

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

AUDITORIAS DE SEGURANÇA

Fábio Mestre



Agenda

- O que é uma Auditoria de Segurança?
- Testes de intrusão
- Ferramentas para auditorias
- Duvidas e questões



O QUE É UMA AUDITORIA DE SEGURANÇA?

O que é uma Auditoria de Segurança?

- É um processo sistemático, independente e documentado para identificar, enumerar e descrever falhas ou vulnerabilidades que podem ser utilizadas para colocar em risco a segurança de informação.
- Pode ser definida como uma auditoria interna ou externa, manual ou automatizada.

O que é uma Auditoria de Segurança?

- Tem como missão analisar os controlos de segurança de informação implementados, bem como uma análise e gestão de risco operacional na infraestrutura de sistemas e tecnologias de informação.
- Deve ser organizada em intervalos planeados para disponibilizar informação sobre se o sistema de gestão de informação está conforme com os requisitos da Organização.

O que é uma auditoria de Segurança?

- Visa garantir que o Sistema de Gestão de Informação respeita o modelo de Segurança de Informação composto por Confidencialidade, Integridade e Disponibilidade da informação.

TESTES DE INTRUSÃO

Testes de Intrusão

- São um tipo de auditoria técnica que tem como objetivo avaliar a segurança de um sistema ou rede de computadores, simulando ataques de fonte maliciosa aos serviços disponíveis.
- Servem para medir o impacto de determinados ataques ou vulnerabilidades, bem como identificar novas falhas de segurança.

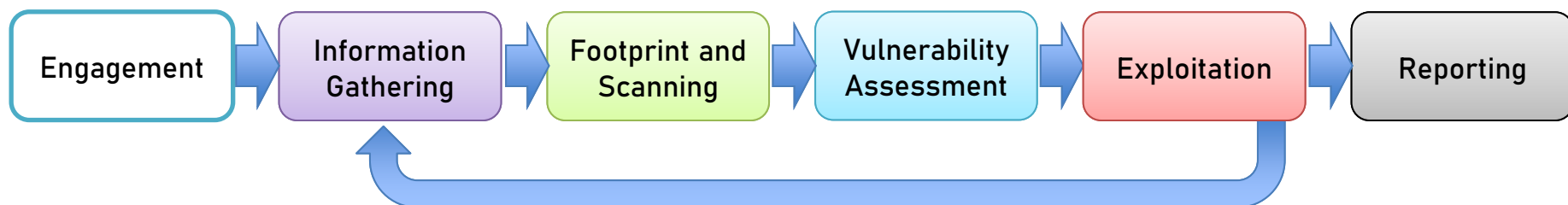


Testes de Intrusão

- Podem ser do tipo white-box, black-box ou grey-box.
- Podem simular diferentes tipos de ataques:
 - Engenharia Social
 - Ataques à rede e/ou à infraestrutura de rede
 - Ataques aos serviços e/ou aplicações web
 - Ataques de Negação de Serviço
 - Ataques aos serviços Cloud
 - Outros

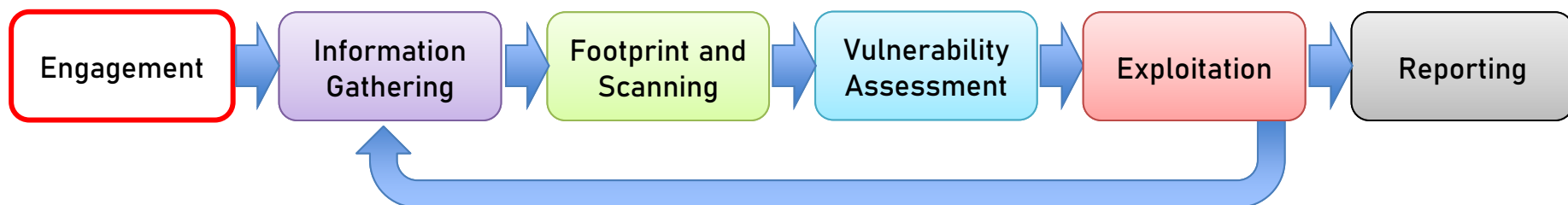
Ciclo de um teste de intrusão

- Um teste de intrusão tem seis fases distintas:
 - Definição de Requisitos (Engagement)
 - Recolha de Informação (Information Gathering)
 - Mapeamento (Footprint and Scanning)
 - Análise de Vulnerabilidades (Vulnerability Assessment)
 - Exploração de Vulnerabilidades (Exploitation)
 - Reportar os resultados (Reporting)



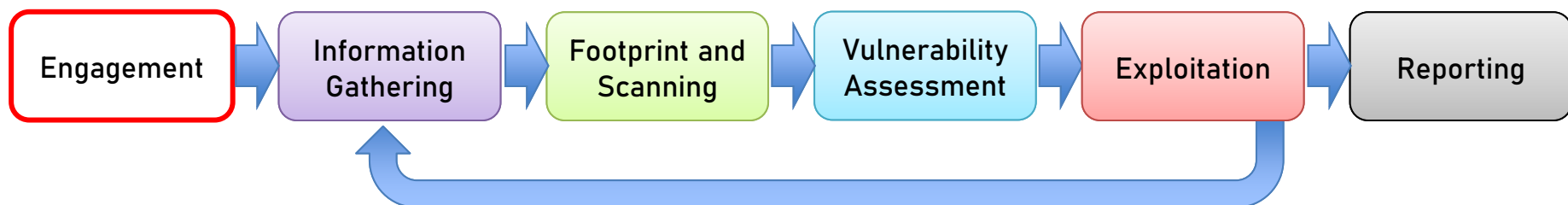
Requisitos (Engagement)

- São definidos os requisitos dos testes de intrusão
- É definido o contexto dos testes (scope)
- Que recursos serão testados com base no contexto
- Autorizações das entidades responsáveis pelos recursos



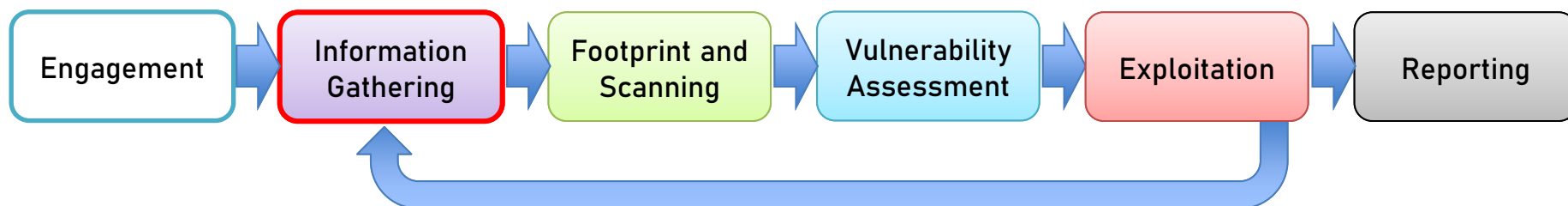
Requisitos (Engagement)

- Contactos de suporte da infraestrutura e da gestão de incidentes, se aplicável
- É tratada a documentação legal, se aplicável, que permite que o auditor seja autorizado a fazer os testes de intrusão respeitando a Lei do país em questão e respeitando acordos de confidencialidade



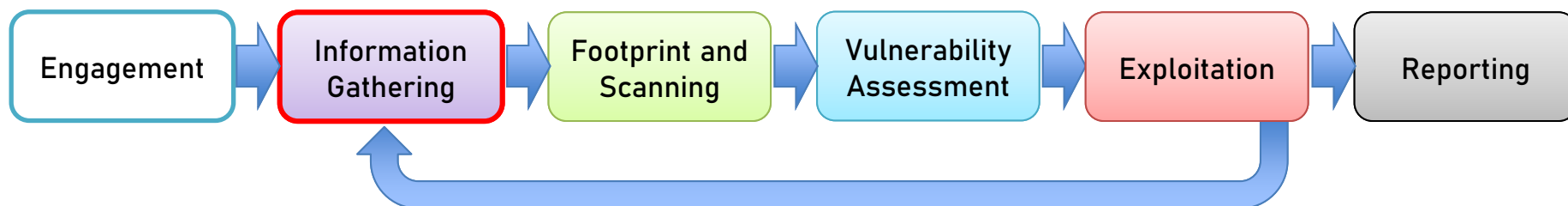
Recolha de Informação (Information Gathering)

- Início assim que os requisitos dos testes estão definidos e a partir da data de início definida
- O objetivo é recolher o máximo possível de informação do alvo dos testes, seja uma organização ou empresa, uma infraestrutura de rede ou uma aplicação



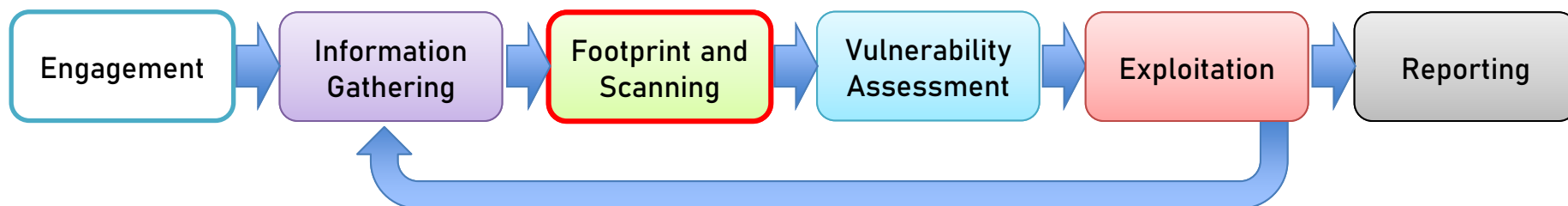
Recolha de Informação (Information Gathering)

- Infraestrutura (DNS, Servidores de Email, Servidores Web, Tecnologias, Frameworks)
- Conhecimento prévio do tipo de negócio que a organização presta, a fim de perceber o que é crítico e vital para o cliente dos testes de intrusão



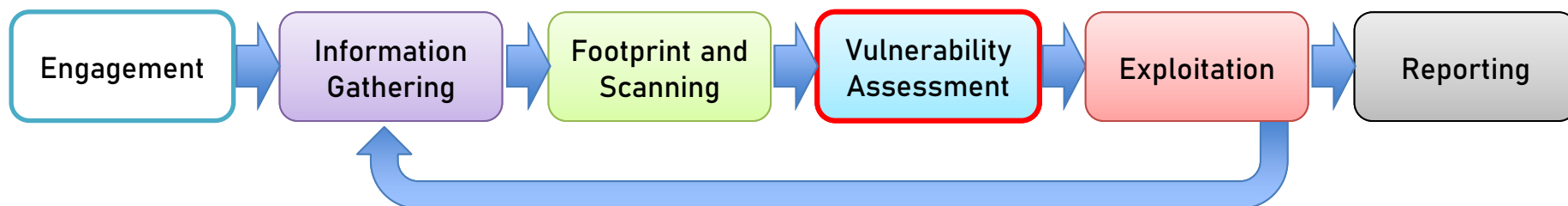
Mapeamento (Footprint and Scanning)

- Versões de Sistemas Operativos e aplicações (Footprinting)
- Scans de portas para descobrir que tipo de serviços e versões estão a correr (Scanning)
- A recolha nesta fase é feita de forma ativa, utilizando diversas ferramentas especializadas



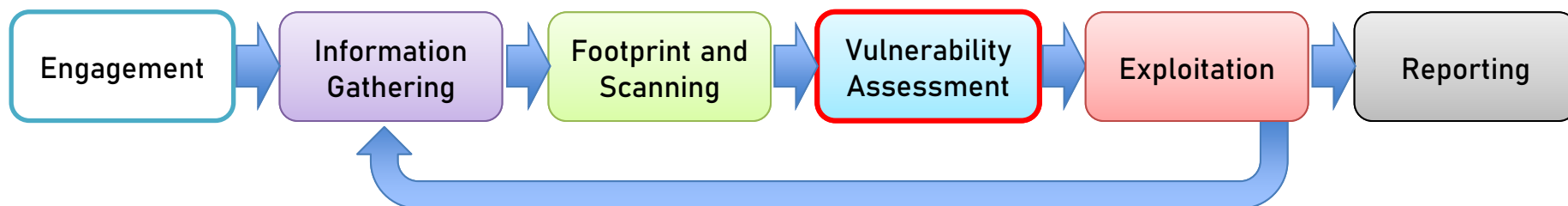
Análise de Vulnerabilidades (Vulnerability Assessment)

- É criada uma lista de todas as vulnerabilidades que estão presentes em todos os alvos testados
- Quanto maior a lista de vulnerabilidades criada, mais hipóteses existem de encontrar uma vulnerabilidade que permita o acesso não autorizado a sistemas ou aplicações



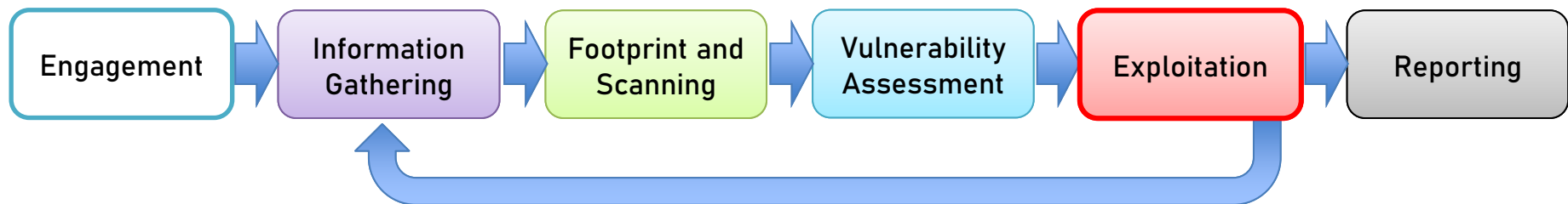
Análise de Vulnerabilidades (Vulnerability Assessment)

- Estas análises de vulnerabilidades podem ser feitas manualmente utilizando a informação recolhida anteriormente ou automaticamente através de ferramentas especializadas



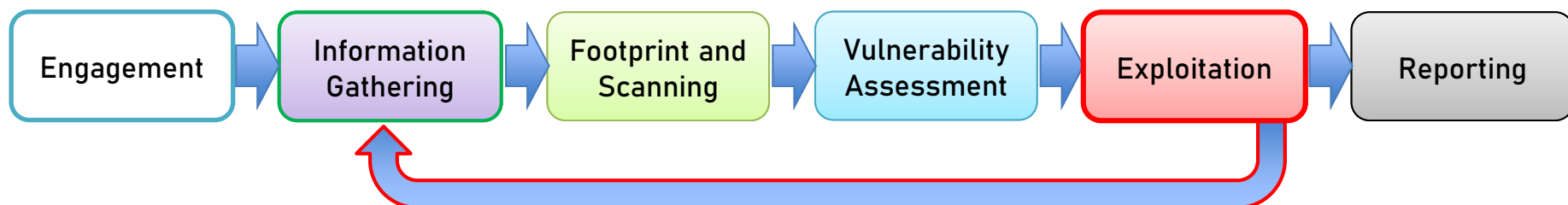
Exploração de Vulnerabilidades (Exploit)

- Nesta fase são verificadas se as vulnerabilidades existentes na lista criada anteriormente podem ser exploradas para ganhar acesso indevido a um sistema ou informação, contas de utilizador ou recursos protegidos, entre outros



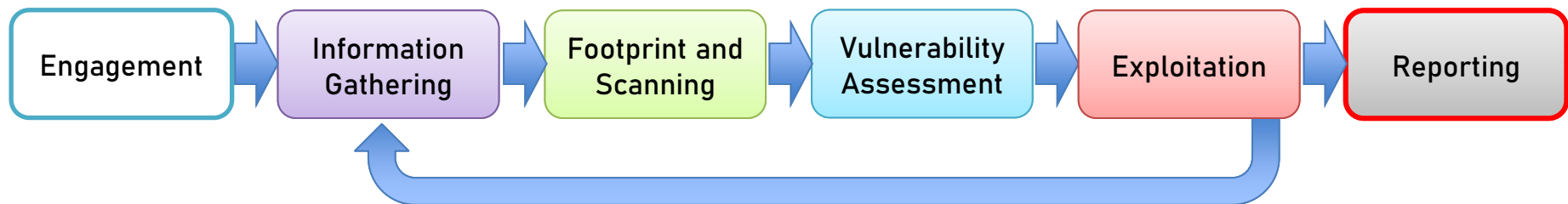
Exploração de Vulnerabilidades (Exploit)

- Muitas vezes uma exploração bem sucedida leva a que seja necessário mais recolha de informação de um ponto de vista diferente (dentro de um servidor por exemplo) e a repetir o ciclo dos testes de intrusão de modo a ganhar ainda mais privilégios e a explorar ainda mais vulnerabilidades



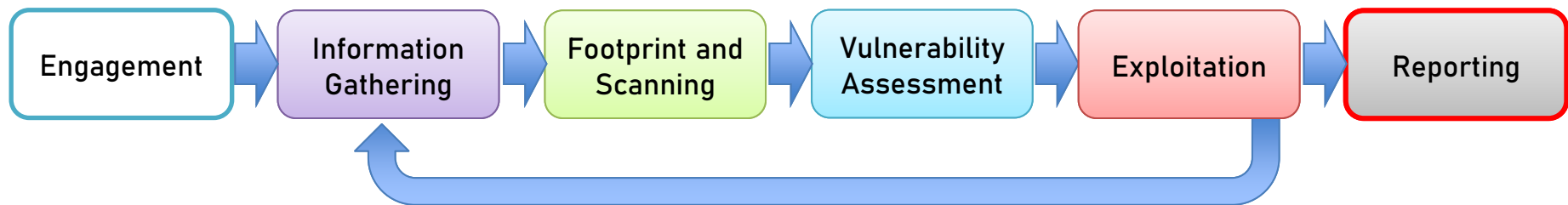
Reportar os resultados (Reporting)

- Esta fase começa quando já não existem mais alvos para explorar, ou quando o tempo definido para os testes é alcançado ou excedido



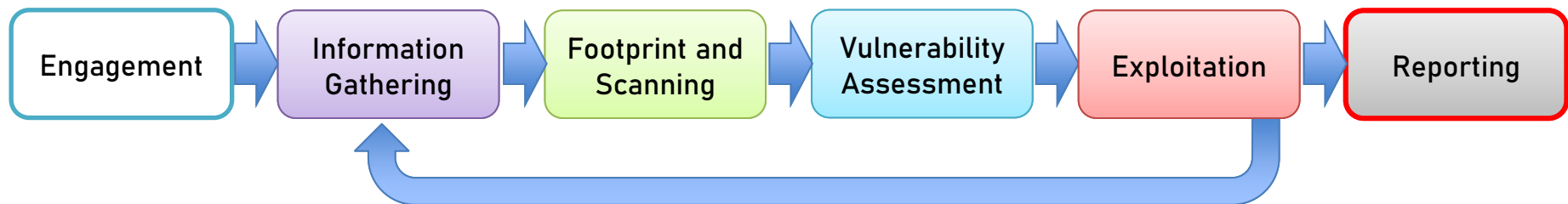
Reportar os resultados (Reporting)

- É a fase mais importante pois é aqui que a informação recolhida e obtida sobre todas as vulnerabilidades encontradas é colocada num documento que vai ser entregue e/ou comunicado à organização, empresa ou entidade responsável pelos recursos que testámos



Reportar os resultados (Reporting)

- Estes resultados devem referir técnicas utilizadas, vulnerabilidades encontradas, exploits utilizados, análise de risco e de impacto para cada vulnerabilidade encontrada e, se possível, como corrigir as mesmas.



FERRAMENTAS PARA AUDITORIAS

Ferramentas para Auditorias

- Existem ferramentas diferentes para cada fase de um teste de intrusão, embora algumas ferramentas possam ser utilizadas em várias fases.
- Algumas ferramentas são gratuitas e/ou open source, outras são pagas.
- Existem ferramentas para automatizar algumas fases do processo de testes de intrusão.




Ferramentas para Auditorias

- Além de diferentes ferramentas disponíveis, existem também sistemas operativos adaptados para testes de intrusão, com centenas de ferramentas:
 - Kali Linux
 - Black Arch
 - Parrot OS
 - Command VM
 - BackBox



WPScan

Em Resumo

-  Garante que os nossos sistemas de segurança de informação funcionam como é suposto
-  Frequência é importante, uma vez que surgem vulnerabilidades novas todos os dias
-  As ferramentas automatizadas ajudam a identificar vulnerabilidades. No entanto são necessários testes manuais para evitar falsos positivos.



Obrigado