O TCC pode ser o primeiro passo para um projeto de negócios, uma investigação científica ou um produto diferenciado. Parece que o caso do Uniscan, *scanner open source* de vulnerabilidades em serviços Web e distribuído gratuitamente online, está nessa categoria de iniciativas conscientes de seu potencial. Desenvolvido pelo formando de Ciência da Computação Douglas Poerschke Rocha sob orientação do professor Diego Kreutz, no Campus Alegrete da Universidade Federal do Pampa (UNIPAMPA), o
Uniscan
já somava mais 5 mil downloads feitos por usuários de diversos países, antes mesmo da apresentação da monografia.

Douglas afirma que o interesse pelo projeto na área de Segurança de TI surgiu da necessidade de ter uma ferramenta gratuita e que detecte de forma eficiente alguns tipos de vulnerabilidades contidas em aplicações Web. Na fase de estudos ele constatou que a maioria dos scanners não conseguiam detectar vulnerabilidades como inclusão local de arquivos (Local File Inclusion, ou LFI), inclusão remota de arquivos (Remote File Inclusion, ou RFI) e execução remota de comandos (Remote Command Execution, ou RCE).
- O objetivo foi criar uma ferramenta que pudesse ser útil para equipes de desenvolvimento e segurança de sistemas Web, como era o caso do NTIC *[Núcleo de Tecnologia da Informação e Comunicação]* da UNIPAMPA - explica o desenvolvedor.

Projeto se tornou alvo de atenção para a comunidade de desenvoledores antes da defesa do TCC (da dir. para a esq.: Roberlei e o criador do Uniscan, Douglas Poerschke Rocha)

A motivação para identificar essas brechas de segurança vem da necessidade de evitar vazamento de dados e invasões. Douglas conta que o Uniscan ajudou a identificar e reparar vulnerabilidades no sistema da Universidade, que foram reportados ao NTIC e corrigidas. A verificação prévia é importante, segundo ele:
- A identificação de vulnerabilidades deve ser sempre incluída nos testes dos softwares antes deles entrarem em produção. Com isto, é reduzida a possibilidade de um comprometimento futuro.

O orientador e ex-diretor do NTIC, professor Diego Kreutz, afirma que são "incomuns" os TCCs que viram um projeto real e concreto, com continuidade após a sua conclusão e apresentação em banca. Para ele, o Uniscan é "excelente" e algo até então inédito na vivência profissional do orientador, com perspectivas de continuidade e longevidade "muito boas":
- O Uniscan faz parte de um grupo seleto de projetos de conclusão de curso ímpares. O conjunto de usuários e os retornos da comunidade vem crescendo a cada dia. A aplicabilidade da ferramenta é boa e importante, pois ajuda equipes de desenvolvimento de sistemas e segurança da informação a diagnosticarem problemas e melhorarem a qualidades de sistemas Web.

O desenvolvimento

Segundo Douglas Rocha, a decisão de desenvolver o Uniscan surgiu antes de iniciar as disciplinas relacionadas ao TCC. Como os primeiros resultados já estavam disponíveis quando o acadêmico terminou a disciplina de TCC I, a cadeira seguinte foi dedicada a ciclos de maturação e melhoramento do trabalho.

A primeira versão do Uniscan foi definida e projetada a partir de um estudo inicial de outros scanners de vulnerabilidades, com a definição de um conjunto inicial de funcionalidade e recursos. Ferramentas e plataformas livres, como é o caso da linguagem de programação Perl, foram focalizadas para o desenvolvimento.
- A implementação da primeira versão, simplificada, levou aproximadamente dois meses. A partir da primeira versão, foram realizadas várias melhorias, aperfeiçoamentos e mudanças mais radicais, como uma reestruturação completa da arquitetura do scanner - conta Douglas.

Esse processo de maturação e evolução perdurou até o final do TCC II. Hoje, a ferramenta dispõe de uma arquitetura modular e flexível, permitindo uma ampla utilização e possibilidades de adaptação do scanner. Outro avanço foi a ampliação do alcance de detecção da ferramenta, graças à colaboração entre desenvolvedores, em especial quando se trata de software livre. O futuro cientista da Computação explica que na primeira versão o Uniscan detectava apenas três tipos de vulnerabilidades (LFI, RFI e RCE), escolhidas devido ao alto grau de risco e o impacto que elas têm sobre o sistema operacional que hospeda as aplicações Web vulneráveis.

O professor Diego Kreutz destaca que o TCC trouxe resultados a partir de mais de 30 exemplos de sites com várias vulnerabilidades detectadas durante o desenvolvimento e teste do Uniscan. Os relatórios técnicos davam informações sobre brechas de segurança em sistemas de empresas e órgãos públicos:
- Com os relatórios, as equipes de TIC das respectivas entidades puderam realizar as devidas correções e ajustes nos sistemas, evitando potenciais e perigosos problemas futuros, como ataques e furto de informações internas.

A criação do site para o projeto, cuja criação e manutenção está a cargo de Roberlei Martins Vieira, permitiu que os usuários oferecessem opiniões e análises sobre o scanner - e foi por meio desse canal de comunicação que a detecção de mais três tipos de vulnerabilidades (SQL injection, Blind SQL injection e Cross-site scripting, ou XSS), também causadoras potenciais de grandes danos para os sistemas Web, foram sugeridas ao desenvolvedor do produto, que hoje está na versão 5.2.

Esforço e ganhos

O Uniscan é um programa *open source*, o que significa que sua codificação está aberta para modificações e aprimoramentos por usuários, e está sendo distribuído gratuitamente. Então, é razoável que o desenvolvedor busque transformar o trabalho em algum tipo de retorno. Douglas conta que o fato de criar e executar o projeto em software livre trouxe benefícios diretos:

- o retorno da comunidade, permitindo melhoramentos e evolução, fazendo com que o Uniscan ganhe em qualidade, robustez e funcionalidades;
- colaboração direta e indireta de outras pessoas;
- visibilidade, pois o software está disponível para todos testarem e utilizarem;
- currículo, pois um projeto com milhares de downloads e usuários no mundo inteiro passa a impressão de habilidade e maturidade na área em específico.

A expectativa é de que na hora de procurar um emprego no setor de segurança de TI, projetos e experiências práticas como a que o Uniscan está proporcionando certamente farão diferença no processo de seleção.

- Na área da computação, em especial, é bastante comum as empresas procurarem pessoas com bons conhecimentos e boas experiências práticas. Projetos como o Uniscan vão nessa direção, ou seja, servem muito bem para abrir portas e oportunidades. Por fim, um projeto de software livre é algo extremamente instigante e desafiador - enumera Douglas.

O professor Diego Kreutz avalia que a repercussão do Uniscan se deve a alguns fatores: o fato de ser um dos poucos projetos em software livre de scanner de vulnerabilidades para aplicações Web; a oferta de mais conhecimentos técnicos na área de segurança de sistemas para a comunidade, em especial para equipes e amantes de TIC; e por atacar problemas reais, encontrados em muitos sistemas Web. Em face desse caso, o professor enumera as qualidades de um projeto de segurança em TI - uma avaliação especialmente interessante para os estudantes da área de Computação e Software:

- Um projeto precisa basicamente: ser inovador; ser aplicável na prática, trazendo resultados palpáveis; ser simples, funcional, flexível e extensível; gerar retorno ou ganho direto ou indireto para as empresas, órgãos ou usuários.

Heleno Nazário para Assessoria de Comunicação Social