FACULDADE DE TECNOLOGIA ALCIDES MAYA - AMTEC
CURSO TECNOLÓGICO EM REDES DE COMPUTADORES

Pedro Henrique da Silva Teixeira

AUTENTICAÇÃO DE USUÁRIO: GARANTINDO A INTEGRIDADE DOS DADOS ATRAVÉS DE CRIPTOGRAFIA

Porto Alegre, 2019

PEDRO HENRIQUE DA SILVA TEIXEIRA

AUTENTICAÇÃO DE USUÁRIO: GARANTINDO A INTEGRIDADE DOS DADOS ATRAVÉS DE CRIPTOGRAFIA

Trabalho de conclusão apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade de Tecnologia Alcides Maya - AMTC, como exigência parcial para a obtenção do grau de Tecnólogo em Rede de Computadores.

Orientador: Prof Fagner Coin Pereira.

Porto Alegre, 2019

RESUMO

Com a crescente utilização de serviços através da internet, nossa forma de identificação para utilização de determinados serviços são as credenciais de acesso, ou seja, informações de login e senha. Através destes dados, somos autenticados em um servidor que irá nos reconhecer e redirecionar para uma área onde somente o proprietário destes dados deverá ter acesso. Porém, um serviço que requer unicamente informações de texto para autenticação, pode sofrer falhas, como por exemplo, um usuário malicioso ter a posse dos dados e acessar as informações de outro usuário e, podendo assim, agir de forma fraudulenta. Para ter posse destes dados, é possível utilizar uma simples captura de tráfego de rede e analisando os pacotes enviados entre usuário e servidor. Caso não exista nenhum tipo de proteção criptográfica, os dados podem ser lidos em texto claro. Com algum tipo de proteção criptográfica aplicada, é dificultada a visualização destes dados, embora não impossibilitada a visualização dos dados, dependendo unicamente da capacidade computacional para quebrar a criptografia utilizada. Através do método "*Brute Force*" (Força bruta ou tentativa e erro) um algoritmo pode ficar tentando predizer a senha do usuário, desde que se tenha algumas informações sobre a vítima. Sendo assim, é indispensável que seja utilizado algum tipo de criptografia para proteção da informação de login e senha enquanto trafegam pela rede, garantindo assim a integridade daquela informação e de seu proprietário.

Palavras-chave: Autenticação de usuário. Criptografia. Captura de dados. Wireshark, Senhas fracas.

ABSTRACT

With the increasing use of services over the internet, our identification for use of certain services is the access credentials, ie login and password information. Through this data, we are authenticated on a server that will recognize us and redirect us to an area where only the owner of this data should have access. However, a service that requires only text information for authentication may fail, such as a malicious user owning the data and accessing another user's information and thus acting fraudulently. To have possession of this data, it is possible to use a simple capture of network traffic and analyzing packets sent between user and server. If no cryptographic protection is available, the data can be read in plain text. With some kind of cryptographic protection applied, the visualization of this data is difficult, although the visualization of the data is not impossible, depending solely on the computational capacity to break the encryption used. Through the “Brute Force” method, an algorithm can be trying to predict the user's password, provided it has some information about the victim. Therefore, it is essential that some kind of encryption be used to protect the login and password information while traveling the network, thus ensuring the integrity of that information and its owner.

Keywords: User authentication, Cryptography, Data Sniffer. Wireshark. Weak passwords.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

DES	Data Encryption Standard
MD	Message Digest)
NIST	National Institute of Standards and Technology – Instituto Nacional de padrões e Tecnologia
SHA	Secure Hash Algorithm
SSL	Security Socket Layer
TLS	Transport Security Layer

SUMÁRIO

1 INTRODUÇÃO

Com a modernidade e avanços tecnológicos, nosso cotidiano cada vez mais ganha tarefas virtuais utilizando a internet.

Com a internet podemos pagar contas, realizar compras, trocar mensagens com pessoas de qualquer parte do mundo, fazer reuniões, entre outros. Dado o aumento da utilização da internet, e também o desenvolvimento de diversos aplicativos para todo tipo de situação, seja uma rede social ou um site de compras, sempre teremos que nos “associar” a estes sites, na forma de usuários.

Quando nos tornamos um usuário na internet, teremos nossa própria identidade virtual, esta será utilizada pela maioria dos serviços interconectados. Com tantos serviços e sites requisitando um cadastro único para utilização, acabamos por criar diversas senhas diferentes para serviços distintos, e em alguns casos utilizamos a mesma senha apenas para facilitar a fixação desta.

Algo que pode não ser muito claro para muitos usuários é o funcionamento desta etapa de troca de informações entre o servidor e o usuário, onde enviamos as informações de acesso. Com as informações de acesso, o servidor realiza um processo que é chamado de autenticação. A autenticação é o momento onde um sistema nos reconhece e permite acesso ao que desejamos acessar.

Esse acesso pode se dar devido a um plano pré-pago de algum serviço, uma conta de e-mail, ou até mesmo um serviço de banco. Quando nos conectamos a um site, e existe a necessidade de utilizarmos um usuário e senha para acesso, estaremos nos autenticando, uma problemática nesta etapa é quando criamos a senha de acesso, que para facilitar, muitas vezes utilizamos algo simples como a data de aniversário, o próprio nome ou de times de futebol, entre outros.

Quando uma senha não segue um padrão mínimo de complexidade, ou seja, utilizando-se de caracteres alfanuméricos e especiais, a possibilidade de visualização desta senha se torna muito maior do que outra que seguiu o padrão mínimo. Com algum tipo de criptografia, é possível ocultar esta senha e deixar ela o mais segura possível, porém, ao utilizar um padrão de baixa complexidade,

a possibilidade de alcançar a senha verdadeira é extremamente maior em relação ao de uma de alta complexidade.

Morimoto (2014) afirma que a senha de um usuário pode ser o elo mais fraco de um sistema, não importando a quão robusta seja a estrutura e quais políticas de segurança são seguidas.

Neste presente trabalho, será visto como funciona a autenticação de usuários e como manter a integridade da informação através de criptografia, formas de criptografias paras evitar acesso indevido, como a informação pode ser capturada e visualizada através de uma captura de pacotes do tráfego de uma rede de computadores.

1.2 Problema

Garantir a autenticidade de dados transmitidos pelos usuários através do uso de senhas é algo importante. Mas há um grande problema em utilizarmos senhas com baixo nível de complexidade, e principalmente dependendo do algoritmo criptográfico que será utilizado para proteger esta senha posteriormente. De acordo com Moraes (2010) existem dois pré-requisitos básicos no momento em que iremos criar a senha. Devemos levar em consideração qual a criptografia será utilizada para efetuar a troca de informações e também devemos utilizar caracteres alfanuméricos e especiais para composição de uma senha segura. Pois uma grande vulnerabilidade em um sistema é justamente uma senha que será facilmente descoberta.

1.3 Delimitações do Tema

Neste trabalho serão abordados somente os quesitos que tangem a problemática correspondente às boas práticas na criação e manutenção das senhas para autenticação de acesso dos usuários aos seus serviços comuns do cotidiano e quais problemas derivam da falta de atenção na definição de suas senhas em sua complexidade.

O foco desta abordagem é especificamente a complexidade das senhas utilizadas pelos usuários, embora possam existir diversos cenários que poderiam ser analisados para proteção dos acessos entre cliente para servidor e servidor para cliente, ambiente local do usuário, ambiente local do servidor, se são seguidas boas práticas ou não para criação das senhas, se os softwares são

licenciados ou não, se possuem equipamentos de proteção de rede ou até mesmo se são utilizados mínimos cuidados por onde trafegam e onde utilizam dados privados.

Não serão tratadas formas de invasão ou métodos de acesso ilícito a uma rede.

1.4 Objetivos

Os objetivos dividem-se em: geral e específicos.

1.4.1 Objetivo Geral

Através desta pesquisa é demonstrado a questão de segurança no caminho percorrido pelas informações privadas em ambientes virtuais. Serão abordados temas como tipos de criptografias e métodos de captura através dos dados trocados entre usuários e servidores, além de abordar formas de precaução para evitar que esse tipo de captura seja efetivo em visualizar as informações transferidas.

Com isso objetiva-se avaliar prevenções e apresentar formas de manter a integridade da autenticação e principalmente a integridade das informações privadas que são transmitidas em ambientes virtuais.

1.4.2 Objetivos Específicos

- Elucidar sobre a importância da autenticação de usuários.
- Demonstrar a facilidade com que as credenciais dos usuários podem ser capturadas no ambiente virtual e comprometidas devido ao baixo nível de complexidade das senhas.
- Demonstrar como uma criptografia pode ocultar a informação.
- Pesquisar vulnerabilidades relacionadas à senhas não complexas.
- Verificar tipos de ataques e capturas possíveis em senhas não complexas.
- Apresentar maneiras de evitar sites e serviços possivelmente inseguros.

1.5 Justificativa

É necessário que todos os usuários tenham entendimento de como funciona a autenticação de suas contas virtuais, de como suas informações trafegam pela rede mundial de computadores e, principalmente, meios de manter a integridade destes dados. Com um maior entendimento deste assunto por parte dos usuários, é possível mitigar vazamentos de dados e também ações fraudulentas.

Nem sempre são necessários altos investimentos para termos uma boa proteção no mundo virtual, alguns bons hábitos são suficientes para manter credenciais em segurança. Senhas com um nível maior de complexidade são importantes justamente para que seja possível evitar ao máximo qualquer tipo de quebra por algoritmos maliciosos ou até mesmo por outras pessoas que podem visualizar a digitação, por exemplo.

Não importando a maneira de captura dos dados do usuário é um risco enorme, principalmente em situações onde o usuário não compreende como as informações são transmitidas pela rede, de acordo com Stallings (2005) algumas medidas de segurança são necessárias, como o uso de criptografia, para garantirmos a segurança de nossos dados trafegando pela rede.

2 REFERENCIAL TEÓRICO

O referencial teórico da presente pesquisa foi estruturado em seis tópicos, a saber: sobre como funciona o ambiente virtual. Como são elaboradas as políticas de segurança e como podem ser aplicadas. Como funciona a autenticação de usuário perante a uma entidade. Sobre a segurança da informação e seus pilares essenciais e como métodos de criptografia podem auxiliar na proteção dos dados trafegados pela rede.

2.1 Ambiente virtual

Assim como vivemos em um ambiente real, onde é possível visualizar as coisas acontecendo ao redor, também é necessário pensar nas possibilidades de um mundo que não enxergamos, mas fazemos parte dele, chamado de mundo virtual, onde é possível navegar na web, realizar compras, utilizar serviços bancários, entre outros. Segundo Levy (2015) estamos física e virtualmente em lugares distintos graças às técnicas de comunicação e de telepresença.

O mundo real e virtual segue muito semelhante um ao outro, pois ambos possuem criminosos. Com o mundo virtual crescendo devido a sua praticidade, este torna-se cada vez mais parecido com o mundo real.

No meio corporativo possuímos dados estritamente particulares, sejam informações sobre a empresa, novos projetos, métodos de gerenciamento, e até mesmo algum programa que gerencie estes dados, tais como: contas bancárias, dados de funcionários, informações sobre produtos ou serviços, informações sobre clientes e funcionários, inclusive, em um caso mais específico, informações sobre cartões de crédito de clientes.

Conforme Carissimi (2009), para agilizar alguns processos internos e também manter a economia sob eles, diversas empresas utilizam a internet como ferramenta fundamental e indispensável para envio e recebimento de informações com fornecedores de serviços, clientes, filiais, etc. A maior consequência disso é que cada vez mais um maior número de informações sensíveis e confidenciais são armazenadas em computadores e são transmitidas pela internet, o que os torna em potenciais alvos de crimes cibernéticos.

Desta forma, é imprescindível que tenhamos um conjunto de regras visando maior proteção em ambientes virtuais, protegendo dados de terceiros, além de proteger nossos próprios dados. Para tanto, deve-se avaliar os pontos com maior vulnerabilidade dos sistemas, seja corporativo ou particular.

É possível traçar um comparativo entre o ambiente real e o virtual, assim como há a possibilidade de acidentes e ocorrências de crimes, o mesmo ocorre no ambiente virtual. Por acidente, podemos exemplificar quando clicamos em um link desconhecido ou trafegamos por um site falso, e há também a incidência de crimes cibernéticos, desde falsificações, pirataria, roubos de dados, etc.

No ambiente virtual, um ataque não difere muito de um ataque em um ambiente real, pois os itens de valor são os dados do usuário desde *e-mails*, aplicações de banco, entre outros ao contrário de pertences pessoais como relógios, tênis, joias ou qualquer outro objeto que será subtraído do proprietário,

Nem sempre o atacante estará buscando saber qual a rede social favorita da vítima, e a mesma dificilmente descobre no início o que está acontecendo, e somente quando o problema toma uma proporção maior é que se torna perceptível, ou seja, é provável que tenha ocorrido um ato fraudulento em nome do usuário vitimizado.

Conforme afirmado por Bruce Schneier (2004) as ameaças no ambiente virtual refletem as ameaças do ambiente real. Se o peculato é uma ameaça, o peculato digital também é uma ameaça. Se bancos físicos podem ser roubados, os bancos virtuais também podem ser roubados.

Com a invasão de privacidade ocorre o mesmo problema, independentemente de a invasão assumir a forma de um fotógrafo que estará invadindo sua privacidade com a câmera, ou de um hacker que pode espionar sessões de bate-papo privadas ou até mesmo câmeras de dispositivos como smartphones ou notebooks. O crime no ambiente virtual inclui tudo o que se esperaria do ambiente real: roubo, extorsão, voyeurismo, exploração, trapaça ou fraude. Existe até a ameaça de danos físicos: ataques contra o sistema de controle de tráfego aéreo, etc.

2.2 Políticas de Segurança.

A proteção de uma rede de computadores não está apenas na preocupação se a senha do usuário é segura ou não, mas sim, como são tratados os dispositivos físicos. É necessário definir quais dispositivos ficarão encarregados de realizar a proteção e autorização de cada acesso e como serão utilizados os recursos do sistema que foi acessado. É importante o entendimento das formas possíveis que estes dispositivos podem atacar ou invadir uma rede.

Conforme Carvalho (2005) as políticas de segurança são compostas de um conjunto de padrões e regras sobre o que deverá ser executado de modo a garantir a proteção aos serviços e informações relevantes de uma determinada empresa, para assim assegurar a confidencialidade, integridade e disponibilidade dos dados.

É notável que a evolução dos dispositivos tecnológicos está se tornando cada vez mais rápida e eficiente, o que pode ser benéfico ou maléfico dependendo da situação em que é aplicada. Em paralelo com um novo sistema de segurança sempre haverá alguma vulnerabilidade a ser explorada e, na maioria dos casos os fabricantes ou desenvolvedores não informam tais vulnerabilidades até o momento da correção, tornando necessário um regimento de regras para diminuir a incidência de problemas relacionados a estas vulnerabilidades, “Uma política de segurança da informação tem como propósito fornecer orientação e apoio às ações de gestão de segurança. [...]” (CARVALHO, 2005, apud SÊMOLA, 2003)

Através das políticas de segurança, sendo elas internas ou externas, é possível mitigar alguns processos que logicamente tornam o ambiente virtual menos seguro. Para Stallings (2005) as políticas de segurança nos trazem um ambiente favorável para que medidas de segurança pré-estabelecidas sejam extremamente funcionais, seguras, autenticas e otimizadas, posteriormente tornando-se parte da rotina diária do usuário no seu ambiente corporativo ou doméstico.

No ambiente corporativo, se o administrador do sistema não realizar um breve levantamento de vulnerabilidades com as devidas projeções para os ataques mais comuns e devastadores, principalmente quais e quantos ataques o sistema poderia suportar sem que houvesse um *downtime* rigoroso, ou quanto

tempo levaria para deixar toda a estrutura afetada online novamente, dificilmente este ambiente seria mantido sem falhas.

Ao fazer uso das Políticas de Segurança e elaborando documentações específicas, além de implementá-las e auditá-las, o administrador do sistema poderá aprimorar suas defesas e identificar de forma ágil qualquer situação anormal com seu ambiente. Haverá um período de resposta muito mais ágil para resolução de qualquer incidente.

Para que isso aconteça em ambiente corporativo, é imprescindível contar com a colaboração da equipe envolvida, bem como afirma Carvalho (2005), que para uma política de segurança ser bem-sucedida, é essencial que exista um grupo envolvido para sua divulgação e auditoria. Esta equipe deve saber bem suas atribuições e estar motivada para manter o comprometimento com o trabalho de segurança a ser executado.

Devemos sempre manter determinadas políticas de segurança, não apenas no ambiente corporativo, mas no ambiente doméstico também, evitando assim que ocorram capturas de nossos dados ou atos fraudulentos. Mesmo quando acontecem grandes incidentes de segurança com empresas fornecedoras de serviços, como e-mail, redes sociais e etc., podemos estar protegidos por nossas próprias medidas de segurança com o simples hábito de trocar de senha periodicamente.

Segundo Bruce Schneier (2007) é melhor assumir que todos os concorrentes são melhores do que se é esperado. Reconheça que a ciência e tecnologia poderão fazer coisas que são impossíveis para os tempos atuais. Dê a si mesmo uma boa margem para errar, sempre mantenha o máximo de cautela com as medidas de segurança do ambiente virtual.

2.3 Autenticação de Usuário

Autenticar um usuário, tem como premissa validar a identificação de um usuário perante a uma entidade para acesso a um sistema ou recursos específicos providos por um servidor, essa etapa após a identificação é chamada de autorização. Conforme Carissimi et al. (2009), para que essa autenticação e autorização ocorram, é necessário que o usuário passe por um procedimento de

verificação, realizado de forma que apenas usuários legítimos possuam o devido acesso.

Para esta validação de uma identidade, ou seja, autenticar um usuário, pode-se utilizar os seguintes itens: algo que o usuário sabe; algo que o usuário tem; algo que o usuário é. No que diz respeito a “Algo que o usuário sabe”, compreende as senhas utilizadas, chaves criptografadas ou PIN. Já o que o “Usuário possui” é relativo a itens físicos, como *tokens*, *smart cards* e cartões.

logo que o “Usuário é” abrange as características físicas, e são realizadas as identificações através do reconhecimento de íris, reconhecimento facial ou biometria.

Em nosso mundo particular é possível pensar que ataques contra os dados privados dificilmente ou nunca aconteceriam com nossas contas de e-mail, redes sociais, e até mesmo em um cenário pior, aplicativos de banco ou cartão de crédito.

Conforme Carissimi et al. (2009), uma vez que a autenticação do usuário é confirmada pelo sistema o acesso às informações é concedido e a grande falha neste processo é que o sistema não tem capacidade de reconhecimento para ter certeza de que o usuário é de fato o proprietário daquelas informações que foram inseridas.

Este é um problema comum quando é utilizado apenas o método de autenticação por algo que o usuário sabe. Desta forma é totalmente possível enganar o sistema autenticador, pois existem diversas formas de adquirir a senha de um usuário.

De maneira a aumentar o nível de segurança na autenticidade dos usuários, pode-se utilizar a combinação de métodos de autenticação. Um exemplo comum é o banco onde o cliente dispõe de um cartão (algo que ele possui) e de uma senha (algo que ele sabe), neste caso, temos a autenticação de dois fatores. Atualmente já existem casos, onde além destes fatores, pode-se ser exigido também a biometria (algo que o usuário é).

Os dados que o usuário possui, bem como o exemplo dado anteriormente, são suscetíveis ao compartilhamento de forma intencional, no momento em que o usuário empresta seu cartão de crédito para um terceiro utilizar. O mesmo acontece no ambiente virtual, onde um usuário fornece seus dados (usuário e

senha) para outra pessoa utilizar para efetuar alguma compra online, ou seja, o sistema não reconhece que o usuário não é ele de fato.

Referente ao ambiente virtual, onde o nome do usuário e senha talvez sejam fornecidos para que um terceiro para uma ação específica, deve-se também levar em consideração o pior caso, hipoteticamente até o momento, se ocorrer qualquer situação atípica que gere um conflito direto entre as partes, como por exemplo o usuário se apropriar das credenciais que lhe foram providas para outros acessos indevidos anteriormente restritos a este.

Caso nesta empresa hipotética não existam políticas bem definidas e aplicadas, neste momento qualquer ação que podem ocasionar registros deletados ou alterados. O registro destas ações estaria em nome do cedente das credenciais e não do autor que se aproveitou da situação.

Neste momento esta ação indevida realizada de forma fraudulenta fere um dos pilares da segurança da informação que é a Integridade, ao mesmo tempo que os outros desmoronam junto, pois além de não termos plena certeza da veracidade das informações registradas, não sabemos quais informações foram vazadas, alteradas ou apagadas, e principalmente, quem realmente alterou aquelas informações.

Logo, é essencial que existam regras de segurança, um nível de privilégios específicos para cada tipo de usuário, e que as regras sejam periodicamente auditadas, pois o primeiro passo para mitigar um problema como este, é tratar as causas constantemente.

Essa situação se repete no meio particular, quando deixamos alguém utilizar nossos dados por alguma razão, neste caso deve ser levado em consideração quem cria, implementa e audita as políticas, pois de certa forma, o próprio usuário é administrador do seu sistema. Logo as políticas de segurança não se aplicam apenas para empresas.

Não importa a robustez da infraestrutura de uma empresa, o elo mais fraco sempre estará em uma das pontas. Conforme afirmado por Morimoto (2010) a questão das senhas é outro tema importante, já que elas são o ponto fraco de qualquer sistema, no momento que é dito que a senha é pessoal e intransferível, isso deveria realmente ser levado a sério, evitando assim atos fraudulentos.

2.4 Segurança da informação

Segurança da informação compete à proteção de dados essenciais de uma determinada corporação ou pessoa, ou seja, suas informações.

Definimos como informação todo dado ou conteúdo digital que é produzido e que tenha valor para a entidade, seja uma empresa, pessoa, governo, etc.

As prioridades primárias da segurança da informação são conhecidas como CID, que é a sigla para: Confidencialidade, Integridade e Disponibilidade. Ao longo dos anos foram adicionadas mais questões para se levar em conta, e assim se tornaram 5 os pilares da segurança da informação. Foram acrescentados: Autenticidade e Irretratabilidade (ou não repúdio).

Abaixo estão descritos cada um deles:

Confidencialidade: Garante que as informações sigilosas estarão protegidas, para tanto pode-se adotar o uso de criptografia de dados, também compete a confidencialidade as restrições de acesso á determinados dados.

Integridade: É essencial que a informação transmitida não sofra nenhuma alteração sem que seja autorizado pelo emissor. É necessário assegurar que as informações não serão alteradas em seu armazenamento, tráfego ou processamento, ou seja, que sejam íntegras.

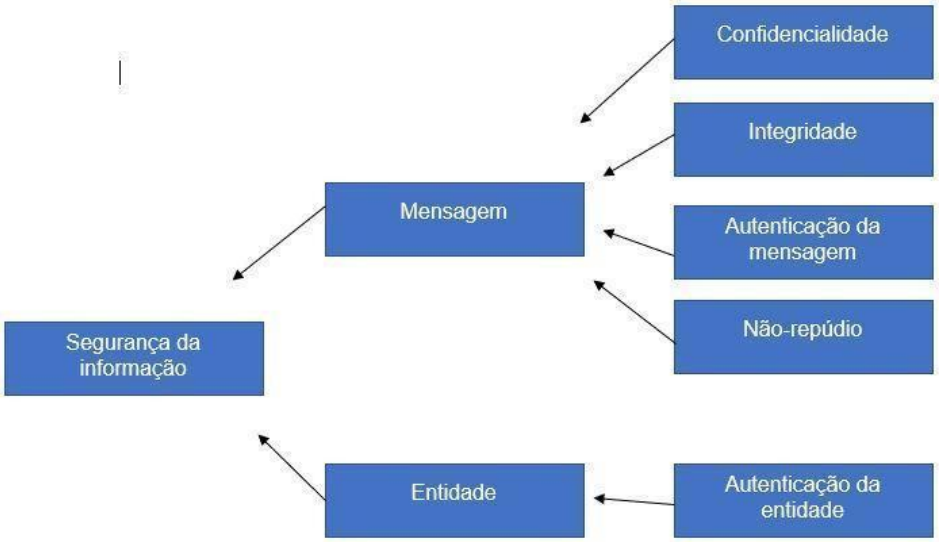
Disponibilidade: Toda informação deve estar sempre disponível ao usuário, ou seja, quando ele quiser acessar, ela deverá, estar disponível desde Softwares, hardwares, dados e conexões devem ser oferecidos aos usuários, para que eles tenham acesso às informações. Logicamente respeitando as premissas das políticas de segurança.

Autenticidade: Atesta a veracidade de uma informação, garantindo que sejam provenientes de uma fonte confiável

Irretratabilidade (ou não repúdio): Para impedir que algum usuário negue a autoria de determinada informação, garantindo assim a sua autenticidade. Assim, nem a fonte ou receptor poderão contestar qualquer transação de dados realizada por eles.

Já na Figura 1, conforme Forouzan (2008), estão descritos como podem ser aplicados.

Figura 1- Fluxo da Segurança da Informação



Fonte: Forouzan (2008).

Com o crescimento dos meios de comunicação através da internet, vem se tornando cada vez mais comum e indispensável na vida das pessoas o uso dos serviços providos online. Utilizar a internet para compartilhar dados, fazer compras online com cartão de crédito e consultar o extrato bancário, são apenas algumas, entre muitas, atividades realizadas online. Milhares de indivíduos utilizam dados confidenciais para acessar estes serviços. Todo o conceito de segurança da Informação foi padronizado pela norma ISO/IEC 17799:2005.

De acordo Carissimi et al. (2009), essas atividades online em sua maioria acabando fazendo com que os indivíduos deixem rastros de seus acessos pelo mundo virtual, criando um determinado padrão de comportamento, favorecendo assim a ocorrência dos crimes cibernéticos.

Para segurança virtual, não bastam apenas protocolos específicos para segurança na navegação, ou até mesmo uma criptografia específica, pois nem sempre os sites por onde navegamos estão seguros.

Mesmo que a empresa mantenedora do site em questão se preocupe fortemente com a segurança, ainda assim nosso próprio meio de acesso pode estar comprometido caso não tenhamos os devidos cuidados com nossos equipamentos e softwares utilizados.

Logo, é indispensável aceitar que assim como cuidamos por onde andamos, horários e locais que podemos ou não transitar evitando alguns riscos, também devemos pensar desta forma para nossa vida virtual.

2.4.1 Criptografia

Muitas das diversas formas de proteger informações e redes de computadores são baseadas em criptografia. Como afirmam Carissimi et al. (2009), a palavra criptografia vem do grego que significa escrita (*graphos*) secreta (*crypto*), significando que se o indivíduo não tiver conhecimento delas, seria impossível compreender uma determinada informação.

Usar criptografia aumenta a segurança do sistema e das comunicações em rede. Criptografia é a ciência de ocultar informações. Ela possui uma larga e rica história que precede o tempo do uso dos computadores. Devido ao forte uso de algoritmos matemáticos, a criptografia foi migrada facilmente para o ambiente da informática.

O principal uso da criptografia em um sistema, é codificar os dados para assim ocultar as informações de usuários não autorizados, e decodificar (descriptografar) os dados para usuários autorizados. Esse processo de criptografar e descriptografar, utiliza algoritmos matemáticos especiais para cada tarefa, estes algoritmos são conhecidos como: Cifras criptográficas.

Cifras criptográficas exigem um dado específico, tanto para criptografar quanto para descriptografar, que são conhecidas como chaves. Existem dois tipos de chaves, simétrica e assimétrica.

Conforme Negus (2014) a criptografia de chave simétrica, que também é conhecida como de chave secreta ou chave privada, criptografa um texto simples utilizando uma cifra codificada uma vez apenas. E apenas com a utilização da mesma chave é possível descriptografar esses dados. É uma forma rápida de criptografia, com a única desvantagem de haver a necessidade do envio da chave quando outra pessoa precisar ler os dados.

Ainda em seu texto, Negus (2014) fala sobre a criptografia de chave assimétrica, ou de chave pública. A criptografia de chave pública opera com duas chaves. Existe uma chave privada que somente o usuário a que criou o arquivo

a possui e uma chave pública que é de conhecimento de todos os usuários que querem se comunicar com este usuário.

Quando um usuário enviar uma mensagem cifrada, a criptografia é feita utilizando-se da chave pública, e para conseguir ler o conteúdo, o receptor irá utilizar sua chave privada e sua chave pública em conjunto para que a mensagem seja decodificada. Estas chaves estão matematicamente relacionadas, de forma que somente com as duas é possível decodificar a mensagem.

2.4.2 Padrões Criptográficos

Com o passar do tempo, diversos padrões foram criados, alguns já puderam ser totalmente decifrados e acabaram em desuso.

Conforme Negus (2014) o tamanho da chave (bits) está relacionado de forma direta com a facilidade com que pode ser quebrada, um exemplo é a cifra DES com chave de 56 bits que poderia ser decifrada facilmente, enquanto uma cifra com 256 bits levaria trilhões de anos para quebrar com tentativa e erro (força bruta). O que ditaria isso seria apenas a capacidade computacional do sistema utilizado e se o sistema está configurado para entender quando um ataque de força bruta está acontecendo e como poderia mitigar o mesmo.

Para os dois diferentes tipos de criptografias como já vimos anteriormente, temos simétricas que correspondem às chaves privadas e as criptografias assimétricas que correspondem às chaves públicas.

Alguns são padrões ainda utilizados nos dias de hoje, e abaixo podemos visualizar uma breve explicação das técnicas de encriptação mais comuns, segundo o autor Diaa *et al* (2008).

DES: (*Data Encryption Standard*), Foi o primeiro padrão de encriptação a ser recomendado pelo *NIST (National Institute of Standards and Technology* – Instituto Nacional de padrões e Tecnologia*)*. DES possuí uma chave com tamanho e bloco de 64 bits, mas somente 56 são utilizados e os outros 8 bits são utilizados para verificar a paridade e depois são excluídos. Desde tempos atrás diversos ataques e métodos de para quebra do DES foram registrados, tornando-o assim uma cifra de bloco insegura.

3DES É a cifra DES aprimorada. Os dados são codificados até 48 vezes com 3 diferentes chaves de 56 bits antes do processo de criptografia estar concluído.

RC5 é uma cifra de bloco de 64 bits e com uma chave de tamanho variável entre 32, 64 ou 128 bits e utiliza as mesmas chaves até 2048 bits para criptografar e descriptografar.

Blowfish Cifra de bloco, criptografa os dados em blocos de 64 bits utilizando as mesmas chaves entre 32 e 448 bits para criptografia e descriptografia.

AES também conhecida como Rijndael, é uma cifra de bloco e criptografa os dados em blocos de 128, 192 e 256 bits.

RC6 é uma cifra de bloco, derivada do RC5. O RC6 propriamente tem um bloco equivalente a 128 bits e suporta chaves de tamanho de 128, 192 e 256 bits.

Também existe a função de Hash criptográfico, ou apenas Hash. O Hash é uma sequência de bits que tem como objetivo identificar um arquivo, isso significa que se realizarmos um processamento num arquivo será gerado um Hash que é único, e dessa forma, alcançamos a garantia da integridade. Utilizando o Hash também temos a propriedade da unidirecionalidade onde o caminho de volta não é possível.

Além disso, com o Hash não há a necessidade de chaves e, temos a garantia da consistência, pois se introduzirmos a mesma mensagem de Hash teremos exatamente o mesmo Hash sendo gerado. Por fim, o Hash também nos oferece as propriedades de aleatoriedade e unicidade onde nunca temos a mesma mensagem de Hash para diferentes mensagens.

Dentre os tipos de Hash temos o MD (*Message Digest*) que é composto pelos MD2 (lento e com saída de 128 bits), MD3, MD4, MD5 que é amplamente utilizado atualmente. O criador do MD5, Ron Rivest (1992), declara que a dificuldade de produzir duas mensagens idênticas é de 2^64 operações e que para reproduzir uma mensagem é de 2^128 operações.

O segundo principal algoritmo de hash utilizado atualmente é o SHA (*Secure Hash Algorithm*) projetada pela NSA publicadas como um padrão do governo Norte-Americano. Também existem os tipos SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512.

Cada algoritmo é diferenciado pelo tamanho da mensagem de entrada suportada, tamanho do bloco, tamanho da palavra, tamanho do *Message Digest* e a segurança do algoritmo.

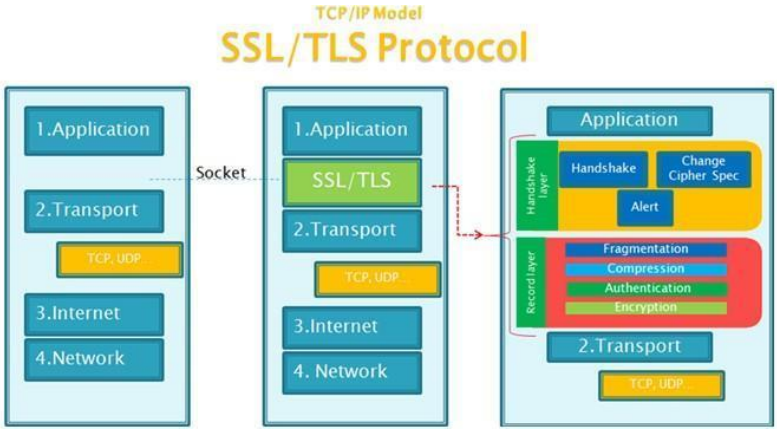
No SHA-1 sucessora do MD5, é utilizada em uma grande variedade de aplicações e protocolos de segurança, incluindo TLS, SSL, PGP, SSH, S/MIME e IPSec. Tanto o SHA-1 quanto o MD5 têm vulnerabilidades comprovadas, sendo sugerido que o SHA-256 ou superior a este seja utilizado para tecnologia crítica. A primeira função desta família foi publicada em 1993 e foi oficialmente chamada de SHA. Dois anos mais tarde foi publicado o SHA-1 que é o primeiro sucessor do SHA.

Segundo Kurose e Ross (2007) a troca pelo SHA-1 foi necessária para garantir a segurança dos dados, pois com o uso do MD5 o resumo da mensagem retornava apenas 128 bits, enquanto o SHA produz um resumo de 160 bits, além de ser um padrão federal.

É importante saber também que é possível ter uma proteção na parte mais baixa da rede, onde trataremos a criptografia não apenas em protocolos de aplicações, mas sim em sockets de segurança e no transporte da informação.

Uma proteção pelo socket de segurança, também chamada de SSL(*Security Socket Layer*) é utilizada como base do protocolo da camada de segurança de transporte ou simplesmente TLS (*Transport Security Layer*), que foi inicialmente desenvolvida pela Netscape, é um protocolo criado para projetar criptografia dos dados e autenticação entre um servidor web e o cliente que o está acessando. Conforme Kurose (2007) os protocolos SSL e TLS não estão limitados apenas para aplicações Web. A camada SSL pode ser visualizada como uma camada intermediária entre a aplicação e o transporte como pode ser visto na Figura 2. No lado da origem, o SSL recebe os dados, criptografa e os envia para um socket TCP no destinatário. No lado do destinatário o SSL lê o socket TCP, descriptografa os dados e os direciona para uma aplicação.

Figura 2 - SSL/TLS no Modelo TCP/IP



Fonte: Vircom (2011)

A autenticação de um servidor por SSL permite a confirmação da identidade do servidor por uma unidade certificadora, ou seja, possui um certificado digital válido isso permite que o navegador autentique o servidor antes que o usuário possa inserir qualquer tipo de dado, como por exemplo usuário e senha, ou até mesmo informações financeiras.

Já a autenticação de um cliente por SSL permite que um servidor confirme a identidade de um usuário, semelhante a autenticação do servidor, o usuário possui certificados também gerados por uma unidade certificadora. Isso é um importante, pois, se um banco precisa enviar informações para um usuário, o banco precisa saber a identidade do mesmo.

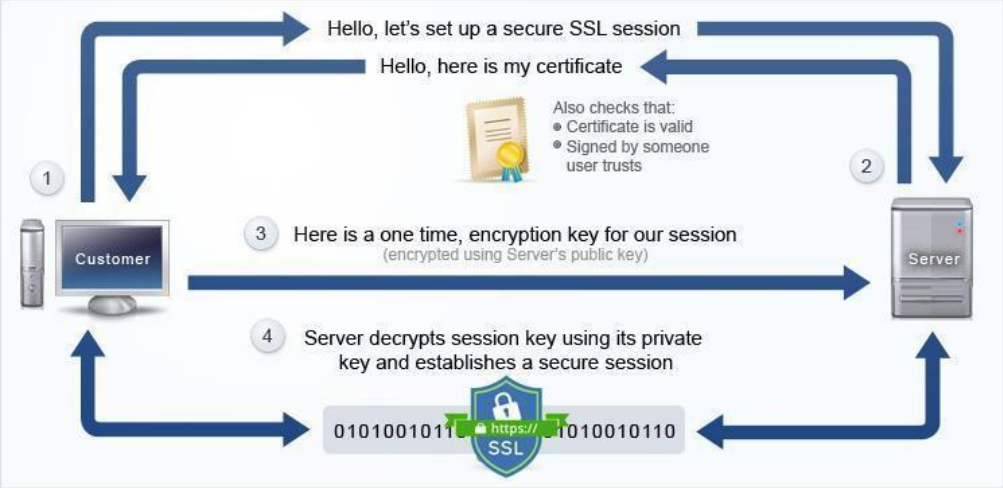
O SSL funciona basicamente de uma forma mútua entre dois pontos de comunicação, neste caso cliente e servidor, pode ser superficialmente resumido da seguinte forma:

1. Cliente A consulta a página segura do servidor B,
2. O servidor B envia seu certificado ao cliente A;
3. O cliente A extrai a chave pública do servidor B;
4. O cliente A gera uma chave simétrica aleatória e a criptografa usando a chave pública do servidor B;
5. O servidor B extrai a chave simétrica.

Toda troca de mensagens entre cliente e servidor nesta sessão serão feitas através desta chave gerada e compartilhada entre os dois, o que fará com que seja garantida a integridade dos dados.

Podemos ver este passo-a-passo exemplificado na Figura 3:

Figura 3- Como o SSL Funciona



Fonte: Toshost (2019)

Apesar da segurança aplicada com o protocolo SSL/TLS, o mesmo possuí uma certa problemática bem simples, o protocolo SSL cumpre sua função e garante a integridade dos dados, mas não pode garantir que o servidor ou estabelecimento é realmente confiável e que irá realizar a transação normalmente, e também não garante que o cliente acessando o servidor ou fazendo compras é quem realmente deve ser, no caso, se o cartão não é clonado, devido á isso podemos ter fraudes mesmo com criptografia aplicada.

3 METODOLOGIA

Para este trabalho foi realizado uma pesquisa bibliográfica utilizando-se de diversos autores especializados para tratamento dos temas sobre criptografia, autenticação de usuários e integridade dos dados.

Foi realizado um cenário prático utilizando-se de pesquisa explicativa onde foram feitas as respectivas demonstrações de como é possível reaver os dados trafegados pela rede através de uma simples captura de dados.

4 ATAQUES A SENHAS

Após verificar como funcionam alguns métodos de criptografia e descriptografia, autenticação por meio de senhas, distribuição de chaves de

segurança e principalmente sobre a importância de uma informação integrada serão analisados como ocorrem os ataques a este tipo de informação.

De acordo com Kurose e Ross (2007) é comum que um ataque seja precedido de uma coleta de informações, assim como no mundo real, bandidos “vigiam o ponto” onde pretendem atacar, a razão é óbvia, para que o ataque seja o mais assertivo possível e com a menor probabilidade de serem pegos.

O mesmo ocorre no ambiente virtual, um invasor certamente faria um levantamento de informações, buscando saber quais os sistemas operacionais são utilizados, qual o endereçamento padrão da rede, quais serviços são providos naquela rede, assim causando um menor impacto quando concluir a invasão. Chamamos este tipo de coleta de informações de mapeamento.

Para o cenário prático, será focado apenas a questão de captura de senhas, independente do uso de criptografia e alguns casos devido a sua simplicidade, ou seja, senhas com poucos caracteres, apenas com números ou letras, em uma situação extrema contendo informações reais da pessoa que a possui, sendo nome de familiar, nome de cachorro, nome de amigos, time de futebol favorito, data de aniversário, etc.

Existem pessoas que possuem informações tão importantes que podem ser vítimas de um ataque, podendo este ser a rede social, ao e-mail, ou até mesmo fraudes com os dados da vítima ou do aplicativo “inofensivo” do banco que é usado para acessar informações financeiras.

De acordo com Bruce Schener (2004) é lógico que quem sofre mais com essa prática são os governos, afinal, já ouvimos falar sobre vários vazamentos de informações estritamente sigilosas atualmente se protegem contra esta prática, que possui uma comunidade que cresce cada vez mais.

Será efetuado uma captura dos dados transmitidos de um ponto A para um ponto B, buscando encontrar o padrão de criptografia utilizada, e também como poderemos reaver a mensagem que foi enviada entre os dois pontos.

4.1 Configurações

As seguintes configurações e programas serão utilizados para a aplicação prática e gerando os resultados apresentados posteriormente:

- Placa-mãe: ASrock H81M-HG4

- Processador: Intel Core I5-4440
- Ram: 16Gb(2x8) em dual-channel
- Disco: SSD Kingston SHFS37A120G
- Sistema Operacional: Windows 10 Build 1903
- Software de Virtualização: Oracle Virtual Box V. 6.0.6 r130049
- VM-1
- Windows 7 SP 1.

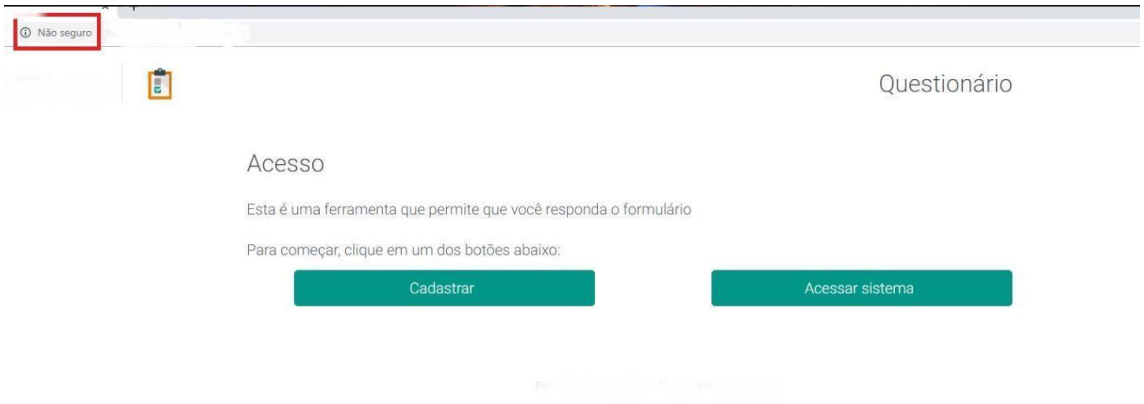
4.1.1 Captura de dados com Wireshark:

Este tipo de prática, é conhecido como “*sniffing*”, algo como “cheirar” os pacotes. É importante ressaltar o seguinte sobre a captura de dados que será realizada, não serão levados em consideração os métodos de invasão pelo qual foi-se possível acessar o conteúdo transmitido. Apenas serão analisadas as trocas de mensagens entre cliente e servidor, onde um servidor utilizará HTTP (sem criptografia) e outro HTTPS (com criptografia).

Não foram utilizados parâmetros para a captura, somente ao término foi utilizado um filtro para localizar o pacote que carregava as informações desejadas.

Os sites não serão divulgados para evitar problemas autorais. Inicialmente iremos para um acesso qualquer a um servidor com HTTP apenas. Nota-se que o próprio navegador já demonstra o site como inseguro devido ao uso de HTTP conforme figura 4.

Figura 4 - Captura de pacotes 1



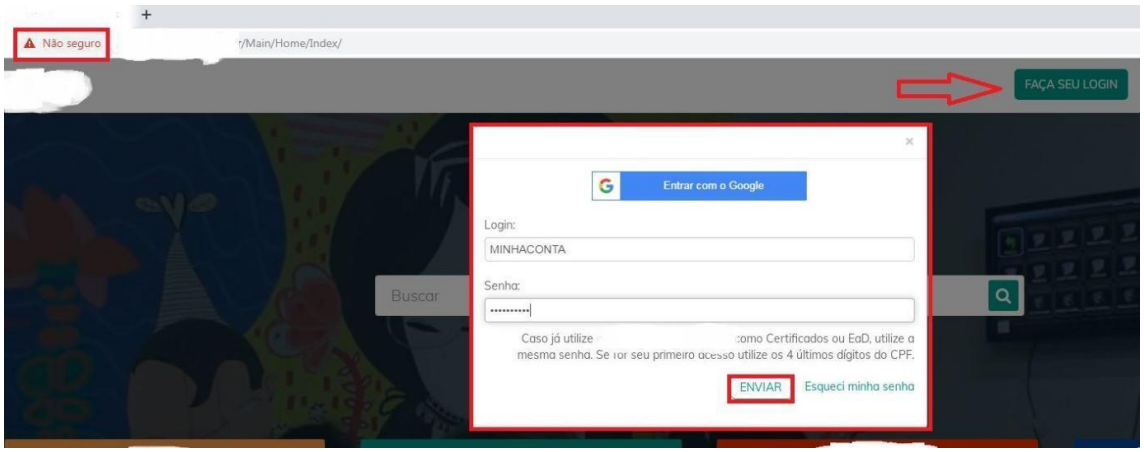
Fonte: Elaborado pelo autor

Após clicarmos em “Acessar Sistema”, somos redirecionados para outra página, está também em HTTP. Ainda constando o aviso sobre o acesso não estar criptografado, clicamos em login, e um pop-up abre solicitando as credenciais para acesso como visto na figura 5, que neste teste foram utilizados como informações:

usuário: MINHACONTA

senha: MINHASENHA

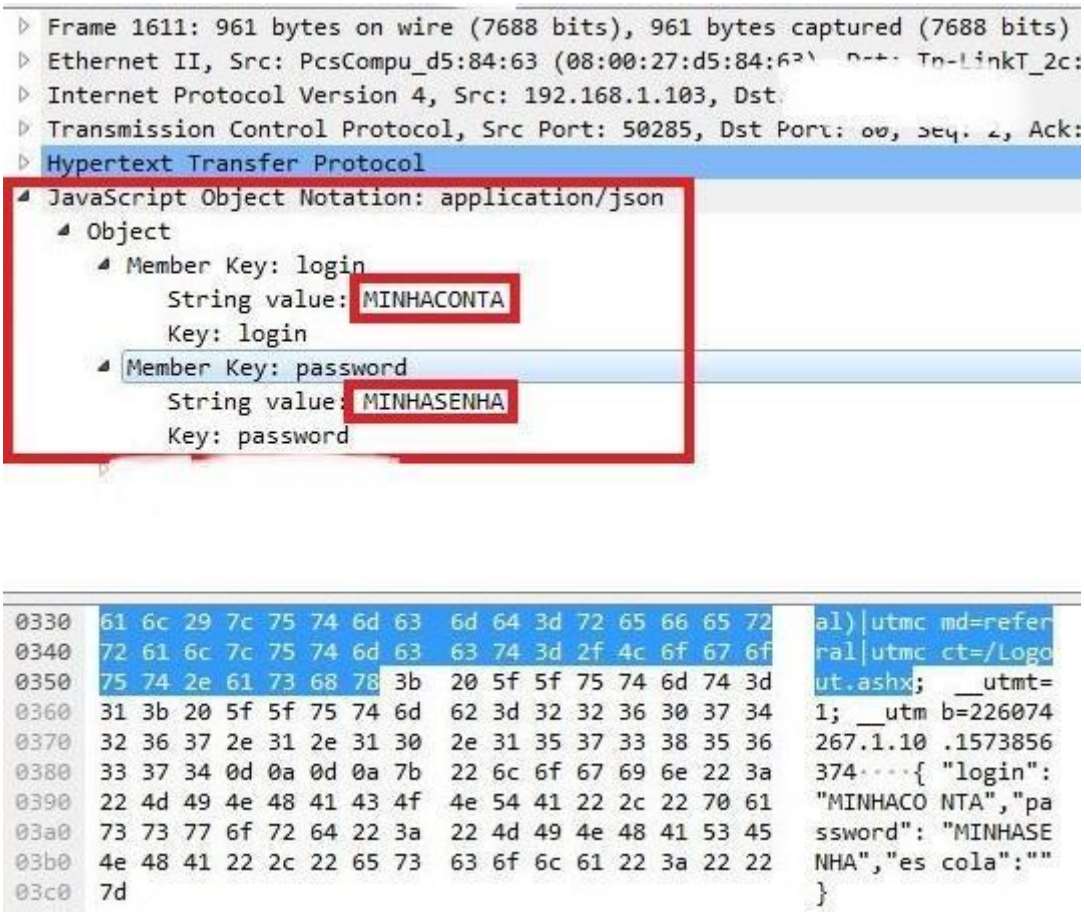
Figura 5 - Captura de pacotes 2



Fonte: Elaborado pelo autor

Partindo para a tela de captura dos dados pelo programa Wireshark, podemos verificar que os campos referentes a usuário e senha estão em texto claro, na Figura 6.

Figura 6 - Captura de pacotes 3



Fonte: Elaborado pelo autor

Como é possível verificar, é uma página web que solicita autenticação por parte do usuário, mas não utiliza nenhum tipo de criptografia para garantir a autenticidade do mesmo.

Alguns navegadores ao clicar no cadeado próximo ao endereço do site/servidor alertam o que pode ocorrer quando não há proteção à conexão que irá ser estabelecida como pode ser visto na Figura 7.

Figura 7 - Captura de pacotes 4

Fonte: Elaborado pelo autor

Para o segundo momento do cenário prático aplicado, será verificado como funciona a troca de mensagens entre um servidor que utiliza HTTPS para garantir a autenticidade da conexão.

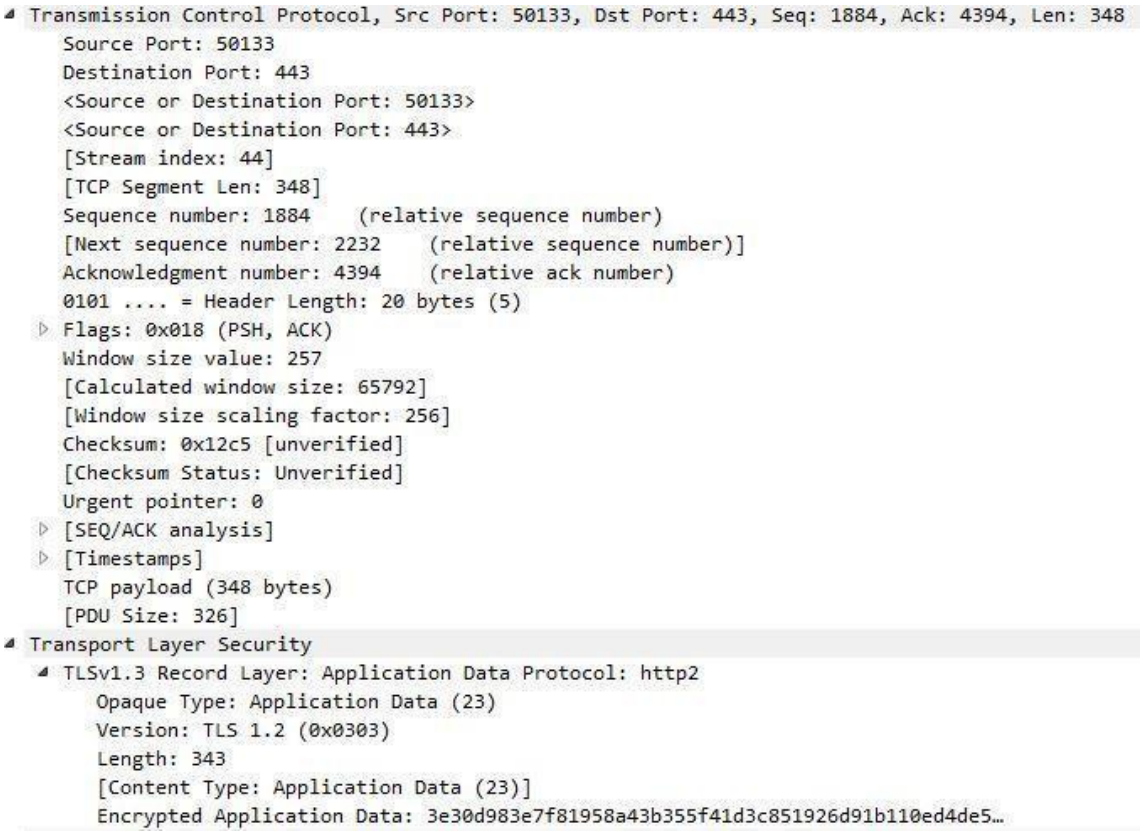
Para este exemplo, tentamos acessar uma conta do servidor de e-mails do Google, o Gmail. É possível notar no campo de endereço que o site começa com “https” ao contrário do anterior que era apenas “http”, o “S” significa *security* (segurança), para esta tentativa de acesso usaremos as seguintes informações:

Usuário: minhaconta

Senha: minhasenha

Na tela do Wireshark utilizado para a captura, podemos notar que a troca de mensagens ocorreu da forma como especificada anteriormente, utilizando o SSL/TLS para criptografar a troca de informações entre cliente e servidor, conforme pode ser visto na Figura 8.

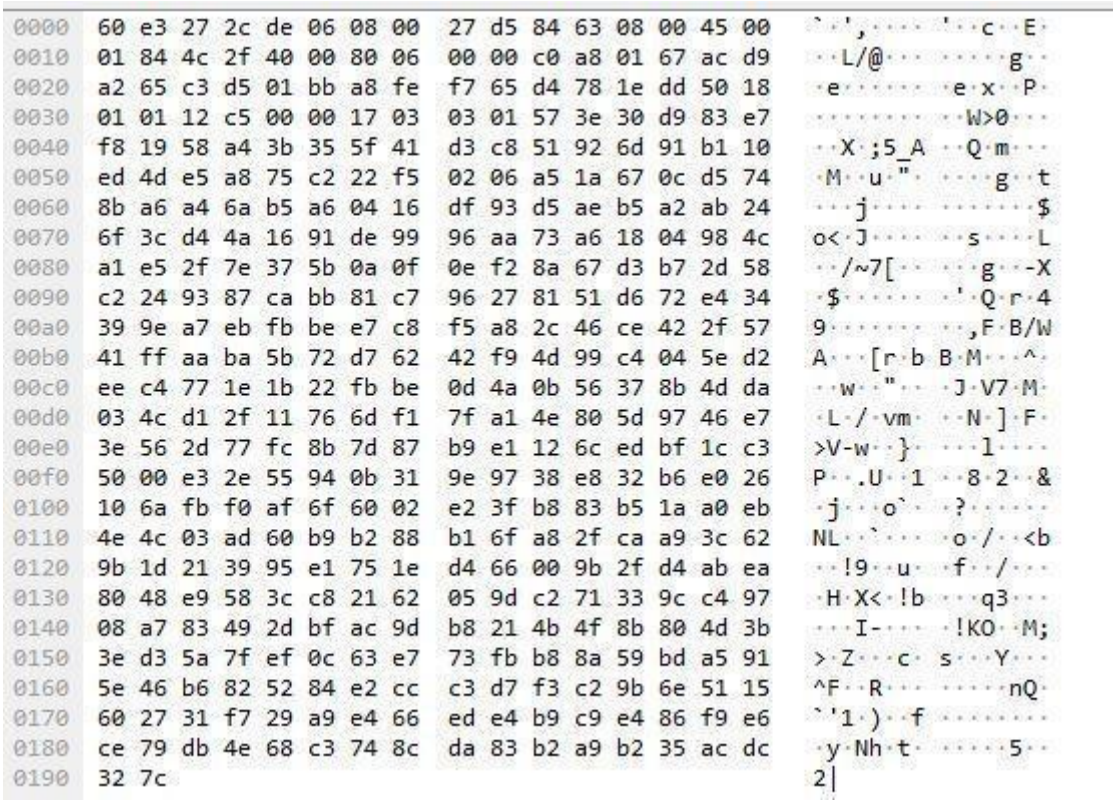
Figura 8 - Captura de pacotes 5



Fonte: Elaborado pelo autor

Já com relação ao esperado do conteúdo desta transação de dados, não é possível entender nada das informações contidas nos pacotes, pois está criptografado com as chaves trocadas pelo cliente e servidor conforme visto na Figura 9.

Figura 9 - Captura de pacotes 6



```
0000  60 e3 27 2c de 06 08 00  27 d5 84 63 08 00 45 00   `·',···· '··c··E·
0010  01 84 4c 2f 40 00 80 06  00 00 c0 a8 01 67 ac d9   ··L/@··· ·····g··
0020  a2 65 c3 d5 01 bb a8 fe  f7 65 d4 78 1e dd 50 18   ·e····· ·e·x··P·
0030  01 01 12 c5 00 00 17 03  03 01 57 3e 30 d9 83 e7   ········ ··W>0···
0040  f8 19 58 a4 3b 35 5f 41  d3 c8 51 92 6d 91 b1 10   ··X·;5_A ··Q·m···
0050  ed 4d e5 a8 75 c2 22 f5  02 06 a5 1a 67 0c d5 74   ·M··u·"· ····g··t
0060  8b a6 a4 6a b5 a6 04 16  df 93 d5 ae b5 a2 ab 24   ···j···· ·······$
0070  6f 3c d4 4a 16 91 de 99  96 aa 73 a6 18 04 98 4c   o<·J···· ··s····L
0080  a1 e5 2f 7e 37 5b 0a 0f  0e f2 8a 67 d3 b7 2d 58   ··/~7[·· ···g··-X
0090  c2 24 93 87 ca bb 81 c7  96 27 81 51 d6 72 e4 34   ·$····· ·'·Q·r·4
00a0  39 9e a7 eb fb be e7 c8  f5 a8 2c 46 ce 42 2f 57   9····· ··,F·B/W
00b0  41 ff aa ba 5b 72 d7 62  42 f9 4d 99 c4 04 5e d2   A···[r·b B·M···^·
00c0  ee c4 77 1e 1b 22 fb be  0d 4a 0b 56 37 8b 4d da   ··w··"·· ·J·V7·M·
00d0  03 4c d1 2f 11 76 6d f1  7f a1 4e 80 5d 97 46 e7   ·L·/·vm· ··N·]·F·
00e0  3e 56 2d 77 fc 8b 7d 87  b9 e1 12 6c ed bf 1c c3   >V-w··}· ···l····
00f0  50 00 e3 2e 55 94 0b 31  9e 97 38 e8 32 b6 e0 26   P···.U··1 ··8·2··&
0100  10 6a fb f0 af 6f 60 02  e2 3f b8 83 b5 1a a0 eb   ·j···o`· ·?·····
0110  4e 4c 03 ad 60 b9 b2 88  b1 6f a8 2f ca a9 3c 62   NL··`··· ·o·/··<b
0120  9b 1d 21 39 95 e1 75 1e  d4 66 00 9b 2f d4 ab ea   ··!9··u· ·f··/···
0130  80 48 e9 58 3c c8 21 62  05 9d c2 71 33 9c c4 97   ·H·X<·!b ···q3···
0140  08 a7 83 49 2d bf ac 9d  b8 21 4b 4f 8b 80 4d 3b   ···I-··· ·!KO··M;
0150  3e d3 5a 7f ef 0c 63 e7  73 fb b8 8a 59 bd a5 91   >·Z···c· s···Y···
0160  5e 46 b6 82 52 84 e2 cc  c3 d7 f3 c2 9b 6e 51 15   ^F··R··· ·····nQ·
0170  60 27 31 f7 29 a9 e4 66  ed e4 b9 c9 e4 86 f9 e6   `'1·)··f ········
0180  ce 79 db 4e 68 c3 74 8c  da 83 b2 a9 b2 35 ac dc   ·y·Nh·t· ·····5··
0190  32 7c                                             2|
```

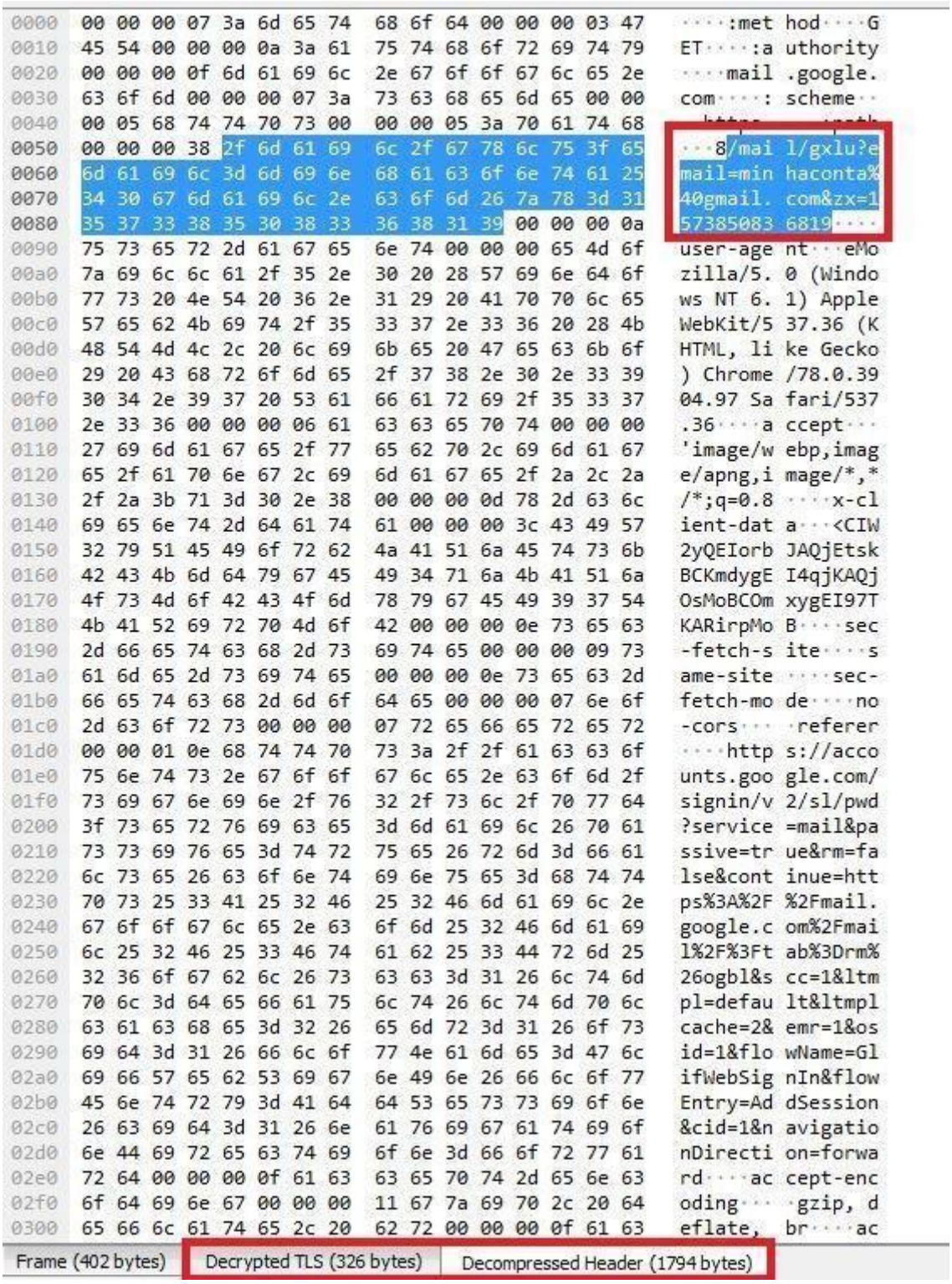
Fonte: Elaborado pelo autor

Porém, é possível capturar essa troca de chaves entre cliente e servidor, utilizando o próprio sistema operacional pelo seguinte caminho (Anexo 1).

Propriedades do computador > Configurações avançadas do sistema > aba Avançado > Variáveis de Ambiente > nova variável > e criar com o nome “SSLKEYLOGFILE” e direcionar para onde este arquivo deverá ir quando criado.

Após acessar a página, um arquivo deverá ser criado no local pré-definido anteriormente, lá estarão as chaves trocadas para aquela sessão. Depois de realizar o acesso e a captura dos dados, é possível inserir este arquivo no programa wireshark para que ele realize a descriptografia das informações trocadas entre cliente e servidor, deixando acessível as informações visto na Figura 10.

Figura 10 - Captura de pacotes 7



Fonte: Elaborado pelo autor

Para uma melhor visualização, utilizaremos outra imagem, conforme apresentada na Figura 11 a seguir:

Figura 11 - Captura de pacotes 8

Fonte: Elaborado pelo autor

Mesmo com a utilização de uma criptografia, ainda assim foi possível reaver parte do conteúdo transmitido. No arquivo de chaves, existem diversas chaves que foram trocadas entre cliente e servidor, porém somente uma é compatível com a descriptografia, o que começa a dificultar a ação de reaver a informação completa, mas uma parte dela já é possível ter, que é o usuário a ser utilizado para o acesso.

O próximo passo seria buscar uma senha que encontra-se junto com o usuário durante a transmissão, pois mesmo criptografada, caso desejado pelo atacante é possível reaver aquela informação.

Com a tecnologia aplicada para proteção ponto-a-ponto temos uma boa proteção, porém é muito simples reaver este fluxo de dados trocados entre clientes e servidores, bastando apenas saber quem é o alvo e buscar entender o seu comportamento, e posteriormente ter uma busca mais assertiva e assim concluindo o propósito de reaver toda a informação e utiliza-lá como bem entender, seja para fraudes ou outras ações.

4.2 Quebrando uma criptografia

Anteriormente foi possível verificar que é muito provável visualizar o que é transmitido pela rede, não necessariamente entendemos o que está escrito, pois é uma linguagem que não conhecemos, porém, em um momento que

soubermos qual o tipo de cifragem utilizada, seria possível reaver todo o conteúdo da mensagem.

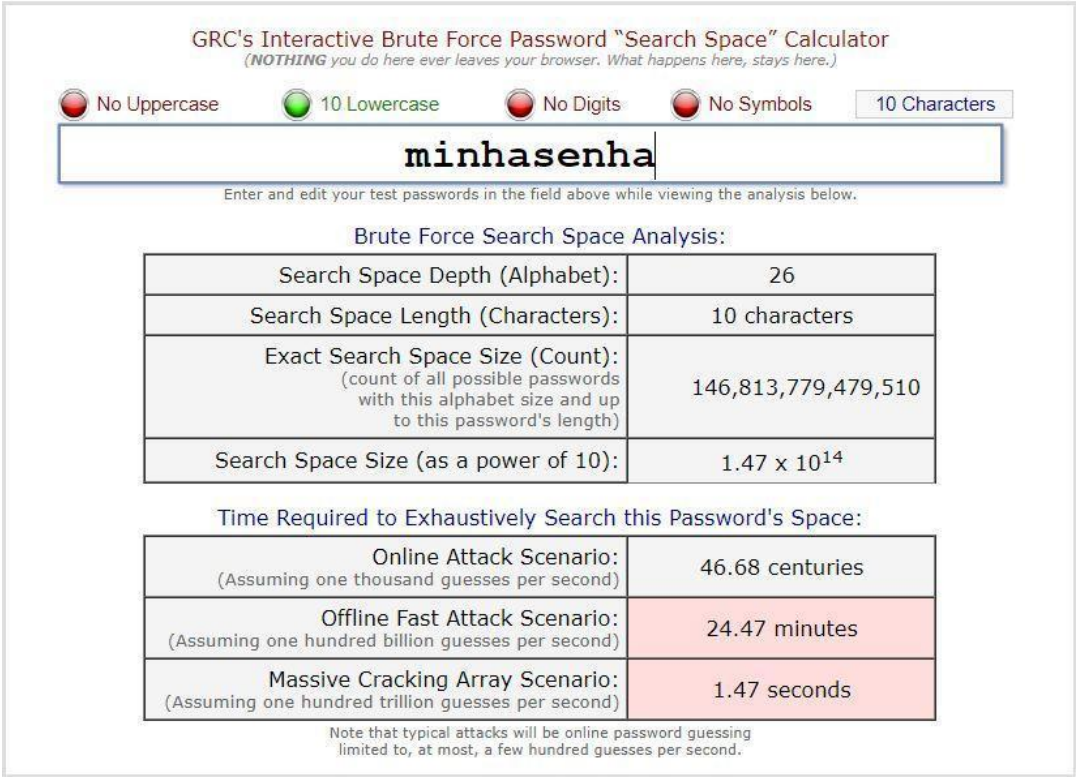
Existe um tipo de ataque chamado de Man In The Middle (Homem no meio), onde o atacante já faz parte da rede local, e fica no meio do tráfego das mensagens, podendo alterar e re-enviar a mensagem. Neste caso, seria necessário saber quais os métodos de cifragem estão sendo utilizados, e também qual a importância destas mensagens.

Para verificarmos a velocidade com que se pode quebrar uma senha, utilizaremos o site <https://www.grc.com/haystack.htm> como base de exemplo:

Conforme comentado por Negus (2014), é muito importante verificar como anda a qualidade das senhas do cotidiano, inclusive, o nome do tópico site é: “Quão Grande é sua pilha de feno? E o quão bem escondida está sua Agulha!”. Usaremos os exemplos anteriores como senha, que foram: “minhasenha” e “MINHASENHA”.

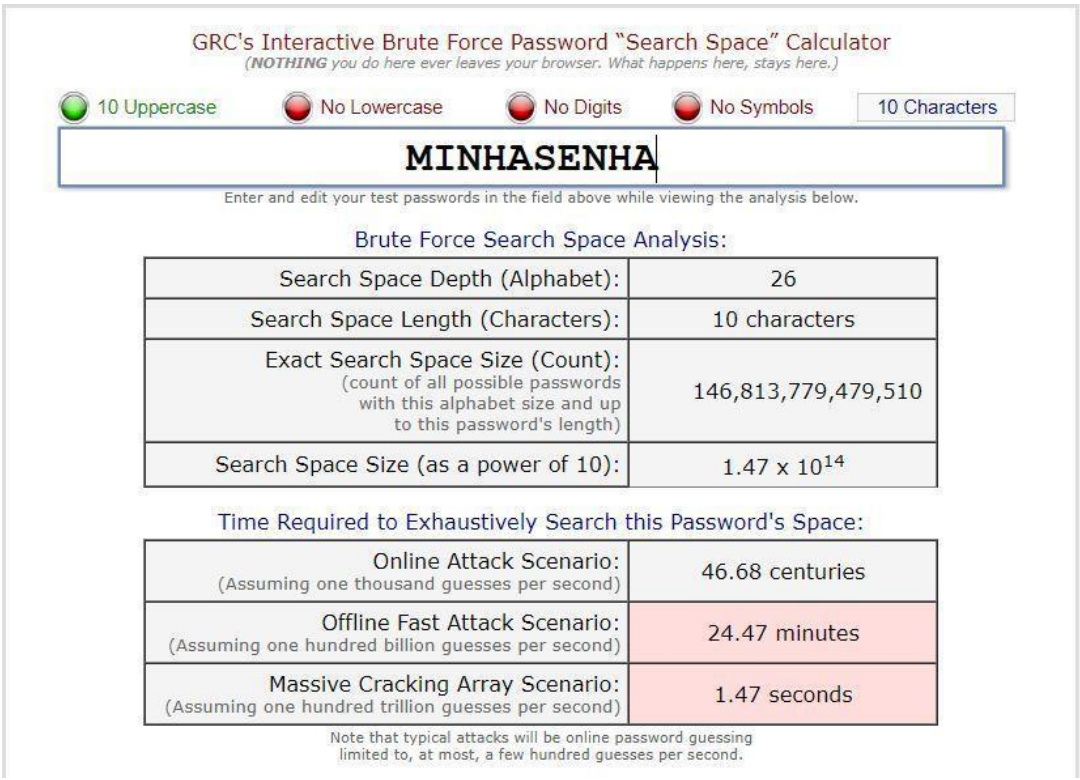
Como podemos verificar nas Figura 12 e 13, levariam apenas 1.47 segundos para reaver esta senha, é claro que com um poder computacional gigantesco e um fluxo massivo de tentativas de quebra, o que pode-se evitar com configurações por parte dos servidores, onde é possível colocar um temporizador para cada tentativa de acesso, mitigando assim ataques de força bruta, também constam os possíveis tempos para um cenário offline, em um caso onde o atacante obteve acesso ao arquivo de senhas de determinado servidor, com tempo de 24.47 minutos, e em um cenário mais tranquilizante levariam 46.68 séculos para reaver esta simples senha, o tempo indifere se a senha está em maiúscula ou minúsculas, o período de quebra seria o mesmo.

Figura 12 - Captura de pacotes 9



Fonte: Gibson Research Corporation (2016)

Figura 13 - Captura de pacotes 10

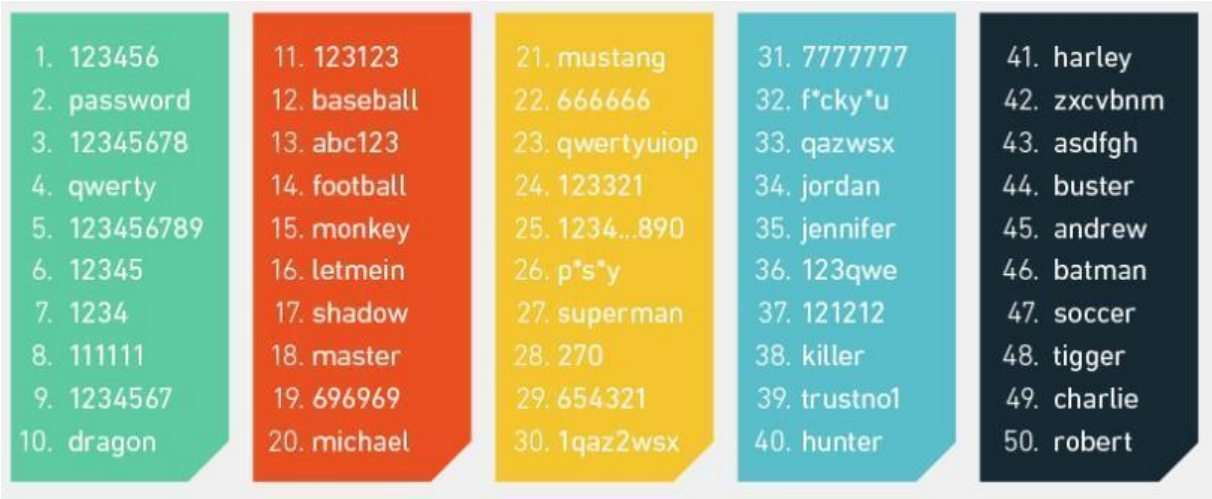


Fonte: CORPORATION, Gibson Research (2016)

4.2.1 Problemas com senhas simples em todo mundo

Conforme foi possível ver em capítulos anteriores, apesar do uso de uma criptografia, ainda foi possível reaver uma parte da informação, no caso do cenário anterior, o usuário, requerendo logicamente a senha para conclusão da autenticação. Este problema não se aplica a um país ou outro, conforme podemos ver na Figura 14.

Figura 14 - As 50 senhas mais comuns no mundo



Fonte: WpEngine (2015)

Já em 2017, uma pesquisa realizada pelo site WeLiveSecurity, demonstrou os seguintes dados sobre as 10 senhas mais utilizadas:

Tabela 1 - 10 Senhas mais utilizadas

123456
Password
123456789
12345678
12345
111111
1234567
Sunshine
Qwerty

Iloveyou

Fonte: WeLiveSecurity (2017)

Como é possível ser visualizado, existem sequências numéricas, nomes de animais, nomes próprios, nomes de carros, nomes de super-heróis, diversas palavras que existem em dicionários, entre outros.

Existem também os padrões que podem ser gerados através de sequências executadas seguindo uma linha reta, seja horizontal ou vertical diretamente no teclado, como podemos ver na Figura 15, estas são as combinações padrão encontradas em 10 milhões de senhas, segundo pesquisa do site WpEngine (2015) conforme Figura 15:

Figura 15 - 20 senhas mais comuns no mundo

1. QWERTY	11. ASDFASDF
2. QWERTYUIOP	12. QAZWSXEDC
3. 1QAZ2WSX	13. ASDFGHJKL
4. QAZWSX	14. Q1W2E3
5. ASDFGH	15. 1QAZXSW2
6. ZXCVBNM	16. 12QWASZX
7. 1234QWER	17. QWEASDZXC
8. Q1W2E3R4T5	18. MNBVCXZ
9. QWER1234	19. A1B2C3D4
10. Q1W2E3R4	20. ADGJMPTW

Fonte: WPENGINE (2019)

Para termos um exemplo sobre nosso país, possuímos os seguintes dados de quais são as senhas com maior utilização pelos usuários brasileiros, e segundo Almeida (2018), abaixo estão as 10 senhas mais utilizadas no Brasil:

Tabela 2 - 10 Senhas mais utilizadas no Brasil

Sucesso
Brasil
Felicidade
Qwerty
Musica
Estrela
Linkedin
Rental
Família
Assinantes

Fonte: Almeida (2018)

4.3 Protegendo suas senhas

Como pôde ser visto anteriormente, as senhas são componentes básicos na segurança de qualquer sistema informatizado e devido a isso se torna o recurso com maior número de ataques.

Segundo Negus (2014), métodos de força bruta são utilizados para obter acesso a um sistema, tentativas com informações populares produzem ótimos resultados. Se podemos acessar qualquer mecanismo de busca e pesquisarmos por “senhas comuns” então os atacantes também podem fazer o mesmo.

Para escolhermos uma boa senha, existem algumas premissas a serem seguidas como por exemplo: Não deve ser fácil de adivinhar, não deve ser comum ou estar vinculada de alguma forma a vida pessoal do portador.

Em sua obra, Negus (2014) provê a seguintes regras que não devemos utilizar para criar uma senha:

1. Variações do seu login nem seu próprio nome.
2. Palavras que estejam no dicionário.

3. Nomes próprios de qualquer tipo.
4. Endereço, telefones, sobrenomes ou nomes de animais de estimação.
5. Linhas contínuas de padrões do teclado.

Para garantir uma maior proteção, Negus (2014) recomenda as seguintes regras para serem levadas em consideração no momento de elaborar uma nova senha:

1. Pelo menos 15 caracteres.
2. Letras Minúsculas.
3. Letras Maiúsculas.
4. Números.
5. Caracteres especiais, Ex.: !, #, $, @, <,>, (,), -, =, +.

Também é possível a utilização de pequenos truques para criar uma boa senha. A seguinte frase formaria uma senha complexa o bastante:

MeuCarroVermelhoDe2018TemProblemasComOEspelhoDoCarona!

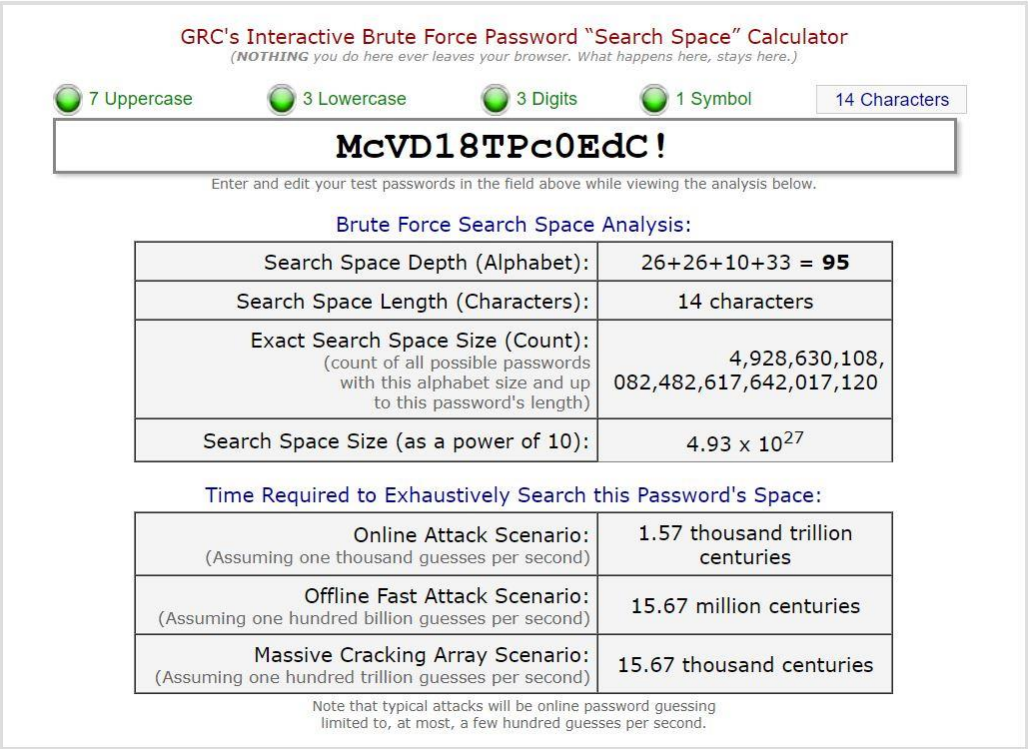
McVD18TPc0EdC!

A parte interessante desta forma de criar uma senha, é que só fará algum sentido para o portador, desta forma poderíamos carregar esta mesma mensagem em um pedaço de papel na carteira ou deixar salvo no celular, ou computador, pois haveriam diversas formas de combinações para transformar essa sentença em uma senha.

Esta acaba sendo uma das formas para criar uma senha forte o bastante para resistir a ataques e também fácil de ser carregada por seu portador, logicamente levaria algum tempo para memorizar tudo.

Podemos ver abaixo na figura 16 é muito mais forte, em comparativo com a senha utilizada no cenário prático e “quebrada” conforme a figura 13.

Figura 16 - Senha com padrões de complexidade



GRC's Interactive Brute Force Password "Search Space" Calculator

(*NOTHING* you do here ever leaves your browser. What happens here, stays here.)

7 Uppercase | 3 Lowercase | 3 Digits | 1 Symbol | 14 Characters

McVD18TPc0EdC!

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	14 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	4,928,630,108, 082,482,617,642,017,120
Search Space Size (as a power of 10):	4.93×10^{27}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.57 thousand trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	15.67 million centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	15.67 thousand centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Fonte: CORPORATION, Gibson Research (2016)

Como pode ser visto na figura 16, a senha ficou extremamente forte, mesmo se combatida com um ataque massivo para quebra-lá.

5 CONCLUSÃO

Não há dúvida de que a conscientização se faz necessária para a solução deste problema com autenticação de usuários. Sendo um cuidado maior por parte do usuário com o entendimento de como funciona, mesmo que parcialmente, um fluxo de dados entre destino e origem.

A utilização de senhas para autenticação é algo extremamente comum para qualquer serviço online hoje em dia. Como pôde ser visto, alguns autores observaram este problema com autenticação muitos anos atrás, porém, ainda assim é uma situação muito atual.

Alguns serviços já dispõem da opção de autenticação por mais de um meio, como por exemplo a biometria. Muitos usuários não têm entendimento de como esses métodos funcionam e como são úteis para garantir a autenticidade das informações.

Desta forma se tornam dependentes da qualidade da própria senha juntamente com o tipo de segurança aplicada pelo provedor de serviço.

No momento em que não se utiliza nenhuma proteção nos dados, estes se tornam passíveis de vazamentos de informações e fraudes.

Se faz necessário uma preocupação com relação aos caracteres selecionados na hora de definir uma senha, pois com um poder computacional elevado é possível quebrar uma senha fraca em milésimos de segundos, como exemplificado no cenário prático apresentado no capítulo 4.1.1. Utilizando a mais simples forma de captura de dados, sem nenhum recurso especial ou filtros tecnológicos foi possível reaver a informação de forma simplificada, inclusive uma parte dela mesmo ao utilizar proteção criptográfica.

Em paralelo ao problema, podemos ver que muitos usuários não se importam com a complexidade de suas senhas, como pôde ser visto nos dados apontados no capítulo 3.3. Tão breve os usuários consigam compreender a importância que ele carrega nesta corrente de informações, logo ele poderá começar a se proteger e também poderá divulgar sites falsos ou reconhecer quando estiver em um lugar arriscado para os seus dados.

Têm se tornado comum alguns sites e provedores de serviços exigirem de forma clara quando o usuário vai realizar o cadastro que é preciso uma senha forte, e deixam específicos os pré-requisitos a serem atingidos para criar a senha

para acesso. Com o conteúdo deste trabalho é possível entender o motivo desta preocupação.

Para concluir este estudo, como usuários devemos partir do cuidado geral com as páginas e serviços na internet que são acessados e como são solicitados os dados para autenticação, se é um site que possui um certificado válido e se é confiável acessar aquele servidor.

Todavia é importante cuidar principalmente os meios que são utilizados para acessar determinados serviços. Um exemplo são as redes disponíveis em cafeterias, aeroportos, bares, etc. Não é possível saber se há algum controle de segurança virtual nestes locais, ou se até mesmo, o meio de acesso já não está comprometido propositalmente.

É interessante entender como estes tipos de captura funcionam justamente para evitar o acesso aos dados dos que utilizarem aquele meio de acesso que pode ser um computador, notebook, tablet ou qualquer item que se conecte à rede e que seja possível acessar a internet.

Existem várias outras formas de proteção aos dados, além das citadas neste presente trabalho. Podem ser encontrados diversos outros métodos utilizados pelas empresas, este assunto é uma sugestão de futura evolução deste mesmo conteúdo, tratando assuntos como controles de invasão e controles de acesso.

REFERÊNCIAS

ALMEIDA, FELIPE. **Infográfico: Perfil da senha do brasileiro** Disponível em: **<** https://blog.axur.com/pt/infografico-perfil-da-senha-do-brasileiro >

BERGHEL, Hal. **The SCDOR Hack: Great Security Theater in Five Stages.** Disponível em: <https://icitech.org/wp-content/uploads/2017/01/ICIT-Analysis-Security-Theatre.pdf>. Acesso em 05 de setembro de 2019.

CARISSIMI, Alexandre; GRANVILLE, Lisandro; ROCHOL, Juergen. **Séries livros didáticos informática ufrgs – Redes de Computadores**. 1.ed. São Paulo: Artmed Editora AS, 2009.

CARVALHO, Luciano Gonçalves de. **Segurança de Redes**. 1.ed. Rio de Janeiro: Editora Ciência Moderna, 2005.

COMER, Douglas. **Redes de computadores e internet:** abrange transmissão de dados, ligações inter-redes, web e aplicações. 4. ed. Porto Alegre: Bookman, 2007.

CORPORATION, Gibson Research. **How Big is your Haystack?** And how well hidden is your needle? Disponível em: <https://www.grc.com/haystack.htm>. Acesso em 15 de novembro de 2019.

DIAA, Salama Abdul Elminaam; HATEM, Mohamed Abdul Kader; MOHIE, Mohamed Hadhoud. **Performance Evaluation of Symmetric Encryption Algorithms**. Disponível em: <https://www.researchgate.net/profile/Mohiy_M_Hadhoud/publication/50996668_Performance_Evaluation_of_Symmetric_Encryption_Algorithms/links/0deec51b8a2cddd0b2000000.pdf>. Acesso em 24 de novembro de 2019.

DONOHUE, Brian. **Hash:** o que são e como funcionam. Disponível em: <https://www.kaspersky.com.br/blog/hash-o-que-sao-e-como-funcionam/2773/>. Acesso em 15 de novembro de 2019.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 4.ed. São Paulo: AMGH editora, 2008.

JAROSZEWSKI, Przemek. **How to get good seats in the security theater**. Disponível em: <https://pt.slideshare.net/PrzemekJaroszewski/how-to-get-good-seats-in-the-security-theater>. Acesso em 05 de Setembro de 2019.

LÉVI, Pierre. **O que é o Virtual?**. 1. ed. São Paulo: Editora 34, 1996.

MORIMOTO, Carlos. **Redes Guia Prático.** 2. ed. Porto Alegre: Sul Editores, 2010.

NEGUS, Christopher; BRESNAHAN, Christine. **Linux A Bíblia:** o mais abrangente e definitivo guia sobre Linux. 8.ed. Rio de Janeiro: Altas Book, 2014.

RIVEST, R. **The MDS Message-Digest Algorithm,** 1992. Disponível em: <https://tools.ietf.org/html/rfc1321>. Acesso em 17 de novembro de 2019.

SCHNEIER, Bruce. **Secrets and Lies**. Kindle. ed. Indiana: Wiley, 2004.

SCOTT, James; SPANIEL, Drew. **The Cyber Security Show Must Go On.** Disponível em: <http://www.berghel.net/col-edit/out-of-band/mar-13/oob_3-13.pdf>. Acesso em 05 de setembro de 2019.

SHNEIER, Bruce. **Don't fear the TSA cutting airport security. Be glad that they're talking about it. Disponivel em:** <https://www.washingtonpost.com/news/posteverything/wp/2018/08/07/dont-fear-the-tsa-cutting-airport-security-be-glad-that-theyre-talking-about-it/?utm_term=.33ae51250549 >. Acesso em 05 de setembro de 2019.

SHNEIER, Bruce.**In Praise of Security Theater.** Disponivel em: <https://www.schneier.com/blog/archives/2007/01/in_praise_of_se.html> Acesso em 27 de Setembro de 2019.

SHNEIER, Bruce.**The Vulnerabilities Market and the Future of Security**. Disponivel em: <https://www.schneier.com/blog/archives/2012/06/the_vulnerabili.html> Acesso em 27 de Setembro de 2019.

SOUSA, Lindeberg Barros de. **Tcp/ip & Conectividade em Redes** 5. ed. São Paulo: Érica, 2009.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados**: teoria e aplicações corporativas. 5.ed. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Elsevier: Campus, 2003.

TEAM, News Top500. **Poder Computacional.** Disponível em: <https://www.top500.org/news/top500-becomes-a-petaflop-club-for-supercomputers/>. Acesso em 15 de novembro de 2019.

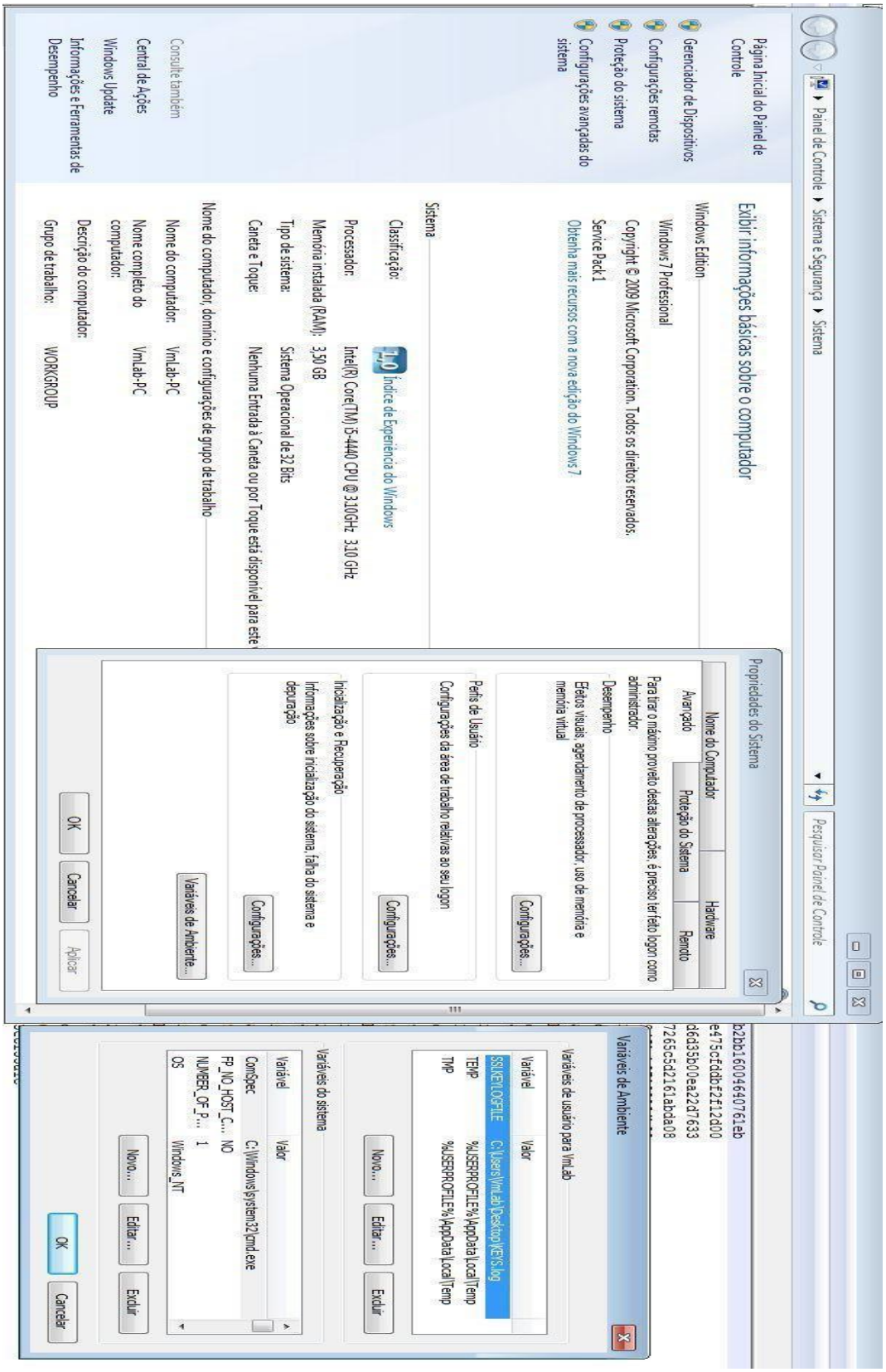
TOSHOST LTDA. **What is SSL and how it works?** Disponível em: <https://toshost.com/a/what-is-ssl-why-useful-ssl>. Acesso em 17 de novembro de 2019.

VIRCOM. **How to use SSL/TLS to Secure Your Communications:** The Basics. Disponível em: <https://www.vircom.com/blog/how-to-use-ssltls-to-secure-your-communications-the-basics/>. Acesso em 17 de novembro de 2019.

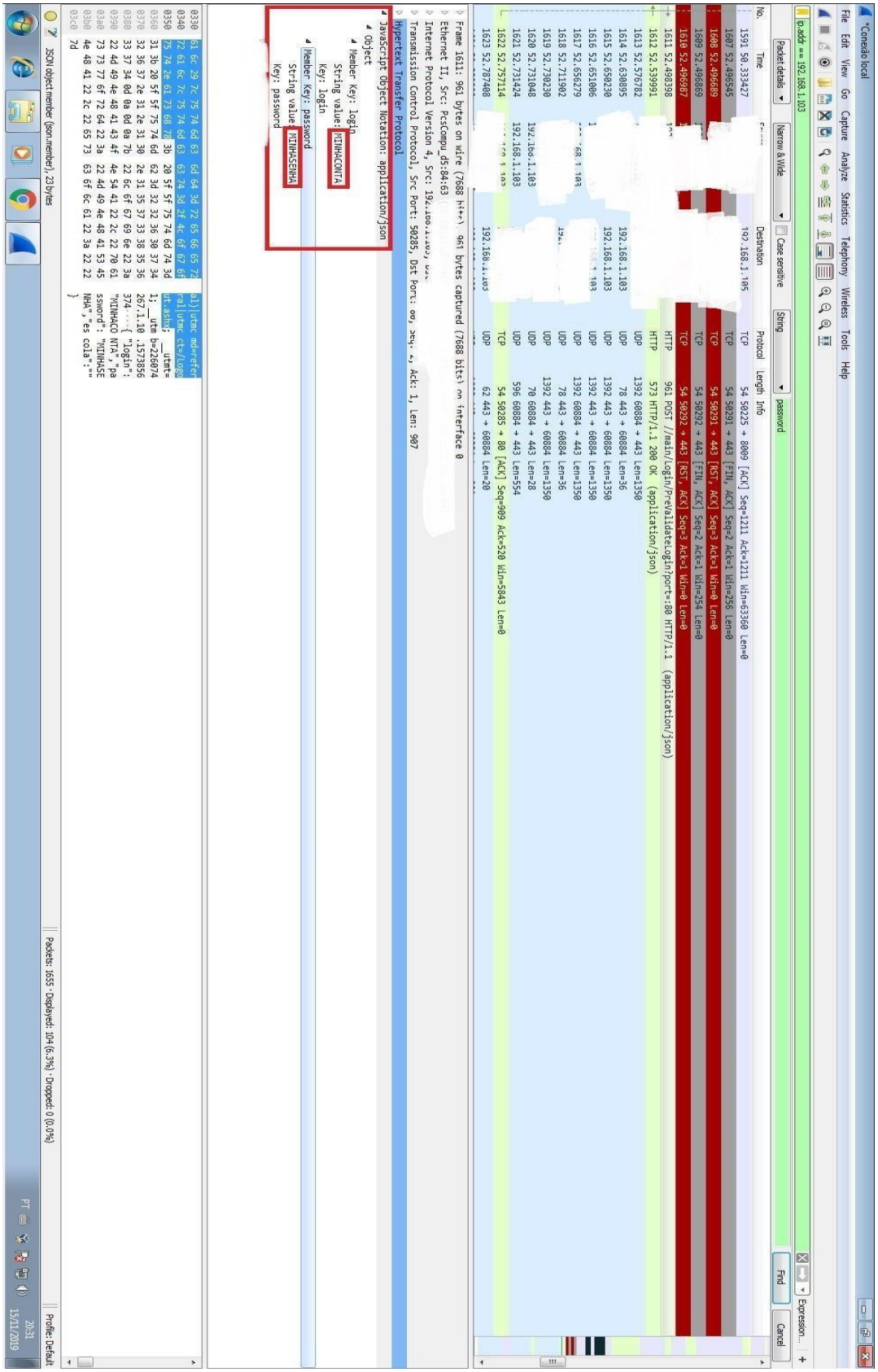
WELIVESECURITY. **AS 25 SENHAS MAIS POPULARES EM 2018** Disponivel em: <https://www.welivesecurity.com/br/2018/12/21/as-25-senhas-mais-populares-de-2018/ >. Acesso em 24 de novembro de 2019.

WPENGINE. **Unmasked: What 10 million passwords reveal about the people who choose them** Disponível em: < https://wpengine.com/unmasked/ >. Acesso em 24 de novembro de 2019.

Anexo 1



Anexo 2


*Conexão local
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.103
Packet details
Narrow & Wide
Case sensitive
String
password
Find
Cancel
Expression...
No. Time Destination Protocol Length Info
1591 50.333427 192.168.1.105 TCP 54 50225 → 8009 [ACK] Seq=1211 Ack=1211 Win=63360 Len=0
1607 52.496545 TCP 54 50291 → 443 [FIN, ACK] Seq=2 Ack=1 Win=256 Len=0
1608 52.496689 TCP 54 50291 → 443 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
1609 52.496869 TCP 54 50292 → 443 [FIN, ACK] Seq=2 Ack=1 Win=254 Len=0
1610 52.496987 TCP 54 50292 → 443 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
1611 52.498398 HTTP 961 POST /main/Login/PreValidateLogin?port=80 HTTP/1.1 (application/json)
1612 52.533991 HTTP 573 HTTP/1.1 200 OK (application/json)
1613 52.576782 UDP 1392 60884 → 443 Len=1350
1614 52.630895 192.168.1.103 UDP 78 443 → 60884 Len=36
1615 52.650230 192.168.1.103 UDP 1392 443 → 60884 Len=1350
1616 52.651006 UDP 1392 443 → 60884 Len=1350
1617 52.656279 UDP 1392 60884 → 443 Len=1350
1618 52.711902 UDP 78 443 → 60884 Len=36
1619 52.730230 UDP 1392 443 → 60884 Len=1350
1620 52.731048 192.168.1.103 UDP 70 60884 → 443 Len=28
1621 52.731424 192.168.1.103 UDP 596 60884 → 443 Len=554
1622 52.757114 TCP 54 50285 → 80 [ACK] Seq=909 Ack=520 Win=5843 Len=0
1623 52.787408 192.168.1.103 UDP 62 443 → 60884 Len=20
Frame 1611: 961 bytes on wire (7688 bits), 961 bytes captured (7688 bits) on interface 0
Ethernet II, Src: PcsCompu_d5:84:63
Internet Protocol Version 4, Src: 192.168.1.103,
Transmission Control Protocol, Src Port: 50285, Dst Port: 80, Seq: 1, Ack: 1, Len: 907
Hypertext Transfer Protocol
JavaScript Object Notation: application/json
Object
Member Key: login
String value: MINHACONTA
Key: login
Member Key: password
String value: MINHASENHA
Key: password
0330 61 6c 29 7c 75 74 6d 63 6d 64 3d 72 65 66 65 72 al)|utmcmd=refer
0340 72 61 6c 7c 75 74 6d 63 63 74 3d 4c 6f 67 69 6e ral|utmcct=Login
0350 75 74 6d 7a 3b 20 5f 75 74 6d 74 3d 31 3b 20 5f utmz=__utmt=1;__
0360 31 30 20 5f 75 74 6d 62 3d 32 36 30 37 34 2e 31 utmb=26074.1
0370 32 36 37 2e 31 2e 31 30 2e 31 35 37 33 38 35 36 267.1.10.1573856
0380 33 37 34 0d 0a 0d 0a 7b 22 6c 6f 67 69 6e 22 3a 374....{"login":
0390 22 4d 49 4e 48 41 43 4f 4e 54 41 22 2c 22 70 61 "MINHACONTA","pa
03a0 73 73 77 6f 72 64 22 3a 22 4d 49 4e 48 41 53 45 ssword":"MINHASE
03b0 4e 48 41 22 2c 65 73 63 6f 6c 61 22 3a 22 22 7d NHA","escola":""}
JSON object:member (json.member), 23 bytes
Packets: 1655 · Displayed: 104 (6.3%) · Dropped: 0 (0.0%)
Profile: Default
PT
20:31
15/11/2019