3.1-Ciclo-de-Vida-de-uma-VA.md

localhost/

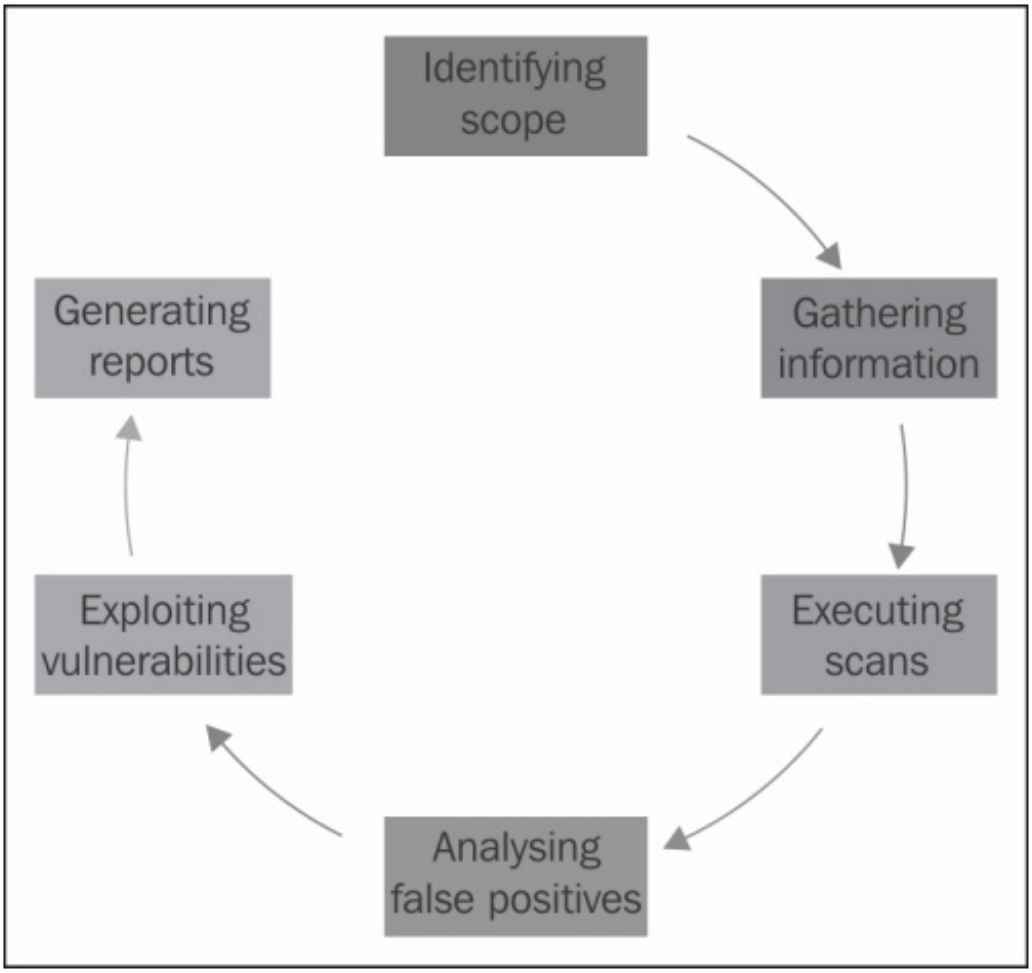
Ciclo de Vida de uma Análise

Processo de Análise de Vulnerabilidades e Pentest possuem um Ciclo de Vida comum referente às fases que devem ser executadas é que vão desde da definição do escopo até a entrega do relatório do que fora executado.

Para execução de um uma Análise de Vulnerabilidades completa os seguintes passos são necessarios:

- 1 - Definição de Escopo;
- 2 - Levantamento de Informações;
- 3 - Varredura e Escaneamento;
- 4 - Análise de Falsos Positivos;
- 5 - Exploração de Vulnerabilidades (Caso seja um pentest);
- 6 - Geração de Relatório e Report de Resultados;

A imagem abaixo ilustra esse processo de Análise:



[[images/lifecicle.png]]

FASE 1 - Definição de Escopo:

O primeiro passo da execução de uma Análise é identificar corretamente o Escopo da infraestrutura ou Sistema sobre a qual o processo será conduzido, no caso de plataformas de desenvolvimento e sistemas isso inclui verificação do tipo de sistema, linguagem utilizada, banco de dados, plataforma de hospedagem e ou publicação do conteúdo etc. O Escopo dependerá diretamente do objetivo de seu teste, ferramentas a serem utilizadas, data e horário de execução devem ser acordados, outro ponto importante é documentar o processo a ser executado e garantir que todas as partes envolvidas estão de acordo quando o teste a ser executado envolver elementos além de seu código / infraestrutura.

Testes do Tipo "BlackBox"

Existe uma modalidade específica de testes de invasão chamada ***BlackBox*** neste modelo apenas informações como endereço IP do alvo são oferecidas ao Analista ou Pentester esse tipo de teste não involve qualquer fornecimento de informações e tem a finalidade de similar o cenário encontrado por um atacante ao executar um pentest na plataforma envolvida.

Testes do Tipo "GreyBox"

Testes do tipo "GreyBox" incluem algumas informações referentes ao alvo como a Versão de Software utilizada, configurações relevantes ou até mesmo credenciais de acesso, Essa abordagem é utilizada para obter relatórios mais completos e avaliar Resiliência de um ambiente e a existência de Vulnerabilidades conhecidas.

FASE 2 - Levantamento de Informações

A segunda fase de uma análise é o levantamento de informações, essa fase é essencial principalmente em testes no formato BlackBox onde inicialmente nenhuma informação foi fornecida, ela envolve desde questões simples como definição exata de quem é seu alvo (o comando "whois" disponível em sistemas Linux é um bom começo), até identificacao exata das plataformas envolvidas, nesse ponto ferramentas de rede como o NMAP e o Telnet serão úteis, outras informações podem ser obtidas por scaners como o Nikto.

A informação obtida aqui será importante para redução do escopo definido inicialmente e escolha das ferramentas utilizadas na FASE 3 e na FASE 4.

FASE 3 - Escaneamento de Vulnerabildiades

Essa fase inclui o processo de escaneamento em si e levantamento de vulnerabilidades encontradas, este processo envolve o uso de ferramentas definidas de acordo com as informações obtidas na fase anterior, como exemplo para esta disciplina utilizaremos Frameworks Opensource como o w3af e o Arachni e soluções proprietários como o Nessus, o retorno desse escaneamento também será a base para um pentester definir quais os exploits a serem utilizados contra seu alvo.

FASE 4 - Analise de Falsos Positivos

Conforme descrito no material na base deste conteúdo, é comum que durante um processo de analise haja a ocorrencia de falsos positivos, uma vez que a ferramenta utilizada deve gerar o retorno baseado em sua base de dados e em seu modelo de classificação de riscos, esses elementos devem ser minerados e analisados pelo analista responsável pelo teste a fim de isolar dentro do relatório obtidos os elementos que realmente representem uma vulnerabildiade.

FASE 5 - Exploração de Vulnerabilidades

Essa fase se aplica a processos de pentest e a situações onde será necessário apresentar uma prova conceito ao dono da aplicação esclarecendo o tipo de vulnerabilidade e como um atacante tomaria proveito disso.

FASE 6 - Geração de Relatórios e Report de Resultados;

Após execução da Analise é necessário a geração de uma relatório final contendo o detalhamento técnico do processo, esse relatório deverá inglobar alguns itens conforme descrito abaixo:

- O escopo da avaliação, itens abordados, alvos e objetivos;
- A gestão/resumo do processo executado;
- Uma sinopse das falhas descobertas com a severidade do risco relacionado;
- Detalhamento sobre cada falha e seu respectivo impacto;
- Recomendações para corrigir a vulnerabilidade;

Material de Referência:

Boa parte da base teórica descrita acima foi baseada nos primeiros capitulos do livro Learning Nessus for Penetration Testing do autor Himanshu Kumar publicado pela PUCKT

- Nessus for Penetration Testing By Himanshu Kumar

Free Software, Hell Yeah!