

## Plano de Projeto (Pentest)













### Plano de Projeto (Pentest)


- 1 Introdução
  - 1.1 Cenário de Ataque:
  - 1.2 Objetivos Gerais:
  - 1.3 Escopo:
- 2 METODOLOGIA
  - 2.1 Fase 0 - Planejamento e Preparação de Ambiente Controlado
  - 2.2 Fase 1 - Identificação e Análise de Vulnerabilidades
  - 2.3 Fase 2 - Exploração das Vulnerabilidades
  - 2.4 Fase 3 - Pós Exploração e Análise do grau de Risco das vulnerabilidade
  - 2.5 Fase 4 - Relatório e Documentação
  - 2.6 Fase 5 - Plano de correções de segurança no Servidor
- 3 CRONOGRAMA DO PROJETO
- 4 Ferramentas que serão Utilizadas:
  - links Anexos:

### Colaboradores do Projeto:

- @Silas Marques
- @Eduardo Tavares Sousa
- @Alisson dos Santos Machado
- @Fabricio Amaral
- @Paulo Vinicius
- @Larissa Freitas De Oliveira

### Mapa de Tudo que será feito:

Type	Key	Resumo	Responsável	Prioridade	Status	Atualizado(a)
<input checked="" type="checkbox"/>	PW-41	SRV: Instalar rsyslog e Intregar com grayLog (Opcional)	 Silas Marques	Medium	EM ANDAMENTO	16 de abr. de 2025, 22:09
<input checked="" type="checkbox"/>	PW-40	SRV: Configurar/instalar UFW	 Alisson dos Santos Ma...	Medium	TAREFAS PENDE...	5 de abr. de 2025, 13:31
<input checked="" type="checkbox"/>	PW-39	SRV: Instalar Iptable e configurar	 Silas Marques	Medium	CONCLUÍDO	16 de abr. de 2025, 22:08
<input checked="" type="checkbox"/>	PW-38	SRV: Instalar de configurar Fail2ban	 Silas Marques	Medium	CONCLUÍDO	16 de abr. de 2025, 22:09
<input checked="" type="checkbox"/>	PW-37	DVWA: Mysql	 Eduardo Tavares Sousa	Medium	TAREFAS PENDE...	5 de abr. de 2025, 13:31
<input checked="" type="checkbox"/>	PW-36	SRV Serviço: OpenSSH	 Eduardo Tavares Sousa	Medium	TAREFAS PENDE...	5 de abr. de 2025, 13:31
<input checked="" type="checkbox"/>	PW-35	DVWA Desabilitar a Geração de ETags ou Modificar a Geração ...	 Silas Marques	Medium	CONCLUÍDO	16 de abr. de 2025, 22:08
<input checked="" type="checkbox"/>	PW-34	DVWA && SRV: Atualização do Servidor Apache	 Fabricio Amaral	Medium	TAREFAS PENDE...	5 de abr. de 2025, 13:31
<input checked="" type="checkbox"/>	PW-33	SRV: Revisão das Configurações do Apache	 Eduardo Tavares Sousa	Medium	TAREFAS PENDE...	5 de abr. de 2025, 13:31
<input checked="" type="checkbox"/>	PW-32	DVWA: Configuração do robots.txt	 Silas Marques	Medium	CONCLUÍDO	16 de abr. de 2025, 22:08
<input checked="" type="checkbox"/>	PW-31	DVWA: Restringir o Acesso aos Diretórios Sensíveis:	 Eduardo Tavares Sousa	Medium	TAREFAS PENDE...	5 de abr. de 2025, 13:30
<input checked="" type="checkbox"/>	PW-30	DVWA: Configuração de HttpOnly	 Silas Marques	Medium	CONCLUÍDO	16 de abr. de 2025, 22:08
<input checked="" type="checkbox"/>	PW-29	Relatorio dde Incidente e Resposta		Medium	TAREFAS PENDE...	19 de mar. de 2025, 14:06

 Sincronizado agora · 41 itens

# 1 Introdução

**Pentest (Teste de Penetração)** é um processo de segurança cibernética que simula ataques a um sistema, rede ou aplicação para identificar vulnerabilidades exploráveis. O objetivo do teste é avaliar a segurança do ambiente, identificar falhas antes que sejam exploradas por atacantes reais e fornecer recomendações para mitigar os riscos.

Os principais objetivos do pentest incluem:

- ✓ **Identificar vulnerabilidades** em sistemas, redes e aplicações.
- ✓ **Avaliar impactos** caso uma falha seja explorada.
- ✓ **Testar a efetividade das defesas** e mecanismos de segurança.
- ✓ **Cumprir normas e regulamentos** de segurança.
- ✓ **Reforçar a postura de segurança** da organização.

Esse teste pode ser realizado de diferentes formas, como **caixa branca** (com conhecimento prévio do sistema), **caixa preta** (sem informações internas) ou **caixa cinza** (com acesso parcial a informações).

Neste contexto o presente documento visa detalhar um plano de pentest com fim puramente didático que será realizado envolvendo uma rede corporativa fictícia que possui um servidor, o qual terá algumas vulnerabilidade que serão exploradas e por fim corrigidas pela equipe de segurança. O projeto sera composto por três equipes:

## 1. Equipe de Ataque (red-rat)

- @Fabricio Amaral
- @Eduardo Tavares Sousa

## 2. Equipe de defesa (white-rat)

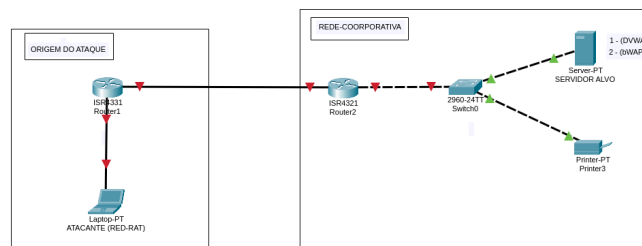
- @Silas Marques
- @Alisson dos Santos Machado

## 3. Equipe cliente (rede corporativa)

- @Paulo Vinicius
- @Larissa Freitas De Oliveira

## 1.1 Cenário de Ataque:

A rede que será analisada será um rede de teste corporativa que possui para fim de exemplo um servidor com aplicações web que possuem, intencionalmente vulnerabilidades que serão exploradas. Nesse servidor contém além das informações de vendas da empresa, aplicações rodando cheias de falhas de segurança. O roteador dessa pequena rede está totalmente mal configurado de com brechas de segurança. O gerente da empresa, para corta custos, resolveu não investir muito em segurança. Dois Hacker conseguiram a principio fazer um reconhecimento da rede e depois atravez de um ataque de negação de serviço (DDoS) conseguiram acessar o roteador e por fim acessar todos os host conectados na rede da empresa inclusive o servidor que tinha informações financeiras de vendas de grande valia para a empresa. O modelo da rede esta abaixo. Então os Hackers resolveram lançar um ataque de ransomware para poder no futuro poder pedir dinheiro em troca da chave para descriptografar os dados.



CISCO - Packet Tracer 8

## 1.2 Objetivos Gerais:

1. Encontrar vulnerabilidade no sistema de uma empresa
2. Avaliar o impacto financeiro de uma possível exploração
3. Testar a eficácia das defesas de segurança
4. avaliar a segurança do ambiente
5. Validar a conformidade com as políticas segurança
6. mitigar os riscos
7. Implementar Correções de segurança no servidor com base nos relatórios
8. Construir insights, gráficos sobre os resultados
9. Refletir sobre os resultados

## 1.3 Escopo:

### 1.2.1 Sistemas que serão testados:

- Aplicações rodando no Servidor




### 1.2.2 Sistema de ataque:

- laptop-PT (Rat Rat)

## 2 METODOLOGIA

### 2.1 Fase 0 - Planejamento e Preparação de Ambiente Controlado

#### 2.1.2 Objetivos da Fase:

- Criar os planos e procedimentos que serão realizados
- Preparar ambiente do ataque <  [Preparação do Host de Ataque](#) >
- preparar ambiente do cliente <  [Preparação do host Client \(10.0.0.6/24\)](#) >
- preparar ambiente de defesa <  [Preparação do Ambiente de Proteção](#) >

#### 2.1.3 Procedimentos:

##### • Ambiente de Ataque:


1. instalar ferramentas comuns (curl, wget, git, OpenSSH)
2. Instalar Ferramentas de Pentest (*Metasploit, Framework, Nmap, Aircrack-ng*)

##### • Ambiente Cliente:

@Eduardo Tavares Sousa

1. Baixar e Instalar o Ubuntu Server 20 numa maquina virtual do [Oracle VirtualBox](#)
2. Atualizar a lista de repositórios
3. Realizar atualizações de pacotes
4. instalar ferramentas comuns (curl, wget, git, OpenSSH)
5. configurar time-zone e teclado
6. configurar placas de rede do serviços
7. instalar aplicações vulneraveis

##### • Ambiente de Proteção

- ☐  [@Silas Marques](#) @Alisson dos Santos Machado
  - Instalar ferramentas de proteção (iptables, UFW, Fail2ban)
  - Implementar medidas de segurança conforme relatórios

### 2.2 Fase 1 - Identificação e Análise de Vulnerabilidades

#### 2.2.1 Objetivos da Fase:

- Usar as ferramentas de análise para realizar os teste no servidor a partir da maquina de ataque
- Levantar as possíveis vulnerabilidades do Servidor.
- Realizar a análise das vulnerabilidades encontradas

#### 2.2.3 Procedimentos:

- Usar os comandos do nmap listados em  [Pentest com as Ferramentas](#) para realizar teste de varreduras do servidor e nas aplicações
- User os comando do nikito listados em  [Pentest com as Ferramentas](#) para realizar teste e coletar dados de falhas e vulnerabilidades

### 2.3 Fase 2 - Exploração das Vulnerabilidades

#### 2.3.1 Objetivos:

- Listar as falhas e verificar os possíveis riscos de cada uma
- Usar as ferramentas citadas ou outras para tentar realizar teste profundos e mais pesados no servidor atravez da exploração das falhas encontradas

### 2.4 Fase 3 - Pós Exploração e Análise do grau de Risco das vulnerabilidade

#### 2.4.1 Objetivos:

- Listar as vulnerabilidades
- construir uma escala bem como analisar os riscos de cada falhas encontrada na fase 1
- Avaliar as consequências que poderão ser geradas pelos riscos
- Avaliar os danos e prejuízos financeiros que poderão ser gerados pelos riscos ao cliente

2.4.2 Procedimentos:

## 2.5 Fase 4 - Relatório e Documentação [🔗](#)

### 2.5.1 Objetivos:

- Fazer relatórios, insights ou gráficos a respeito das falhas ou vulnerabilidades encontrada bem como os riscos de uma
- Documentar todo o processo

### 2.5.2 Procedimentos:

## 2.6 Fase 5 - Plano de correções de segurança no Servidor [🔗](#)

### 2.6.1 Objetivos:

- Implementar um plano de ação de mitigação de riscos conforme relatórios de falhas
- Relatório de mitigação

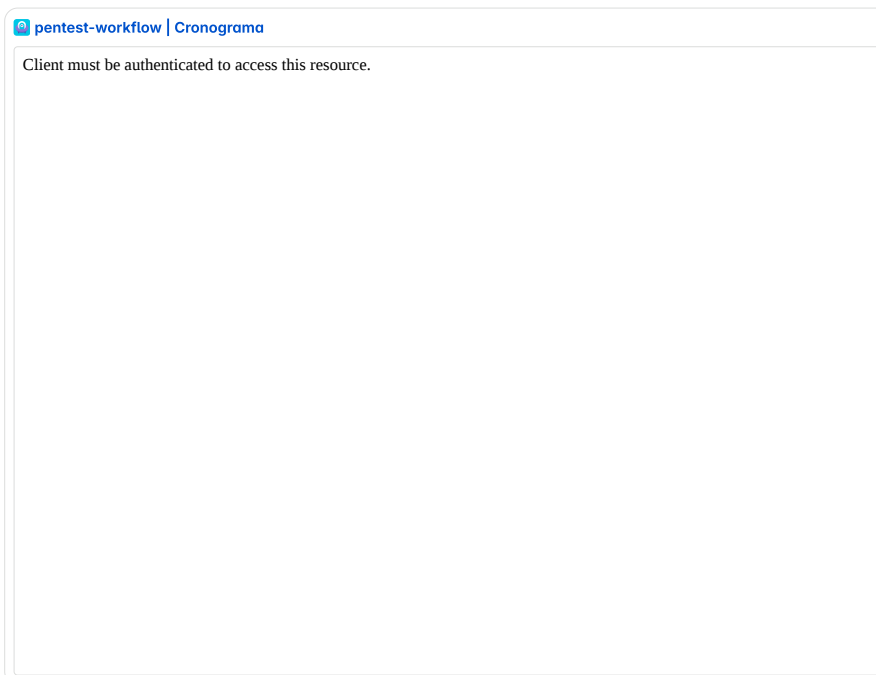
## 2.7 Fase 6 - Mitigações, Correção e Simulação

### 2.7.1 Objetivos:

- Colocar o plano em ação
- Mitigar ameaças
- Implementar as medidas de segurança de acordo com o plano de ação
- Simular um novo ataque e resposta do servidor
- Relatório de Incidente de Resposta

### 2.7.1 Procedimentos:

## 3 CRONOGRAMA DO PROJETO [🔗](#)



## 4 Ferramentas que serão Utilizadas: [↗](#)

- **Nmap:** Ferramenta para varredura de redes e descoberta de hosts e serviços.
- **Aircrack-ng:** Conjunto de ferramentas para avaliar a segurança de redes
- **Nikto**
  - **Descrição:** Ferramenta de scanner de vulnerabilidades web que verifica servidores web em busca de mais de 6.700 falhas potenciais, como configurações incorretas, vulnerabilidades conhecidas e versões desatualizadas de software.
  - **Funcionalidades:** Identificação de versões de servidores, falhas de configuração, e vulnerabilidades em aplicativos web.
  - **Link:** Nikto
- **OWASP ZAP (Zed Attack Proxy)**
  - **Descrição:** Uma das ferramentas mais populares e amplamente utilizadas para testes de segurança em aplicações web. Ela realiza varreduras automáticas e oferece funcionalidades para testes manuais de segurança.
  - **Funcionalidades:** Escaneamento automatizado, proxy reverso, fuzzing, detecção de vulnerabilidades como SQL Injection, Cross-Site Scripting (XSS), entre outras.
  - **Link:** [OWASP ZAP](#)

## links Anexos: [↗](#)

- [Projeto no Jira](#)
- <https://github.com/silasMarquess/pentest-repo-docs.git> [Conectar a conta do Github](#)