Escola Superior de Redes RNP

Teste de Invasão de Aplicações Web

Capítulo 10

Escrita de relatórios e exercício completo

Objetivos

- Ilustrar como os resultados de um teste de invasão de aplicação web podem ser apresentados para as equipes técnicas e gerenciais, considerando-se a gravidade de cada vulnerabilidade encontrada.

Escola Superior de Redes RNP

- **Relatório detalhado, relatório executivo, common vulnerability scoring system.**

Tópicos abordados

- Introdução
- Common Vulnerability Scoring System
- Tipos de relatórios
- Apêndice

Introdução

Uma vez finalizado um teste de invasão em aplicações web, o resultado deve ser apresentado ao cliente.

Esta etapa é extremamente importante, pois é ela que norteará quais problemas serão tratados.

Subsídios suficientes devem ser fornecidos ao cliente, para que ele, com base em uma análise de risco, seja capaz de traçar um plano de ação realístico.

Escola Superior de Redes RNP

Os entregáveis e atividades de um teste de invasão de aplicações web incluem:

- Relatório detalhado
- Apresentação técnica
- Relatório executivo
- Apresentação executiva

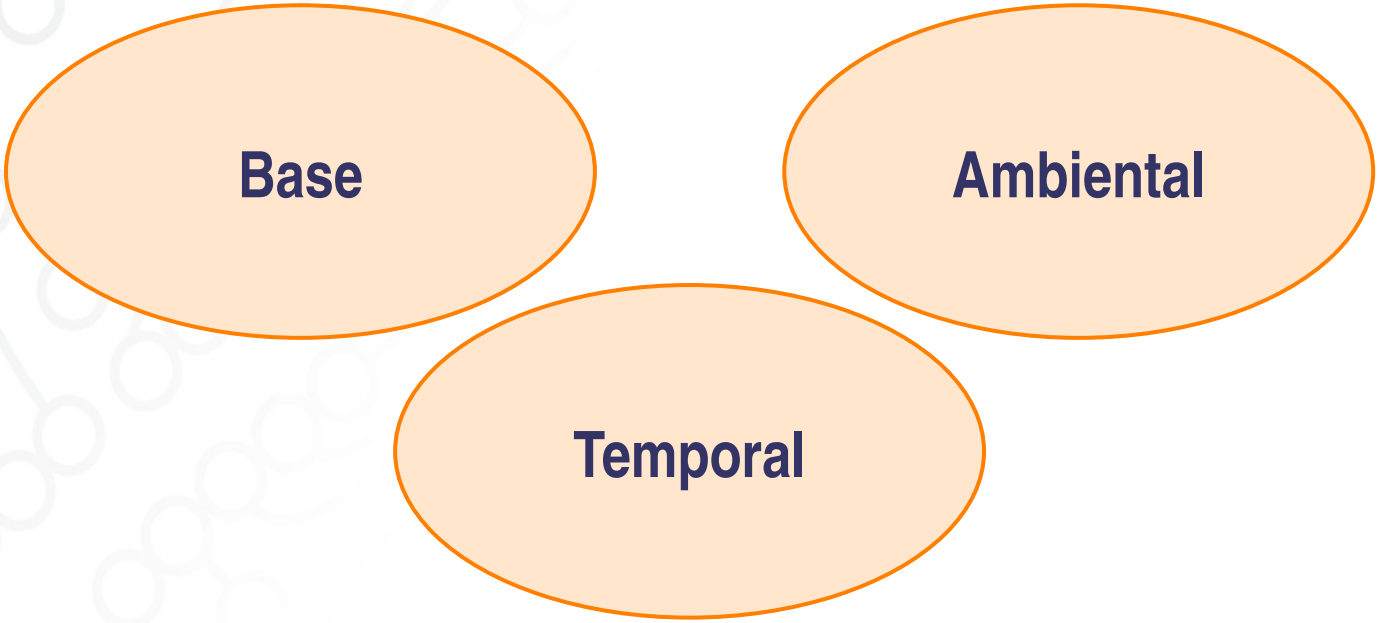
Common Vulnerability Scoring System

Escola Superior de Redes RNP

O Common Vulnerability Scoring System (CVSS) define métodos para estimar a gravidade de vulnerabilidades de TI, de modo que seja possível avaliá-las sob um critério uniforme.

Common Vulnerability Scoring System

São três escores, os quais resumem métricas relacionadas entre si:



Common Vulnerability Scoring System

Escola Superior de Redes RNP

Enquanto o grupo base apresenta as propriedades fundamentais da vulnerabilidade, os demais adicionam informações referentes ao contexto particular, no qual o defeito é encontrado.

Em inúmeras situações, somente o escore base é utilizado.

Um vetor textual, contendo as escolhas de cada métrica, deve acompanhar o respectivo escore.

Escore de Base

O grupo base de métricas considera as características fundamentais de uma vulnerabilidade:

Vetor de acesso	Autenticação	Complexidade de acesso
Impacto à integridade	Impacto à confidencialidade	Impacto à disponibilidade

Métrica: Vetor de acesso (AV)

Quanto maior o número de pessoas com acesso ao ambiente vulnerável, maior é a criticidade do defeito de segurança, pois o potencial de atacantes cresce.

Valor da métrica	f(AV)	Critérios
Local (L)	0,395	A vulnerabilidade pode ser explorada somente com acesso local ao ativo vulnerável.
Rede adjacente (A)	0,646	É possível explorar a vulnerabilidade apenas a partir da rede local na qual se encontra o ativo inseguro.
Rede (N)	1,0	O defeito de segurança pode ser explorado remotamente. No caso de aplicações web, normalmente, esse é o cenário encontrado.

Figura 10.1 - Avaliação da métrica Vetor de Acesso.

Métrica: Complexidade de acesso (AC)

Avalia o nível de dificuldade de execução do ataque, com base em diversos fatores, como privilégios necessários no sistema alvo, por exemplo.

Valor da métrica	f(AC)	Critérios
Alto (H)	0,35	Existem condições especiais para que o ataque seja bem-sucedido, como nível de acesso elevado ao ambiente e necessidade de comprometimento de outros ativos, por exemplo.
Médio (M)	0,61	Algumas condições não tão restritivas existem para efetuar a exploração da vulnerabilidade com sucesso. Exemplos incluem a necessidade de levantamento de informações sobre o ambiente e agentes de ameaça limitados a um pequeno grupo de pessoas.
Baixo (L)	0,71	Não há condições especializadas para exploração da vulnerabilidade. Um exemplo consiste na existência de ferramentas automatizadas para execução de um ataque.

Figura 10.2 – Avaliação da métrica Complexidade de Acesso

Métrica: Autenticação (Au)

Considera quantas vezes um atacante necessita se autenticar no sistema alvo, antes de executar um ataque explorando a vulnerabilidade.

Valor da métrica	f(Au)	Critérios
Múltiplas vezes (M)	0,45	Para conseguir explorar a vulnerabilidade, o atacante necessita se autenticar duas ou mais vezes no ambiente.
Uma vez (S)	0,56	O usuário malicioso precisa se autenticar uma vez no ambiente antes de realizar o ataque.
Nenhuma vez (N)	0,704	Não há necessidade de autenticação para a realização de um ataque.

Figura 10.3 – Avaliação da métrica Autenticação.

Métrica: Impacto à confidencialidade (C)

Escola Superior de Redes RNP

Considera o montante de informações que pode ter o sigilo comprometido, se a vulnerabilidade é explorada com sucesso.

Valor da métrica	f(C)	Critérios
Nenhum (N)	0,0	Nenhuma informação sigilosa é revelada, como resultado de uma exploração bem-sucedida da vulnerabilidade.
Parcial (P)	0,275	Parte das informações sigilosas é comprometida se um ataque é realizado com sucesso.
Completo (C)	0,660	Todas as informações sigilosas são reveladas em decorrência de um ataque bem-sucedido.

Figura 10.4 - Avaliação da métrica Impacto à confidencialidade.

Métrica: Impacto à integridade (I)

Esta métrica considera o montante de informações que tem a integridade comprometida, caso um ataque consiga explorar a vulnerabilidade.

Valor da métrica	f(I)	Critérios
Nenhum (N)	0,0	Nenhuma informação tem a integridade comprometida, como resultado de uma exploração bem sucedida da vulnerabilidade.
Parcial (P)	0,275	Parte das informações tem a integridade comprometida se um ataque é realizado com sucesso.
Completo (C)	0,660	Todas as informações são adulteradas em decorrência de um ataque bem-sucedido.

Figura 10.5 - Avaliação da métrica Impacto à integridade.

Métrica: Impacto à disponibilidade (A)

Mede o impacto à disponibilidade do sistema, caso a vulnerabilidade seja explorada em um ataque bem sucedido.

Valor da métrica	f(A)	Critérios
Nenhum (N)	0,0	Não há impacto à disponibilidade do sistema vulnerável.
Parcial (P)	0,275	Se a vulnerabilidade é explorada com sucesso, há redução do desempenho do ativo ou interrupção de parte dos serviços.
Completo (C)	0,660	O sistema fica totalmente indisponível em decorrência de um ataque bem-sucedido.

Figura 10.6 - Avaliação da métrica Impacto à disponibilidade (A).

Cálculo de escore de base

IMPACTO

$$Impacto = 10{,}41 \times (1-(1-f(C)) \times (1-f(I)) \times (1-f(A)))$$

F(IMPACTO)

$$f(Impacto) = \begin{cases} 0; & \text{se Impacto} = 0 \\ 1{,}176; & \text{caso contrário} \end{cases}$$

EXPLORABILIDADE

$$Explorabilidade = 20 \times f(AV) \times f(AC) \times f(Au)$$

ESCORE DE BASE

$$Escore\ de\ Base = arredonda\_1\_casa\_decimal((0{,}6 \times Impacto + 0{,}4 \times Explorabilidade - 1{,}5) \times f(Impacto))$$

Vetor textual

Escola Superior de Redes RNP

O vetor textual indica que valor foi escolhido para cada métrica, de acordo com os critérios estabelecidos.

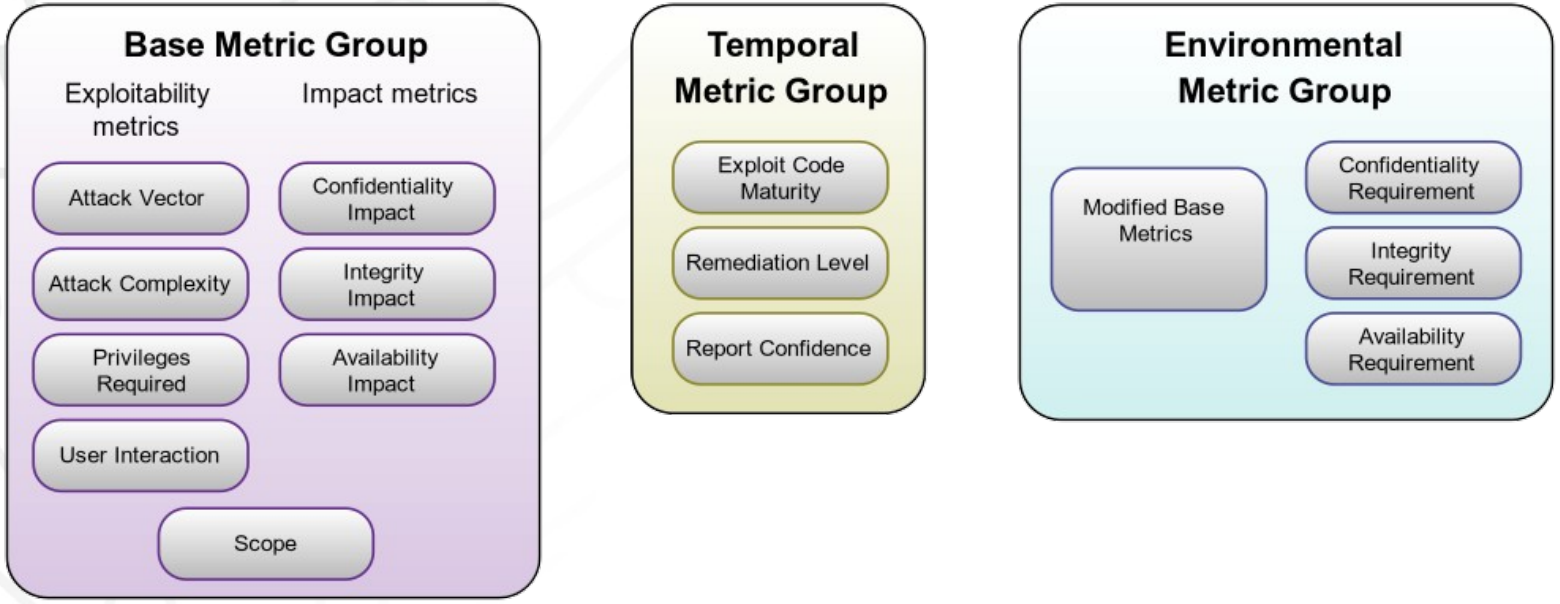
O formato geral está abaixo apresentado:

AV:<L|A|N>/AC:<H|M|L>/Au:<M|S|N>/C:<N|P|C>/I:<N|P|C>/A:<N|P|C>

Exemplo CVSS

- **Vetor de acesso –** Rede (N), f(AV) = 1,0**;**
- **Complexidade de acesso –** Baixo (L), f(AC) = 0,71**;**
- **Autenticação –** Nenhuma vez (N), f(Au) = 0,704**;**
- **Impacto à confidencialidade –** Completo (C), f(C) = 0,660**;**
- **Impacto à integridade –** Completo (C), f(I) = 0,660**;**
- **Impacto à disponibilidade –** Completo (C), f(A) = 0,660**.**
- **10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)**

CVSS 3.1


Base Metric Group
Exploitability metrics
Impact metrics
Attack Vector
Attack Complexity
Privileges Required
User Interaction
Confidentiality Impact
Integrity Impact
Availability Impact
Scope
Temporal Metric Group
Exploit Code Maturity
Remediation Level
Report Confidence
Environmental Metric Group
Modified Base Metrics
Confidentiality Requirement
Integrity Requirement
Availability Requirement

CVSS 3.1 – Escala de Gravidade

Avaliação	Pontuação CVSS
Nenhum	0,0
Baixo	0,1 – 3,9
Médio	4,0 – 6,9
Alto	7,0 – 8,9
Crítico	9,0 – 10,0

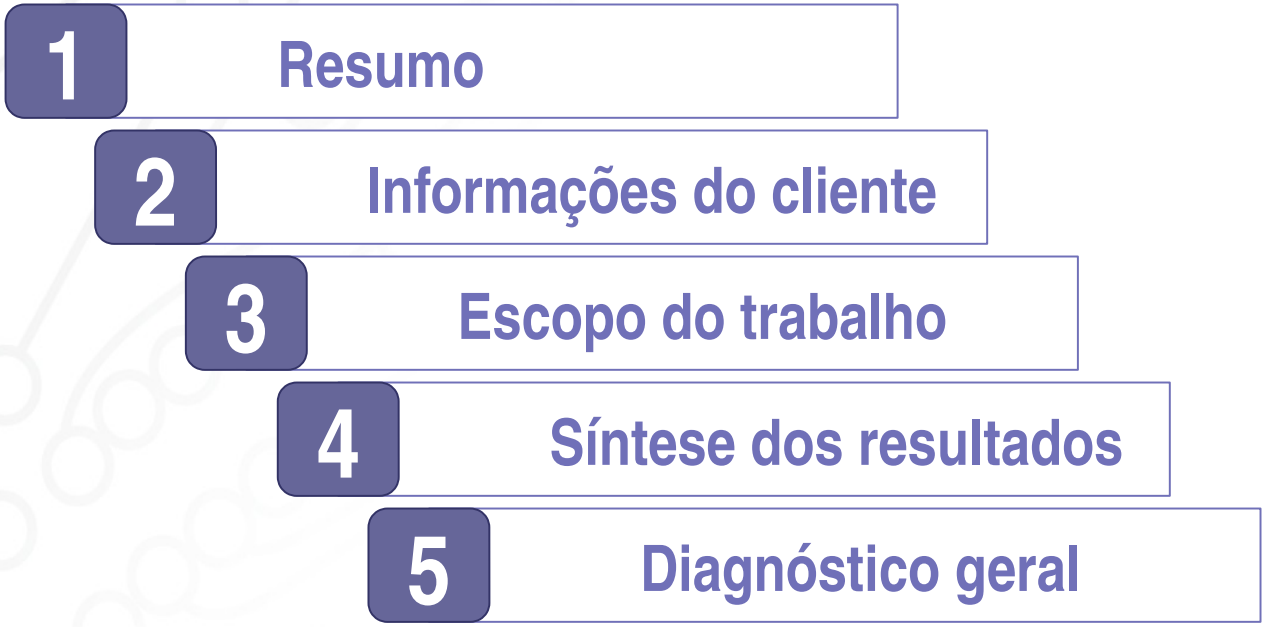
Tipos de relatório

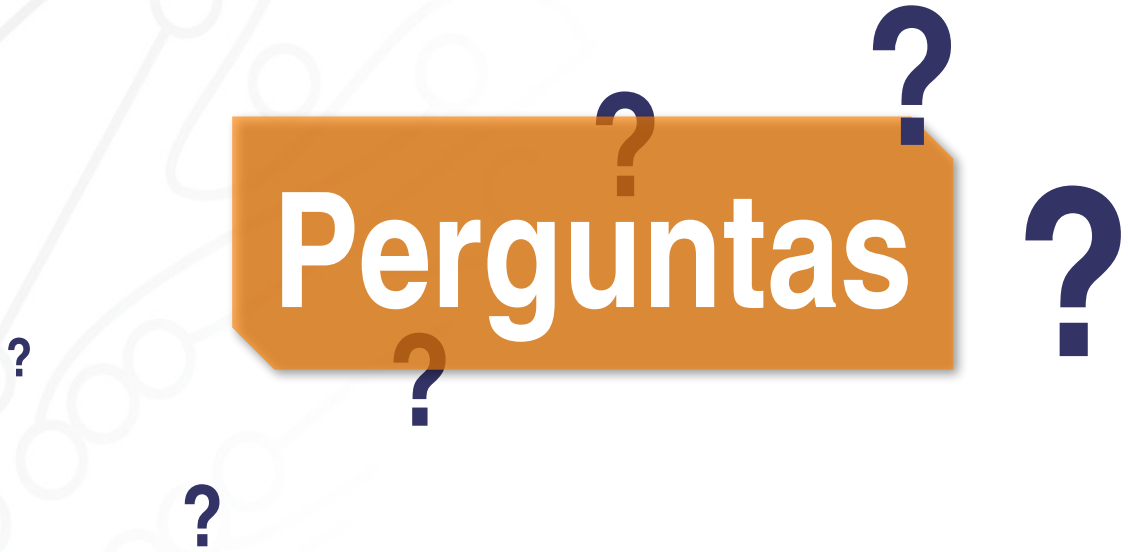
Relatório detalhado	**contém todas as informações, gerais e técnicas, acerca do trabalho realizado.**
Relatório executivo	**baseado no conteúdo do relatório detalhado, engloba apenas os fatos mais relevantes do teste de invasão executado.**

Relatório detalhado

1. Resumo
2. Informações do cliente
3. Escopo do trabalho
4. Descrição do teste
5. Resultados
6. Referências
7. Anexos

Relatório executivo




Perguntas