

# MÓDULO: AUDITORIA E ANÁLISE FORENSE

Louise Altvater  
RCTS CERT





# AGENDA

Auditoria

Análise Forense

Actividade Auditoria

Almoço (1h)

Actividade Análise Forense

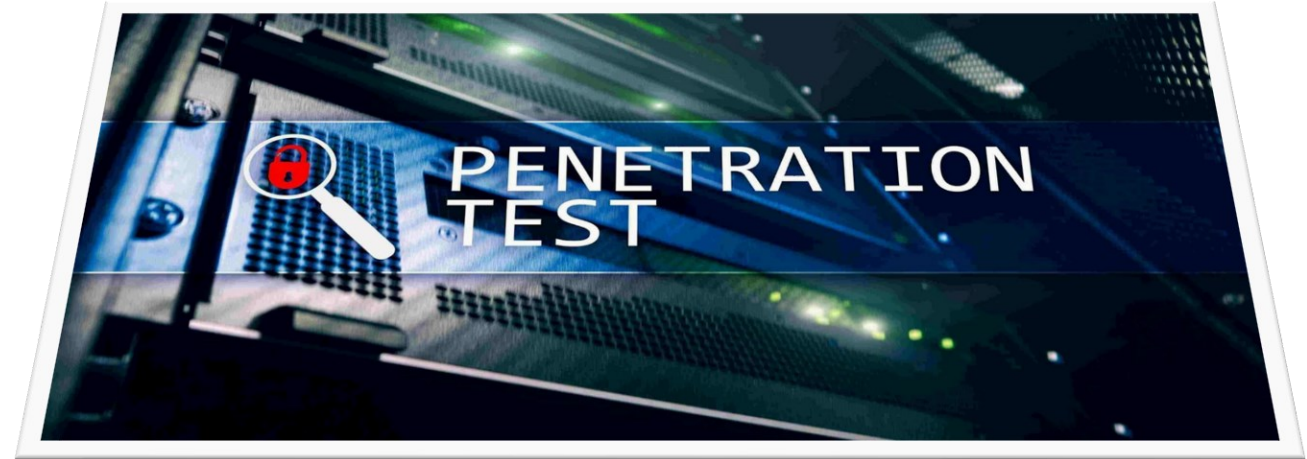
# AUDITORIA



Testar Sistemas

Vulnerabilidades

Estratégias de mitigação



# TIPOS DE AUDITORIA

Auditoria de Rede

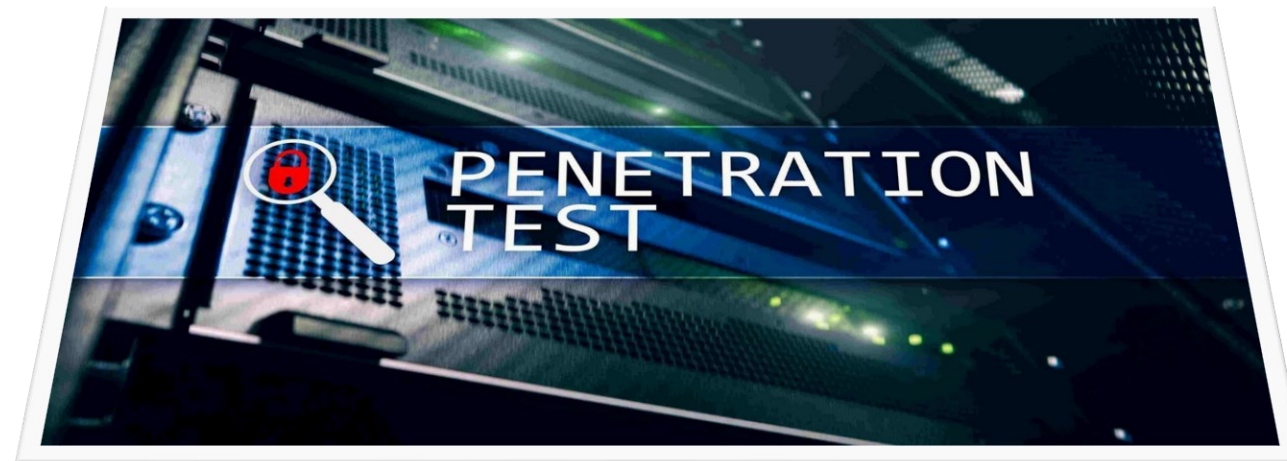
Auditoria de Hardware

Auditoria de Aplicações Web

Auditoria de Dispositivos Móveis

Auditoria Wireless

Auditoria física





# TIPOS DE AUDITORIA



## Auditorias Black Box

❖ Nenhuma informação

## Auditorias White Box

❖ Informação detalhada

## Auditorias Gray Box

❖ Informação parcial

# FASES DA AUDITORIA



## Planeamento e Recolha de Informações

- ❖ Recolha Activa
- ❖ Recolha Passiva

## Scanning e Exploração

## Análise e elaboração de Relatório



# FERRAMENTAS



**NMAP**



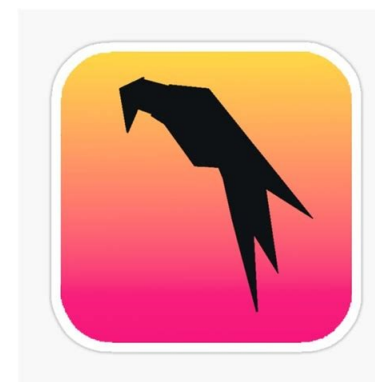
WPScan



OWASP  
Zed Attack Proxy



metasploit®





# ANÁLISE FORENSE



Incidentes de Segurança

Crimes cibernéticos

Investigações  
criminais





# PASSOS DE UMA ANÁLISE FORENSE

Desenvolvimento de Políticas e Procedimentos

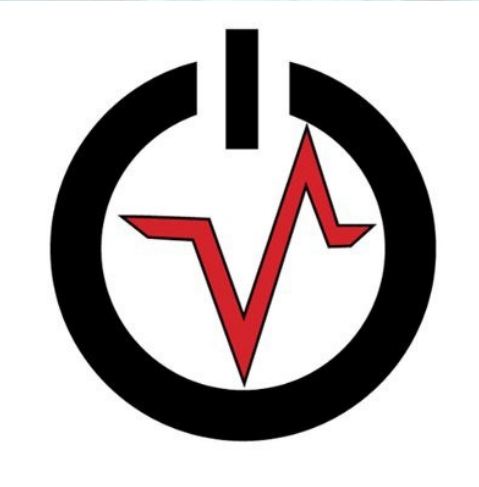
Avaliação das Evidências

Aquisição de Evidências

Exame de Evidências

Documentação e Relatório

# FERRAMENTAS





Obrigado!