FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Bruno Henrique de Paula Ferreira

UM ESTUDO SOBRE ATAQUES DE ALTERAÇÕES DE DNS EM ROTEADORES SEM FIO

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Bruno Henrique de Paula Ferreira

UM ESTUDO SOBRE ATAQUES DE ALTERAÇÕES DE DNS EM ROTEADORES SEM FIO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Henri Alves de Godoy.

Área de concentração: Redes de computadores.

Americana, SP.

2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

F439u FERREIRA, Bruno Henrique de Paula

Um estudo sobre ataques de alterações de DNS em roteadores sem fio. / Bruno Henrique de Paula Ferreira. – Americana, 2017.

36f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Henri Alves de Godoy

1 Redes sem fio 2. DNS – rede de computadores I. GODOY, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519

Bruno Henrique de Paula Ferreira

UM ESTUDO SOBRE ATAQUES DE ALTERAÇÕES DE DNS EM ROTEADORES SEM FIO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Redes de computadores.

Americana, 13 de dezembro de 2017.

Banca Examinadora:

Henri Alves de Godoy (Presidente)
Mestre
Fatec Americana

Benedito Aparecido Cruz (Membro)
Mestre
Fatec Americana

Jeferson Wilian de Godoy Stenico (Membro)
Doutor
Fatec Americana

AGRADECIMENTOS

Agradeço primeiramente a Deus, a minha esposa que me acompanha, aos meus pais, e aos professores pelo conhecimento compartilhado ao longo dos semestres.
Aproveito também para agradecer a Prof.ª Dr.ª Maria Cristina Aranda, que em sua disciplina, auxiliou em todas as etapas para a formatação e melhores práticas deste trabalho, e ao meu orientador Prof. Me. Henri Alves de Godoy, que contribuiu de forma ativa para a elaboração deste trabalho de conclusão de curso.
É com muita honra e satisfação que termino este primeiro ciclo acadêmico na FATEC de Americana, e espero que este trabalho possa acrescentar alguma contribuição para a instituição ou aos que por ele se interessem.

DEDICATÓRIA

Dedico este trabalho a meu avô José de Paula Dias (*in memorian*), grande homem, padrinho e que em 1998 me proporcionou o primeiro curso de informática.

RESUMO

Este trabalho foi desenvolvido com o objetivo de conceituar e apresentar o valor e a importância das informações, em um mundo cada dia mais conectado, móvel e com dispositivos cada vez mais inteligentes. Para embasar a pesquisa, foram utilizadas revisões bibliográficas de diversos autores dentro da área de redes, segurança da informação e auditoria em sistemas de informação. Ainda referente a pesquisa foram extraídos dados sobre a utilização da Internet em domicílios brasileiros através da Internet, assim como os usuários de Internet que possuem a tecnologia Wi-Fi em sua residência. Durante o trabalho foi abordado também o ciclo da informação que gera conhecimento, o tripé de segurança da informação que visa garantir a confidencialidade, disponibilidade e integridade dos dados, além de outros aspectos importantes referente a informação. São tratados também alguns conceitos e padrões desenvolvidos para a rede sem fio, gerando assim a compatibilidade necessária para sua efetiva aceitação e crescimento de uso, sua evolução que proporciona maiores velocidades e alcance. Ainda no desenvolvimento teórico é apresentado o funcionamento básico e hierarquia dos servidores DNS, a vulnerabilidade que explora a alteração do servidor DNS em roteadores e modens, além de seu mecanismo de alteração, que uma vez explorado, tende a comprometer dados sigilosos de usuários que estão conectados através da rede. Está vulnerabilidade tem grande possibilidade de ser explorada em roteadores e modens de operadora que possuem configurações padrão de fábrica. Para concluir, no desenvolvimento prático, são apresentadas algumas formas para minimizar os riscos na rede sem fio, para que esta proporcione um aumento na segurança dos dados trafegados.

Palavras Chave: rede sem fio; DNS; segurança da informação.

ABSTRACT

This work was developed with the aim of conceptualizing and presenting the value and importance of information in a world increasingly connected, mobile and with increasingly intelligent devices. To support the research, bibliographical reviews of several authors were used within the area of networks, information security and information system auditing. Also related to the research were extracted data on the use of the Internet in Brazilian households through the Internet, as well as Internet users who have the Wi-Fi technology in their home. During the work the information cycle that generates knowledge was also discussed, the information security tripod that aims to guarantee the confidentiality, availability and integrity of the data, as well as other important information aspects. Also discussed are some concepts and standards developed for the wireless network, thus generating the necessary compatibility for its effective acceptance and growth of use, its evolution that provides greater speeds and reach. The basic development and hierarchy of DNS servers, the vulnerability that exploits the DNS server change in routers and modems, and its change mechanism, which once exploited, tends to compromise sensitive data of users who are connected through the network. This vulnerability is highly likely to be exploited on routers and carrier modems that have factory default settings. To conclude, in practical development, some ways are presented to minimize the risks in the wireless network, so that it provides an increase in the security of the data trafficked.

Keywords: wireless network; DNS; information security.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AES	*Advanced Encryption Standard*
CDMA	*Code Division Multiple Access*
CETIC	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CPF	Cadastro nacional de pessoa física
CVE	*Common Vulnerabilities and Exposures*
DDOS	*Distibuibuted Denial Of Service*
DNS	*Domain Name System*
DOS	*Denial Of Service*
DVR	*Digital Video Recorder*
GBPS	Gigabit por segundo
GHZ	Giga-hertz
GPRS	*General Packet Radio Service*
GSM	*Global System for Mobile Communications*
IEEE	*Institute of Electrical and Electronic Engineers*
IP	*Internet Protocol*
KRACK	*Key Reinstallation Attacks*
MBPS	Megabit por segundo
RG	Registro Geral
SIG	*Special Interest Goup*
SSID	*Service Set Identifier*
TI	Tecnologia da Informação
TLD	*Top-Level Domain*
UFCG	Universidade Federal de Campina Grande
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*
WI-FI	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WMAN	*Wireless Metropolitan Area Network*
WPA2-PSK	*Wi-Fi Protected Acces 2- Pre-Shared Key*
WPAN	*Wireless Personal Area Network*
WPS	*Wi-Fi Protected Setup*
WWAN	*Wireless Wide Area Network*

1. INTRODUÇÃO

Este trabalho busca evidenciar o valor das informações e a necessidade da aplicação de meios, que auxiliem e aumentem a segurança dos dados, pois com a maior quantidade de dispositivos inteligentes, também cresceu a necessidade de mobilidade e de conectividade, gerando uma maior dependência das redes sem fio. A utilização desta tecnologia é possível pois em meados de 1895 Guglielmo Marconi, engenheiro e inventor conseguiu efetuar a primeira transmissão via rádio.

Com o passar dos anos, a criação de padrões possibilitou um aumento de compatibilidade, barateamento de equipamentos e consequentemente uma maior utilização de dispositivos sem fio.

Em paralelo a crescente utilização e trafego de dados, cibercriminosos buscaram meios para obter dados dos usuários, explorando vulnerabilidades nos dispositivos de acesso à Internet. Desta maneira a configuração correta das redes sem fio, torna-se um passo muito importante para a segurança dos dados trafegados.

O objetivo geral deste trabalho é mostrar o valor que uma informação possui e a necessidade de meios para mitigar riscos e ameaças, que comprometem a segurança dos dados, expondo ou captando informações que deveriam ser mantidas em sigilo.

Como objetivo específico serão apresentados testes feitos com um roteador de rede sem fio, ora com sua configuração padrão de fábrica e posteriormente com configurações que visam aumentar a segurança dos dados trafegados. O foco consiste em evitar a alteração dos servidores de DNS (*Domain Name System ou Sistema* de Nomes de Domínio) do roteador, um ataque muito frequente em equipamentos mal configurados ou que mantém apenas as configurações padrão de fábrica.

No desenvolvimento teórico deste trabalho foi utilizado o método científico de pesquisa descritiva e explicativa, com base em revisão bibliográfica, traz autores importantes da área de redes de computadores e segurança da informação, dentre

eles o autor Kurose, além de dados encontrados na Internet, que demonstram o aumento do número de domicílios com Wi-Fi no Brasil.

O trabalho foi estruturado em cinco capítulos, onde o primeiro apresenta a introdução.

O segundo capítulo conceitua a informação, fatores importantes como a segurança da informação, políticas de segurança da informação, além do tema redes sem fio, como sua descoberta, criação e evolução de padrões, seu crescimento no país e classificação quanto ao alcance.

O terceiro capítulo abordará uma vulnerabilidade simples de ser explorada por atacantes em roteadores com configuração padrão, também conhecida como configurações de fábrica, que pode acarretar na alteração dos servidores DNS que por sua vez, compromete o acesso a endereços de Internet e pode causar outras complicações que serão expostas ao longo deste capítulo.

No quarto capítulo, é evidenciado um caso de estudo, que explora a alteração de DNS em roteadores e modens de operadora e sugeridas configurações que visam minimizar a vulnerabilidade.

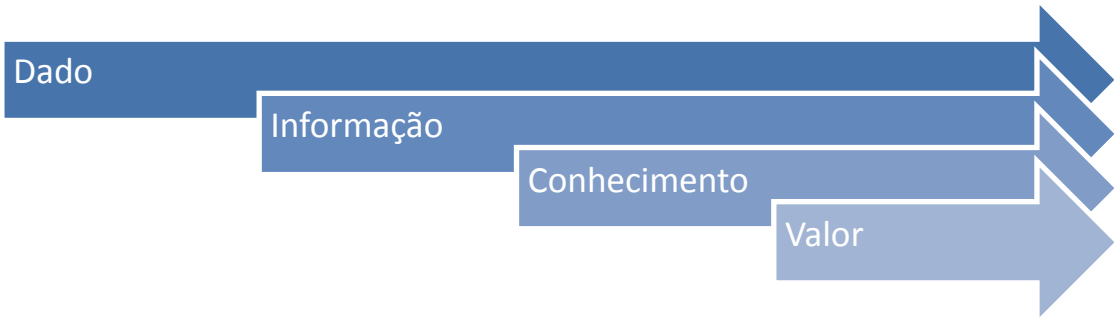
No quinto e último capítulo estão as considerações finais, que remetem a todo o conteúdo apresentado neste trabalho.

2. SEGURANÇA DA INFORMAÇÃO

Há algum tempo, devido a informatização, digitalização de documentos e evolução da tecnologia, observa-se o grande aumento na produção de dados em aplicativos de computador, seja através da inserção de dados em planilhas, editores de texto ou sistemas internos. Estes dados após serem inseridos nestes aplicativos, passam a representar informações, que por sua vez podem ser transformadas em conhecimento após serem interpretadas, o que gera valor, este ciclo pode ser observado na Figura 1. Esta ideia é reforçada pelo autor Alves (2010), conforme a seguir:

> “Hoje em dia, a informação é o ativo mais valioso das organizações. Ao mesmo tempo passa também a ser o mais visado e desejado por pessoas mal intencionadas com objetivo de vasculhar por curiosidade, furtar para obter informações sigilosas e valiosas, trazer danos seja por diversão, benefício próprio ou vingança, descobrir segredos e etc. Por isso, mais do que nunca, existe uma preocupação enorme com relação à segurança das informações nas organizações e até mesmo nos lares, pois ela representa a inteligência competitiva dos negócios (competitividade) e lucratividade. Por isso está exposta a uma enorme variedade de ameaças e vulnerabilidades.”

Figura 1 Ciclo da Informação



Fonte: Elaborada pelo autor

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. (ABNT(2005), *apud* ALVES, (2010, p. 18)).

De acordo com Schimdt *et al*. (2006) é possível verificar alguns riscos para as informações:

> "Todo sistema está sujeito a falhas, erros e mau uso de recursos em geral. Tanto o computador como a mente humana são instrumentos para grandes realizações, porém não são infalíveis.
> Devido a existência deste risco, administradores e proprietários de pequenas e grandes empresas devem ter um interesse comum pela manutenção da integridade dos sistemas e das pessoas envolvidas no ambiente de tecnologia de informação."

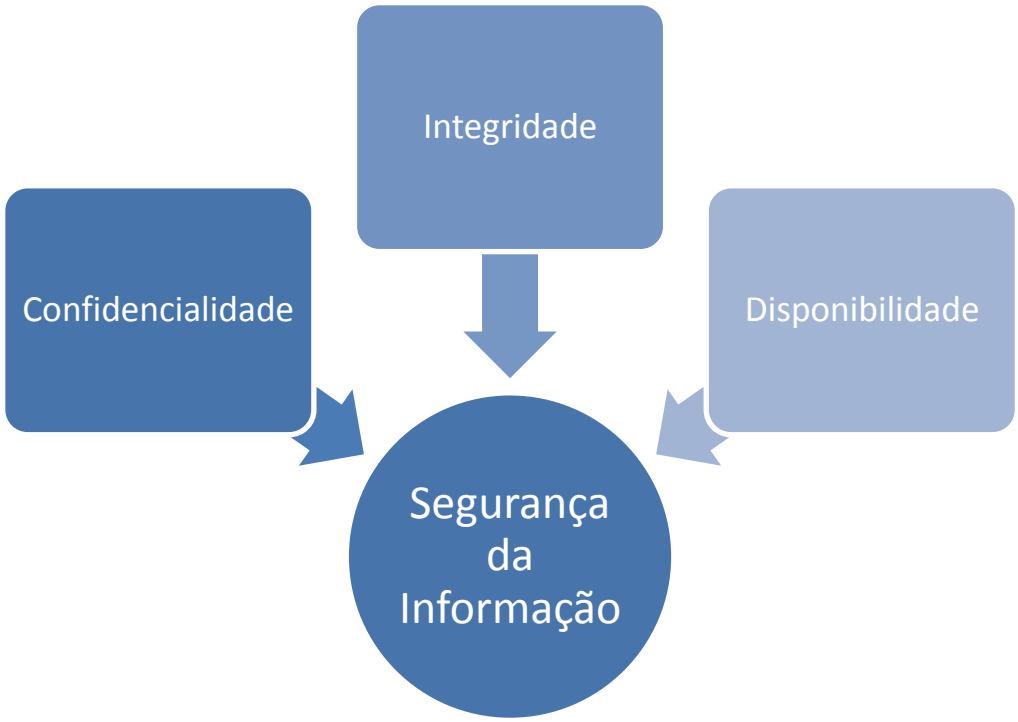
A segurança da informação visa proteger a informação de diversos tipos de ameaças, com os objetivos de garantir a continuidade dos negócios, minimizar possíveis riscos, proteger investimentos, preservar a confidencialidade de dados sensíveis, entre outros, conforme cita OLIVEIRA (2009, p.8):

> "Busca garantir a continuidade do negócio da organização e minimizar os danos causados a ela, por meio da prevenção e redução dos impactos causados por incidentes/acidentes relacionados à segurança.
> No âmbito da TI (Tecnologia da Informação), ela não inclui apenas a segurança de dados, mas também a segurança dos sistemas, recursos e serviços."

Dentre os vários aspectos importantes na segurança da informação, é possível destacar três como sendo os pilares, conforme apresentado na Figura 2 e definido por Lyra (2008, p.3) como:

> "Confidencialidade: Capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo que impede que outros, não autorizados a vejam.
> Integridade: A informação deve estar correta, ser verdadeira e não estar corrompida.
> Disponibilidade: a informação deve estar disponível para todos que precisem dela para a realização dos objetivos empresariais."

Figura 2 Pilares da Segurança da Informação



Fonte: Elaborada pelo autor

Ainda segundo Lyra (2008,p.3-4), além dos aspectos principais, é possível listar outros como:

> “Autenticação: garantir que um usuário é de fato quem alega ser;
> Não Repúdio: Capacidade do sistema de provar que um usuário executou uma determinada ação;
> Legalidade: garantir que o sistema esteja aderente à legislação pertinente;
> Privacidade: capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre usuário e suas ações, exemplo, sistema de voto eletrônico.
> Auditoria: capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque.”

A união destes itens, visa garantir que as informações estejam seguras e pressupõem que ações são tomadas para que os pilares citados na figura 2 e demais aspectos sejam aplicados e evitem um incidente de segurança, ou seja, não permitir que um evento venha a ocasionar interrupções e ou violações dos dados.

2.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Para Ferreira e Araújo (2006), a política de segurança é entendida como o uso de normas, métodos e procedimentos, que buscam garantir a segurança das informações, assim, a política deve ser formal e acessível a todos que façam uso dos ativos de informática.

O desenvolvimento de uma política depende de uma avaliação técnica criteriosa, pois é através dela que será possível definir quais as melhores formas de se configurar e adquirir ativos de informática, atribuição de responsabilidades, além disso, assegurar que essas políticas estejam alinhadas com o negócio e que expressem as aspirações dos proprietários e acionistas.

Ainda segundo Ferreira e Araújo (2006), possuindo um papel imprescindível para a determinação de normas e diretrizes, após a sua implementação, evidenciam-se os seguintes aspectos:

> "Estabelecimento do conceito de que as informações são um ativo importante da organização;
> Envolvimento da Alta Administração com relação à Segurança da Informação;
> Responsabilidade formal dos colaboradores da empresa sobre a salvaguarda dos recursos da informação, definindo o conceito de irrevogabilidade;
> Estabelecimento de padrões para a manutenção da Segurança da Informação."

Para Imoniana (2011), no intuito de alcançar os objetivos administrativos é importante que:

> "[...]estabelecer claramente as políticas de tecnologia de informações e, a partir dessas, cabe aos gerentes traduzir isso em linguagem operacional através de procedimentos administrativos, detalhando inclusive as definições e os princípios, evitando-se dupla interpretação."

Desta forma, fica exposto que uma política para ser efetiva e acarretar benefícios a organização, precisa balancear o uso de tecnologia, clareza nas informações, aceitação da diretoria e alinhamento com as atividades do negócio.

Os itens de segurança mencionados nesse capítulo, são importantes para o subcapítulo a seguir, que expõe o crescente uso de tecnologias sem fio no país.

2.2 REDES SEM FIO

Em meados de 1895, o engenheiro e inventor Guglielmo Marconi conhecido como o pai do rádio, conseguiu efetuar uma transmissão a distância sem a utilização de fio, através das ondas de rádio, na época tal transmissão ficou conhecida como telegrafia sem fio. (UFCG[1], [s.d]). Ainda segundo Jobstraibizer (2010 p.10), podemos acompanhar a evolução da rede sem fio:

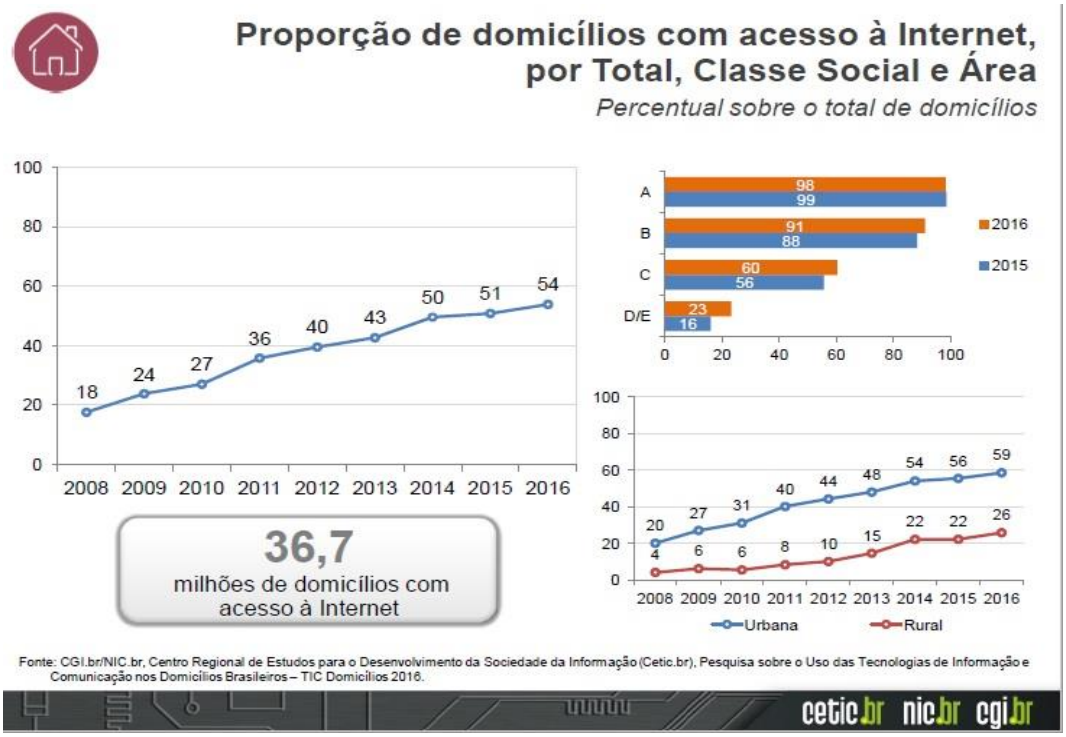
> "[...] a comunicação sem fio evoluiu muito. A explosão de seu uso deu-se por volta dos anos 1970, com a invenção do telefone celular por Martin Cooper. O mercado de comunicação sem fio deu um salto gigantesco em direção ao futuro, e muitas portas se abriram para profissionais visionários, que perceberam o potencial das comunicações sem fio.
>
> [...]comunicar-se de qualquer lugar e a qualquer momento, sem necessidade de nenhum aparelho gigantesco especial. Desta forma, utilizando ainda as ondas de rádio, deu-se origem ao protocolo WLAN, ou Wireless Local Area Network.
>
> O WLAN usa basicamente ondas de rádio para transmitir qualquer tipo de comunicação sem fio, e para isso, utiliza-se de um ponto de acesso, que pode ser um roteador,[...]. [...] Assim também é o WI-FI, tecnologia bastante popular no Brasil, e que utiliza faixas de rádio frequência que não precisam de licença para serem utilizadas;[...]."

Com o crescimento do número de domicílios com acesso à Internet no Brasil, somado a evolução da tecnologia e consequentemente o lançamento de diversos dispositivos inteligentes, ou seja, que possuem acesso à Internet, tais como televisores, *smartphones*, *tablets* entre outros, a conexão física através de cabo de rede, passou a ser obsoleta para muitos destes dispositivos devido a mobilidade. As tecnologias sem fio estão, a cada dia, preenchendo um espaço maior na vida dos usuários de informática, sejam experientes ou não. (JOBSTRAIBIZER, 2010)

A Figura 3, demonstra o contínuo aumento de uso da Internet nos domicílios brasileiros, que em 2016 chegou a 54% dos lares. Esse crescimento aliado a diversificação de dispositivos, torna também imprescindível e crescente o uso de tecnologia sem fio.

[1] UFCG – Universidade Federal de Campina Grande – Disponível em: <http://www.dec.ufcg.edu.br/biografias/Guglielm.html>. Acesso em: 16 nov. 2016.

Figura 3 - Número de Domicílios com Acesso à Internet no Brasil



Fonte: Cetic [1](2017)

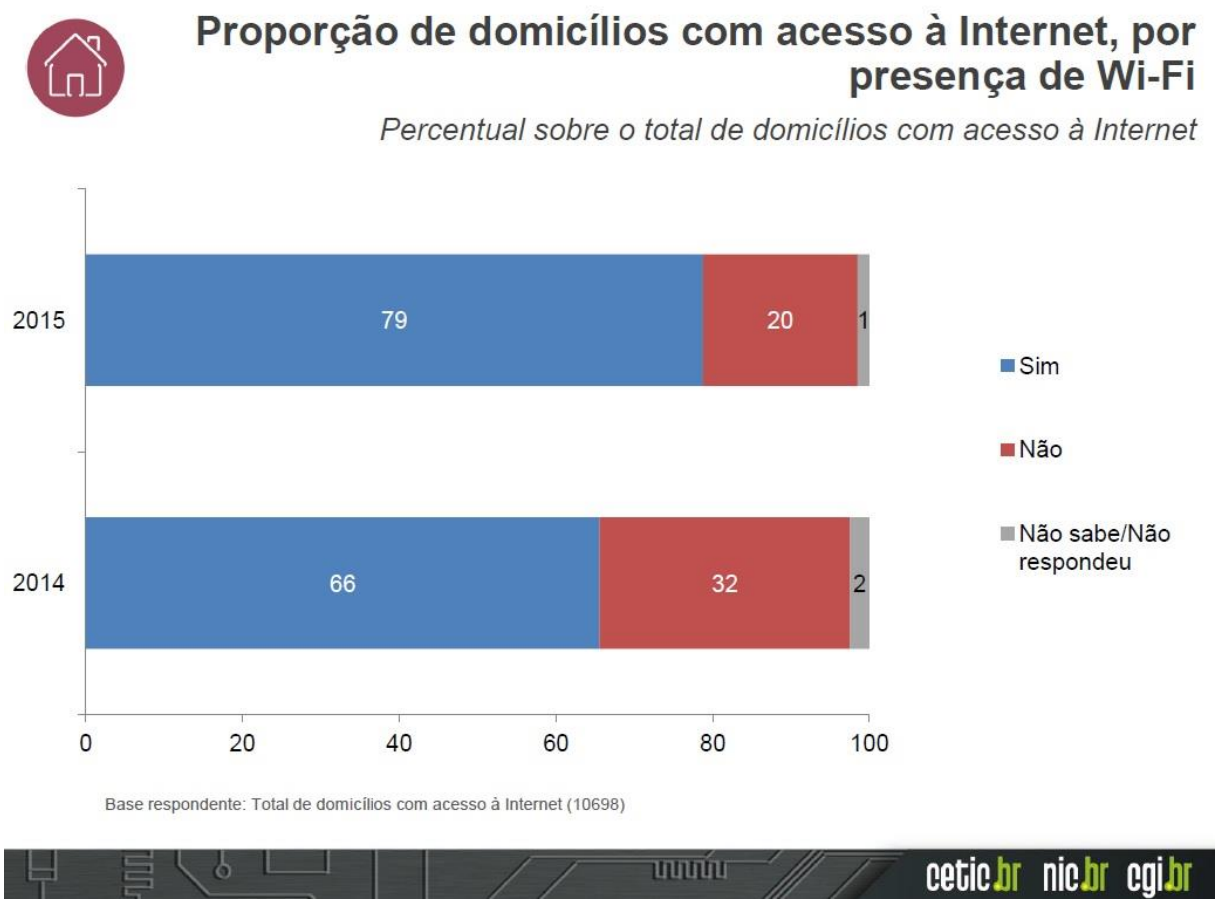
Com o passar do tempo, os equipamentos roteadores, responsáveis pela gestão da conexão sem fio, tiveram os preços reduzidos, aumentando massivamente o uso das redes sem fio, e o compartilhamento de dados e Internet passou a ser essencial para a execução de muitas tarefas do dia a dia, na Figura 4 é possível observar o crescimento das redes Wi-Fi, que em 2015 era presente em 79% dos domicílios com acesso à Internet.

De acordo com Dantas (2010, p.362), os ambientes *wireless* se destacam a cada dia:

> "As tecnologias das redes sem fio vem a cada dia se destacando como elementos mais fundamentais para agregar valor às redes de comunicação e computadores das organizações e empresas responsáveis pela infraestrutura de comunicação e entretenimento. Por esta razão tem sido observado um crescimento na utilização de diferentes técnicas orientadas aos ambientes wireless de uma maneira nunca imaginada."

[1] Cetic – Disponível em: http://cetic.br/media/analises/tic_domicilios_2015_coletiva_de_imprensa.pdf. Acesso em: 15 out. 2017.

Figura 4 Domicílios com Acesso à Internet via Wi-Fi



Fonte: Cetic[1] (2016)

As redes sem fio possuem algumas classificações, como: WPAN, WLAN, WMAN e WWAN, cada classificação leva em consideração o alcance desta rede e suas características, conforme descreve a seguir.

WPAN (*Wireless Personal Area Network*), é uma rede pessoal que visa atender a interligação de equipamentos de um indivíduo, como exemplo, será citado o *bluetooth* em subcapítulo posterior que tem o alcance médio aproximado de 10 metros.

WLAN (*Wireless Local Area Network*), é uma rede sem fio local que permite um maior número de dispositivos conectados, além de maior velocidade e maior alcance

[1] Cetic - Disponível em: < http://cetic.br/media/analises/tic_domicilios_2015_coletiva_de_imprensa.pdf> Acesso em: 30 set. 2016.

que a WPAN. Um Exemplo desta classificação é o Wi-Fi, onde o alcance médio aproximado é de cerca de 100 metros.

WMAN (*Wireless Metropolitan Area Network*) é uma rede sem fio metropolitan, normalmente de uso corporativo, pode atravessar cidades ou estados, um exemplo de uso desta tecnologia é o de uma operadora de Internet, que por meio de antenas espalhadas em uma ou em várias cidades, prove o acesso aos seus usuários.

WWAN(Wireless Wide Area Network) é uma rede sem fio de longa distância, que pode fazer uso da tecnologia usada pelas operadoras de celular, como GSM(Global System for Mobile Communications), CDMA (Code Division Multiple Access) e GPRS(General Packet Radio Service). Outro exemplo é a própria Internet com usuários conectados no mundo todo.

2.2.1 BLUETOOTH 802.15

Bluetooth é um padrão e uma tecnologia sem fio, para conexão e comunicação entre dispositivos. Sua rede possui curto alcance, e permite a conexão de vários dispositivos, como *smartphones, mouses,* teclados*,* impressoras, notebooks, computadores pessoais, entre outros dispositivos que contenham a tecnologia.

O *Bluetooth* é considerado uma tecnologia de baixo custo, onde a conexão é feita através de ondas de rádio com frequências entre 2402 a 2480 Ghz, frequência esta que é padronizada, o que garante a compatibilidade entre dispositivos com a tecnologia. O padrão é desenvolvido por diversas empresas líderes em comunicação, redes e computação, como Motorola, Lenovo, Microsoft, Intel, dentre outras, formando uma espécie de consorcio para gerir o projeto, que leva o nome de SIG (*Special Interest Goup*). Mesmo atuando em uma frequência amplamente utilizada por outros dispositivos, como roteadores e telefones, a tecnologia tende a sofrer poucas interferências dentro do seu alcance.

A tecnologia *Bluetooth*, segue em continuo desenvolvimento, segundo o site da própria SIG, a última versão, *Bluetooth* 5.0 foi lançada ao final de 2016, e traz ganhos significativos quanto ao alcance e velocidade.

2.2.2 WI-FI 802.11

Uma rede local sem fio, apresenta uma maior mobilidade, facilidade de acesso e comodidade aos usuários, porém a falta de padrão na área, representou um grande obstáculo para que esta tecnologia se tornasse amplamente aceita. Devido a essa falta de padrão, já que cada fornecedor oferecia um tipo de solução, muitos usuários deixavam de investir nesta tecnologia com receio de incompatibilidades.

Segundo Dantas (2010, p.397), isso mudou ao ser criado o padrão IEEE 802.11, conforme a seguir:

> "Um dos fatores que ajudou a reverter o quadro do uso da tecnologia wireless em redes locais foi o padrão IEEE 802.11 e a associação Wi-Fi. O IEEE 802.11 (2009) é uma orientação com as melhores práticas e um padrão para implementação das redes locais sem fio. Por outro lado, o Wi-Fi (2009) é uma associação internacional, cujo objetivo é a certificação e a interoperabilidade dos dispositivos e redes baseadas na especificação padrão IEEE 802.11. A razão do padrão está justamente na convergência da interoperabilidade entre diversos dispositivos de diversos fabricantes e a certificação Wi-Fi. A introdução do IEEE 802.11 permitiu que diferentes empre4sas pudessem prover serviços de redes locais sem fio baseados em um sistema aberto[...].[...] o padrão permitiu um aumento do número de fabricantes, que por sua vez levou a uma redução nos custos da solução (exemplo das placas de redes e dispositivos)."

Através da criação padrão IEEE 802.11, aumentou-se a compatibilidade e gradativamente a utilização do Wi-Fi, que hoje pode ser encontrado com facilidade em muitos domicílios.

Tabela 1 Evolução do padrão IEEE 802.11

Evolução 802.11			
Padrão	**Ano**	**Velocidade**	**Alcance Interno**
802.11b	1999	11Mbps	35 Metros
802.11g	2003	54mbps	38 Metros
802.11n	2009	300mbps	70 Metros
802.11ac	2013	> 1gbps	Até 200 metros

Fonte: Tabela Elaborada pelo autor,

A Tabela 1 apresenta dados da evolução da tecnologia com relação a velocidade e alcance em ambientes internos, com base em pesquisas e equipamentos

facilmente achados no mercado, esta evolução permite mais agilidade alcance e traz também melhorias nos modos de transmissão, visando sempre a otimização da comunicação dos dados. O principal equipamento utilizado para prover o acesso as redes sem fio é o roteador, que inclusive será o equipamento com maior foco neste trabalho.

2.2.3 WIMAX 802.16

O Wimax, é um padrão de rede sem fio que possui alcance mais extenso de transmissão, bem como maior velocidade para transmissão de dados. Assim como ocorre com o padrão *Bluetooth,* o padrão Wimax também possui um consórcio de empresas fabricantes de equipamentos, conhecido como Wimax Fórum[1], que visa manter o desenvolvimento desse padrão e garantir a compatibilidade entre dispositivos.

Um ponto favorável das redes Wimax é possibilitar a conexão de múltiplos usuários em uma região mais ampla, como uma cidade, através de uma rede sem fio de alta velocidade, dispensando o uso de gastos com infraestrutura física, como cabeamento e mão de obra, o que consequentemente gera uma redução de custos.

[1] Wimax Forum: Disponível em: <http://wimaxforum.org/> Acesso em: 15 out. 2017.

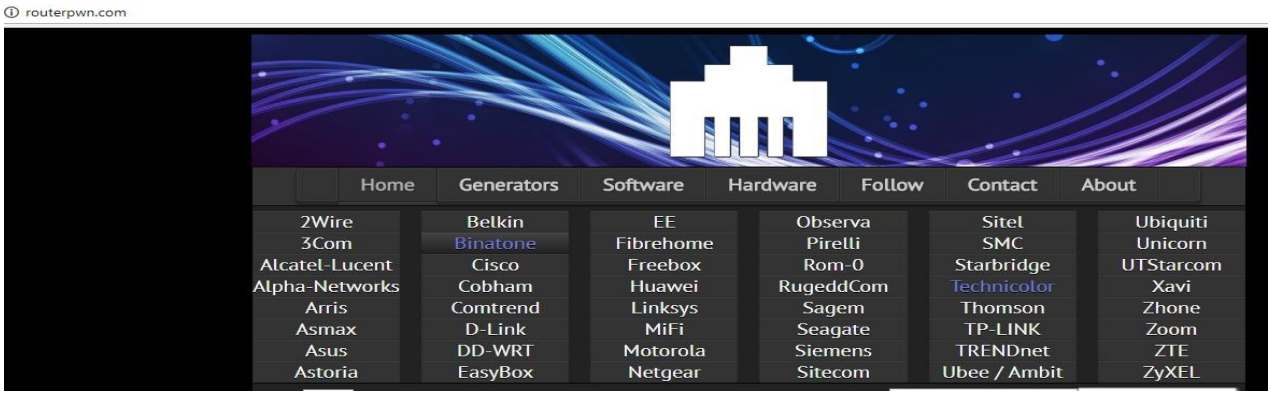
3. CONFIGURAÇÕES PADRÃO DE ROTEADOR E A ALTERAÇÃO DE DNS.

A segurança em roteadores e na rede sem fio é um item muito importante a todos que utilizam essas tecnologias, e por vezes passa despercebida, já que em algumas ocasiões pessoas com pouco conhecimento técnico buscam realizar as configurações, ou simplesmente mantém os padrões de fábrica do equipamento, o que não permite a utilização dos mecanismos de segurança disponíveis. Essa ideia fica clara de acordo com o exposto por Rufino (2005, p.49):

> “A segurança das redes sem fio foi pensada desde a sua concepção e desde esse momento tem evoluído rapidamente. Porém, a despeito de os equipmanetos terem vários, e muitas vezes modernos, mecanisnmos de segurança, eles não vêm (por várias razões, como incompatibilidade com equipamentos de outros fornecedores, facilidade de instalação etc.) habilitados de fábrica. Isso faz com que os administradores com pouca experiência em redes sem fio e/ou com prazos de implantação vencidos coloquem os equipamentos com cinfigurações de fábrica, em que os mecanismos de segurança não forem habilitados corretamente,serão alvos fáceis de ataques.”

A Figura 5, demonstra diversas vulnerabilidades conhecidas de roteadores e modens, disponíveis no site Routepwn. Na página é possível localizar vulnerabilidades organizadas por fabricante, com esse conhecimento o atacante poderá explora-las e trazer riscos para as informações dos usuários.

Figura 5 - Site com possíveis vulnerabilidades de diversos equipamentos



Fonte: Site Routerpwn[1]

[1] Routerpwn – Disponível em: < http://routerpwn.com/ > Acesso em: 15 nov. 2017.

3.1 DNS

Assim como os seres humanos possuem mais de uma forma de identificação, tais como Nome, CPF, RG, etc, os sites hospedados na Internet também possuem mais de uma forma de identificação. Kurose (2010) No caso dos sites, a forma mais simples e fácil de ser lembrada para os humanos é através do nome do domínio, exemplo www.brasil.gov.br, porém por traz deste nome de domínio ou simplesmente endereço, existe um número único para possibilitar a localização deste site, tal número é chamado de endereço IP (*Internet Protocol*). No endereço www.brasil.gov.br, o respectivo endereço IP é: 170.146.252.243. Quando um acesso pelo nome do domínio é solicitado, o servidor DNS *(Domain Name System* ou sistema de nomes de domínio) é o responsável por localizar e traduzir o nome de domínio em número IP, a Figura 6 a seguir ilustra tal tradução:

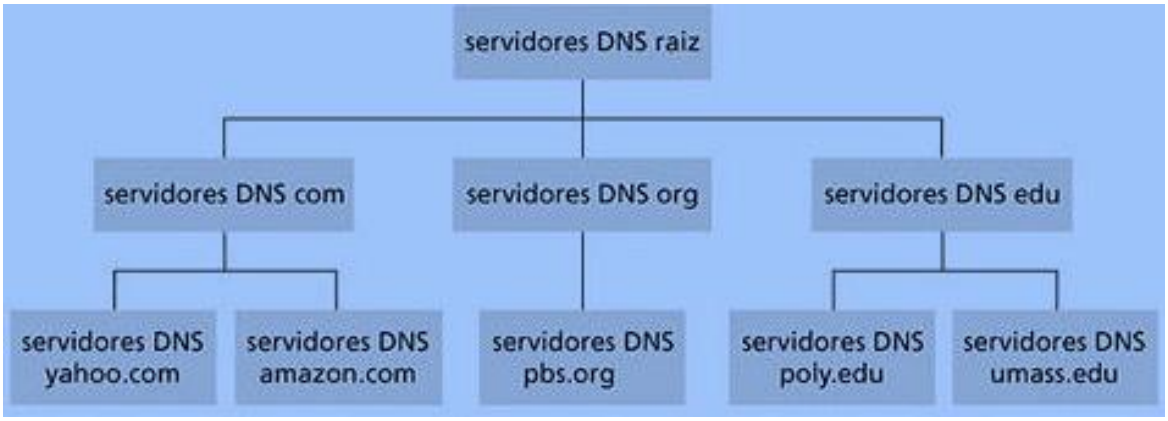
Figura 6 - Funcionamento Básico do DNS

Fonte: Elaborada pelo autor.

Os servidores DNS, *Domain Name System* ou simplesmente sistema de nomes de domínio, são divididos de maneira hierárquica em três níveis e espalhados pelo mundo, esses níveis são classificados como: servidores de nomes raiz, servidores

DNS de domínio de alto nível (top-level domain – TLD) e servidores DNS com autoridade, conforme apresentado na Figura 7. Esta hierarquia existe, pois é impossível para apenas um servidor conhecer todos os endereços. Kurose (2010)

Figura 7 - Hierarquia Servidores DNS



Fonte: Kurose (2010)

Servidores DNS Raiz: São 13 servidores Raiz, sendo que a maioria fica localizado na América do Norte. Este é o primeiro passo para a resolução de um nome de domínio, uma vez que o servidor raiz possui um mapa de onde estão localizados os servidores DNS de alto nível.

Servidores DNS de alto nível ou TLD: Responsáveis pela resolução de domínios de alto nível como: .gov, .org, .com, .net, .edu e pelos domínios de países como: .br, .pt, .ar, etc.

Servidores de nomes com Autoridade: Este tipo de servidor é o que contém o final da cadeia de endereços, fornecem a resolução dos nomes de domínio para endereços de IP, são geralmente mantidos por organizações ou provedores de serviços.

Cache DNS: Uma característica de extrema importância do DNS é o cache, esse permite aumentar o desempenho na resolução de nomes, diminuindo o número de consultas feitas em toda a hierarquia vista anteriormente. De maneira simples quando o servidor solicitante recebe a informação do endereço, ele guarda essa informação por um dado tempo, assim em caso de uma solicitação de outro usuário para o mesmo endereço, a resposta é encaminhada mais prontamente, já que boa parte dos passos não precisa ser refeito. (KUROSE, 2010)

3.2 VULNERABILIDADES DO DNS

Existem diversos ataques ao servidor DNS, que buscam impedir o correto funcionamento do sistema, como por exemplo tentar inunda-lo com milhares de solicitações, fazendo com que consultas legítimas possam não ser respondidas, este tipo de ataque é conhecido como ataque de negação de Serviço ou DoS (*Denial Of Service*). Existe ainda o DDoS (*Distibuibuted Denial Of Service*), que também busca a negação de serviço, porém de forma distribuída, isso é, um computador principal pode gerenciar o ataque utilizando assim milhares ou milhões de outros computadores espalhados. Este tipo de ataque pode visar atacar quaisquer dos níveis da hierarquia do DNS.

Segundo Skoudis (2006) *apud* Kurose (2010, p.105) outros ataques também são possíveis, como apresentado a seguir:

> “O DNS poderia ser atacado potencialmente de outras maneiras. Eu um ataque de homem do meio, o atacante intercepta consultas do hospedeiro e retorno respostas falsas. No ataque de envenenamento, o atacante envia respostas falsas a um servidor DNS, fazendo com que o servidor armazene os registros falsos em sua cache. Ambos os ataques podem ser utilizados, por exemplo, para redirecionar um usuáro da Web inocente ao site Web do atacante. Esses ataques, entretanto, são difíceis de implementar, uma vez que requerem a interceptação de pacotes ou o estrangulamento de servidores”.

Apesar desse tipo de ataque ter eficácia reduzida diretamente nos servidores DNS, conforme citado por Kurose, o ataque de alteração de DNS diretamente em dispositivos de usuários finais como roteadores, modens de operadoras ou mesmo nas configurações da máquina do usuário, podem comprometer o acesso e causar exposição de dados, como poderá ser visto a seguir.

3.3 ALTERAÇÃO DO SERVIDOR DNS EM ROTEADORES

A alteração dos servidores de DNS, é algo que vem sendo explorada por criminosos da Internet, conhecidos como cibercriminosos. Com esse tipo de alteração o cibercriminoso busca conseguir informações importantes e pessoais como senhas, números de cartão de crédito, dados bancários, dentre outras informações sigilosas, as quais pretende usar em benefício próprio.

Aproximadamente 600 vulnerabilidades encontradas em roteadores foram relatadas por pesquisadores e identificadas com um Número de Vulnerabilidades e Exposições (CVE)[1], de 1999 até os dias atuais. (TREND MICRO[2] [s.d], p.5) Como exemplo, podem ser citadas falhas no firmware, vulnerabilidades em serviços e nas páginas de gerenciamento do dispositivo. Estes dados demonstram a grande exploração de vulnerabilidades dos dispositivos roteadores, uma vez que eles são os responsáveis por receber e compartilhar o acesso a Internet e a rede interna existente, centralizando assim todo o trafego de dados do seu local de uso.

Este trabalho será focado em explicar e minimizar a vulnerabilidade que tenta explorar a alteração do servidor de DNS, contido no roteador e ou equipamento de acesso à Internet instalado pelas operadoras de Internet banda larga. Essa alteração dos servidores DNS, visa redirecionar as requisições para sites maliciosos e executar a técnica conhecida como *phishing.* Segundo Cassanti (2014, p.15) pode-se definir o phishing da seguinte forma:

> “Phishing é um exemplo bastante simples e muito utilizado na engenharia social e que consiste, na maioria dos casos, no envio de e-mails não solicitados para a vítima, estimulando-a a acessar páginas (sites) fraudulentas, preencher formulários com seus dados privados ou despertar curiosidade fazendo com que clique em um link para fazer download de um arquivo malicioso (malware) capaz de transmitir para o atacante as informações que lhe interessam.”

Ainda de acordo com Cassanti (2014, p.47), o *phishing* poderá ocorrer de outra maneira como abaixo:

---

[1] CVE (Common Vulnerabilities and Exposures) – Disponível em: https://cve.mitre.org/ Acesso em: 5 out. 2017.

[2] Trend Micro – Empresa de Segurança em conteúdo para internet e segurança da computação – Disponível em: <https://documents.trendmicro.com/assets/wp/wp-securing-your-home-routers.pdf> Acesso em: 5 out. 2017.

> "É muito simples clonar a aparência de um site ou até mesmo criar uma url parecida com a original que leve o usuário a acreditar que está em uma loja de confiança (ataque conhecido como phishing)."

Outra técnica utilizada com o intuito de manipular os dados do usuário objetivando fraudes é a técnica conhecida como *pharming, que segundo* Avast Software[1] (2017) tem as seguintes características:

> "Pharming é uma prática fraudulenta semelhante ao phishing, com a diferença que, no pharming, o tráfego de um site legítimo é manipulado para direcionar usuários para sites falsos, que vão instalar softwares maliciosos nos computadores dos visitantes ou coletar dados pessoais, tais como senhas ou informações financeiras. Este tipo de ataque é particularmente traiçoeiro porque, se um servidor de DNS for comprometido, mesmo os usuários com aparelhos protegidos e livres de malwares podem se tornar vítimas."

As técnicas acima são amplamente exploradas, podem ocorrer havendo ou não a alteração dos servidores DNS no dispositivo roteador ou *modem*, no entanto, sempre que a modificação por servidores DNS maliciosos é concretizada, *phishing*, *pharming* e o redirecionamento dos navegadores para propagandas poderão ser verificados como sintomas. Na Tabela 2, é possível observar alguns números dos cibercrimes no Brasil, que no ano de 2016 afetou cerca de 42.4 milhões de usuários e gerou um prejuízo superior a dez bilhões de dólares.

Tabela 2 - Alguns dados sobre o cibercrime no Brasil

PRINCIPAIS RESULTADOS	BRASIL
Usuários afetados pelo cibercrime em 2016	**42.4 milhões (39%)**
Prejuízo financeiro gerado pelo cibercrime em 2016	**US$10.3 bilhões**
Tempo gasto lidando com consequências cibercrime em 2016	**16.9 horas**

Fonte: Tabela adaptada pelo autor de Norton Cyber Security Insights Report 2016[2]

[1] Avast Software – Empresa de segurança e antivírus – Disponível em: <https://www.avast.com/pt-br/c-pharming> Acesso em: 1 nov. 2017.

[2] Norton Cyber Security Insights Report 2016 - https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf acesso em: 5 out. 2017

3.4 MECANISMO DA ALTERAÇÃO DO DNS

Basicamente existem duas formas para alteração dos servidores DNS em um roteador ou *modem*, por acesso local ou acesso remoto, onde a alteração é feita pela Internet.

Alteração Local: Uma vez que o atacante possui o acesso a rede sem fio, ele pode facilmente acessar o endereço do roteador ou *modem*, e na tela de login, onde são solicitados usuário e senha de acesso, inserir os dados de acesso padrão do fabricante. Essas informações de acesso padrão, são facilmente encontradas na internet, basta realizar uma busca e serão apresentadas diversas informações, e caso o atacante saiba a marca do equipamento, suas chances são ainda maiores, pois encontrará exatamente o que procura.

Outro exemplo de alteração local, é a alteração feita com *scripts*, onde instruções escritas em texto são seguidas sequencialmente para obter os resultados desejados, este trabalho é feito automaticamente ao invés de ser executado por um humano linha a linha. Essa técnica pode ser executada ao acessar uma página maliciosa, que por sua vez desencadeia o download de um *script* que tentará realizar a mudança do DNS no roteador (TREND MICRO [s.d], p.7).

Figura 8 - exemplo de uma função extraída de um script malicioso.

```
var f = function(url) {
    $('body').append('<iframe style=="display:none" src="'+url+'"></iframe>
}

f('http://admin:admin@192.168.0.1/);
f('http://admin:1234@192.168.0.1/);
f('http://admin:@192.168.0.1/);
f('http://admin:admin@10.0.0.1/');
f('http://admin:admin@10.0.0.1/');
```

Fonte: Trend Micro [s.d], p.7)

O trecho de script apresentado na Figura 8, é uma função que busca realizar o acesso ao equipamento utilizando força bruta, onde traz diversos usuários, senhas e endereços de acesso ao roteador ou *modem*. A Figura 9 mostra os dados de acesso tentados na primeira linha da função:

Figura 9 - dados usados para tentar acesso ao equipamento.

Fonte: Trend Micro [s.d], p.7)

Ainda na Figura 9, é possível observar os dados de usuário, senha e endereço do roteador ou *modem*, para tentar acessar as configurações do equipamento. É importante ressaltar que com essa simples combinação, o atacante, poderia garantir o acesso a equipamentos de diversas marcas, pois muitos trazem estes dados como padrão de fábrica.

Alteração Remota: Os roteadores e modens, possuem em suas configurações a opção de acessa-los remotamente, quando este acesso está habilitado, é possível realizar as mesmas tentativas de credenciais padrão, ou mesmo um ataque de força bruta, que consiste em tentar diversos usuários e senhas, até conseguir entrar no dispositivo. Na Figura 10 é possível observar 140 tentativas de acesso a um dispositivo, um exemplo de ataque de força bruta, que visa acessar as configurações do roteador e ter controle total sobre o equipamento.

Figura 10 - Exemplo de ataque de força bruta

```
123     // Set up passwords
124     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root
125     add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root
126     add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root
127     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin
128     add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root
129     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root
130     add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root
131     add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root
132     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root
133     add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root
134     add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support
135     add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root
136     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin
137     add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root
138     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root
139     add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user
140     add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                      // admin
```

Fonte: Trend Micro [s.d], p.11)

No capítulo a seguir, serão efetuados testes em dispositivos da Internet e rede interna para constatar vulnerabilidades e configurações que tornem o dispositivo mais seguro.

4. APLICAÇÃO PRÁTICA

Este capítulo é dedicado a realizar varreduras, a fim de encontrar dispositivos vulneráveis na Internet e um teste local feito com um roteador utilizando configurações padrão de fábrica.

Os testes apresentados a seguir seguirão aos seguintes requisitos:

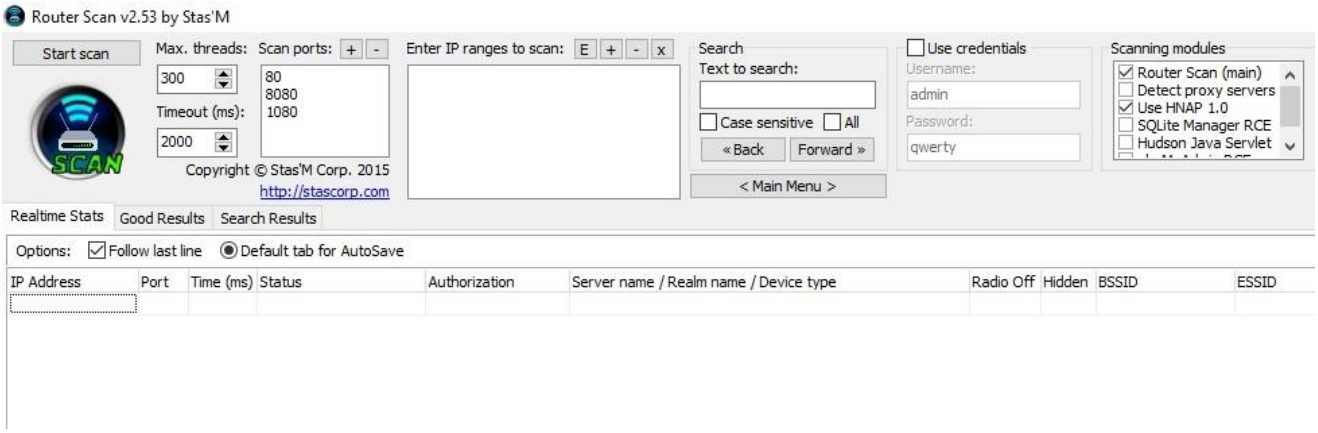
- Serão feitas varreduras em ranges de endereços IPS [1] aleatórios.
- As varreduras serão feitas com o aplicativo Router Scan versão 2.53.
- Não será executado nenhum comando adicional no aplicativo e também não será usada a técnica de força bruta, citada no capítulo anterior.
- Os dispositivos de rede mais vulneráveis serão acessados, desprezando servidores, câmeras IP(*internet protocol*) e gravadores DVR (*Digital Video Recorder, gravador digital de vídeo*).
- Os dispositivos da Internet escolhidos e acessados aleatoriamente, não sofrerão nenhuma alteração de suas configurações, o acesso é apenas para demonstração.
- O último teste será realizado localmente, com um equipamento roteador com configuração padrão de fábrica.

4.1 VARREDURA EQUIPAMENTOS EXTERNOS (INTERNET)

Varredura 1: Na Figura 11, é possível observar o aplicativo Router Scan v2.53, que traz uma interface bastante simplificada para utilização. O objetivo deste desenvolvimento prático é o de demonstrar a vulnerabilidade de roteadores ou modens de operadoras com configuração padrão de fábrica, não serão abordadas nem exploradas outras funcionalidades do aplicativo.

[1] Ranges de IPS – Uma faixa de endereços ex: de 192.168.0.1 até 192.168.0.254.

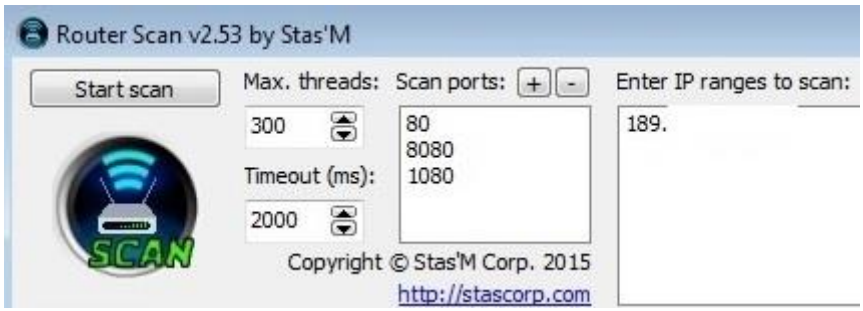
Figura 11 - Imagem do Aplicativo Router Scan v2.53



Fonte: Elaborada pelo autor.

A seguir na Figura 12, foi inserido o range de endereços IP 189.**.**.0-165, com busca nas portas 80, 8080 e 1080, que representam portas habitualmente usadas por serviços de internet. Após essas indicações, inicia-se a varredura através do botão *Start scan.*

Figura 12 - Início da primeira varredura

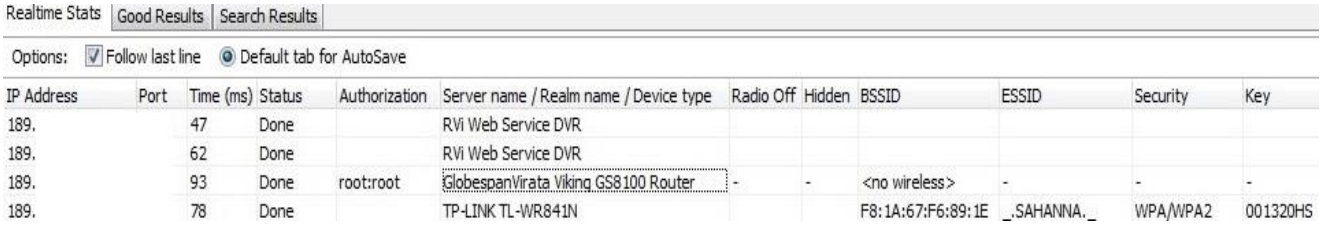


Fonte: Elaborada pelo autor.

Ao final da primeira varredura, um dispositivo com configurações padrão de fábrica foi encontrado e assim escolhido para a tentativa de acesso. O usuário e senha para acesso está localizado na coluna *Authorization* conforme demonstra a Figura 13. Além das informações de acesso ao dispositivo, onde é possível modificar as

configurações, ficam expostas também as informações da rede sem fio, como SSID (*Service Set Identifier,* ou nome da rede) *e a Key (chave de acesso ou senha da rede).*

Figura 13 – Resultado da varredura inicial no range 189..**.0-165**



Realtime Stats | Good Results | Search Results

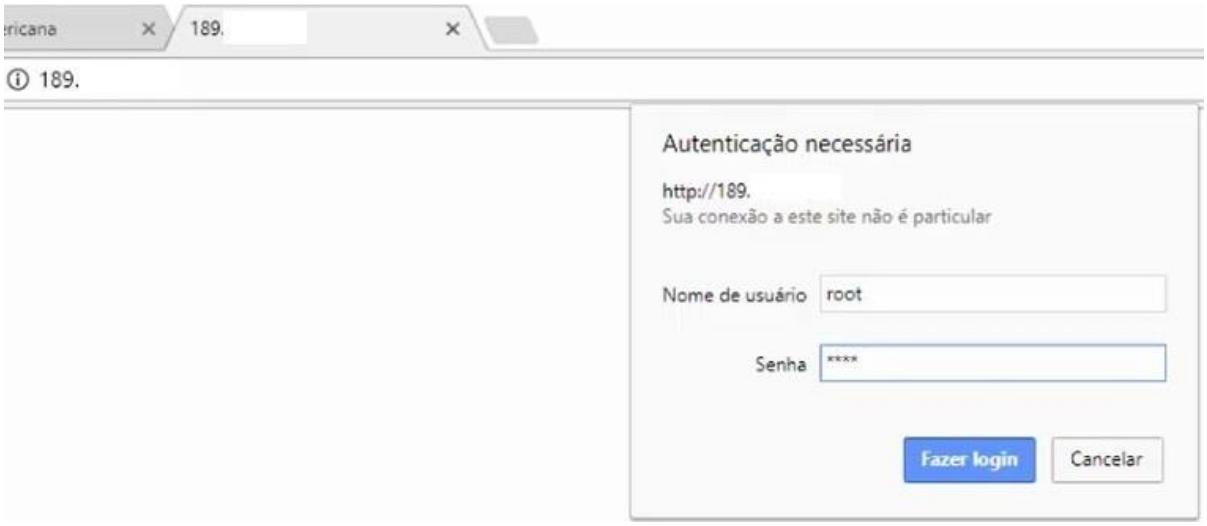
Options: Follow last line | Default tab for AutoSave

IP Address	Port	Time (ms)	Status	Authorization	Server name / Realm name / Device type	Radio Off	Hidden	BSSID	ESSID	Security	Key
189.		47	Done		RVi Web Service DVR						
189.		62	Done		RVi Web Service DVR						
189.		93	Done	root:root	GlobespanVirata Viking GS8100 Router	-	-	<no wireless>	-	-	-
189.		78	Done		TP-LINK TL-WR841N			F8:1A:67:F6:89:1E	_.SAHANNA._	WPA/WPA2	001320HS

Fonte: Elaborada pelo autor.

Na Figura 14, é executada a tentativa de login no equipamento, através do endereço 189.**.**.*** e com o usuário e senha: root.

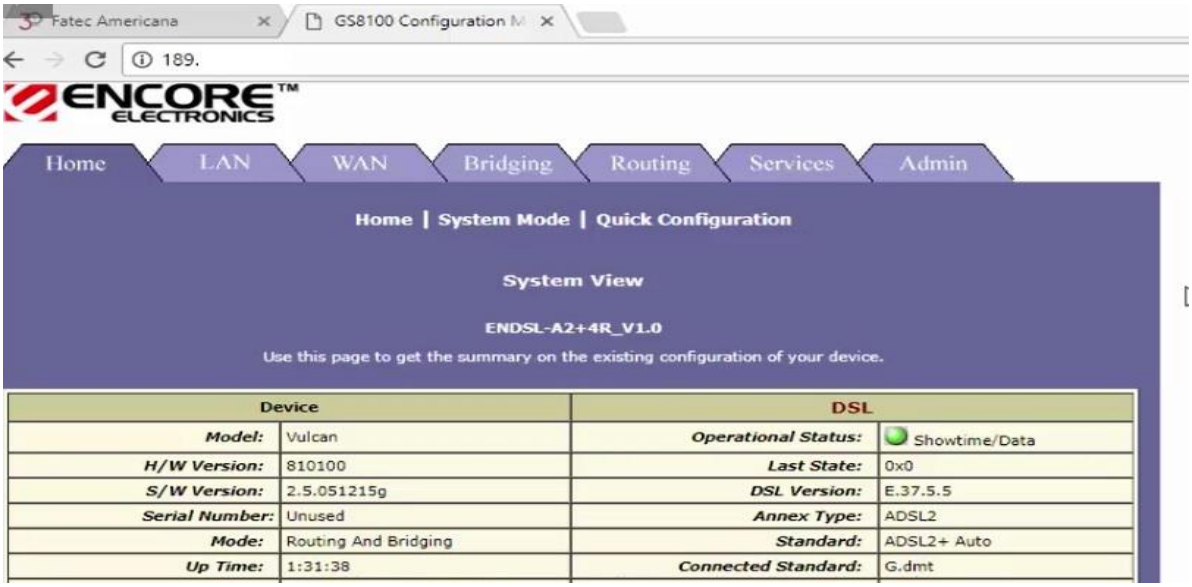
Figura 14 - Login no dispositivo encontrado



Fonte: Elaborada pelo autor.

O login foi executado com êxito, na Figura 15 é apresentada a tela de configuração do equipamento da Marca Encore, modelo ENDSL-A2+4R, que é um *modem* usado por algumas operadoras de Internet.

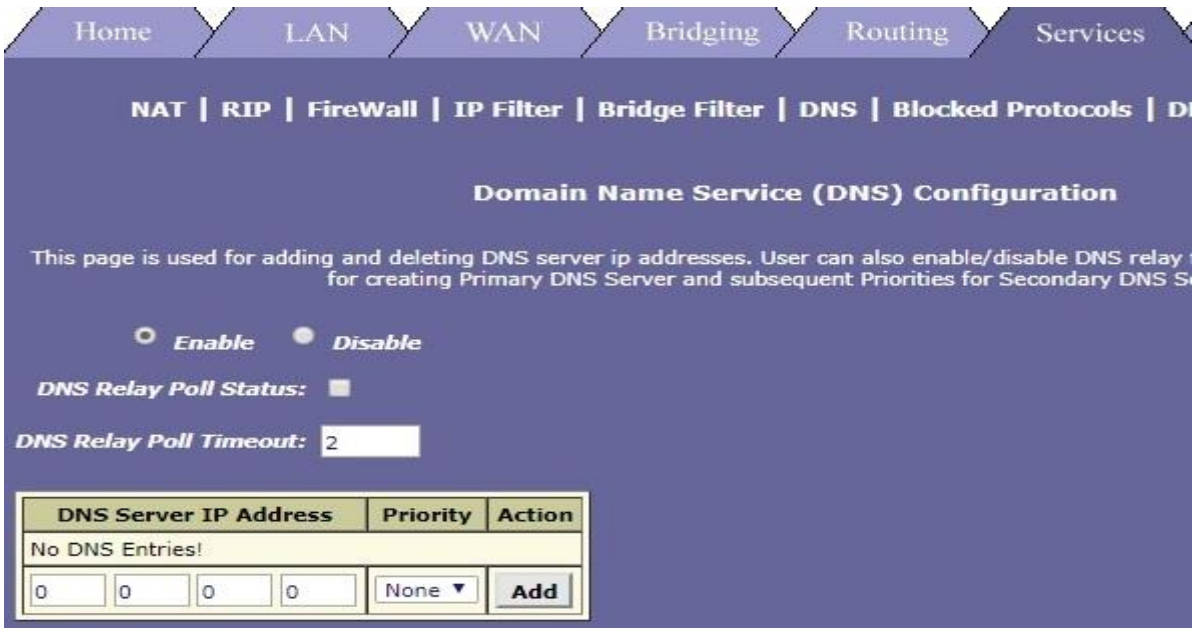
Figura 15 Login efetuado com sucesso



Fonte: Elaborada pelo autor.

Uma vez dentro das configurações do modem, basta navegar pelo menu de configuração e acessar a opção DNS, para que seja realizada a alteração dos endereços de servidor, como mostra a Figura 16.

Figura 16 Navegando pelo dispositivo para alteração do DNS.



Fonte: Elaborada pelo autor.

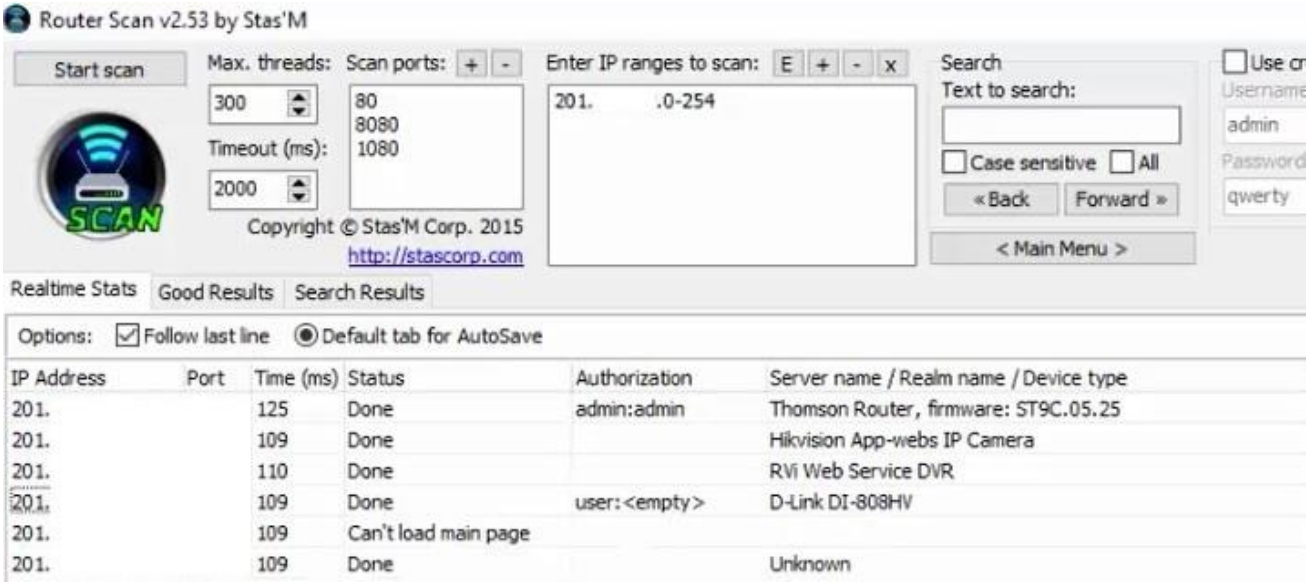
Neste último passo, são inseridos os novos endereços de servidor DNS e em seguida confirmadas as alterações, de acordo com a Figura 17. A partir deste momento, o atacante passaria a aguardar o acesso aos sites maliciosos, ao qual o usuário da rede passaria a ser direcionado.

Figura 17 - Efetuando a alteração de Servidores DNS

Fonte: Elaborada pelo autor.

Varredura 2: Nesta segunda varredura o range de endereços buscado foi 201.**.***.0-254, com as mesmas portas 80,8080 e 1080, conforme observado na Figura 18.

Figura 18 - Segunda varredura utilizando range de endereços IP 201..***.0-254**

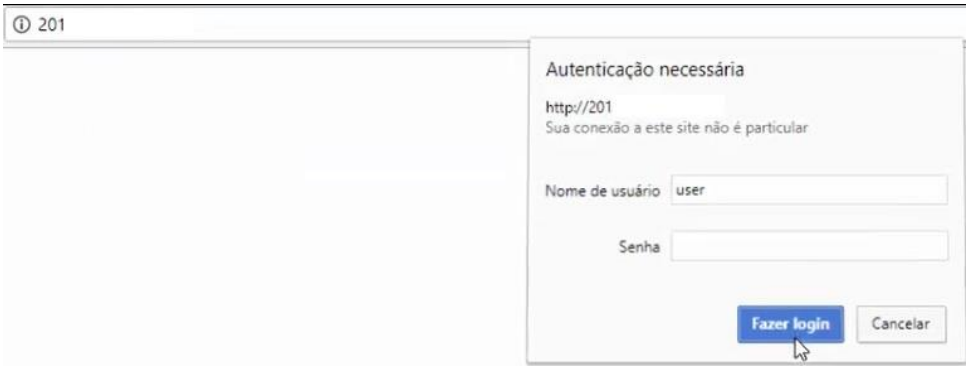


Fonte: Elaborada pelo autor.

Ainda na Figura 18 é possível observar o endereço 201.**.***.**, porta 1080, que traz as informações de usuário e senha na coluna *Authorization.* Assim como realizado na varredura anterior, será feita uma tentativa de acesso com os dados trazidos na varredura.

Na Figura 19 é iniciada a tentativa de acesso ao dispositivo, usando o usuário: user e a senha em branco, padrão de fábrica para este equipamento.

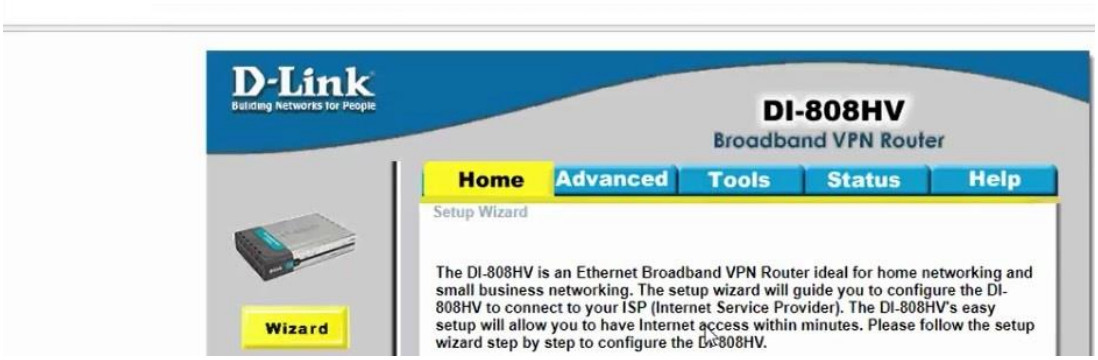
Figura 19 - Tentativa de login no segundo dispositivo



Fonte: Elaborada pelo autor.

Após clicar em login, o acesso é efetuado com sucesso no equipamento marca D-link, modelo DI-808HV, conforme a Figura 20, que é um roteador com o recurso de VPN (*Virtual Private Network*, rede privada virtual), onde é possível criar uma conexão entre a rede interna de uma empresa. Este recurso permite que a rede interna seja acessada de qualquer lugar, através da Internet, em “segurança”. Mas neste caso, o roteador está totalmente vulnerável e coloca em risco todas as informações trafegadas internamente, ou na utilização da VPN.

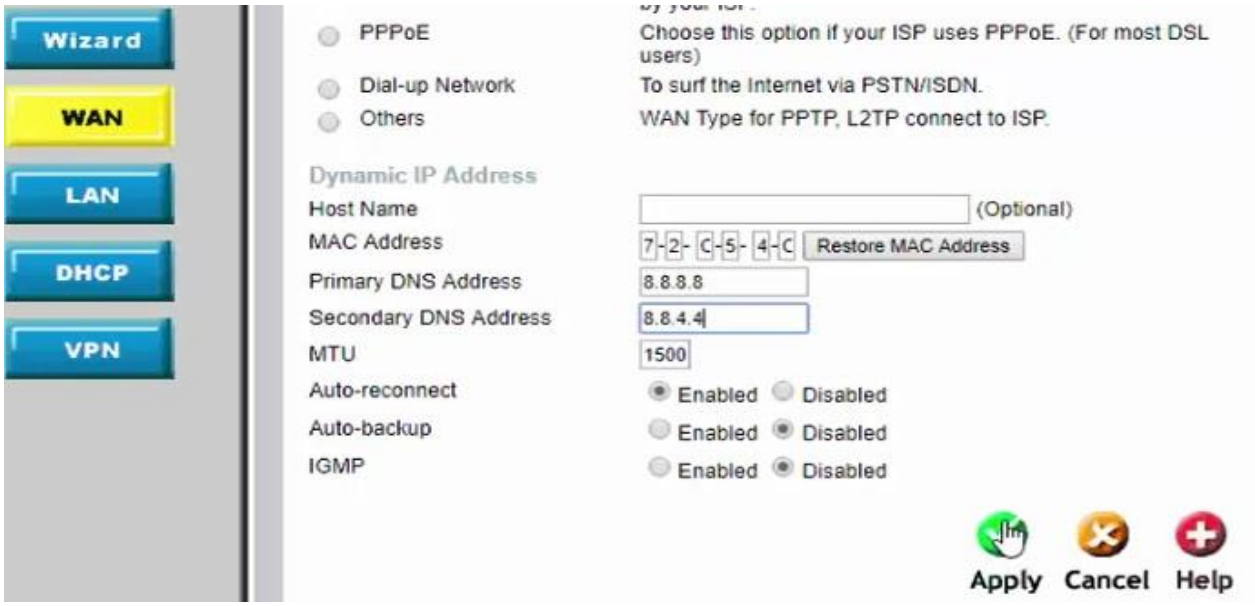
Figura 20 - Acesso efetuado com sucesso no Equipamento DI-808HV



Fonte: Elaborada pelo autor.

Após realizar o acesso ao dispositivo e navegar pelas configurações, é possível facilmente alterar os servidores DNS, bastando inserir os novos endereços e aplicar as alterações, conforme a Figura 21, comprometendo assim a navegação de todos os dispositivos que façam parte desta rede.

Figura 21 - Alteração de endereço DNS no Roteador D-Link



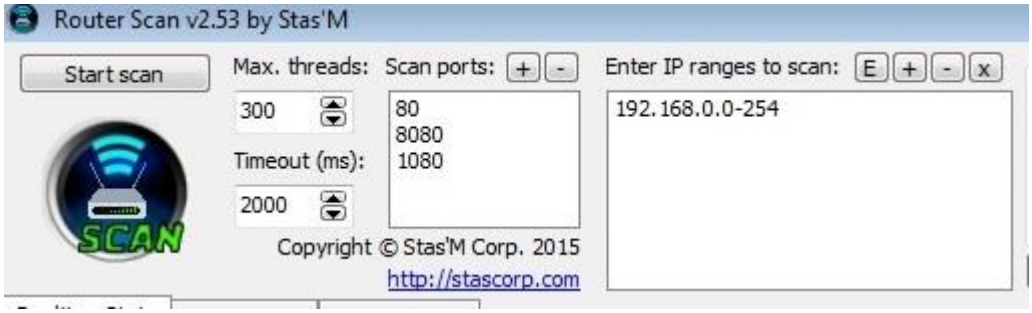
Fonte: Elaborada pelo autor.

4.2 VARREDURA DE EQUIPAMENTO INTERNO (REDE LOCAL)

Varredura Interna: A varredura interna utilizará o mesmo aplicativo Router Scan para obter detalhes de dispositivo.

Na Figura 22 é iniciada a varredura na rede interna com range de endereços:192.168.0.1, portas 80, 8080 e 1080.

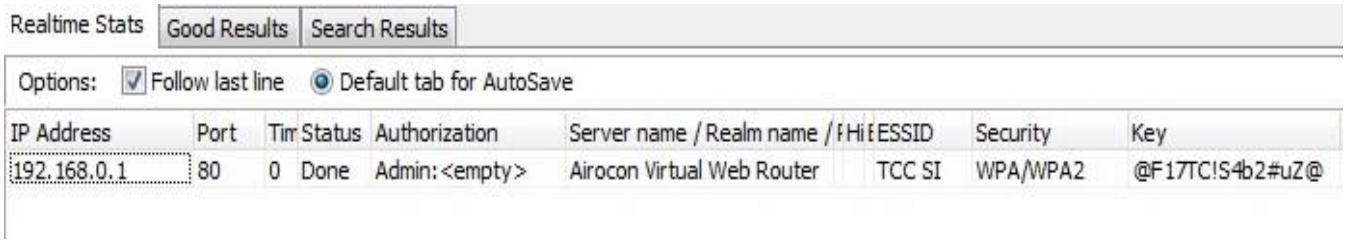
Figura 22 - Varredura interna no range de IP 192.168.0.1-254



Fonte: Elaborada pelo autor.

Ao terminar a varredura são apresentadas as informações do equipamento, como endereço de IP, porta, usuário e senha de acesso as configurações, SSID e senha de acesso à rede sem fio. Neste momento é possível ressaltar que não adianta criar uma senha forte de rede sem fio, mantendo as configurações padrão de fábrica no equipamento, pois elas serão facilmente acessadas e disponibilizadas ao atacante. Estes dados podem ser vistos na Figura 23.

Figura 23 - Resultado da varredura interna



Fonte: Elaborada pelo autor.

Nesta etapa será efetuada a tentativa de login, com os dados informados na coluna *Authorization* do aplicativo, onde o usuário é admin e a senha em branco, conforme Figura 24.

Figura 24 - Acesso ao roteador através das informações da varredura

Fonte: Elaborada pelo autor.

Assim como efetuado nos roteadores externos acessados, é possível navegar pelas configurações e efetuar a substituição do DNS, para o endereço pretendido. Nos testes, foram simuladas trocas pelos servidores 8.8.8.8 e ou 8.8.4.4, conforme Figura 25. Ambos são endereços IP de servidores públicos disponibilizados pelo google, e são considerados confiáveis, mas ao acessar o dispositivo, o atacante poderá redirecionar para o endereço que desejar.

Figura 25 - Endereço de DNS alterado

Fonte: Elaborada pelo autor.

4.3 TORNANDO AS CONFIGURAÇÕES DO ROTEADOR OU MODEM MAIS SEGURAS

Os itens mencionados a seguir podem ser encontrados na grande maioria de roteadores e modens disponíveis no mercado, independente da marca, algumas

configurações simples, podem tornar o dispositivo mais seguro, tornando-o menos vulnerável. É preciso levar em consideração que não existe procedimento totalmente seguro, ou sem falhas, mas o atacante tende a buscar o caminho mais fácil e rápido.

- Verificar se existe uma atualização de *firmware* (software que controla o roteador).

O *firmware* precisa ser atualizado, pois através dele podem ser resolvidas falhas e vulnerabilidades descobertas desde o software anterior.

- Alteração de usuário e senha padrão de acesso ao dispositivo.

Este é um passo primordial, pois como visto anteriormente nos capítulos 4.1 e 4.2, um dispositivo com usuário e senha padrão fica totalmente exposto, permitindo que o atacante tenha alcance a todas as configurações do equipamento. Uma busca na Internet pela marca e modelo do *modem* ou roteador, poderá ajudar a determinar a necessidade desta troca, pois as senhas padrão são facilmente encontradas, mesmo nos modens de algumas operadoras de Internet.

- Desabilitar serviços não necessários ou não utilizados.

Os dispositivos podem vir com serviços e funções habilitadas de fábrica, deve-se manter somente o necessário habilitado, alguns exemplos: desativar rede de convidados (caso não esteja em uso), desabilitar opção de gerenciamento remoto, desabilitar WPS (*Wi-Fi Protected Setup*), desativar protocolos Telnet e SSH (Secure Shell).

- Troca do endereço padrão de acesso ao roteador.

O endereço padrão de acesso é muito previsível e normalmente conhecido por todos, sua troca é necessária para dificultar que um possível invasor possa facilmente localizar o equipamento e tentar acessar as configurações.

- Desabilitar a transmissão SSID (nome da rede).

A transmissão do SSID deve ser desabilitada, pois desta forma para ingressar na rede, será necessário saber o seu nome e senha, não permitindo que o nome da rede fique disponível para todos.

- Habilitar o isolamento sem fio.

Esta etapa permite que os dispositivos que estão conectados, apenas troquem informações com o roteador, não possibilitando o acesso aos demais dispositivos conectados à rede, seja através de cabo ou sem fio.

- Segurança WPA2-PSK AES

Atualmente este é o padrão mais seguro, onde existe a combinação do padrão WPA2-PSK (*Wi-Fi Protected Acces 2- Pre-Shared Key*) e o algoritmo de segurança mais avançado AES (*Advanced Encryption Standard*).

Estas são configurações simples e possíveis de realização em diversos modelos de equipamento, e que podem aumentar significativamente a segurança na rede, seja ela com ou sem fio.

Na Figura 26, foi efetuada uma nova varredura após seguir alguns passos da configuração. Nota-se uma melhora significativa, pois o atacante já não possui os dados de acesso à configuração ou rede sem fio. Os passos seguidos foram: troca de usuário e senha padrão de acesso ao roteador, troca de endereço de acesso ao roteador e desabilitar SSID de rede sem fio, estas alterações elevaram a segurança do dispositivo e diminuíram a previsibilidade da configuração.

Figura 26 - Varredura após configuração do dispositivo

Fonte: Elaborada pelo autor.

Nas varreduras efetuadas nos subcapítulos 4.1 e 4.2, é possível notar que muitos equipamentos são mantidos com configurações padrão de fábrica, tornando os dispositivos vulneráveis e suscetíveis a ataques. Isto se dá, pois, o atacante pode facilmente adentrar no equipamento e efetuar as alterações que deseja, como por exemplo a já citada alteração de DNS.

Algumas medidas que visam minimizar vulnerabilidades e trazer um aumento na segurança dos dispositivos, são apresentadas no capítulo 4.3, que de acordo com os testes efetuados promovem uma significativa melhora.

5. CONSIDERAÇÕES FINAIS

Uma rede residencial ou de pequenas empresas, tem como ponto principal e mais crítico o dispositivo roteador ou *modem*, que é o equipamento responsável por gerenciar as diversas conexões feitas pelos dispositivos. É preciso levar em consideração que uma vez conectado à Internet, este equipamento poderá ficar vulnerável e visível para todos que também tenham acesso à Internet.

Com base nos dados apresentados, é nítido o crescimento da Internet nos domicílios brasileiros, assim como o aumento do uso da Internet em *smartphones, tablets, notebooks,* entre outros dispositivos. Esse crescimento faz com que os dispositivos tragam mobilidade e comodidade a seus usuários, tornando o uso da rede Wi-Fi indispensável.

Em contrapartida é preciso considerar que o número de cibercrimes no Brasil também possui um número expressivo, e de acordo com os dados mencionados no desenvolvimento teórico, muitos usuários já foram afetados, causando prejuízo financeiro.

A partir deste cenário, onde temos maior facilidade de acesso à Internet e as informações, é preciso ressaltar a necessidade de se empregar segurança para que estas informações continuem disponíveis, integras, confidenciais e mais seguras.

Fica claro que o emprego de configurações adequadas nos roteadores e modens, ajudam a mitigar possíveis riscos de ataques e invasões, sem causar grande ônus ao proprietário da rede, uma vez que os passos descritos neste trabalho, são funções disponíveis de configuração e ativação nativas dos equipamentos.

Assim, em um passo inicial e muito importante, os usuários deveriam criar a cultura de preservação de dados, a começar por suas redes residenciais, tomando conhecimento claro sobre o valor que possui a informação. A partir deste

entendimento, será mais simples empregar e seguir políticas de segurança mais complexas e cuidadosas que garantiriam um ganho maior em segurança das informações.

ESTUDOS FUTUROS

A área de segurança da informação está em constante mudança, pois a cada dia são descobertas novas vulnerabilidades, necessitando assim de estudos que busquem mitigar riscos ou mesmo soluções que antecipem futuras explorações de vulnerabilidades. Recentemente, mais precisamente no mês de outubro de 2017, houve a quebra do protocolo de segurança WPA2 para redes Wi-Fi, com uma vulnerabilidade conhecida como KRACK (*Key Reinstallation Attacks* ou Ataques de Reinstalação de Chaves), que consta no registro de vulnerabilidades conhecidas CVE-2017-13077[1], sendo este um bom tema para estudos futuros.

Outra sugestão para estudo é a segurança para Internet das Coisas, pois é um campo com amplo potencial de crescimento e consequentemente com possíveis explorações de vulnerabilidades. Desta forma a aplicação de configurações que busquem minimizar ataques, são também um tema para continuidade e estudos futuros.

[1] CVE-2017-13077 – CVE(Common Vulnerabilities and Exposures) – Disponível em: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13077, Acesso em 10 dez. 2017.

REFERÊNCIAS

ALVES, C. B. **Segurança da informação vs engenharia social**. Brasilia: [s.n.], 2010.

AVAST SOFTWARE. Disponivel em: <https://www.avast.com/pt-br/c-pharming>. Acesso em: 1 nov. 2017.

CASSANTI, M. D. O. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

DANTAS, M. **Redes de comunicação e computadores:** abordagem quantitativa. Florianópolis: Visual Books, 2010.

FEREIRA, F. N. F.; ARAÚJO, M. T. **Política de segurança da informação**. Rio de Janeiro: Ciência Moderna, 2006.

IMONIANA, J. O. **Auditoria de sistemas de informação**. São Paulo: Atlas, 2011.

JOBSTRAIBIZER, F. **Desvendando as redes sem fio**. São Paulo: Digerati Books, 2010.

KUROSE, J. F. **Redes de computadores e a Internet:** uma abordagem top-down. 5. ed. ed. São Paulo: Pearson, 2010.

LYRA, M. R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Moderna, 2008.

MONTICO, M. **Guia avançado de redes wireless**. São Paulo: Digerati Books, v. v2, 2010.

OLIVEIRA, H. A. Disponivel em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwivjfer59DXAhVIWpAKHSiGA0YQFggnMAA&url=http%3A%2F%2Fportal.tcu.gov.br%2Flumis%2Fportal%2Ffile%2FfileDownload.jsp%3FfileId%3D8A8182A14E01F8FC014E02CA0C3626DE&usg=AO>. Acesso em: 10 set 2016.

Routerpwn, 2017. Disponivel em: <http://routerpwn.com/>. Acesso em: 2017 out. 15.

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

SCHIMDT, P.; SANTOS, J. L. D.; ARIMA, C. H. **Fundamentos de auditoria de sistemas**. São Paulo: Atlas, 2006.

SYMANTEC CORPORATION, 2016. Disponivel em: <https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf>. Acesso em: 2017 out. 5.

TREND MICRO, [s.d]. Disponivel em: <https://documents.trendmicro.com/assets/wp/wp-securing-your-home-routers.pdf>. Acesso em: 31 out. 2017.

UFCG. Guglielmo Marconi. **UAEC/UFCG**, 2016. Disponivel em: <http://www.dec.ufcg.edu.br/biografias/Guglielm.html>. Acesso em: 16 nov. 2016.