instalado o *Kali* no laboratório de informática para que os palestrantes pudessem usá-lo para demonstrar na prática o conceito e como ela funciona.

Primeiramente foi abordado sobre o tema através de slides, apresentado o que é engenharia social, os tipos existentes e como ela é usada pelos atacantes, para conseguir as informações dos usuários.

Após feita a explanação conceitual, a equipe levantou o servidor na máquina *kali linux* e preparou uma página falsa que solicitava as credenciais do *facebook* para acessá-la, a ferramenta utilizada para a prática foi o *Social Engineering Toolkit - SEToolkit*. Os alunos estavam na mesma rede e podiam acessar o servidor pelo endereço IP e visualizar a página. Antes de tudo, foram informados para não colocarem as suas credenciais verdadeiras, pois elas seriam mostradas em texto claro à todos. Ao realizarem os testes e informarem suas credenciais, todos puderam ver o relatório de logins e senhas informadas pelos mesmos, perplexos.

Dessa forma, todos os presentes ficaram impressionados com o ato, pois o desconheciam. Não tinham ideia de que ao informar suas credenciais em um site, elas poderiam ser interceptadas, visualizadas por um terceiro e usadas com fins ilícitos. Passaram a ter um pouco mais de preocupação com as formas de *Phishing* e como elas se lhes apresentam no dia a dia.

4.1.3 Sql injection

O evento iniciou com a equipe fazendo uma apresentação de slides explicando os conceitos de *SQL Injection*, suas formas, ferramentas utilizadas e o perigo que essa falha representa para as empresas, pois através dessa técnica, bancos de dados inteiros podem ser capturados.

Após as explicações iniciais, partiu-se para uma demonstração prática usando o site <http://testphp.vulnweb.com/> que é um site voltado para testes de penetração, com diversas vulnerabilidades, dentre elas, a falha de Injeção de SQL. Começou-se com comandos básicos de forma manual para exemplificar como a falha funciona e logo após foi feito o uso de ferramentas que automatizam o processo, tais como, *Havij* e *SQLMap*.

Através do *SQLMap*, foi acessado e listado o cadastro de usuários do site, mostrando o login e senha para acesso ao painel de controle do mesmo. O painel de controle foi acessado com o login e senha obtidos e os dados foram alterados, para demonstrar que uma vez de posse das credenciais do administrador do site, pode-se sequestrar o mesmo, além de roubar os dados presentes no banco de dados ou fazer modificações no mesmo.

4.1.4 Segurança de senhas

No projeto segurança de senhas foram abordados temas conceituais, tais como, complexidade de senhas, ou seja, o tamanho, caracteres utilizados para formar uma senha considerada segura, senhas mais utilizadas nos últimos três anos, armazenamento seguro de senhas através de *hashes*, como as senhas são quebradas, força bruta, *rainbow tables*, o problema de senhas grandes, autenticação em dois fatores, cofres de senhas, os problemas ao ter uma senha vazada, geradores de senhas seguras, etc.

4.1.5 Vulnerabilidades do wordpress

O projeto de vulnerabilidades do WordPress foi bastante interessante e instigante para o público presente. Para o desenvolvimento do mesmo foram criados slides para a apresentação conceitual sobre vulnerabilidades web, especificamente em grandes portais.

Foram utilizadas duas máquinas virtuais para a demonstração do escaneamento de vulnerabilidades em um portal com WordPress, uma máquina virtual com o *Kali Linux* contendo a ferramenta *WPScan* e a outra contendo o WordPress vulnerável, preparada especificamente para o evento.

Na máquina com as vulnerabilidades foi colocada uma senha conhecida para o administrador do portal, claro que não era conhecida do público presente. Foi utilizada a ferramenta *WPScan* para listar as vulnerabilidades do WordPress, logo após foi realizada a listagem de usuários, onde apareceu o usuário administrador. Então foi feita uma força bruta contra a senha do administrador usando a *wordlist rockyou* presente no *kali linux*.

O público ficou surpreso quando a ferramenta apresentou o resultado de uma senha válida para o administrador do portal. De posse dessa senha, a equipe acessou o painel de controle do WordPress e realizou logon no portal. Mostrando que haviam se tornado administradores do mesmo e que poderiam atuar como bem quisessem em relação ao portal, inserindo e modificando conteúdos, bem como usuários e senhas, podendo até mesmo trocar a senha do administrador.

Após essa fase, foi explicado maneiras de se proteger quando se utiliza o WordPress para construir portais. Foram explanados assuntos tais como, atualizar o WordPress, fazer um especie de *hardening*, removendo plugins desnecessários, instalando plugins de segurança, ativando *captcha* para o logon, não permitindo tentativas de acesso infinitas, dentre outras.

4.1.6 Ransomware wannacry

O projeto com o WannaCry foi mais um projeto que obteve bastante admiração pelos presentes no evento, pois muitos deles haviam ouvido falar do WannaCry e do seu grande poder de destruição, bem como, da sua propagação pelo mundo. Contudo, não haviam visto ele em ação.

Para a realização desse projeto, foi criado um ambiente seguro, um computador isolado da rede e com uma máquina virtual vulnerável ao WannaCry dentro dele. A equipe desenvolvedora, após explanar sobre o conceito de Ransomware, falar dos problemas causados por eles, fez uma demonstração na máquina virtual, executando o artefato. Antes, contudo, foi feito um *snapshot* da máquina virtual para poder restaurá-la ao seu estado inicial. Criar o *snapshot* foi de grande valia, pois os presentes solicitaram que o procedimento fosse realizado mais de uma vez.

5 CONCLUSÃO

Com o sucesso da execução dos projetos pelos alunos, pode-se concluir que é muito melhor trabalhar com projetos no ensino médio técnico, pois os alunos ficam mais motivados em concluir um projeto do que apenas ter aulas teóricas sobre o mesmo, é o que se percebeu na disciplina técnica de Segurança da Informação, onde tais projetos foram desenvolvidos.

Os alunos foram capazes de pegar um tema que não conheciam, estudar sobre ele, elaborar um pequeno referencial teórico, instalar as ferramentas necessárias, praticarem sobre o tema, elaborarem slides para a apresentação no evento e abordarem o tema de forma prática, executando comandos diante do público presente, demonstrando como encontrar as vulnerabilidades, explorando as mesmas e discorrendo como proceder para mitigá-las.

Nas palestras, o público presente interagia bastante com os alunos, devido ao fato deles estarem apresentando coisas práticas e que eram novidades para a maioria, pois tratavam de temas que eles ouviam falar constantemente, mas que nunca haviam participado de uma abordagem prática, tal como, ver um site WordPress ter a senha do administrador descoberta e

o seu painel de controle invadido, bem como, um computador ser infectado com o Ransomware WannaCry.

AGRADECIMENTOS

Agradecemos ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), Campus Ariquemes, pelo aporte financeiro destinado à publicação dessa produção.

REFERÊNCIAS

BERTOGLIO, Daniel Dalalana; ZORZO, Avelino Francisco. Tramonto: Uma estratégia de recomendações para testes de penetração. **XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, Porto Alegre, RS, v. 1315, 2016.

CERT.BR. Cartilha de Segurança para Internet. **https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf**, Comitê Gestor da Internet no Brasil, São Paulo - SP, p. 142, 2012.

COUTINHO, Severino Colier. **Números inteiros e criptografia RSA**. [S.l.]: IMPA, 1997.

CRUZ, Carlos Magno Bispo Rosal da. **Auditoria de Segurança da Informação em Sistemas e Aplicações**. Dissertação (Mestrado) — Universidade de Brasília, Brasília, 2017.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: [s.n.], 2002. 175 p. ISSN 85-224-3169-8. ISBN 8522431698.

LEWIS, T. **WordPress Statistics 2019 (Users, Growth + INFOGRAPHIC) | HostSor-ter**. 2019. Disponível em: <https://hostsorter.com/wordpress-statistics/>.

MACKENZIE, Peter. **The WannaCry hangover – Sophos News**. 2019. Disponível em: <https://news.sophos.com/en-us/2019/09/18/the-wannacry-hangover/>.

MAGNO, Carlos; ROSAL, Bispo. **Universidade de Brasília Auditoria de Segurança da Informação em Sistemas e Aplicações**. Tese (Doutorado), 2017.

OWASP. **OWASP Top 10-2017**. [S.l.], 2018. 26 p. Disponível em: <https://owasp.org>.

_____. **OWASP Testing Guide v4 Table of Contents - OWASP**. 2019. Disponível em: <https://www.owasp.org/index.php/OWASP{_}Testing{_}Guide{_}v4{_}Table>.

SFAKIANAKIS, Andreas et al. **ENISA Threat Landscape Report 2018 15 Top Cyberth-reats and Trends About ENISA Contributors Editors**. [S.l.], 2018. 139 p. Disponível em: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.

SILVA, Carlos Alberto. **O elo mais fraco mais fraco da segurança da informação: Pes-soas representam o maior desafio**. Edição do kindle. Oliveira, MG: [s.n.], 2015. 122 p.

SILVA, Evelyn Gomes da. **Criptografia RSA: da teoria à aplicação em sala de aula**. 65 p. Tese (Doutorado) — Universidade de São Paulo, São Carlos, aug 2019. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55136/tde-22082019-110952/>.

SUCURI. **WordPress Security: How to Secure & Protect Your WP Site | Sucuri**. 2018. Disponível em: <https://sucuri.net/guides/wordpress-security/>.

THELINUXCHOICE. **Blackeye: The most complete Phishing Tool, with 32 templates +1 customizable**. 2019. Disponível em: <https://github.com/thelinuxchoice/blackeye>.