**RELATÓRIO TÉCNICO**

Data:

**Janeiro de 2019**

Necessidade:

**Relatório técnico – Resultado do Penetration test**

**TERMO DE CONFIDENCIALIDADE**

A **<EMPRESA>** se compromete a manter sigilo sobre qualquer informação recebida pelo **CLIENTE**, bem como quaisquer informações obtidas durante a prestação de serviços. O conteúdo deste documento é sigiloso, assim como os resultados obtidos após a execução dos trabalhos e não deve ser copiado sem prévia autorização da **<EMPRESA>**, sendo de uso exclusivo do **CLIENTE**, devendo ser utilizada apenas internamente, por razões de segurança das informações ao longo de todo o processo.

**LAUDO TÉCNICO SOBRE AS VULNERABILIDADES**

Atualmente, a infraestrutura de rede do **<cliente>** possui um ambiente heterogêneo de diferentes tipos de equipamentos, incluindo Roteadores e Switches de diferentes fabricantes, assim como servidores que operam tanto com os sistemas Linux e Windows.

Alguns pontos iniciais identificados durante o Pentest:

* Os servidores SRV-LINUX1 e SRV-LINUX2 possuem acesso telnet habilitado para todos. Sugestão: desabilitar e permitir apenas o SSH.
* Os servidores SRV-Windows1 e SRV-Windows2 estão com o SMBv1 habilitado, o que permite ataques de Ransonwares como o WannaCry. Sugestão: desabilitar.  
    
  **<Use imagens dos testes aqui>**

Relação dos problemas encontrados de forma resumida:

|  |  |  |
| --- | --- | --- |
| Servidor/site | Recurso | Vulnerabilidade identificada |
| SRV-WEB1 | /livro-de-visitas.php | Vulnerável a ataque XSS |
| SRV-FTP1 | FTP sem restrição de logins | Vulnerável a força-bruta |
| etc | etc | etc |
|  |  |  |

**RECOMENDAÇÕES DE CURTO e LONGO PRAZO :**

Portanto, tendo como base as informações coletadas, recomenda-se as seguintes medidas de curto e médio prazo:

* Atualização dos Sistemas Linux para uma versão mais recente do Kernel (curto prazo).
* Configuração de cabeçalhos anti-XSS nos servidores web (curto prazo)
* Implementação de um plano de segurança da informação (longo prazo)
* Etc...