RELATÓRIO DE PENTEST

CLIENTE:

VERIFACT

TIPO DE RELATÓRIO:

Relatório Executivo de teste de invasão

DATA:

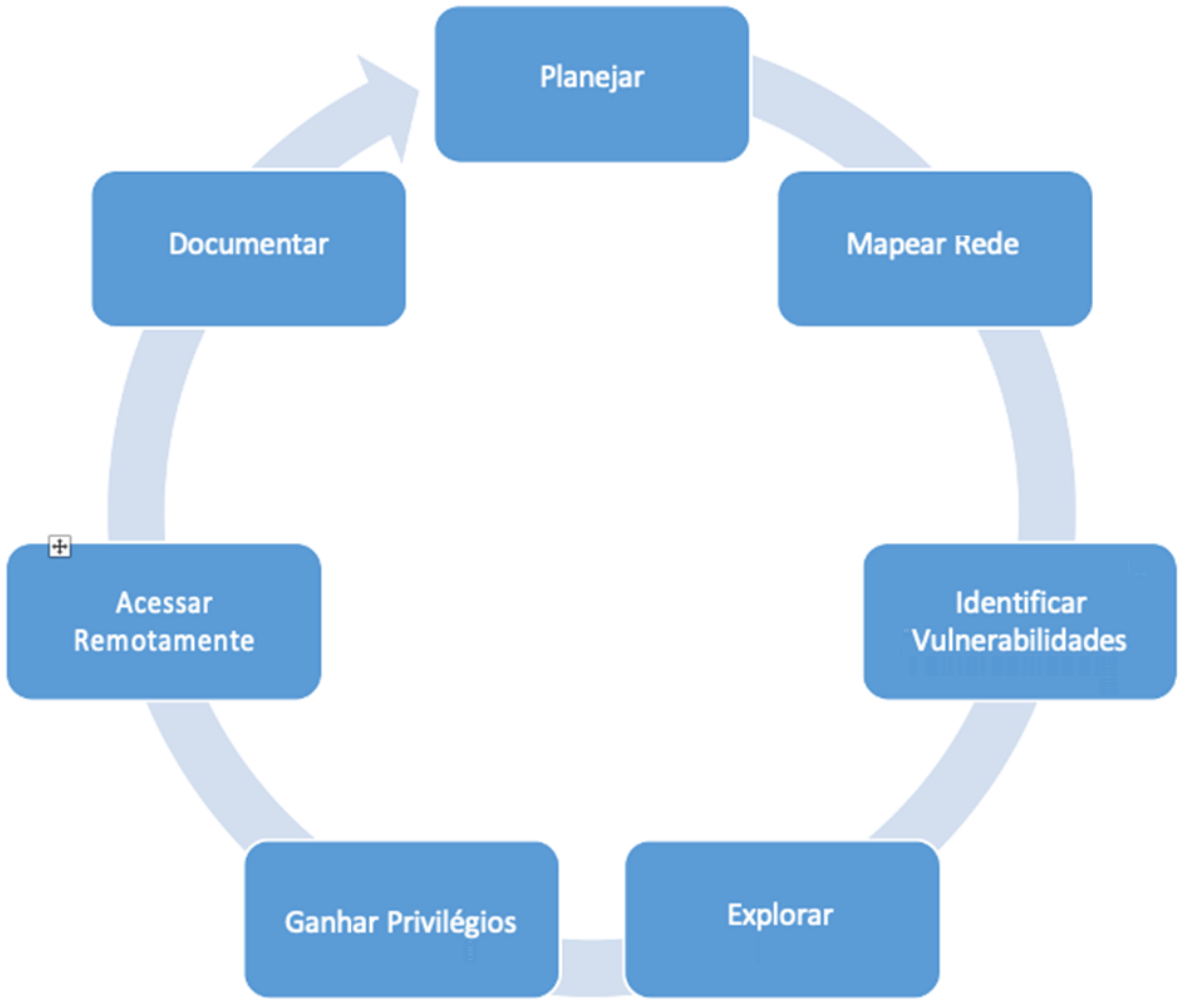
24/01/2024

1. Objetivo

Este documento visa alertar as vulnerabilidades encontradas e testar a segurança da infraestrutura no ambiente externo da **Verifact**, identificadas durante as atividades de mapeamento e teste de intrusão realizadas no período de **15/11/2023** a **15/12/2023**.

2. Metodologia

Pelas características do serviço, o projeto será divido em 7 fases, distribuídas conforme o ciclo de execução de testes, descrito na metodologia abaixo:



3. Escopo do Projeto

O projeto de PenTest realizado pela **STWBRASIL** foi desenvolvido seguindo a Metodologia de trabalho hibrida, Black Box e Graybox, isto é, com e sem o conhecimento do ambiente de rede interna e com visão apenas exterior e com uma credencial válida de usuário, visando simular um cenário real de ameaça existente proveniente da Internet.

Foram analisados diversos vetores de ataques a fim de conseguir informações e identificação de vulnerabilidades que possibilitem um atacante explorar o ambiente da empresa ou causar indisponibilidades de serviços, através do seguinte acesso:

Links:

- app.verifact.com.br
- verifact.com.br

4. Indicadores do teste realizado

As vulnerabilidades encontradas durante os testes realizados, tiveram seus riscos classificados da seguinte forma:

Classificação do Risco	Quantidade de Vulnerabilidades
Crítica	0
Alta	0
Média	0
Baixa	0
Total	**0**

NENHUMA VULNERABILIDADE ENCONTRADA.

5. Conclusão

Durante as análises realizadas no produto **Verifact**, não foi identificada nenhuma vulnerabilidade que permita acessar e/ou manipular provas coletadas e armazenadas na plataforma.

Apesar de inúmeras tentativas, não foi possível realizar qualquer manipulação dos dados coletados durante a sessão de uso do produto, ou qualquer outra manipulação que permita comprometer o propósito da ferramenta em coletar informações voláteis na internet.

Nenhuma informação referente a usuários do sistema, bem como documentos armazenados na solução foram encontradas em vazamento de dados, seja em fóruns indexados na internet ou em lista de vazamentos comercializadas na deep web / dark web.

Não foi detectada nenhuma falha de segurança ou falha de programação no produto avaliado, que permita extração / vazamento de dados, sejam eles pessoais ou de qualquer outra natureza, garantindo assim a aderência da solução **Verifact** em relação a lei geral de proteção de dados (LGPD).

Não foi possível realizar a alteração de nenhum relatório de aquisição forense gerado pela plataforma (arquivo formato *PDF*), sem que a assinatura digital fosse corrompida, garantindo assim, a lisura dos relatórios gerados pela plataforma **Verifact** de acordo com as normas definidas pelo ICP-BRASIL, no que se refere a assinatura eletrônica qualificada de documentos (assinatura com uso de certificado digital), de acordo com a Lei Federal 14.063/2020.

Afirmamos que todas as informações contidas neste relatório são verdadeiras, tendo suas evidencias técnicas coletadas e armazenadas, devidamente auditadas por estes responsáveis que firmam o presente documento.

São Paulo, 24 de janeiro de 2024.

Leandro Morales Baier Stefano
CEH – ISFS – CHFI - EHF

Marcelo Nagy
EHF – ISFS – ICSI - CISCO

6. Qualificações dos Analistas Responsáveis

Os especialistas descritos a seguir são os responsáveis pelos trabalhos de análise e relatórios técnicos emitido pela divisão de **Cibersegurança** da **STWBrasil**:

Leandro Morales

- Sócio-Diretor da **STWBrasil**;
- Perito judicial em Sistemas de Informação/Informática;
- Consultor em Tecnologia e Segurança de Dados;
- Atua na área de segurança da informação para a Polícia Judiciária;
- Ministra palestras e treinamentos na área de Segurança da Informação;
- Associado APEJESP/ OPERB/ APCF;
- Membro do HTCIA;
- Membro da SBCF;
- Membro da Associação Portuguesa de Ciências Forenses - APCF;
- Certificado CEH / CHFI / CCNA/ CCNP/ LPI I e II / RHCT / RHCE / ISO 27001 / Ethical Hacking Exin;
- Certificado Instrutor Cellebrite – CCMF / CCO / CCPA / CASA;
- Certificado ISO e DPO GDPR;

Marcelo Nagy

- Sócio-Diretor da **STWBrasil**;
- Chefe de Segurança da Informação na QualiSign S.A;
- Perito Judicial na área Computacional;
- Curador na **Universidade Presbiteriana Mackenzie**;
- Instrutor oficial da **Academia de Forense Digital**;
- Formação acadêmica em Processamento de dados, Ciências da Computação e Gestão em Tecnologia da Informação.
- Pós-graduado em **Cibersegurança**.
- Pós-graduado em **Investigação de Crimes Digitais**.
- Pós-graduado em **Perícia Judicial e Extrajudicial**.
- Certificado pelo EXIN em ISO 27.001, Ethical Hacking, CISCO, dentre outras.