Seja um especialista na análise de código de malware para combater as modernas pragas virtuais e fortalecer a segurança da informação em sua organização

Engenharia Reversa de Código Malicioso

Voltado para profissionais de segurança de nível avançado, este curso trata da análise estática de programas maliciosos, também conhecidos como malware. Percorrendo técnicas para analisar o código de um arquivo desconhecido e entender o seu funcionamento, o curso fornece métodos, ferramentas e dicas para reverter o impedimento da análise empregado pelos desenvolvedores de programas maliciosos.

Na etapa final do curso, o aluno será conduzido pelas diversas fases da análise completa de um programa malicioso real, aplicando todo o conhecimento adquirido e simulando as situações que encontrará em sua atividade profissional.

Características

- O curso está dividido em dez sessões, totalizando 40 horas de aula.
- Aborda a análise estática de malware, não tratando da análise dinâmica, ou seja, sem a execução do código malicioso.
- É composto por apresentações teóricas e a consolidação dos conceitos na prática. Cada aluno tem sua própria estação de trabalho.
- O material didático é exclusivo e rico em atividades práticas em laboratório. Ao final, o aluno recebe a máquina virtual utilizada para uso em futuras análises.
- Material desenvolvido por renomado profissional brasileiro, com ampla experiência de mercado e na análise de artefatos maliciosos.

Competências desenvolvidas

- Utilização de ferramentas de análise de binários.
- Reconhecimento e análise do funcionamento de um programa desconhecido, identificando suas funções e características e entendendo seu objetivo.
- Capacidade de criar um ambiente controlado para analisar programas suspeitos.

Conhecimentos prévios

- Conhecimento de programação, de preferência em linguagens de assembly básico para arquitetura x86.
- Funcionamento de sistemas operacionais e redes.
- Funcionamento de programas maliciosos, vírus e trojans, entre outros.
- Para um aproveitamento satisfatório, recomenda-se fortemente que os alunos

Escola Superior de Redes RNP

esr.rnp.br

RNP

façam uma revisão prévia dos conceitos de assembly
- Ter realizado o curso *Análise Forense* ou possuir conhecimento equivalente.

Investimento

- R$ 2.560,00

Programa do curso

- Analisar um programa utilizando IDA Pro e OllyDBG.
- Conhecer a estrutura de arquivos executáveis.
- Reconhecer técnicas usadas para dificultar a identificação de programas maliciosos.
- Descompactar um arquivo desconhecido, usando ferramentas de análise de binários.
- Analisar um vírus conhecido, entendendo e identificando suas funções internas e mapeando seu funcionamento.

Escola Superior de Redes RNP

esr.rnp.br

RNP

Próximas turmas

Setembro 2019

Engenharia Reversa de Código Malicioso (SEG8)
Brasília (DF), 16 a 20/09/2019 (2ª a 6ª) – integral (9h às 18h hora local)

Escola Superior de Redes RNP
esr.rnp.br

RNP