3.-VA---Vulnerability-Assessment.md

localhost/

[[images/1844081.jpg]]

Avaliação de vulnerabilidades

É muito comum encontrarmos definições e bibliografias em inglês que utilizem o termo "VA" Vulnerability Assessment ou Avaliação de Vulnerabilidades, a ideia por trás deste tipo de processo é avaliar e auditar um determinado ambiente, solução ou sistema utilizando ferramentas voltadas para tal finalidade, como por exemplo o Nessus, o Nikto ou o Arachni.

Muitas dessas ferramentas a primeira vista parecem simples e até são do ponto de vista de ux e usabilidades (O Nessus é um belo exemplo disso), porém a parte complicada está na mineração, análise e interpretação dos resultados apresentados; Configurações incorretas e mal uso tendem a levar a resultados inconclusivos cheios de falsos positivos, cabe ao auditor responsável pelo uso da ferramenta aseparar que o tipo de informação levantada realmente importa, identificando situações, configurações e exploits que possam levar ao comprometimento da informações e consquentemente do negócio.

Falsos Positivos e Falsos Negativos

Uma etapa importante no uso de um VA para levantamento de vulnerabilidades é a análise do resultado obtido removendo possíveis falsos positivos ou falso negativos, falsos positivos são muito comuns no output de ferramentas de análise, eles referem-se a vulnerabilidades relataras como ativas no sistema mas que na realidade não existem ou já foram mitigadas utilizando um patch de atualizações por exemplo.

Já os chamados Falsos Negativos são na maioria das vezes mais complicados de se identificar e dependem diretamente do conhecimento técnico do Analista ou Developer responsável pelo processo de análise trata-se de situações e outputs que não foram relacionados a vulnerabilidades pela ferramenta usada, neste caso o uso de mais de uma ferramenta por exemplo permitirá um resultado mais acertivo.

> ***Importante:*** *Falsos positivos e vulnerabilidades de baixo score ou difícil exploração são coisas diferentes, uma vulnerabilidade pode ser classificada como "Low" segundo o score da CVSS mas ainda assim continua sendo uma vulnerabilidade reportada uma vez que esteja ativa no sistema.*

Prova Conceito

Caso o responsável pelo teste possua acesso ao sistema, aplicação ou servidor no qual o VA executou o scan é

interessante que as informacoes levantadas sejam cruzadas com a realidade do alvo ou seja, se possível testar a vulnerabilidade desde que isso não afete a aplicação ou preferencialmente atuando em janelas de manutenção.

Como um VA classifica uma vulnerabilidade?

A maioria das ferramentas e frameworks de segurança utilizam algum modelo de ranking para classificação dos riscos encontrados, a título de padronização e para facilitar o endendimento usando uma linguagem comum temos o CVSS como principal recurso para esse processo de "ranking" ou "raiting".

CVSS

O CVSS ou Common Vulnerability Scoring System é um sistema open source cuja função é classificar as vulnerabilidades conhecidas baseado nas características e no impacto de uma vulnerabilidade, a vantagem desse modelo é que sua atualização é constante, uma classificação pode mudar com base em um novo recurso explorado a partir dessa vulnerabilidades ou na quantidade de sistemas a serem afetados por exemplo.

O nessus por exemplo utiliza o CVSS como base na classificação que aparece em seu relatório, mais informações sobre isso podem ser obtidas diretamente no site do projeto www.first.org/cvss;

CVE

Common Vulnerability and Exposures (CVE): O CVE é uma base de dados pública relativa a vulnerabilidades é exploits conhecidos e já documentados, cara vulnerabilidades relatada é assinada como um número único de identificacão, chamamos esse número de "CVE Number" ferramentas de análise como o Nessus e o W3af referenciam esse número ao gerar um relatório de vulnerabilidades. Esses relatórios podem ser consultados no cve.mitre.org.

CWE

Common Weakness Enumeration (CWE): O CWE é conceitualmente similar ao CVE, trata-se de outra base de dados pública, só que referente a um dicionário com tipos de fraquezas/vulnerabilidades conhecidas, sua base de dados pode ser consultada em cwe.mite.org;

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!