Insper

Atividade Prática Supervisionada – APS2

Tecnologias Hacker

Objetivo: Criação de Escaneamento de Portas com Python.

Descrição: Atividade de pesquisa e desenvolvimento de uma aplicação que realize o escaneamento de portas de comunicação de um destino por meio de bibliotecas de desenvolvimento da Linguagem de programação Python.

Carga horária: 5 horas

Prazo para entrega: 04/10/2018 até às 12h (via GIT ou presencialmente em sala de aula)

Introdução

As ferramentas de escaneamento permitem a descoberta de vulnerabilidades em ambientes computacionais, entre outras funcionalidades. Os escaneadores estão disponíveis como ferramentas especializadas projetadas apenas para "escanear" vulnerabilidades em um host, como por exemplo determinar se suas portas de comunicação estão sendo ou não usadas. São extremamente úteis no processo de descoberta e reconhecimento do alvo em um PENTEST, bem como, para a administração de ambientes computacionais. Muitas portas estão associadas a serviços específicos de rede. Para isso, é fundamental o conhecimento sobre sockets e dos protocolos de transporte, bem como, suas características como cabeçalho e *flags*.

Insper

Existem basicamente três tipos de escaneamento:

- **Escaneamento de porta (*port scanner*):** Seu objetivo é verificar portas abertas e serviços disponíveis em um host.
- **Escaneamento de rede:** Permite identificar os hosts que estão ativos em uma rede.
- **Escaneamento de vulnerabilidades:** Busca por vulnerabilidades conhecidas em um host.

O *port scanner* será o objeto de pesquisa desta APS.

Port scanner

É a técnica mais popular e usada por Hackers/Crackers para descobrir serviços vulneráveis em um sistema e o NMAP a mais popular das ferramentas.

Tarefa

Você deverá realizar uma pesquisa dos módulos e bibliotecas que permitem o desenvolvimento de uma ferramenta para o escaneamento de portas TCP e UDP, de acordo com as premissas a seguir:

- Ser em linguagem Python;
- Permitir o escaneamento de um host ou uma rede;
- Permitir selecionar o Protocolo TCP ou UDP;
- Permitir inserir o range (intervalo) de portas a serem escaneadas;
- Além da função de escaneamento, espera-se que seu código relacione as portas Well-Know Ports e seus serviços, e apresente em sua saída (imprimir) o número da porta e o nome do serviço associado.

Insper

Indicação para pesquisa:

Capítulo 1 : O'CONNOR, T. J. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, 2012, ISBN-13: 978-1597499576
DUFFY, Christopher. Aprendendo Pentest com Python. Novatec, 2015, ISBN: 978-85-7522-505-9

Rua Quatá, 300 – Vila Olímpia 04546-042 São Paulo SP Brasil
55 11 4504-2400 www.insper.edu.br