ALLELE
SECURITY INTELLIGENCE

TREINAMENTO LINUX KERNEL EXPLOITATION

DESCRIÇÃO

(Nível Avançado)
Carga horária: 48h

Neste treinamento o estudante 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, como corrigi-las e como podemos explorá-las. Posteriormente, discutiremos as proteções e mitigações que visam dificultar a exploração de vulnerabilidades no *kernel* e como podemos burlá-las. Ao final, discutimos sobre o futuro de exploração de vulnerabilidades.

Nossa metodologia visa que qualquer pessoa interessada 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
- *Assembly*

MÓDULO 02 - AMBIENTE DE TRABALHO / PESQUISA

- Linux
- Ecossistema
- Instalação do sistema
- Código-fonte do *kernel* / Binário com símbolos
- Compilação do *kernel*
- Principais ferramentas

MÓDULO 03 - DEPURAÇÃO (*DEBUGGING*)

- Depuração usando VMware e QEMU

- GDB e principais comandos
- Automação

MÓDULO 04 - LINUX *KERNEL INTERNALS*

- Espaço de endereçamento
- Contexto de execução
- Chamadas de sistema
    - Processos
    - Memória
    - Arquivo
    - Rede
    - *Namespace*
    - Chaveiro
    - Dispositivos
- Subsistemas
    - *Capabilities*
    - *Namespaces*
- *Modules autoloading*
- Principais estruturas do *kernel*
- *Kernel* API
- Subsistema de Memória
    - Alocação dinâmica
    - *Page Allocator*
- Linguagem C para o *kernel* do Linux

MÓDULO 05 - EXPLORANDO VULNERABILIDADES EM MÓDULOS VULNERÁVEIS NO *KERNEL* DO LINUX

- Apresentação do módulo vulnerável
- Identificação das vulnerabilidades
- Primitivas de exploração
    - Leitura arbitrária
    - Escrita arbitrária
    - Execução arbitrária
- Correção das vulnerabilidades

MÓDULO 06 - MITIGAÇÕES E *BYPASSING*

- SMEP - *Supervisor Mode Execution Prevention*
    - ROP - *Return Oriented Programming em kernel mode*
- SMAP - *Supervisor Mode Access Prevention*
- KASLR - *Kernel Address Space Layout Randomization*

MÓDULO 07 - CONCLUSÃO, FUTURO e CONSIDERAÇÕES FINAIS

- Conclusão, futuro e considerações finais.

PRÉ-REQUISITOS

- Experiência com distribuições Linux, especialmente Debian;
- Linguagem de programação C e *assembly* nível intermediário;
- Conhecimento intermediário sobre sistemas operacionais e arquiteturas de computador;
- Conhecimento intermediário sobre gerenciamento de memória;
- Experiência intermediária 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 no *kernel* do 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). A recomendação oficial é utilizar Linux;
- 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 Debian 12, *kernel* 6.1.

AO FINAL DO TREINAMENTO, VOCÊ SERÁ CAPAZ DE:

- Identificar e explorar vulnerabilidades no *kernel* e em seus módulos;
- Analisar as vulnerabilidades com relação a impacto, criticidade e identificação de causa raiz;
- Escrever *exploits* e provas de conceitos;
- Identificação e compreensão do funcionamento de mitigações de segurança modernas presentes no Linux e em processadores e como a exploração de vulnerabilidades ocorre mesmo com recursos de segurança presentes.

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 Kernel (Linux Kernel Exploitation) – Agosto 2026

https://allelesecurity.com/treinamento-kernel-agosto-2026/

E-mail de contato:

info@allelesecurity.com