Etapa - Análise de Vulnerabilidades

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Processo
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Seguem-se as seguintes etapas:
1. Identificar o possível SO
2. Identificar a possível versão so software / aplicação / sistema
3. Buscar por vulnerabilidades conhecidas
4. Tentar identificar vulnerabilidades ainda não conhecidas
5. Se possível, tentar outros tipos de ataques (exemplo: Brute Force)

Bases de dados de vulnerabilidades e exploits:
https://www.exploit-db.com/
https://www.securityfocus.com/vulnerabilidades
https://cvedetails.com/
https://nvd.nist.gov/vuln/search
https://www.rapid7.com/db/?q=&type=
https://packetstormsecurity.com/files/tags/exploit/

searchsploit - utilitário para busca de exploits (exploit-db)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Fase de Análise de Vulnerabilidade
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Durante o processo de um pentest, chegaremos à fase de análise de vulnerabilidades, ou melhor, fase onde devemos procurar por possíveis vulnerabilidades existentes no ambiente testado.

As vulnerabilidades podem aparecer em vários locais, em aplicações, software, sistema operacional, serviços, configurações, comunicação, ou seja, não existe uma receita de bolo, mas um processo

Seguindo nosso método de trabalho:
- Information Gathering | Coleta de Informações
- Scanning | Varredura
- Enumeration | Enumeração
- Vulnerability Analysis | Análise de Vulnerabilidades ←
- Exploitation | Exploração
- Post Exploitation | Pós Exploração