Teste de invasão em dispositivos móveis

José Lucio C. Azevedo, Ausberto S. Castro Vera
joselucio_sf@hotmail.com, *ascv@uenf.br*
UENF – CCT – LCMAT – Ciência da Computação

Com os avanços tecnológicos e da cultura de hacking, mesmo com equipes de segurança extremamente competentes, é quase impossível se criar um programa computacional sem falhas. Para eliminar ou minimizar esse defeito da segurança, o desenvolvedor usa a ideia de pensar e atuar como o atacante para descobrir as vulnerabilidades de um sistema e dessa maneira neutralizá-las antes de um ataque real. Testes de invasão ou pentest, é a simulação de ataques reais para avaliar os riscos associados a possíveis brechas de segurança em um projeto. Os pentesters não só identificam vulnerabilidades, mas também as exploram para avaliar o que os invasores poderiam obter após uma exploração bem-sucedida das falhas. Nesse contexto, o objetivo do projeto é mostrar os métodos, ferramentas e processos utilizados em testes de invasão em dispositivos móveis, sinalizando a importância destas ações para a segurança da informação. As metodologias utilizadas foram pesquisas bibliográficas, aulas com especialista, utilização de ferramentas de segurança como a proxy Burp Suit, o decompilador Jadx-gui, softwares de análise como MobSF e Qark, bem como, o kit de desenvolvimento do Android e do próprio terminal do Linux e seus comandos. O pentest, mesmo tendo vários padrões de execução, é uma atividade intuitiva e criativa. Para ambientes mobile, geralmente é seguido, mas não limitado, o previsto no padrão OWASP (Open Web Application Security Project). Primeiro é feita a engenharia reversa para a obtenção do código fonte, por meio de ferramentas como Jadx-gui. Depois é realizada a análise estática do aplicativo por métodos manuais ou até ferramentas automatizadas como o MobSF e o Qark. Por sua vez é realizada uma análise dinâmica mais aprofundada e na comunicação por meio de proxys como a Burp Suit, assim descobrindo vulnerabilidades que passaram nas duas etapas anteriores. Por último um relatório de todos os dados obtidos. O trabalho atualmente se encontra na fase de aprendizado e testes em aplicativos e cenários controlados. O próximo passo é o avanço para um cenário mais real, como o teste da segurança de aplicativos reais respeitando as limitações legais que os desenvolvedores e empresas impõe em seus programas.

Instituição do Programa de IC, IT ou PG: **UENF**
Fomento da bolsa: **CNPq**