

TREINAMENTO



EXPLORAÇÃO DE VULNERABILIDADES NO ESPAÇO DO KERNEL (KERNEL EXPLOITATION)

DESCRIÇÃO

Neste treinamento o aluno aprenderá o que é necessário para realizar exploração de vulnerabilidades no espaço do kernel. O treinamento seguirá uma abordagem teórica e prática (hands-on). Inicialmente discutiremos os fundamentos teóricos que envolvem exploração de vulnerabilidades no espaço do kernel e posteriormente abordaremos detalhadamente como as vulnerabilidades acontecem e como podemos explorá-las. No final discutiremos as proteções e mitigações que visam dificultar a exploração de vulnerabilidades no kernel e como podemos burlá-las.

DATA

30 de Janeiro a 02 de Fevereiro de
2020

VAGAS

Vagas Limitadas

LOCAL

São Paulo

CARGA HORÁRIA

4 dias, total de 32 horas

INVESTIMENTO

R\$ 3.000,00 (09/12/2019 até 20/01/2020)

R\$ 3.300,00 (21/01/2020 até 29/01/2020)

R\$ 2.800,00* (09/12/2019 até 29/01/2020)

* DESCONTO ESPECIAL PARA INSCRIÇÕES EM GRUPO (3 PESSOAS), ENTRE EM CONTATO.

Para inscrições e mais informações, acesse nosso site

www.allelesecurity.com.br



EMENTA

Dia 01

Arquitetura de computadores e sistemas operacionais
Gerenciamento de memória
Ambiente de trabalho/pesquisa

Dia 02

Diferença entre userspace e kernelspace
Vulnerabilidades em kernelspace
Depuração (Debugging)

Dia 03

Kernel internals
Exemplos de vulnerabilidades reais e exploração
Alocação dinâmica em kernelspace

Dia 04

Mitigações e bypassing
Vulnerabilidades de hardware e microarquitetura
Conclusão e futuro

* A ementa está sujeita a alteração.



INSTRUTOR

ANDERSON EDUARDO

Realiza pesquisa e exploração de vulnerabilidades no espaço do usuário e do kernel desde 2010. Atua como diretor e principal pesquisador em Segurança da Informação na Allele Security Intelligence. Publicou duas provas de conceito para as vulnerabilidades afetando o kernel do FreeBSD identificadas por CVE-2012-0217 e CVE-2012-4576. Realiza palestras principalmente sobre vulnerabilidades e segurança de sistemas operacionais.