Relatório de *Pentest*

Rede Tonato™

Diego M. M. Malta

14 de Fevereiro de 2020
GRIS-UFRJ

INTRODUÇÃO

Este relatório possui informações de vulnerabilidade da empresa *Rede Tonato*™, obtidos através de testes de invasão(*Pentest* e Engenharia Social) realizados por Diego Malta, aluno de Ciência da Computação na UFRJ em treinamento para o GRIS - Grupo de Respostas à Incidentes de Segurança. Todos os métodos de invasão foram consentidos pelos devidos representantes da *Rede Tonato*™, permitindo que estes fossem realizados para tentativa de melhoria da segurança de informação da empresa.

O tipo de teste realizado foi **Grey Box**, em que somente há conhecimento prévio de parte do sistema da empresa. Além disto, os funcionários da empresa não tinham conhecimento dos testes.

Vulnerabilidades Encontradas

1. A Rede *Tonato*™ é vulnerável à SQL Injection. ' or 1=1; drop table notes; --
   é aceito no campo de usuário e senhas, conseguindo facilmente permitir acesso ao usuário administrador do site.

2. Ausência de tempo de espera para tentar logar após sucessivas falhas. Isso causa a aplicação suscetível a ataques de *bruteforce* de usuários maliciosos, tornando mais fácil conseguir fazer ataques com lista de palavras ou de senhas. Usando a lista de 10 milhões de senhas comuns disponível no link abaixo, foi possível acessar a conta de alguns usuários existentes no sistema: https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt?fbclid=IwAR22zWaWFazDYoOkNy2WWRLo4c3_xRsK0Tp93vQPOJ6b_VPBVDxm4rpPts0

3. Facilidade de entrar na empresa como suposto conhecido. Acessando redes sociais de empregados da ***Rede Tonato*™**, foi possível coletar dados de pessoas que se conheciam mais dentro do local e de como era. Isso torna possível falsamente comprovar que é uma pessoal familiar com o conhecimento físico da empresa ou de seu corpo de funcionários. Isso garante acesso facilitado para poder chegar na sala de transmissão e me permitir instalar malwares na rede.

Recomendações

1. É necessário na página de login, usar SQL dinâmico, como na linha de código abaixo. Ele espera retornar de uma vez com os detalhes de usuário da Tabela de Usuários do banco de dados, como resultado igual ao que foi colocado nas linhas de Usuário e senha inseridos.
   SELECT * FROM Users WHERE User_Name = '" & strUserName & "' AND Password = '" & strPassword & "';"

2. Colocar um tempo de espera para quando muitas requisições de acesso são negadas por senhas ou usuários errado.

3. Avisar aos funcionários para tomarem cuidado com o quê é compartilhado nas redes sociais, e evitar que qualquer um possa entrar sem devidas permissões comprovadas.

DADOS

Vulnerabilidades	Nível de Risco
SQL Injection	Alto
Ausência de Time-out para sucessivas tentativas falhas de login	Médio
Facilidade de acesso físico ao local da empresa sem devida permissão	Médio

CONCLUSÃO

A empresa ***Rede Tonato***™ possui falhas simples de segurança, porém poucas. É necessário que estas sejam resolvidas logo, pois podem acarretar em prejuízo para a empresa caso ocorra danos ou vazamento de dados de usuários ou até mesmo danos diretamente à empresa. Caso boas práticas de segurança sejam aplicadas, será possível mitigar tais problemas e tornar o serviço da ***Rede Tonato***™ mais seguro e confiável.