Processo Seletivo GRIS/2020 - Relatório do teste de invasão (*pentest)* ao sistema de banco de dados da instituição de Ensino Maria Chagas

Empresa requerente: Centro Educacional Maria Chagas

Pentester: Leonardo de A.S. de Andrade

Período: 02/2020 a 03/2020

Modelo: Gray box

Ambiente: Interno

Confidencialidade deste documento

Este documento contém informações sigilosas e privilegiadas, sua confidencialidade está protegia por lei. Tanto o contratante quanto o *pentester* estão assegurados por um contrato escrito e reconhecido oficialmente, o qual permitiu que o *pentester* realizasse os testes de invasão pelo período de tempo predeterminado pelo contratante. O serviço prestado pelo contratado será remunerado, e este fornece o relatório do *pentest* realizado apenas para o contratante, sendo proibido qualquer tipo de divulgação deste documento.

As informações aqui presentes são de responsabilidade do contratante, sendo vetadas qualquer ação tomada com base nelas por parte terceiros, incluindo o *pentester* (sujeito à multa e pena de prisão de acordo com o Art 154-A do Código Penal – Decreto de Lei 2848/40).

Sumário

1. Resumo Executivo

Este relatório contém toda metodologia e ferramentas utilizadas no teste de invasão. Além disso aborda as vulnerabilidades encontradas pelo *pentester*, junto com seus impactos e dicas de prevenção e defesa contra possíveis invasores mal intencionados. Os testes foram realizados por um profissional capacitado e certificado no âmbito de segurança da informação. O objetivo do procedimento foi avaliar a segurabilidade do banco de dados da empresa "Centro Educacional Maria Chagas", além de verificar a conscientização sobre ataques e golpes virtuais por parte dos funcionários.

Durante o período de 02/2020 a 03/2020, o *pentester* realizou acessos ao banco de dados para avaliar a segurança de infraestrutura da aplicação e obteve informações confidenciais de estudantes matriculados e de seus respectivos responsáveis. Como se trata de uma empresa com diversas filiais no estado, o contratante escolheu a unidade de Duque de Caxias para ser avaliada. Com isso, o *pentester* procurou interceptar o tráfego de informações entre a filial e a sede (Barra da Tijuca). Conseguindo invadir o banco de dados da filial e obter as credenciais do diretor local, o *pentester* fez requisições de acesso ao sistema da sede em nome deste diretor, e com sucesso pode navegar entre os dados dos clientes tanto da sede quanto do restante das filiais. Além disso, pode coletar as informações de matrícula e mensalidade, sendo possível alterar esse tipo de informação, falsificando confirmações de pagamento e desligar clientes da empresa.

Inicialmente o Centro Educacional Maria Chagas forneceu o endereço de IP da filial de Duque de Caxias, as informações e aplicação do sistema de banco de dados utilizado, e-mail do diretor e da secretária-chefe da filial e o *site* da instituição conforme previsto pelo acordo. O banco de dados foi elaborado pela equipe de TI da própria empresa e não está aberta ao público, sendo acessada apenas por funcionários autorizados da empresa. A partir do que foi fornecido, o *pentester* identificou vulnerabilidades que poderiam causar consequências desastrosas tanto para empresa como para seus clientes, conforme foi supracitado.

O profissional contratado para realização dos testes recomenda fortemente a análise detalhada deste documento e a adoção das medidas preventivas recomendadas, fortalecendo a segurança das informações da empresa. Vale ressaltar que o procedimento avalia o estado de segurança apenas no período predeterminado, e que é essencial revisar periodicamente o sistema adotado e renovar as medidas de proteção.

2. Escopo

Todas as estratégias e métodos utilizados neste *Pentesting* foram previamente discutidos e debatidos em reuniões entre os diretores executivos do Centro Educacional Maria Chagas e o profissional contratado. Tudo para garantir que os interesses de ambas as partes fossem bem planejados e atendidos.

O Centro Educacional Maria Chagas se submeteu ao *Pentesting* com os seguintes objetivos:

- Testar a eficiência dos mecanismos de defesa da sua aplicação de bancos de dados;
- Verificar a segurabilidade das informações confidenciais dos clientes e da própria empresa;
- Analisar a segurança do tráfego de informações entre as filiais e a sede da empresa;
- Verificar o nível de conhecimento e conscientização dos funcionários a respeito de golpes, ataques virtuais, ou seja, crimes cibernéticos;
- Compreender as falhas e adotar as medidas de segurança necessárias, como adotar novos mecanismos de defesa e criar um departamento específico de TI direcionado para a segurança da informação.

O p*entester* recebeu autorização para analisar funcionários, coletar informações, praticar engenharia social e realizar ataques a fim de conseguir acesso a sistemas e informações confidenciais. As únicas exceções definidas foram a não-divulgação dos dados obtidos e das vulnerabilidades encontradas.

O estilo de teste executado foi o *Gray-box*, no qual o profissional que realizou os testes teve acesso a apenas algumas informações da empresa e do sistema, sendo ele responsável por adquirir os demais dados. Esse tipo de teste não foi anunciado aos funcionários.

2.1 Identificação

Inicialmente o *pentester* colocou em prática o reconhecimento do ambiente interno da empresa. Passou-se por uma responsável de um aluno que iria fazer uma suposta matrícula. Assim ele pode tirar dúvidas sobre questões de documentação que a escola guarda dos alunos e responsáveis, tomou conhecimento do horário de funcionamento e carga horária, observou credenciais e vestimenta e modo de conversa dentro do ambiente de trabalho. Enquanto fazia o cadastro de seu suposto filho, pediu para a secretária mostrar o monitor para ele, então ele pode ver o sistema e versão do banco de dados, como ele funciona e o login (sem a senha) da secretária. Após isso, foi ao tesoureiro para efetuar um pagamento. Dizendo que era profissional de segurança da informação, com certa facilidade conseguiu se aproximar do funcionário e levar o assunto para a área financeira da escola, perguntou para onde o dinheiro ia, como o sistema funcionava, se deveria haver confirmação tanto da filial quanto da sede e quem tinha acesso a esse sistema da tesouraria. Além disso, pediu o e-mail do tesoureiro para poder tirar supostas dúvidas de pagamento de mensalidade que pudessem surgir no futuro.

Em resumo, foram coletadas informações relevantes sobre o dia a dia dos funcionários, seus conhecimentos e cuidados em expor informações sensíveis da empresa. O *pentester* adquiriu o conhecimento de que apenas o tesoureiro e a diretora da escola tinham acesso ao sistema financeiro. Ademais, o *pentester* pediu informações sobre a equipe de TI, se eles faziam manutenção constante, atualização do sistema e dos dados, verificação de malwares, etc. Como ele estava se passando por um cliente, os funcionários se viram na obrigação de garantir que todo o processo de matrícula fosse concluído sem transtorno, então forneceram essas informações ao suposto responsável.

Vale ressaltar que foi observado que a rede Wi-Fi disponível aos clientes era a mesma que a usada pelos funcionários ali para acessar o banco de dados e o sistema financeiro. A senha estava disponível a todos os responsáveis que requisitassem o acesso à rede.

A partir disso, o profissional contratado iniciou um "*stalk"* nas redes sociais da secretária, do tesoureiro e da diretora da escola para poder coletar informações pessoais e pensar o que poderia aplicar ao *pentest*. Pelo Instagram pode destacar hábitos e hobbys dos três. Notou que o tesoureiro era um fã assíduo de jogos eletrônicos, a secretária tinha gosto por viagens e que um dos *hobbys* diretora era ir ao teatro.

3. Metodologia

A metodologia utilizada neste procedimento consiste em quatro etapas:

- **Identificação (coleta de informações);**
- **Reconhecimento de vulnerabilidades;**
- **Exploração de vulnerabilidades;**
- **Pós-exploração.**

3.1 Ferramentas

BurpProxy - Inspecionar e modificar o tráfego entre o navegador e o aplicativo destino.

WireShark - Análise de pacotes transmitidos na rede. Possibilita um reconhecimento minucioso da troca de dados entre o cliente e o host.

Kali Linux - Distribuição do GNU/Linux, contém diversas aplicações e ferramentas voltadas para segurança da informação.

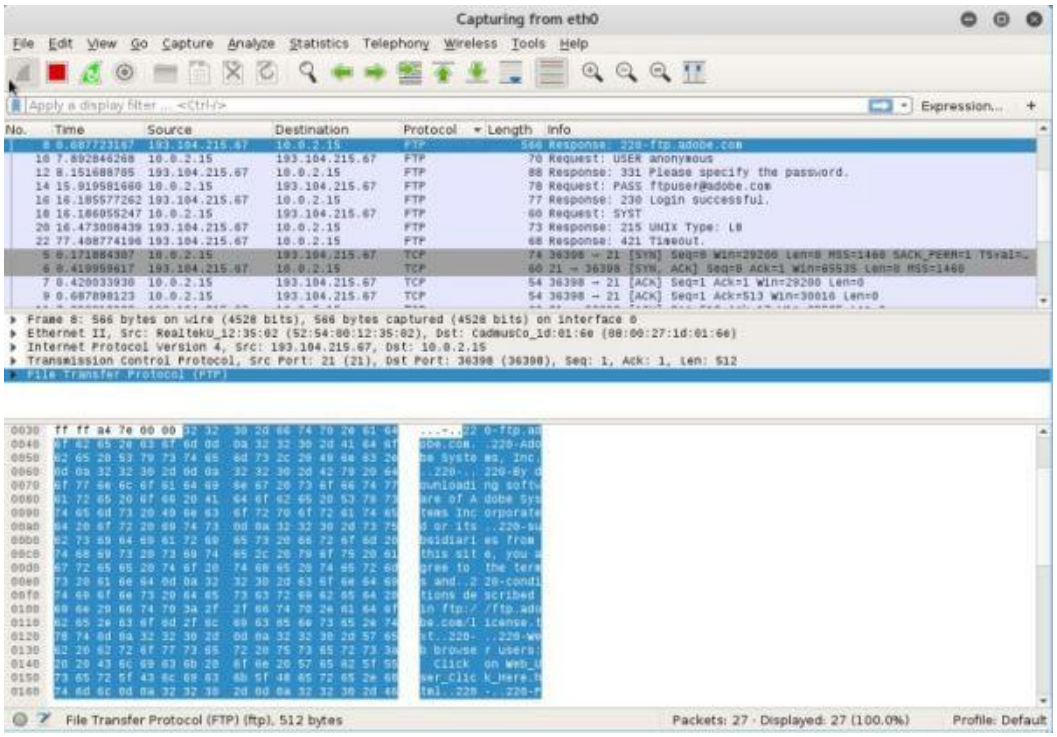
The Social-Engineer Toolkit (SET) - Uma das aplicações do Kali Linux, possibilita testes de penetração pensados a partir da engenharia social.

4. Relatório de exploração

A seguir o prosseguimento dos testes adotados, vulnerabilidades encontradas, consequências e recomendações.

4.1 *Man in The Middle (MITM)*

Com acesso à rede Wi-Fi da empresa, o *pentester* levou seu notebook e ficou na recepção após dizer que estava à espera do término do horário de aula para poder levar seu filho embora. Com a senha em mãos e sem incômodo de terceiros, o atacante teve toda a liberdade para interceptar o tráfego de dados entre o cliente (filial) e o servidor utilizando o Kali Linux e o WireShark. Com isso, não houve dificuldades na interceptação de informações (como confirmação de matrículas e pagamentos de mensalidade) enviadas da filial para a sede.



(imagem meramente ilustrativa)

Além disso, o *pentester* poderia ter interceptado o tráfego de dados dos demais usuários da rede, nesse caso os clientes que estavam na recepção. Ou seja, uma rede aparentemente segura estava colocando a exposição não somente informações do contratante, mas também daqueles que estavam conectados apenas por um curto período de tempo.

Recomendação

Recomendamos fortemente a utilização de redes Wi-Fi separadas na empresa. Uma destinada a uso interno do ambiente corporativo e outro destinado aos clientes para uso pessoal. Conseguinte o uso de VPN e de plugins HTTPS para a ocultação das atividades online também é uma ótima medida preventiva.

Referências

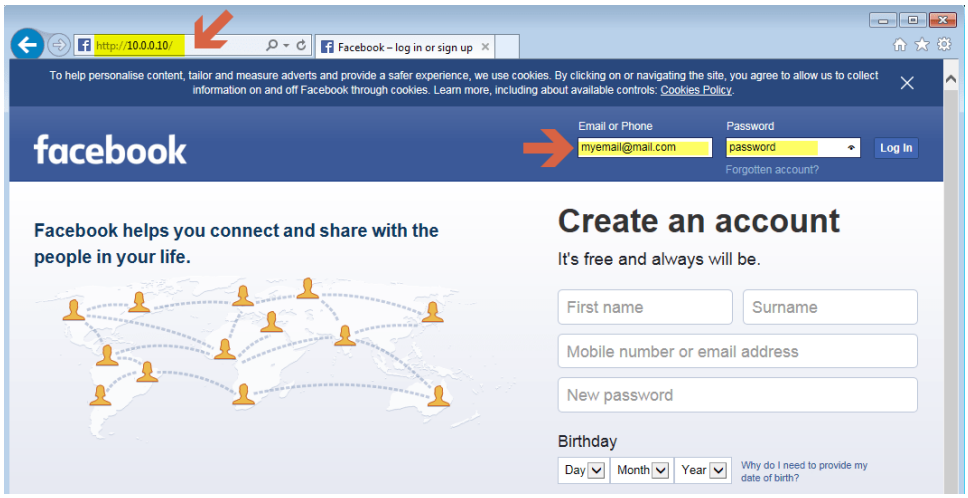
https://www.diegomacedo.com.br/introducao-ao-wireshark-deteccao-e-captura-de-trafego-em-redes/

https://www.avg.com/pt/signal/man-in-the-middle-attack

https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/

4.2 *Phishing*

A partir do SET, o *pentester* fez uso de engenharia social para tentar obter dados confidenciais da diretora, do tesoureiro e da secretária. Com o material coletado das redes sociais dos respectivos alvos, o atacante enviou um e-mail falso para eles, com supostas promoções nas áreas de interesse de cada um e para ter acesso ao cupom de desconto oferecido era necessário "curtir" a página do Facebook da empresa que oferecia o bônus. O link da página estava no texto da mensagem, e quando a vítima clicou, se deparou uma página falsa de login do Facebook gerada pelo SET e os dados ali inseridos seriam direcionados para o *penstester*.



(imagem meramente ilustrativa)

Com este teste, o profissional de segurança conseguiu coletar as senhas dos perfis do Facebook da secretária e da diretora, mas não a do tesoureiro. Com essas senhas em mãos o *pentester* verificou se elas eram as mesmas usadas pelas funcionárias para o ambiente profissional. A partir dessa tentativa, percebeu que a diretora usava o mesmo *password* tanto para rede social quanto para o e-mail de trabalho. Descobrindo isso, enviar mensagens falsas e até novas tentativas de *phishing* em nome da diretora seria algo totalmente possível a alguém mal intencionado.

Além deste teste, o atacante se passou também pela equipe de TI e enviou um e-mail aos funcionários requisitando as contas de acesso de cada um ao banco de dados para uma suposta manutenção de serviço. Foi possível obter login e senha da secretária, porém o tesoureiro e a diretora fizeram a verificação da veracidade do e-mail enviado.

Recomendação

Quanto ao *phishing*, recomenda-se que a empresa promova palestras sobre golpes cibernéticos aos seus funcionários a fim de que eles sejam conscientizados sobre os cuidados necessários ao receber ou acessar qualquer tipo link ou e-mail. Verificar a veracidade das mensagens e nunca clicar em links suspeitos e tendenciosos são ótimas medidas de prevenção.

Referências

https://cartilha.cert.br/golpes/

https://linuxhint.com/kali-linux-set/

5. Conclusão

A partir dos testes executados, foram identificadas diversas vulnerabilidades que poderiam comprometer informações sigilosas da empresa Centro Educacional Maria Chagas e de seus clientes, colocando em risco não somente a reputação e finanças do contratante, mas também dados de estudantes menores de idade e de seus respectivos responsáveis. Um invasor mal intencionado poderia trazer complicações desastrosas a partir da exploração das falhas encontradas. Todas estas podem ser consideradas de **alto risco**.

Portanto, atenta-se para as prevenções e cautelas recomendadas neste relatório. Essas vulnerabilidades podem ser facilmente atenuadas pela adoção de novas medidas de segurança.