

# FERRAMENTA NESSUS

NOME: ARTHUR PRETTO E BRUNO RAMOS.

# BIOGRAFIA:



- Origens da ferramenta
- País de Origem
- Evolução e Desenvolvimento da ferramenta

# Funcionalidades e Uso

O Nessus é conhecido por sua capacidade de identificar uma ampla variedade de vulnerabilidades em sistemas, redes e aplicativos. Ele utiliza um banco de dados extenso de plugins que são atualizados regularmente para garantir a detecção eficaz de ameaças recentes. A ferramenta é usada por profissionais de segurança, administradores de sistemas e equipes de resposta a incidentes para avaliar a postura de segurança de sistemas e redes.

# O QUE A FERRAMENTA FAZ

- Varredura de Vulnerabilidades;
- Detecção de Falhas de Configuração;
- Avaliação de Políticas de Segurança;
- Análise de Malware e Backdoors;
- Relatórios Detalhados;
- Integração com Outras Ferramentas;
- Atualizações Constantes.

The screenshot displays a web-based security tool's interface for managing scans. At the top, there are tabs for 'Scans' and 'Settings'. Below the tabs, a header shows 'Live Results Scan' and 'Back to My Scans'. On the right side, there are buttons for 'Configure', 'Audit Trail', 'Launch', and 'Export'. The main content area is titled 'Live Results Scan' and shows a table of vulnerabilities. The table has columns for 'Hosts' (1), 'Vulnerabilities' (45), and 'History' (1). A 'Filter' dropdown and a search bar are at the top of the table. The table lists 45 vulnerabilities, categorized by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). Most vulnerabilities are listed under the 'Mozilla Firefox' family, with counts ranging from 1 to 16. A note on the right side of the interface states: 'Notice: This scan has been updated with live results. Launch a new scan to confirm these findings or remove them.' Below this note, 'Scan Details' are provided, including the name, status, policy, scanner, and modification date. A legend on the right indicates the color coding for vulnerability levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Hosts	Vulnerabilities	History		
1	45	1		
Filter <input type="button" value="Search Vulnerabilities"/> 45 Vulnerabilities				
Sav	Name	Family	Count	
<input type="checkbox"/>	Critical	LIVE Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 59 Multiple Vulnerabilitie ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 59.0.1 Multiple Code Executi ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 59.0.2 Denial of Service Vuln ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 60 Multiple Critical Vulnerabi ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 61 Multiple Critical Vulnerabi ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	High	LIVE Mozilla Firefox < 62 Multiple Critical Vulnerabi ...	MacOS X Local Security Checks	1
<input type="checkbox"/>	Medium	SSL Certificate Cannot Be Trusted	General	1
<input type="checkbox"/>	Info	Netstat Portscanner (SSH)	Port scanners	16
<input type="checkbox"/>	Info	Service Detection	Service detection	4

Scan Details

Name: Live Results Scan  
Status: Completed  
Policy: Advanced Scan  
Scanner: Local Scanner  
Modified: Today at 6:03 PM (Live Results)

Vulnerabilities

Critical (Red)  
High (Orange)  
Medium (Yellow)  
Low (Green)  
Info (Blue)

# É open source ?

Como já foi falado inicialmente era uma ferramenta de código aberto, mas virou uma solução comercial. No entanto, a Tenable oferece uma versão gratuita chamada "Nessus Essentials" que fornece funcionalidades básicas de varredura, mas com limitações em comparação com a versão paga. Existe o Nessus expert e o Nessus professional, o expert tem o valor de aproximadamente 28 mil reais por ano e o outro aproximadamente 19 mil.

# Em quais distribuições de S.O. ela roda/executa?

- Linux;
- Unix;
- Windows.

# VANTAGENS:

- Detecção Abrangente de Vulnerabilidades;
- Atualizações Constantes;
- Relatórios Detalhados;
- Integração com Outras Ferramentas;
- Suporte a Padrões de Segurança;
- Opção Gratuita Disponível

# DESVANTAGENS:

- Licenciamento Comercial;
- Complexidade para Iniciantes;
- Consumo de Recursos;
- Necessidade de Atualizações Constantes;
- Limitações na Versão Gratuita.

# Curiosidades:

- Origem do Nome;
- Líder de Mercado;
- Versão Gratuita para Uso Pessoal;
- Suporte a Múltiplos Protocolos;

# Pontos Positivos na Instalação e Utilização do Nessus:

- Interface Amigável para Usuários Avançados;
- Variedade de Plataformas;
- Atualizações Contínuas;
- Relatórios Detalhados;
- Integração com Outras Ferramentas.

# Pontos Negativos na Instalação e Utilização do Nessus:

- Curva de Aprendizado para Iniciantes;
- Licenciamento Comercial;
- Consumo de Recursos;
- Limitações na Versão Gratuita.

# FIM