ALLELE
SECURITY INTELLIGENCE

TREINAMENTO LINUX BINARY EXPLOITATION

DESCRIÇÃO

(Nível Intermediário)
Carga horária: 48h

Neste treinamento o estudante aprenderá o que é necessário para realizar exploração de vulnerabilidades no espaço do usuário. O treinamento seguirá uma abordagem teórica e prática (*hands-on*). Inicialmente, discutiremos os fundamentos teóricos, arquiteturais e fundamentais que envolvem exploração de vulnerabilidades no espaço do usuário e posteriormente abordaremos detalhadamente como as vulnerabilidades acontecem, como corrigi-las e como podemos explorá-las. Posteriormente, discutiremos as proteções e mitigações que visam dificultar a exploração de vulnerabilidades em binários e como podemos burlá-las. Ao final, o treinamento será concluído com uma discussão sobre o futuro da área de explorações de vulnerabilidades de binário e as considerações finais.

Nossa metodologia visa que qualquer pessoa interessada e motivada entenda e aproveite o conteúdo do treinamento. Buscamos explicar os conceitos fundamentais claramente, evitar jargões e termos desconhecidos, ensinar o conteúdo de diversas formas para ajudar na assimilação do conhecimento. Sem contar que o treinamento tem uma grande abordagem prática, mão na massa.

EMENTA

MÓDULO 01 - ARQUITETURA DE COMPUTADORES

- Microarquitetura vs macroarquitetura
- Segmentação
- Paginação
- Arquitetura AMD64 / x86-64

MÓDULO 02 - *EXECUTABLE AND LINKABLE FORMAT* (ELF)

- História
- Formato ELF
- Estruturas ELF
- Ferramentas
- Laboratório

MÓDULO 03 - DEPURAÇÃO (*DEBUGGING*)

- Depuração usando VMware e QEMU
- GDB e principais comandos
- Automação
- Laboratório

MÓDULO 04 - *ASSEMBLY* E LINGUAGEM C

- Sintaxes
- Instruções básicas, *flags* e registradores
- *Linker* / *Loader* / Código objeto / *Shared library*
- *System calls*
- Ferramentas

MÓDULO 05 - ESCRITA DE *SHELLCODES* (*SHELLCODING*)

- Ferramentas
- Construção de *shellcodes*
- Laboratório

MÓDULO 06 - CLASSES DE VULNERABILIDADES E SUAS EXPLORAÇÕES

- *Buffer overflow*
- *Format string*
- Falhas lógicas
- Laboratório

MÓDULO 07 - MITIGAÇÕES E *BYPASSING*

- *No-Execute* / *Data Execution Prevention* (NX / DEP)
- *Stack cookies* / *Canaries*
- *Address Space Layout Randomization* (ASLR)
- *Position-Independent code* (PIE)
- *Relocation Read-Only* (RELRO) / *Full* RELRO
- Abusando de primitivas de *arbitrary read* e *arbitrary write* (laboratório)

MÓDULO 08 - CONCLUSÃO, FUTURO E CONSIDERAÇÕES FINAIS

- Conclusão, futuro e considerações finais

PRÉ-REQUISITOS

- Experiência com distribuições Linux, especialmente Ubuntu;
- Linguagem de programação C e *assembly* nível básico;
- Conhecimento básico sobre sistemas operacionais e arquiteturas de computador;
- Conhecimento básico sobre gerenciamento de memória;
- Experiência básica com ferramentas de *debugging* como GDB.

Considerando os pré-requisitos, o treinamento é adaptado de acordo com o perfil e experiência da turma. Esta é sua chance de expandir seus conhecimentos e alcançar o próximo nível na sua carreira.

PÚBLICO ALVO

- Pesquisadores em Segurança e Tecnologia da Informação;
- Profissionais em Segurança e Tecnologia da Informação;
- Gestores em Segurança e Tecnologia da Informação;
- Estudantes de Segurança da Informação, Sistema de Informação, Análise de Sistema, Ciência da Computação e Engenharia da Computação;
- Profissionais e Agentes de Segurança Pública;
- Profissionais de TI com interesse e afinidade na área da Segurança da Informação.

BENEFÍCIOS

- Conteúdo atualizado com o que há de mais moderno em pesquisa e exploração de vulnerabilidades de binários no Linux;
- Treinamento prático (*hands-on*);
- Linguagem acessível;
- Instrutores experientes em pesquisa e exploração de vulnerabilidades em ambiente profissional;
- Suporte aos estudos sobre o tema por até 6 meses após a conclusão do treinamento;
- Acesso à lista de discussão privada para alunos.

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Linux, Mac OS ou Windows);
- Configuração mínima de 16 GB de RAM, 200 GB de espaço livre em disco, acesso à Internet e processador da arquitetura x86 com no mínimo 4 CPUs.

MATERIAL FORNECIDO

- *Slides*;
- Material complementar;
- Certificado de conclusão;
- Videoaulas gravadas;
- Será disponibilizada previamente uma máquina virtual com Ubuntu 22.04.

AO FINAL DO TREINAMENTO, VOCÊ SERÁ CAPAZ DE:

- Identificar e explorar vulnerabilidades em binários em ambiente Linux;
- Analisar as vulnerabilidades com relação a impacto, criticidade e identificação de causa raiz;
- Escrever *exploits* e provas de conceitos;

- Identificar e compreender o funcionamento das mitigações de segurança modernas presentes no Linux e em processadores e como a exploração de vulnerabilidades ocorre mesmo diante da presença desses mecanismos de proteção.

INSTRUTOR

Anderson Nascimento é diretor e principal pesquisador em segurança da informação na Allele Security Intelligence.

Como pesquisador profissional, possui mais de 10 anos de experiência trabalhando diretamente com empresas renomadas de *security research* e clientes internacionais. Escreveu e disponibilizou publicamente provas de conceito para as vulnerabilidades identificadas no *kernel* do Linux e do FreeBSD.

Anderson Nascimento possui sólidos conhecimentos sobre arquitetura de computadores x86 e AMD64, sistemas operacionais e principalmente técnicas de ataque e proteção do *kernel* do Linux.

EMPRESA

A Allele Security Intelligence é uma empresa independente especializada em pesquisa em segurança da informação. Pesquisa e desenvolvimento são princípios fundamentais que orientam nossa tomada de decisão para oferecer serviços eficientes e de excelência aos nossos clientes.

Para inscrições e mais informações, acesse o link abaixo:

Treinamento de Exploração de Vulnerabilidades no Espaço do Usuário (Linux Binary Exploitation) – Maio 2026

https://allelesecurity.com.br/treinamento-binario-maio-2026/

E-mail de contato:

contato@allelesecurity.com.br