Scanners de Vulnerabilidades

+ São ferramentas capazes de automatizar o processo de descoberta de vulnerabilidades
→ Nessus → Comercial | Versão básica 'free'
→ Qualys → Comercial
→ OpenVAS → Open Source

https://www.tenable.com/plugins
→ Nesse site, podemos ver os plugins do nessus
→ Plugins são progamas que detectam vulnerabilidades

~~~~~~
Como Funciona?
~~~~~~
Um bom scanner de vulnerabilidades vai tentar automatizar o processo da seguinte forma:
1. Tenta identificar se o host está ativo
2. Realiza um portscan
3. Tenta identificar o Sistema Operacional
4. Tenta identificar os serviços encontrados
5. Faz a verificação de vulnerabilidades de acordo com sua base de vulnerabilidades

OBS: Logicamente, isso pode gerar falsos positivos