CENTRO UNIVERSITÁRIO DO PARÁ - CESUPA
ESCOLA DE NEGÓCIOS, TECNOLOGIA E INOVAÇÃO - ARGO
CURSO DE CIÊNCIA DA COMPUTAÇÃO

FILIPE DO COUTO CASTRO
LUCAS DAVI MONTEIRO MORAES
LUCAS MIGUINS DA SILVA
YUSSEF LOBATO TOUTENGE

ANÁLISE E IMPLEMENTAÇÃO DA TÉCNICA DE INVASÃO MAN-IN-THE-MIDDLE EM REDES SEM FIO IEEE 802.11 COM A ELABORAÇÃO DO RELATÓRIO INCIDENTE

BELÉM
2019

FILIPE DO COUTO CASTRO
LUCAS DAVI MONTEIRO MORAES
LUCAS MIGUINS DA SILVA
YUSSEF LOBATO TOUTENGE

ANÁLISE E IMPLEMENTAÇÃO DA TÉCNICA DE INVASÃO MAN-IN-THE-MIDDLE EM REDES SEM FIO IEEE 802.11 COM A ELABORAÇÃO DO RELATÓRIO INCIDENTE

Trabalho de conclusão de curso apresentado à Escola de Negócios, Tecnologia e Inovação do Centro Universitário do Estado do Pará como requisito para obtenção do título de Bacharel em Ciência da Computação na modalidade MONOGRAFIA.

Orientador: Esp. Eudes Danilo da Silva Mendonça.

BELÉM
2019

FILIPE DO COUTO CASTRO
LUCAS DAVI MONTEIRO MORAES
LUCAS MIGUINS DA SILVA
YUSSEF LOBATO TOUTENGE

ANÁLISE E IMPLEMENTAÇÃO DA TÉCNICA DE INVASÃO MAN-IN-THE-MIDDLE EM REDES SEM FIO IEEE 802.11 COM A ELABORAÇÃO DO RELATÓRIO INCIDENTE

Trabalho de conclusão de curso apresentado à Escola de Negócios, Tecnologia e Inovação do Centro Universitário do Estado do Pará como requisito para obtenção do título de Bacharel em Ciência da Computação na modalidade MONOGRAFIA.

Data da aprovação: / /
Nota final aluno I:_____
Nota final aluno II:_____
Nota final aluno III:_____
Nota final aluno IV:_____

Banca examinadora

_____

Prof. Esp. Eudes Danilo da Silva Mendonça
Orientador e Presidente da banca

_____

Prof. Itamar Jorge Vilhena de Brito
Examinador

“Você não pode vencer sem estar faminto,
mas não faminto como um vilão,
e sim em uma maneira muito mais nobre de ser.”
(Jonathan Joestar)

AGRADECIMENTOS

Gostaríamos de agradecer as nossas famílias, ao orientador, Eudes Danilo, por ter aceitado trabalhar conosco, à professora Alessandra Natasha por permitir a nossa pesquisa de campo em seu horário de aula, aos nossos grandes amigos Luis Flávio Clink, Renato Souza, Luan Pereira, Luan De Risse, Rafael Julio, Antonio Eduardo Junior, Arthur Victor Damous, Victor Hugo Ferreira, Franklin Sobrinho, Isabelle David, Renan Mello e Victor Hugo Telles por nos auxiliarem durante este último capítulo da nossa graduação.

Autores

RESUMO

Com o avanço da tecnologia, as pessoas acabam se tornando mais suscetíveis a invasões em redes, e a invasão *Man-in-the-middle* acaba se tornando de extremo perigo, pelo motivo da facilidade em sua implementação. O intuito desta monografia é criar um documento de resposta a incidente, tendo como base uma implementação de um ataque *Man-in-the-middle* realizada na rede o Centro Universitário do Estado do Pará - CESUPA.

Palavras-chave: *Man-in-the-middle*. Wi-fi. Implementação.

ABSTRACT

As technology advances, people become more susceptible to network intrusions, and the Man-in-the-Middle invasion becomes extremely dangerous because of its ease of implementation. The purpose of this monograph is to create an incident response document, based on an implementation of a Man-in-the-middle attack carried out on the Centro Universitário do Estado do Pará - CESUPA *network.*

Palavras-chave: *Man-in-the-middle*. Wi-fi. *Implementation*.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AP - *Access Point*

ARP - *Address Resolution Protocol*

BIT - *Binary Digit*

BSS - *Basic Service Set*

CESUPA - Centro Universitário do Estado do Pará

DHCP - *Dynamic Host Configuration Protocol*

DNS - *Domain Name System*

ESS - *Extended Service Set*

GSM - *Global System for Mobile*

HTML - *HyperText Markup Language*

IDS - Intrusion Detection System

IP - *Internet Protocol*

LAN - *Local Area Network*

MAC - *Media Access Control*

MITM - *Man-in-the-middle*

SQL - *Structured Query Language*

SSID - *Service Set Identifier*

TLS - *Transport Layer Security*

SUMÁRIO

1 INTRODUÇÃO

As redes sem fio representam um avanço e trouxeram grandes mudanças na forma com que as pessoas se comunicam e transmitem dados e informações. Diferente das redes cabeadas, que exigem certo conhecimento técnico para a sua implementação, as redes que utilizam radiofrequência, em especial as redes WI-FI, são fáceis de configurar permitindo que qualquer usuário possa implementá-las. Outra grande vantagem em sua utilização é o baixo custo necessário para adoção dessa tecnologia, graças a essa simplicidade, o acesso a internet se popularizou de forma nunca vista antes em empresas e residências do Brasil.

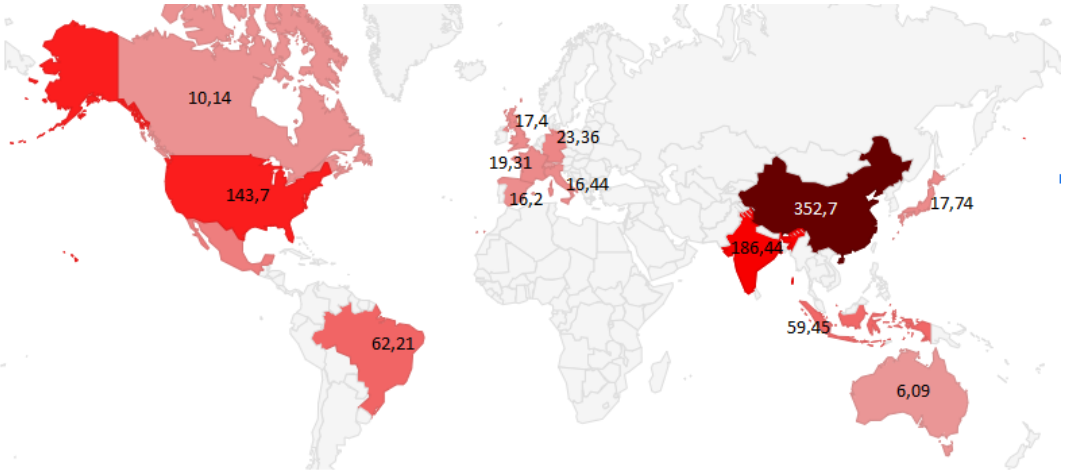
No país, segundo dados do IBGE (2018), o percentual de domicílios em que havia a utilização de internet em 2017 era de 74,9%, um aumento de 8% se comparado ao ano anterior. Nessa pesquisa constatou-se que, do total de domicílios com acesso à rede mundial de computadores, em 98,7% destes o aparelho Celular, através de uma rede WI-FI, era utilizado como um meio de acesso para navegar na web.

Em consequência a grande aderência da tecnologia sem fio em residências e estabelecimentos comerciais, o número de casos de cibercrimes aumentou pois, devido às características de transmissão de dados de uma rede sem fio, na qual os bits são difundidos através de ondas eletromagnéticas, mais especificamente ondas de rádio (RUFINO, 2005, p. 19), a informação pode ser interceptada e a segurança da rede é um fator primordial a se considerar para que ataques e roubo de informações sejam evitados.

1.1 SITUAÇÃO PROBLEMA

O Brasil é um dos países com o maior número de casos de cibercrime do mundo. Segundo a Symantec (2017), a Cyber Norton Security realizou uma pesquisa em que foram relatados dados de crimes na internet ao redor do mundo (Figura 1), o Brasil chegou a ficar em segundo lugar em relação ao número de crimes cibernéticos, atingindo em torno de 60 milhões de pessoas e gerando um prejuízo de US$ 22,5 bilhões. Devido a isso, medidas de segurança estão sendo cada vez mais necessárias.

Figura 1 - Mapa de relação de pessoas atingidas.



Fonte: Adaptado de SYMANTEC (2017).

Dentre os cibercrimes, o ataque *Man-in-the-middle* - MITM, acaba se tornando um dos mais utilizados, uma vez que, segundo a CISCO (2017), até 2022 haverá cerca de 549 milhões de pontos Wi-Fi públicos mundialmente, um aumento de quatro vezes quando comparado ao número em 2017.

Assim, através de uma implementação e o estudo de um ataque *Man-in-the-middle* - MITM, será possível identificar seu funcionamento, viabilizando a criação de um relatório incidente para prevenir possíveis ataques em redes locais, e responder a pergunta "Como se defender de um ataque *Man-in-the-middle*?".

1.2 OBJETIVOS DO ESTUDO

1.2.1 Objetivo Geral

Criar um documento de resposta a incidente, tendo como base uma implementação de um ataque *Man-in-the-middle* realizada na rede o Centro Universitário do Estado do Pará - CESUPA.

1.2.2 Objetivos Específicos

- Estudar os fundamentos de um ataque MITM e as falhas que permitem sua execução em redes locais.
- Implementar um ataque MITM na rede do CESUPA utilizando um roteador Mikrotik.

- Pesquisar e expor meios de prevenção de um ataque MITM.

1.3 JUSTIFICATIVA

Devido à grande utilização de redes Wi-Fi e as vulnerabilidades nelas presente, muitas organizações e seus usuários acabam sendo alvos fáceis para aqueles que desejam realizar ataques como o MITM.

No caso de uma empresa, dados perdidos se tornam grandes prejuízos, como relatado na notícia do O Liberal (2019) em que a empresa Centrais Elétricas do Pará - CELPA sofreu uma invasão, resultando em um prejuízo de dois milhões de reais. Para usuários, ter seus dados roubados pode resultar em contas indevidas com seus dados de compra, como relatado na reportagem da SC Magazine (2019), onde o programa de fidelidade *MasterCard* alemão sofreu uma invasão, deixando expostos dados de cartões de crédito de cerca de noventa mil clientes.

Deste modo, com um estudo aprofundado de um ataque MITM, e uma implementação, é possível avaliar seu funcionamento, e identificar maneiras de como preveni-lo.

1.4 METODOLOGIA DA PESQUISA

Neste trabalho foi realizada uma pesquisa exploratória e descritiva, possuindo uma abordagem qualitativa, utilizando a pesquisa de campo como técnica principal. O objetivo da mesma é entender o funcionamento de um ataque MITM em uma rede e as possíveis variáveis que permitiram esta invasão, visto que uma pesquisa qualitativa não busca medir resultados ou apresentar estatísticas (NEVES, 1996, p.01). O estudo foi realizado a partir de dois procedimentos:

1. Pesquisa bibliográfica: foram analisados conceitos como: "*Man-in-the-middle*", "DNS", "IEEE 802.11", tendo como principal referência autores como: Forouzan (2006), Soares (1995), Hussain (2016), Patni *et al* (2017), IEEE 802.11 WORKING GROUP *et al* (2010).
2. Pesquisa de campo: feita com a implementação do ataque MITM em uma rede de uma instituição privada, tendo natureza exploratória. Os dados adquiridos fazem parte dos resultados obtidos, sendo devidamente excluídos como citado no termo de aceitação de participação dos usuários (APÊNDICE A).

A implementação do ataque MITM ocorreu na rede do CESUPA no mês de junho de 2019. As vítimas foram 15 alunos do primeiro semestre do curso de Ciência da Computação da

instituição. Além disso, após o ataque concluído, todas as vítimas foram identificadas e o termo de aceitação de participação foi entregue.

1.5 ESTRUTURA DO TRABALHO

O presente trabalho divide-se em quatro capítulos, nos quais serão abordados o estudo e a implementação do ataque MITM, com um relatório de instrução de como agir e prevenir o ataque. No segundo capítulo, em que se encontra o referencial teórico, serão abordados os conceitos pertinentes relacionados a redes sem fio e a segurança da informação, explanando as principais concepções e princípios de funcionamento das redes Wi-fi e seus padrões de transmissão, além de explicar conceitos necessários para se entender um ataque MITM, divididos em:

1. IEEE 802.11;
2. *Service Set Identifier;*
3. *Internet Protocol;*
4. Endereço Lógico;
5. *Media Access Control*;
6. *Domain Name System*;
7. DNS *SPOOFING;*
8. *MAN-IN-THE-MIDDLE.*

No terceiro capítulo é realizado o ataque MITM, utilizando um dispositivo Mikrotik como roteador, para simular um aparelho dentro da rede do CESUPA e adquirir informações confidenciais de usuários, considerando as características essenciais que permitiram sua efetivação na instituição. O quarto capítulo aborda os resultados do ataque juntamente em como defendê-lo e preveni-lo, seguido do quinto capítulo com as considerações finais.

2 REFERENCIAL TEÓRICO

2.1 IEEE 802.11

É o protocolo que define as especificações para as redes sem fio, que cobre as camadas física e de enlace de dados. No nível físico são tratadas as transmissões com frequência de rádio e infravermelho. Já no enlace foi definido o protocolo de controle de acesso ao meio (MAC). Além de definir dois tipos de serviços, o conjunto básico de serviços, denominado *BSS* (*Basic Service Set*), o conjunto estendido de serviços, denominado ESS (*Extended Service Set*). O BSS define o componente básico de uma rede sem fio, que é composto por estações sem fio, conhecidas como *Access Point*. Já o ESS, é composto por dois ou mais BSS com APs, conectados geralmente através de uma LAN cabeada. (FOROUZAN, 2006, p. 59; SOARES, 1995).

2.2 *SERVICE SET IDENTIFIER*

O *Service Set Identifier* - SSID ou *Basic Service Set Identifier* - BSSID é um campo de 48 bits com o mesmo formato do endereço MAC. O campo identifica unicamente cada BSS. O valor desse campo, em uma infraestrutura de BSS, é o endereço MAC em uso no AP do BSS. (IEEE 802.11 WORKING GROUP *et al*, 2010).

2.3 *INTERNET PROTOCOL*

O *Internet Protocol* - IP, é o mecanismo de transmissão de dados pelo protocolo TCP/IP. Ele transporta dados chamados de datagramas, eles podem ser transmitidos por diferentes rotas, podendo chegar ao destino duplicados ou desordenados (FOROUZAN, 2006, p. 32).

2.4 ENDEREÇO LÓGICO

O endereço lógico, ou endereço IP, foi projetado para que hosts possam ser identificados exclusivamente independentemente da rede física subjacente, funcionando na camada de rede. Dois hosts públicos na internet não podem ter o mesmo endereço IP (FOROUZAN, 2006, p. 37). Ou seja, um site, por exemplo, tem um endereço IP que é único na internet, e esse é usado para identificá-lo.

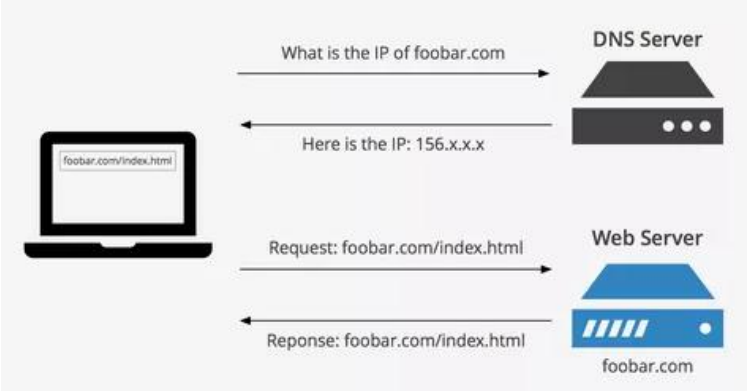
2.5 *MEDIA ACCESS CONTROL*

O endereço *Media Access Control* ou MAC *Address* é um endereço permanente atribuído pelas empresas de fabricação de dispositivos a qualquer aparelho com conexão à internet, funcionando como identificador de comunicação na camada de enlace de redes. (ARCHANA, 2012).

2.6 *DOMAIN NAME SYSTEM*

O *Domain Name System* - DNS é uma aplicação cliente/servidor responsável por mapear um nome de host na camada de aplicativo para um endereço IP na camada de rede (FOROUZAN, 2006, p. 582). Como por exemplo o site “www.exemplo.com” tem um endereço IP "210.220.30.40". Assim, quando um usuário, ao acessar um site através de seu endereço, o DNS faz a tradução para seu endereço lógico, como demonstrado na Figura 2.

Figura 2 - Funcionamento do DNS.



Fonte: KeyCDN (2019).

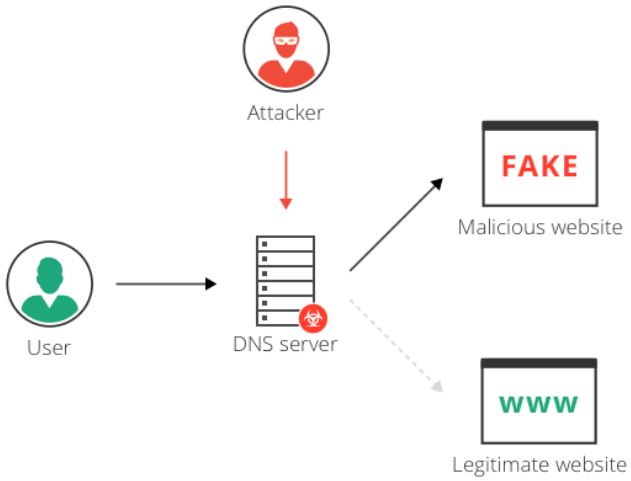
Para evitar um grande tempo de espera no acesso, os sistemas operacionais automaticamente armazenam DNSs acessados mais recentemente em memória *cache*[1], acelerando o acesso do usuário à página (DIAS, 2010). O servidor DNS pode, também, ser sobrescrito por um arquivo existente em todos os sistemas operacionais, nomeado de *Hosts*. Modificar esse arquivo faz com que sua máquina redirecione um DNS para um determinado IP especificado nele, sobrescrevendo até mesmo o DNS em *cache* (RACKSPACE, 2019).

[1] *Cache* é o tipo de memória de rápido acesso (MILUTINOVIC, 1999).

2.7 DNS *SPOOFING*

O DNS *Spoofing* ou DNS *Hijacking*, é uma técnica em que o invasor deve interceptar o tráfego de informações entre cliente e gateway por meio de um envenenamento de cache do ARP. Assim, é possível alterar o IP de direcionamento do DNS para o IP que o invasor desejar (HUSSAIN, 2016).

Figura 3 - Funcionamento do DNS *Spoofing*.



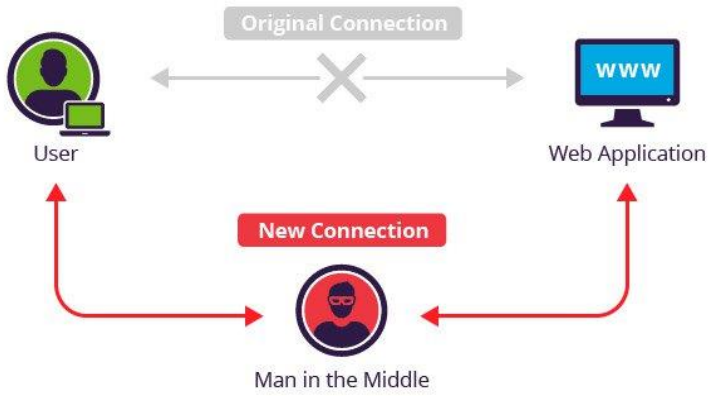
Fonte: Imperva (2019).

A Figura 3, refere-se ao caso de um DNS *Spoofing* remoto por envenenamento de *cache*. Em uma tentativa de *Spoofing* por meio do arquivo *Hosts*, o invasor teria que envenenar todas as máquinas da rede, dificultando o processo de invasão.

2.8 *MAN-IN-THE-MIDDLE*

O ataque *Man-in-the-middle* - MITM é um ataque em que o invasor intercepta a comunicação entre duas partes de uma conexão, sem que nenhuma delas saiba, podendo retransmitir, alterar ou até mesmo armazenar os dados contidos na transmissão. Sendo assim, em teoria, qualquer dispositivo que use protocolos de comunicação que não implementam recursos de segurança podem ser atacados. (PATNI *et al*, 2017; EIGNER, KREIMEL, TAVOLATO, 2016).

Figura 4 - Funcionamento do *Man-in-the-middle*.



Fonte: Imperva (2019).

Ele é normalmente utilizado em redes locais. Uma das maneiras de se utilizar o MITM, é através do envenenamento do DNS, uma das técnicas utilizadas neste trabalho na implementação do MITM.

2.9 TRABALHOS RELACIONADOS

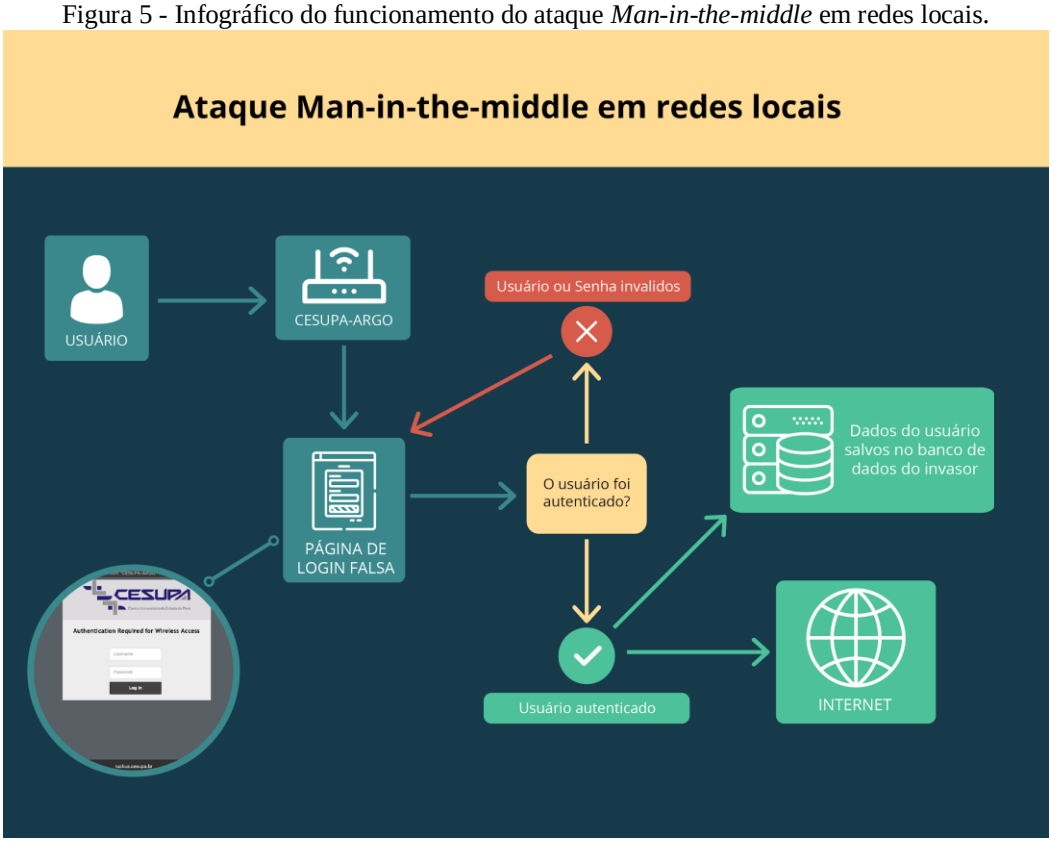
Através do estudo bibliográfico, foi possível encontrar trabalhos em que foram feitas implementações similares de um ataque MITM, porém utilizando técnicas diferentes, como é o caso de Patni *et al (2017)*, em que um ataque MITM foi realizado em um ambiente HTTP/2 que faz o uso do certificado TLS - *Transport Layer Security* para encriptação e autenticação. Além disso, foi feito o uso de técnicas como DNS cache *poisoning*, *Phishing* e o forjamento de um falso certificado TLS. O trabalho consistia em implementar três ataques bem-sucedidos, utilizando as três técnicas citadas.

Outro trabalho aborda uma técnica diferente, mais focado na detecção do ataque em si. Neste caso, Chen *et al* (2007) decidiu abordar o modelo de invasão *Tunneled model* (T-*model*) para desenvolver métodos de detecção, estudando o ataque por meio de um GSM - *Global System for Mobile*. O trabalho implementa o ataque T-*model* e utiliza a autenticação do GSM para validar as mensagens enviadas e suas rotas, verificando caso haja um equipando invasor.

3 DESENVOLVIMENTO DA PROPOSTA

Para realizar a pesquisa de campo, foi necessário replicar a interface de login da instituição (Figura 7) em um dispositivo Mikrotik 951Ui 2HnD com o diferencial que, ao efetuar o login, o usuário teria suas credenciais armazenadas em um banco de dados PostgreSQL hospedado localmente na rede.

Figura 5 - Infográfico do funcionamento do ataque *Man-in-the-middle* em redes locais.



Fonte: Autores (2019).

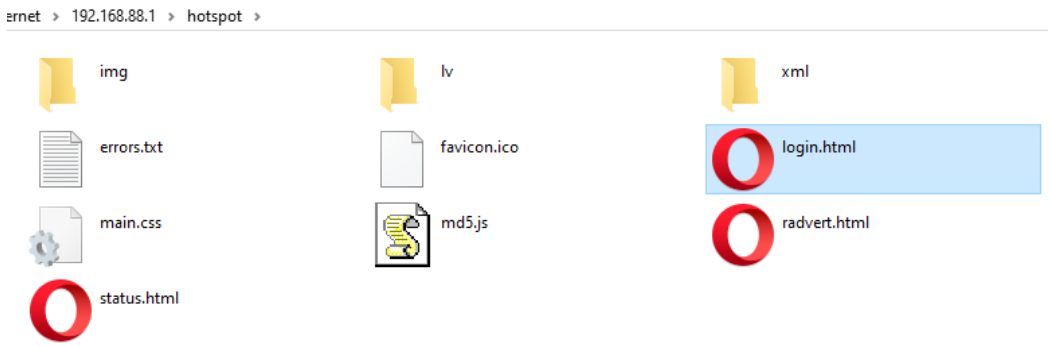
A Figura 5 representa o processo pelo qual o usuário vai passar, detalhadamente. Primeiro ele irá conectar-se ao roteador, o qual possui a página de login falsa em que o usuário deve autenticar-se. Caso seja autenticado, os dados informados serão transmitidos para o banco de dados do invasor e o usuário terá acesso a internet, sem saber o que realmente aconteceu. Caso não seja autenticado, ele voltará a página de login.

Antes do ataque, é preciso efetuar algumas configurações no roteador. Primeiramente, deve-se estabelecer o nome do *Access Point* para o mesmo presente na rede do CESUPA, sendo esse “CESUPA-ARGO”. O nome da rede nas configurações é definido como SSID. Por padrão, caso haja mais de uma rede na região com o mesmo SSID, o aparelho do usuário, irá captar

somente o roteador com o maior sinal, ou seja, caso existam dois *Access Points* com o mesmo nome (SSID), somente um será exibido no dispositivo.

Com isso, quando o usuário se conectar à rede, ele deverá encontrar a página falsa da instituição. Para configurá-la, deve ser criado dentro do roteador o *HotSpot*[2] e configurado o *Walled Garden*[3]. Após a criação de ambos, no *HotSpot*, é trocada a página padrão do roteador localizada dentro do Mikrotik como demonstrado na Figura 6.

Figura 6 - Pasta contendo arquivos do Hotspot dentro do Mikrotik.



Fonte: Autores (2019).

O arquivo login.html na Figura 6 é substituído por um arquivo *HyperText Markup Language* - HTML de mesmo nome contendo a página clonada da instituição (APÊNDICE B). A página possui os aspectos do site original, como mostra a Figura 6.

[2] *HotSpot* é nome do fornecedor de autenticação para clientes em roteadores Mikrotik (MIKROTIK, 2017).

[3] *Walled Garden* é o bloqueador de requisições HTTP e HTTPs em roteadores Mikrotik, autorizando após identificação (MIKROTIK, 2018).

Figura 7 - Página de login falsa.

Fonte: Autores (2019).

Como parte da pesquisa, durante o processo de desenvolvimento da página da Figura 7, alguns aspectos foram modificados, para verificar se os usuários notariam alguma diferença ao tentar se conectar, que no caso acima a diferença está apenas no espaçamento superior da caixa de login. A Figura 8 refere-se à página original.

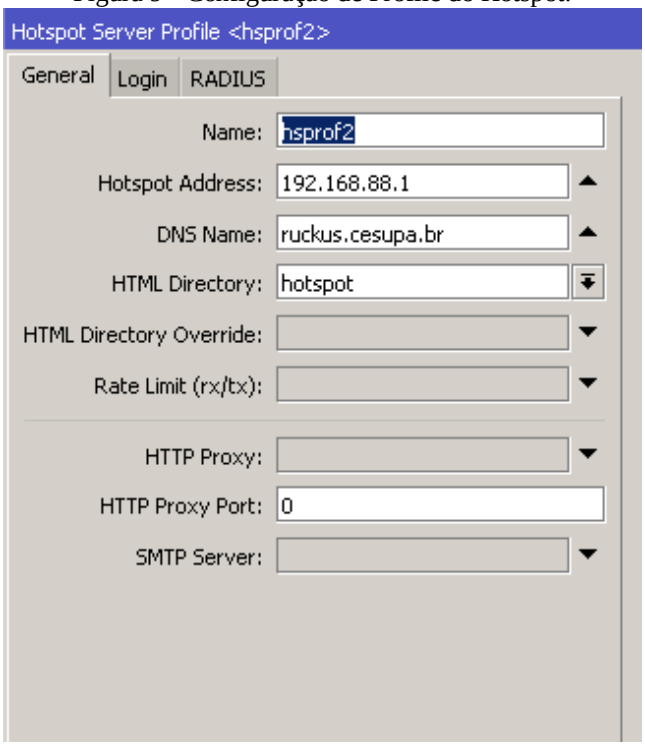
Figura 8 - Página de login da instituição.

Fonte: Autores (2019).

Mas também, ainda nas configurações do Mikrotik é importante notar, também, que, nas Figuras 7 e 8, o endereço de DNS das páginas é igual. Utilizando a técnica do DNS

Spoofing, um usuário que está tentando conectar, ao verificar o endereço ruckus.cesupa.br, acredita estar acessando o endereço original, por mais que haja diferenças entre eles. Essa configuração se torna mais fácil na utilização do *HotSpot* pelo fato da configuração de *Profile* não restringir a adição de um endereço DNS qualquer, como mostra a Figura 9.

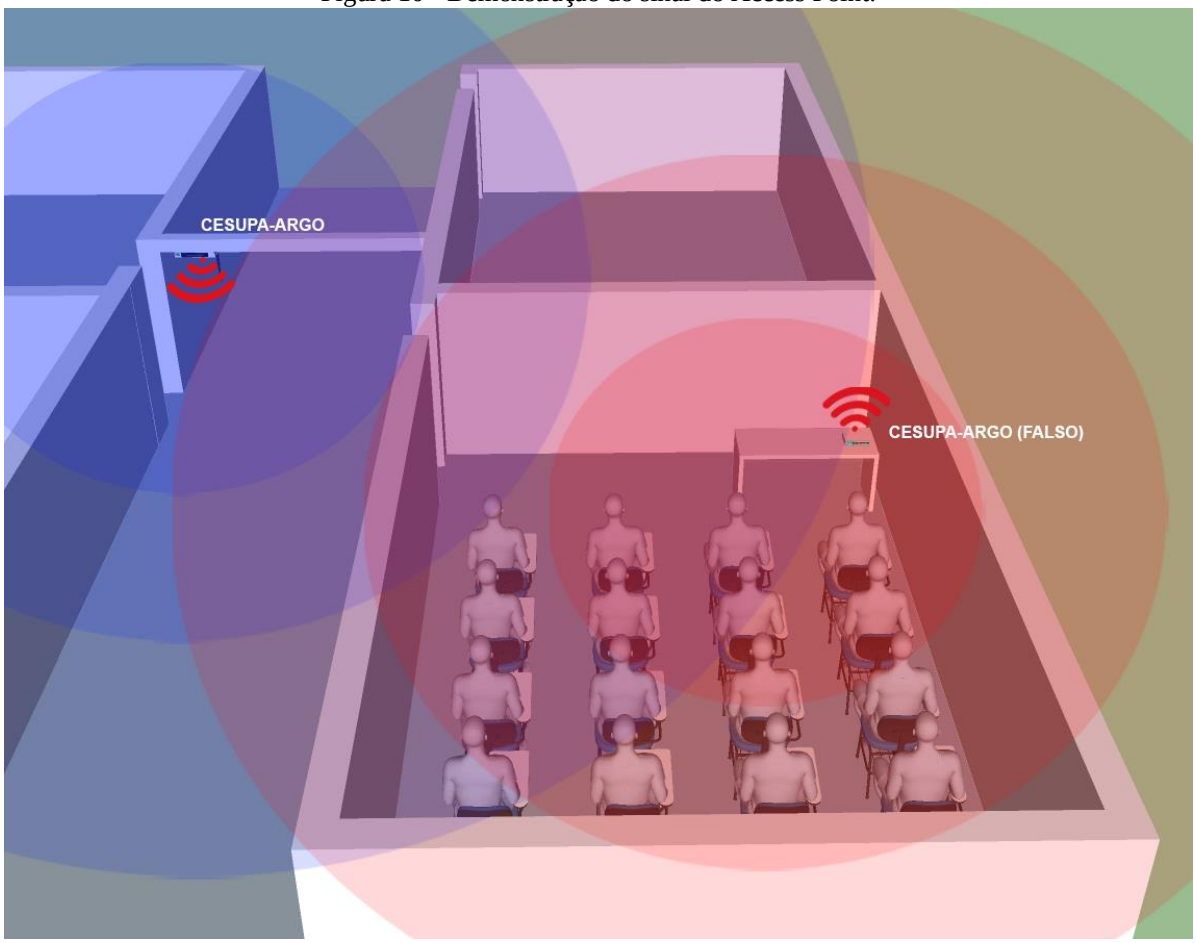
Figura 9 - Configuração de Profile do Hotspot.



Fonte: Autores (2019).

Tendo feito essas configurações, o sistema do ataque está concluído, agora partimos para a etapa de pesquisa de campo, onde a invasão foi implementada dentro da sala de aula. Tendo o conhecimento sobre o funcionamento do SSID, o Mikrotik foi posicionado em cima de uma das mesas onde seu sinal estava melhor que o *Access Point* do CESUPA, como demonstrado na Figura 10.

Figura 10 - Demonstração do sinal do Access Point.



Fonte: Autores (2019).

Com isso, os alunos foram instruídos a fazer autenticação na rede do CESUPA, sem saber que estariam entrando por um *Access Point* invasor, entregando seus dados como as matrículas e senhas, como apresenta a Tabela 1.

Tabela 1 - Algumas matrículas coletadas.

Matrícula	**Senha**
19070006	********
19070031	********
18070207	********
19070015	********
19070203	********
19070017	********

Fonte: Autores (2019).

Com a obtenção destes dados, o ataque é concluído, os danos foram causados de forma imperceptível aos alunos e à instituição.

4 ANÁLISE DO INCIDENTE

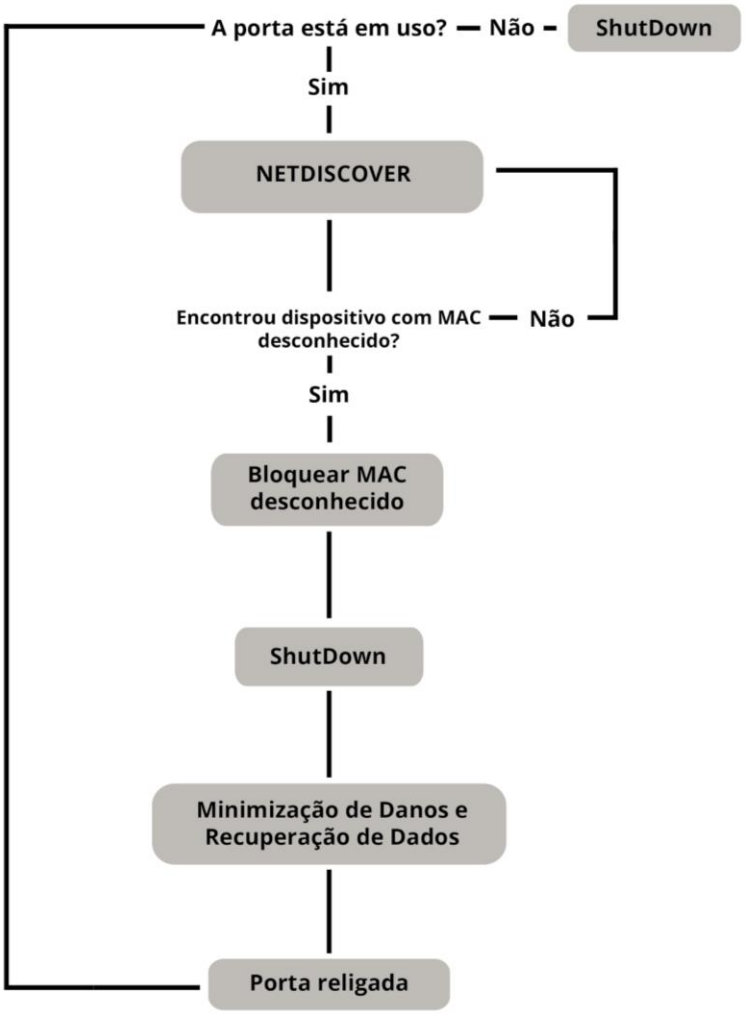
Após o experimento, são definidos fatores que permitiram a execução de ataque MITM. Uma tentativa de ataque que possa comprometer dados ou operações de um sistema ou rede, sendo ela mal ou bem-sucedida, é nomeada como incidente. Esses episódios, que podem alterar o funcionamento normal de um sistema, devem ser catalogados e descritos pela equipe da instituição e registrados em um documento nomeado de Resposta a Incidente (CICHONSKI *et al*, 2012).

O principal objetivo de um documento de Resposta a Incidente é a detecção de tentativas de invasão de um sistema, não só resolvendo um incidente em andamento, mas também avaliando os passos que tornaram este incidente possível, apresentando prevenções contra o mesmo (UCISA, 2004, p.1). Um documento é criado dependendo da modelagem do sistema avaliado e, com base no experimento realizado nesta pesquisa, foi elaborado passos para sua criação:

1. Identificação do incidente: verificar se realmente ocorreu um incidente ou uma tentativa dele, e possíveis ameaças na rede.
2. Resolução: definir como eliminar as ameaças.
3. Diagnóstico: investigação dos erros que permitiram o incidente juntamente com a busca das partes atingidas do sistema.
4. Recuperação: definir plano de recuperação de dados perdidos ou modificados.
5. Lições aprendidas: definir planos para prevenção do incidente no sistema.

Seguindo estes passos, neste capítulo foi elaborado o fluxograma (Figura 10) de como seria a ação feita para tratar o incidente em caso de ataque MITM com um aparelho físico.

Figura 11 - Fluxograma de funcionamento da solução.



Fonte: Autores (2019).

Como mostra a Figura 11, primeiramente é identificado se uma porta qualquer do *Switch*[4] da instituição está aberta. Se não estiver, é desligada sua internet. Caso esteja conectada, é feita a procura por aparelhos desconhecidos conectados à rede, utilizando o *NetDiscover*[5] como buscador de dispositivos. Se não houver algum dispositivo desconhecido conectado, o *NetDiscover* continua rodando enquanto houver conexão com um dispositivo. Caso haja detecção de um aparelho desconhecido, é determinado um incidente e é feito o diagnóstico da situação, identificando os usuários atingidos e o local de ação.

No experimento, o foco da invasão era se passar como um dispositivo da própria rede. Com o êxito nesta etapa, o invasor está com acesso aos usuários. Logo a utilização do

[4] O *Switch* é um controlador que cria uma rede, fazendo os dispositivos nela se comunicarem mais eficientemente. (CISCO, 2006)

[5] Esse aplicativo, utilizado em um sistema operacional Linux, realiza uma investigação eletrónica em aparelhos conectados à rede, identificando os tipos e marca de cada um deles (SHVETSOV, 2008).

NetDiscover identificará para o administrador da rede o endereço IP ou MAC do dispositivo desconhecido em que houve a conexão.

Em seguida, é iniciada a resolução do incidente, onde é realizado o bloqueio do dispositivo invasor e, para isso, basta acessar as configurações de MAC *Filtering*[6] dentro da rede e bloquear seu endereço MAC. Após isso, é necessário desconectar o cabo *ethernet* que permitiu a conexão do aparelho, para que não haja mais incidentes durante a recuperação de dados. Visto que, no experimento, os usuários eram autenticados na rede, o trabalho de recuperação foi facilitado. Uma busca no controle de usuários é capaz de identificar os atingidos, e assim a instituição pode recomendá-los a trocar seus dados de login (usuário e senha).

Após o incidente, é realizada uma análise do que pode ser feito para que o mesmo não ocorra novamente. Para isso, foi feita uma divisão na análise entre instituição e usuário, uma vez que, para a prevenção, são realizadas abordagens diferentes.

Para os usuários, devem sempre ter atenção quando estiverem utilizando redes sem fio públicas ou desconhecidas, mesmo que sejam de uma instituição privada. Para a instituição, devem ser feitas investigações recorrentes através do *NetDiscover*, visando identificar equipamentos não pertencentes à instituição.

Além disso, existe um programa que realiza o processo automatizado, o Cisco *Port Security*, uma solução que faz a varredura na porta do *Switch*, caso encontre um endereço MAC não registrado, é feito o bloqueio, contudo, é uma solução de alto custo e exclusivo a dispositivos roteadores e *Switches* Cisco (CISCO, 2018).

Os passos para a prevenção da instituição, mais especificamente do CESUPA, estão expostos no documento incidente (APÊNDICE C).

[6] MAC *Filtering* refere-se a limitar o tráfego de pacotes de um ou mais endereços MAC (CISCO, 2015)

5 CONSIDERAÇÕES FINAIS

Durante o estudo dos tópicos do segundo capítulo, foram identificados pontos que permitiram o sucesso do ataque, assim como pontos que podem impedi-lo de acontecer e, por fim, a questão de pesquisa "Como se defender de um ataque *Man-in-the-middle*?" Foi respondida por meio da análise do ataque.

Sendo uma solução possível ao problema as investigações recorrentes na rede segundo as instruções do quarto capítulo. Contudo, uma das dificuldades desta solução é o fato dessas investigações não serem realizadas de forma automatizada e, em alguns casos, podem levar tempo para ser detectado e/ou tomado uma ação pelo administrador da rede. Em nosso cenário real, ao ser analisada a rede do CESUPA (/21, 2046 hosts), levou aproximadamente 16 minutos para verificar toda a rede. Caso o invasor consiga inserir um dispositivo malicioso em um tempo menor a este, é possível que ele não seja detectado.

Uma das propostas para soluções futuras seria um processo de automatização a este incidente, totalmente de graça, em que o administrador da rede fornece os endereços MAC dos dispositivos da instituição para um programa que irá fazer a varredura na rede utilizando o *NetDiscover*, caso encontre algum endereço desconhecido, ele é imediatamente bloqueado.

Mas também, a solução CISCO, apresentada no tópico anterior, não é uma solução de fácil acesso pelo fato de ter um preço elevado, portanto a utilização de uma aplicação IDS - Intrusion Detection System, seria mais acessível, uma vez que é uma aplicação que tem o objetivo de monitorar a rede ou o sistema e detectar se há ou não problemas, além de coletar dados de tráfego da rede em busca de atividades maliciosas (HENDRAWAN, 2019).

REFERÊNCIAS

ARCHANA, Hatkar; GAURI, V.; ARVIND, H. Media Access Control Spoofing Techniques and its Counter Measures. **International Journal of Scientific & Engineering Research**, v. 2, n. 6, p. 1-5, 2012.

CICHONSKI, Paul *et al*. Computer security incident handling guide. **NIST Special Publication**, v. 800, n. 61, p. 1-147, 2012.

CISCO. **Cisco Visual Networking Index: Forecast and Trends, 2017 - 2022 White Paper**. Disponível: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256799. Acesso em 17/08/2019.

CISCO. **Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW**. Disponível em: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html. Acesso em: 12/10/2019.

CISCO. **What Are the Most Common Cyber Attacks?**. Disponível em: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks. Acesso em: 5/11/2019.

CISCO. **What is a switch vs. a router ?**. Disponível em: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-what.html#~switches. Acesso em: 12/10/2019.

CHEN, Zhe et al. Modeling of man-in-the-middle attack in the wireless networks. In: **2007 International Conference on Wireless Communications, Networking and Mobile Computing**. IEEE, 2007. p. 2255-2258.

DIAS, Pedro Rogério Vieira. **Trabalho Final da Disciplina de Segurança da Dados: Ataques de envenenamento de cache DNS (DNS cache poisoning)**. Disponível em: https://cic.unb.br/~rezende/trabs/PedroRogerio.pdf. Acesso em: 19/11/2019.

EIGNER, Oliver; KREIMEL, Philipp; TAVOLATO, Paul. Detection of man-in-the-middle attacks on industrial control networks. In: **2016 International Conference on Software Security and Assurance (ICSSA)**. IEEE, 2016. p. 64-69.

FOROUZAN, Behrouz A.; FEGAN, Sophia Chung. **TCP/IP protocol suite**. McGraw-Hill, 2006.

HENDRAWAN, Hendrawan; SUKARNO, Parman; NUGROHO, Muhammad Arief. Quality of Service (QoS) Comparison Analysis of Snort IDS and Bro IDS Application in Software Define Network (SDN) Architecture. In: **2019 7th International Conference on Information and Communication Technology (ICoICT)**. IEEE, 2019. p. 1-7.

HUSSAIN, Mohammed Abdulridha *et al*. DNS protection against spoofing and poisoning attacks. In: **2016 3rd International Conference on Information Science and Control Engineering (ICISCE)**. IEEE, 2016. p. 1308-1312.

IBGE. **Acesso à internet e à televisão e posse telefone móvel celular para uso pessoal 2017**. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 01/09/2019.

IEEE 802.11 WORKING GROUP *et al*. IEEE standard for information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments. **IEEE Std**, v. 802, n. 11, 2010.

IMPERVA. **Man in the middle (MITM) attack**. Disponível em https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/. Acesso em: 21/09/2019.

MIKROTIK. **Manual:IP/Hotspot/Walled Garden**. Disponível em: https://wiki.mikrotik.com/wiki/Manual:IP/Hotspot/Walled_Garden. Acesso em: 12/10/2019.

MIKROTIK. **Manual:IP/Hotspot**. Disponível em: https://wiki.mikrotik.com/wiki/Manual:IP/Hotspot. Acesso em: 12/10/2019.

MILUTINOVIC, Velijko; VALERO, Mateo. **Guest Editors' Introduction Cache Memory And Related Problems: Enhancing And Exploiting The Locality.** IEEE Transactions on Computers, v. 48, n. 2, p. 97-99, 1999.

NEVES, José Luis. Pesquisa qualitativa: características, usos e possibilidades. **Caderno de pesquisas em administração, São Paulo**, v. 1, n. 3, p. 1-5, 1996.

O LIBERAL. **Quadrilha zerou mais de R$ 2 milhões em dívidas do sistema da Celpa**. Disponível: https://www.oliberal.com/policia/quadrilha-zerou-dividas-que-chegam-a-mais-de-r-2-milhoes-do-sistema-da-celpa-1.206445. Acesso em: 1/11/2019.

PATNI, Parth *et al*. Man-in-the-middle attack in HTTP/2. In: **2017 International Conference on Intelligent Computing and Control (I2C2)**. IEEE, 2017. p. 1-6.

RACKSPACE. **Modify your hosts file**. Disponível em: https://support.rackspace.com/how-to/modify-your-hosts-file/. Acesso em: 19/11/2019.

RUFINO, N. M. de O. **Segurança em redes sem fio**. 2.ed. São Paulo: Novatec, 2005.

SC MAGAZINE. **Mastercard says German Priceless Specials loyalty program breached**. Disponível em: https://www.scmagazine.com/home/security-news/mastercard-says-german-priceless-specials-loyalty-program-breached/. Acesso em: 1/11/2019.

SHVETSOV, Alexey *et al*. **NetDiscover**. Disponível em: https://github.com/alexxy/netdiscover. Acesso em: 12/10/2019.

SYMANTEC. **Norton Cyber Security Insights Report Global Results**. Disponível em https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf. Acesso em: 17/08/2019.

UCISA. **ITIL - A guide to incident management**. Disponível em: https://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/service_operation/incident_management/ITIL_a%20guide%20to%20incident%20management%20pdf.ashx. Acesso em: 13/10/2019.

APÊNDICE A – Termo de consentimento.

TERMO DE CONSENTIMENTO

Eu, _____, matriculado sob número _____, declaro que participei, por vontade, do experimento de Redes de Computadores, realizado pelos alunos do Curso Ciência da Computação, TURMA CC8MA, do Centro Universitário do Pará - CESUPA, consentindo que os mesmos obtivessem acesso ao meu número de MATRÍCULA e SENHA do sistema aluno online, via técnica MAN-IN-THE-MIDDLE, como forma de pesquisa científica de meios tecnológicos para o Trabalho de Conclusão de Curso, orientado pelo professor Eudes Danilo Mendonça. Estou ciente do objetivo deste experimento ser unicamente utilizado para fins acadêmicos. Declaro, ainda, ter sido orientado a modificar a senha de acesso após a referida atividade.

Belém,_____de _____de 2019.

_____
Assinatura do Participante

_____
Assinatura do Orientador

_____
Assinatura do Coordenador do Curso

APÊNDICE B – Arquivo login.html.

```
<!DOCTYPE html>
<html>

<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>Page Title</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" type="text/css" media="screen" href="main.css"
/>
    <script src="main.js"></script>
</head>

<body>

    <div id="dialog">

        <div id="dialog_header" style="background-color: rgb(221, 219,
221);">
            <div>
                <a href="" class="img-card">
                    <img src="./logo.png" alt title class="img">
                </a>
            </div>

            <div style="color: inherit; font-family: inherit;">
                <h1 id="header_h" style="background-color: rgb(236, 237,
236);">Authentication Required for Wireless
                    Access</h1>
            </div>
        </div>

        <div id="dialog_content" style="background-color: rgb(236, 237,
236);">

            <form>
                <table id="userpass" class="separator">
                    <tbody>
                        <tr class="gap">
                            <th> </th>
                            <td> </td>
                        </tr>
```

```
                        <tr>
                            <td><input class="login_input form-control"
align="center" type="text" name="username"
                                       placeholder="Username" id="username"
maxlength="256" autocomplete="OFF"></td>
                        </tr>
                        <tr>
                            <td><input class="login_input form-control"
align="center" type="password" name="password"
                                       placeholder="Password" id="password"
maxlength="64" autocomplete="OFF">
                                    <input     type="hidden"     name="email"
id="email">
                                    <input     type="hidden"     name="user"
id="user">
                                    <input     type="hidden"     name="ssid"
id="ssid">
                                </td>
                        </tr>
                        <tr>
                            <td align="center">
                                <input    type="submit"    class="submit"
name="ok" value="Log In">
                                </td>
                        </tr>

                    </tbody>
                </table>
            </form>

        </div>

        <div id="dialog_footer" style="background-color: rgb(236, 237,
236);"></div>

    </div>
</body>

</html>
```

APÊNDICE C – Documento Incidente.

INSTRUÇÕES NECESSÁRIAS CONTRA ATAQUES MITM

Este documento tem o objetivo de apresentar instruções necessárias para a prevenção de um ataque Man-in-the-middle. Expondo ferramentas e dispositivos que podem prevenir esses ataques..

Prevenção :

- Utilização de ferramentas capazes de realizar uma varredura na rede, para identificar os dispositivos nela conectados.
  - NetDiscover: ferramenta Linux para varredura de rede.
- Bloqueio do endereço MAC de dispositivos desconhecidos através do MAC FIltering.
- Utilização de dispositivos CISCO com Port-Security.
- Utilização de aplicações IDS.