Pentest Request

# **Objetivo do Teste de Penetração**

Este pedido de autorização tem como objetivo obter consentimento formal para a realização de um teste de penetração (PenTest Request) no domínio \*\*\*\* associados a Nome da Empresa. O teste vem identificar potenciais vulnerabilidades que possam comprometer a segurança da infraestrutura, ajudando assim a melhorar as defesas contra ameaças cibernéticas e garantindo a integridade dos sistemas e dados.

# **Testes**

**Domínio:** cm-leiria.pt

**Subdomínios e Sistemas Encontrados:** [ex.: portal.exemplo.com, api.exemplo.com]

**Serviços e Aplicações:** Aplicações web, APIs, servidores, entre outros.

**Limitações e Restrições:**

O teste será limitado aos sistemas e serviços explicitamente listados acima.

Sistemas críticos não mencionados estarão fora do escopo do teste para evitar possíveis interrupções no funcionamento.

# **Data e Duração do Teste**

**Período de Realização**: De até

**Horário Planeado**: Das 22h às 06h –  fora do horário de trabalho para minimizar riscos.

**2. Relatório de Footprinting**

**Objetivo:** Este relatório é o resultado do processo de footprinting realizado no domínio [Nome do domínio]. O objetivo é identificar informações que possam ser usadas em um ataque, como nomes de servidores, IPs e informações de DNS.

**Estrutura do Relatório:**

1. **Informações Básicas**
   * **Domínio Alvo:** [Nome do domínio]
   * **Descrição Geral:** [Breve descrição do domínio e dos serviços em uso]
2. **Informações Coletadas**
   * **Endereços IP associados:** Listagem de IPs
   * **Registros DNS:** Listagem de registros, incluindo A, MX, NS, etc.
   * **Tecnologias Detectadas:** Descrição das tecnologias usadas no site, como CMS, linguagens de programação e bibliotecas.
   * **Portas e Serviços Abertos:** Listagem de portas abertas e serviços identificados.
3. **Conclusão**
   * **Resumo de Vulnerabilidades Potenciais:** Com base nas informações coletadas.
   * **Recomendações de Melhoria:** Sugestões para melhorar a segurança.

**Relatório de Teste de Penetração**

**Objetivo:** O relatório documenta as descobertas da fase de penetração, com detalhes sobre cada vulnerabilidade encontrada, seu impacto e as recomendações.

**Estrutura do Relatório:**

1. **Introdução**
   * **Domínio Alvo:** [Nome do domínio]
   * **Resumo do Escopo:** Serviços e sistemas testados.
2. **Metodologia Utilizada**
   * Explicação das ferramentas e técnicas usadas para identificar e testar vulnerabilidades.
3. **Resultados e Descobertas**
   * **Descrição de Vulnerabilidades Encontradas:** Para cada vulnerabilidade, incluir:
     + **Nome da Vulnerabilidade**
     + **Descrição**
     + **Impacto**
     + **Provas de Exploração (screenshots ou logs)**
4. **Recomendações**
   * Medidas recomendadas para corrigir as vulnerabilidades e melhorar a segurança geral.
5. **Conclusão**
   * Resumo dos principais pontos, incluindo as vulnerabilidades mais críticas e recomendações.