Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

TECNOLOGIAS E FERRAMENTAS PARA PREVENÇÃO DE ATAQUES EM REDES DE COMPUTADORES

Alexandre Gomes da Silva[1]
Anderson Roberto de Sousa Mesquita[2]
Cláudio Eduardo Paiva[3]

Resumo

A rápida propagação da internet mudou a perspectiva de segurança em rede. A condição de fácil acesso faz com que as redes de computadores fiquem vulneráveis a várias ameaças de ataque. Ameaças às redes são numerosas e potencialmente devastadoras. Assim, pesquisadores desenvolvem métodos e sistemas de detecção de invasões capazes de identificar e monitorar anomalias e ataques em vários ambientes disponíveis. Muitas das tecnologias propostas são complementares umas às outras, pois, para diferentes tipos de ambientes, algumas ferramentas têm melhor desempenho do que outras. Este artigo levantará, classificará e analisará sistemas de detecção de invasão (Intrusion Detection System – IDS) em uso atualmente. Com o objetivo de mostrar as vulnerabilidades presentes em redes sem fio, foram feitos testes de intrusão em um ambiente controlado, demonstrando falhas presentes em redes de computadores sem a devida proteção. A análise consiste no princípio de detecção de invasão e depois de certos aspectos operacionais do sistema para a prevenção da rede contra esses ataques.

Palavras-chave: Segurança em rede. Sistemas de detecção de invasões. Sistemas de prevenção de invasões. Testes de intrusão.

Abstract

The rapid spread of the Internet has changed the perspective of network security. The easy access condition makes computer networks vulnerable to multiple attack threats. Threats to networks are numerous and potentially devastating. Thus, researchers are always developing methods and intrusion detection systems capable of identifying and monitoring anomalies and attacks in various available environments. Many of the proposed technologies are complementary to each other, as for different types of environments require different types of tools. This article will gather, classify and analyze intrusion detection systems (IDS) currently in use. In order to show the vulnerabilities present in wireless networks, intrusion tests were made in a controlled environment, demonstrating failures present in computer

[1] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Dr Thomaz Novelino – Franca/SP. Endereço eletrônico: x3.computadores@hotmail.com
[2] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Dr Thomaz Novelino – Franca/SP. Endereço eletrônico: mesquitaads@gmail.com
[3] Professor Esp. Fatec Dr Thomaz Novelino – Franca/SP. Endereço eletrônico: claudiopaiva2@yahoo.com.br

networks without proper protection. The analysis consists of the principle of detection of invasion and also of certain operational aspects of the system for the prevention of the network against these attacks.

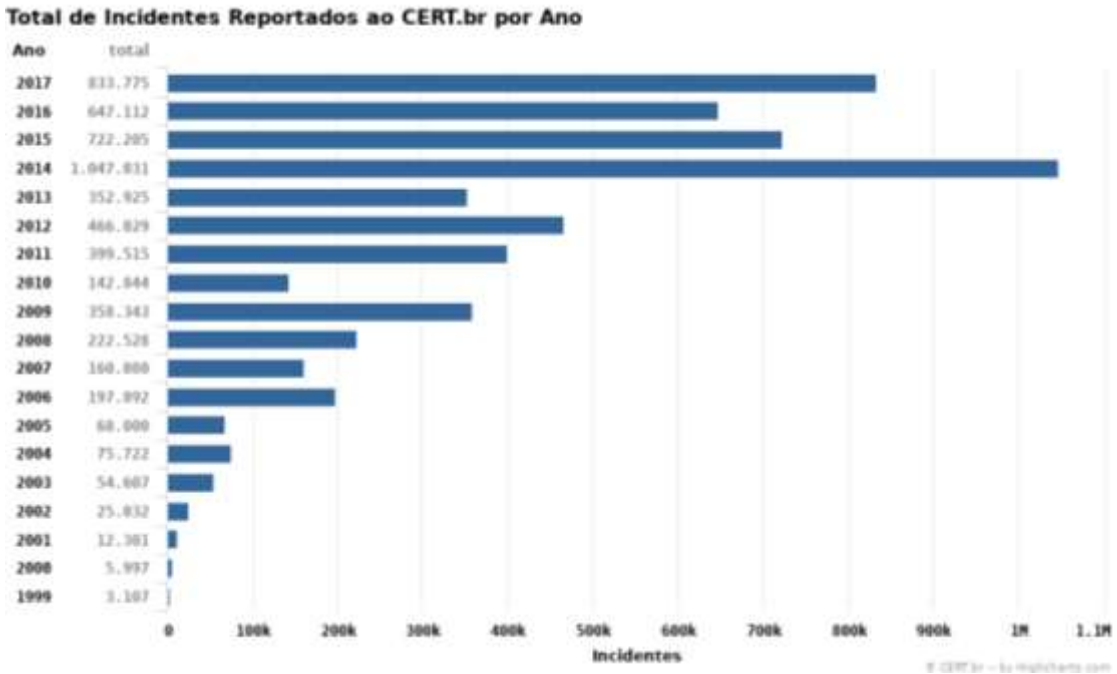
Key words: *Network security. Intrusion detection System. Intrusion prevention System. Intrusion Tests.*

1 Introdução

Com o rápido crescimento da Internet, os sistemas de computadores em rede estão desempenhando um papel cada vez mais vital na sociedade moderna, porém junto com os enormes benefícios que a Internet traz, ela também pode oferecer riscos aos seus usuários.

Novas ameaças são criadas todos os dias por indivíduos e organizações que atacam e inutilizam sistemas informatizados. Conforme relatado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2017) e exibido na Figura 1, o número de ataques a computadores no Brasil aumentou significativamente de 2016 para 2017. Segundo informações do Laboratório Especializado em Cyber Segurança da PSafe (DFNDR LAB), o número de ataques cibernéticos praticamente dobrou no Brasil em 2018 (PSAFE.COM, 2018).

Figura 1 – Estatísticas dos Incidentes Reportados ao CERT.br



Fonte: CERT.br, 2017

Além disso, a severidade e a sofisticação dos ataques também estão aumentando, como pode ser observado na Figura 2. Por exemplo, o *Sapphire/Slammer Worm* considerado o mais rápido da história, em apenas 10 minutos se espalhou por toda a Internet e infectou pelo menos 75.000 *hosts* causando interrupções de rede e consequências imprevisíveis, como cancelamento de voos de avião, interferência em eleições e falhas no Modo de Transferência Assíncrona (ATM[4]).

Dois aspectos devem ser levados em conta ao garantir a segurança de uma rede: proteção e supervisão. A proteção é composta por políticas de *hardware*, *software* e segurança. Mesmo tendo a melhor proteção possível, será sempre vulnerável a ataques, devido a *bugs* (quando o programa age de maneira inesperada ou fora do comum). Na supervisão são abordados os sistemas de controle que monitoram o comportamento da rede. Eles foram desenvolvidos especialmente com o objetivo de obter maior segurança.

As implementações de redes estão em constantes mudanças, aumentando assim a possibilidade de criar vulnerabilidades na segurança.

A fim de ajudar os administradores dessa área de segurança em rede, foram desenvolvidos os sistemas de detecção de invasão (*Intrusion Detection System* – IDS).

Os IDS são componentes essenciais de uma arquitetura de defesa para segurança da rede de computadores. Eles são uma tecnologia de segurança eficaz e podem detectar, prevenir e, possivelmente, reagir em função de ataques. Seu papel é monitorar as fontes-alvo de atividades, coletar e inspecionar os dados de auditoria procurando evidências de comportamentos intrusivos. Quando detecta tentativas suspeitas ou maliciosas, uma mensagem ou alarme é enviado ao administrador da rede dando a oportunidade de reagir prontamente. O principal objetivo dos IDS é detectar todas as intrusões de forma eficiente e sua capacidade de detecção e proteção dentro de uma rede é um dos principais atributos para a segurança das informações.

Diante do grande risco a que as redes de computadores estão expostas e, considerando a importância de se prevenir ou estar preparado contra ataques, este

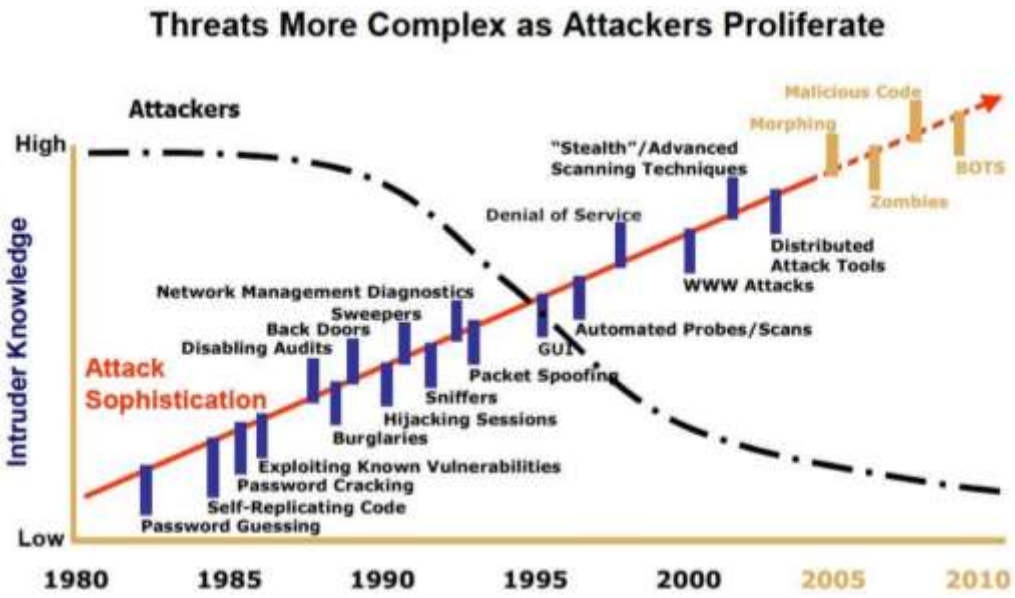
[4] ATM é uma técnica de comutação usada por redes de telecomunicação que usa multiplexação de divisão de tempo assíncrona para codificar dados em células pequenas e de tamanho fixo (Techopedia.com, 2018).

artigo se propõe a apresentar um material condensado com definições de mecanismos de segurança, métodos de ataques e ameaças, além de descrever tecnologias e procedimentos utilizados para confirmar a vulnerabilidade que algumas redes de computadores possam ter.

2 Redes de computadores, ataques e invasões

Em meados da década de 60, quando surgiram as primeiras redes de computadores, para que ocorressem ataques consistentes era necessária uma compreensão profunda do ambiente. No entanto, hoje em dia pessoas com conhecimentos em sistemas baseados em Linux, podem explorar mais facilmente as vulnerabilidades de um computador devido à ampla disponibilidade de ferramentas de invasão.

Figura 2 – Sofisticação do ataque vs. conhecimento técnico do intruso



Fonte: Hahn, Guillen e Anderson, 2005, p. 4

Invasões em sistemas de computadores são geralmente causadas por *hackers*, acessando a rede de internet, ou até mesmo por usuários autorizados dos sistemas, que tentam utilizar abusivamente as permissões dadas a eles e/ou obter privilégios para os quais não estão autorizados.

A fim de minimizar o impacto deste problema, grandes esforços são feitos no sentido de descobrir o quanto antes estas invasões, especialmente na criação de

sistemas específicos chamados sistemas de detecção de invasão. Este tipo de sistema pode ser definido como combinações de *softwares* e *hardwares* que monitoram os sistemas de computadores e disparam um alerta quando uma invasão acontece.

O site DEVMEDIA, 2011, classifica a detecção de invasão como:

> Um sistema automatizado de segurança e defesa detectando atividades hostis em uma rede ou em um computador (host ou nó). Além disso, o IDS tenta impedir tais atividades maliciosas ou reporta ao administrador de redes responsável pelo ambiente.

Existem vários métodos para detecção de uso indevido e de anomalias. Os IDSs monitoram e coletam dados da rede, analisando os pacotes transmitidos e geralmente não agem como reação operativa contra ataques ocorridos, mas tem o papel de informar ao administrador da rede as ocorrências de uma invasão.

Segundo Schetina e Carlson (2002), é preciso mais do que bons técnicos e grandes administradores de rede para que os sistemas de computadores não fiquem vulneráveis, é necessário também ter uma visão mais ampla da segurança da informação.

Pesquisas recentes apontam que as invasões dentro das organizações estão crescendo exponencialmente (ERNST & YOUNG, 2013). Para evitar tais intrusões são propostos IDS's habilitados com agentes móveis para detectar invasões em um tempo rápido no ambiente.

A fim de detectar anomalias, os perfis de atividade do usuário são criados e uma faixa de pontuação de similaridade (limite superior e inferior) é atribuída ao conjunto padrão normal de cada usuário. Quando em ação, o sistema calcula a pontuação de similaridade dos padrões da atividade atual e se essa pontuação não estiver na escala da contagem da semelhança, a atividade é considerada como uma anomalia.

Autores que tratam sobre segurança da informação apresentam várias definições para ataques de computadores e invasões. A mais popular definição de intrusão é que ela representa uma falha operacional induzida externamente. No entanto, outras definições da palavra ataque que a diferenciam da intrusão também foram propostas na literatura de detecção (GOODRICH; TAMASSIA, 2013).

Um sistema pode ser atacado (seja de fora ou no interior), mas o *firewall* defensivo em torno do sistema ou recurso visado pelo ataque pode ser suficientemente eficaz para evitar tal intrusão. Pode-se dizer que um ataque é uma tentativa de intrusão e uma intrusão resulta de um ataque que tenha sido (pelo menos parcialmente) bem sucedido.

São observados diferentes aspectos de segurança, pois existem sistemas de computadores com falhas de projetos no seu funcionamento que os deixam vulneráveis. Além disto, há ainda a questão do uso indevido de equipamentos por parte dos usuários, onde pessoas tentam obter o acesso a sistemas, ou dados, sem autorização.

2.1 Tipos comuns de ataques e invasões

O critério para se classificar os ataques e invasões a computadores é de acordo com a forma da implementação utilizada nessa tentativa de intrusão. De acordo com (MUNDODOSHACKERS.COM.BR, 2011), as técnicas mais comuns e utilizadas são:

Ataques de negação de serviço, ou *Denial of Service Attack* (DoS): estes ataques tentam encerrar uma rede, computador ou processo ou, de outra forma, negar o uso de recursos ou serviços a usuários autorizados. Há dois tipos de ataques DoS: ataques ao sistema operacional, que visam *bugs* em operações específicas nos sistemas, mas podem ser corrigidos com *patches* de atualizações; e ataques de rede, que exploram as limitações inerentes aos protocolos e infra-estruturas da rede. Um exemplo de ataque ao sistema operacional é Teardrop, em que um invasor explora uma vulnerabilidade do código de *re-assembly* de fragmentação de TCP/IP. Outro exemplo de ataques DoS incluem interromper conexões que impedem o usuário de acessar um determinado serviço. No ataque dos (DDoS) distribuído, que é uma variação avançada do ataque DoS, várias máquinas são implantadas para atingir esse objetivo. Os ataques DoS e DDoS representam uma ameaça crescente a Internet, e as técnicas para impedi-los tornaram-se um ativo para os pesquisadores.

Ataques por sondagem (vigilância, escaneamento): estes ataques são feitos através de escaneamentos nas redes para identificar endereços IP válidos e coletar informações sobre os sistemas executados. Muitas vezes, esta informação

fornece ao invasor uma lista de vulnerabilidades que posteriormente podem ser usadas para executar um ataque contra máquinas e serviços selecionados. Exemplos de ataques de sondagem incluem IPsweep (escaneamentos dos computadores de rede para um serviço em uma porta específica de interesse), Portsweep (escaneamento através de muitas portas para determinar qual os serviços são suportados em um único *host*), Nmap (ferramenta para mapeamento de rede), entre outros. Embora estes ataques sejam comuns, as ferramentas de detecção de varreduras baseadas nestas técnicas são bastante ineficientes.

Ataques por comprometimentos: esses ataques usam vulnerabilidades conhecidas, como estouro de *buffer (buffer overflow)* utilizando-se de pontos de segurança fracos para invadir o sistema e obter acesso privilegiado aos *hosts*. Dependendo da origem do ataque (ataque externo ou ataque interno), são divididos em duas categorias:

R2L: são ataques sem autorização, onde um invasor de um computador remoto tem a capacidade para enviar pacotes para uma máquina através de uma rede. Na maioria dos ataques R2L, a intrusão no sistema é feita através da Internet. Exemplos típicos de R2L são os ataques que incluem descobertas de senhas através de *wordlist* (arquivo contendo várias combinações de letras, números e caracteres especiais que são testados aleatoriamente) em *brute force (*força bruta*)*.

U2R: são ataques onde um invasor tem uma conta em um sistema de computador e é capaz de usar abusivamente seus privilégios, explorando uma vulnerabilidade nos mecanismos eletrônicos, um *bug* no sistema operacional ou em um programa que está instalado no sistema. Ao contrário dos ataques R2L, onde o *hacker* invade o sistema de um meio externo, no U2R, o usuário/invasor já está no sistema local e normalmente se torna um usuário com maiores privilégios.

Vírus: são programas que se reproduzem rapidamente, anexando-os a outros programas para infectá-los. Eles podem causar danos consideráveis (por exemplo, apagar arquivos no disco rígido), ou talvez, apenas alguns truques inofensivos mais irritantes, exibindo algumas mensagens na tela do computador. Os vírus geralmente necessitam de interação humana para replicação e difusão para outros computadores, como por exemplo, abrir arquivos de um *pendrive* ou anexos de um e-mail.

Worms: são programas de replicação própria que se espalham agressivamente através de uma rede, aproveitando o envio automático de pacotes e recebem informações ou recursos encontrados nos computadores.

Cavalos de Tróia: são definidos como programas maliciosos de quebra de segurança que estão disfarçados como algo benigno. Por exemplo, o usuário pode baixar um arquivo imaginando se tratar de um jogo, mas quando o programa é executado, ele pode apagar todos os arquivos do computador.

2.2 Sistemas disponíveis para segurança do usuário

Sistemas de detecção de intrusão, em geral, se baseiam em:

• Detecção por assinatura: as atividades do sistema são analisadas à procura de eventos correspondentes aos padrões pré-definidos. A sua desvantagem é que identifica apenas ataques conhecidos, já definidos na relação de assinaturas que o sistema possui.
• Detecção por anomalia: age em ações diferentes das atividades normais do sistema. Gera um perfil que representa o comportamento habitual do usuário, monitorando o que está fora do normal. Sua desvantagem é a incidência de alarmes falsos devido ao comportamento imprevisível dos usuários ou do próprio sistema.
• Detecção realizada por captura de pacotes: faz análise dos cabeçalhos e a carga útil de pacotes, comparando-os com padrões ou assinaturas conhecidas.
• Sistema de Prevenção de Intrusão (*Intrusion Prevention System* - IPS): tem objetivo de prevenir e diminuir a quantidade de alarmes falsos dos ataques sofridos.

Alguns sistemas de detecção de intrusão conhecidos são:

• **Snort[5]:** sistema de detecção de invasão de rede de código aberto capaz de analisar o tráfego em tempo real e o registro dos seus pacotes. É composto

[5] https://www.snort.org/

por dois elementos principais: um mecanismo de detecção que utiliza a arquitetura de *plugin* modular conhecido como “Mecanismo do Snort” e uma linguagem de regras flexíveis.

• **Ossec[6]:** sistema hospedeiro de detecção de intrusão (*Host Intrusion Detection System* – HIDS) escalável e multiplataforma. Possui um poderoso mecanismo de correlação e análise, integrando análise de *log*, verificação de integridade de arquivos, monitoramento de registro do Windows, aplicação de políticas centralizadas, detecção de *rootkit* (tipo de trojan), alertas em tempo real e resposta ativa. Ele é executado na maioria dos sistemas operacionais e pode trabalhar em conjunto com o Snort, pois avalia os *logs* gerados por ele, classificando-os de acordo com os alertas e assinaturas geradas pelo administrador.

• **TripWire[7]:** sistema HIDS que permite detectar alterações de arquivos em sistemas Linux.

• **KALI LINUX[8]:** utilizado para realizar auditorias de computadores, em geral, efetuando testes de penetração mais avançadas.

2.3 Problemas e desafios em IDS

Embora existam muitas ferramentas de detecção de invasão, ainda há um vasto trabalho a ser feito em busca de mais eficiência. Há um grande número de problemas e desafios em sistema de detecção de invasão que precisa de atenção.

Segundo Nakamura e Geus (2007), entre as questões que necessitam de melhor abordagem pelas comunidades de pesquisas para melhorar os IDS, podem-se destacar:

• A deficiência ou conjunto de dados incompletos de alguns IDS é um problema e faz com que as informações geradas por eles não sejam consistentes. Conjunto de dados pode ser definido como uma coleção de todos os dados ou informações coletadas durante a pesquisa analisada. Uma vez que no IDS, os conjuntos de dados desempenham papel importante na precisão dos resultados.

[6] https://www.ossec.net/about.html
[7] https://www.tripwire.com/
[8] https://www.kali.org/about-us/

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

• O algoritmo para detecção utilizado no IDS é a parte principal para a segurança. Ele deve ser extremamente competente e precisa ser muito rápido com as informações geradas. A política da detecção pode ser por anomalia ou até mesmo por uso incorreto do sistema.

• A dependência de plataforma é um problema a parte. No mundo tecnológico atual, diferentes IDS estão disponíveis, alguns gratuitos e outros comerciais mas, independentemente da forma como ele é distribuído, é necessária uma plataforma para a sua execução e alguns só podem ser executados em uma plataforma específica.

• Alguns IDS possuem o *design* fraco (interface do sistema com cores não convidativas, botões mal definidos e usabilidade complexa). Todos são muito compactos e se o usuário quiser mudar alguma configuração do IDS, é preciso parar a detecção de intrusão, fazer as mudanças necessárias e depois inicia-lo. Esta alteração de configuração na ferramenta oferece riscos, já que, se no momento de paralização ocorrer alguma intrusão, o administrador da rede não saberá que está sendo atacado.

3 A importância da segurança

A importância de se proteger de ataques mal intencionados que resultam em roubo de dados confidenciais, negação de serviços, espionagem e modificação de sites aumenta a responsabilidade individual e coletiva, implantando políticas de segurança e treinamentos para a prevenção de incidentes indesejados.

Violações de segurança de computador ou rede são comuns, e ocorrem em todo o mundo todos os dias. Alguns são considerados menores, com pouca perda de dados ou recursos monetários, mas muitos deles são considerados importantes, ou mesmo catastróficos.

Os *Hackers* estão constantemente à procura de vulnerabilidades para explorar. Quando as redes não são seguras, as informações sobre organizações e indivíduos, e até mesmo o governo, correm o risco de serem invadidas e expostas.

De acordo com SANS Institute (2002), a segurança das redes está relacionada à prevenção física e de software, protegendo a infraestrutura de rede do acesso sem permissão, uso indevido, *bugs*, alteração, dano ou publicação indevida, preservando informações importantes com as características básicas da segurança

da informação como confidencialidade, disponibilidade e integridade de uma plataforma segura.

A segurança é um assunto primordial e muito importante para as redes domésticas, bem como no mundo dos negócios. Muitos hotéis, aeroportos, *shoppings* e restaurantes possuem conexões de alta velocidade de Internet sem fio disponíveis para seus clientes e que poderiam ser explorados facilmente se não estiverem protegidas corretamente.

Inúmeros ataques à segurança podem acontecer em uma organização moderna onde a informação transita de forma rápida e tem valor incalculável. Facilmente são encontradas ações de agentes externos e internos que, de alguma forma, tentam capturar informações que não deveriam ter acesso.

A utilização inadequada da tecnologia da informação, seja intencional ou mesmo por despreparo, tem obrigado as empresas a buscarem mecanismos de proteção a fim de se resguardarem de qualquer inconveniente ou prejuízo em relação à perda de informações sigilosas.

A proteção das informações de um sistema, seja ele de uma empresa ou mesmo particular, consiste basicamente na segurança que existe na sua captura, armazenamento e posterior acesso.

Esta proteção visa garantir a integridade, autenticidade, disponibilidade, confidencialidade e confiabilidade da informação, formando assim os pilares de sustentação da proteção de um sistema de segurança.

Os mecanismos de proteção salvaguardam os mais variados tipos de ameaças, mas são insuficientes se na organização não houver uma política de segurança vinculada a recursos tecnológicos, *software* e *hardware* adequados e uma eficiente medida educativa e de conscientização dos colaboradores.

É importante estabelecer o controle de acesso aos dados e informações, implantando sistemas com senhas que limitem os níveis de acessos e permitam o contato com as informações que correspondam a área específica de cada usuário. Neste sentido, destaca-se também a importância de se realizar cópias de segurança (*backups*) armazenando-as em meios independentes, como *pen-drives* e unidades de discos externos, sendo uma medida preventiva de baixo custo e que minimiza o impacto negativo para a organização.

Além desses esforços, é indispensável à utilização de antivírus e *firewalls* que têm a função de proteger os arquivos internos de ameaças externas.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

Ao assumir uma identidade virtual, operando por meio de *e-mails* e *sites*, a organização precisa entender os riscos a que se expõe e criar formas de se proteger contra possíveis ataques.

Dentre os tipos de ameaças volúveis e de difícil monitoramento, que roubam informações e são capazes de espionar os locais que os usuários costumam navegar, segundo Paiva (2007), os que mais se destacam são os vírus e *worms*. Eles podem atuar por meio de:

Spywares: código espião que captura informações importantes sobre costumes de navegação do usuário e repassa tais dados para pessoas ou organizações externas, sem a autorização ou permissão do usuário.

Spam: são *e-mails* em forma de propaganda, podendo conter vírus. Recomenda-se a sua exclusão imediata por ter origem desconhecida.

Essas tentativas são caracterizadas como crime (Lei nº 12.737, de 30 de novembro de 2012) e tratam-se de ameaças crescentes à sociedade, provocadas por indivíduos que tiram vantagem generalizada da vulnerabilidade da Internet e das Intranets.

É indispensável que as organizações tenham atitudes proativas e preventivas, desenvolvendo uma política de segurança na área de sistemas, livrando-se de problemas, prejuízos materiais, financeiros e até mesmo sociais, utilizando e explorando recursos e ferramentas como criptografia, antivírus, *anti-spywares*, *anti-spam* entre outros. Muitas destas ferramentas são disponibilizadas para uso livre na Internet.

Assim, a escolha dos dispositivos corretos para segurança da informação é fundamental para o sucesso e eficácia no trato da questão, proporcionando proteção e tranquilidade no manuseio das informações.

4 Testes de exploração da vulnerabilidade em um ambiente controlado

A fim de demonstrar as vulnerabilidades presentes em redes sem fio mal configuradas, foi criado um ambiente controlado onde algumas ferramentas de intrusão encontradas em distribuições Linux foram testadas. Tais ferramentas são de fácil acesso pelas pessoas com acesso à Internet.

Foram realizados testes de intrusão em um cenário de rede sem fio 802.11 (tecnologia de transmissão e codificação para comunicação por radiofrequência),

abordando alguns métodos de uso e integração de ferramentas disponíveis na distribuição KALI LINUX.

4.1 Descrição do cenário de testes

Os testes foram realizados utilizando-se:

- 1 AP (*Access Point*) *Wireless-g Linksys* Wap54g.

- 1 dispositivo móvel com sistema operacional *Windows Seven*, configuração padrão de fábrica, com 4 GB de memória principal, *Hard Disk* de 500 GB e 2 núcleos de processador i3-7100, conectado a rede sem fio para ser usado para gerar tráfego como estação no AP. Este dispositivo será chamado neste trabalho de dispositivo móvel estação (DME).

- 1 dispositivo móvel com a distribuição KALI LINUX, com ferramentas de intrusão nativas, com 8 GB de memória principal, *Hard Disk* de 1TB e 3 núcleos de processador i5-M480, usado como atacante para realizar os testes de intrusão. Este dispositivo será chamado neste trabalho de dispositivo móvel intrusão (DMI).

4.2 Utilizando o KALI LINUX para o *Pentest*

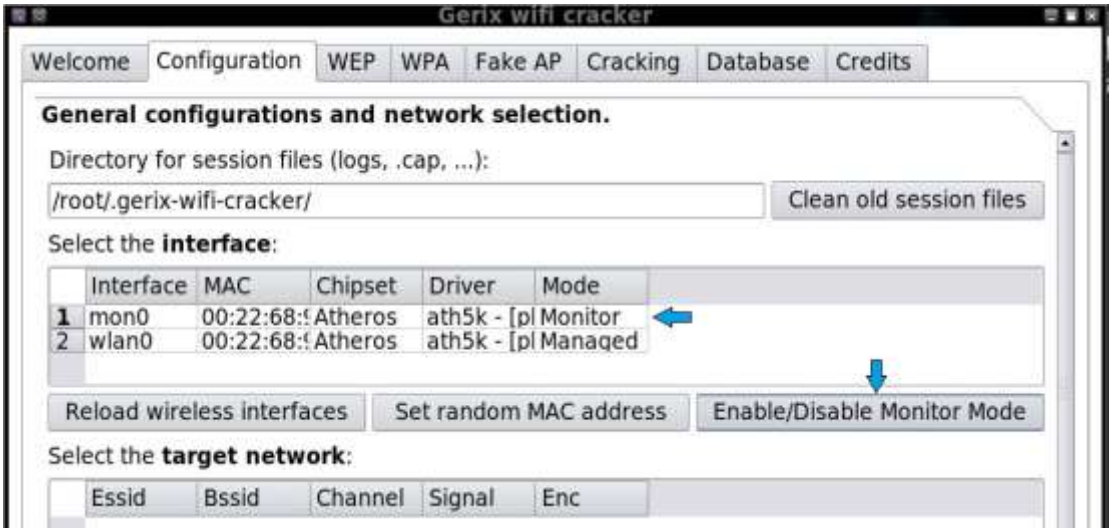
O KALI é uma distribuição Linux baseada no Debian, destinado a testes avançados de penetração e auditoria de segurança (KALI.ORG, 2016). O KALI contém várias ferramentas que são voltadas para tarefas de segurança da informação, tais como *pentest*, pesquisa de segurança, computação forense e engenharia reversa. Ele é desenvolvido, financiado e mantido pela *Offensive Security*, uma empresa líder de treinamento de segurança da informação (OFFENSIVE-SECURITY.COM, 2016).

A fim de obter informações específicas sobre o local de rede sem fio, foi utilizado um *sniffer* de pacotes (trata-se de *software* para captura de informações em uma rede), localizado nas ferramentas do KALI LINUX, chamado Gerix-Wifi-Cracker. Ele é um *sniffer* de intrusão que pode obter várias informações sobre a rede sem fio, incluindo SSID, endereço MAC, canal, protocolo de criptografia, potência do sinal e, através de utilização de uma *wordlist* pode-se conseguir a chave criptografada dessa rede.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

Utilizando-se o dispositivo DMI, com a ferramenta Gerix-Wifi-Cracker aberta na aba *Configuration,* o primeiro passo é verificar qual será a Interface de rede a ser utilizada e ativar o modo monitor, conforme exibido na Figura 3.

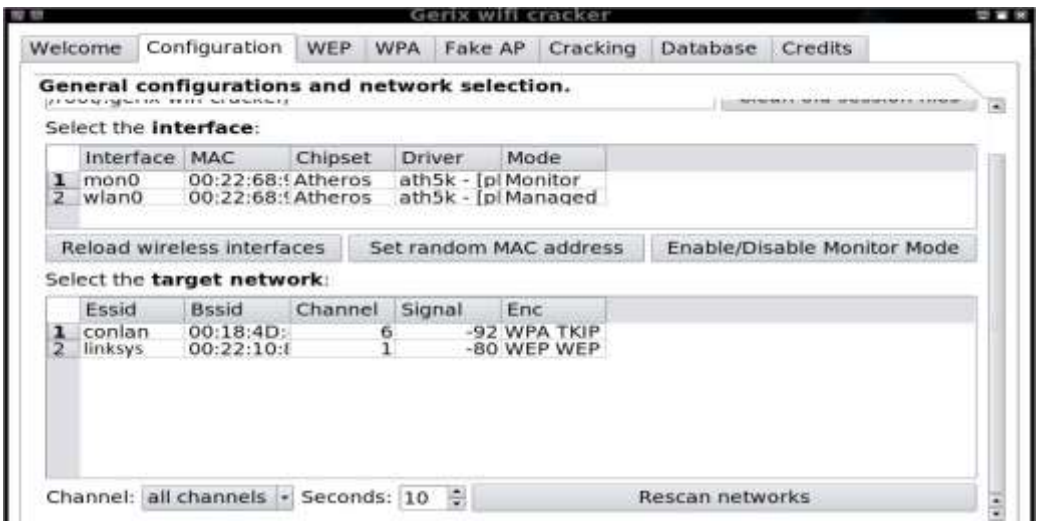
Figura 3 – Tela de configuração do Gerix-Wifi-Cracker.



Fonte: elaborado pelos autores.

Na Figura 4, após ter selecionado a interface mon0 e clicado em *Rescan networks*, pode-se observar as informações retornadas, incluindo o nome da rede (ESSID), endereço MAC (BSSID), canal (CHANNEL), potência de sinal (SIGNAL) e protocolo de criptografia (ENC).

Figura 4 – Seleção da interface de rede do Gerix-Wifi-Cracker.

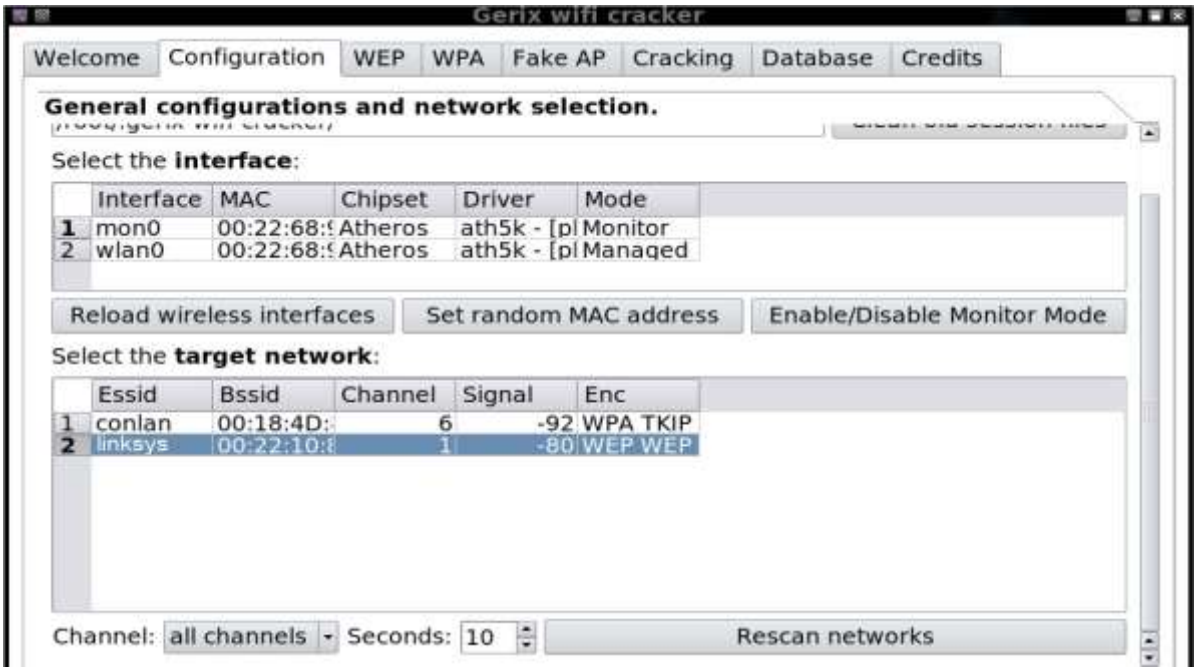


Fonte: elaborado pelos autores.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

Após o processo de escaneamento das redes *wifi* disponíveis, na Figura 5 é exibida a seleção da rede para o *pentest*.

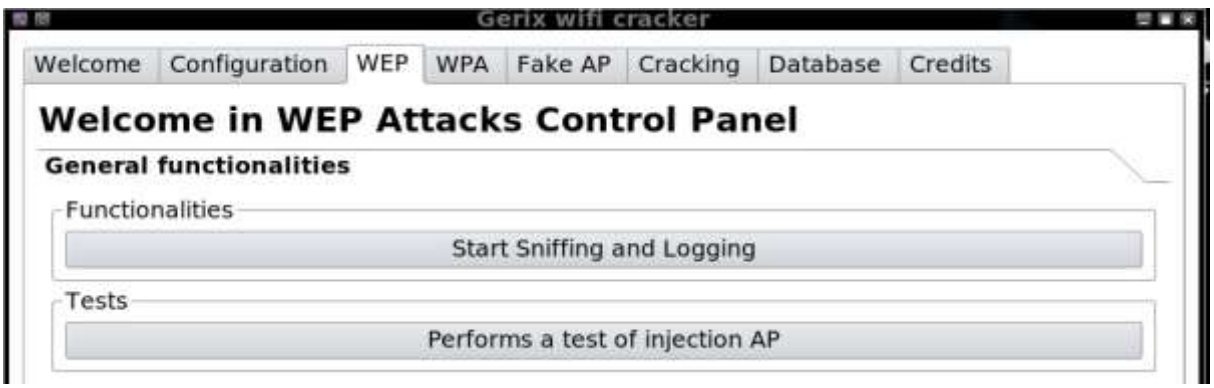
Figura 5 – Seleção da rede disponível para o *pentest*.



Fonte: elaborado pelos autores.

Depois que selecionar a rede sem fio de nome (Essid) “linksys” e de criptografia (Enc) “WEP”, o próximo passo foi percorrer até aba/guia WEP, como pode ser observado na Figura 6. Nesta aba/guia, no menu *General functionalities,* há duas funções importantes para o *pentest*, o *Start Sniffing and Logging* (verifica os dispositivos conectados ao AP) e o *Performs a test of Injection AP* (executa um teste de injeção no AP).

Figura 6 – Tela da aba WEP.

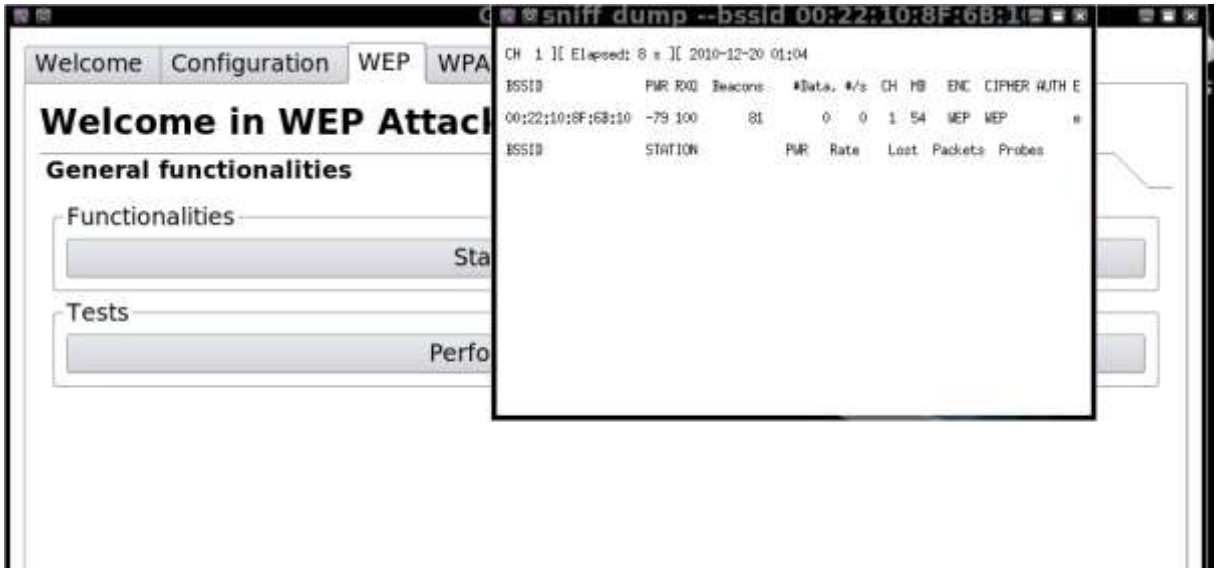


Fonte: elaborado pelos autores.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

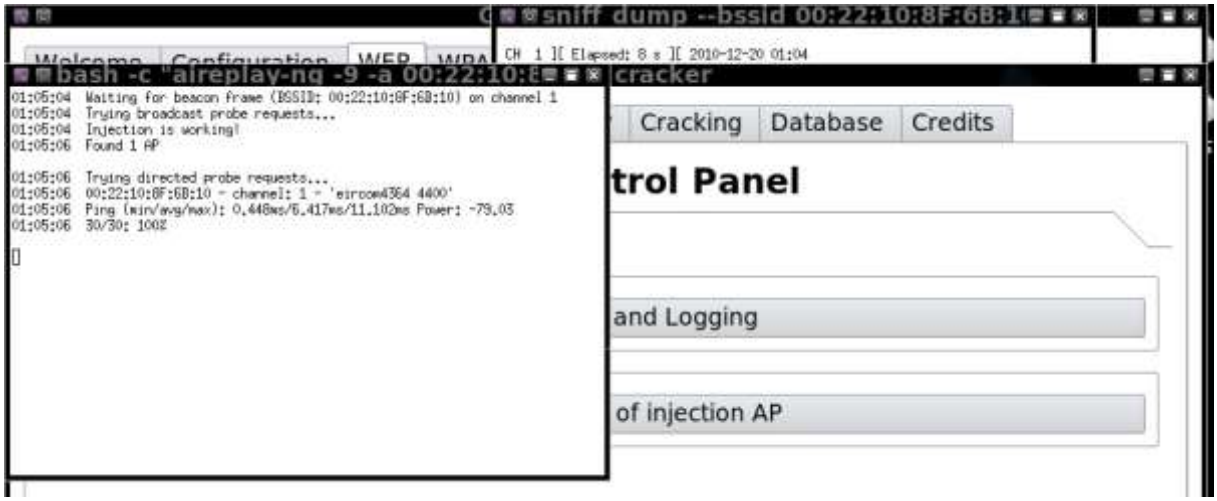
Na Figura 7 verifica-se que, após escolher a opção *Start Sniffing and Logging* é gerado uma pequena tela, onde são exibidos os dispositivos conectados a rede sem fio. Em seguida foi ativada a função *Performs a test of Injection AP* na tentativa de injetar pacotes no *Access Point* para derrubar os dispositivos conectados ao AP. A Figura 8 ilustra esta etapa.

Figura 7 – Tela gerada pelo *Start Sniffing and Logging*.



Fonte: elaborado pelos autores.

Figura 8 – Tela gerada pelo *Performs a test of Injection*.



Fonte: elaborado pelos autores.

Como o objetivo neste teste foi derrubar o dispositivo DME e ao mesmo tempo se passar por um falso AP, na aba/guia WEP (conforme Figura 9) clicou-se no menu *WEP Attacks (no-client)* e, em seguida, na opção *Start false access point*

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

authentication on victim. Isto fez com que fosse criado um ponto de acesso falso a vítima DME, para que a mesma possa fazer uma conexão com a autenticação (conforme Figura 10).

Figura 9 – Tela de funções do menu *WEP Attacks (no-client)*.

Fonte: elaborado pelos autores.

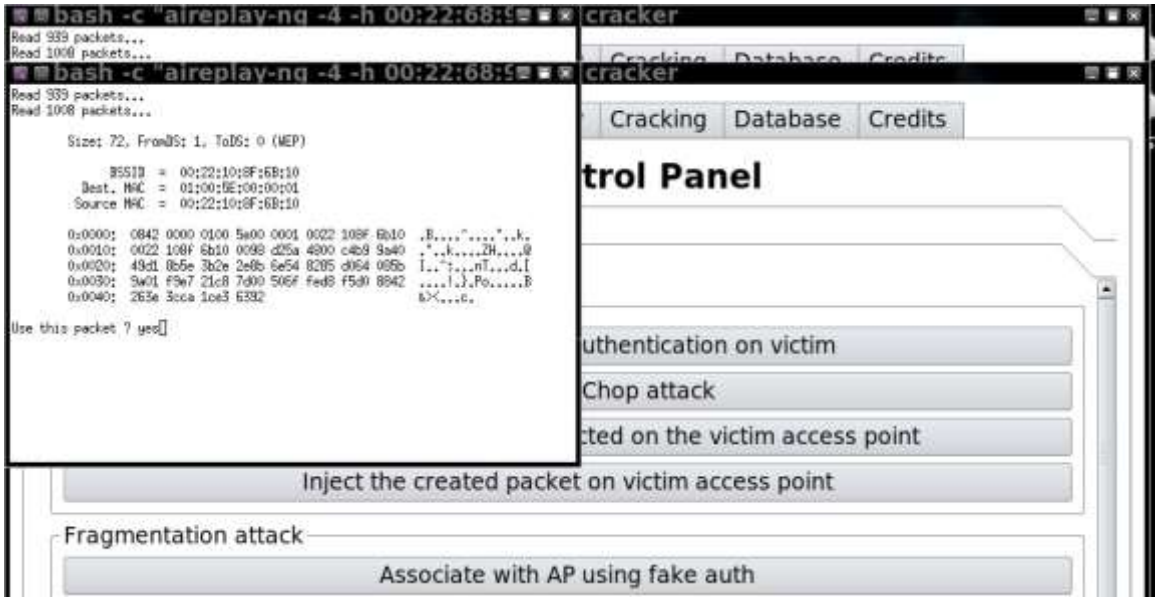
Figura 10 – Tela gerada pelo *Start false access point authentication on victim*.

Fonte: elaborado pelos autores.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

No momento que o dispositivo DME estava tentando autenticar no AP falso, iniciou-se a função *Start the ChopChop Attack*. Após a conclusão da leitura dos dados foi gerada tela para confirmação, exibida na Figura 11.

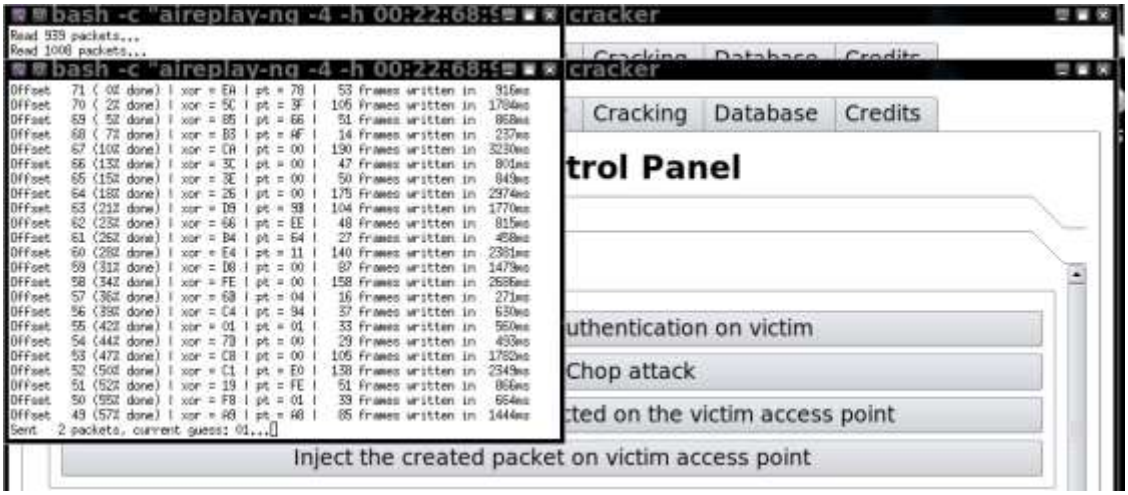
Figura 11 – Tela gerada após concluir a função *Start the ChopChop Attack.*



Fonte: elaborado pelos autores.

Depois da confirmação *"yes",* na Figura 12 pode-se acompanhar as informações sendo geradas pelo procedimento da função *Start the ChopChop Attack*.

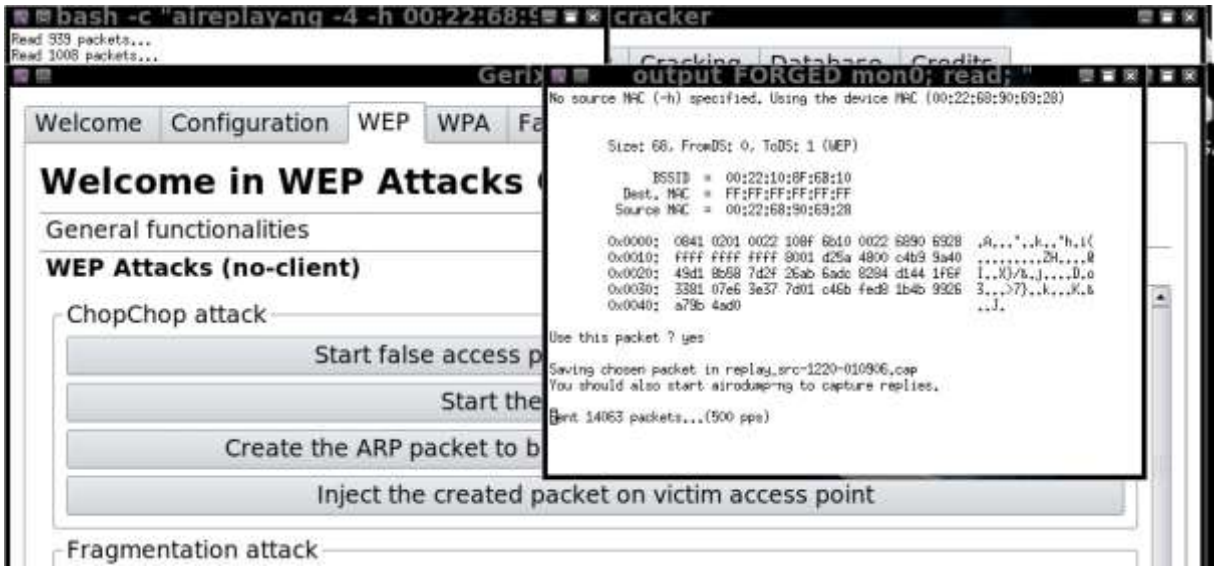
Figura 12 – Tela de informações sendo geradas após confirmação.



Fonte: elaborado pelos autores.

A Figura 13 exibe a injeção dos pacotes de Protocolo de Resolução de Endereços (*Address Resolution Protocol* – ARP) no dispositivo DME, realizada após se clicar em *Create the ARP Packet to be injected*. Após a confirmação *"yes",* foi possível verificar os detalhes da quantidade de pacotes injetados.

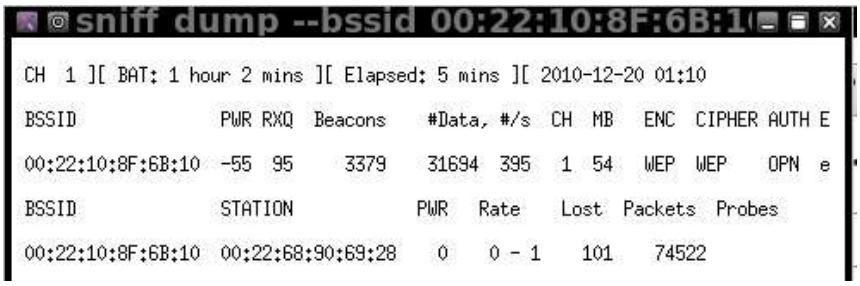
Figura 13 – Injetando pacotes ARP.



Fonte: elaborado pelos autores.

A tela gerada pela inicialização do *Sniffing and Logging* permaneceu aberta para consultas e análise dos dados percorridos. Na Figura 14 observa-se o campo #Data, que precisa exibir um valor acima de 5000. São os pacotes injetados para a descriptografia da chave, quanto maior esse valor, as chances de obtermos a senha de autenticação do AP aumentam.

Figura 14 – Tela de dados gerada pelo *Sniffing and Logging*.

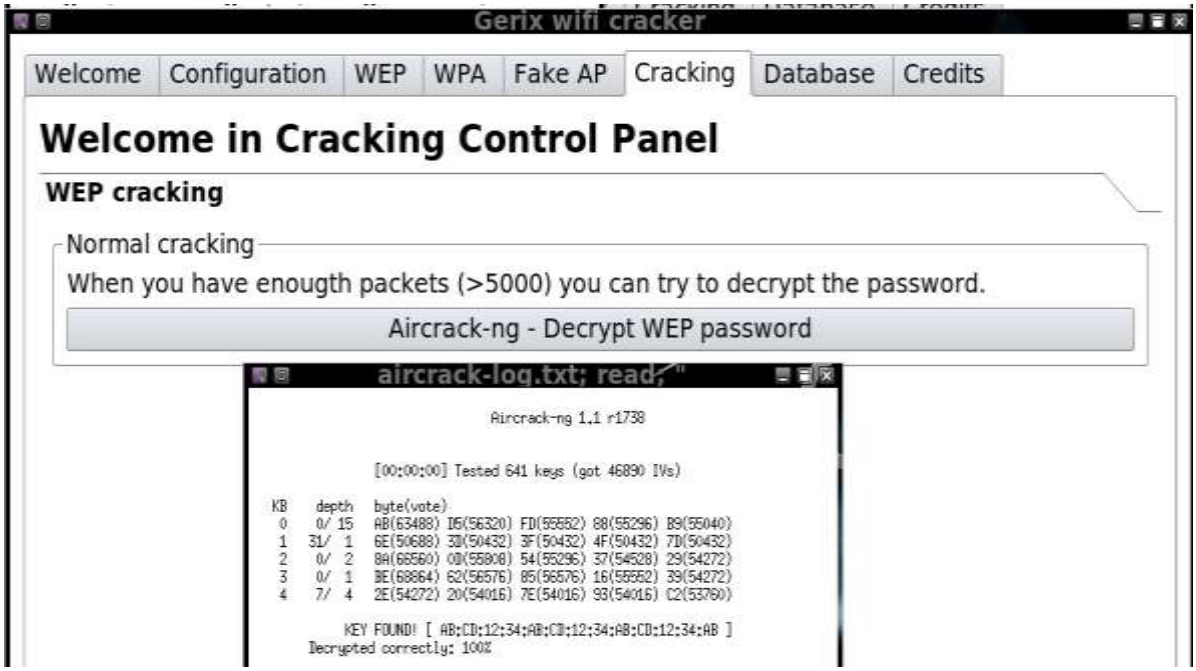


Fonte: elaborado pelos autores.

Na aba/guia *Cracking* utilizou-se o menu *WEP cracking* e o submenu *Normal cracking* para ativar a função *Aircrack-ng - Decrypt WEP password*. Isto fez com que

fosse possível obter a chave/senha de autenticação do AP em alguns segundos, como exibido na Figura 15.

Figura 15 – Tela gerada pelo *Aircrack-ng - Decrypt WEP password*.



Fonte: elaborado pelos autores.

4.3 Formas de garantia da segurança em redes de computadores

A fim de minimizar os danos que podem ser causados por usuários mal intencionados, é importante estar certo de que toda a política de segurança é executada por mecanismos íntegros o suficiente. Existem muitas metodologias organizadas e estratégias de avaliação de riscos para garantir a qualidade das políticas de segurança e garantir que elas sejam completamente aplicadas.

Nesta seção estão elencadas algumas prioridades e recomendações a serem observadas quando o assunto é segurança em redes de computadores.

- Os direitos de administrador devem ser concedidos com cautela. Os usuários que têm direitos de administrador podem potencialmente criar eventos seriamente prejudiciais. Até mesmo involuntariamente, fazer alterações que diminuem o nível de segurança da rede, ou ser induzidos a executar um *malware* que seria hospedado com privilégios de administrador do usuário.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

• É muito importante proteger seus detalhes de autenticação, caso seu nome de usuário e senha forem roubados, isto poderá permitir que terceiros não autorizados efetuem *login* e realizem ações nocivas, intencionalmente ou acidentalmente. Para uma melhor segurança, certifique-se de que os usuários tenham um nível de privilégio apropriado para as tarefas que realizam e minimize o número de usuários com privilégios de administrador.

• Deve-se determinar quem tem realmente a necessidade de execução de *downloads* e *uploads* nas aplicações de um *website*. A filtragem da *web* é extremamente necessária para restringir o acesso das pessoas e garantir que os poucos selecionados são orientados em como baixar arquivos com segurança. Os arquivos muitas vezes podem ser baixados de vários locais na Internet, mas nem todos os locais são igualmente seguros. Certifique-se de que os usuários só podem fazer o *download* de sites confiáveis.

• Realizar constantemente auditorias de ações de rede. Os usuários só devem ter acesso a arquivos e pastas que necessitem como parte de seu trabalho diário. O administrador da rede deve estar ciente de que *malwares* podem se espalhar através da rede. Isso geralmente é devido a pouca, ou nenhuma, segurança em compartilhamentos de arquivos e pastas. Deve-se remover o acesso a ações desnecessárias e proteger seus conteúdos para limitar a propagação de programas maliciosos.

• As redes normalmente usam intervalos de IP padrão, como 10.1.x.x ou 192.168.x.x. Essa abordagem padrão significa que as máquinas configuradas para procurar esse intervalo podem se conectar acidentalmente a uma rede fora do seu controle. Alterar o intervalo de IP padrão para que os computadores tenham menos probabilidade de encontrar um intervalo semelhante é mais seguro. Deve-se também considerar a inclusão de regras de *firewall*, que permite que somente usuários aprovados se conectem.

• Periodicamente, fazer auditorias nas portas abertas da rede e bloquear todas não utilizadas. Deixá-las abertas por longos períodos de tempo sem inspecioná-las, aumenta as chances de intrusão, permitindo que *trojans* e *worms* as utilizem para se comunicar com terceiros não autorizados.

• Usar uma rede segmentada para proteger suas informações. Há uma série de vantagens para segmentar a rede.

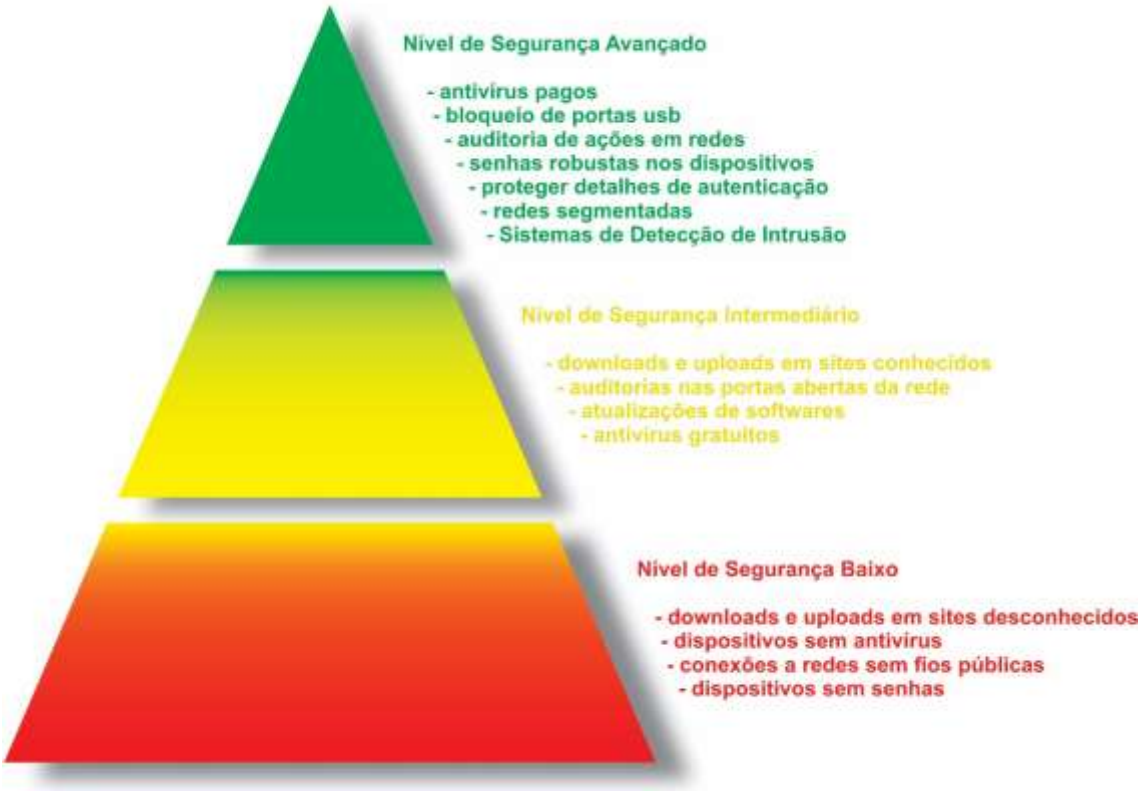
Revista EduFatec: educação, tecnologia e gestão
V.1 N.2 julho-dezembro/2018

• Para garantir que uma nova versão ou atualizações de *softwares* não cause problemas é importante testá-la em um sistema virtual e verificar seus efeitos antes de implantar a rede real.

• Muitos dispositivos, quando conectados a uma porta USB (*Universal Serial Bus*), podem ser detectados automaticamente e montados como uma unidade. As portas USB também podem permitir que dispositivos conectados, executem automaticamente o *software* armazenado. Os usuários não devem se esquecer de que mesmo os dispositivos mais seguros e confiáveis podem potencialmente introduzir *malware* no computador e na rede. Para evitar este tipo de ação é seguro desativar todas as portas e apenas ativá-las com a autorização do administrador da rede.

A Figura 16 apresenta diferentes níveis de segurança que o usuário pode ter para garantir uma melhor proteção de acordo com as tecnologias e ferramentas utilizadas.

Figura 16 – Níveis de Segurança das tecnologias e ferramentas utilizadas



Fonte: elaborado pelos autores

À medida em que mais ferramentas de proteção são aplicadas pelo usuário, maior é a segurança que se consegue e, quanto mais atenção se emprega a estas técnicas, mais segura fica a utilização de uma rede de computadores.

Considerações finais

Com o aumento dos crimes virtuais e a evolução da internet, tendo como objetivo prejudicar ou tirar proveito dos usuários, obtendo informações sigilosas, percebe-se a necessidade da implantação de sistemas de segurança mais robustos e com segurança reforçada.

O trabalho desenvolvido permitiu testar a vulnerabilidade em um exemplo prático da utilização de sistema de intrusão de redes, em que foram utilizadas, em um ambiente controlado, ferramentas para intrusão de computadores em uma pequena rede.

Foram analisadas ferramentas de segurança disponíveis atualmente e destacados pontos importantes de cada uma, como forma de auxílio aos administradores de redes na escolha daquela que melhor lhes atenderá, baseado no tipo de situação vivenciada.

Trabalhos futuros podem ser desenvolvidos com técnicas de mineração de dados através dos sistemas de detecção de intrusão por anomalias abordando as redes neurais. Outros trabalhos futuros podem ser abordados com testes de intrusão em Sistema Gerenciador de Banco de Dados, revelando algumas vulnerabilidades e considerando alguns IDSs para a proteção dos dados desses SGBD.

Agradecimentos

Agradecemos a Deus, por ter nos dado saúde e sabedoria para superar as dificuldades.

A toda FATEC Franca, seu corpo docente, aos orientadores e aos colegas com quem convivemos nesses espaços ao longo desses anos.

As nossas famílias, pelo amor, apoio e compreensão nos momentos de nossas ausências dedicados ao estudo superior, com muito carinho e apoio, não mediram esforços para que nós chegássemos até esta etapa de nossas vidas.

Referências

ASYNCHRONOUS Transfer Mode (ATM). Disponível em: <https://www.techopedia.com/definition/5339/asynchronous-transfer-mode-atm>. Acesso em: 10 ago. 2018.

ERNST & YOUNG. **Na mira dos ataques cibernéticos.** Disponível em <https://www.ey.com/Publication/vwLUAssets/LR_Giss_Portugues_EY_Brasil/%24FILE/LR_Giss_Portugues.pdf>. Acesso em 30 de setembro 2018.

ESTATÍSTICAS dos Incidentes Reportados ao CERT.br: **Total de Incidentes Reportados ao CERT.br por Ano. 2017**. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 13 abr. 2018.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução a Segurança de Computadores.** Porto Alegre: Bookman, 2013.

HAHN, J.; GUILLEN D. P.; ANDERSON, T. **Process Control Systems in the Chemical Industry: Safety vs. Security.** In: Annual CCPS International Conference, 20., 2005, EUA. Disponível em <https://inldigitallibrary.inl.gov/sites/sti/sti/3169874.pdf>. Acesso em 10 junho 2018.

HERTZOG, Raphaël; O'GORMAN, Jim; AHARONI, Mati. **KALI LINUX Revealed.** EUA, 2017.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Corporativos.** São Paulo: Novatec, 2007.

NETWORK Security Resources. Disponível em: <https://www.sans.org/network-security/>. Acesso em: 15 set. 2018.

PAIVA, Simone. **A importância da Proteção dos Sistemas de Informação**. 2007. Disponível em <https://www.classecontabil.com.br/a-importancia-da-protecao-dos-sistemas-de-informacao-2>. Acesso em 15 agosto 2018.

PENETRATION Testing Training with KALI LINUX: **Online Security Training. 2016**. Disponível em: <https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/>. Acesso em: 22 set. 2018.

SANTOS, Victor. **Sistemas de Detecção de Intrusões (IDS – Intrusion Detection Systems) usando unicamente softwares Open Source**, JUNHO 21, 2010. Disponível em <https://seginfo.com.br/2010/06/21/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-softwares-open-source/>. Acesso em 25 agosto 2018.

SCHETINA, Erik; CARLSON, Jacob. **Sites seguros: Aprenda a desenvolver e construir.** Rio de Janeiro: Campus, 2002.

SILVA, Edelberto Franco; JULIO, Eduardo Pagani. **Sistema de Detecção de Intrusão - Artigo Revista Infra Magazine 1**. Disponível em <https://www.devmedia.com.br/sistema-de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819>. Acesso em 28 julho 2018.

SIMONI, Emílio. **Relatório da Segurança Digital no Brasil**: Segundo trimestre - 2018. 4ª. 2018. Disponível em: <https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf>. Acesso em: 30 jul. 2018.

STALLINGS, William. **Criptografia e Segurança de Redes.** São Paulo: Pearson Prentice Hall, 2008.

TACIO, Paulo. **TÉCNICAS HACKER**: O QUE É DOS E DDOS. 2011. Disponível em: <http://www.mundodoshackers.com.br/tecnicas-hacker-o-que-e-dos-e-ddos>. Acesso em: 16 set. 2018.

TANENBAUM, Andrew Stuart. **Redes de Computadores.** Rio de Janeiro: Campus, 1994.