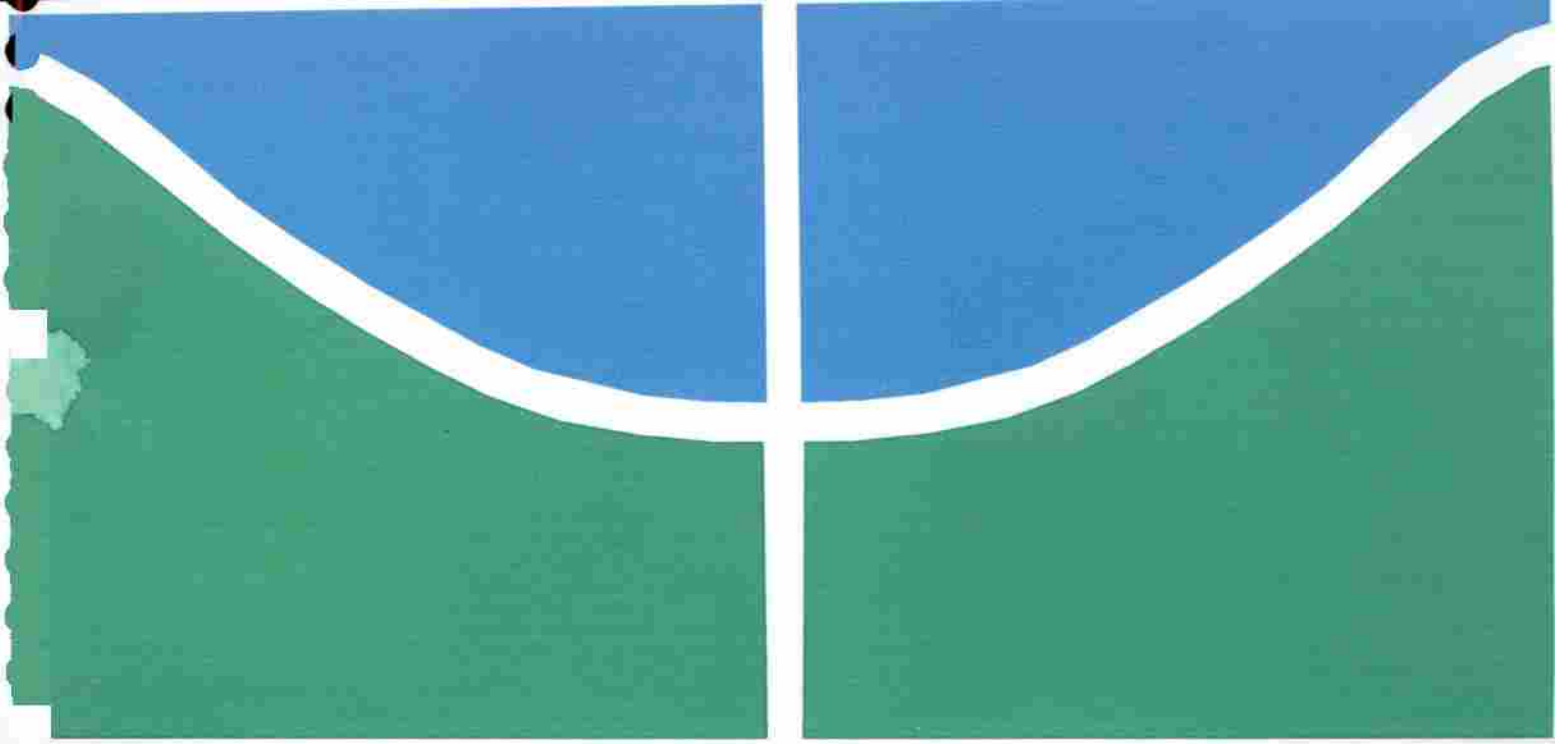


VULNERABILIDADES E IMPACTOS EM SISTEMAS ERP WEB

LUIS ALEXANDRE HADDAD MARQUES

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

VULNERABILIDADES E IMPACTOS EM SISTEMAS ERP WEB

LUIS ALEXANDRE HADDAD MARQUES

ORIENTADOR: Dr. RAFAEL TIMOTEO DE SOUSA JUNIOR

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: UnBLabRedes.MFE.XXX / 2017

BRASÍLIA, DF: AGOSTO / 2017.

Inspetor Slide 35
Lo orientare Documentos

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

VULNERABILIDADES E IMPACTOS EM SISTEMAS ERP WEB

LUIS ALEXANDRE HADDAD MARQUES

MONOGRAFIA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

APROVADO POR:

_____
RAFAEL TIMOTEO DE SOUSA JUNIOR
DOUTOR, UNB/ENE (ORIENTADOR)

_____
XXXXXXXXXXXXXXXXXXXX
MEMBRO 1 (EXAMINADOR INTERNO)

_____
XXXXXXXXXXXXXXXXXXXX
MEMBRO 2 (EXAMINADOR EXTERNO)

BRASÍLIA, DF, XX DE AGOSTO DE 2017.

FICHA CATALOGRÁFICA

Marques, Luis A. Haddad. Vulnerabilidades e Impactos em Sistemas ERP WEB [Distrito Federal], 2017. Monografia – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica	
1. Man-In-The-Middle	2. Interceptação de dados
3. ARP Poisoning	4. Tráfego de redes
5. Furto de dados	II. Título (série)
I. ENE/FT/UnB	

REFERÊNCIA BIBLIOGRÁFICA

Marques, Luis A. Haddad. (2017). Vulnerabilidades e Impactos em Sistemas ERP WEB. Monografia, Publicação UnBLabRedes.MFE.XXX/2017, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 70p.

CESSÃO DE DIREITOS

AUTOR: Luis Alexandre Haddad Marques

TITULO DA TESE: Vulnerabilidades e Impactos em Sistemas ERP WEB

GRAU / ANO: ESPECIALISTA / 2017

Luis Alexandre Haddad Marques

QMSW 5 Lote 02, Bloco C Apartamento 235

Setor Sudoeste

CEP: 70.680-500 - Brasília – DF

Tel. 55 – 61 – 99340-5577 / luis_haddad@hotmail.com

DETICATÓRIA

Aos meus pais dedico todos os meus bons atos, toda a minha vida e a conclusão de mais essa etapa, pois é a força e o amor que eles emanam que me mantém forte, seguro e em paz.

AGRADECIMENTOS

A minha grande irmã Lana cuja amizade é imensurável, sem sua ajuda e apoio a conclusão de mais essa etapa em minha vida não seria possível.

A minha querida tia Márcia, uma segunda mãe que sempre se preocupou comigo, agradeço a vocês duas que me acolheram quando precisei e me deram força pra continuar.

"1.Meu filho, se entrares para o serviço de Deus, permanece firme na justiça e no temor, e prepara a tua alma para a provação;
2.humilha teu coração, espera com paciência, dá ouvidos e acolhe as palavras de sabedoria; não te perturbes no tempo da infelicidade,
3.sofre as demoras de Deus; dedica-te a Deus, espera com paciência, a fim de que no derradeiro momento tua vida se enriqueça.
4.Aceita tudo o que te acontecer. Na dor, permanece firme; na humilhação, tem paciência.
5.Pois é pelo fogo que se experimentam o ouro e a prata, e os homens agradáveis a Deus, pelo cadinho da humilhação.
6.Põe tua confiança em Deus e ele te salvará; orienta bem o teu caminho e espera nele. Conserva o temor dele até na velhice."

(BÍBLIA, Eclesiástico 2, 1-6)

RESUMO

O mundo contemporâneo tem uma realidade de velocidade de trocas de informações na qual não é mais possível retornarmos à situação analógica preservando os serviços existentes em diversos segmentos.

A dependência da tecnologia para a vida moderna é notória e crescente, fazendo com que se agregue a ela cada vez mais valor, despertando o interesse de pessoas mal-intencionadas, pois a medida que a tecnologia se inova atuando como um facilitador, os criminosos também se reinventam adaptando-se a elas com muita rapidez.

Este trabalho aborda a questão de segurança em sistemas de gestão WEB, posto que o aumento da lucratividade de um negócio não ocorre somente na realização de seu objetivo final, isto é, a venda. Mas também na informação bem gerida e utilizada, sob seus cuidados.

Fica evidente que a gestão de informações em uma corporação, não apresenta eficiência necessária quando realizada manualmente. Neste sentido, os sistemas são essenciais não só para atenderem a legislação vigente como na manipulação e apresentação das mesmas a seus administradores.

Estes sistemas reúnem a história da empresa que por meio deles gerenciam suas operações, sendo essencial a garantia da segurança desses dados. Este trabalho aborda a cerca da segurança de um sistema de gestão operado em nuvem, uma tendência vendida ao público alvo devido à mobilidade de acesso, bem como avalia os impactos negativos concernentes as vulnerabilidades encontradas pelos testes realizados no sistema ERP case deste trabalho, abordando as possíveis consequências diretas e indiretas de uma invasão aos consumidores do software e corporação proprietária do sistema de gestão WEB.

Palavras-chave: Man-In-The-Middle, interceptação de dados, ARP Poisoning, tráfego de rede, furto de dados.

ABSTRACT

Considering nowadays reality, analog computing services are no longer viable to attend the needs of society in particular due to the information exchange speed of many different sectors and industries.

We cannot deny that modern life heavily relies on technology and it is a clear increasing tendency. We can also note that the demand for it has been adding value to technology as well as calling for the criminal's attention who are constantly trying to fraud the systems.

This paper intends to question and to prove the viability of ERP inasmuch as profitability and process optimization for the companies cannot be measured by sales numbers itself but should also be considered from a spectrum which includes information care and safety.

To sum it up we aim to show on this research that the efficiency companies strive to guarantee on electronically handling information cannot be offered on the old fashion ways, such as analog or manual not automatic systems. Moreover, we understand that ERPs are essential to attend theses needs, to allow better access to managements as to abide the law related to the subject.

As per previously said ERPs incorporate all the company's history and records, through which, they can manage its processes imperatives the daily operations and to the data's safety. ERPs based on cloud computing will be the core of this paper. They are currently very trendy due to its portability. It has also assessed the vulnerabilities found by data collected on the ERP case enclosed, which has evaluated the direct and indirect impact of final software consumers and for the EPR developer company being invaded or present a failure.

Keywords: Man-In-The-Middle, data interception, ARP Poisoning, network traffic, data theft.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

ARP	Address Resolution Protocol (Protocolo de Resolução de Endereço)
BM&F	Bolsa de Mercadorias de Futuros
CNAB	Centro Nacional de Automação Bancária
CRM	Customer Relationship Management (Gestão de Relacionamento com Cliente)
DDOS	Distributed Denial of Service (Negação de Serviço Distribuída)
DOC	Documento de Ordem de Crédito
ERP	Enterprise Resource Planning (Planejamento de Recursos da Empresa)
FABRABAN	Federação Brasileira de Bancos
HTTP	HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto)
HTTPS	HyperText Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro)
LAN	Local Area Netword (Área de Rede Local)
MITM	Man-In-The-Middle (Homem do Meio)
NFC-e	Nota Fiscal ao Consumidor Eletrônica
POS	Point of Sale (Ponto de Venda)
S.O	Sistema Operacional
TCP	Transmission Control Protocol (Protocolo Controle de Transmissão)
TED	Transferência Eletrônica Disponível

SUMÁRIO

1 INTRODUÇÃO

Neste capitulo serão apresentados os objetivos deste trabalho, as justificativas da escolha do tema e as metodologias aplicadas em sua execução.

1.1 Apresentação

O mundo chegou a um estágio onde os processos do nosso cotidiano demandam uma velocidade na troca de informações inimagináveis alguns anos atrás, diversos atos, processos e rotinas de nossas vidas já não possuem mais viabilidade de serem efetuados se houvesse um retorno a era analógica de troca de informações, que caso catastroficamente ocorresse, tornaria o mais próximo do impossível a execução e controle, por exemplo, da infinidade de transações bancárias que ocorrem nos dias atuais, fazendo o uso de papéis, fichas e arquivos.

A interceptação de dados comunicados pela internet é algo que todos os usuários de serviços web estão suscetíveis, a quantidade e diversidade de serviços e informações presentes na rede são imensuráveis e estão em contínuo crescimento devido a facilidade e velocidade de acesso as ferramentas e informações em diversos segmentos públicos e privados.

A velocidade da troca de informações através dos meios tecnológicos existentes permite uma via cada vez mais larga dos dados trafegados, levando a sociedade a uma dependência desses meios, o que nos faz ter um julgamento da impossibilidade de realização de certas tarefas sem os meio propiciados pela evolução da tecnologia.

O furto de informações na era digital é mais comum que leigos no assunto possam imaginar, o desenvolvimento tecnológico cresce exponencialmente seja em benefício ou em malefício, se de um lado pesquisadores realizam seu trabalho com objetivos benéficos a sociedade, de outro temos os que fazem o uso de suas habilidades dando uma nova roupagem ao mundo do crime.

É gigantesca a parcela da sociedade que faz o uso de tecnologia para troca de informações, desde a troca de e-mails a transações bancárias realizadas de suas residências. A interceptação destes dados pode trazer prejuízos diretos de cunho moral ou financeiro de modo que estes também possam estar intimamente ligados.

O prejuízo financeiro de uma corporação cliente de um Software não seguro pode ser consequência de um furto direto de informações ou utilização de sua credibilidade para

fraudes a terceiros, e para a empresa desenvolvedora pela divulgação de suas fragilidades de segurança ao mercado, o que a levaria a uma queda credibilidade.

A preocupação com a segurança da informação ainda não atinge uma parcela aceitável da população que faz o uso de redes, isto decorre por desconhecimento da existência de ameaças, das ferramentas existentes para sua mitigação e de como realizar o uso destas entre outros aspectos relativos à educação sobre segurança da informação.

Os serviços WEB (Rede) estão muito presentes na esfera corporativa, onde é cada vez mais comum a utilização de softwares de gestão com camadas de banco de dados e aplicação armazenadas em nuvem, o que permite a mobilidade dos gestores no acompanhamento e fiscalização em tempo real de seus negócios de maneira dinâmica e de qualquer parte do mundo sem que dependam de servidores locais, transferindo a responsabilidade de armazenamento, backup, atualizações e diversas outras rotinas de manutenção de seus sistemas para empresas terceirizadas especializadas neste segmento.

É com foco neste nicho que este trabalho realiza uma abordagem a cerca da segurança na utilização de sistemas de gestão WEB.

1.2 Objetivos

Aqui serão apresentados os objetivos gerais e específicos deste trabalho.

1.2.1 Objetivo Geral

O objetivo deste trabalho é demonstrar que empresas de pequeno a grande porte podem estar suscetíveis a grandes prejuízos financeiros devido à falta de conhecimento em relação às vulnerabilidades dos softwares que utilizam ao não observar certos aspectos de segurança na hora da escolha de seu sistema de gestão. Esse fator acompanhado muitas vezes pelo foco dado as empresas de desenvolvimento nos resultados comerciais, produz uma linha frágil que divide o sucesso comercial dos negócios da queda de credibilidade com a divulgação de tais falhas de segurança, por consequência uma empresa sem credibilidade não expande como deveria e gostaria, podendo perder espaço no mercado.

A preocupação ainda é maior principalmente quando estas são corporações de capital aberto, cuja imagem ilibada de reputação, competência e faturamento são pontos essenciais.

Será abordada a vulnerabilidade de segurança na autenticação de um usuário em um grande sistema ERP Web e as conseqüências de um invasor mal intencionado ter acesso ao mesmo. Serão abordadas soluções de simples implantação de métodos de segurança a fim de mitigar os riscos de furtos de dados para acesso, desde divulgação de conhecimento aos clientes do software para seu uso seguro a utilização de meios existentes de autenticação segura.

1.2.2 Objetivos Específicos

Os seguintes passos foram seguidos para a realização deste trabalho:

a) Investigação e testes a cerca das vulnerabilidades para captação de senha de acesso ao sistema ERP WEB.

b) Análise das consequências diretas aos clientes do sistema WEB que forem alvo de interceptação de senhas devido à vulnerabilidade de acesso ao sistema.

c) Pesquisa a respeito do alcance da empresa case no cenário nacional e seu porte para análise do impacto de divulgação das vulnerabilidades encontradas.

d) Análise das consequências da divulgação das vulnerabilidades para empresas de sistemas com capital aberto.

e) Criticas e soluções existentes que poderiam ser aplicadas para mitigar os riscos levantados e evitar a perda de credibilidade da corporação case proprietária do sistema analisado e perdas de clientes do Software.

1.3 Justificativa

Este tema foi escolhido pela experiência adquirida ao trabalhar em empresas de softwares de grande porte voltadas para o varejo, bem como a utilização de seus produtos por grandes marcas e franquias presentes no país. Ao longo do trabalho desempenhado foi verificado que grandes redes com faturamentos gigantescos estavam suscetíveis a diversas vulnerabilidades, pois além de acessarem seus sistemas de diversos locais e computadores, estes acessos não possuíam a mínima garantia de segurança para a autenticação de seus

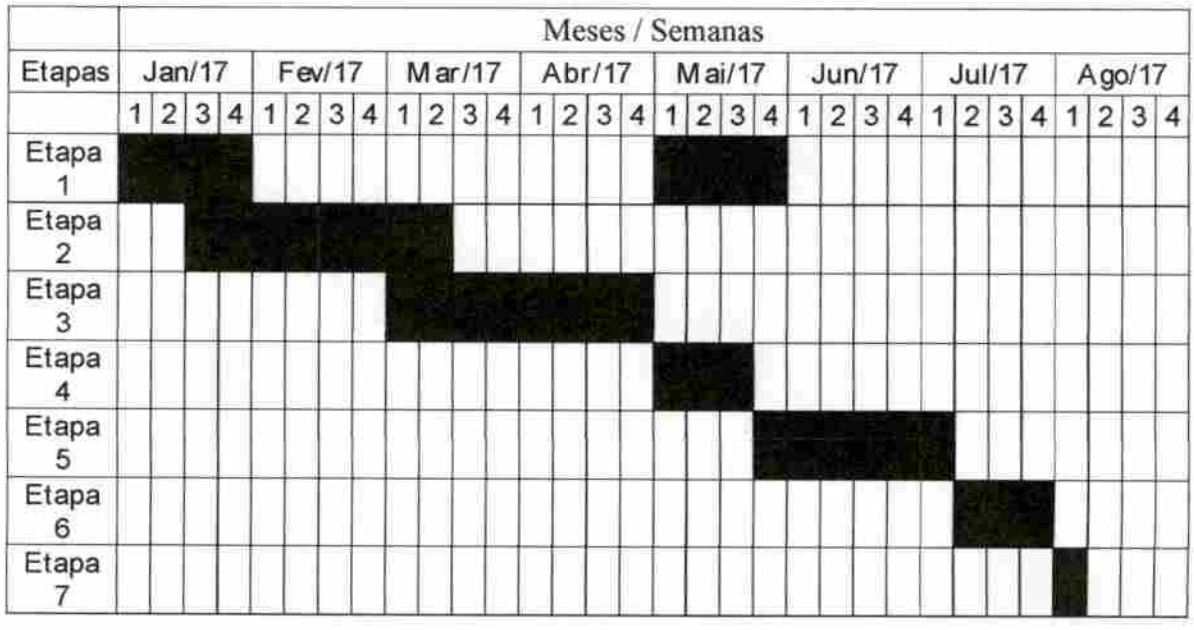
usuários em relação à captura de suas credenciais para acesso. A obtenção de dados para acesso ao sistema por pessoas mal intencionadas pode gerar um impacto muito maior que apenas a divulgação de dados sigilosos dos clientes finais, os prejuízos financeiros podem atingir altos patamares através de adulteração de ordens e controles de pagamentos além do impacto a imagem da corporação detentora do sistema analisado que pode ser significante, impactando diretamente seu valor por se tratar de uma empresa de capital aberto.

1.4 Metodologia

O trabalho foi realizado utilizando os método de pesquisa bibliográfica, do método indutivo, através da reunião de dados e a realização prática de interceptação de dados e análise de fluxo de dados em rede.

A realização do ataque consistiu em computadores inseridos em uma rede local, no qual um assumiu o papel de invasor a fim de interceptar o tráfego de informações do outro, em outro teste a máquina que intercepta os dados foi utilizada para a captura de dados trafegados em rede para a posterior análise destes.

1.5 Cronograma Proposto



Etapa 1 – Pesquisa bibliográfica técnica

Busca de informações em materiais impressos e internet a respeito de vulnerabilidades em autenticação de sistemas WEB (rede).

Etapa 2 – Contextualização e conceitos

Explanação a respeito dos conhecimentos essenciais sobre interceptação de senhas e análise de tráfego de redes.

Etapa 3 – Pesquisa bibliográfica corporativa

Pesquisa sobre o impacto em grandes empresas de capital aberto com a divulgação de vulnerabilidades.

Etapa 4 – Testes práticos

Realização de testes para a captação de dados para acesso ao sistema ERP Web.

Etapa 5 – Pesquisa bibliográfica, métodos de proteção

Pesquisa de soluções existentes para a mitigação das vulnerabilidades levantadas.

Etapa 6 – Revisão do texto

Etapa reservada para a revisão, correção e formatação do texto para apresentação para envio de TCC final.

Etapa 7 – Apresentação a banca avaliadora

1.6 Cronograma Executado

	Meses / Semanas																													
Etapas	Jan/17				Fev/17				Mar/17				Abr/17				Mai/17				Jun/17				Jul/17				Ago/17			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Etapa 1																																
Etapa 2																																
Etapa 3																																
Etapa 4																																
Etapa 5																																
Etapa 6																																
Etapa 7																																

2 CONTEXTUALIZAÇÃO

Serão abordados aqui dados pertinentes para a compreensão da abordagem do tema deste trabalho.

2.1 Sobre a empresa

Serão abordados aqui dados quanto à dimensão da empresa a qual um de seus softwares comercializados será alvo dos testes de interceptação de login e senha para acesso. A dimensão desta companhia nos dará uma noção das possíveis conseqüências com a queda de credibilidade se divulgadas as falhas de seguranças aqui apresentadas. A partir deste momento o nome do software será suprimido e o chamaremos de software X, bem como a empresa será referenciada como companhia XYZ.

Todos os dados relativos a seu cronograma de crescimento, quadro de funcionários, sedes e faturamento foram extraídos do site da própria companhia, e os dados de faturamento comprovados no balanço de ações da Bovespa.

2.1.1 Breve história

As atividades desta empresa iniciaram-se à 30 anos oferecendo softwares de gestão ERP e POS. Com sua especialidade voltada ao varejo ela atende diversos segmentos como: Postos de combustíveis e conveniências, concessionárias, alimentação, moda e acessórios, óticas, farmácias, hipermercados, eletro, casa e decoração, telefonia, cosméticos, varejo de serviços, livrarias, estética e saúde, lavanderias entre outros.

Ela ainda conta com um número superior a 3.000 funcionários distribuídos entre sua matriz na cidade de São Paulo (SP) e demais filiais próprias, localizadas no Rio de Janeiro (RJ), Belo Horizonte (MG), Recife (PE), Porto Alegre (RS), Joinville (SC), Bauru (SP), Cascavel (PR), Bebedouro (SP), Campinas (SP), Blumenau (SC), Uberlândia (MG), Florianópolis (SC) e Manaus (AM). A empresa ainda possui credenciadas franquias para comercialização e relacionamento com clientes em 15 estados brasileiros e atende hoje cerca de 44 mil clientes com suas soluções.

2.1.2 Cronologia

No ano 2000 inicia o programa de canais para a comercialização de seu software principal, este ainda não é o software X alvo dos testes realizados neste trabalho, em 2004 se constituiu como S.A. Quatro anos depois faz a aquisição de outra empresa do mesmo segmento e expande com mais uma filial em uma capital Brasileira.

No ano de 2009 a XYZ inicia oferta de Cloude Services (Serviço em Nuvem), base para armazenamento dos dados do software X e sua principal bandeira nas atividades de marketing para sua comercialização, prezando a mobilidade que os gestores de empresas teriam em realizar transações, consultas e acompanhar em tempo real o faturamento das companhias que o utilizassem, neste mesmo ano ela adquiri outras 3 empresas do segmento.

Em 2010 a XYZ adquire mais 2 empresas e expandiu com mais duas filiais, no mesmo ano teve declarada sua entrada no BNDESPar como sócio investidor, no ano seguinte, 2011, adquire 3 outras empresas sendo uma destas a desenvolvedora do software X, além de declarar sua entrada no Fundo Americano General Atlantic.

Entre os anos de 2012 a 2014 ela adquire mais 7 outras empresas além da abertura do capital no segmento novo mercado da BM&F Bovespa, no ano seguinte a empresa XYZ comemora 30 anos de atividade e realiza a aquisição de outras duas companhias e no ano de 2016 faz a aquisição de mais uma empresa no mesmo ramos de desenvolvimento e comercialização de softwares.

E mais recentemente adquiri por mais de16 milhões de dólares uma grande empresa de Software ERP Argentina se expandindo para a América Latina.

2.1.3 Faturamento

Os dados mais atuais divulgados referentes ao faturamento da empresa XYZ são do ano de 2016, no qual a empresa encerrou o último semestre com receita operacional bruta de R$ 150,6 milhões, este valor, segundo o site Investimentos e Notícias, seria 8,4% maior que o mesmo período do ano anterior. A companhia atingiu uma receita bruta neste mesmo ano no valor de R$ 569,2 milhões e receita líquida de R$ 495,8 milhões.

Demonstração do Resultado - Consolidado	01/01/2016 a 31/12/2016	01/01/2015 a 31/12/2015
Receita de Venda	485.799	449.183
Resultado Bruto	348.435	320.916
Resultado de Equivalência Patrimonial	0	0
Resultado Financeiro	24.723	11.605
Resultado Líquido das Operações Continuadas	88.501	63.816
Lucro (Prejuízo) do Período	88.501	63.816
Lucro (Prejuízo) do Período Atribuído à Controladora	88.501	63.816

Figura 1 - Captura de Tela – Demonstração do Resultado Consolidado (Fonte: http://www.bmfbovespa.com.br)

2.2 Vulnerabilidades em sistemas WEB

São 4 os grandes grupos de ameaças as quais sistemas distribuídos estão suscetíveis, são eles: Interrupção, interceptação, modificação e fabricação.

2.2.1 Interrupção

A interrupção se caracteriza quando dados ou serviços ficam indisponíveis, sendo por uma queda no serviço forçada ou destruição de dados. A negação do serviço pode ser ocasionada, por exemplo, por um ataque de DDOS (Distributed Denial of Service), mesmo sendo uma importante questão de segurança em sistemas WEB não é foco das vulnerabilidades pesquisadas neste trabalho.

2.2.2 Interceptação

A interceptação de dados ocorre quando alguém não autorizado adquire acesso a um sistema, tráfego de dados ou diretório de arquivos ao se estabelecer entre partes comunicantes. Temos como exemplo de interceptação de dados, o ataque conhecido como MITM – Man-In-The-Middle. Este tipo de ataque ocorre quando a parte atacante se estabelece entre duas entidades comunicantes, os dados são interceptados e podem ser copiados, modificados ou destruídos.

O MITM é uma das técnicas utilizadas na pesquisa de vulnerabilidade realizada neste trabalho pela facilidade com que pode ser utilizado para a captação de senhas em conjunto com técnica de engenharia social ou análise de trêfego de redes, este processo será detalhado em 3.1 e 3.2.

Como ilustrado na figura 2 o ataque MITM ocorre quando o atacante se estabelece entre duas entidades podendo "escutar" o fluxo de informações nos dois sentidos. Um ataque MITM realizado com sucesso garante que a entidade destino da mensagem a receba normalmente, assim as partes legais comunicantes não percebem que os dados transmitidos podem estar sendo copiados por uma parte não autorizada a obtê-los.

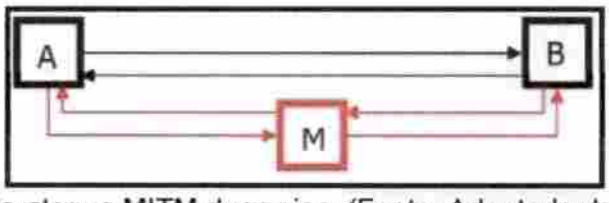


Figura 2 - Esquema de ataque MITM duas vias. (Fonte: Adaptado de CUNHA et al., 2005)

Em uma rede interna, escritório ou residência, um cenário mais real de como ocorre uma interceptação de dados por ser exemplificado conforme a figura 3 abaixo.

Tomando o computador B como alvo da interceptação da comunicação entre os computadores entre B e A ou entre B e o roteador, o invasor se estabelece entre as partes comunicantes, neste caso entre B e o roteador da rede.

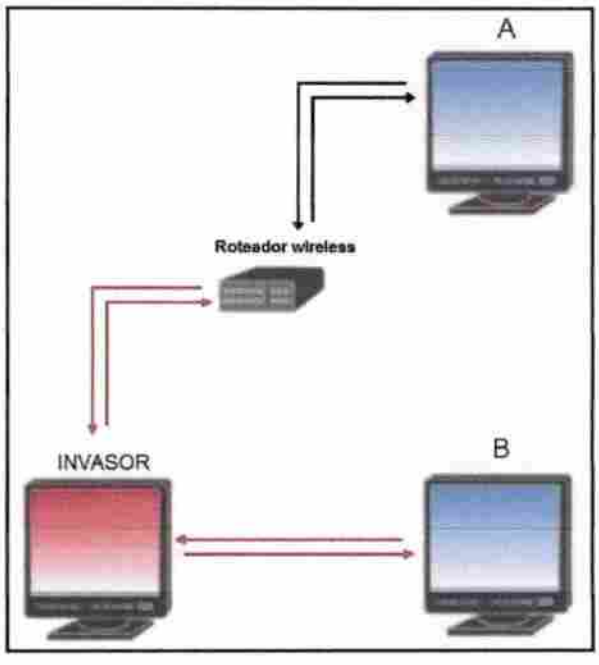


Figura 3 - Rede wireless com invasor (Fonte: Adaptado de CUNHA et al., 2005)

As informações que se originam da entidade B, requisições a serviços ou envios de dados, passam primeiro pelo invasor para depois serem encaminhados ao seu destino original, assim é possível que o invasor realize uma cópia das informações.

Outras topografias para a utilização deste tipo de ataque podem ser utilizadas, mas será aprofundada no capítulo 3 esta topologia de ataque, utilizando a técnica ARP Poisoning para o teste de vulnerabilidade do sistema ERP além na análise de tráfego de rede. O MITM se mostra simples de ser executado o tornado acessível a um leque maior de atacantes com objetivos ilícitos.

2.2.3 Modificação

A modificação é nada mais que o próprio nome descreve, ocorrerá quando dados ou sistemas são alterados por um invasor não autorizado. Um sistema pode ser alterado fazendo com que suas funções corretas sejam comprometidas a fim de o atacante que o fez obter vantagens sobre isso.

O ataque de modificação será exemplificado mais adiante e abordadas as conseqüências da modificação de dados por atacantes que garantem acesso a sistemas de gestão de uma empresa.

2.2.4 Fabricação

A fabricação é o ato da inclusão de informações, por agente não autorizado, que antes não existiam, por exemplo a inclusão de um login de acesso a um sistema, de uma permissão para alteração de determinada tabela de um banco de dados ou ainda a geração de faturas alteradas para envio. Este último será mais detalhado em 3.3 como uma das conseqüências a um sistema de gestão vulnerável e invadido.

3 INTERCEPTANDO DADOS DE ACESSO DO SISTEMA ERP WEB

O ataque de interceptação se caracteriza pela utilização de qualquer meio ilícito com a finalidade de captar dados de acesso e demais informações em transmissão entre duas partes comunicantes em rede por uma terceira parte intrusa, onde esta não deveria fazer parte do sistema comunicante por não ter acesso prévio autorizado.

Esse tipo de ataque é crime, como consta na Lei Nº Nº 12.737/2012 em seu Artigo 154-A.

> Lei 12.737/2012 no Art. 154-A invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL. LEI Nº 12.737, de 30 de novembro de 2012.).

A captura dos dados para acesso ao sistema referido será realizada de duas maneiras para demonstrar a vulnerabilidade de segurança na autenticação do sistema. Primeiro utilizando o ataque Man-In-The-Middle com a técnica Arp Poisoning em conjunto com uma técnica de engenharia social, e depois através do monitoramento do tráfego de rede com auxílio do MITM.

Dessa forma será possível demonstrar dois pontos distintos e vulneráveis do sistema, o que faz com que as empresas que o utilizam se tornem vulneráveis bem como os clientes varejo das corporações cujas gestões são administradas por este Software.

3.1 Utilizando Man-In-The-Middle – Arp Poisoning

O ataque Man-In-The-Middle com a técnica de Arp Poisoning é relativamente simples de ser executado, dessa maneira usuários mal intencionados podem utilizá-lo sem exigir muito conhecimento de redes, Linux e demais áreas de conhecimento ligadas a este assunto.

A interceptação, neste caso em um ambiente teste, será realizada entre uma máquina vítima e um roteador wirelles, desta maneira a entidade vítima terá na resolução de sua tabela ARP a associação do endereço IP do roteador, Gatway da rede, ao MAC Address da máquina invasora.

Assim quando a vitima fizer a requisição a URL ao sistema de gestão web ela será respondida pela entidade atacante que proverá com um clone do layout de autenticação do sistema, neste ponto que foi utilizada a técnica de engenharia social.

A união entre o MITM e a Engenharia Social permite que o invasor visualize os dados de acesso ao sistema em texto claro, sem criptografia, caso este sistema ou qualquer outro sistema WEB utilize deste recurso.

3.1.1 Ambiente teste

O ambiente utilizado para a realização dos testes de vulnerabilidade do sistema de gestão WEB consiste em uma rede wireless construida com um roteador D-link modelo DIR-615, SSID da rede "LA_HADDAD", configurada no canal 8 e encriptação WAP2-PSK AES.

Dois computadores foram utilizados, ambos de propriedade do autor deste trabalho, um notebook marca Asus modelo X45C o qual foi preparado com o Sistema Operacional Open Source Linux distribuição Kali Linux 4.0.0 baseada em Debian.

> O Kali Linux é um sistema operacional Linux baseado no Debian, que é desenvolvido pela pequena e consagrada equipe da Offensive Security. Ele contem mais de 300 ferramentas nativas para testes de invasão, penetração, força bruta, forense entre outras. Atualmente é um dos sistemas mais famosos no mundo na área de e segurança da informação. Muito utilizado por hackers, pentesters, analistas e auditores de segurança da informação. (FRAGA, Bruno, 2016)
>
> *Este texto foi retirado da URL* "https://tecnicasdeinvasao.com/linux/kali-linux/voce-sabe-o-que-e-o-kali-linux/"

Esta máquina foi preparada com o objetivo de ser o realizador do ataque Arp Poisoning com a utilização da técnica de engenharia social.

A segunda máquina utilizada foi um notebook Asus modelo K45A com sistema operacional Windows 10 original, este computador fará acesso a URL do sistema ERP alvo dos testes. A escolha do S.O. Windows na máquina vitima deu-se por este ser o mais comum utilizado no varejo Brasileiro.

3.1.2 Ferramentas utilizadas

O teste de interceptação foi realizado com a técnica ARP Poisoning, que consiste em um atacante de posicionar entre a vitima e o roteador da rede, o objetivo deste ataque é fazer com que a resolução da tabela ARP do alvo do ataque seja constituída atrelando ao IP do roteador da rede o MAC Address do computador que realiza o ataque, desta forma as requisições ao Gateway da rede serão enviadas ao atacante ao invés de serem enviadas ao roteador.

Isso ocorre pelo fato de um dispositivo que se conecta a uma rede possuir dois endereços, um endereço IP lógico e o MAC Address, endereço fisico gravado da interface de comunicação do dispositivo. A comunicação de dados em uma rede depende destes dois endereços, pois os pacotes são criados pela camada de enlace e divididos em frames pela camada de rede, os quais possuem cabeçalhos com os endereços de origem e destino e estes são os endereços fisicos, conforme mostra figura 4.

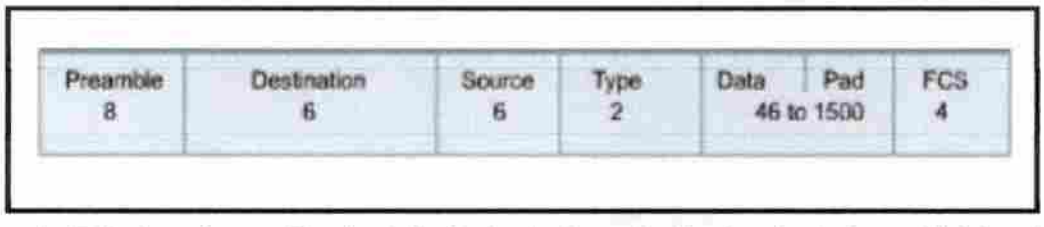


Figura 4 - Estrutura frame (Fonte: Adaptado da Associação dos Instrutores Net Academy, 2007)

O frame é criado através de um pacote IP, porém para seu envio é necessário o endereço fisico de seu destino o qual é obtido através do protocolo ARP. Quando uma entidade conectada a uma rede deseja enviar um pacote, esta faz uma requisição em broadcast, ou seja, envia a todas os dispositivos conectados a rede uma solicitação a fim de saber quem detém o endereço fisico que remete ao endereço IP ao qual deseja enviar o pacote, a entidade destino da mensagem responde com seu endereço fisico e assim se constitui a tabela ARP na máquina que deseja iniciar a comunicação. A figura 5 mostra um exemplo de resolução de uma tabela ARP.

```
Interface: 192.168.0.5 --- 0x8
  Endereço IP           Endereço físico       Tipo
  192.168.0.1           6c-72-20-75-a5-dd     dinâmico
  192.168.0.4           b0-72-bf-76-1f-b4     dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  224.0.0.253           01-00-5e-00-00-fd     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

Figura 5 – Tabela ARP (Fonte: Autor)

Para que essa interceptação ocorra através da fraude da resolução da tabela ARP na máquina vítima, foi utilizada a ferramenta Open Source Ettercap 0.8.2, criada por ORNAGHI, Alberto; VALLERI, Marco em Boston, MA, USA, porém apenas seu uso não bastou para a finalidade do ataque.

O Ettercap é um programa farejador, porém a autenticação segura em sistemas, sites e demais serviços WEB, geralmente, e sempre deveriam ser, são seguras, ou seja, criptografadas. Portanto para passar pelo problema da autenticação segura, junto à interceptação usou-se da engenharia social com o programa Social Engineer Toolkit – SET. Na realização dos testes será possivel verificar a facilidade com que os dados limpos para acesso ao sistema de gestão WEB poderão ser vistos com a utilização dessas duas ferramentas em conjunto.

O SET também é uma ferramenta open source, foi desenvolvido por KENNEDY, David da TrustedSec.com. A aplicação será usada no ataque para realizar uma cópia fiel do template de autenticação do sistema alvo, sendo assim a vítima fará a autenticação neste template clonado enganando a vítima, enviando ao atacante a senha "pura", sem criptografia envolvida.

3.1.3 Realização do teste

É pré-requisito que o atacante esteja inserido na mesma rede LAN (Local Area Network) que a vítima, o acesso a esta rede local nos remete a discussão de outras vulnerabilidades a cerca de ameaças internas, onde o atacante já possui acesso a rede local e

as ameaças externas, que envolvem diversos outros pontos a respeito de questões de segurança em redes, como a utilização de redes híbridas em corporações por exemplo.

Posto que o atacante já esteja inserido na mesma rede da vítima o próximo passo é a identificação do endereço lógico do alvo, um scan na rede local é facilmente realizado pelo S.O Linux. No ambiente teste montado o Gatway da rede é 102.168.0.1, o comando "nmap –sn 192.168.0.1-255" realiza uma busca no range de Ip´s de 192.168.0.1 a 192.168.0.255, lembrando que o comando foi dado dessa maneira considerando que o endereçamento da rede foi estruturado com classe C.

O "nmap" é software nativo das distribuições Linux desenvolvido para avaliar a segurança dos computadores em redes e descobrir serviços e servidores disponíveis em uma rede. O parâmetro "-sn" instrui ao programa nmap a não realizar um scan de portas filtrando apenas os hosts ativos, que neste caso é apenas o que nos interessa para identificar o endereço lógico do alvo do ataque.

O resultado do scan na rede teste é mostrado na figura 6, na qual o IP 192.168.0.5, em destaque, é o endereço lógico na máquina alvo no ambiente teste com seu respectivo endereço físico.

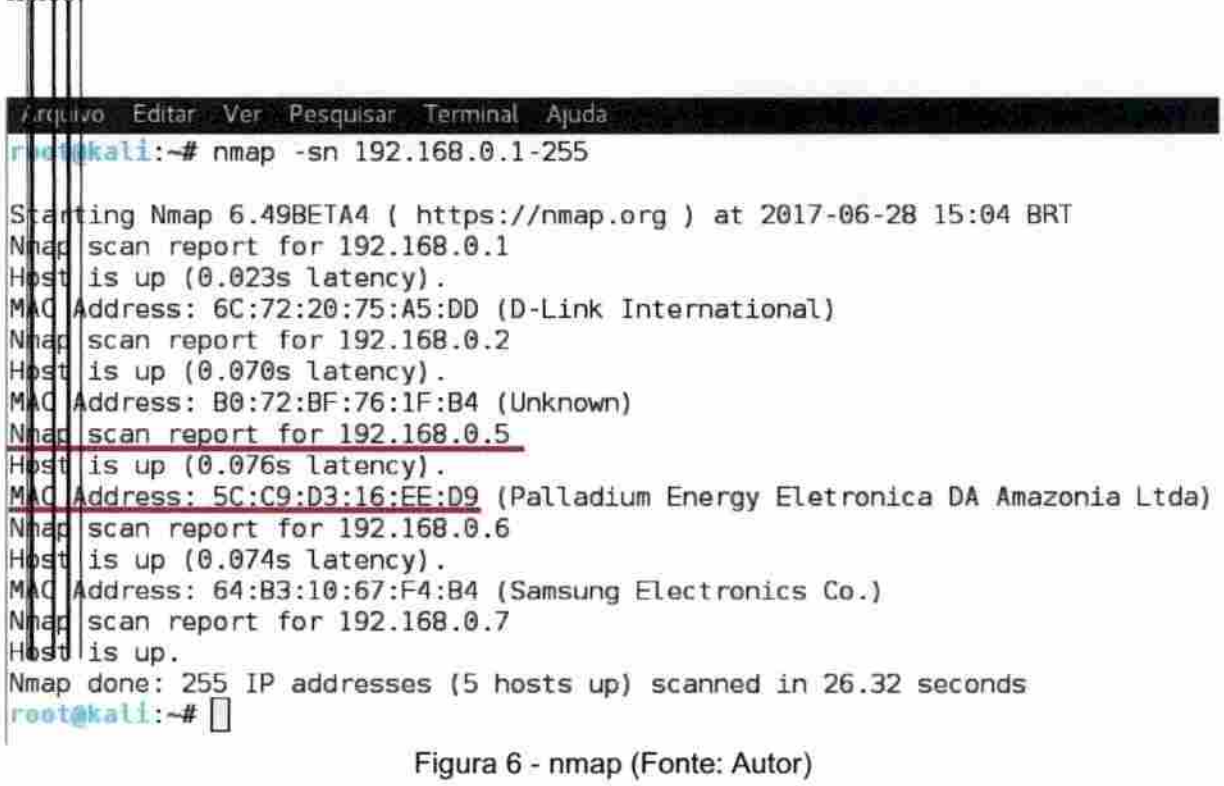


Figura 6 - nmap (Fonte: Autor)

Com o endereço da vítima identificado podemos ilustrar o seguinte cenário de rede mostrado na figura 7.

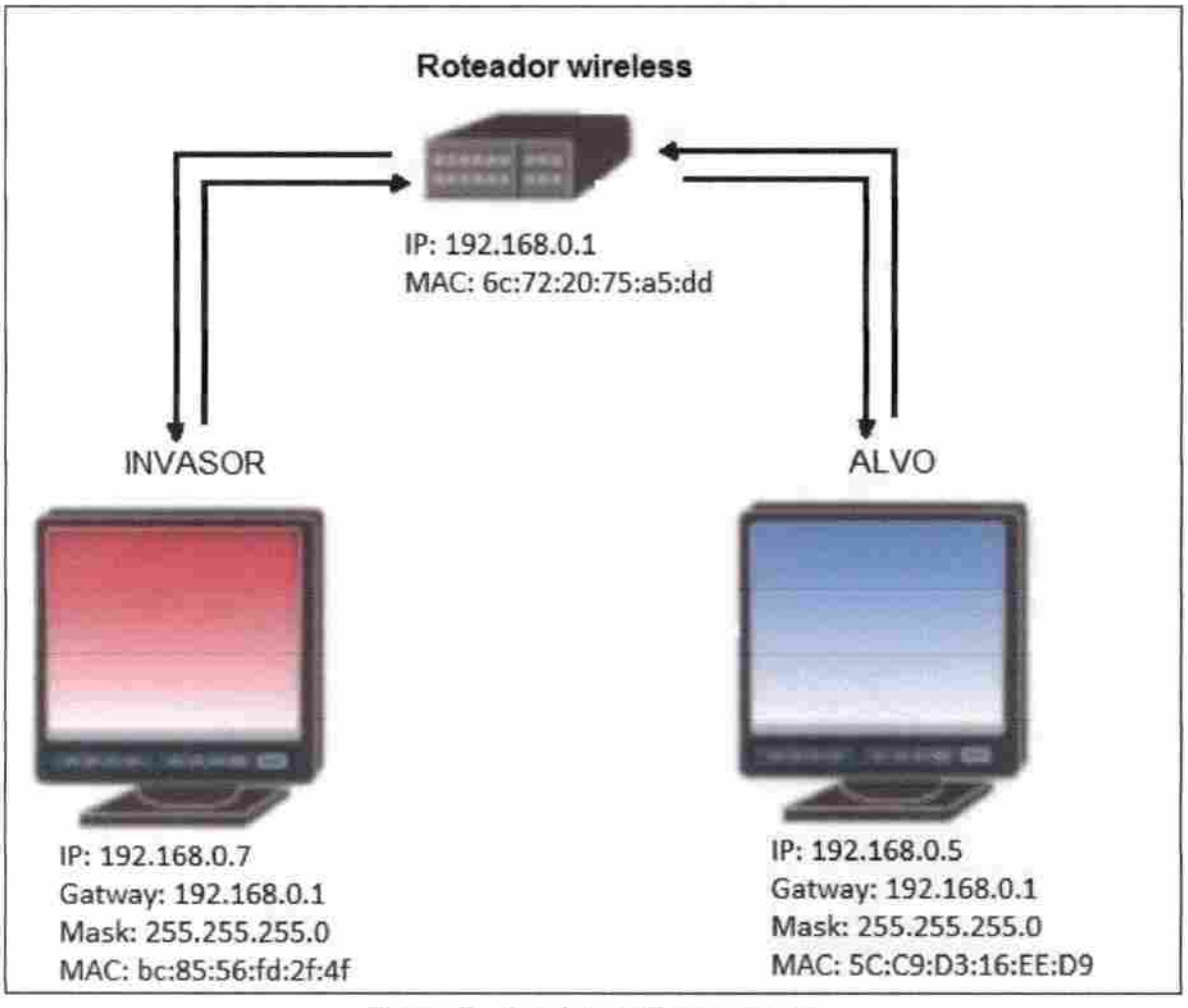


Figura 7 - Cenário 1 (Fonte: Autor)

Ainda na preparação do cenário para o teste da captura dos dados pra aceso com a utilização do Man-In-The-Middle, será necessário fazer a clonagem do layout da URL utilizada para autenticação no sistema de gestão WEB ao qual o cliente fará o login. Para isso foi utilizado o SET – Social Engineer Toolkit, o processo de cópia é simples e pode ser realizado no seguinte caminho nas opções do programa:

1) Social-Engineering Attacks (Ataques de Engenharia social)

2) Website Attack Vectors (Vetores de Ataque a Site)

3) Credential Harvester Attack Method (Método de Ataque Credencial Harvester)

2) Site Cloner (Clonagem de Site)

Ao escolher nas opções o Site Cloner, o programa solicita o endereço IP da mensagem de volta, o endereço onde o layout será salvo, o endereço a ser colocado deve ser o da máquina que fará o papel de servidora WEB, a que proverá o layout a vitima, e em seguida ele solicita a URL a ser copiada, a figura 8 mostra essas funções suprimindo o endereço que identificaria a proprietária do sistema alvo.

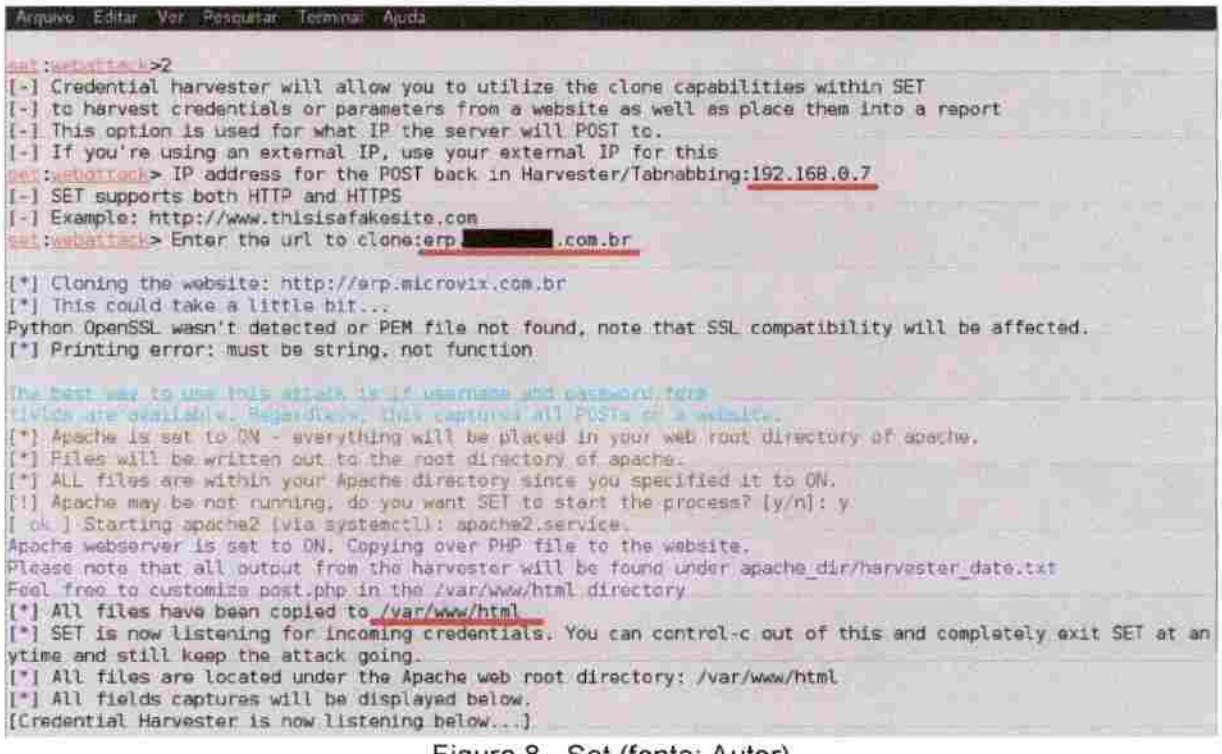


Figura 8 - Set (fonte: Autor)

Após realizada a clonagem, em "/etc/setoolkit/set.config" vamos ativar o "APACHE_SERVER", figura 9, assim quando a interceptação for realizada pelo Ettercap o SET fornecerá o layout armazenado na máquina atacante, é importante que o SET esteja ativo quando a interceptação pelo uso do Ettercap for realizada, pois ele mostrará a string dos dados digitados nos campos para autenticação.

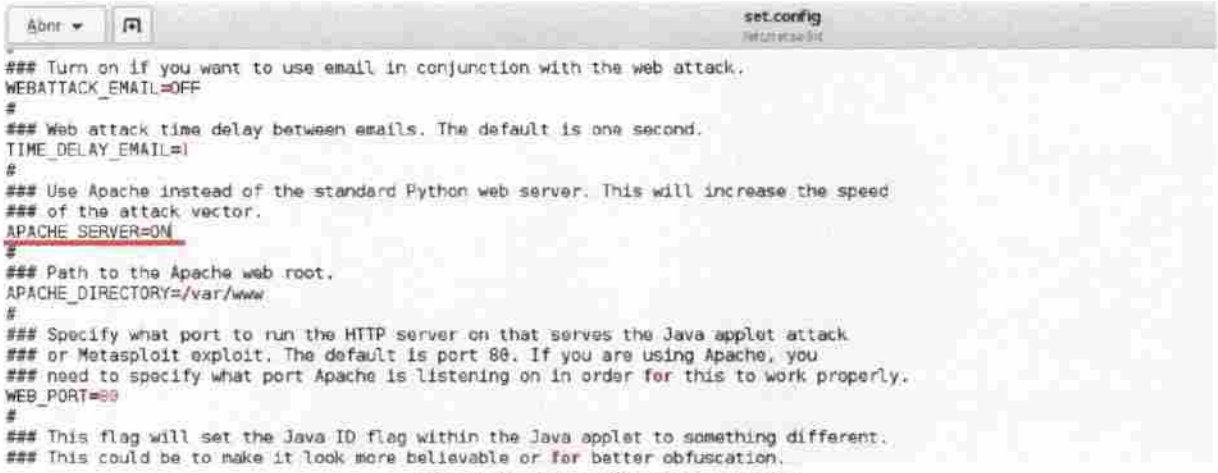


Figura 9 – set.config (Fonte: Autor)

Com o processo da engenharia social preparado agora será parametrizado o ataque de interceptação, o ataque Man-In-The-Midle será realizado com a técnica Arp Poisoning porém antes um ajuste deverá ser feito. Ao atacante se estabelecer entre as partes, vítima e roteador, todo o tráfego será capturado, porém interessa para este ataque somente quando a máquina vítima fizer uma requisição ao sistema de gestão WEB, portando o Ettercap será preparado para que responda somente a esta requisição provendo o layout clonado pelo SET.

Em "/etc/ettercap/etter.dns" deverão ser adicionadas as seguintes linhas conforme a figura 10, o domínio que identifica a empresa proprietária do software foi suprimido.

```
##############################################################################
#                                                                            #
#  ettercap -- etter.dns -- host file for dns_spoof plugin                   #
#                                                                            #
#  Copyright (C) ALoR & NaGA                                                 #
#                                                                            #
#  This program is free software; you can redistribute it and/or modify      #
#  it under the terms of the GNU General Public License as published by      #
#  the Free Software Foundation; either version 2 of the License, or         #
#  (at your option) any later version.                                       #
#                                                                            #
##############################################################################
#                                                                            #
# Sample hosts file for dns_spoof plugin                                     #
#                                                                            #
# the format is (for A query):                                               #
#   www.myhostname.com A 168.11.22.33                                        #
#   *.foo.com          A 168.44.55.66

[redacted].com.br                 A       192.168.0.7
erp.[redacted].com.br             A       192.168.0.7
http://erp.[redacted].com.br      A       192.168.0.7
*.[redacted].com.br               A       192.168.0.7
http://erp.[redacted].com.br      PTR     192.168.0.7
```

Figura 10 - etter.dns (Fonte: Autor)

O parâmetro "A" vincula o referido domínio alvo ao IP do invasor, mapeamento de nome para endereço IP, enquanto o parâmetro "PTR" faz o papel inverso, mapeamento de um endereço IP para um nome.

Com o Ettercap preparado a interceptação pode ser realizada por modo texto ou gráfico. Para iniciar a interceptação via modo texto no terminal basta o comando "ettercap -T -i wlan0 -q -M ARP:remote /192.168.0.1/192.168.0.5/". Abaixo segue a definição dos parâmetros utilizados, porém a interceptação pelo Ettercap será detalhada em modo gráfico.

-T, Ettercap em modo texto

-i, indicação da interface a ser utilizada, wlan0, interface de rede wireless

-q, suprime a apresentação do conteúdo dos pacotes interceptados

-M, indica o método Man-In-The-Middle

ARP:remote, plugin utilizado para que o MAC do invasor seja atribuído ao endereço lógico na resolução da tabela ARP da vítima

Os endereços lógicos "/192.168.0.1/192.168.0.5/" pertencem respectivamente ao Gatway da rede e a máquina vítima.

A configuração o Ettercap em modo gráfico é muito simples, na opção Unified Sniffing do módulo Sniff (Farejar), seleciona-se a interface de rede que será utilizada para o monitoramento e interceptação, neste caso wlan0, figura 11.

Figura 11 - ettercap interface de rede (Fonte: Autor)

Escolhida a interface para a interceptação, em Manage the plugins no módulo Plugins, seleciona-se o plugin dns_spoof, figura 12, e em seguida no módulo Hosts faz-se uma buscas pelos host´s ativos na rede em Scan for hosts.

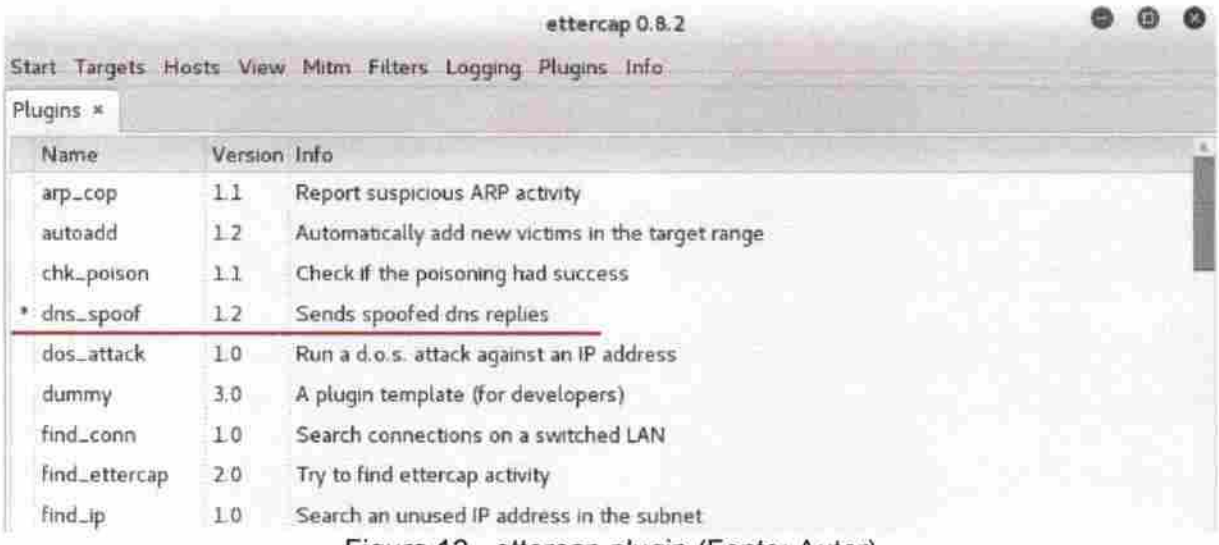


Figura 12 - ettercap plugin (Fonte: Autor)

Após a busca das entidades ativas na rede as exibimos em Hosts list, no mesmo módulo, o resultado da busca realizada na rede local teste, a figura 13 mostra estes resultados, os endereços fisicos e lógicos em destaque se referem respectivamente ao roteador da rede e a máquina alvo do ataque.

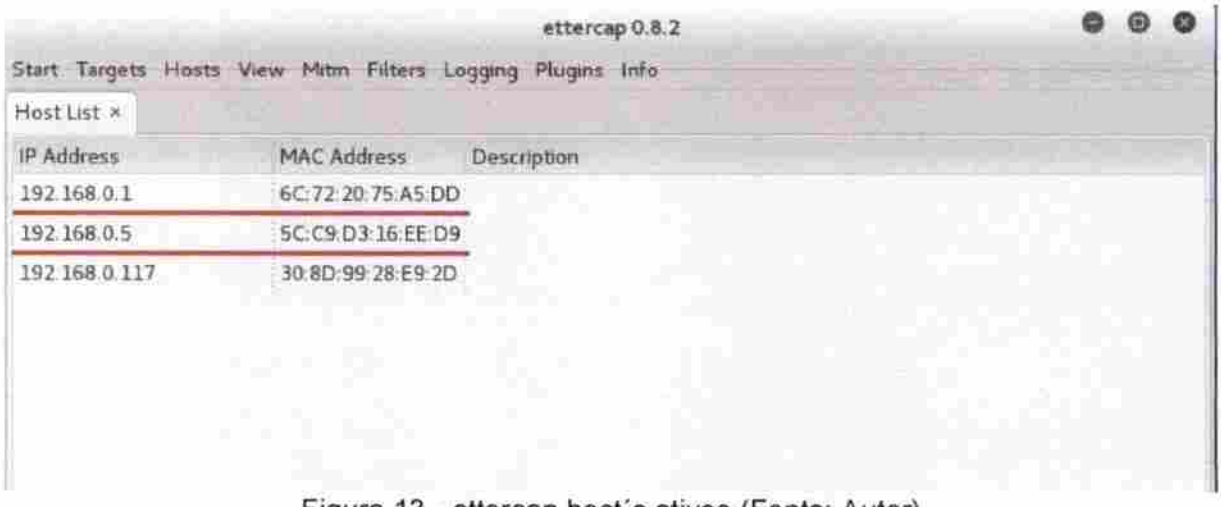


Figura 13 - ettercap host´s ativos (Fonte: Autor)

Os hosts, do roteador e vítima, devem ser selecionados e adicionados ao Target 2, é a comunicação entre estes que será escutada pela aplicação.

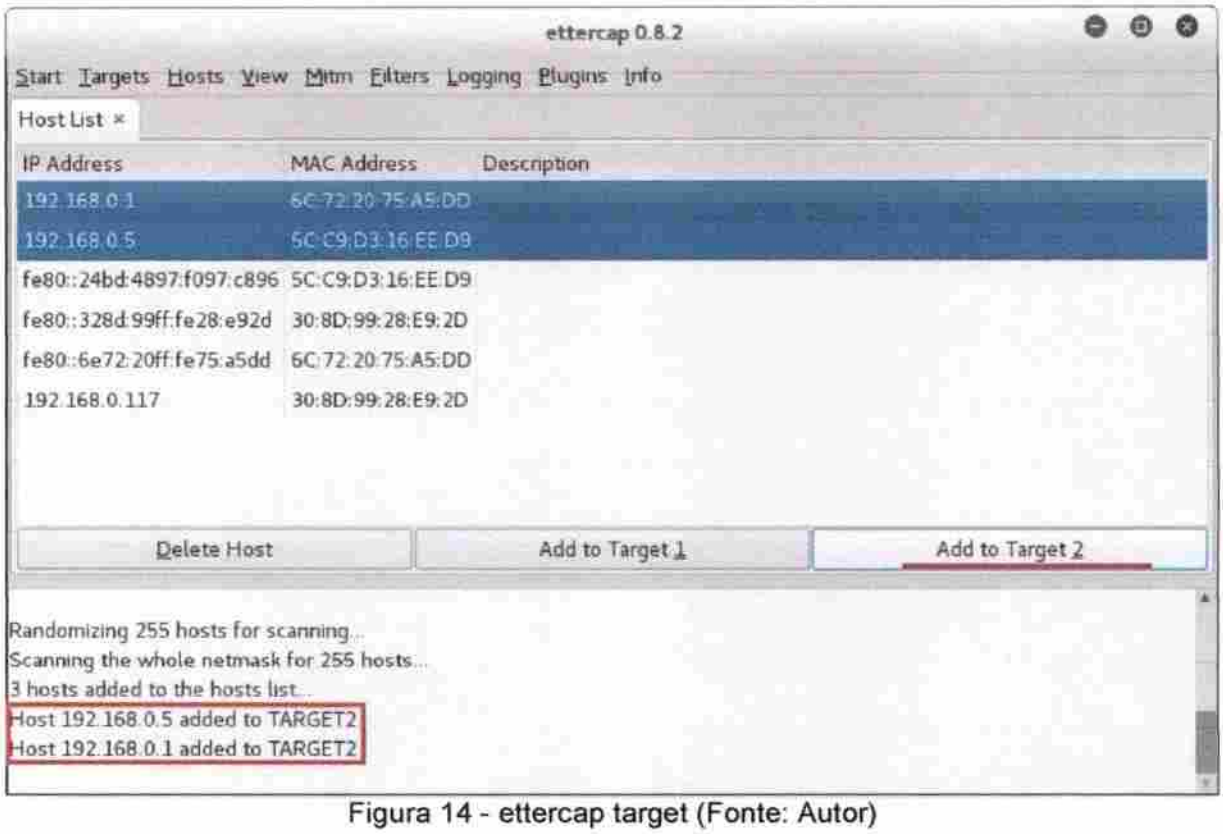


Figura 14 - ettercap target (Fonte: Autor)

Antes de iniciar a interceptação, no módulo MITM, seleciona-se o método ARP poisoning indicando o parâmetro Sniff remote connections (farejar conexões remotas).

Preparado o ettercap a interceptação pode ser iniciada em Star sniffing no módulo Start.

As figuras 15 e 16 mostram a resolução da tabela ARP na máquina vítima antes e após a interceptação, pode-se notar que agora o endereço lógico 192.168.0.1 que pertence ao roteador da rede não mais está resolvido com seu endereço fisico 6C:72:20:75:A5:DD, o MAC Address associado ao endereço lógico do roteador na resolução da tabela ARP da vítima agora é BC-85-56-FD-2F-4F, endereço fisico da interface de rede da máquina que realiza a interceptação.

```
C:\Users\luis>arp -a

Interface: 192.168.0.5 --- 0x9
  Endereço IP           Endereço físico       Tipo
  192.168.0.1           6c-72-20-75-a5-dd     dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
```

Figura 15 - Tabela ARP vítima, antes ataque (Fonte: Autor)

```
C:\Users\luis>arp -a

Interface: 192.168.0.5 --- 0x9
  Endereço IP           Endereço físico       Tipo
  192.168.0.1           bc-85-56-fd-2f-4f     dinâmico
  192.168.0.7           bc-85-56-fd-2f-4f     dinâmico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
```

Figura 16 - Tabela ARP vítima, após ataque (Fonte: Autor)

Com o ambiente preparado a máquina alvo fará o acesso a URL do sistema de gestão, neste momento o ettercap identifica a requisição ao endereço como mostrado na figura 17.

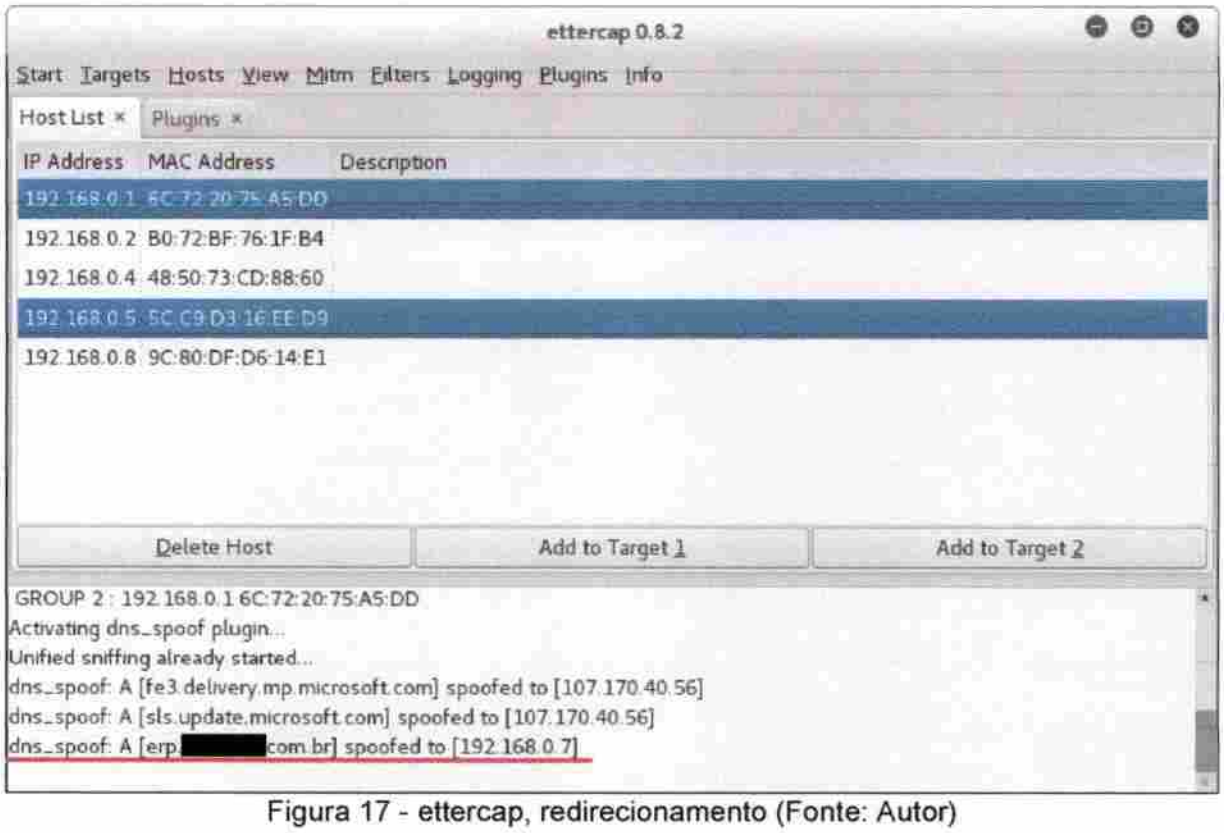


Figura 17 - ettercap, redirecionamento (Fonte: Autor)

A figura 18 mostra a página de autenticação do sistema com os dados de login, senha e frase de segurança preenchidos, porém a página acessada se trata do layout provido pelo atacante, com a mensagem de credenciais incorretas para acesso pois uma tentativa de acesso foi realizada. Nota-se que na barra de endereços o navegador indica acesso a site não seguro, a presença de um cadeado indicaria autenticação segura, essa observação será tratada mais adiante quando demonstrado a captura de dados para acesso ao sistema pela análise do tráfego de dados em rede no subtítulo 3.2, de qualquer forma isso demonstra que a autenticação não utiliza de criptografia, ou seja, os dados são transmitidos em texto claro por se tratar de um acesso ao site clone. Isso também ocorreria caso o ataque fosse realizado em quaisquer serviços como e-mail ou redes sociais.

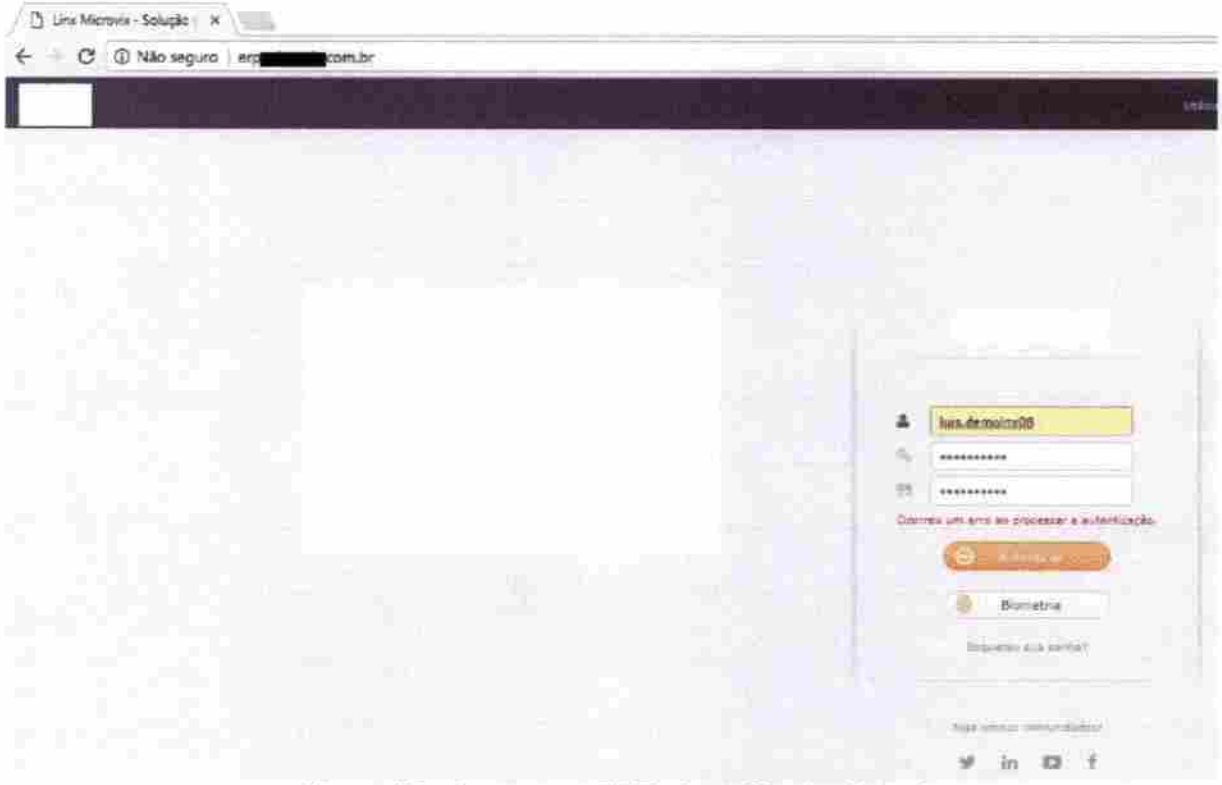


Figura 18 - Acesso ao ERP clone (Fonte: Autor)

Ao tentar a autenticação no sistema os dados de acesso são capturados e mostrados pelo SET de forma clara, figura 19.

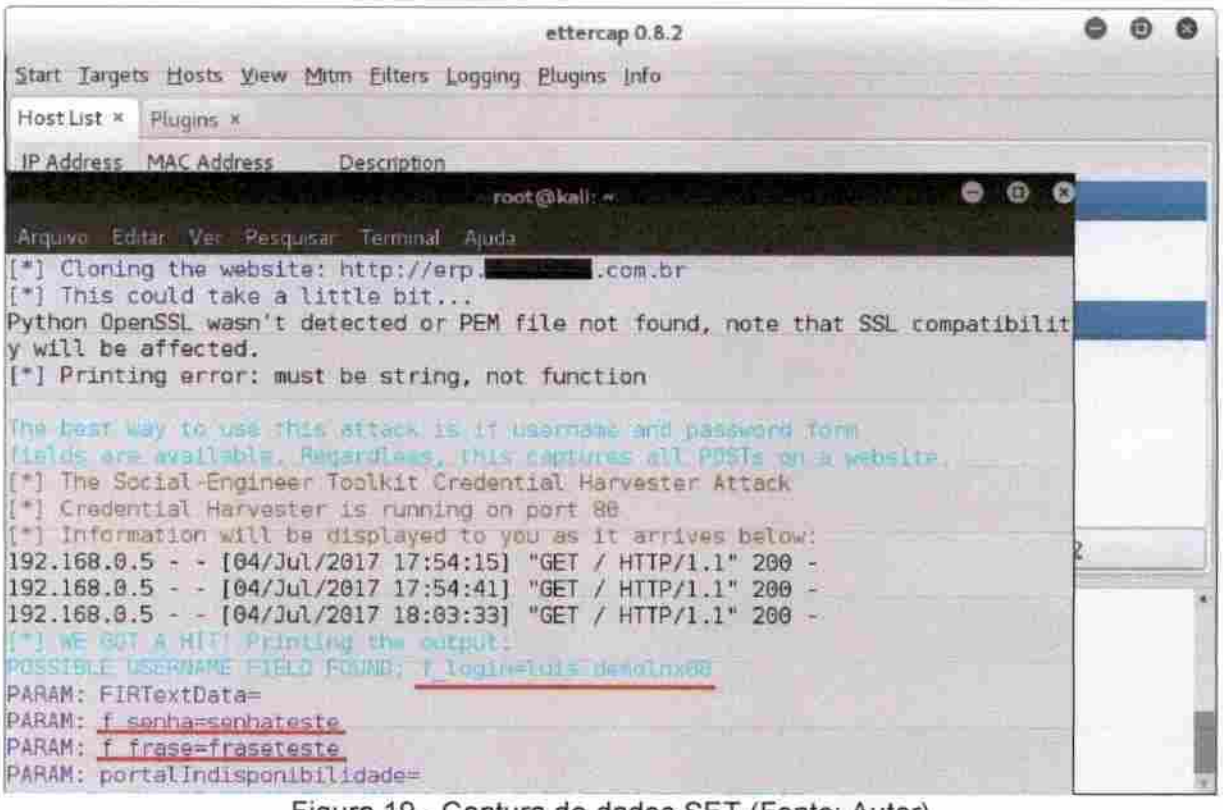


Figura 19 - Captura de dados SET (Fonte: Autor)

Com este teste foi possível detectar que o furto dos dados para acesso ao sistema de gestão é de fácil realização, porém cabe ressaltar que qualquer outro serviço WEB é passível deste tipo de ataque, cabe aos usuários e empresas que forneçam tais serviços proverem procedimentos de segurança pertinentes a cada perfil de usuários, tais questões serão tratadas no capítulo 4.

3.2 Captura de senhas pelo tráfego de dados em rede

No subtítulo 3.1.3 foi demonstrado em ambiente teste a interceptação de dados que permitiu o furto das credenciais acesso ao sistema de gestão WEB. Aqui será demonstrado outro método para essa interceptação valendo-se de uma segunda vulnerabilidade grave de segurança para autenticação no sistema, esta vulnerabilidade permite o furto das informações de maneira bem menos robusta que o ataque MITM em conjunto com técnicas de engenharia social, o qual já não demanda demasiado conhecimento sobre o tema para ser realizado.

3.2.1 Ambiente teste

O ambiente para a realização deste teste foi o mesmo utilizado para o ataque Man-In-The-Middle, 3.1.

3.2.2 Ferramentas utilizadas

Para este teste a ferramenta utilizada foi a aplicação Open Source Wireshark 2.2.7.

> Wireshark é o analizador de protocolo de rede mais amplamente utilizado em todo o mundo. Ele permite que veja o que acontece em sua rede a um nível microscópico se tornando de fato padrão em muitas empresas sem fins lucrativos, agências governamentais e instutuições educacionais. O deselvolvimento do Wireshar prospera graças a contribuição voluntária de especialistas ao redor do mundo sendo a continuação de um projeto iniciado por Gerald Combs em 1998.
>
> Este texto foi retirado e traduzido da URL "https://www.wireshark.org/"

Analisadores de pacotes em redes ou farejadores são ferramentas capazes de registrar todo o tráfego de dados em uma rede. Os analisadores podem ser aplicados de maneira maliciosa, acadêmica ou utilizados por gerenciadores de redes com o objetivo de identificar eventuais problemas e vulnerabilidades para obter auxílio em diagnósticos de redes.

Neste teste o Wireshark será utilizado com objetivo malicioso, irá captar os dados para acesso ao sistema ERP WEB com a utilização de poucos filtros que facilitarão a análise de um intenso tráfego de dados, trazendo para o invasor uma quantidade de informações reduzida e mais fáceis de serem analisadas com o objetivo de identificação do login, senha e frase de segurança para acesso ao sistema.

3.2.3 Realização do teste

A configuração inicial do Wireshark é muito simples, a princípio se define a interface de rede a ser utilizada pela máquina que fará a análise do tráfego de dados na rede em Interface List e inicia-se a análise em Start capturing packets (Começar a capturar os pacotes), figura 20.

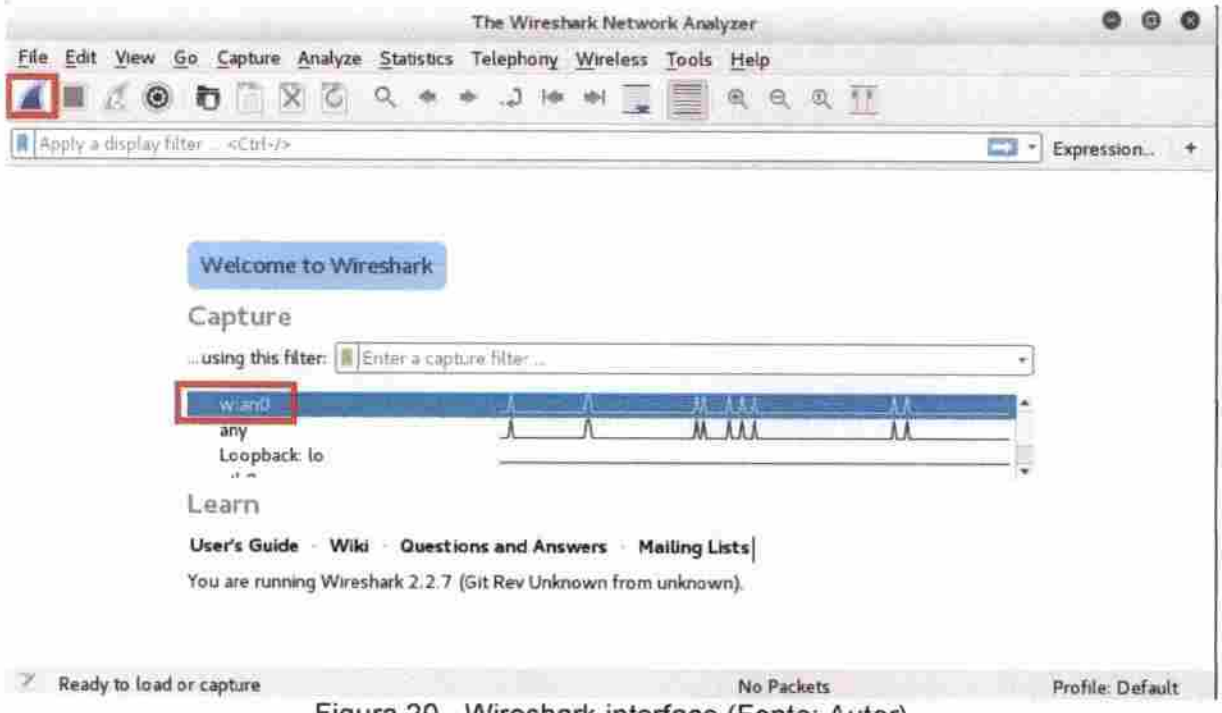


Figura 20 - Wireshark interface (Fonte: Autor)

Feito isso o Wireshark já está captando os dados trafegados na rede em que está inserido. A quantidade de pacotes interceptados em segundos de análise pelo farejador pode ser imensa mesmo em uma pequena rede como a do ambiente teste utilizado nesta experiência, filtros devem ser utilizados para reduzir a quantidade de pacotes e tipos informações mostradas facilitando a busca pelos dados de autenticação no sistema de gestão.

Preparado e iniciado o farejador, os pacotes transmitidos passam a ser captados e mostrados pelo programa, no alvo foi acessada a URL do sistema, figura 21, para verificar se estas requisições são analisadas pelo Wireshark.

Figura 21 - Acesso ERP segundo teste (Fonte: Autor)

O layout fornecido da figura anterior é o do sistema de gestão e não a cópia fornecida pela técnica de engenharia social como no subtítulo 3.1, na imagem podemos notar novamente a ausência do cadeado que indicaria autenticação segura, esta é a vulnerabilidade que será explorada neste teste.

Na figura 22 abaixo podemos verificar que pacotes originados do alvo IP 192.168.0.5 são captados, porém são dados comunicados entre esta e a máquina atacante, portando requisições HTTP não foram captadas.

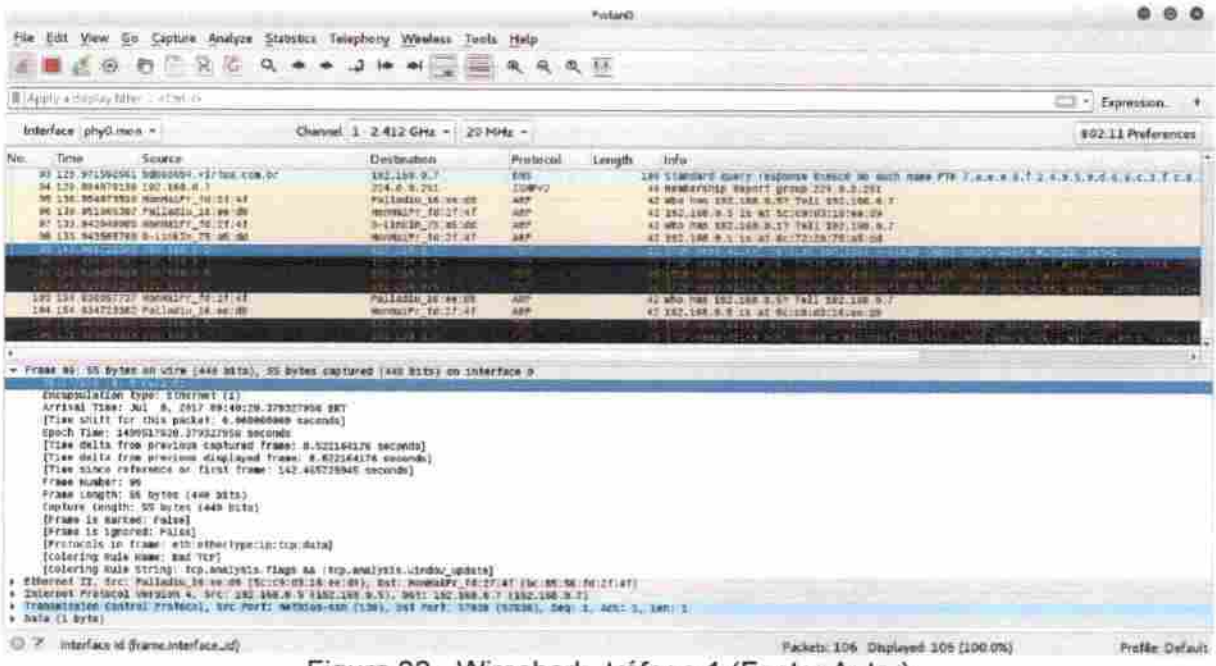


Figura 22 - Wireshark, tráfego 1 (Fonte: Autor)

Como as requisições HTTP não foram captadas pelo farejador, novamente iremos nos valer do MITM mas desta vez sem o recurso da engenharia social. O alvo fará o acesso ao sistema de gestão WEB autêntico, se autenticará normalmente sem mensagens de erro por estar no sistema real provido pelos servidores da empresa desenvolvedora. O MITM facilitará a análise dos dados fazendo com que todas as requisições, inclusive HTTP, passem pelo atacante graças à fraude realizada na resolução da tabela ARP do computador alvo, de modo que todos os dados enviados pela vítima sejam escutados pelo Wireshark.

Já conhecido os parâmetros do Ettercap desta vez ele será executado em modo texto com o comando: "ettercap -T -i wlan0 -q -M ARP:remote /192.168.0.1/192.168.0.5/", figura 23.

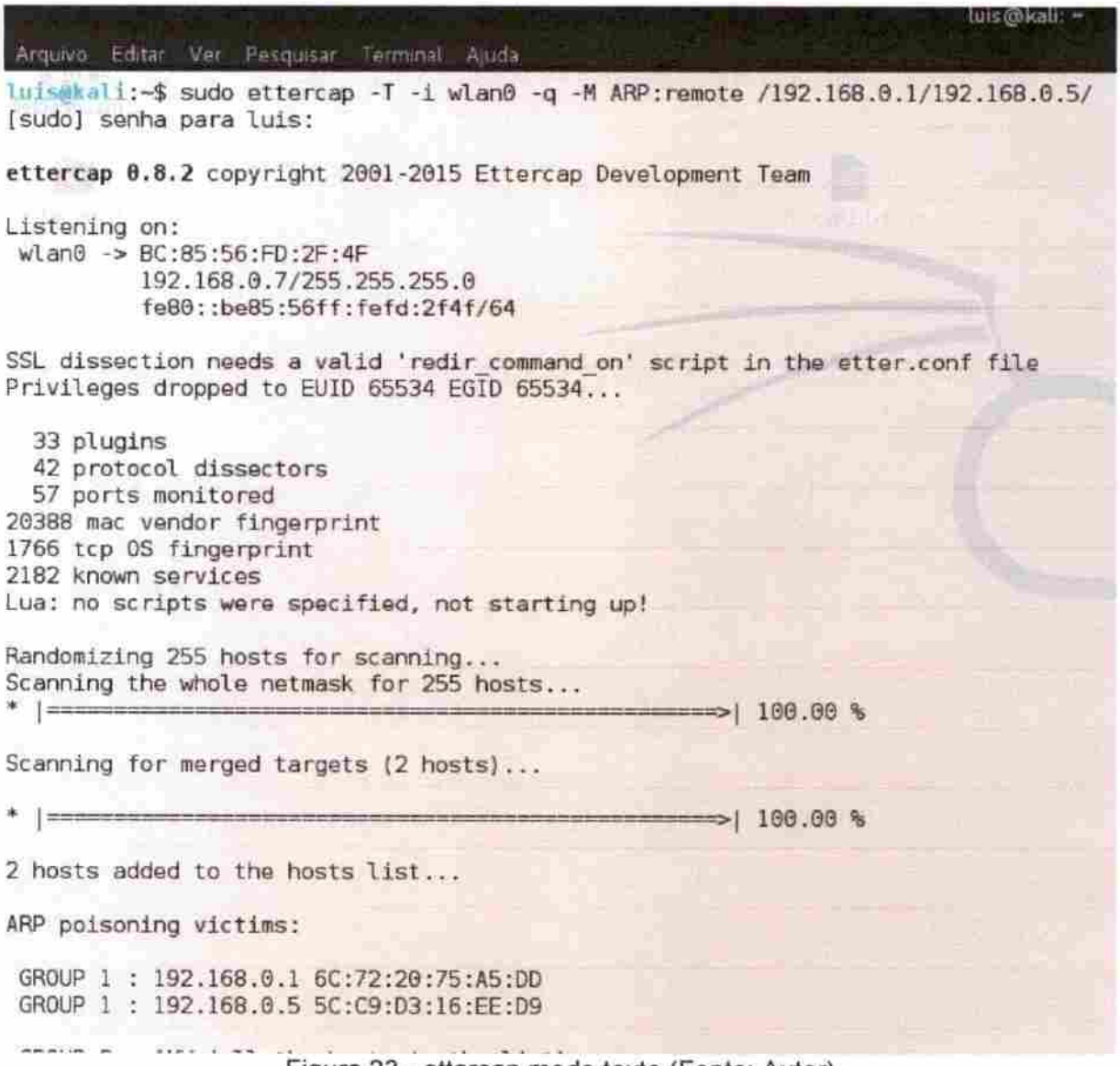


Figura 23 - ettarcap modo texto (Fonte: Autor)

Agora podemos verificar a alteração na resolução da tabela ARP do alvo, as figura 24 e 25 mostram sua resolução antes da e depois da interceptação respectivamente.

```
C:\Users\luis>arp -a

Interface: 192.168.0.5 --- 0x9
  Endereço IP           Endereço físico       Tipo
  192.168.0.1           6c-72-20-75-a5-dd     dinâmico
  192.168.0.7           bc-85-56-fd-2f-4f     dinâmico
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
```

Figura 24 - Tabela ARP alvo antes da interceptação, em modo texto (Fonte: Autor)

```
C:\Users\luis>arp -a

Interface: 192.168.0.5 --- 0x9
  Endereco IP          Endereco físico       Tipo
  192.168.0.1          bc-85-56-fd-2f-4f     dinâmico
  192.168.0.7          bc-85-56-fd-2f-4f     dinâmico
  192.168.0.255        ff-ff-ff-ff-ff-ff     estático
  224.0.0.2            01-00-5e-00-00-02     estático
  224.0.0.22           01-00-5e-00-00-16     estático
  224.0.0.251          01-00-5e-00-00-fb     estático
  224.0.0.252          01-00-5e-00-00-fc     estático
  239.255.255.250      01-00-5e-7f-ff-fa     estático
```

Figura 25 - Tabela ARP alvo antes da interceptação, em modo texto (Fonte: Autor)

Com a tabela ARP fraudada o sistema será acessado novamente e uma tentativa de login feita enquanto se verifica os dados captados pelo Wireshark, a imagem 26 mostra que a autenticação ocorreu com sucesso, sendo este a retaguarda do sistema de gestão e não o layout clone da página de autenticação.

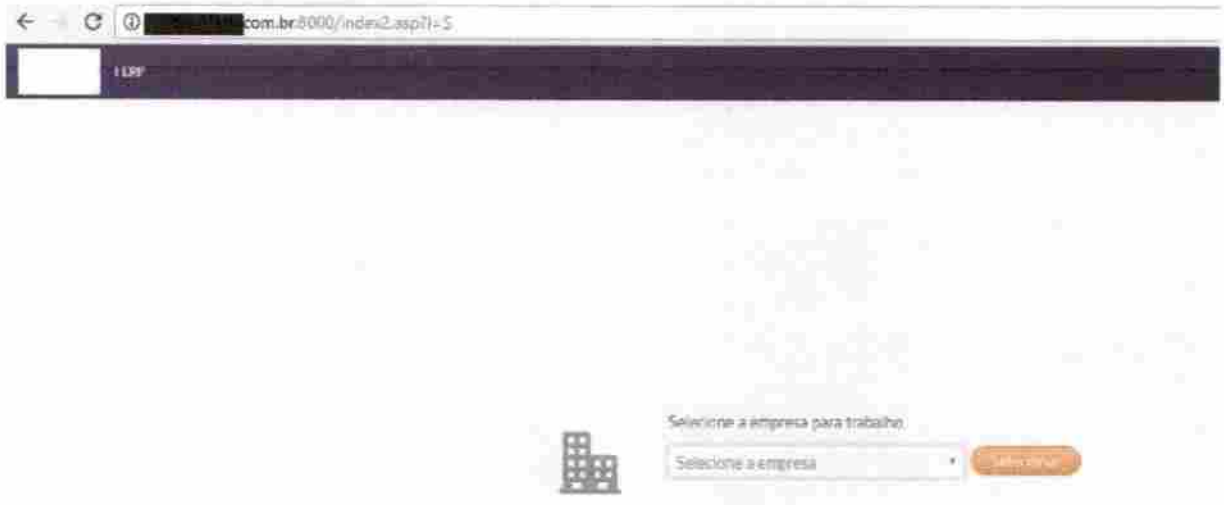


Figura 26 - Autenticação ERP (Fonte: Autor)

Acessado o sistema verificamos que o analisador de tráfego capta os pacotes do protocolo HTTP, pela quantidade de pacotes mostrados pelo programa farejador foi utilizado um filtro de protocolo para que somente estes sejam mostrados, figura 27.

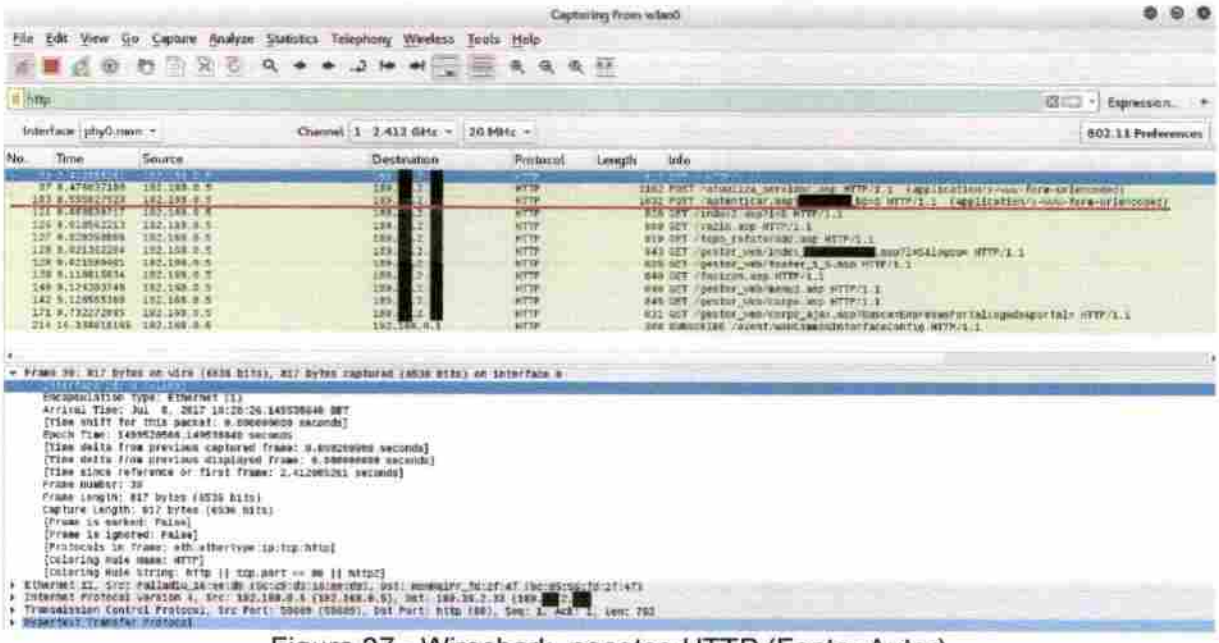


Figura 27 - Wireshark, pacotes HTTP (Fonte: Autor)

Sobre o pacote nº 103 marcado na imagem anterior, iremos detalhar o fluxo de dados TCP, no Wireshark isso é possível de se realizar em nas opções de cada pacote baseados em TCP nas opções Follow / TCP Stream.

A figura 28 nos mostra que o login, senha e frase de segurança foram captados sem dificuldade, o que demonstra que os dados passam sem criptografia, assim pode-se concluir que a empresa proprietária do software os possui também.

Mesmo que existam políticas de segurança com registro de logs de alterações e de parametrizações, elas por si só não se mostrariam eficientes pelo fato de que um usuário, seja um invasor externo ou uma ameaça interna ao cliente do sistema de gestão, que faça as alterações na base de dados, ele o fará autenticado com credenciais válidas, portando ao analisar quem fez as autorizações, o log registraria um autêntico usuário com permissão a fazê-las.

Outra questão é o fato dessas credenciais serem salvas nos servidores da desenvolvedora sistema em texto claro, ou seja, os agentes internos desta empresa os possuem.

Alguém de posse dessas informações pode fraudar utilizadores do sistema sendo registrado nos logs como sendo os diretores, gerentes ou usuários autorizados das corporações como os responsáveis por tais alterações, pois eram seus dados de acesso utilizados e registrados.

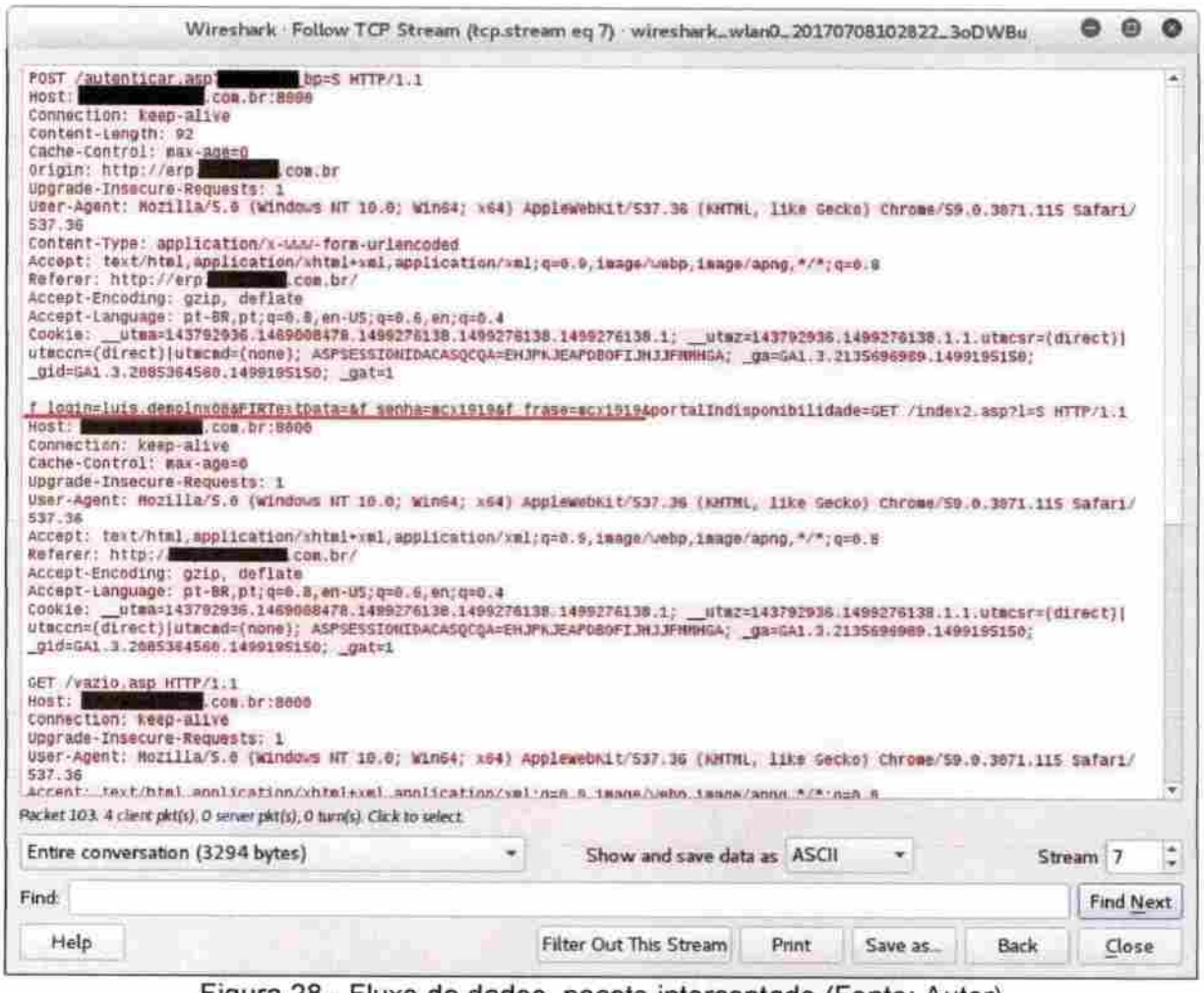


Figura 28 - Fluxo de dados, pacote interceptado (Fonte: Autor)

Este segundo mostrou a fragilidade da segurança na autenticação ao Software, ambos os testes remetem a vulnerabilidades fáceis de serem identificadas mas com impactados muito negativos se dada à devida importância de suas existências em uma divulgação mal intencionada de empresas concorrentes no mercado de sistemas de gestão para o varejo.

3.3 Impactos nas Empresas Clientes do Software

As vulnerabilidades levantadas comprometem as principais propriedades desejáveis na segurança de dados e serviços: Autenticidade, Confidencialidade, Integridade e Disponibilidade.

Um usuário não autorizado a ter acesso ao sistema de gestão de uma empresa pode realizar diversas ações danosas diretas a corporação que o utiliza com a manipulação dos dados e serviços oferecidos pelo Software, seja realizando fabricação, modificação ou a interrupção de serviços. A destruição de dados não é algo que será mensurado como risco em potencial, pois sistemas de gestão consistentes não permitem que dados movimentados sejam excluídos para que o histórico não seja perdido.

A modificação dos dados receberá uma especial atenção devido à gravidade de suas conseqüências.

3.3.1 Modificação de Dados

A ameaça de modificação de dados consiste na alteração de informações existentes por entidade não autorizada, acarretando na alteração do comportamento desejado do sistema ou sua interrupção. Não menosprezando a interrupção, que será tratada mais adiante, a alteração do comportamento de um sistema de gestão será abordada aqui exemplificando uma modalidade de crime, no qual o atacante com acesso a operação do ERP pode utilizá-lo para fraudar ordens de pagamentos lesando a empresa que utiliza o modelo de gestão ou apenas com o objetivo de lesar a imagem do seu alvo de ataque.

- Cobrança eletrônica

Um sistema de gestão independe do sistema bancário para a geração de boletos nos padrões da Febraban, CNAB 400 e CNAB 240. Ao realizar vendas em crediário o sistema utiliza os dados bancários cadastrados para a geração dos layouts dos boletos. A alteração dos dados bancários no sistema, número do banco, agência e conta, fará com que faturas a receber da empresa sejam emitidas destinando outras contas a desejo do invasor.

Gerar tais documentos de cobrança na própria empresa não significa que essas informações não sejam enviadas ao banco, elas são, através de arquivos de remessa. Ocorre

que a geração desses arquivos é realizada pelo emissor dos boletos ao seu desejo de tempo, a gestão da corporação define se estes serão gerados diariamente, mensalmente ou quinzenalmente por exemplo.

O envio desses arquivos traz certa segurança a empresa, pois se por ventura um atacante modificar os dados para a cobrança e os boletos forem emitidos com dados bancários incorretos, o sistema bancário identificará a informação. Porém isso não assegura aos clientes do emissor que estes boletos serão invalidados, pelo menos não de imediato, o layout produzido pelo ERP continuará o mesmo, Banco XXX, por exemplo, mas a linha digitável pode corresponder a outra conta bancária a desejo de quem o fraudar, fazendo assim com que os clientes tenham a posse de boletos com layout do banco correto, dados impressos com as informações corretas, mas linha digitável e código de barras que direcionarão o pagamento a contas não correspondentes a do emissor.

Essa prática de crime é conhecida, ver anexo C, porém essa ameaça de modificação de dados traz ainda mais credibilidade ao documento, pois é a empresa emissora que enviará via sistema a cobrança eletrônica diretamente aos clientes.

- Remessa de arquivos para pagamentos

Diversos sistemas ERP também homologam seus serviços junto a bancos para que clientes desses Softwares realizem seus pagamentos por arquivos de remessa. Estes arquivos consistem na transformação de um lote de contas a pagar da empresa, transferência entre contas de mesmo banco, DOC, TED e boletos em arquivos de formato TXT, é realizado o upload destes no sistema bancários que gera um arquivo de retorno em mesmo formato para a conciliação automática.

Boletos bancários a serem cadastrados nos módulo financeiros de contas a pagar são feitos inserindo na fatura eletrônica do sistema sua linha digitável, já nas transferências as contas bancárias dos beneficiários estão em seus respectivos cadastros no módulo CRM.

A alteração dos dados bancários e informações no CRM de beneficiários os quais um invasor identifique faturas de valor significativo lançadas, fará com que o arquivo de remessa enviado ao banco seja processado em contas bancárias distintas. Existe a possibilidade de reversão de transações como essas, mas demandam um processo burocrático nas agências bancárias e os valores devem ser estornados das contas destinos modificadas antes que sejam

retransmitidos ou sacados. Em situações como essas os bancos podem se eximir da responsabilidade de arcar com os prejuízos posto que não se trata de um erro do sistema bancário pois o arquivo de remessa gerado é de responsabilidade do cliente.

No caso das transferências eletrônicas é possível que o sistema do banco permita o processamento somente de ordens de pagamentos a contas pré-cadastradas, identificado no arquivo gerado pelo sistema e enviado ao banco pela empresa faudrada contas não cadastradas, o erro pode ser identificado a tempo, porém tal recurso de segurança não se aplica a pagamento de boletos bancários.

3.3.2 Interrupção de Serviços

A interrupção dos serviços gerenciados pelo sistema de gestão pode acarretar em enorme prejuízo financeiro ao deixar a empresa com faturamento parado. A simples exclusão ou modificação de uma série própria de NFC-e na retaguarda do sistema, parte do sistema operada pela WEB, fará com que as aplicações POS não consigam mais emitir vendas, pois os documentos de venda serão recusados pela SEFAZ, seja pela série não condizer com o padrão do documento eletrônico ou se a sequência da numeração for alterada por um invasor.

Essa alteração fará com que todas as operações de venda nos caixas sejam interrompidas, o impacto negativo da interrupção no faturamento de uma empresa é incalculável, não sendo possível mensurar o tempo que levará para que a causa do problema seja encontrada e solucionada.

3.3.3 Fabricação de Dados

A fabricação de dados pode ser executada por um invasor por diversos motivos, porém é com modificação que os objetivos financeiros do atacante em relação à vítima se concretizam com mais evidência. Fabricar dados, ou seja, incluir informações na base de dados do cliente que teve seu sistema de gestão invadido após ter seus dados de autenticação furtados, não é algo imaginável como fonte rentável para um criminoso, ao menos que este tenha objetivos alheios a somente lucrar sobre seu ataque, como prejudicar a imagem da empresa que utiliza o sistema.

Sistemas de gestão podem possuir gerenciadores de Newsletter (Boletim de notícias), que é o caso do sistema utilizado como case nestes testes. Este módulo é responsável pelo envio de e-mails com base nos cadastros de clientes, fornecedores e transportadores para envio de promoções, pedidos de compras e ordem para transportadoras.

O atacante pode gerar uma Newsletter para a base de dados da empresa vítima, o conteúdo destas pode ser por exemplo o anuncio de promoções inexistentes ou criando pedidos de compras para fornecedores, colocando a credibilidade da empresa em risco além do desprendimento de tempo que ocorrerá para correção do mal entendido entre as partes envolvidas.

Diversos setores podem ser comprometidos com a fabricação de dados além dos mencionados, a questão é que qualquer desses setores atacados com a fabricação de dados fará com que a empresa sofra com perdas financeiras e de credibilidade com seus relacionamentos.

3.3.4 Furto de Dados

De posse da permissão de acesso os dados da empresa atacada, o invasor tem acesso livre a todo histórico fiscal, de faturamento da empresa e banco de dados de clientes, essas informações, dependendo da dimensão da empresa, podem ser interessantes para comercialização de Mailing Clients (Lista de correspondência). A comercialização deste tipo de listas ocorre comumente na esfera corporativa, o acesso a um banco de dados específico de determinado segmento de varejo pode interessar a concorrentes do mesmo segmento, não que os interessados necessariamente saibam que a origem da lista pode ser fruto de um furto de informações.

3.4 Impactos na Empresa Proprietária Software

No capítulo 2 foram abordadas algumas informações quanto à dimensão da empresa proprietária do Software de gestão WEB sobre a qual os testes de vulnerabilidades de segurança foram aplicados, e são notáveis os segmentos e números de clientes atendidos por essa corporação.

A empresa ainda possui capital aberto, ou seja, possui ações comercializadas em bolsa de valores o que reforça ainda mais a importância de sua imagem no cenário nacional.

A divulgação de falhas graves e notavelmente simples na segurança de seu software de gestão, principal sistema da empresa, pode causar um impacto negativo em sua imagem e consequentemente a perda de credibilidade nas demais aplicações oferecidas por ela. Os desdobramentos da divulgação de tais falhas podem ocasionar uma mancha em sua imagem e impactar inclusive com a queda do valor de suas ações, os anexos A e B nos mostram exemplos reais de empresas que sofreram com esta situação ao serem vítimas de ataques de Hackers.

Claro que a dimensão das empresas destacadas nas reportagens anexas a esse trabalho é de outro patamar, mas o Software case abordado neste trabalho possui a maior abrangência nacional entre os demais do mesmo segmento, o que nos leva a concluir que uma falha de segurança divulgada traria sim conseqüências a sua imagem e ao seu valor capital.

A perda de credibilidade, valor de suas ações e possivelmente clientes, são conseqüências diretas da divulgação destas informações, a retomada da confiabilidade de seus Softwares seria um segundo passo para o retorno do seu crescimento no mercado o que nos leva a analisar que esta retomada desprenderá um investimento em Marketing que superará em alta escala o investimento em segurança de seus sistemas, posto que as vulnerabilidades são graves porém com soluções relativamente simples de serem implementadas.

4 SOLUÇÕES PREVENTIVAS

Diversos outros serviços estão suscetíveis ao ataque Man-In-The-Middle, que pode ser realizado com sucesso em serviços de e-mail como "hotmail.com", *"yahoo.com*.br" ou "gmail.com" por exemplo. Uma arma eficiente para a defesa contra este tipo de ataque a usuários sem experiência ou conhecimento a questões relativas à segurança da informação é o conhecimento.

Saber identificar um acesso seguro, alterar senhas com freqüência ou quando suspeitar de uma autenticação fora do padrão de costume, optar por senhas mais complexas e extensas são exemplos simples ações que demandam apenas informação sobre a questão.

4.1 Autenticação Segura

A segurança na autenticação do sistema avaliado não demonstra ser uma prioridade da empresa desenvolvedora, a real aparência de prioridades se dá nos resultados operacionais que o sistema oferece, sua usabilidade, desempenho e Marketing do produto. O fato de o sistema ser operado via WEB ainda levanta a questão sobre o atacante precisar de apenas um acesso a rede de computadores da empresa, pois de posse dos dados para acesso a fraude pode ser construída com cautela de qualquer lugar sem a necessidade de permanecer na rede.

A autenticação segura é um recurso que implementado no sistema de gestão mitigaria o risco da interceptação dos dados de acesso, ao menos quando tratamos da vulnerabilidade da comunicação de dados entre o cliente e servidor sem criptografia de dados, desse modo, login e senha não seriam transmitidos em texto claro o que é uma falha grave de segurança quando ocorre.

A autenticação e transmissão de dados de forma segura funcionam com a utilização de criptografia simétrica e assimétrica, sendo assim o site utilizado para autenticar-se no sistema de gestão WEB deveria ser reformulado para a utilização de HTTPS ao invés do atual HTTP, desse modo haveria a confidencialidade dos dados transmitidos ao menos na autenticação ao sistema e demais operações sensíveis.

O processo de autenticação segura funciona da seguinte forma:

O cliente para realizar o login no site do sistema de gestão o faria via HTTPS, neste momento seria gerada uma chave de criptografia simétrica, figura 29, esta será utilizada para criptografar os dados a serem enviados ao site de autenticação no servidor. Esta chave não poderá ser enviada via rede da maneira como está, pois se interceptada os dados transmitidos podem ser facilmente descriptografados, é neste ponto que se utiliza a criptografia assimétrica para seu envio.

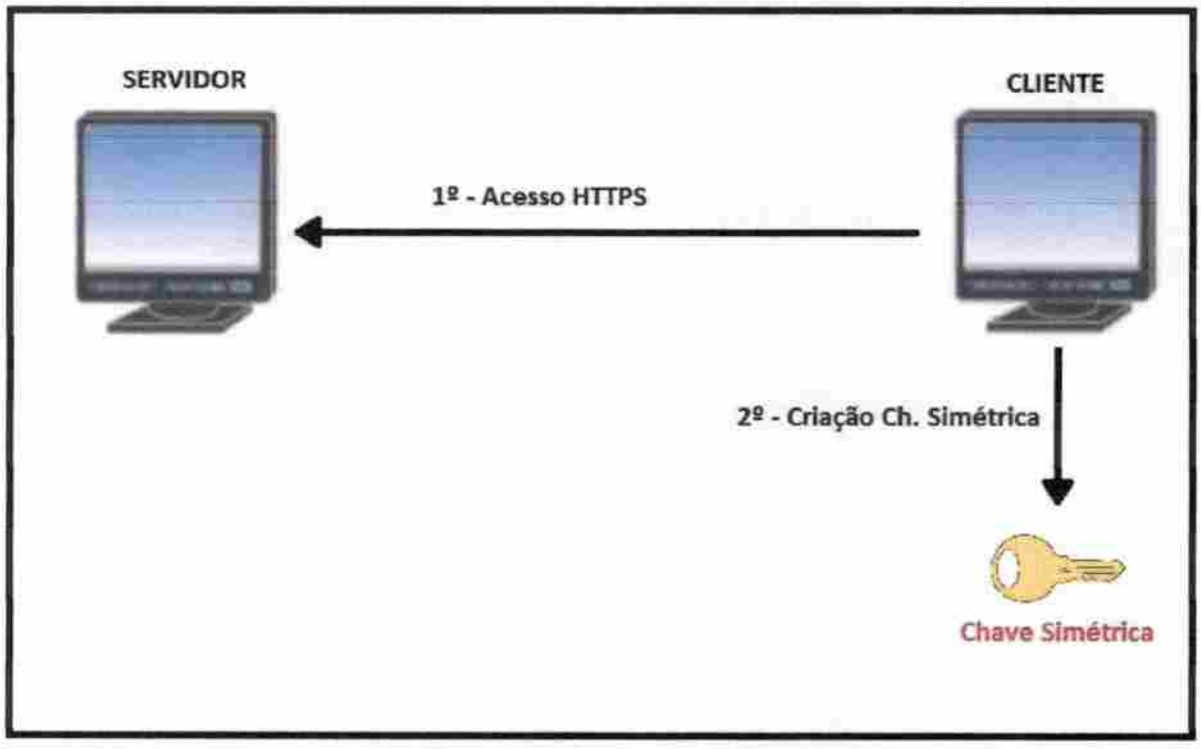


Figura 29 - Autenticação segura 1 (Fonte: Autor)

O servidor, para ler os dados enviados, precisará de uma cópia desta chave simétrica gerada pelo cliente, o processo para ele recebê-la com segurança consiste em primeiro o servidor possuir um par de chaves, a primeira denominada privada, pois apenas o servidor a possuirá, e outra pública, esta segunda é gerada a partir da primeira, privada, e enviada ao cliente, figura 30, aqui entramos na questão da criptografia simétrica.

O cliente irá gerar uma cópia de sua chave simétrica utilizada para a criptografia de seus dados a serem enviados, a cópia desta chave é criptografada com o uso da chave pública recebida pelo servidor.

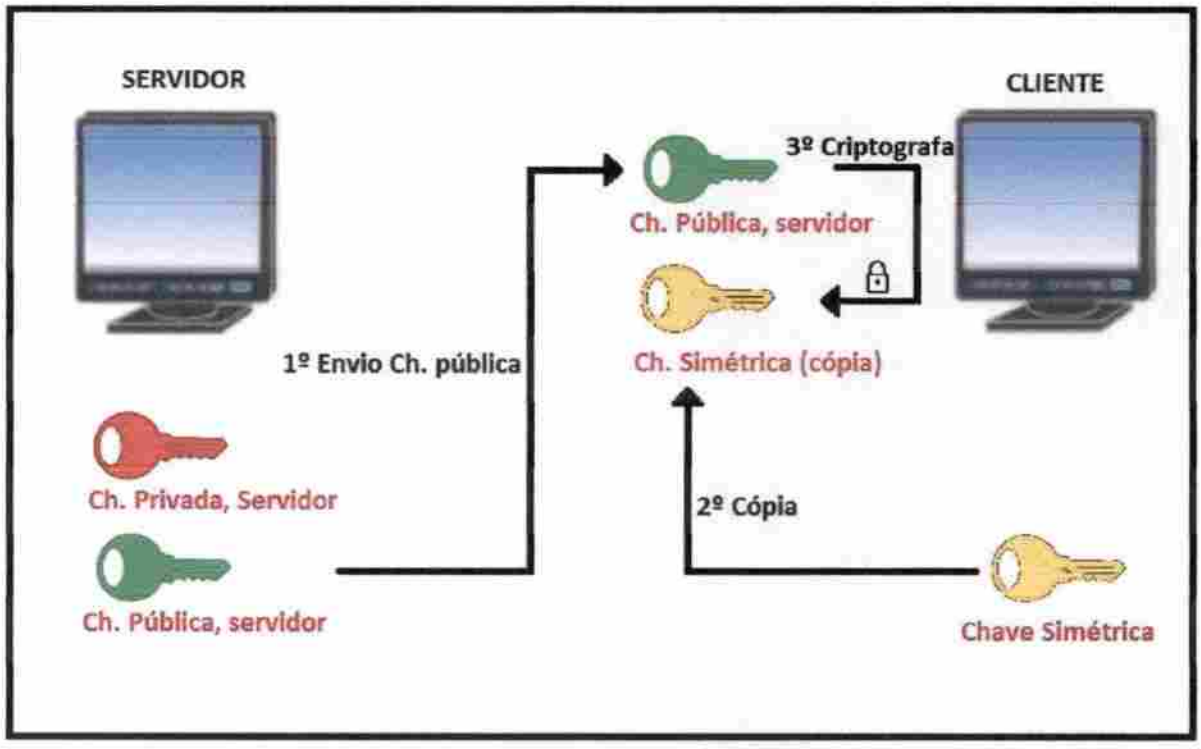


Figura 30 - Autenticação segura 2 (Fonte: Autor)

A chave simétrica criptografada do cliente agora poderá ser enviada com segurança ao servidor, figura 31.

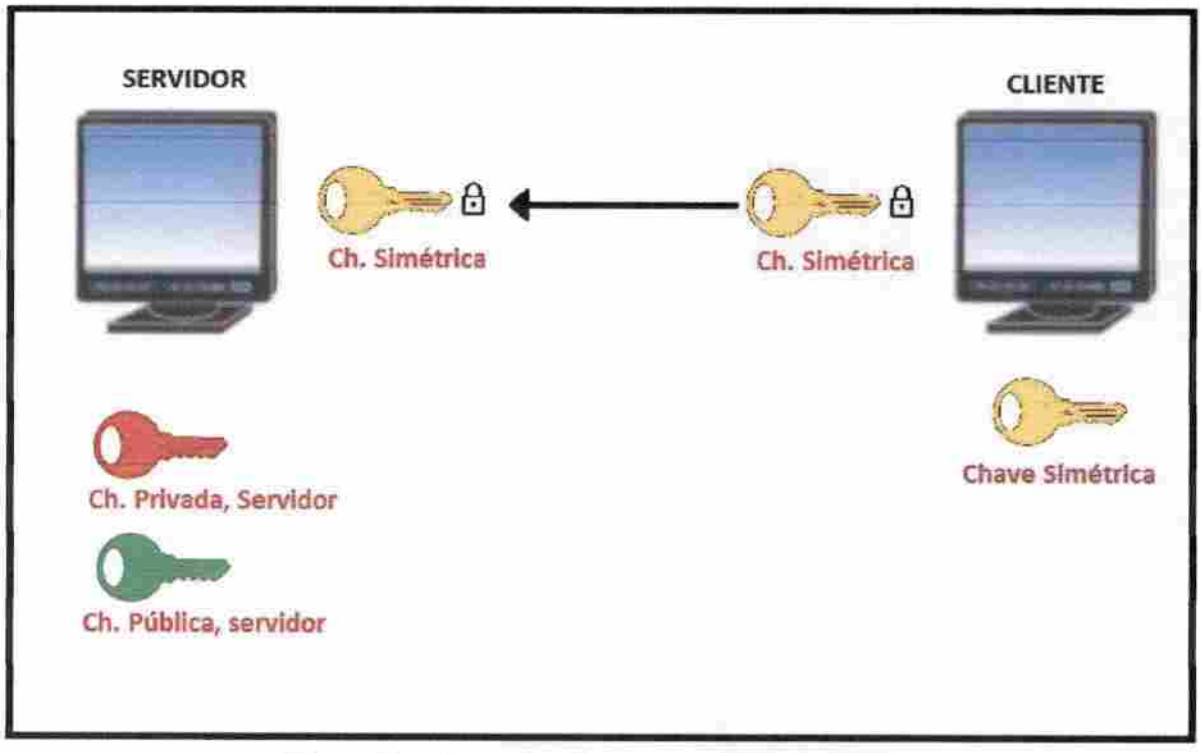


Figura 31 - Autenticação segura 3 (Fonte: Autor)

Se esta transmissão for interceptada, a leitura da chave simétrica enviada pelo cliente não será possível de ser realizada por um atacante, pois o mesmo precisaria ter acesso à chave privada do servidor, só com acesso a esta seria possível descriptografar o que foi criptografado com sua chave pública, já que a chave pública é gerada a partir da chave privada, e como a privada não é enviada ao cliente temos um sistema de autenticação seguro.

Se tratando de um sistema de gestão onde a dinamicidade e desempenho das operações deve manter um padrão de velocidade, a utilização de criptografia assimétrica é aconselhada apenas para o envio dos dados de autenticação.

4.2 Informação ao Usuário

Na figura 21 do subtítulo 3.2.3 podemos verificar a ausência do cadeado que indica autenticação segura no site como mencionado na ocasião, por conclusão lógica a empresa desenvolvedora do Software não forneceria informações sobre a importância de o usuário verificar a presença deste dispositivo de segurança se não disponibiliza tal método seguro.

Informar ao usuário a importância de se verificar se o site para autenticação é o fornecido por seu servidor seria prudente para a desenvolvedora se a mesma utilizasse autenticação segura, sendo assim, ser clara com os clientes quanto os riscos a que estão suscetíveis é um segundo passo após a mudança em seu método de autenticação.

5 CONCLUSÕES

Os dados para acesso ao sistema de gestão WEB foram copiados de duas formas por um atacante em ambiente teste, utilizando o Man-In-The-Middle com a técnica de ARP Poisoning e auxílio de engenharia social e escutando o tráfego de dados em rede com auxílio da mesma técnica de interceptação de dados.

O primeiro teste apesar de não envolver demasiado conhecimento técnico em segurança da informação, mostrou-se eficiente para a captura dos dados, porém vale ressaltar que esta não é uma vulnerabilidade inerente somente ao sistema testado, qualquer serviço WEB que requeira autenticação pode ser alvo deste tipo de ataque, a informação ao usuário quanto à autenticidade do site para acesso ao sistema poderia ser um ponto positivo para a segurança dos usuários, mas a mesma não poderia o fazer se antes não oferecesse um serviço seguro para a autenticação em seu sistema.

O segundo teste demonstra que a empresa desenvolvedora não possui autenticação segura, o primeiro passo a ser resolvido para que esteja embasada a prover informações aos clientes sobre questões de segurança no layout de autenticação ao seu sistema. Com o teste foi possível demonstrar que o sistema de gestão não utiliza criptografia para acesso fazendo com que as informações sejam transmitidas em texto claro pela rede, uma falha grave de segurança ainda mais por se tratar de uma empresa de software de abrangência nacional.

As falhas analisadas podem comprometer a imagem da desenvolvedora, assim como diretamente seus clientes finais vulneráveis a esses tipos de ataques. As conseqüências oriundas de um invasor mal intencionado são dificeis de serem mensuradas, pois em posse do acesso ao sistema de uma empresa é difícil determinar o tempo que levará para identificar e corrigir as alterações e ainda com o risco da interrupção do faturamento.

5.1 Trabalhos futuros

Desenvolvimento de uma cartilha com questões de segurança da informação voltada a em sistema de gestão, com linguagem acessível a gestores de empresas e administradores para que se desperte interesse sobre a importância da questão no momento de escolha do Software de gestão.

O documento deverá abordar sobre questões de autenticação segura a sistemas e serviços WEB, saber identificar se o site é seguro para acesso e demonstrar a importância de um profissional de segurança da informação acompanhar os processos de gestão gerenciados por software.

E posteriormente um estudo sobre como veicular este documento nas federações de comércio de modo de ele seja disseminado em seus eventos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. LEI Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União de 03/12/2012, P. 1.

CASEMIRO, Luciana, 2014. Aumentam os casos de fraudes com código de boletos bancários. Disponível em: < https://oglobo.globo.com/economia/defesa-do-consumidor/aumentam-os-casos-de-fraudes-com-codigo-de-boletos-bancarios-13958447>. Acesso em 11 de julho de 2017.

CLARO, João R. Sistemas IDS e IPS – Estudo e Aplicação de Ferramenta Open Source em Ambiente Linux. 2015. 86 folhas. Monografia (Curso Tecnólogo em Sistemas para a para Internet) – Instituto Federal Sul-Rio-Grandense, Passo Fundo, 2015.

DADOS Econômicos e Financeiros. Disponível em: <http://www.bmfbovespa.com.br/pt_br/produtos/listados-a-vista-e-derivativos/renda-variavel/empresas-listadas.htm?codigo=23035>. Acesso em 25 de abril de 2017.

ÉPOCA NEGÓCIOS. Verizon anuncia compra de Yahoo com Us$ 4,5 bilhões. 2017. Disponível em: <http://epocanegocios.globo.com/Empresa/noticia/2017/06/verizon-anuncia-compra-de-yahoo-por-us-45-bilhoes.html>. Acesso em 08 de julho de 2017.

ETTERCAP. Disponível em: <https://ettercap.github.io/ettercap/downloads.html>. Acesso em: 15 de abril de 2017.

FRAGA, Bruno, 2016. Você sabe o que Kali Linux? Disponível em: < https://tecnicasdeinvasao.com/linux/kali-linux/voce-sabe-o-que-e-o-kali-linux/>. Acesso em 13 de junho de 2017.

IG. Sony Pictures terá prejuíco de R$ 530 milhões após ataque de hackers. Disponível em: < ÉPOCA NEGÓCIOS. Verizon anuncia compra de Yahoo com Us$ 4,5 bilhões. 2017. Disponível em: <http://epocanegocios.globo.com/Empresa/noticia/2017/06/verizon-anuncia-compra-

de-yahoo-por-us-45-bilhoes.html>. Acesso em 08 de Julho de 2017>. Acesso em 08 de julho de 2017.

MARCELINO, Carolina, 2011. Empresas vendem dados do consumidor na internet. Disponível em: <http://www.estadao.com.br/blogs/jt-seu-bolso/2011/02/05/empresas-vendem-dados-do-consumidor-na-internet/>. Acesso em: 17 de julho de 2017.

THE SOCIAL ENGINEER TOOLKIT. Disponível em: <https://www.trustedsec.com/social-engineer-toolkit/>. Acesso em: 17 de abril de 2017.

WIRESHARK. Disponível em: <https://www.wireshark.org/>. Acesso em: 12 de junho de 2017.

XYZ registra receita e lucro líquidos maiores no 4T15. Disponível em: <www.investimentosenoticias.com.br/noticias/negocios>. Acesso em 24 de abril de 2017.

ANEXO A - Verizon anuncia compra de Yahoo por US$ 4,5 bilhões

13/06/2017 – Agência Globo

(http://epocanegocios.globo.com/Empresa/noticia/2017/06/verizon-anuncia-compra-de-yahoo-por-us-45-bilhoes.html)

Verizon Communications, operadora de telefonia móvel número 1 dos Estados Unidos, anunciou nesta terça-feira a compra do Yahoo por US$ 4,48 bilhões, finalizando um acordo que afeta mais de um bilhão de contas do Yahoo. O negócio representa a mais recente jogada das telecomunicações para desafiar o domínio da publicidade online no Vale do Silício.

Sob comando da Verizon, Yahoo e AOL serão combinados para integrar uma nova empresa de mídia e tecnologia chamada Oath. A venda do Yahoo foi anunciada pela primeira vez no ano passado, por US $ 4,8 bilhões. Mas, apenas alguns meses depois, a empresa divulgou uma série de violações de dados que comprometeram as informações pessoais de potencialmente centenas de milhões de pessoas. Após as brechas, o Yahoo e a Verizon finalmente concordaram em desconto do preço de compra em US $ 350 milhões.

ANEXO B - Sony Pictures terá prejuízo de R$ 530 milhões após ataque de hackers

23/12/2014 – IG

(http://on.ig.com.br/imagem/2014-12-23/sony-pictures-tera-prejuizo-de-r-530-milhoes-apos-ataque-de-hackers.html)

O ataque de um grupo de hackers ao sistema da Sony Pictures não só causou constrangimentos e vazamentos de filmes ainda não lançados, como também dará um grande prejuízo. O estúdio terá gastos de mais de R$ 530 milhões para lidar com as consequências da invasão.

Sony terá, ainda, que bancar um novo sistema de segurança da rede compartilhada atacada pelos hackers, além de pagar indenizações para funcionários e ex-funcionários que tiveram informações vazadas.

Outro fato que deve trazer prejuízo ao estúdio é a sua desvalorização na bolsa de valores. Principalmente após o presidente dos EUA Barack Obama ter feito uma declaração desaprovando o cancelamento da estreia de "A Entrevista".

ANEXO C - Aumentam casos de fraudes com código de boletos bancários – Órgãos de defesa do consumidor alertam que empresas devem arcar com prejuízo

17/09/2014 – O Globo

(https://oglobo.globo.com/economia/defesa-do-consumidor/aumentam-os-casos-de-fraudes-com-codigo-de-boletos-bancarios-13958447)

RIO - O nome da empresa e os dados do cliente estão corretos, mas basta a alteração de alguns números no código de barras para que o consumidor, apesar de ter pago a conta, seja considerado inadimplente pela empresa credora. O golpe, da chamada "gangue do boleto", multiplica-se. Mudam-se números do código de barras, e o pagamento feito é redirecionado para a conta da quadrilha. A fraude levou a Associação Brasileira das Administradoras de Imóveis do Rio de Janeiro (Abadi-Rio) a enviar, ontem, comunicado a todas as suas associadas para que alertem condôminos e inquilinos sobre a fraude, mesmo procedimento que tem sido adotado por instituições de ensino, como a PUC-Rio. A maioria dos casos identificados, até o momento, aconteceu quando o consumidor baixava da internet a segunda via do boletos, mas há registros de interceptação de correspondência e troca da fatura.

— Tivemos relatos de algumas administradoras e, na empresa em que trabalho, houve, há alguns meses, um golpe envolvendo número significativo de inquilinos. Por isso, achamos melhor alertar os clientes, pois sem ter como identificar a fraude, eles só descobrem que o dinheiro não foi para conta do credor quando recebem a notificação de inadimplência. Com essas informações, vão poder conferir antes de pagar. E também estamos vendo como a tecnologia pode evitar a fraude e rastreá-la quando acontece — diz Deborah Mendonça, presidente da Abadi e diretora da administradora Cipa.

Fernando Scheneider, diretor da administradora Apsa, que emite mais de cem mil boletos por mês, apesar de ter somente um caso de fraude confirmado até agora, já enviou comunicado a todos os seus clientes em agosto.

— Sei que o número de casos pode ser maior, pois levamos 60 dias para fazer a cobrança e quem está com a fatura paga, naturalmente, demora mais a responder — avalia Scheneider, que registrou o caso na polícia e orientou o cliente a fazer o mesmo.

Para Carlos Thadeu de Oliveira, gerente técnico do Instituto Brasileiro de Defesa do Consumidor (Idec), alerta das empresas é bem-vindo, mas isso não as isenta de responsabilidade.

— Fraudes sempre vão existir, e cabe à empresa buscar todas as precauções para reduzir esse risco, que seja um selo na fatura ou até entrega personalizada. O consumidor é o último que pode pagar por isso. Mesmo sendo uma fraude de terceiro, esse é um vício oculto do serviço, que o cliente não tem como identificar — avalia.

ANEXO D - Empresas vendem dados do consumidor na internet

05/02/2011 - MARCELINO, Carolina

(http://www.estadao.com.br/blogs/jt-seu-bolso/2011/02/05/empresas-vendem-dados-do-consumidor-na-internet/)

Basta o cliente preencher um cadastro em uma loja para que suas informações sejam repassadas para outras empresas sem autorização. A prática viola a privacidade e abre espaço para indenização caso a pessoa se sinta lesada.

Ao preencher um cadastro em uma empresa, o consumidor confia a ela dados como telefone, endereço, e-mail e algumas vezes até a renda. O que muita gente não sabe é que essas informações estão sendo vendidas sem o seu consentimento. O acesso a esse material é muito fácil, basta entrar em um site de buscas na internet e digitar "mailing + comprar", que em segundos aparece uma lista de empresas especializadas no negócio.

"Essa prática viola a privacidade do consumidor", afirma o advogado especializado em defesa do consumidor e consultor do JT, Josué Rios. E foi assim, desrespeitado, que o empresário Roberto Luiz Ravagnani Watanabe, de 44 anos, se sentiu após ter comprado um apartamento na planta da Eztec Empreendimentos. Quando o imóvel estava para ser entregue, várias lojas de móveis planejados contataram Watanabe pelo telefone celular, oferecendo projetos para o apartamento. "Eles sabiam até o número da minha unidade. Quem me garante que os meus dados bancários também não foram passados a essas pessoas", reclama Watanabe.

O Artigo 5º da Constituição Federal diz que a intimidade e a vida privada do cidadão são invioláveis, assegurando à vítima o direito à indenização pelo dano material ou moral de sua violação. Mas na prática, a privacidade do cliente é invadida sim.