Projeto Pedagógico

Segurança Ativa e Defesa Cibernética: Fundamentos

Curso de Aperfeiçoamento Presencial

ORIENTADOR PEDAGÓGICO

Douglas Rafael de Castro Aguiar

CARACTERIZAÇÃO DA ATIVIDADE

Modalidade: Presencial

Carga horária: 35 horas-aula

Local de realização: ESMPU - SGAS II St. de Grandes Áreas Sul 603

Eixo temático: Inovação, Tecnologia e Gestão Pública

OBJETIVO GERAL

Capacitar os participantes a compreender os princípios fundamentais da segurança ofensiva, apresentando conceitos, metodologias e ferramentas essenciais utilizadas na identificação e exploração controlada de vulnerabilidades. O curso visa fornecer uma base sólida para atuação ética em testes de segurança, alinhada às boas práticas e às necessidades institucionais do Ministério Público, integrando teoria e atividades práticas em laboratório.

PÚBLICO ALVO

Servidores das Secretarias de Tecnologia da Informação e Comunicação (STI/STIC) do MPF, MPT, MPDFT, MPM, ESMPU e CNMP, com conhecimento básico de redes de computadores e sistemas operacionais.

VAGAS E PROCESSO SELETIVO

Total de vagas ofertadas: **25 vagas**

Turma presencial: **25 vagas**

Distribuição das vagas para a turma PRESENCIAL

(até 40 vagas presencias, sendo apenas 20 vagas com custeio de bolsa-capacitação e passagens aéreas)

	MPF		MPT		MPM		MPDFT		ESMPU	Total
	Membros	Servidores	Membros	Servidores	Membros	Servidores	Membros	Servidores	-	
COM CUSTEIO										**0**
SEM CUSTEIO		7		5		2		3	5	**22**
Total		**7**		**5**		**2**		**3**	**5**	**0**

	CNMP		MP Estadual		Público Externo	Total
	Membros	Servidores	Membros	Servidores		
SEM CUSTEIO		3				**3**
Total		**3**				

Requisitos para seleção

Ser servidor(a) das Secretarias de Tecnologia da Informação e Comunicação (STI/STIC) do MPF, MPT, MPDFT, MPM, ESMPU e CNMP, mediante indicação do(a) Secretário(a) de TI ou da autoridade máxima de tecnologia da informação do respectivo órgão.

Possuir conhecimento básico de redes de computadores (TCP/IP) e sistemas operacionais Linux e Windows, além de familiaridade com o uso de máquinas virtuais ou ambientes de laboratório.

PLANEJAMENTO PEDAGÓGICO

Cronograma

17/11/2025 **Primeiro dia.**

13h a 18h **INTRODUÇÃO À SEGURANÇA OFENSIVA E AMBIENTE DE LABORATÓRIO**

Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Compreender os conceitos básicos de segurança ofensiva e sua importância para a segurança institucional.
Conhecer a legislação e princípios éticos aplicáveis à atuação ofensiva.
Iniciar a configuração do ambiente de laboratório para execução segura dos experimentos.

Metodologia
Aula expositiva dialogada com apresentação de slides.
Demonstração prática de configuração de máquinas virtuais e ferramentas em ambiente seguro.
Exercícios práticos de familiarização com Kali Linux.

19/11/2025 **Segundo dia.**

13h a 18h **CONFIGURAÇÃO DE LABORATÓRIO E FUNDAMENTOS DE RECONHECIMENTO**

Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Concluir a preparação do ambiente de laboratório.
Entender a fase de reconhecimento nos testes de penetração.
Aprender técnicas iniciais de footprinting.

Metodologia
Aula expositiva com demonstração de técnicas de reconhecimento.
Exercícios práticos no Kali Linux para coleta básica de informações.
Registro estruturado de observações em relatório preliminar.

24/11/2025 **Terceiro dia.**
13h a 18h **VARREDURA DE ALVOS E ANÁLISE INICIAL**
Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Utilizar ferramentas para descoberta de hosts, portas e serviços.
Documentar informações coletadas para etapas futuras.
Compreender o papel da análise inicial no ciclo de um pentest.

Metodologia
Aula prática com Nmap, Netcat e Wireshark em cenários controlados.
Exercícios progressivos de varredura e análise.
Registro estruturado dos achados em relatório parcial.

26/11/2025 **Quarto dia.**
13h a 18h **VULNERABILIDADES COMUNS E TÉCNICAS DE EXPLORAÇÃO (Parte I)**
Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Identificar vulnerabilidades comuns em sistemas e aplicações.
Explorar falhas conhecidas em ambiente de laboratório.
Entender riscos associados ao uso de exploits.

Metodologia
Aula expositiva com estudo de casos (OWASP Top 10, CVEs).
Laboratório guiado com máquinas vulneráveis.
Exercícios práticos de exploração inicial

28/11/2025 **Quinto dia.**
13h a 18h **VULNERABILIDADES COMUNS E TÉCNICAS DE EXPLORAÇÃO (Parte II)**
Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Consolidar técnicas de exploração de vulnerabilidades.
Aplicar práticas em cenários mais complexos.
Discutir impactos e mitigação das falhas exploradas.

Metodologia
Laboratório prático de exploração em máquinas adicionais.
Exercícios orientados de exploração avançada.
Discussão em grupo sobre riscos reais e contramedidas

01/12/2025 **Sexto dia.**
13h a 18h **METASPLOIT FRAMEWORK E EXPLORAÇÃO CONTROLADA**
Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Conhecer a arquitetura e funcionamento do Metasploit Framework.
Utilizar módulos para exploração de falhas em sistemas simulados.
Aplicar técnicas de exploração de forma controlada e segura.

Metodologia
Aula prática com demonstração de uso do Metasploit.
Laboratório guiado com exercícios progressivos.
Discussão em grupo sobre documentação técnica.

03/12/2025 **Sétimo dia.**
13h a 18h **PÓS-EXPLORAÇÃO, RELATÓRIOS E DESAFIO FINAL**
Docente Diego José Sousa de Albuquerque

Objetivo de Aprendizagem
Entender as etapas de pós-exploração (elevação de privilégios, persistência, movimentação lateral).
Produzir relatório técnico estruturado com achados de segurança.
Consolidar conhecimentos em um exercício integrador.

Metodologia
Aula expositiva sobre pós-exploração e relatórios de pentest.
Exercício prático de simulação completa: reconhecimento → exploração → relatório.
Desafio final em equipe, com apresentação dos resultados.

Nome completo	**E-mail**	**Função** *(orientador pedagógico ou instrutor)*	**Cargo** *(Ex: Servidor Federal, Servidor Estadual, Procurador da República, Subprocurador da República, Professor de Universidade...)*	**Celular**	**Carga horária a ser contratada** *(cada docente deve ministrar no mínimo 2 horas-aula)*	**Currículo** *(inserir o link)*
Diego José Sousa de Albuquerque	diego@cnmp.mp.br	**Instrutor**	**Servidor Federal (CNMP)**		**35**	
Douglas Rafael de Castro Aguiar	douglasaguiar@escola.mpu.mp.br	**Orientador Pedagógico**	**Servidor Federal (ESMPU)**		**7**	

Disponibilização dos conteúdos da atividade
Os conteúdos produzidos durante a atividade serão disponibilizados no site da ESMPU para acesso amplo e irrestrito. Caso haja um motivo imperioso que impeça essa divulgação, informe a justificativa. Essa justificativa será submetida à apreciação da Direção Geral da ESMPU.

Motivo legal ou de ordem social que impeça a disponibilização do conteúdo da atividade
Inisira a justificativa que impeça a disponibilização irrestrito do conteúdo da atividade, se houver.

Informações importantes
As atividades acadêmicas poderão ser canceladas nas seguintes situações:
I - o não envio do projeto pedagógico pelo(a) orientador(a) pedagógico(a) da atividade conforme prazos estabelecidos;
II - impossibilidade de contratação de docentes devido à ausência de assinatura ou de envio de documentos necessários nos prazos estabelecidos;
III - impossibilidade de realização de atividade por motivos de força maior, informada pelo(a) orientador(a) pedagógico(a), após manifestação da Coordenação de Ensino do ramo; e
IV - número insuficiente de inscritos para justificar os custos da atividade.