Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

PEDRO MAURICIO DOMINGUES FILHO

ESTRATÉGIAS VOLTADAS A SEGURANÇA DA INFORMAÇÃO EM MICRO E PEQUENAS EMPRESAS, COM O AUXÍLIO DA TECNOLOGIA MIKROTIK

Assis/SP
2018

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

PEDRO MAURICIO DOMINGUES FILHO

ESTRATÉGIAS VOLTADAS A SEGURANÇA DA INFORMAÇÃO EM MICRO E PEQUENAS EMPRESAS, COM O AUXÍLIO DA TECNOLOGIA MIKROTIK

Projeto de pesquisa apresentado ao curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando: Pedro Mauricio Domingues Filho
Orientador: Me. Fábio Éder Cardoso

Assis/SP
2018

FICHA CATALOGRÁFICA

D671e DOMINGUES, Pedro Mauricio.
Estratégias Voltadas a Segurança da Informação em Micro e Pequenas Empresas, com o Auxílio da Tecnologia Mikrotik / Pedro Mauricio Domingues Filho. Fundação Educacional do Município de Assis –FEMA – Assis, 2018.

70p.

Trabalho de conclusão do curso (Ciência da computação). – Fundação Educacional do Município de Assis – FEMA

Orientador: Ms. Fábio Eder Cardoso

1. Mikrotik 2. Segurança da Informação 3. Proteção de Informações.

CDD: 005.8

ESTRATÉGIAS VOLTADAS A SEGURANÇA DA INFORMAÇÃO EM MICRO E PEQUENAS EMPRESAS, COM O AUXÍLIO DA TECNOLOGIA MIKROTIK

PEDRO MAURICIO DOMINGUES FILHO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Me. Fabio Eder Cardoso

Examinador: _____
Dr. Luiz Carlos Begosso

Assis/SP
2018

DEDICATÓRIA

Dedico este trabalho aos meus pais que sempre me apoiaram e me incentivaram nesta longa caminhada.

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, pois nada sou sem Ele.

Em especial a meus pais que não mediram esforços e sempre me apoiaram e me deram condições de estar realizando este curso de nível de superior, independentemente das dificuldades. A minha noiva que sempre esteve ao meu lado, me incentivando e auxiliando em minhas tomadas de decisões.

Agradeço a meu orientador Fábio Éder Cardoso, não só pelo mestre que foi mas, também, pelo amigo que é.

“A tecnologia vai reinventar o negócio, mas as relações humanas continuará a ser a chave para o sucesso”.

- Stephen Richards Covey

RESUMO

Com um significativo aumento na criação de micro e pequenas empresas, o fácil acesso destas a sistemas de gestão de vendas, estoques e notas fiscais, que necessitam da Internet para seu funcionamento, e os eminentes ataques cibernéticos e roubos de dados, surge a necessidade de estratégias e ferramentas que traga ao microempreendedor proteção e praticidade na gestão de sua rede, sem a necessidade de um investimento alto. Tendo em vista estes fatos, este trabalho apresenta uma ferramenta de baixo custo e fácil acesso, que, a partir de estratégias elaboradas, buscará resolver os problemas relacionados e segurança da informação de micro e pequenas empresas.

Palavras-chave: Segurança da Informação, Proteção, Empresas, MikroTik.

ABSTRACT

With a significant increase in the creation of micro enterprises and small enterprises, the easy access to the management systems of sales, inventory and invoices, who need the Internet for its operation, and the eminent cyber attacks and data theft, arises the need for strategies and tools that bring to the microentrepreneur protection and convenience in managing your network, without the need of a high investment.In view of these facts, this work present a tool of low cost and easy access, which, from strategies devised, will seek to resolve problems and information security of micro and small enterprises.

Keywords: Information Security, Protection, Enterprises, MikroTik.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas
AEP - Advanced Encryption Package
ARP - Adress Resolution Protocol BSSID - Basic Service Set Identifier
DHCP - Dynamic Host Configuration Protocol
FTP - File Transfer Protocol
GUI - Graphical User Interface
ICMP - Internet Control Message Protocol
IP - Internet Protocol
ISO - International Organization for Standardization
LAN - Local Area Networks
MAC - Media Access Control
P2P - peer-to-peer
PING - Packet InterNet Grouper
PSK - Pre-Shared Key
SSH - Secure Shell
TCP - Transmission Control Protocol
TI - Tecnologia da Informação
UDP - User Datagram Protocol
VPN - Virtual Private Network
WAN - Wide Area Network
WLAN - Wireless Local Area Network
WPA - Wi-Fi Protected Access

SUMÁRIO

1. INTRODUÇÃO

Com o grande avanço da tecnologia e o acesso fácil à rede mundial de computadores, empresas estão aderindo a sistemas que utilizam da Internet para variados serviços; desde um simples cadastro de clientes até uma transferência bancária. Não apenas grandes multinacionais, mas, também, microempresas e empresas de pequeno porte, utilizam sistemas de e-commerce, devido ao fácil acesso à Internet e os valores de sistemas web. “A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade. (Rezende e Abreu, 2000)”.

O grande problema surge quando os dados estão expostos na Internet. Sem uma devida proteção as informações estão suscetíveis a ataques de hackers, levando, consequentemente, a sequestros e perdas de dados e também de ações e valores. A informação, hoje, pode ser considerada o coração de uma empresa. Tudo sobre ela, seus clientes, serviços, valores, lucros, entre outros, estão nas informações, ou seja, a proteção destas é essencial em qualquer empresa. Em uma empresa, independente do seu tamanho, é indispensável uma política de segurança da informação como estratégia de gestão. Pode-se entender segurança como atitudes em relação aos processos de gestão da informação. Podemos definir Segurança da Informação, como uma grande área do conhecimento que é voltada a proteção das informações contra acessos não autorizados, acessos não autorizados ou sua indisponibilidade (Sêmola, 2003). Porém, a norma ISO/IEC 17799:2001, afirma que a Segurança da Informação entende por proteger as informações contra inúmeras ameaças, a fim de dar continuidade ao negócio (ABNT, 2003).

O objetivo é proteger as informações e dados das empresas. Mesmo não sendo de porte grande, uma empresa, no cenário atual, está predisposta às ameaças à sua segurança, como por exemplo, *worms*, ataques à rede, fraudes, *scans*, *malwares*, entre outros.

Devido a uma dependência das empresas criada pela utilização de sistemas eletrônicos e tecnologias de trabalho, estas estão necessitando de segurança digital, pois suas informações se tornam vulneráveis a ataques. Sendo assim é importante possuir mecanismos de segurança de sistema de informações, a fim de prevenir acessos não autorizados aos recursos e dados (Laureano, 2005).

Tendo como base microempresas e empresas de pequeno porte, cada uma possui sua rede por onde trafegam seus dados. Algumas possuem uma rede local (LAN) e outras possuem, também, uma rede wireless (WLAN) para serviços mais rápidos. Grandes empresas utilizam servidores próprios e redes privadas, como por exemplo a VPN. Porém, devido a um custo elevado nos serviços de Virtual Private Networking, empresas de menor porte buscam outras estratégias e métodos de garantir a integridade de seus dados.

1.1. OBJETIVOS

O objetivo central deste trabalho consiste em elaborar e apresentar estratégias acessíveis e eficientes de segurança da informação à micro e pequenas empresas, baseadas na tecnologia MikroTik.

Com o desenvolvimento deste estudo, será possível traçar estratégias de gerenciamento, monitoramento e proteção das informações de uma empresa, utilizando da tecnologia MikroTik em uma arquitetura de TCP/IP.

A fim de atingir os objetivos desejados, este projeto de pesquisa foi divido em duas fases:

1ª fase: Elaboração de uma estrutura de rede, com o auxílio da tecnologia MikroTik, aplicando políticas de segurança da informação.

2ª fase: Realização de testes de vulnerabilidade na estrutura criada, com o auxílio do sistema operacional Kali Linux.

1.2. JUSTIFICATIVAS

Diante do cenário atual, onde ataques hackers tem preocupado não somente empresas, como também a população em geral, é indispensável medidas de proteção aos dados, principalmente, no que se refere a dados empresariais. Estima-se que cerca de cem países foram afetados com ataques *hackers* em maio de 2017, gerando um lucro aos cyber-criminosos, estimando em cerca de um bilhão de dólares (G1, 2017). Entre as vítimas estavam usuários e empresas, sejam elas de grande ou pequeno porte. Em uma

ocasião, onde há o sequestro de informações, o pagamento de resgate de dados pode variar entre trezentos a quase mil dólares (G1, 2017). Levando em consideração uma micro ou pequena empresa, um valor deste solicitado, poderia facilmente, obrigar o fechamento da mesma.

Apesar do Brasil possuir uma lei no que se refere aos crimes informáticos **(**Lei Nº 12.737, de 30 de Novembro de 2012), a mesma não apresenta a devida eficácia uma vez que, em um ataque cibernético, é árduo encontrar um responsável por tal, tendo em vista o uso de mecanismos de anonimato. Porém, ao encontrar o *hacker* responsável por tal ataque, as penas previstas na lei acima citada, são de natureza leve; detenção, de 3 (três) meses a 1 (um) ano, e multa (Planalto, 2012). Sendo assim, é de suma importância o desenvolvimento de estudos e estratégias de defesas, que possam permitir ao microempreendedor proteger seu patrimônio virtual e sua ferramenta eletrônica de trabalho.

Porém, o investimento em uma rede privada, como por exemplo, a VPN pode ser um pouco elevado no bolso do microempreendedor. Sendo assim, utilizando uma rede local (LAN) e a arquitetura TCP/IP, os dados e informações estariam desprotegidos; sem mencionar o fato do administrador na rede, não poder ter um controle da rede, dos acessos a ela e nem mesmo gerenciar o que pode ser acessado e por quem.

A tecnologia MikroTik poderia ser a opção para solução destes problemas. Com ela, a segurança dos dados, o gerenciamento da rede, as limitações de acesso entre outros fatores, estarão garantidos nas mãos do administrador. As grandes vantagens geram em torno do fácil acesso à tecnologia, do custo acessível e pelo fato de poder sem implementada em uma rede local, seja ela cabeada ou *wireless*.

1.3. MOTIVAÇÃO

Em um mundo globalizado, onde a rede mundial de computadores tornou-se ferramenta indispensável para todos os tipos de empresas, surge a praticidade, mas, por outro lado, junto à ela também a insegurança. Grandes empresas e multinacionais renomadas, tem parte de seu financeiro investido em segurança da informação. Porém, micro e pequenas empresas, principalmente as que estão em início de exercício, pouco tem para um alto investimento em segurança de sua rede. Assim, surge uma necessidade de estratégias que tragam ao microempreendedor, não só segurança, mas também, praticidade e

conforto, a um custo acessível ao financeiro daquela empresa. Atendendo a estas exigências, a tecnologia Mikrotik surge como uma solução. Devido ao fato de micro e pequenas empresas utilizarem, em sua maioria, uma rede do tipo LAN ou WLAN, que são redes utilizadas nas maiorias das residências, as estratégias aqui apresentadas podem ser utilizadas não somente a elas, mas também, em redes domésticas com o auxílio de um MikroTik Ethernet Router, por exemplo. Esta estrutura em rede agrada por sua praticidade, fácil acesso e baixo custo de investimento.

O simples fato de uma micro empresa utilizar de uma rede LAN ou WLAN (tipo de rede utilizada em residências), as estratégias aqui apresentadas, poderão ser implantadas, não somente na micro empresa, mas também, em qualquer residência, onde os usuários poderão proteger suas respectivas redes.

1.4. PERSPECTIVA DE CONTRIBUIÇÃO

A proposta deste estudo será encontrar métodos alternativos para proteção, gerenciamento e controle de rede de uma micro empresa, sem custos mensais e de altos valores. Com ele, será possível desenvolver uma estrutura de rede mais segura e confiável, sem um alto custo de investimento por parte do microempreendedor.

Outro fator positivo está no fato de uma micro empresa possuir redes locais (LAN), como já citado acima; o mesmo tipo de rede presente na maioria das residências. Sendo assim, as estruturas e as políticas de segurança aplicadas neste estudo, podem também, ser aplicadas em qualquer residência, aumentando assim, a segurança e confiabilidade de uma rede doméstica.

2. CONCEITOS E DEFINIÇÕES

Para a implementação da segurança da informação em micro e pequenas empresas, será necessária compreensão desta e suas definições.

2.1. A SEGURANÇA DA INFORMAÇÃO

Segundo a norma ABNT NBR ISSO/IEC 17799 a informação é um importante e essencial ativo para os negócios de uma determinada organização que necessita, consequentemente, de adequada proteção. Esta informação pode vir representada em diferentes formas, desde impressa ou manuscrita até mesmo por ambientes eletrônicos. Porém, independentemente da forma a qual venha a ser representada, compartilhada e armazenada, recomenda-se proteção as mesmas.

Através de um conjunto de controles, políticas de segurança, estruturas bem organizadas e auxílio de *softwares* ou *hardwares* de proteção, é obtida a segurança da informação. Toda esta estrutura e políticas de segurança devem ser, constantemente, monitoradas, analisadas e, se necessário, aperfeiçoadas, a fim de garantir a proteção e integridade das informações, como por consequência, diminuir os riscos que uma má proteção as mesmas desencadeariam, como por exemplo, a perda de dados, investimentos, capital e, consequentemente, uma possível interrupção nos negócios.

Para que haja a segurança da informação, se faz necessário respeitar três pontos importantes, chamados de “pilares da segurança da informação”. Estes pontos são: Confidencialidade, Disponibilidade e Integridade.

Na confiabilidade é necessário proteger as informações com o intuito de evitar perdas e inadequadas divulgações das mesmas. Sendo assim, torna-se necessário a aplicação de algoritmos ou métodos de criptografia. Outras boas práticas sugeridas consistem na ocultação de dados, exclusão de dados após seu devido uso e sistemas ou métodos de autenticação.

A disponibilidade dispõe em garantir acessibilidade ao *software* ou *hardware* através de sistemas. Nela está, também, a redução de vulnerabilidade em sistemas de uso comercial, ou qualquer outro sistema computacional.

Por fim, a integridade deve ser responsável por garantir que dados não sejam alterados, excluídos ou copiados de formas não autorizadas.

2.2. CRIMES VIRTUAIS

Recentemente criada a Lei Nº. 12.737 de 30 de Novembro de 2012, que altera o Decreto-Lei Nº. 2.848 de 7 de Dezembro de 1940 (Código Penal), “dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências” (Planalto, 2012).

O Art. 154-A da mesma lei prevê pena de três meses a um ano de detenção, para o responsável por uma invasão a dispositivo informático alheio.

> *Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.*

De acordo com o parágrafo terceiro da mesma, a pena é agravada em casos de obtenção de informações sigilosas ou segredos comerciais e industriais.

> *§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.*

O parágrafo quarto ainda aumenta a pena prevista no parágrafo terceiro em caso de divulgação ou comercialização dos dados obtidos a terceiros.

> *§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.*

Apesar de ser considerada um avanço no que se refere a crimes cibernéticos e suas punições, muitos especialistas criticam a nova lei apontando falhas e “brechas” na mesma, que a tornariam ineficaz. Um dos pontos criticados é a violação do mecanismo de

proteção do equipamento invadido. Se o computador não possui mecanismos de defesa ou senha não será possível demonstrar violação. (Tomazi, 2013).

Devido a flexibilidade da lei, apontada por especialistas, a proteção das informações e dados acaba por se tornar ainda mais importante.

2.3. ÉTICA HACKER

De acordo com o grego, ética (ou simplesmente *éthos*) pode ser entendido como costume ou apenas propriedades de caráter. Pode-se entender a ética como tudo aquilo que é bom (MOORE, 1975) e que a pessoas realize a sim mesmo como tal, ocupando-se e pretendendo atingir a perfeição humana (CLOTET, 1986).

A ética *hacker* segue uma política ética onde o indivíduo que possui os conhecimentos de *hacking*, aplica estes, com o objetivo defensivo, a fim de detectar falhas e vulnerabilidades que possam causar prejuízos e perdas. A ética *hacker* tem por finalidade buscar e alcançar a perfeição; se um determinado sistema (ou rede – como no caso deste estudo) está suscetível a imperfeições, o *hacker* ético tem como objetivo analisa-las e aperfeiçoa-las.

Embora muitas pessoas tenham a visão preconceituosa quanto ao que se refere aos *hackers,* há o que difere um criminoso virtual e um profissional da área de segurança. Sendo assim, em meados dos anos 80, alguns meios de comunicação denominaram como *crackers,* os indivíduos que faziam o uso destrutivo de um computador por meio da Internet, a fim de evitar quaisquer tipos de transtorno (HIMANEN, 2001).

Hacker é o que busca explorar detalhes de sistemas, ampliando suas capacidades e sendo um indivíduo dedicado a programação, tendo paixão por tal e crendo que seu dever seja compartilhar informações e aplicações de forma gratuita (HIMANEN, 2001).

Por sua vez, o *cracker*, que também pode ser conhecido como *black hat (“*chapéu negro”) tem o objetivo de invadir os sistemas que outros protegem (RAYMOND, 2002).

Neste meio é possível identificar os denominados *white hat,* que são os que identificam falhas e vulnerabilidades em sistemas e que, ao invés de aproveitar esta para benefícios próprios, alertam os responsáveis por tais sistemas, a fim de buscarem aperfeiçoa-los em níveis de segurança (ROUSE, 2007).

Por fim há o indivíduo que está entre o *black hat e o white hat:* o *gray hat.* Este, por sua vez, se assemelha com o *white hat,,*porem, ao encontrar uma determinada falha torna-a publica, expondo a falha encontrada a indivíduos mal intencionados (ROUSE, 2007), tornando aquele sistema e seus responsáveis suscetíveis a ataques.

Muitas empresas na área de segurança ou que dependem de tal área, utilizam de testes de invasão, a fim de atinarem alguma vulnerabilidade, que possa vir a ser prejudicial a instituição. Estes testes são conhecidos na área de segurança da informação como *penTests.*

2.4. PENTEST (TESTE DE PENETRAÇÃO)

Muito utilizado por corporações de segurança da informação, o *pentest* é uma prática de testes em sistemas computacionais que utilizam da Internet, com a finalidade de encontrar vulnerabilidades que poderiam ser exploradas por invasores (ROUSE, 2011) e consequentemente, levando a sérios prejuízos aos proprietários (e usuários) de uma determinada aplicação. O principal objetivo destes testes é desvendar pontos fracos na segurança em uma estrutura de rede ou falhas em aplicações. Como já citado, o *pentest* pode ser também conhecido como ataques *white hat.*

Os *pentests* podem ser realizados de forma manual ou com auxílio de aplicações. As informações obtidas com o *pentest*, sobre qualquer tipo de vulnerabilidade da rede, são expostas aos gerentes de TI (ou proprietários da rede – no caso de uma micro empresa) para auxilia-los em tomadas de decisões e estratégias, a fim de aumentar os níveis de segurança da referida rede.

As estratégias de *pentests* incluem:

• *Targeted testing*: um teste realizado por uma equipe de TI de determinada organização e por uma equipe de teste.

• *External testing*: teste realizado com a finalidade de descobrir se um invasor externo pode ter acesso a dispositivos visíveis fora da empresa.

• *Internal testing*: teste simulando um ataque por trás do firewall. Destinado a funcionários insatisfeitos com a organização e que podem atacar os sistemas por ter privilégios de acesso.

• *Blind testing*: teste que simula as ações reais de um invasor, limitando informações necessárias.

• Double *blind testing*: semelhante ao *blind testing*, porém, poucas pessoas devem estar relacionadas ou cientes ao teste, a fim de verificar não somente as vulnerabilidades da estrutura de segurança, mas também aos procedimentos tomados em caso de invasão.

3. TECNOLOGIAS E MEDOTOLOGIAS

Abordado como solução no aumento da segurança, desempenho e gerência de rede, este capítulo transcreve sobre a empresa MickoTik, as tecnologias utilizadas neste estudo e a metodologia que será aplicada.

3.1. MIKROTIK

Fundada em 1996 na Letônia, a Mikrotik é hoje uma renomada empresa de venda de hardwares e softwares para conectividade com a Internet.

Para este estudo foram escolhidos dois produtos da empresa: o MikroTik RouterOS e o MikroTik hAP lite.

MikroTik RouterOS é um sistema operacional baseado em Linux, que permite que uma plataforma x86 se torne um roteador, com serviços de VPN, Proxy, Controle de Banda, QoS, *firewall* entre outros, sendo possível também, trabalhar com suporte de protocolos de roteamento. Para a administração deste ambiente, será utilizada a ferramenta Winbox.

Desenvolvida para as plataformas MS Windows, Linux e Mac, WInbox é uma Graphical User Interface (GUI) responsável por administrar o RouterOS, permitindo uma conexões File Transfer Protocol (FTP), Telnet e Secure Shell (SSH).

Como dispositivo de hardware foi escolhido o MikroTik hAP (home Access Point), devido sua praticidade, custo acessível e possibilidade de ser configurado para roteamento sem fio (Wi-fi). Equipado com CPU de 650 MHz, 32 GB de RAM e *dual chain* de 2.4 GHz *onboard wireless*.

3.2. KALI LINUX

Kali Linux é uma distribuição GNU/Linux baseada no Sistema Operacional Debian (Linux). O projeto é desenvolvido e distribuído pela Offensive Security Ltd.

O Sistema Operacional fornece diversas aplicações voltadas para *PenTests* (Testes de Intrusão), ou seja, é possível analisar falhas em sites, servidores e redes (que é o foco deste estudo).

Dentre algumas aplicações deste Sistema Operacional, três serão utilizadas neste estudo e serão analisadas: Wireshark e Nmap.

Wireshark é um software, desenvolvido pela empresa de mesmo nome, capaz de analisar o tráfego de uma rede organizá-los por protocolos. Sendo assim, a aplicação poderá analisar, não somente uma máquina, mas sim, outros dispositivos e máquinas conectadas a uma determinada rede.

O Network Mapper, ou simplesmente, Nmap, é uma aplicação de port scanner (scanner de portas). Com este é possível realizar um scanner das portas livres e vulneráveis de dispositivos conectados a uma determinada rede, independente do protocolo utilizado (TCP ou UDP); expor hosts disponíveis na rede; detecção de informações dos dispositivos conectados à rede, além de obter informações furtivas destes.

3.3. METODOLOGIA APLICADA

As fases deste estudo seguirão conforme a Tabela 1.

Fase	Descrição	Objetivo
1: Pentest Pré-Mikrotik	Simular acessos indevidos à rede da vítima, apenas esta dispondo de proteção padrão	Expor as vulnerabilidades que a rede da vítima apresenta
2: Implantar o Mikrotik hAP	Instalação do Mikrotik hAP e configura-lo com as melhores estratégias (cabíveis a micro empresa)	
3: Pentest Pós-Mikrotik	Simular acessos indevidos à rede da vítima, dispondo de proteção implementada com Mikrotik	Apresentar a diferença entre a proteção padrão e a proteção com estratégias elaboradas e com o Mikrotik hAP

Tabela 1: Fases da Metodologia Aplicada
Fonte: Banco de imagens Windows

A importância deste estudo consiste em demonstrar a eficiência de uma política de segurança bem elaborada, levando em consideração, a necessidade de cada micro empresa. Vale ressaltar, que nem sempre as estratégias elaboradas a uma determinada micro empresa, pode ser levada em consideração a outra. É importante analisar, primeiramente, a rotina e as ferramentas de trabalho em cada uma, antes de quaisquer modificações na rede ou segurança, pois, uma modificação mal planejada poderá

acarretar em lentidões ou falhas em determinadas aplicações, prejudicando o andamento do serviço ou prejuízos financeiros.

4. PENTEST PRÉ-MIKROTIK

Com a finalidade de demonstrar a funcionalidade da tecnologia Mikrotik, esta fase será destinada a um *pentest* anterior a instalação do Mikrotik hAP Lite, simulando as vulnerabilidades em que uma micro empresaria estaria exposta, ao utilizar de técnicas de proteção padrão.

4.1. CONFIGURANDO REDE LOCAL

Como já citado acima, micro empresas dispõe de redes locais (LAN), ou seja, o mesmo tipo de Internet encontrada em residências. Sendo assim, com o objetivo de realizar este estudo, será utilizada uma rede local com um roteador *wireless*.

A Figura 1 representa o esquema padrão de conexão; onde um roteador distribui sinal *wireless* (Wi-fi) e, podendo também, possuir *desktops* conectados via cabo.

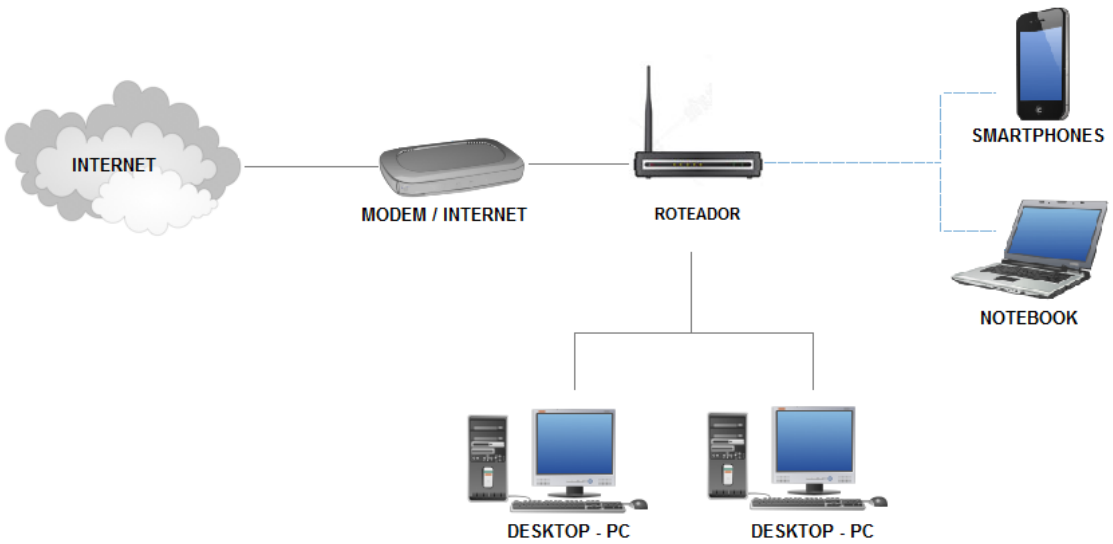

Figura 1: Esquema de Conexão Com Roteador Padrão
Fonte: Banco de imagens Windows

Como a estrutura possui um roteador com a finalidade de distribuir a Internet aos dispositivos nela conectados, será necessário configurá-lo. Neste estudo utilizaremos o

padrão proposto pelo roteador; um usuário protegido por senha. O protocolo de segurança estabelecido é o WPA (Wi-fi Protected Access).

De maneira que o estudo é voltado a micro e pequenas empresas, as configurações serão baseadas em tais, a fim de simular o cotidiano de uma micro empresa.

Muitas micro empresas não dão o devido valor as senhas que protegem suas redes *wireless*. Uma prática comum, não somente em pequenas empresas mas também em residências, é utilizar nos caracteres da senha o mesmo nome da rede.

Como descrito acima, a rede para simulações de ataque deste estudo será configurada conforme a Figura 2.

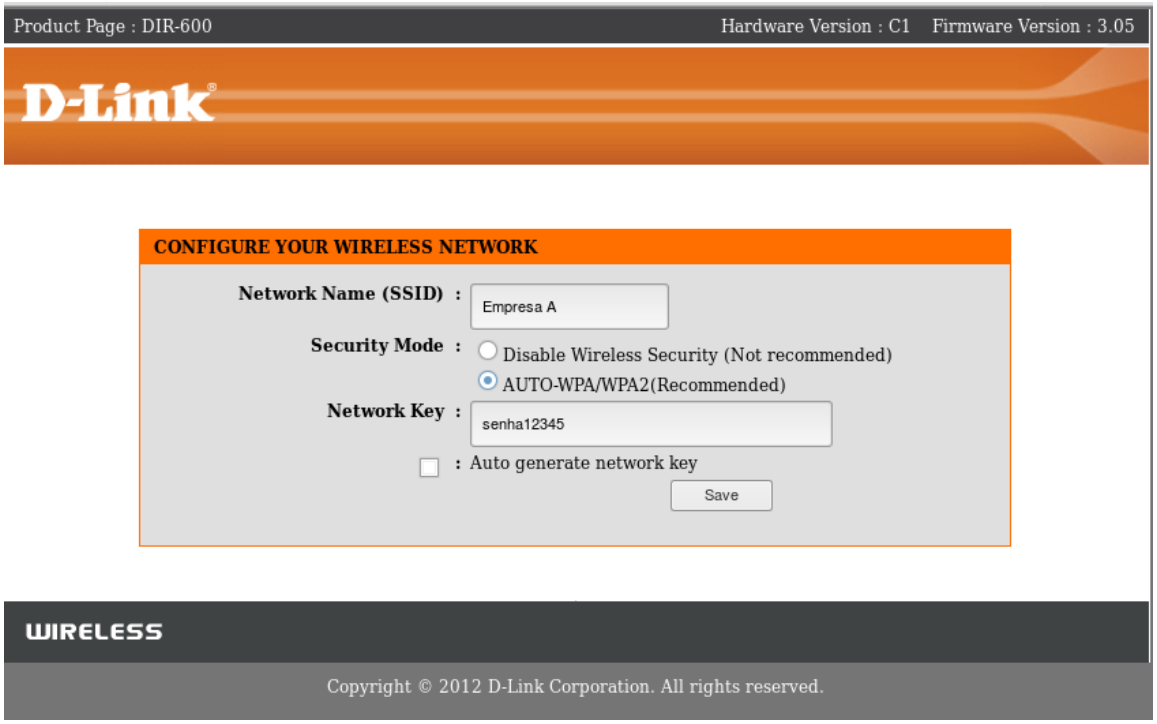

Figura 2: Configuração do Roteador
Fonte: Banco de imagens Windows

Note que em “Network Name” (Nome da Rede) temos *Empresa A;* Enquanto em “Network Key” (Senha da Rede) temos *senha12345*. A senha foi elaborada, tendo como base pesquisas realizadas por empresas de segurança digital. Neste estudo, utiliza-se uma sequência de números e a palavra “senha*” (password – no caso da pesquisa),* que são práticas entre administradores de redes, segundo dados da empresa Keeper Securyti.

Após configurada, a rede poderá ser utilizada por dispositivos móveis, como por exemplo, *smartphones*, *tablets*, *notebooks*, entre outros; por *desktops* conectados via cabo e impressoras.

Seguindo com o estudo, um processo de quebra de proteção no protocolo WPA/WPA2 será realizada, com a finalidade de simular invasões à rede de uma micro empresa. Para este fim, serão utilizados o Sistema Operacional Kali Linux e a ferramenta Aircrack-ng, porém, outros métodos e ferramentas podem ser utilizados. A simulação de ataque será composta por quatro fases: habilitar adaptador *wireless* para modo de monitoramento; scanear as redes próximas; realizar o ataque; descriptografar a senha.

4.2. SIMULAÇÃO DE ATAQUE

Utilizando o Sistema Operacional Kali Linux, o primeiro passo será habilitar o adaptador *wireless* para modo de monitoramento, como mostrado na Figura 3.

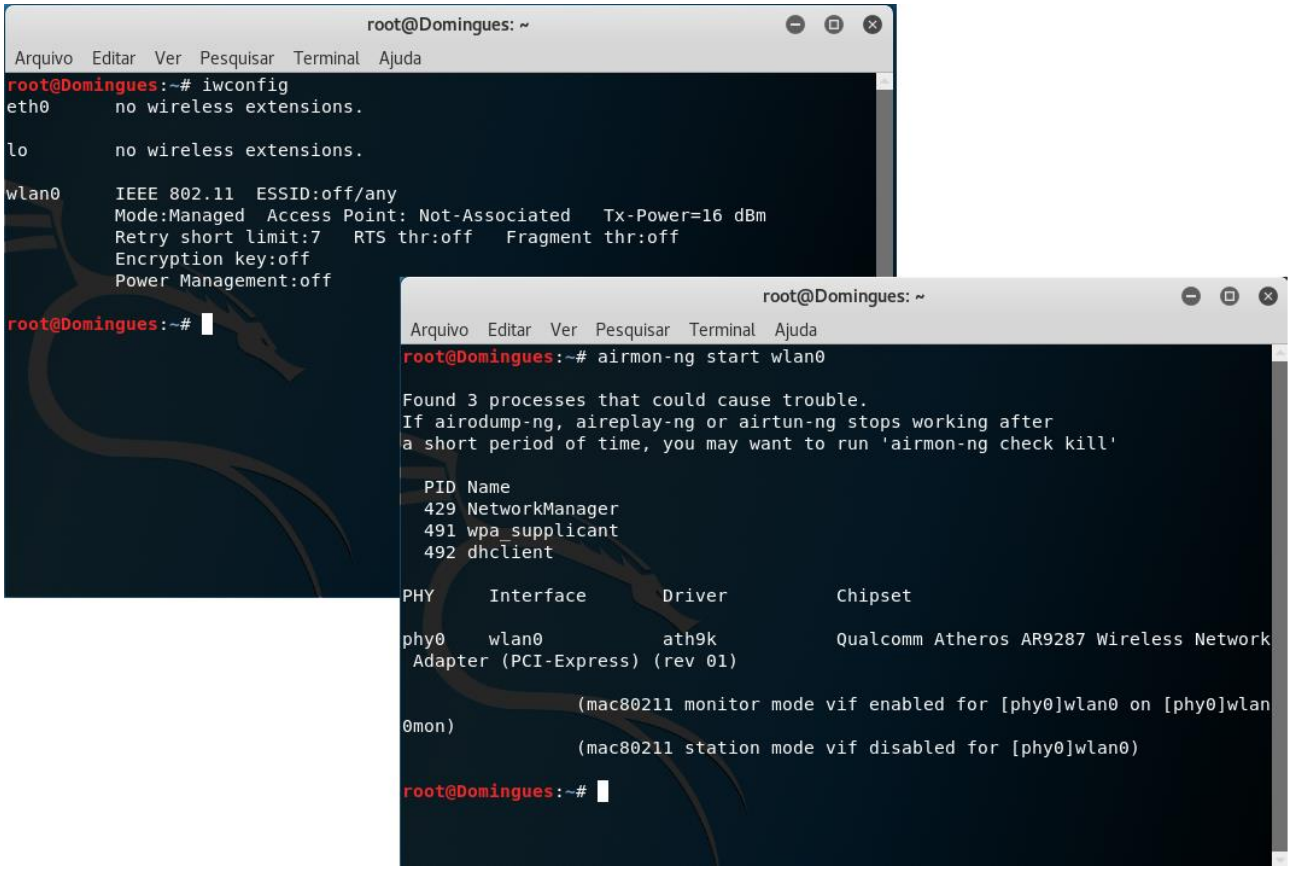

Figura 3: Habilitando Modo de Monitoramento
Fonte: Banco de imagens Windows

A interface gráfica passa de *wlan0* para *wlan0mon.*

Após o processo de escaneamento ser realizado, a rede da empresa fictícia (Empresa A) foi encontrada e, neste processo, foi possível encontrar o endereço de controle da placa do roteador (BSSID) e dos dispositivos nele conectados (STATION), ou seja, seus

respectivos endereços MAC (Media Access Control). A partir daí, será possível interromper a conexão entre roteador e dispositivos conectados utilizando de uma injeção de *frames*. Com isto, o dispositivo será desconectado e tentará nova conexão. A ferramenta, então, irá capturar os *frames* enviados do dispositivo ao roteador e, nestes, estará o chamado Tree-Way-Handshake (estabelecimento de conexão do dispositivo com o roteador). Ao realizar este os *frames* contendo a senha de acesso à rede será capturado; ataque este denomindado "*Handshake* em quatro vias".

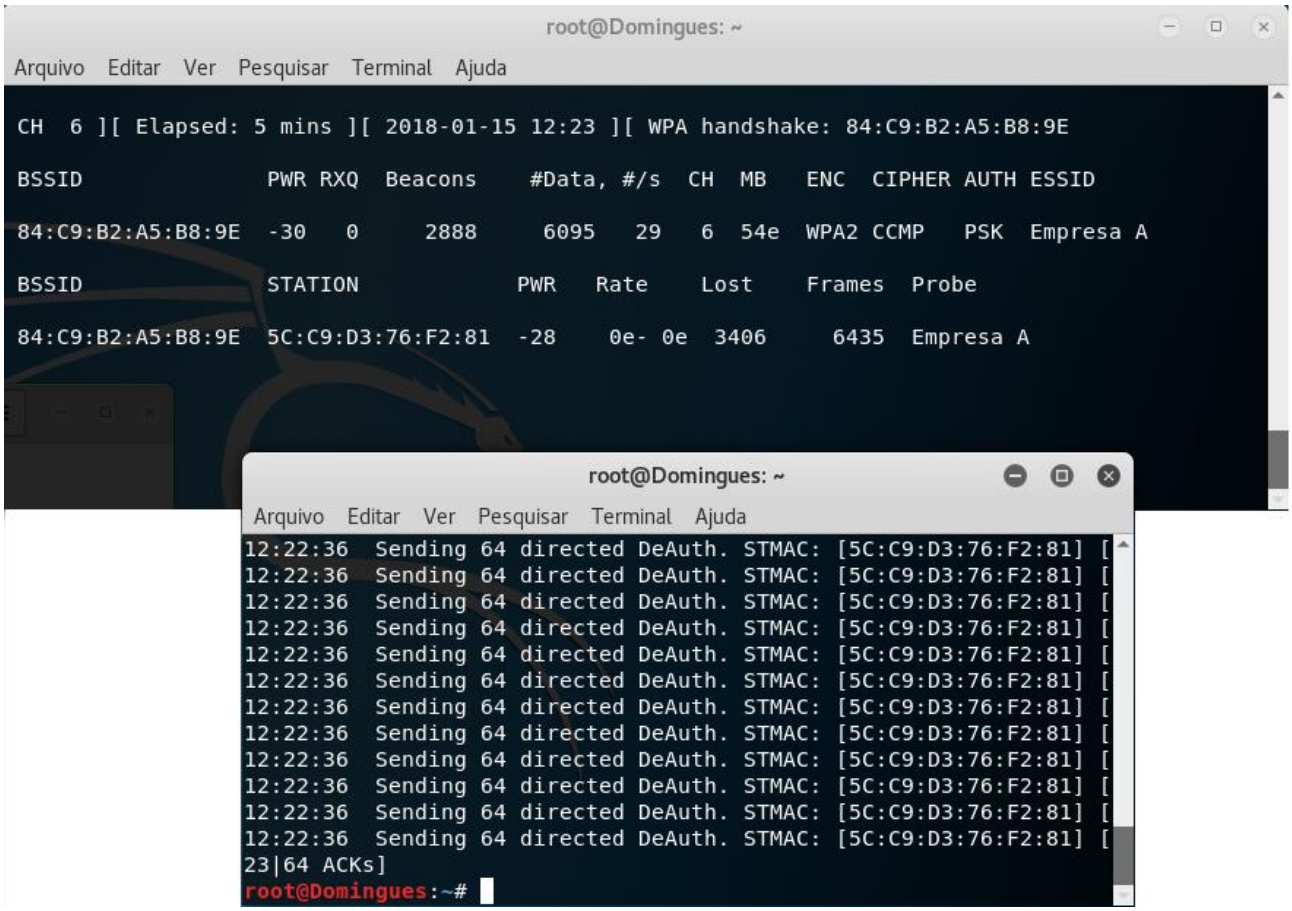

Figura 4: Injeção de Frames e Handshake em Quatro Vias
Fonte: Banco de imagens Windows

Após capturados os *frames*, a ferramenta Aircrack-ng copara o arquivo gerado com a senha da rede atacada a uma lista de senhas (worklist) ou através de combinações geradas pela própria máquina. Após as comparações, a ferramenta encontra a senha da rede atacada, como mostrado na Figura 5.

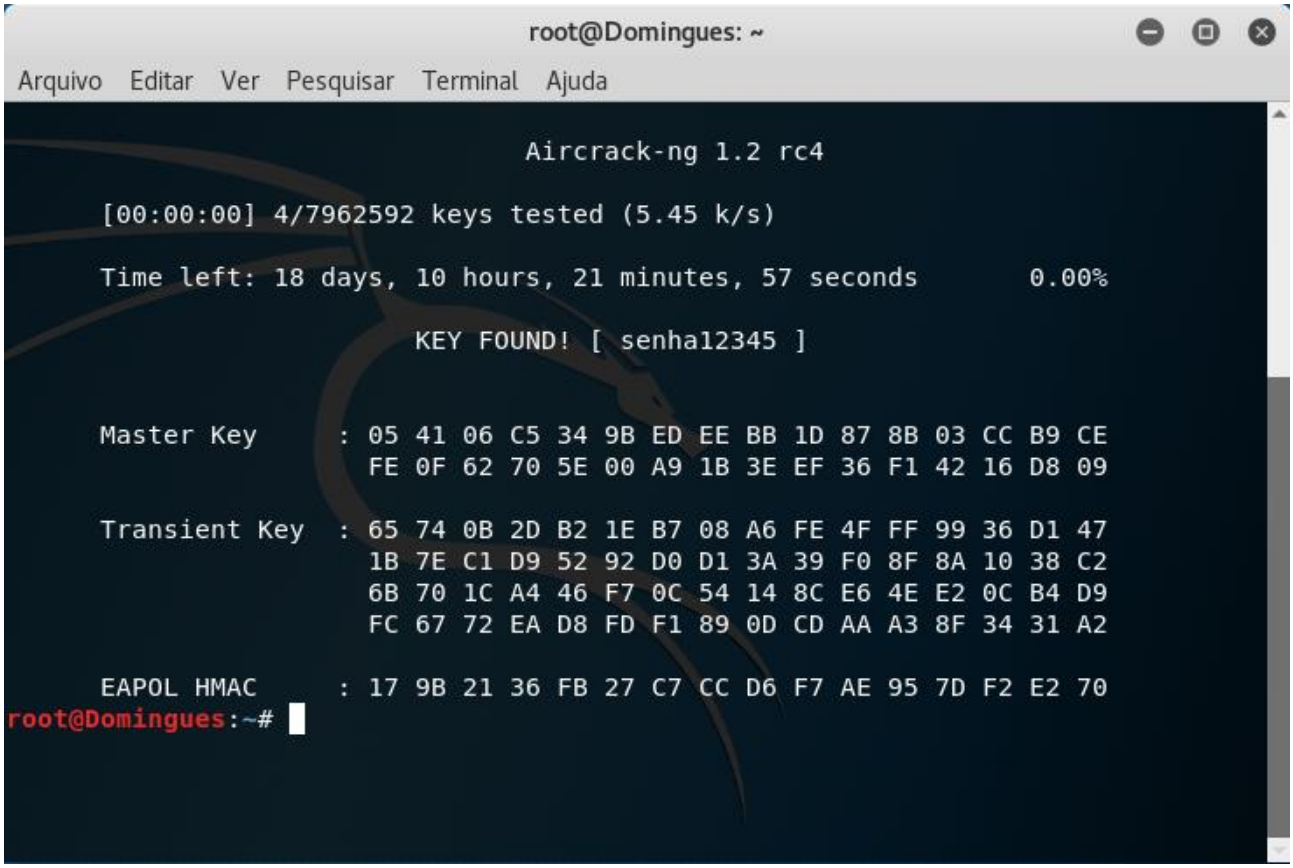

Figura 5: Senha Encontrada
Fonte: Banco de imagens Windows

Este *Pentest* alerta para a necessidade de uma estrutura e estratégias de segurança mais eficazes, no que se diz respeito a redes de micro e pequenas empresas.

O próximo capítulo deste estudo será direcionado a implementação da tecnologia MikroTik e suas configurações, de acordo com estratégias de seguranças que venham a ser viáveis a micro empresa.

5. IMPLEMENTAÇÃO E CONFIGURAÇÃO DO MIKROTIK

Este capítulo transcreve sobre a instalação e configuração do MikroTik hAP Lite, de acordo com estratégias de segurança da informação e proteção da rede de uma micro empresa.

5.1. INSTALAÇÃO DO MIKROTIK HAP LITE

A instalação do MikoTik hAP Lite seguirá um esquema bem semelhante a instalação do Roteador utilizado no capítulo 4, representado na Figura 1. O Roteador será substituído pelo MikroTik, como mostrado na Figura 6.

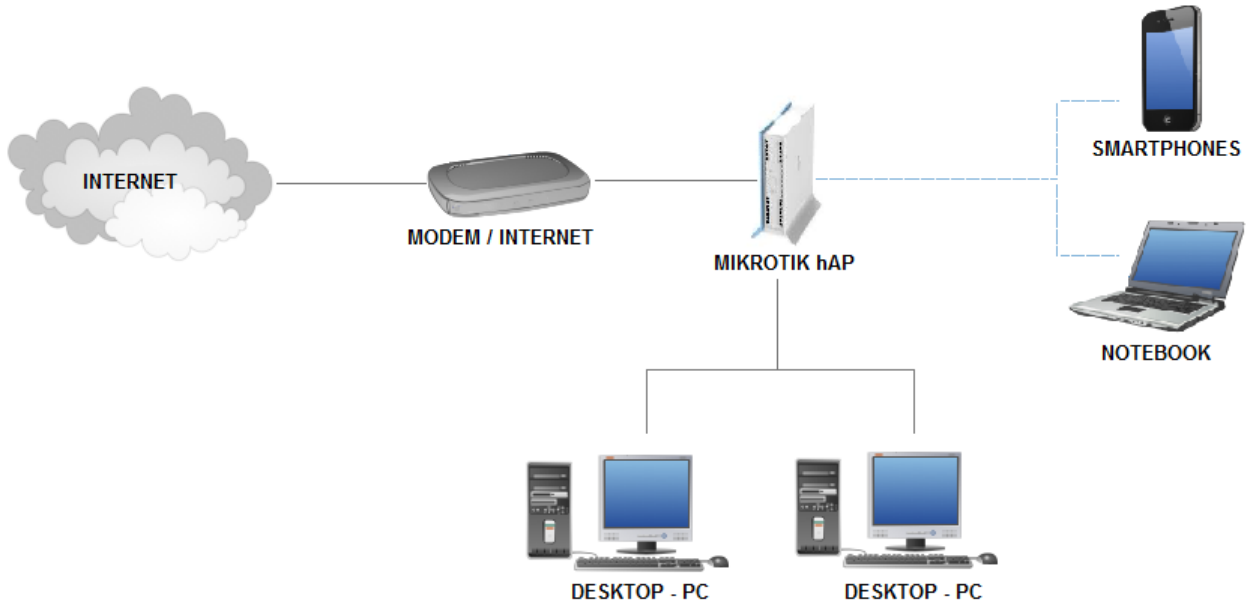

Figura 6: Esquema de Instalação do MikroTik hAP Lite
Fonte: Banco de imagens Windows

5.2. CONFIGURAÇÕES DO MIKROTIK

Após o MikroTik hAP Lite inserido na estrutura da rede, suas configurações de fábrica serão removidas e configuradas. Para este estudo foram utilizados os padrões de Classe C, tendo como endereçamento de rede (*Network*) 192.168.2.0/24, sendo 192.168.2.1 para

a interface “LAN1 – Saída”, que será utilizada como porta de “saída” de Internet, podendo assim ser conectada a um *desktop* ou a outros dispositivos, como por exemplo, um *switch*, caso seja necessário a conexão de mais de um *desktop*. O endereço utilizado para “WLAN1 – Wireless”, que será a conexão sem fio (*Wireless*) será 192.168.2.2/24.

O endereçamento em “WAN1 – Entrada”, que será a interface responsável por “receber” Internet, será 192.168.0.104/24 na rede (*Network*) 192.168.0.0. A figura 7 demonstra a lista de endereços configuradas no MikroTik hAP Lite utilizado neste estudo.

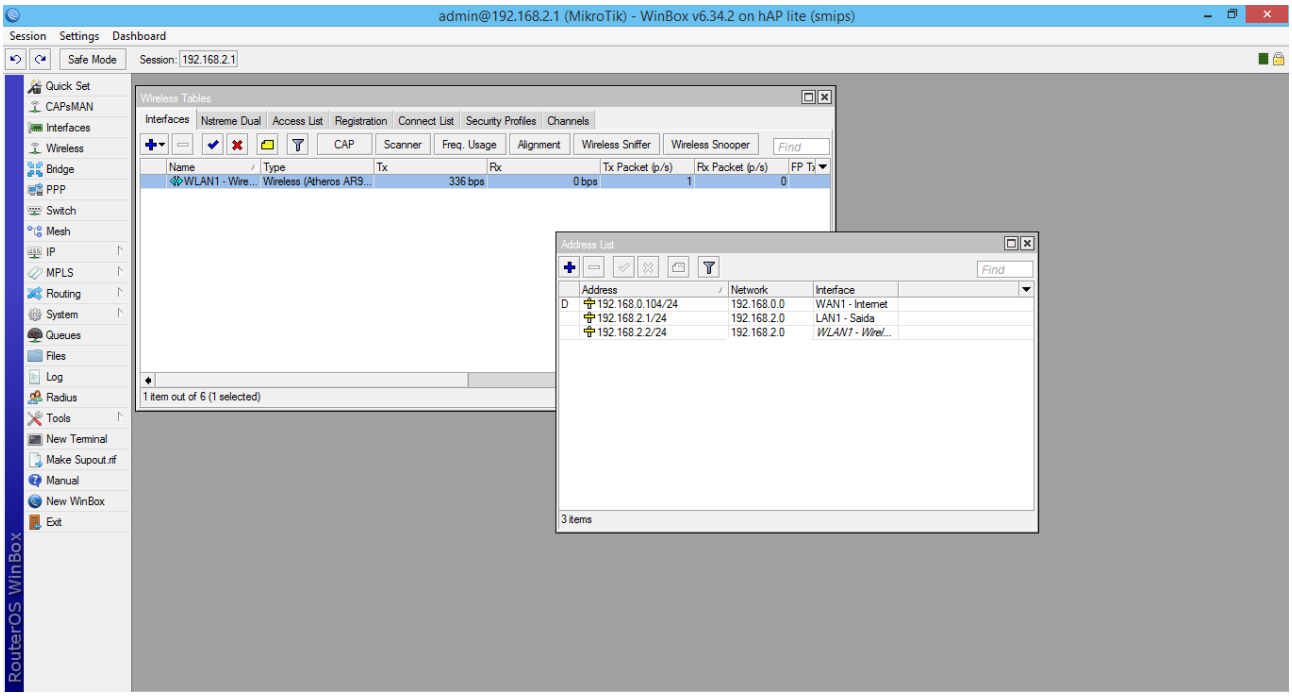

Figura 7: Lista de Endereços
Fonte: Banco de imagens Windows

No próximo capítulo será transcorrida estratégias de proteção a rede de uma micro empresa e, posteriormente, técnicas de invasão que podem ser utilizadas, visando possíveis vulnerabilidades em sua segurança.

5.3. CONFIGURAÇÕES DO WIRELESS

A rede utilizada em computadores de mesa (*Desktop*) é de extrema importância em uma micro empresa. Porém, visando mobilidade e praticidade, o MikroTik hAp Lite oferece, também, um roteador *wireless*, que pode vir a ser uma ferramenta essencial,

principalmente, para microempreendedores, que utilizam de dispositivos móveis, como por exemplo, *smartphones*, *tablets*, entre outros. Uma rede sem fio também seria indispensável, também, em casos de instalação de dispositivos de escritório, como por exemplo, impressoras e multifuncionais.

Sendo assim, este tópico é voltado a configuração da rede *wireless* no MikroTik. Como descrito no tópico anterior, o endereçamento utilizado para esta interface será 192.168.0.2/24. Após isto será configurada uma *bridge* (ponte) entre as interfaces "WLAN1 – Wireless" e "WAN1 – Entrada".

A bridge é tida como um dispositivo que tem a finalidade de interligar duas redes, que utilizam de diferentes protocolos ou dois segmentos de mesma rede, que utilizam o mesmo protocolo, como por exemplo, o Ethernet (utilizado neste estudo). A figura 8 mostra a *bridge* já criada com o nome de "*bridge*-Wifi".

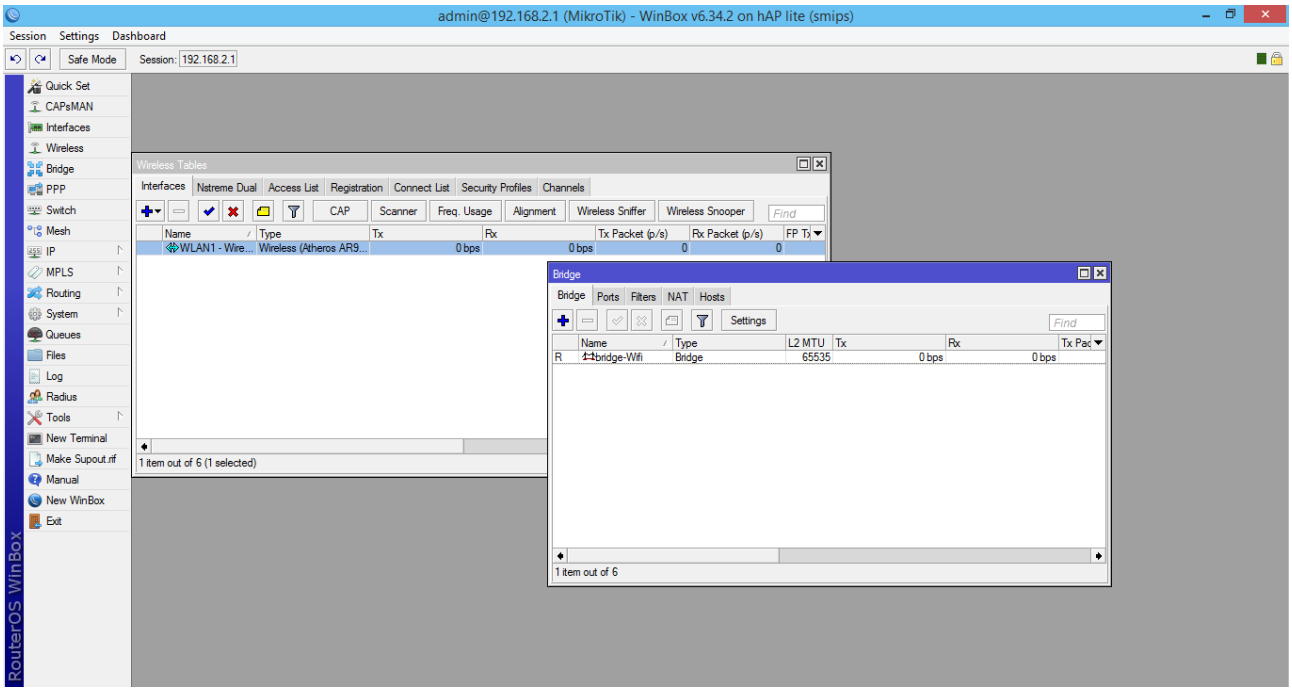

Figura 8: Bridge criada
Fonte: Banco de imagens Windows

Após a criação da bridge será configurada as portas, ou seja, as interfaces que farão parte desta "ligação". A figura 9 demonstra as interfaces inseridas na *bridge*.

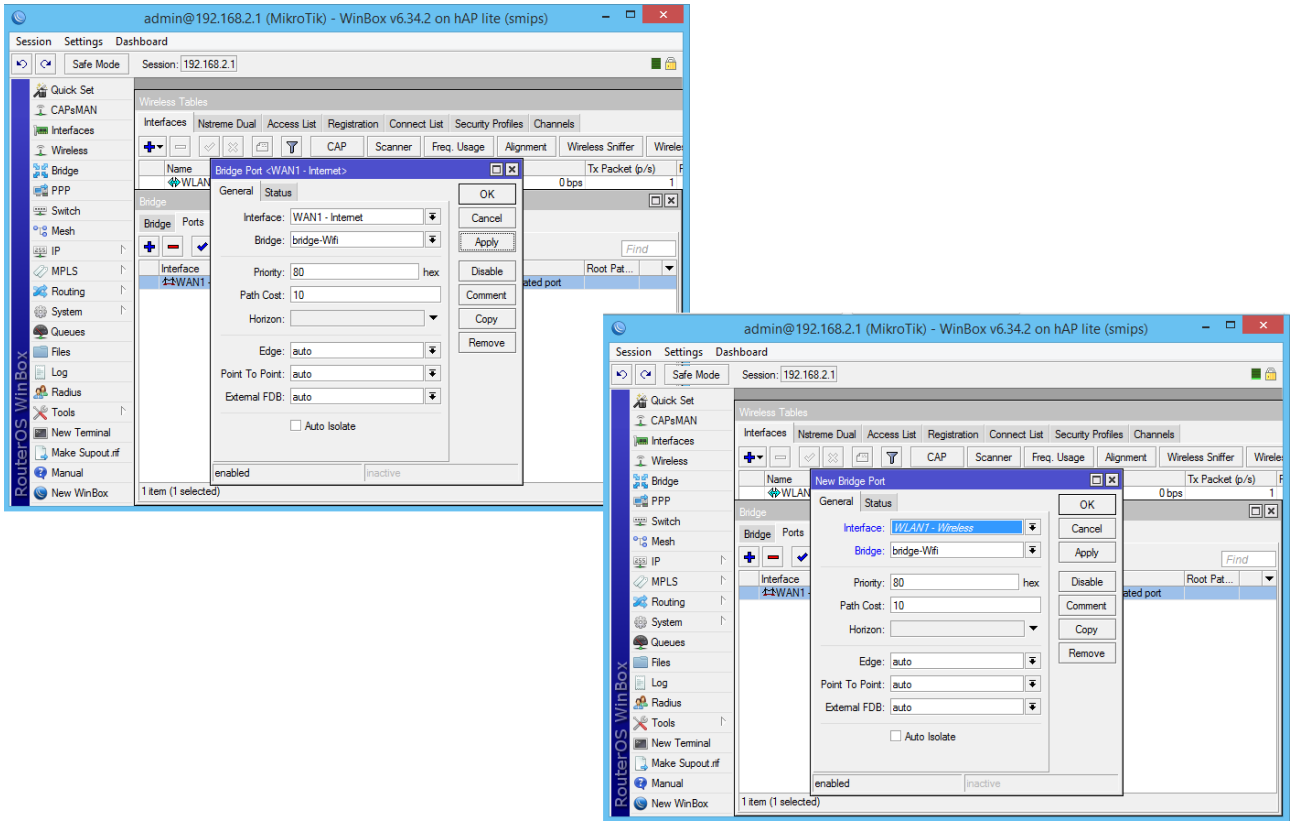

Figura 9: Interfaces da bridge
Fonte: Banco de imagens Windows

O próximo passo é criar um *security profile* (perfil de segurança) da rede. Neste será possível definir o tipo de segurança utilizado na rede sem fio, bem como a senha de acesso a mesma.

Denominada “Segurança Wifi” este *security profile* possuirá um modo de chaves dinâmicas (dynamic keys). A segurança será baseada, em primeiro momento, nos tipos WPA e WPA2, com os protocolos de PSK e AEP. A senha utilizada será a mesma utilizada no item 4.1: “senha12345”. Nos próximos capítulos as técnicas de proteção serão alteradas. A Figura 10 ilustra as configurações do *secury profile.*

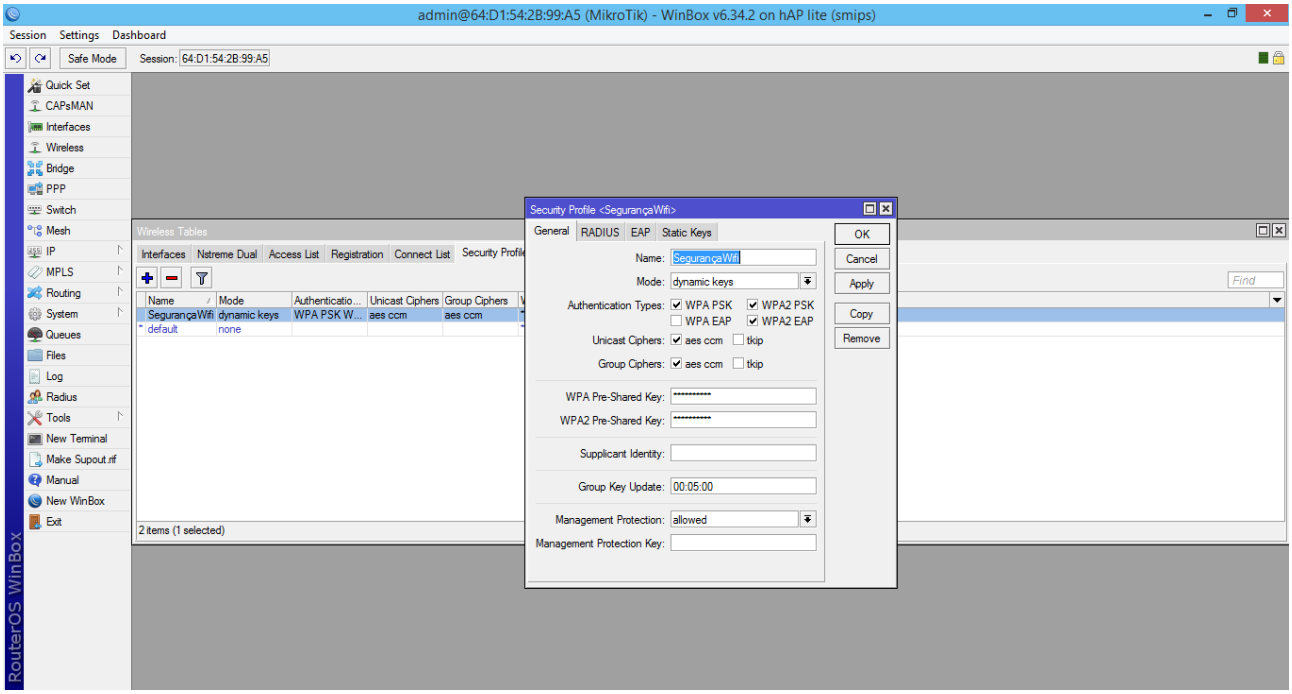

Figura 10: Configurando o security profile
Fonte: Banco de imagens Windows

Por fim, ativa-se a interface que será utilizada para a rede sem fio.

6. SERVIÇOS DE REDE

Neste capítulo será apresentada técnicas de proteção em serviços de rede, que pouco, ou quase nunca, são utilizados em micro e pequenas empresas.

6.1. PING

O Packet Internet Network Grouper, ou simplesmente ‘PING’, é um comando utilizado para testes de conectividade entre dispositivos em uma determinada rede. Utilizando do protocolo ICMP (Internet Control Message Protocol), o comando envia pacotes ao dispositivo, aguardando a resposta do mesmo, sendo assim possível, calcular o “*status*” do dispositivo, ou seja, se o mesmo está conectado ou não, e seu tempo de resposta.

O problema surge quando ao executar este comando, o mesmo retorna algumas informações do dispositivo e, entre estas, seu endereçamento IP. Uma vez descoberto, o IP poderá ser utilizado para uma série de possíveis invasões ao sistema “pingado”, e até mesmo, ataques que intervenham no funcionamento de sistemas e sites.

Um método de proteção seria o bloqueio do PING a um *site* ou servidor. A Figura 11 mostra o comando PING retornando o servidor MikroTik.

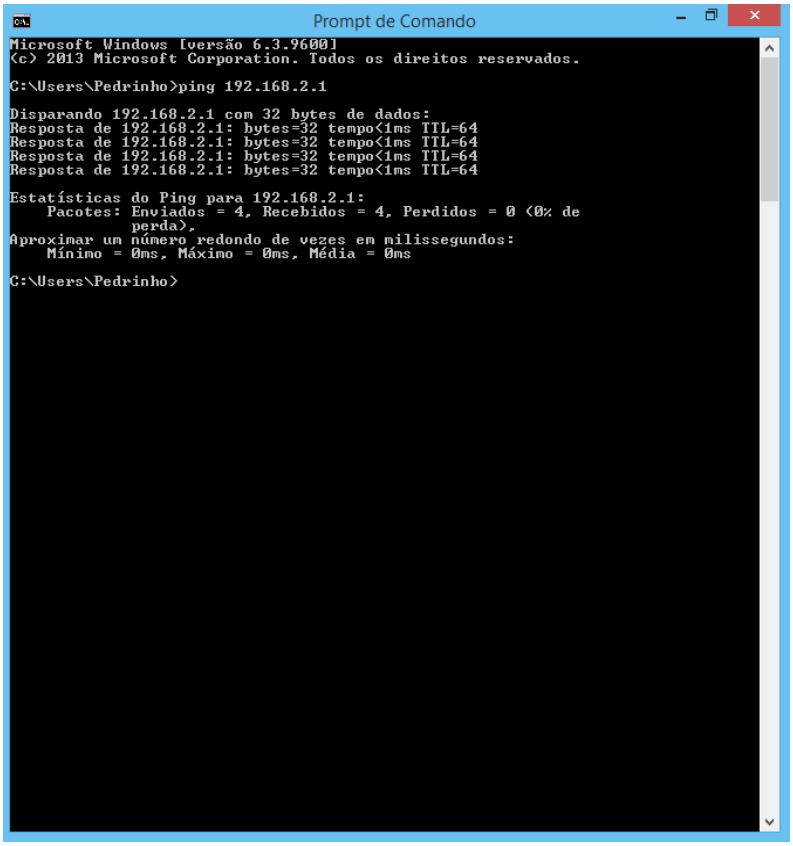

Figura 11: Ping do Servidor MikroTik
Fonte: Banco de imagens Windows

Para que o PING seja bloqueado é necessário aplicar um *firewall* para esta finalidade. A Figura 12 demonstra a configuração deste *firewall*.

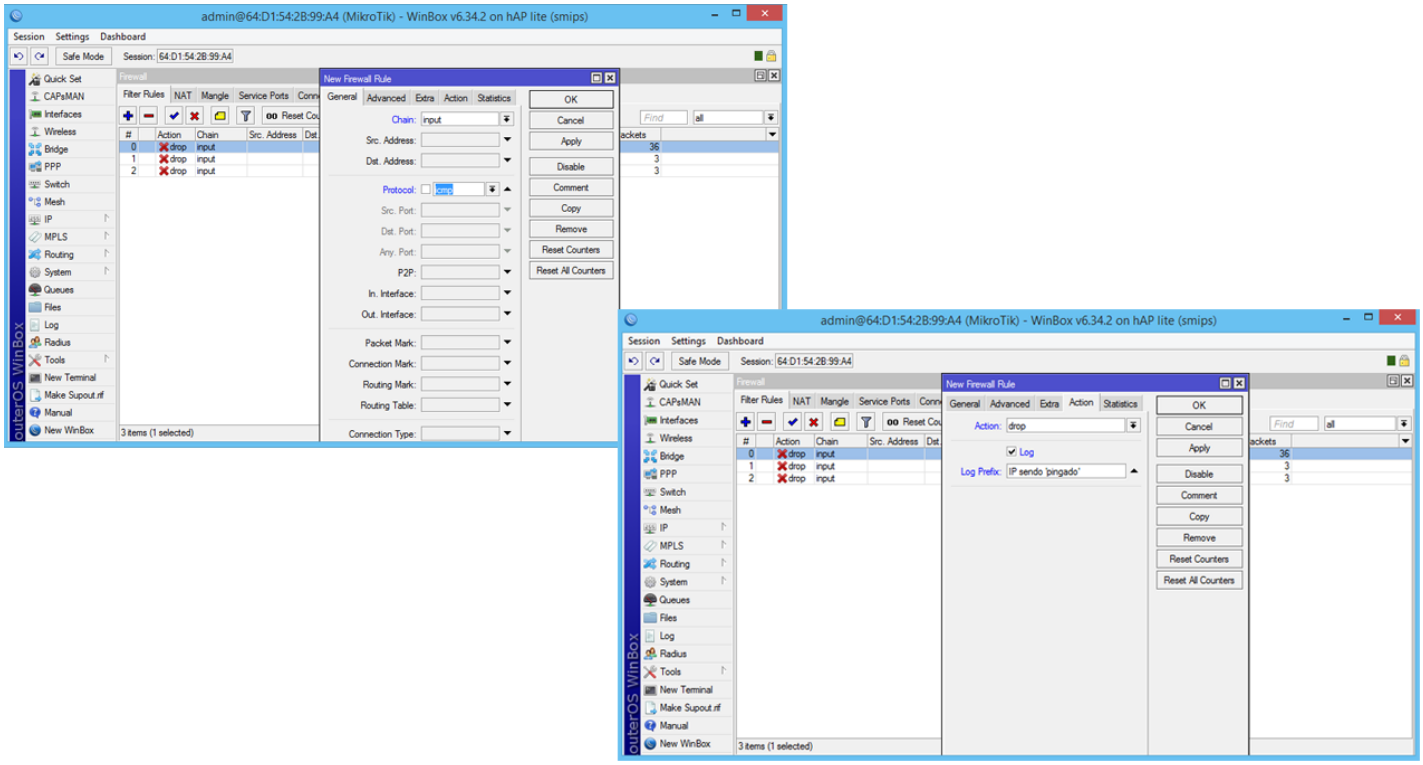

Figura 12: Bloqueando PING no MikroTik
Fonte: Banco de imagens Windows

Nesta configuração a opção de entrada (*input*) e o protocolo (ICMP) são selecionados e, a ação que deverá ser executada será a de bloqueio (*drop*). Sempre que for realizada uma tentativa de “pingar” a rede deste MikoTik o administrador terá acesso aos logs que irão expor “IP sendo ‘pingado’”, demonstrando que a proteção está em funcionamento. A Figura 13 demonstra a proteção contra o PING externo em funcionamento.

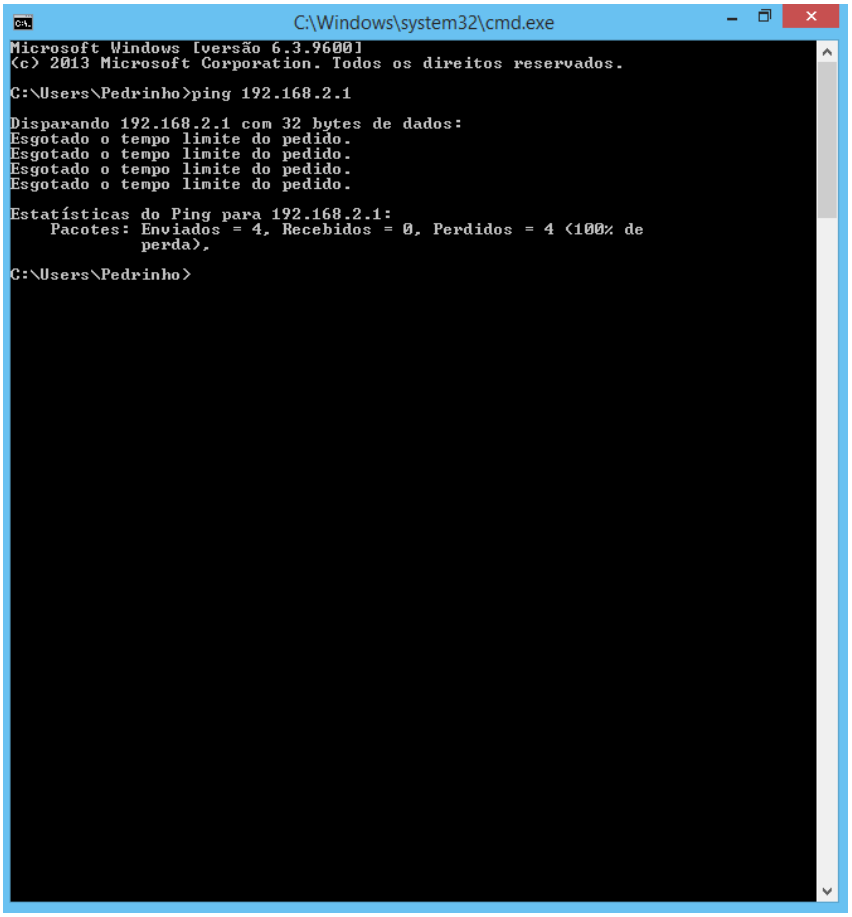

Figura 13: Ping Bloqueado
Fonte: Banco de imagens Windows

6.2. FTP

O FTP (File Transfer Protocol) é um serviço, baseado no protocolo TCP/IP, utilizado para a transferência de arquivos através da Internet. Este serviço utiliza o sistema cliente/servidor, onde um computador fornece arquivos para um cliente, de forma remota, ter acesso aos mesmos. Sendo assim, estando o serviço de FTP habilitado, é possível de acessar remotamente o servidor, apenas utilizando o IP do mesmo; acesso este podendo ser autorizado ou não.

Com a finalidade de evitar um possível ataque por FTP e visando a pouca (ou nenhuma) utilização deste serviço em uma micro empresa, através do MikroTik, a porta 21, utilizada por este serviço, pode ser bloqueada. A proteção do servidor fica ainda mais vulnerável ao utilizar usuário e senha padrões de fábrica. Neste estudo será utilizado os padrões de

usuário “admin” e a senha vazia A Figura 14 demonstra o servidor sendo acessado via FTP.

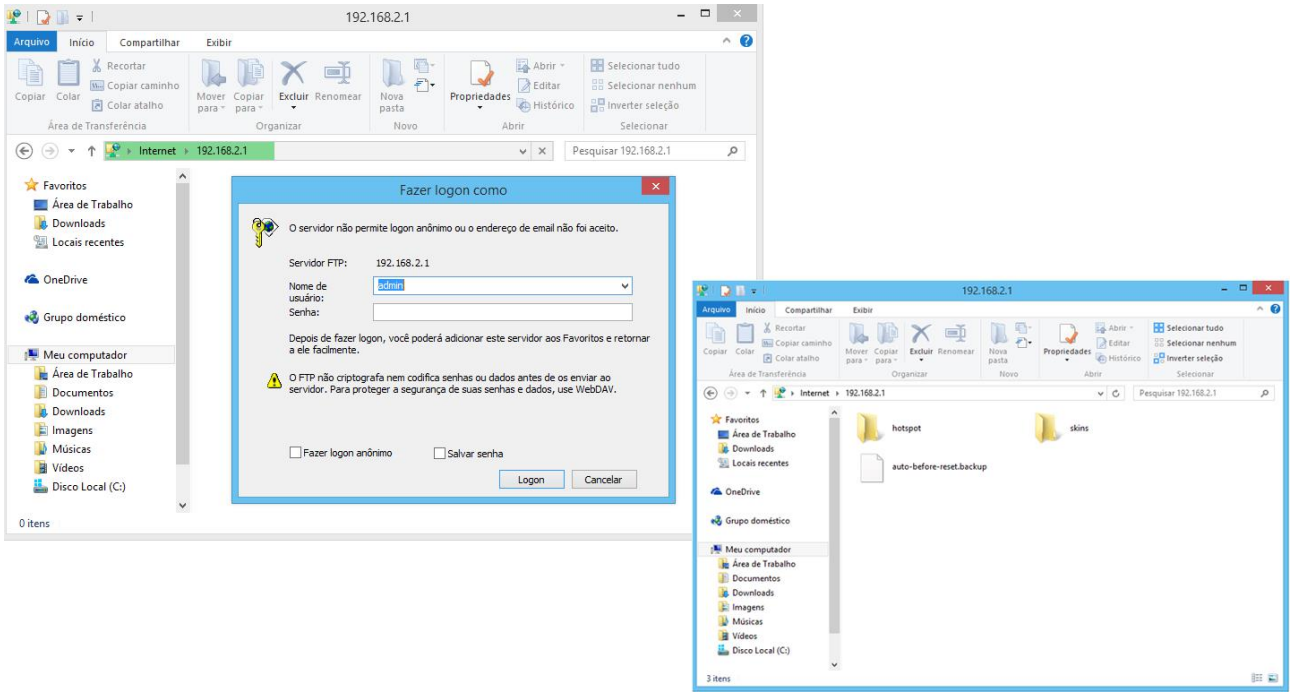

Figura 14: Acesso via FTP
Fonte: Banco de imagens Windows

A configuração do *firewall* para bloqueio de FTP apresenta; o tipo/cadeia (*chain*) como entrada (*input*), o protocolo utilizado (TCP) e porta destinada será 21 (FTP). A ação selecionada será a de bloqueio (*drop*). As configurações estão apresentadas na Figura 15.

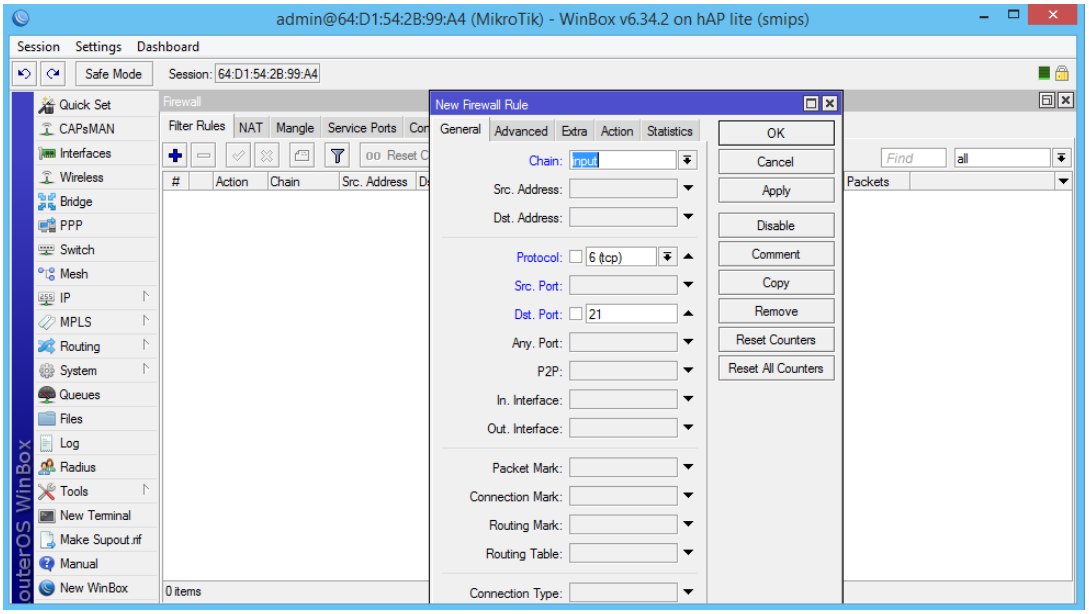

Figura 15: Configurações de bloqueio do serviço FTP
Fonte: Banco de imagens Windows

Sendo assim, o acesso a porta utilizada pelo serviço de FTP será bloqueado, sendo impossibilitado o acesso ao servidor por este método, como demonstra a Figura 16.

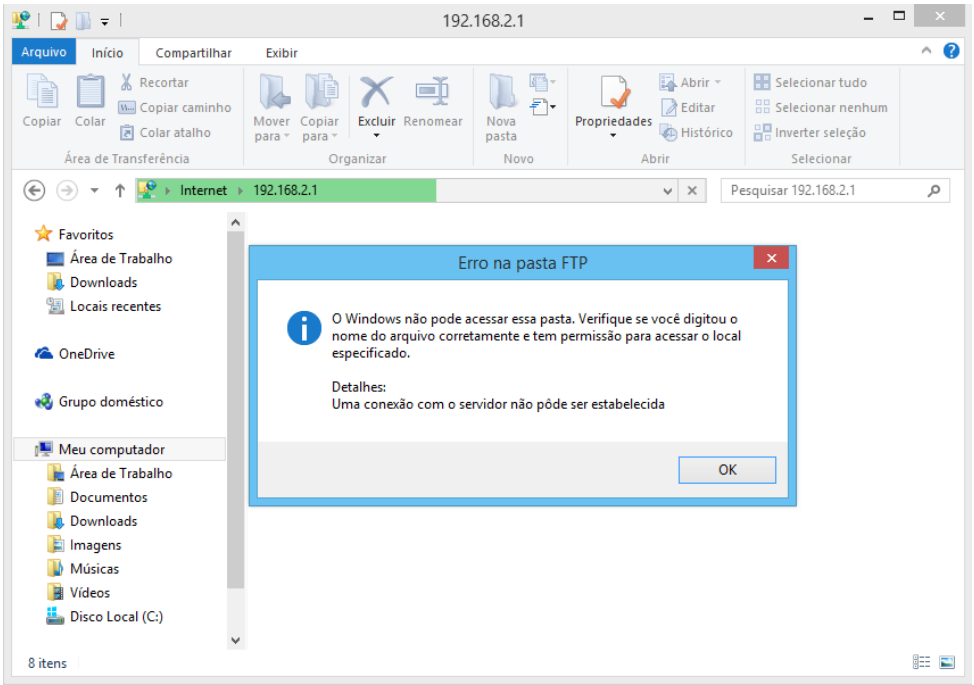

Figura 16: Bloqueio do serviço de FTP
Fonte: Banco de imagens Windows

6.3. TELNET

Telnet é um serviço utilizado para tráfego de dados e informações entre computadores pela Internet, o Telnet apesar de prático pode ser questionável, quando o tema é segurança. Um dos pontos criticados em relação a este serviço é a não utilização de criptografia de dados, facilitando o acesso, como por exemplo, a usuários e senhas, em casos de ataques.

Em relação a sua utilização em uma micro empresa chega a ser praticamente nula, tendo em vista o não conhecimento de usuários menos experientes a este serviço. Portanto, o seu bloqueio também se torna uma boa prática de segurança da informação a uma micro empresa.

A Figura 17 mostra o acesso ao servidor através do serviço de Telnet.

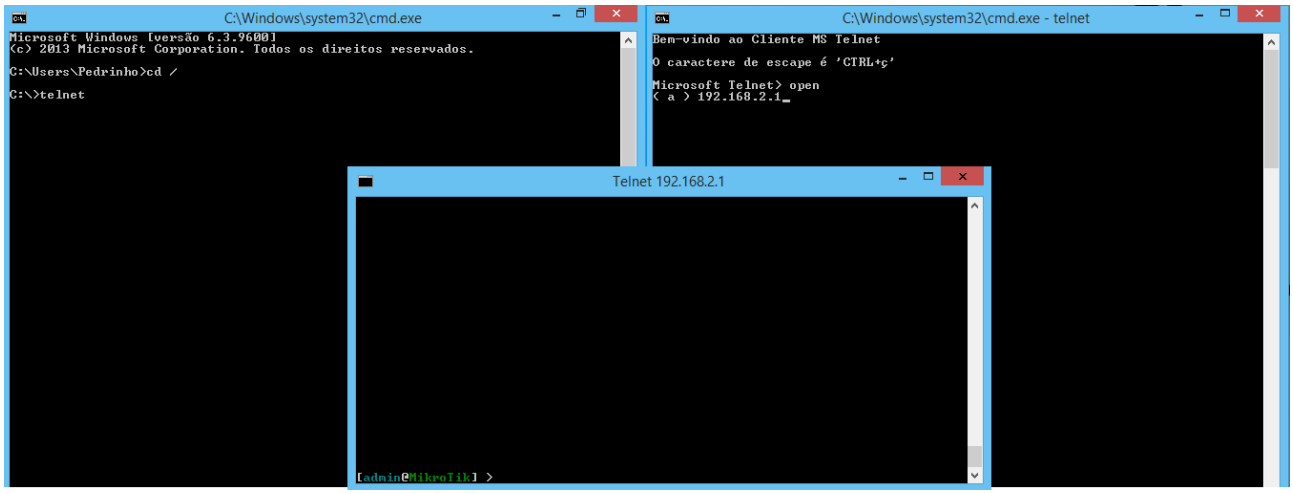

Figura 17: Acessando servidor via Telnet
Fonte: Banco de imagens Windows

Sendo assim, as configurações de bloqueio do serviço Telnet seguem os mesmos padrões utilizados no bloqueio do serviço FTP, diferenciando apenas a porta utilizada, que, neste caso será a porta de número 23, como na Figura 18.

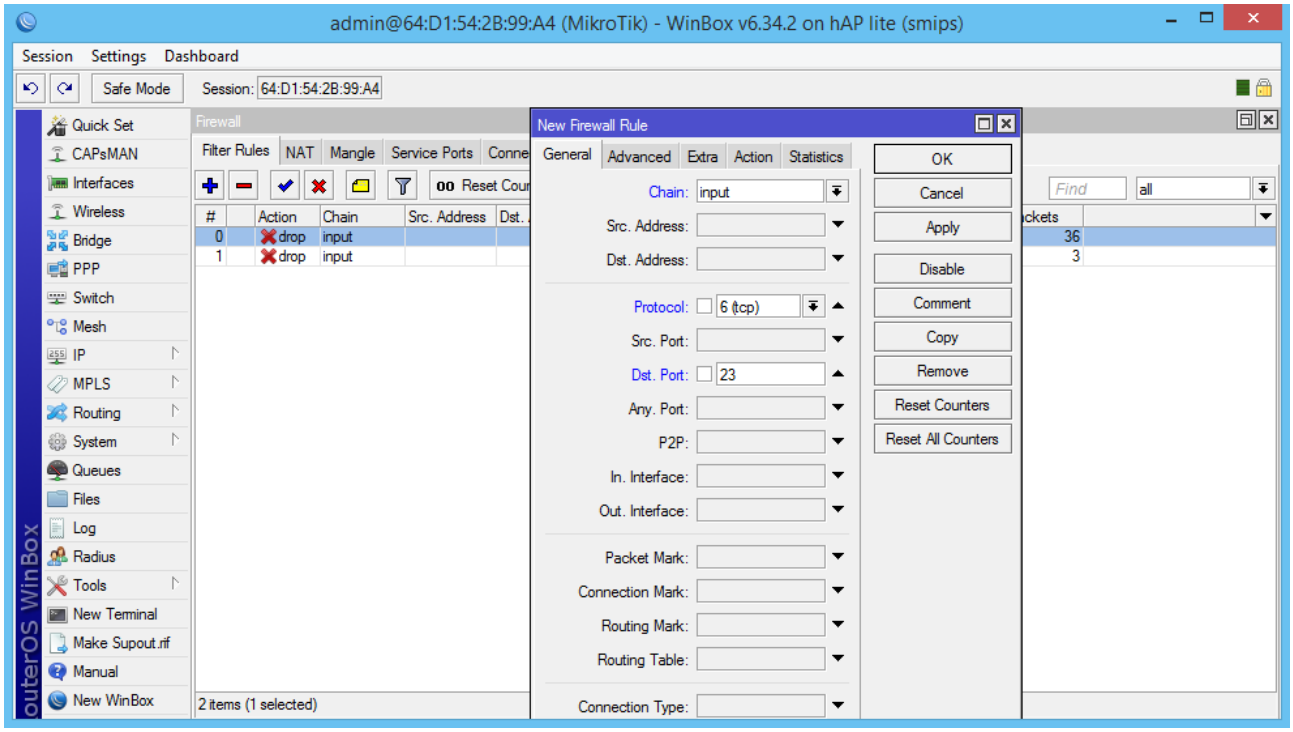

Figura 18: Bloqueio do serviço Telnet
Fonte: Banco de imagens Windows

Após as configurações serem concluídas, as tentativas de conexão ao servidor através do serviço de Telnet não serão concluídas, ficando assim, impossibilitado o acesso. Exemplo na Figura 19.

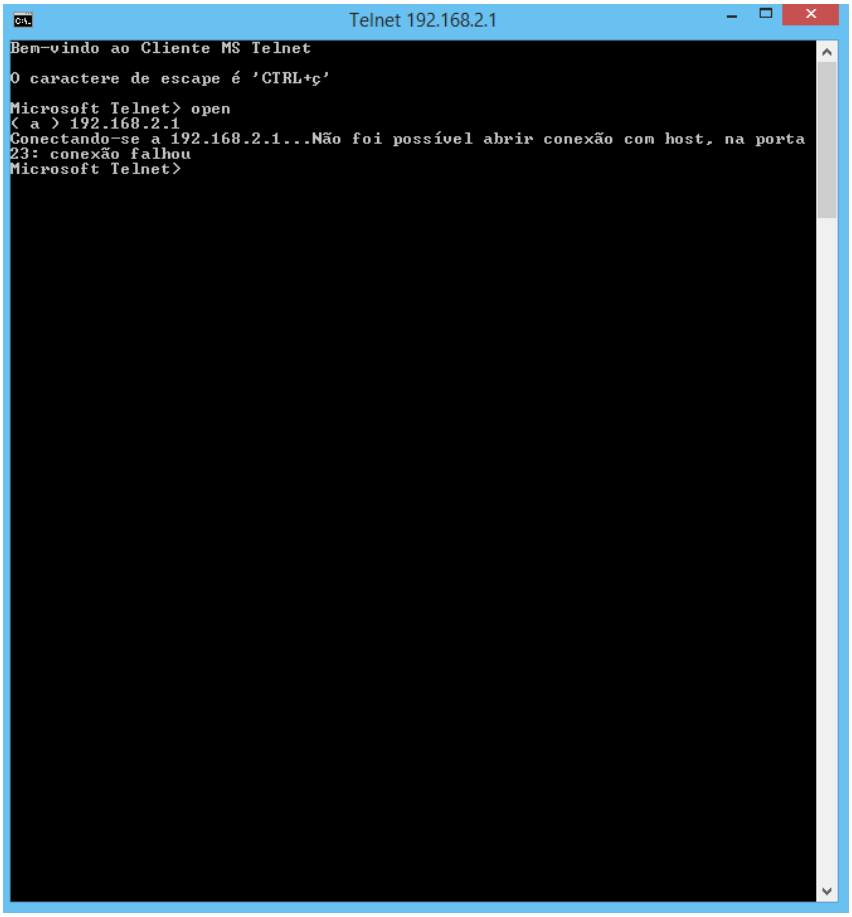

Figura 19: Telnet bloqueado
Fonte: Banco de imagens Windows

6.4. SSH

Semelhante ao Telnet o Secure Shell é um serviço que permite acessar virtual e remotamente um servidor. A diferença está na própria segurança. O SSH é mais seguro, pois utiliza criptografia, tornando mais difícil o sequestro de dados, como por exemplo, usuários e senhas.

Apesar disso, muitos usuários desconhecem este serviço, principalmente em micro empresas. Porém, para ataques em sites e servidos é bastante explorado. Sendo assim, devido a sua, quase que sempre, não utilização, a porta SSH é outra que poderia ser bloqueada, a fim de aumentar a segurança em rede.

Para utilizar do serviço SSH é necessário um programa que acesse a porta equivalente a este serviço. Neste estudo, será utilizado como exemplo o Putty (executável). A Figura 20 mostra o acesso com a aplicação.

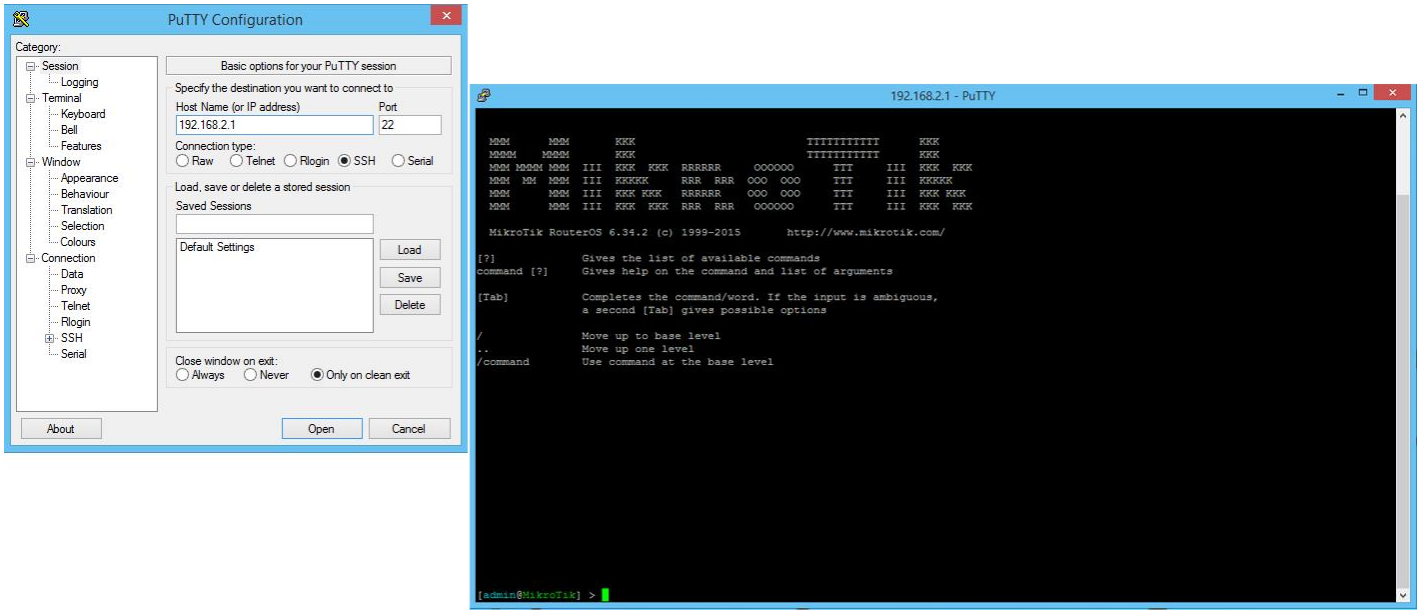

Figura 20: Acessando servidor via SSH
Fonte: Banco de imagens Windows

Utilizando os mesmos padrões de configuração dos serviços de FTP e Telnet, diferenciando, novamente, apenas a porta do serviço, que neste caso será a de número 22, como exemplificado na Figura 21.

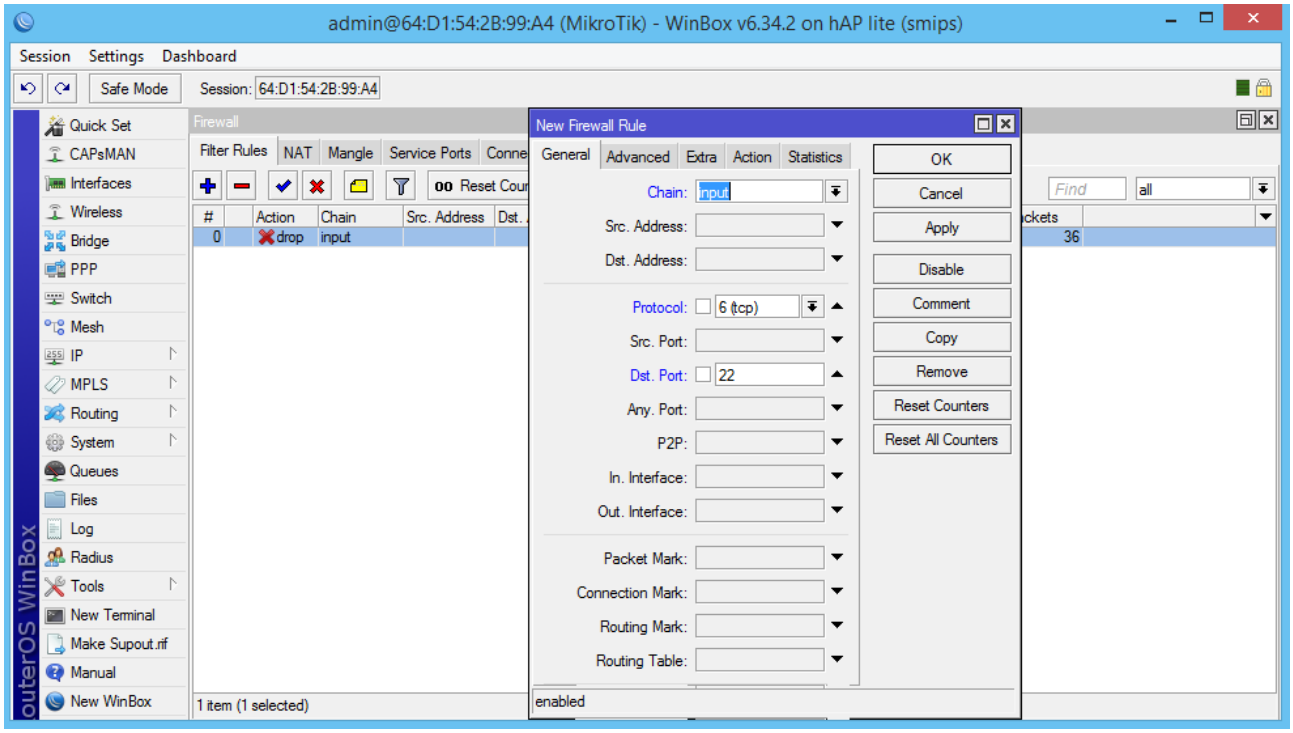

Figura 21: Bloqueio do serviço SSH
Fonte: Banco de imagens Windows

Após concluídas as configurações de bloqueio, a porta 22 fica inacessível, como mostrado na Figura 22.

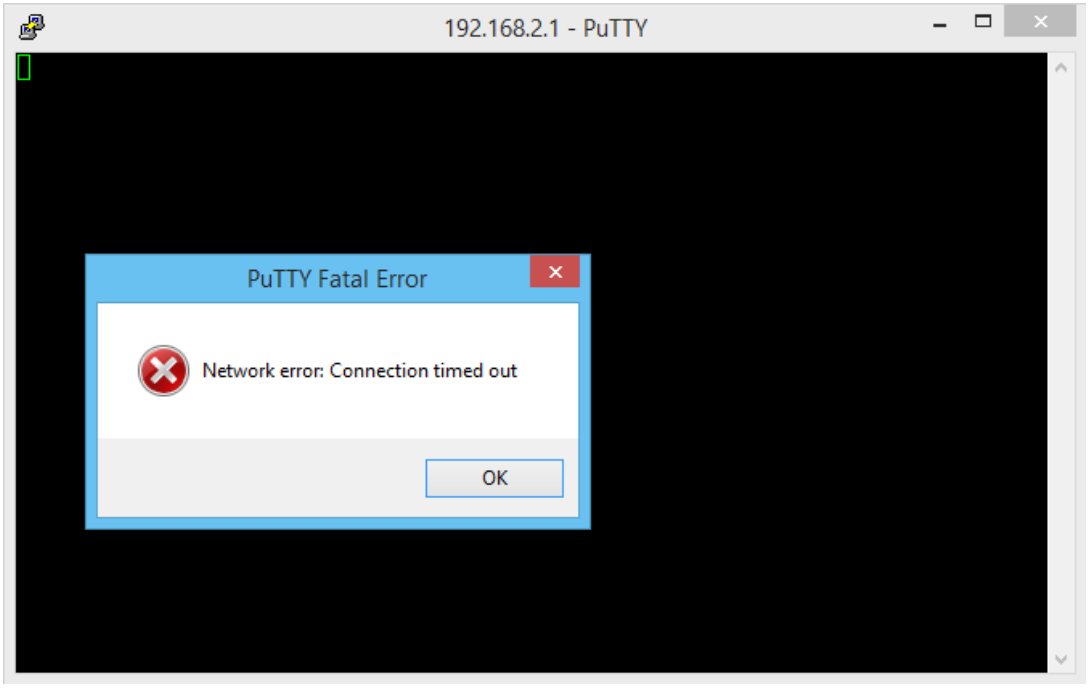

Figura 22: SSH bloqueado
Fonte: Banco de imagens Windows

6.5. P2P

Muito utilizada para compartilhamento de arquivos a tecnologia *peer-to-peer* (P2P), ou como conhecida, par-a-par, é um formato de rede com o objetivo de descentralizar um computador, tornando assim, qualquer máquina conectada a esta rede, um cliente/servidor. Sendo assim, qualquer computador poderá enviar e receber informações, desde que esteja conectado à rede P2P.

Esta tecnologia surgiu como principal objetivo o compartilhamento de informações e serviços, principalmente, para download de músicas, filmes e etc. Porém, sua utilização é nula em uma micro e pequena empresa. Sem destacar a possibilidade de arquivos maliciosos estarem ocultos em arquivos compartilhados, podendo levar a sérios prejuízos.

Sendo assim, o bloqueio da tecnologia P2P seria uma boa prática em políticas de segurança em micro empresas.

As figuras 22 demonstram as configurações para bloqueio do P2P.

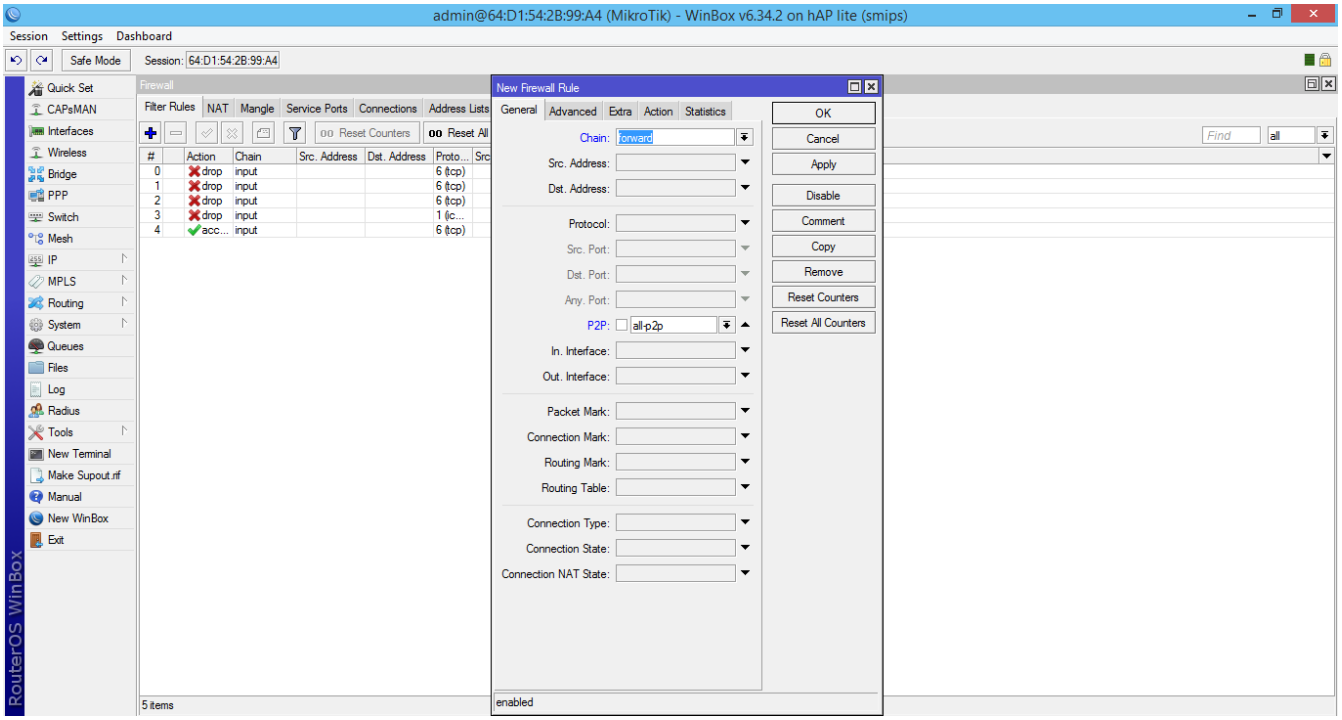

Figura 23: Bloqueio P2P-I
Fonte: Banco de imagens Windows

Em *chain* utiliza-se "*forward"* para gerência de pacotes e na opção *P2P* utiliza-se "*all-p2p"*, indicando que qualquer tipo de conexão P2P será filtrada. A *action* será *"drop"*. Ao tentar realizar alguma conexão deste tipo a lista de logs irá conter a mensagem "Tentativa de conexão P2P". A figura 24 demonstra as últimas configurações.

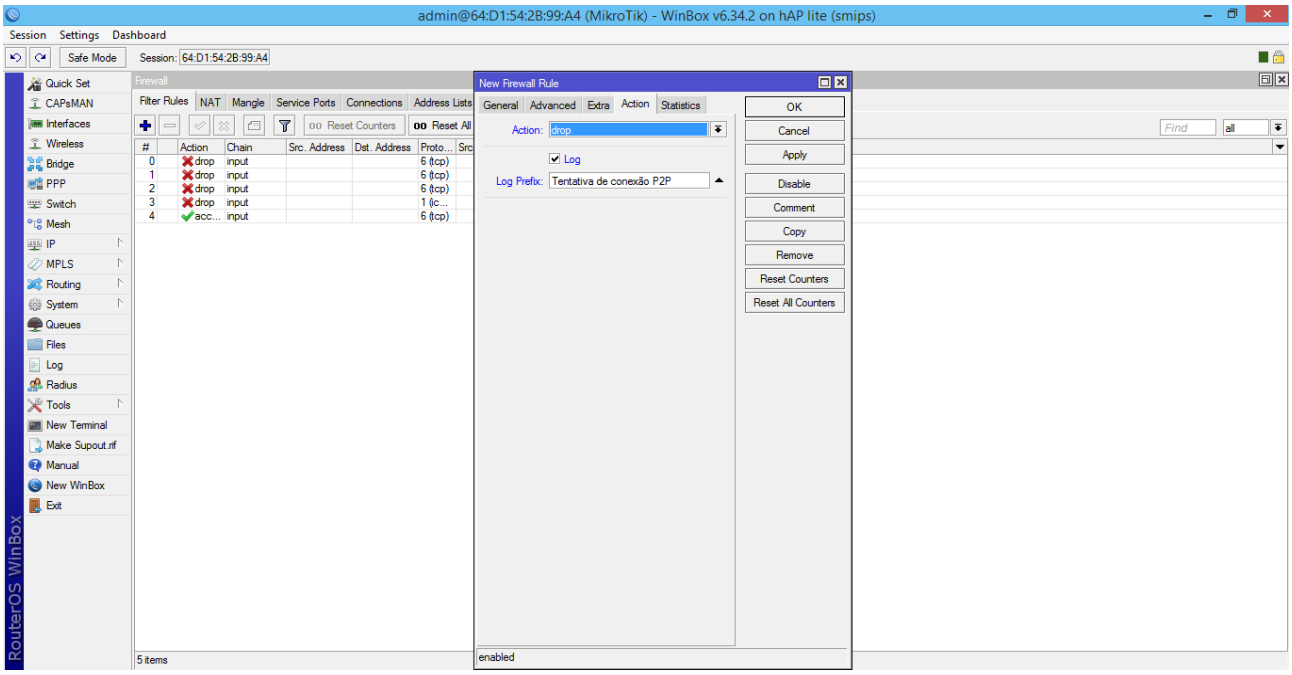

Figura 24: Bloqueio P2P-II
Fonte: Banco de imagens Windows

Após estas configurações, as conexões de tipo P2P serão filtradas e bloqueadas.

7. MEDIA ACESS CONTROL

Uma das melhores estratégias de proteção a uma rede, seja ela *wireless* ou cabeada, é atrelar o endereço IP ao MAC.

O Media Acess Control, ou simplesmente MAC, é um endereço único e exclusivo de cada adaptador ou interface de rede. Após a fabricação de um adaptador de rede, seu fabricante deve adquirir um endereço MAC, junto a entidades reguladoras. O endereço MAC é escrito em formato hexadecimal, sendo cada *byte* separa por hífen. O endereço MAC é de extrema importância pois, o endereço IP pode variar em determinados locais ou até mesmo por valores atribuídos via DHCP; enquanto o MAC permanece único a cada computador.

No MikroTIk há a possibilidade de atrelar o IP ao MAC, ou seja, para que um determinado computador ou dispositivo possa acessar a rede, deverá estar em uma “lista de acesso”, onde estará registrado os endereços IP e MAC.

Neste estudo será utilizada esta estratégia filtrando acesso a um único computador e a um único dispositivo móvel. Por questões de segurança, os endereços MAC utilizado neste estudo não serão expostos por completo. Também visando a privacidade alheia, os nomes das redes de terceiros, que não serão utilizados neste estudo, serão encobertos.

Para esta finalidade será utilizado o protocolo ARP (Adress Resolution Protocol), que é o responsável por reconhecer o endereço MAC a partir de um endereço IP.

7.1. REDES CABEADAS

Para atrelar o IP ao MAC em uma conexão de tipo cabeada será necessário adicionar a “ARP List” qual computador poderá se conectar a saída de rede do MikroTik. Sendo assim será necessário incluir o endereço IP e o endereço físico (MAC) do computador que terá acesso. Após isto, deverá ser escolhida a interface; neste caso a interface escolhida seria a LAN1 - Saída” que representa a saída de rede.

Uma boa dica é nomear os integrantes desta lista de acesso, pois, identificar os computadores e dispositivos apenas por seus respectivos endereços IP e MAC se tornaria

uma tarefe complicada. Neste caso a nomenclatura será “Administrador da Empresa A”. A figura 25 demonstra as configurações acima descritas.

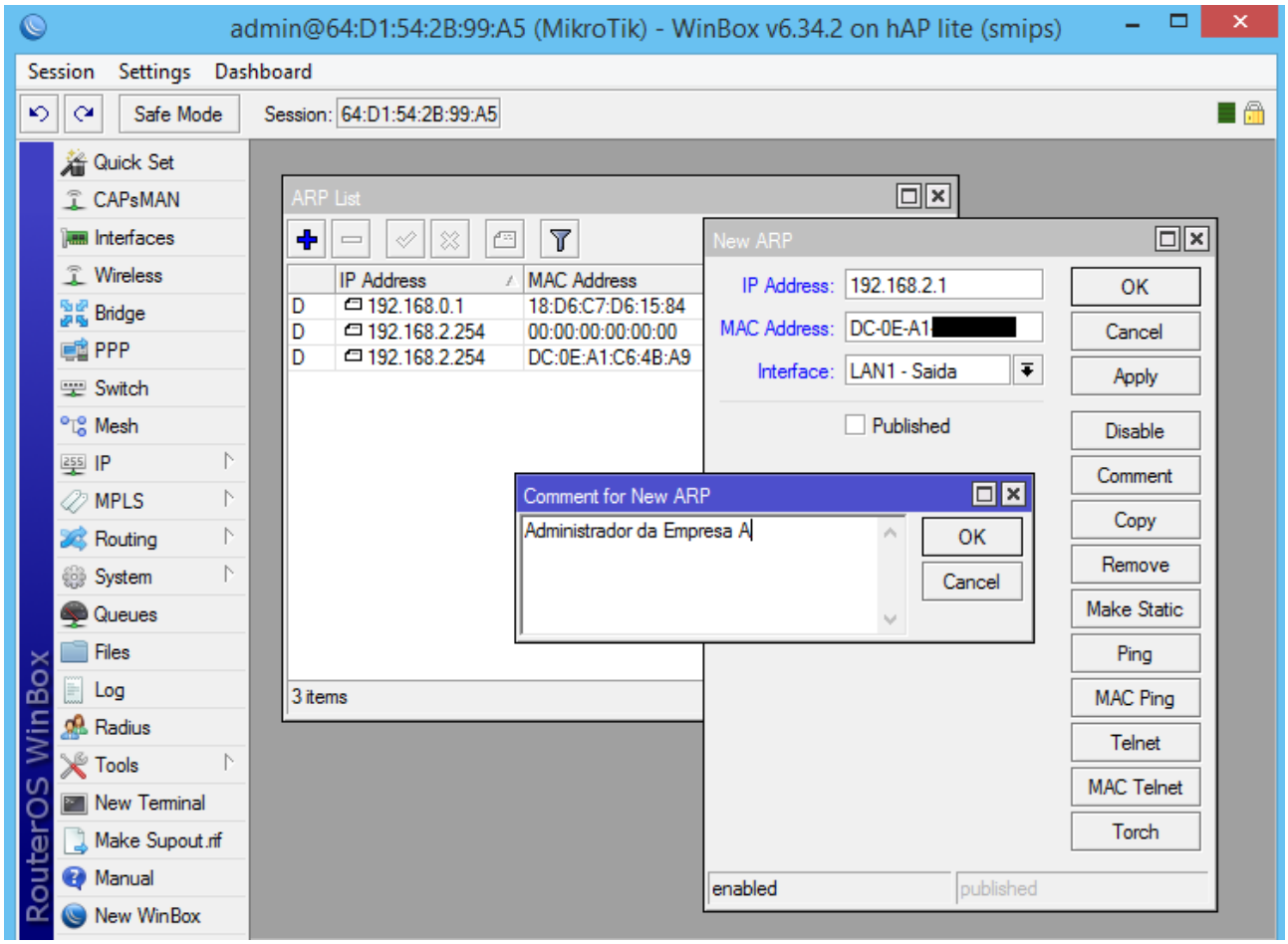

Figura 25: Atrelar IP ao MAC- ARP List
Fonte: Banco de imagens Windows

Após isto uma alteração na interface deverá ser realizada. Neste caso, a interface “LAN1 – Saída” deverá ser alterada em ARP, devendo conter a configuração “*reply-only*”, ou seja, somente quem estiver cadastrado na ARP List terá acesso a rede. A figura 26 demonstra a configuração da interface.

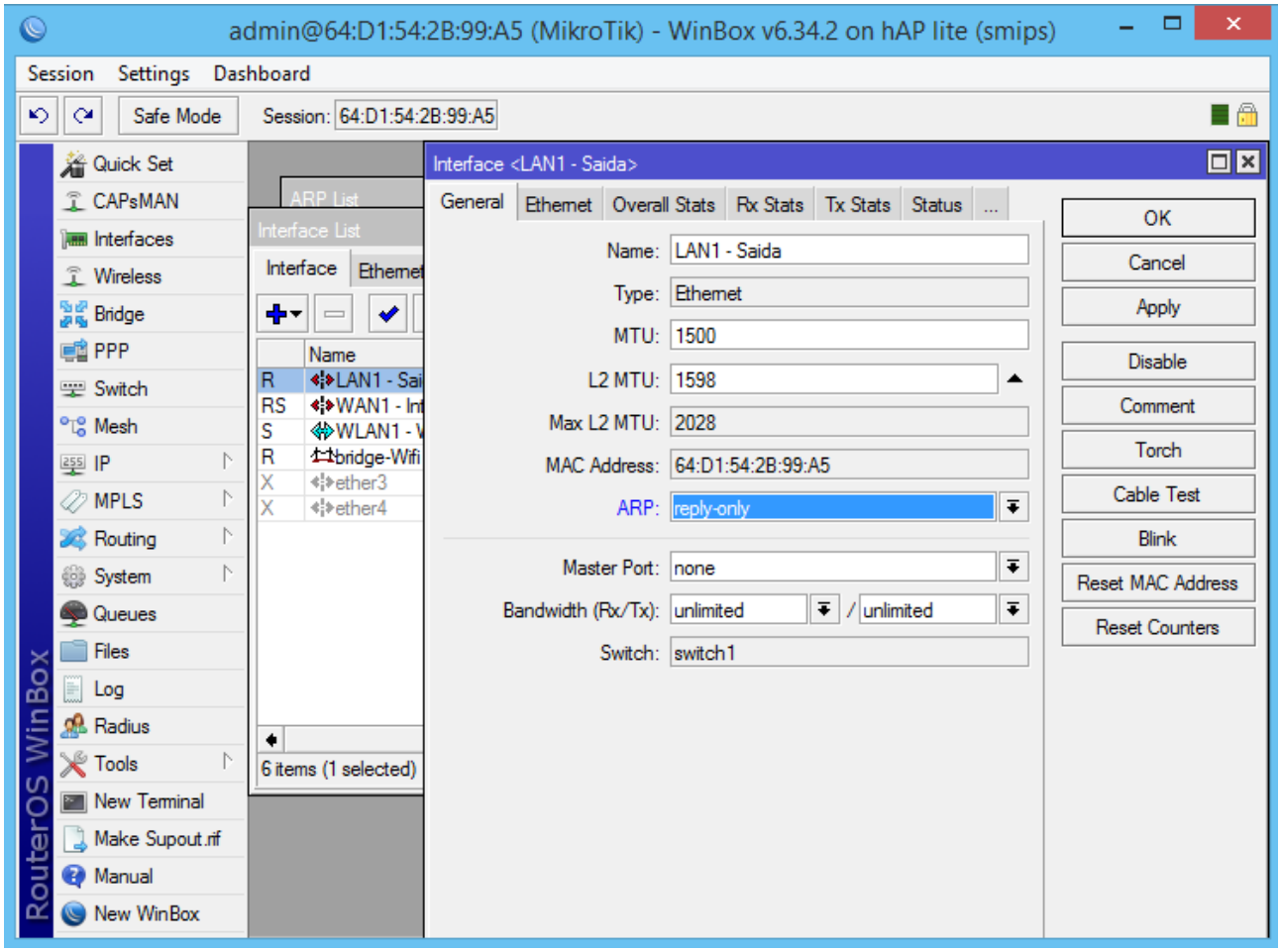

Figura 26: Atrelando IP ao MAC – Interface
Fonte: Banco de imagens Windows

Após as configurações completas, apenas a(s) máquina(s) cadastrada(s) terá(ão) acesso à rede da empresa, como exemplificado na figura 26.

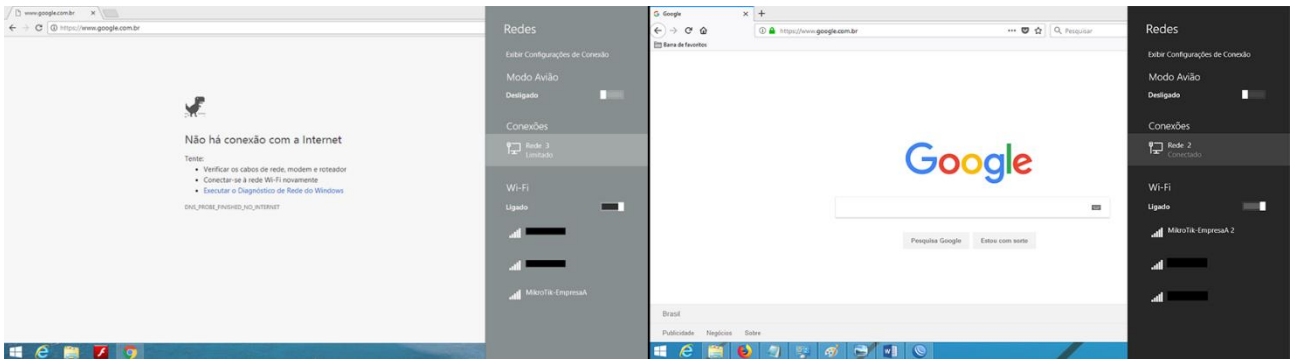

Figura 27: Pós configurações IP ao MAC

Fonte: Banco de imagens Windows

7.2. CONEXÃO SEM FIO

Embora possua uma configuração diferente da utilizada com a rede cabeada, a estratégia de proteção de acessos indevidos a rede sem fio seguirá um modelo semelhante; uma lista de acesso controla quais usuários poderão se conectar à rede wireless da empresa.

A ideia desta estratégia é proteger a rede sem feio através de dois itens de extrema proteção: uma senha e o Media Acess Control (MAC). Sendo assim, o usuário que deseja conectar-se através do “roteador” deverá ter, além do prévio conhecimento da senha utilizada, o número de MAC registrado na lista de acessos permitidos a rede *wireless*.

Sendo assim, a primeira tarefa a ser realizada é desabilitar os padrões de acesso na interface responsável pelo acesso sem fio; neste caso, a interface responsável é a “WLAN1 – Wireless”. Desabilitando as opções “Default Authenticate” e “Default Forward”, os padrões de autenticação e roteamento são desabilitados, ficando sobre responsabilidade das regras de controle de acesso. A figura 28 exemplifica os passos descritos acima.

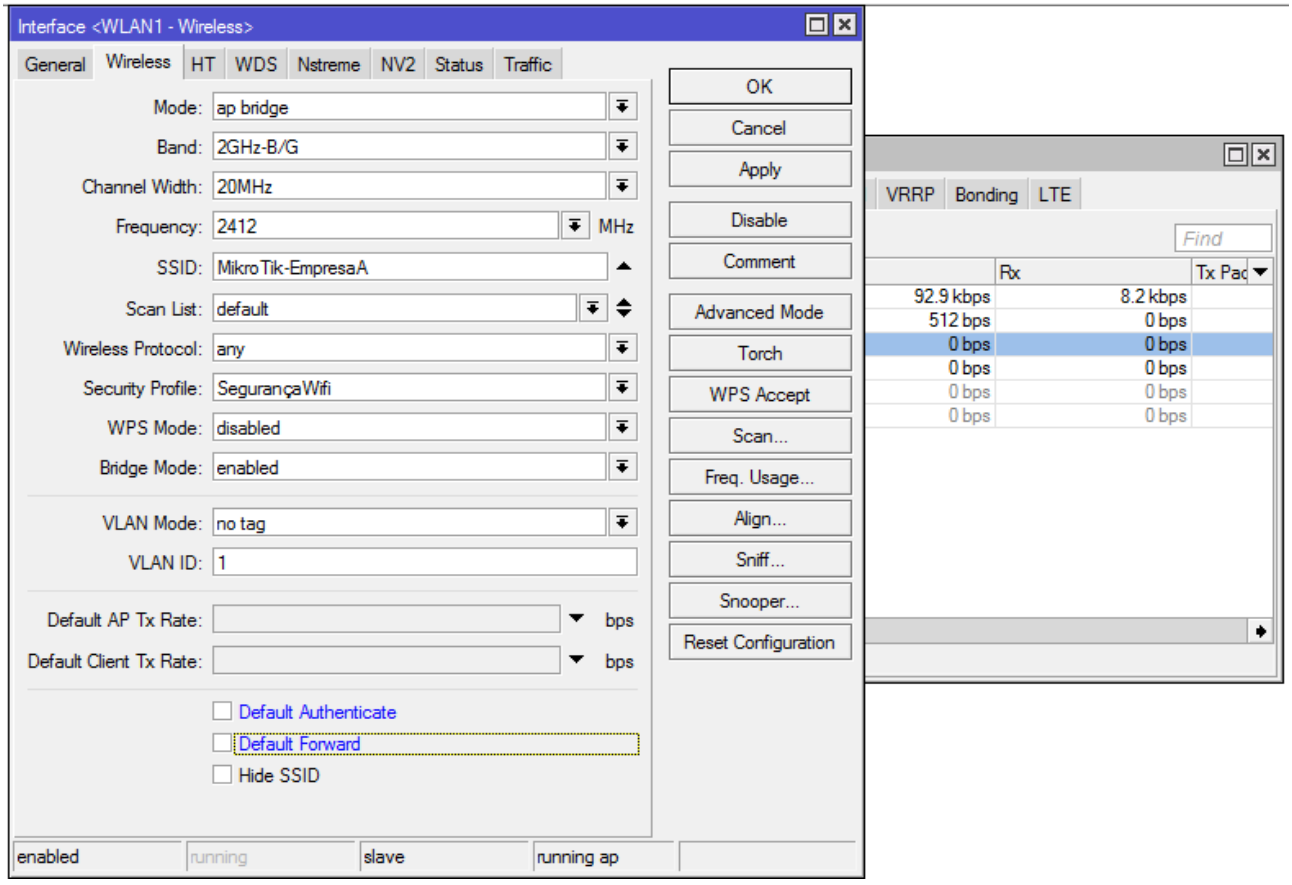

Figura 28: Desabilitar “Default Authenticate” e “Default Forward”

Fonte: Banco de imagens Windows

Em seguida será necessário adicionar quais dispositivos deverão ter acesso a rede *wireless* do MikroTik. Neste estudo será utilizado um computador *notebook* e um *smartphone* (Android), a fim de simular o cotidiano de uma micro empresa.

Sendo assim em *AP Acess Rules",* deverá ser adicionado o endereço MAC do dispositivo e a interface que irá controlar e receber os devidos acessos, neste caso a "WLAN1 – Wireless". As *box* "Authenticate" e "Forward" deverão ser habilitadas, ficando sobre responsabilidade da regra de acesso a autenticação e roteamento. Uma boa prática é nomear os dispositivos, tornando fácil sua identificação e futuras manutenções que venham a ser necessárias. Neste caso, as regras serão nomeadas como "Smartphone Administrador" para o *smartphone* (Figura 29) e "PC Administrador" para o *notebook* (Figura 30).

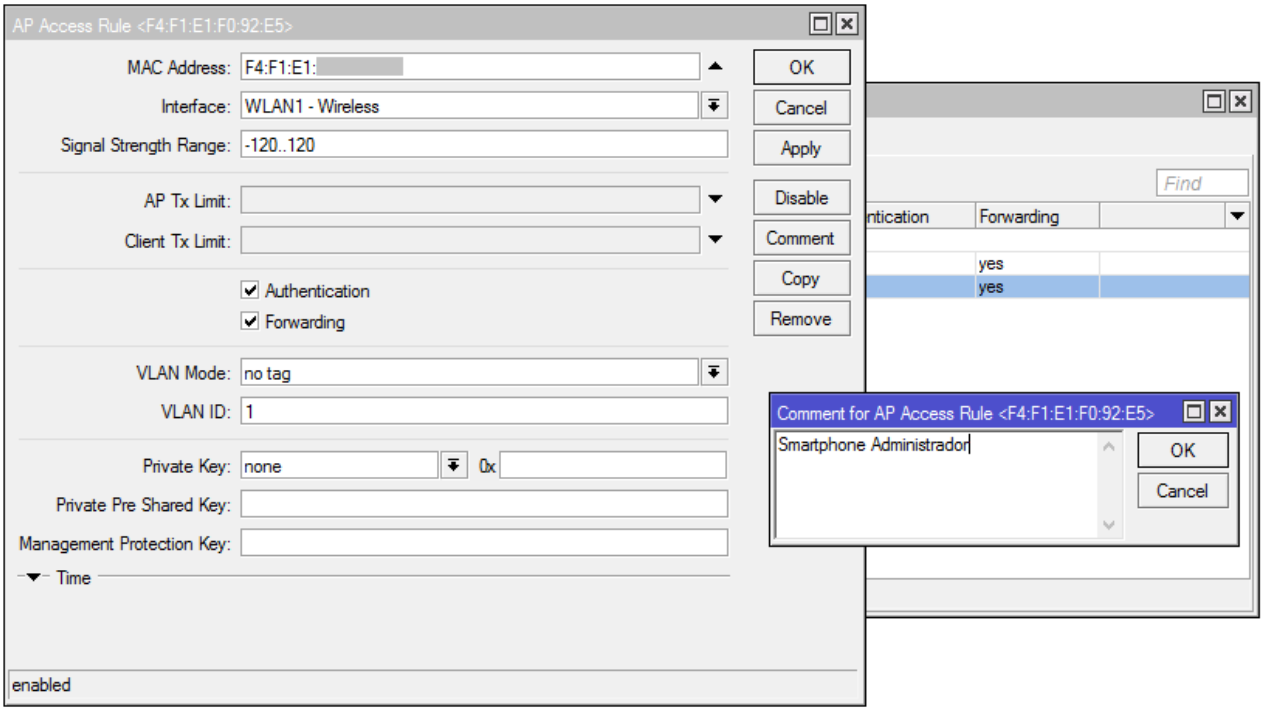

Figura 29: Adicionar Smartphone a AP Acess Rule

Fonte: Banco de imagens Windows

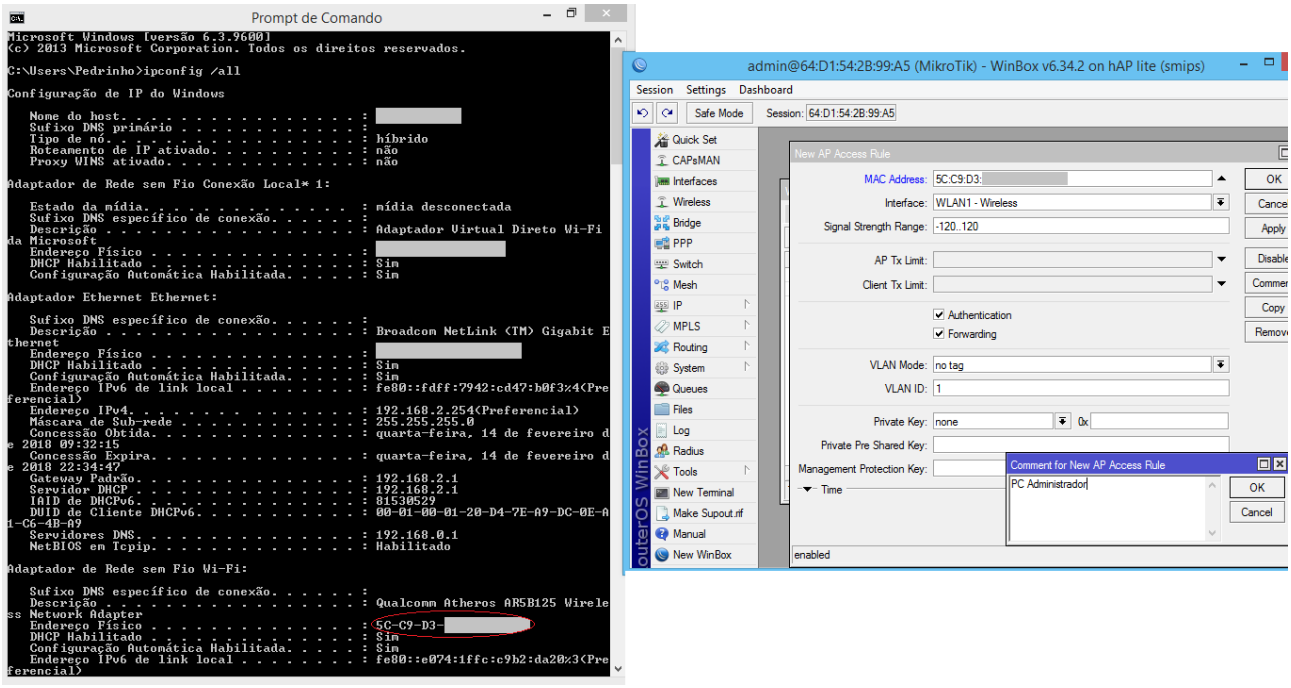

Figura 30: Adicionar Notebook a AP Acess Rule

Fonte: Banco de imagens Windows

Vale ressaltar que, ao utilizar o comando *"ipconfig /all"* na plataforma MS-Windows, o mesmo irá retornar todos os adaptadores de rede disponíveis na máquina. No caso da Figura 30, foram retornados os adaptadores de máquina virtual (instalada no dispositivo), o adaptador Ethernet (para rede cabeada) e o adaptador *wireless*. Cada dispositivo possui um MAC específico, embora estejam em um único dispositivo. Para que o *notebook* possua acesso, o endereço MAC a ser configurado na regra de acesso do MikroTik deverá ser o "Endereço Físico" do adaptador *wireless* (marcado com círculo vermelho na Figura 30).

Após inseridos os dispositivos que terão acesso à rede sem fio, nenhum outro dispositivo fora da lista terá acesso, como demonstram as figuras 31 e 32.

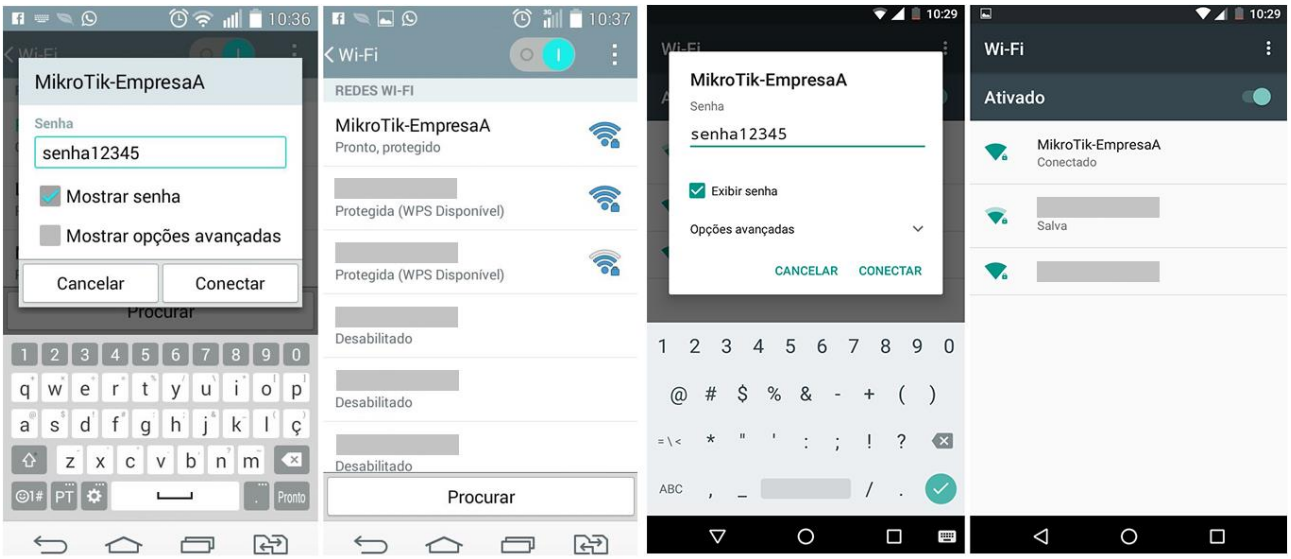

Figura 31: Acessos via smartphone

Fonte: Banco de imagens Windows

Na Figura 31, dois *smartphones* tentam conexão à rede “MikroTik-EmpresaA” (rede deste estudo). A esquerda, o dispositivo que tenta conexão não foi adicionado à lista de acesso, portanto, mesmo inserindo a senha, o mesmo não terá acesso a rede. Diferente do dispositivo a direita, que foi adicionado à lista e, ao inserir a senha, imediatamente já está conectado à rede *wireless*.

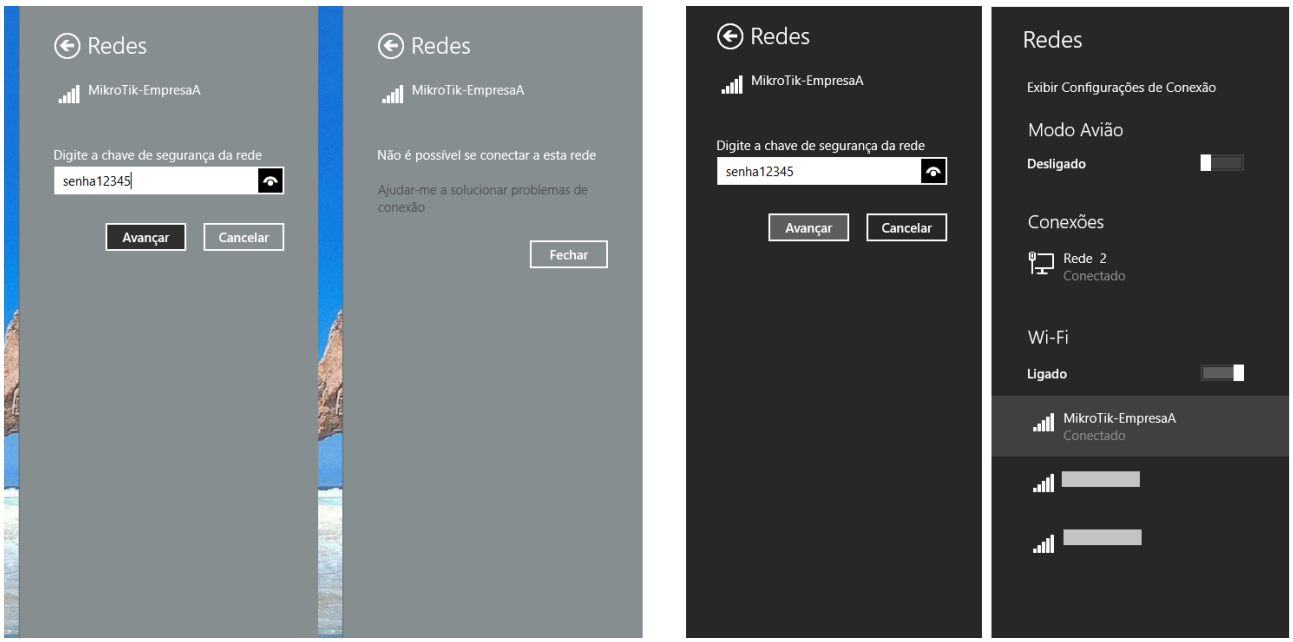

Figura 32: Acessos via notebooks

Fonte: Banco de imagens Windows

Na Figura 32, dois *notebooks* tentam conexão à rede sem fio. O *notebook* a esquerda insere a senha e avança, porém, não consegue realizar a conexão, pois não está na lista de acesso. Por outro lado, o *notebook* à direita insere a senha e logo em seguida já aparece conectado, pois o mesmo foi inserido na lista de acesso, possibilitando-lhe conexão à rede *wireless*.

8. SENHAS DE ACESSO E BLOQUEIO DE SITES INDEVIDOS

Neste capítulo, será dada a devida importância a um elemento muito importante, porém muito ignorado em diversos casos; a senha. Outra boa prática que merece destaque é o bloqueio de sites indevidos.

8.1. SENHA DE ACESSO

A senha possui uma função fundamental na segurança de uma rede (wireless), seja de uma micro empresa ou de um residência. Em diversos casos, usuários deixam de se preocupar com a segurança visando a praticidade, ou seja, ao invés de utilizar de uma senha mais segura, optam por utilizar de caracteres fáceis de recordar, visando simplesmente não esquecer a senha.

Segundo pesquisas da empresa Keeper Security, as senhas mais utilizadas no mundo, são sequencias simples de números e do alfabeto, ou acrescidas a palavra “senha”. No item 4.1 deste estudo, o roteador padrão foi configurado seguindo a pesquisa realizada pela empresa acima mencionada. Tendo consciência disto, crackers do mundo tudo possuem uma “lista” com as senhas mais frequentemente usadas, tornando seu trabalho de invasão mais fácil. Senhas como: “senha”, “123”, “12345”, “qwerty”, bem como datas de nascimento ou nomes, estão tornando a rede, ou qualquer que seja o objetivo de proteção desta senha, vulnerável a acessos indevidos.

Senhas mais seguras utilizam de combinações entre letras maiúsculas e minúsculas, números e símbolos. A utilização de símbolos, principalmente, torna as combinações mais complexas, dificultando o trabalho de softwares de invasão, que poderiam levar meses para tal atividade. Outro detalhe é o número de caracteres; uma quantidade maior de caracteres aumenta as possíveis combinações. A empresa McAffe, por exemplo, apresentou em um de seus artigos uma simples sugestão, que em muito pode auxiliar pessoas que tem dificuldades em lembrar suas senhas: uma frase, que seja fácil de guardar.

A seguir, será utilizada a ferramenta Crunch do Kali Linux, a fim de realizar um teste de combinações de caracteres.

8.2. COMBINAÇÕES DE CARACTERES

Como citado acima, uma senha segura deve dispor de uma combinação de caracteres que não sejam simples. Com o auxílio da ferramenta Crunch, será criada uma wordlist para fins de comparação, onde a senha deverá conter entre oito e dez caracteres, sendo estes números, letras (Maiúsculas e Minúsculas), espaço (que também é um caractere) e caracteres especiais, como por exemplo a arroba (@) ou o cifrão ($).

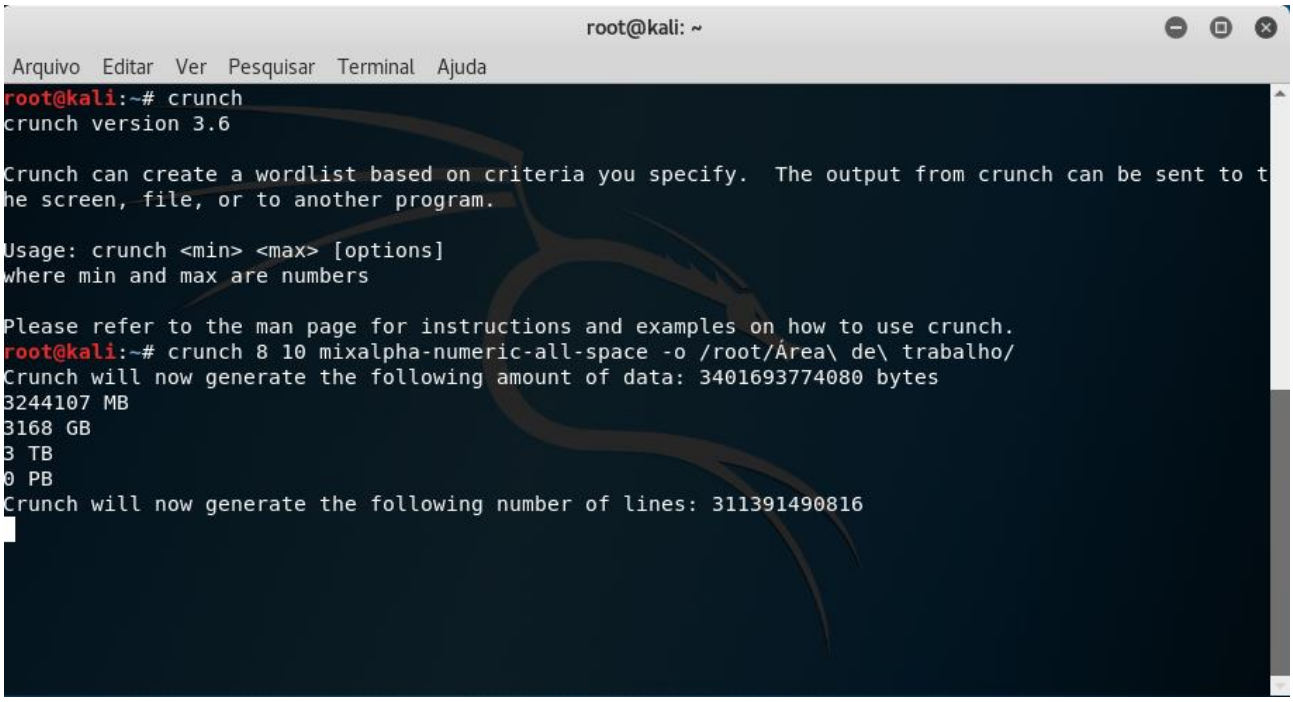

Figura 33: Gerando Combinações com Crunch

Fonte: Banco de imagens Windows

Conforme ilustra a Figura 33, a ferramenta retornou um arquivo de texto contendo 311.391.490.816 (trezentos e onze bilhões trezentos e noventa e um milhões quatrocentos e noventa mil oitocentos e dezesseis) combinações, sendo este arquivo equivalente a 3.168 (três mil cento e sessenta e oito) Gigabytes, ou aproximadamente, três Terabytes de informação.

Porém, é possível acrescentar mais caracteres à combinação, o que tornaria a wordlist com maior número de combinações.

8.3. BLOQUEANDO SITES INDEVIDOS

Quem utiliza da rede mundial de computadores, seja para trabalho ou para lazer, deve sempre estar atento aos sites que frequenta. Sites maliciosos podem conter aplicações maliciosas, com a finalidades de roubos de dados e informações ou, simplesmente, causar danos às máquinas que os acessam. Segundo pesquisas realizadas pela empresa Google LLC, cerca de 9,5 mil sites maliciosos são descobertos por dia, a sua maioria, hospedada no Brasil.

Alguns sites de entretenimento, encontros virtuais, compra e venda de mercadorias ou conteúdo pornográfico, são, em sua maioria, responsáveis por conter “escondidos” alguns programas maliciosos (*Malware*), como por exemplo, *Trojan*, *Ransomware*, *Spyware*, entre outros.

É certo de que uma das melhores formas de prevenção é evitar acessos a sites de conteúdos duvidosos. Porém, o MikroTik oferece a vantagem de bloquear sites específicos, seja por nome ou até mesmo por seu endereço IP.

As figuras 35 e 36 demonstram as configurações de Firewall para bloqueio de sites.

Neste estudo será bloqueado o site da Fundação Educacional do Município de Assis (FEMA).

8.4. BLOQUEANDO SITES POR IP

Como já descrito é possível realizar o bloqueio por IP e nome (Domínio). Caso deseje utilizar o endereço IP do site será necessário descobri-lo. O bloqueio através do endereço IP de um site é mais eficiente do que o bloqueio por domínio, tendo em vista que não seria necessário retornar DNS. Para tal, foi utilizado o comando “*ping*”, como demonstrado na Figura 34.

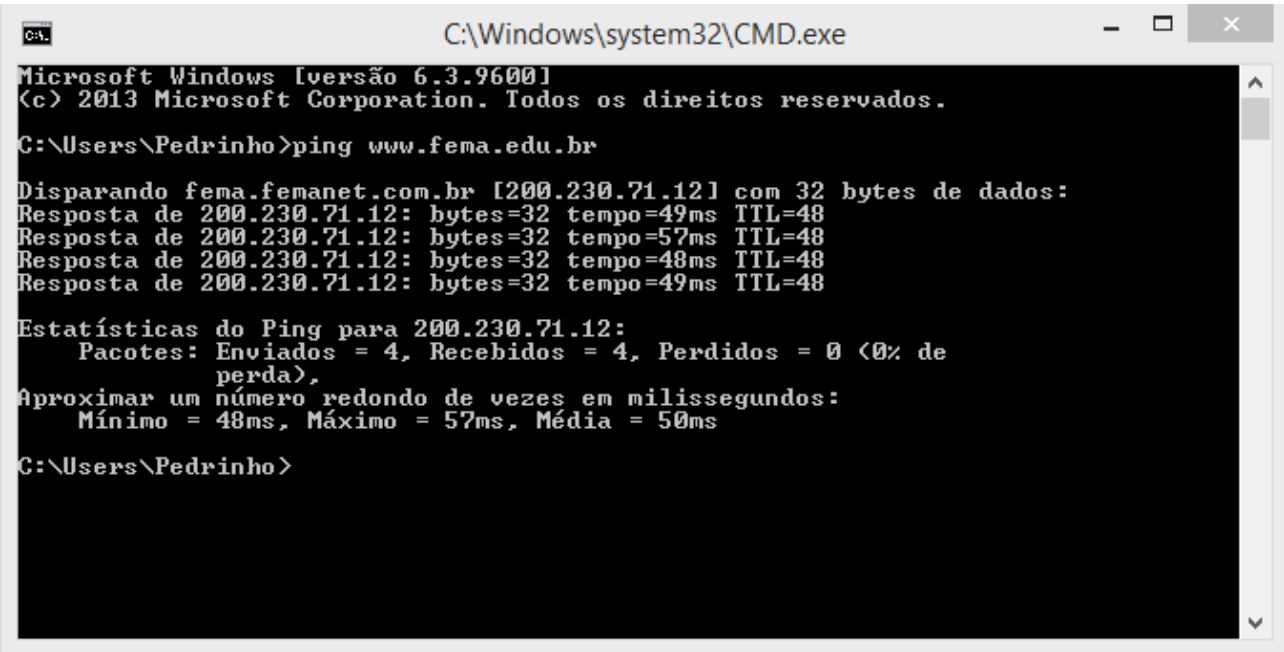

Figura 34: Descobrindo IP de Site para Bloquea-lo

Fonte: Banco de imagens Windows

Após a identificação do endereço IP do site a ser bloqueado, será adicionado um novo filtro ao Firewall do MikroTik. Em *Chain* será utilizado "*forward*"; em *Dst.Addres* será inserido o IP do site (no estudo será 200.230.71.12); *Protocol* irá ser o padrão (TCP); em *Content* será acrescentado a palavra "fema"; *Action* deverá receber *"reject"*, ou seja, a requisição a este site será rejeitada; em *Log* apenas foi diitado "Site da Fema Bloqueado", apenas para fins de controle do administrador, ao acessar os arquivos de *logs* do MickoTik; e em *Reject With* a configuração será "*icmp admin prohibited",* que terá a finalidade de informar ao usuário que realizar tentativa de *ping* ao site, que o mesmo foi bloqueado pelo administrador. As Figuras 35 e 36 demonstram as configurações acima citadas.

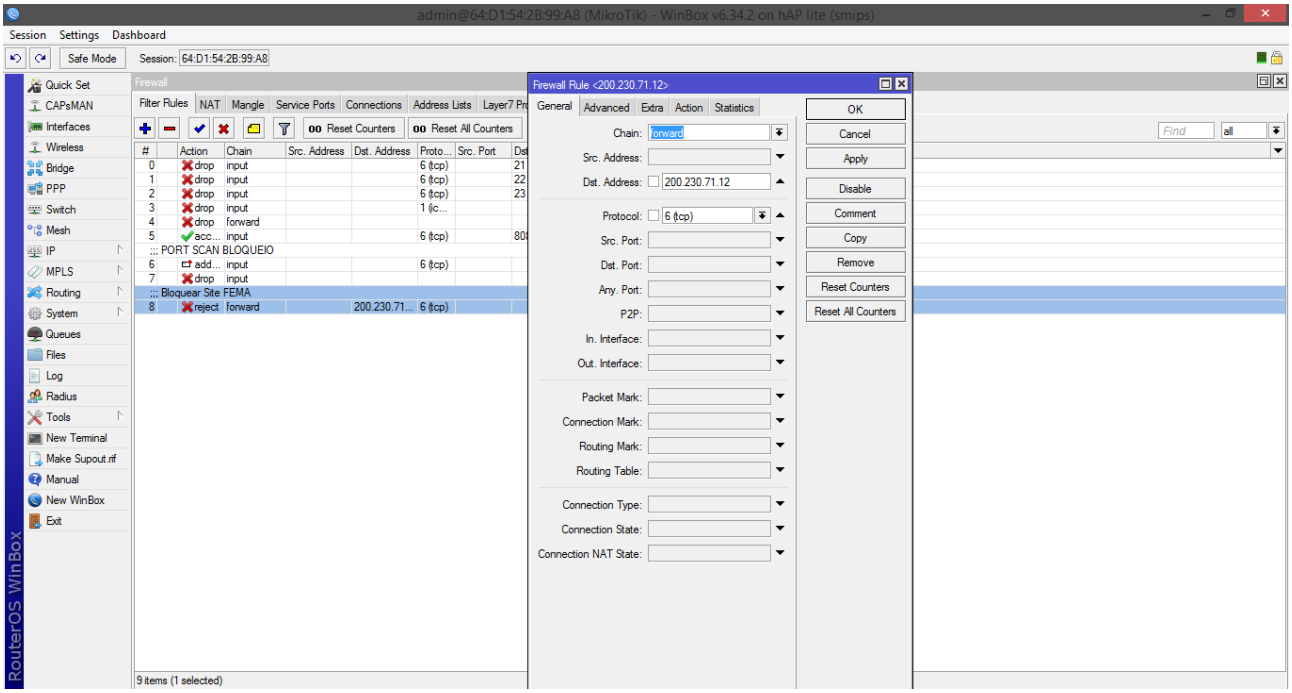

Figura 35: Configuração Bloqueio de Site I

Fonte: Banco de imagens Windows

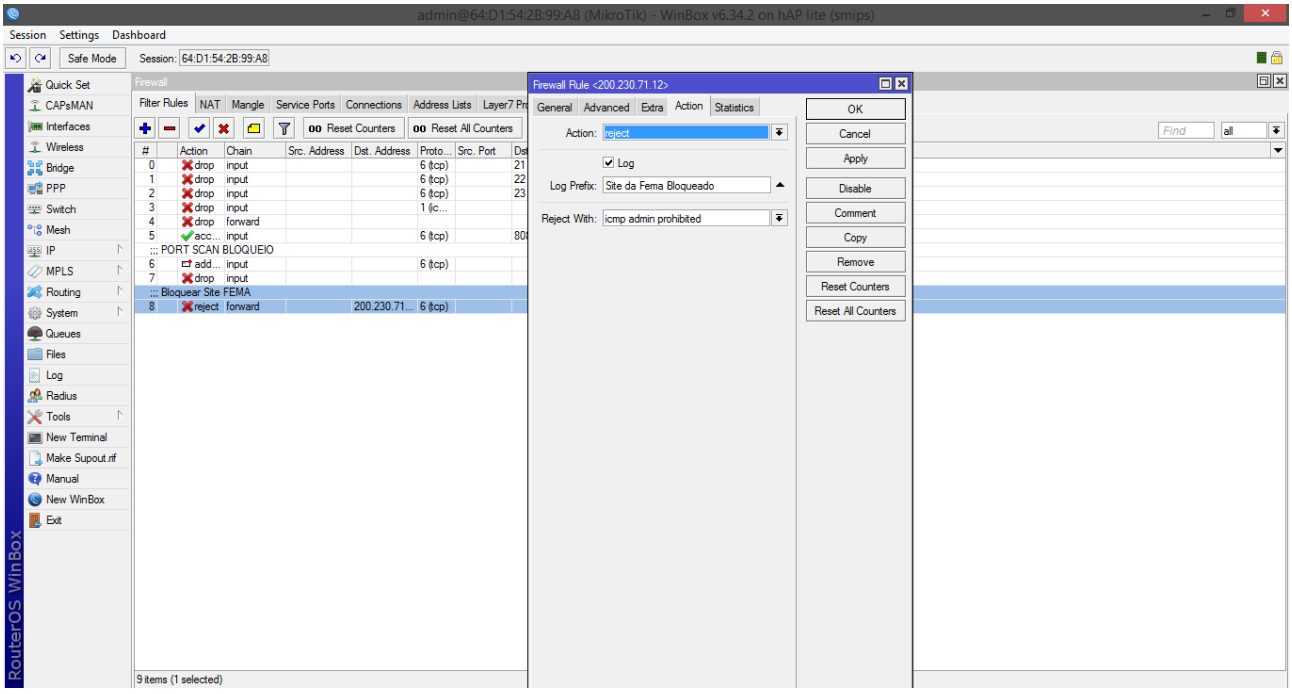

Figura 36: Configuração Bloqueio de Site II

Fonte: Banco de imagens Windows

9. BACKUP DO MICKOTIK

Após as configurações realizadas no MikoTik hAP Lite, uma boa prática, não somente para esta finalidade mas também para documentos de uma micro empresa, é o *Backup*. Utilizando de um *backup* as configurações realizadas no MikroTik poderão ser restauradas quando necessário, seja em uma perda das mesmas, ou por alguma eventualidade.

Em *Files*, o MikoTik permite com que seja criado um *backup* das configurações; O administrador ainda poderá optar por inserir uma senha no arquivo criado, como mostra a Figura 37.

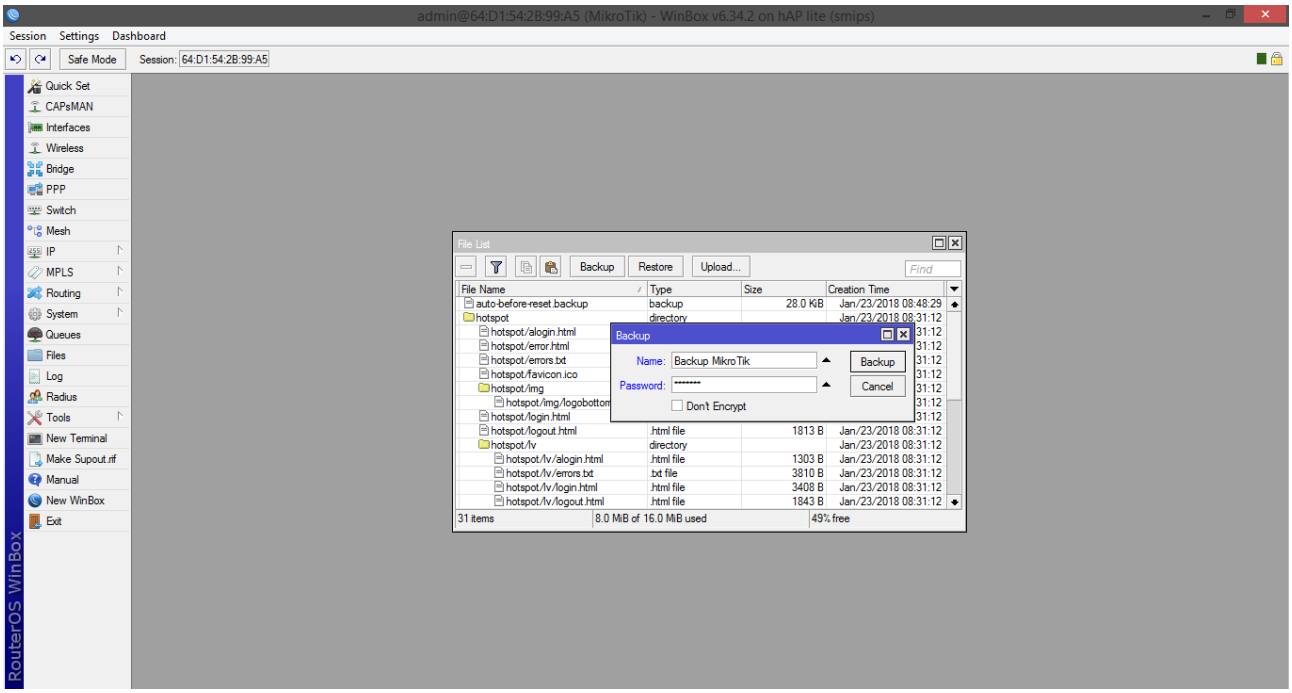

Figura 37: Backup do MickoTik

Fonte: Banco de imagens Windows

Outra boa prática sugerida é que o arquivo de *backup* não esteja apenas no mesmo computador do administrador. Ao clicar (com o botão direito do *mouse*) sobre o arquivo gerado, o MikroTik permite com que seja feito um *download* (cópia) do mesmo, para ser salvo em outro lugar.

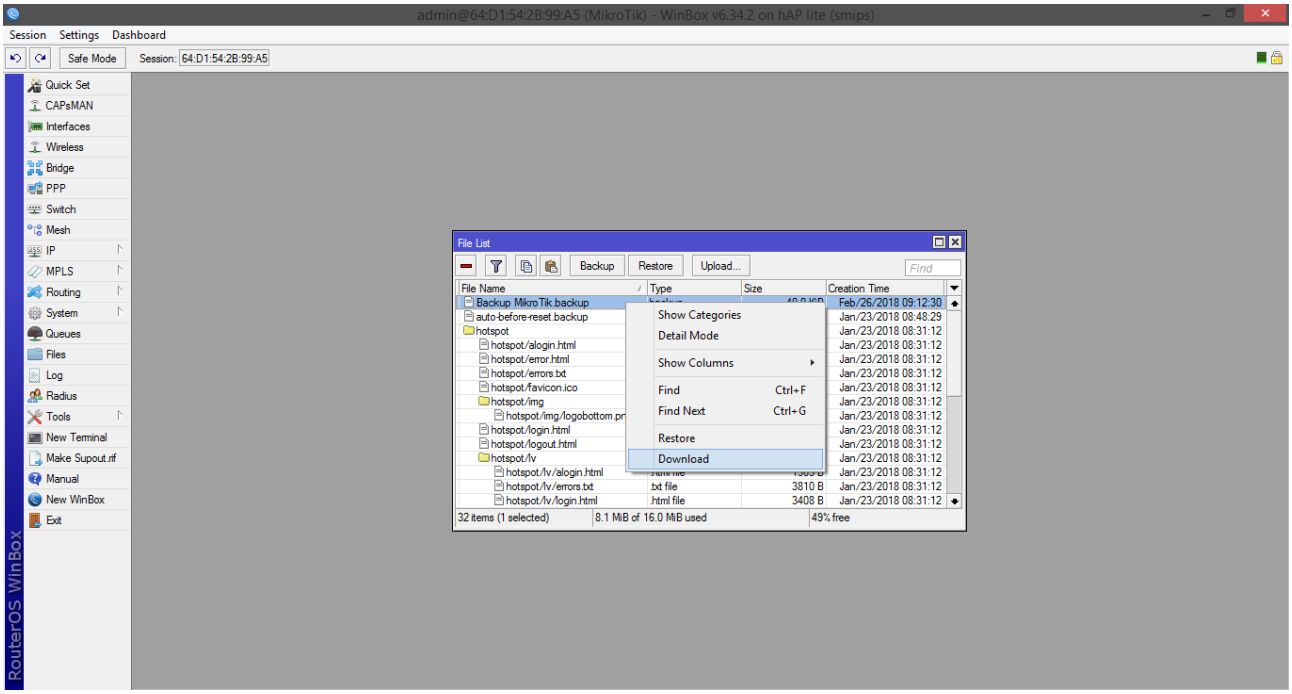

Figura 38: Download Arquivo de Backup

Fonte: Banco de imagens Windows

10. CONCLUSÃO

A facilidade de acesso à rede mundial de computadores e os avanços em softwares, trouxe praticidade e comodidade a todos e, para as empresas não seria diferente. O fato de muitas pessoas estarem investindo em “negócios próprios” torna a Internet um item, praticamente obrigatório, para microempreendedores, seja para divulgação de produtos ou serviços, como também para compra de mercadorias, sistemas de controle de estoque, emissão de notas fiscais até transferências bancárias. Porém, para obter acesso a tudo isso é necessário, além de um serviço de Internet, uma proteção.

Proteções como VPN e outras podem possuir um alto custo de investimento para o microempreendedor.

Este estudo demonstrou soluções práticas em com baixo custo de investimento, concedendo ao microempreendedor, não somente proteção, mas também maior praticidade e opções de monitoramento à sua rede.

A tecnologia apresentada foi a MikroTik hAP e a interface gráfica “*Winbox*”. Além da tecnologia, que auxilia o administrador da rede, foram explanas, ainda, técnicas que podem aumentar a segurança da rede, como por exemplo, desativar serviços de rede que muitos desconhecem (sem ter um determinado conhecimento em redes de computadores), como demonstrado no capítulo seis; limitar dispositivos que podem se conectar à rede, utilizando do Media Acess Control; bloqueio de sites indevidos, que poderiam abrigar programas maliciosos.

De nada serviria técnicas de proteção sem um cuidado primordial em redes de computadores: a senha de acesso. Foi explanado, também, neste estudo, sobre a importância de uma senha complexa, mesclando letras maiúsculas e minúsculas, números e símbolos, o que tornaria mais difícil e longo o processo de combinação de caracteres, utilizados em softwares de invasão.

Pode-se concluir que o MikoTik oferece uma maior proteção ao administrador da rede, porém, em alguns casos, é exigido um alto conhecimento em redes para as configurações necessárias. Sendo o MikoTik um Sistema Operacional sem ambiente gráfico, a ferramenta WinBox oferece um auxílio ao usuário, uma vez que o mesmo dispõe de uma interface gráfica para as configurações, ao invés de um terminal com linhas de comando.

Este estudo foi desenvolvido com objetivo de alertar e oferecer opções de segurança a micro e pequenas empresas, sem um alto custo de investimento.

Outro ponto que merece destaque é o fato de que, as configurações e técnicas aqui explanadas, podem ser utilizadas, não apenas em micro empresas, mas também, em residências que possuem serviço de Internet.

REFERÊNCIAS

ALERTA SECURITY. **Base Capítulo 1 – Os Pilares da Segurança da Informação.** Disponível em: https://www.alertasecurity.com.br/blog/31-base-capitulo-1-os-pilares-da-seguranca-da-informacao. Acesso em: 24 out. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Tecnologia da Informação – Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 177799:2001.** Disponível em: http://www.cienciianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf. Acesso em: 11 jun. 2017.

CISCO. **Usando os Comandos Ping e Traceroute Estendidos.** Disponível em: https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.pdf. Acesso em: 31 jan. 2018.

CLOTED, J. **Uma Introducción al Tema de la Ética**. Disponível em: https://www.ufrgs.br/bioetica/etica.htm. Acesso em: 24 out. 2017.

CORE SECURITY. **Penetration Testing Overview.** Disponível em: https://www.coresecurity.com/content/penetration-testing. Acesso em: 25 out. 2017.

G1. **Ataque Hacker Atingiu Computadores em Quase 100 Países na Sexta**. Disponível em: http://g1.globo.com/jornal-nacional/noticia/2017/05/ataque-hacker-atingiu-computadores-em-quase-100-paises-na-sexta.html. Acesso em: 25 set. 2017.

HIGA, Paulo. **Google Encontra 9,5 Mil Novos Sites Maliciosos Por Dia.** Disponível em: https://tecnoblog.net/104901/google-safe-browsing/. Acesso em: 03 jul. 2018.

HIMANEN, Pekka. **Primeira parte: a ética do trabalho. A ética Hacker.** Disponível em: <L'etica hacker e lo spirito dell'età dell'informazione>. Acesso em: 25 out. 2017.

LAUREANO, Marcos Aurelio Pchek e MORAES, Paulo Eduardo Sobreira. **Segurança como Estratégia de Gestão da Informação.** Pontifícia Universidade Católica do Paraná - PUCPR. Disponível em: http://roitier.pro.br/wp-content/uploads/2016/02/asti_ii_material_apoio_2_seguranca_informacao_texto_base2.pdf. Acesso em: 11 jun. 2017.

Lei Nº 12.737. **Código Penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 out. 2017.

MALAGÓN, Constantino. **Nebrija Universidad - Hacking Ético. ProSeLex**. Disponível em: https://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_0.pdf. Acesso em: 25 out. 2017.

MOORE, GE. **Princípios Éticos**. Disponível em: https://www.ufrgs.br/bioetica/etica.htm. Acesso em: 24 out. 2017.

NUNES, Mauricio. **Bloqueio Por Conteúdo da URL.** Disponível em: https://www.mundotibrasil.com.br/bloqueio-por-conteudo-da-url/. Acesso em: 03 jul. 2018.

OFFENSIVE SECURITY. **About Kali Linux**. Disponível em: https://www.kali.org/about-us/. Acesso em: 25 out. 2017.

RAYMOND, Eric. **The New Hacker's Dictionary. ProSeLex**. Disponível em: http://www.proselex.net/Documents/The%20New%20Hacker's%20Dictionary.pdf. Acesso em: 25 out. 2017.

REZENDE, D.A.; ABREU, A.F. **Tecnologia da Informação Aplicada a Sistemas de Informações Empresariais: O Papel Estratégico da Informação e dos Sistemas da Informação nas Empresas.** Disponível em: http://semanaacademica.com.br/system/files/artigos/dalvancunha-asegurancadainformacaoeasuaimportanciaparaaauditoriadesistemas.pdf. Acesso em: 23 out. 2017.

ROUSE, Margaret. **Black Hat**. Disponível em: http://searchsecurity.techtarget.com/definition/black-hat. Acesso em: 25 out. 2017.

ROUSE, Margaret. **Gray Hat.** Disponível em: http://searchsecurity.techtarget.com/definition/gray-hat. Acesso em: 25 out. 2017.

ROUSE, Margaret. **Pen Test (Penetration Testing).** Disponível em: http://searchsoftwarequality.techtarget.com/definition/penetration-testing. Acesso em: 25 out. 2017.

ROUSE, Margaret. **White Hat.** Disponível em: http://searchsecurity.techtarget.com/definition/white-hat. Acesso em: 25 out. 2017.

SABER COM LÓGICA. **Camada de Enlace**. Disponível em: http://sabercomlogica.com/pt/ebook/camada-de-enlace-endereco-mac-e-arp. Acesso em: 14 fev. 2018.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva**. Disponível em: http://semanaacademica.com.br/system/files/artigos/dalvancunha-asegurancadainformacaoeasuaimportanciaparaaauditoriadesistemas.pdf. Acesso em: 12 jun. 2017.

TECH TARGET. **Penetration Testing Strategies.** Disponível em: https://searchnetworking.techtarget.com/tutorial/Penetration-testing-strategies. Acesso em: 25 out. 2017.

TOMAZI, Sandra. **Uma Lei, Muitas Dúvidas.** Disponível em: http://www.gazetadopovo.com.br/vida-publica/justica-direito/uma-lei-muitas-duvidas-0amq7lj8b0skxnonfd5qh1glq. Acesso em: 24 out. 2017.

VEJA. **Vazamento Revela as 25 Senhas mais Comuns do Mundo**. Disponível em: https://veja.abril.com.br/economia/vazamento-revela-as-25-senhas-mais-comuns-do-mundo/. Acesso em: 24 jan. 2018.

WIKIPÉDIA. **Kali Linux**. Disponível em: https://pt.wikipedia.org/wiki/Kali_Linux. Acesso em: 25 out. 2017.