Logo da empresa/professional

# Relatório de Pentest – White/Black Box

# Nome da empresa/professional

# Data

# Controle de versões

*Para casos de atualizações dos relatórios*

|  |  |  |
| --- | --- | --- |
| **Versão** | **Data** | **Responsável** |
| V01 | 1/11/2022 | Nome do Pentester |
|  |  |  |

# Termo de confidencialidade

*Se refere a questão da privacidade das informações. É uma forma de deixar claro quem poderá acessar e com quem o documento pode ser compartilhado.*

# Contato

|  |  |  |  |
| --- | --- | --- | --- |
| **Nome** | **Função** | **Telefone** | **Email** |
| Nome do Pentester | Pentester | (00)00000-0000 | aaaa@sss.com |
|  |  |  |  |

# Aviso Legal

*Estabelece qual foi o limite que a empresa contratante disponibilizou para a ação do pentester e deixa claro que os resultados são baseados nas informações disponibilizadas pelo contratante.*

# Sumário Executivo

*O sumário executive descreve de forma compacta e resumida os resultados obtidos no Pentest. Aqui é apenas um resumo, sem detalhes técnicos, apenas uma breve descrição do resultado para dar uma visão geral.*

# Metodologia

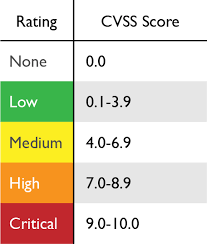
*Detalhamento das etapas percorridas no processo de Pentest. Pode usar como base o Framemork PTES ou outros.*



* *Interações iniciais: primeiros contatos com o cliente para definir as regras do Pentest;*
* *Obtenção de informações: descoberta das vulnerabiliades;*
* *Modelagem de ameaças: Modelagem dos ataques a serem realizados;*
* *Análise de vulnerabilidades: Análise das vulnerabilidades encontradas;*
* *Exploração: realização do ataque sobre as vulnerabilidades encontradas;*
* *Pós-exploração: Estabelecimento da sessão e captura dos dados;*
* *Relatórios: compilação e relato das vulnerabilidades encontradas e exploradas.*

# Escala de severidade - CVSS 3

*Pode-se utilziar como base o score do CVSS para padronizar os níveis de comprometimento da vulnerabilidade*



# Sumário de vunerabilidades encontradas

*Geralmente uma tabela com dados sucintos sobre os hosts comprometidos e a vulnerabilidade*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID Host** | **IP do Host** | **Vulnerabilidade** | **Risco** | **Impacto** |
| 01 | 172.16.2.2 | MS17-010 - Eternalblue | Crítico | Alto |
| 02 | 172.16.2.3 |  |  |  |

# Detalhamento das vulnerabilidades

### Alvo 01

#### Nome da vulnerabilidade: MS17-010-Eternalblue

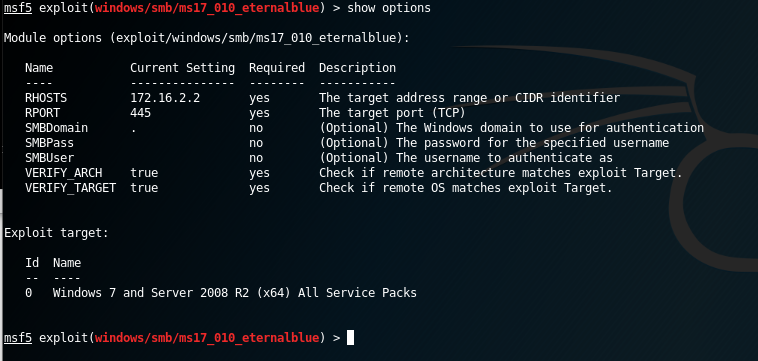
#### Descrição da vulnerabilidade:

*O EternalBlue é um exploit desenvolvido pela Agência Nacional de Segurança dos Estados Unidos (NSA). Faz parte de um conjunto de programas secretosdo governo dos EUA revelados pelo grupo Shadow Brokers em 14 de abril de 2017.*

*O Eternalblue foi o exploit utilizado no ciberataque mundial com o ransomware WannaCry e pelo malware Adylkuzz.*

#### Descrição da prova de conceito:

*A ferramenta utilizada foi o Metasploit no SO Kali Linux.*



#### Recomendações

*A documentação a respeito das contramedidas está disponível em:* [*https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010*](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010)

### Alvo 01

#### Nome da vulnerabilidade:

#### Descrição da vulnerabilidade:

#### Descrição da prova de conceito:

#### Recomendações