UNIVERSIDADE FUMEC
FACULDADE DE CIÊNCIAS EMPRESARIAIS MESTRADO PROFISSIONAL
EM SISTEMAS DE INFORMAÇÃO E GESTÃO DO CONHECIMENTO

DAVIS ANDERSON FIGUEIREDO

ANÁLISE DA SEGURANÇA DE REDES WI-FI ATRAVÉS DE TESTE DE PENETRAÇÃO EM INSTITUIÇÕES DE ENSINO SUPERIOR DE BELO HORIZONTE

Belo Horizonte – MG

2015

DAVIS ANDERSON FIGUEIREDO

ANÁLISE DA SEGURANÇA DE REDES WI-FI ATRAVÉS DE TESTE DE PENETRAÇÃO EM INSTITUIÇÕES DE ENSINO SUPERIOR DE BELO HORIZONTE

Projeto de pesquisa apresentado ao Curso de Mestrado Profissional em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC como requisito parcial para obtenção do grau de mestre.

Área de concentração: Gestão de Sistemas de Informação e Conhecimento

Linha de pesquisa: Gestão da Informação e Conhecimento

Orientador: Prof. Dr. Rodrigo Moreno Marques

Co-Orientador: Prof. Dr. Henrique Cordeiro Martins

Belo Horizonte – MG

2015

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AP	*Access Point*
BSS	*Basic Service Set*
DOS	*Denial of Service*
DSSS	*Direct Sequence Spread Spectrum*
ESS	*Extended Service Set*
FCC	*Federal Communications Commission*
FHSS	*Frequency Hopping Spread Spectrun*
IBSS	*Independent Basic Service Set*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
ISM	*Industrial Sientific and Medical*
ISO	*International Organization for Standardization*
ISSAF	*Information System Security Assessment Framework*
LAN	*Local Area Network*
LLC	*Logical Link Control*
MAC	*Media Access Control*
MIMO	*Multiple-Input Multiple-Output*
MITM	*Man In The Middle*
MU-MIMO	*Multi-User MIMO*
OFDM	*Orthogonal Frequency Division Multiplexing*
OSI	*Open Systems Interconnection*
OSSTMM	*Open Source Security Testing Methodology Manual*
RAP	*Rogue Access Point*
SISO	*Single-Input Single-Output*
SOHO	*Small Office Home Office*
SRAP	*SmartPhone Rogue Access Point*
WDS	*Wireless Distribution System*
WLAN	*Wireless Local Area Network*

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Com a evolução tecnológica e a convergência das redes de nova geração, as infraestruturas Wi-Fi tornaram-se onipresentes nos ambientes corporativos. Apesar de trazerem os benefícios da mobilidade, as redes sem fio ainda são algo novo para usuários e administradores e vários riscos, ameaças e vulnerabilidades estão associados ao padrão de redes sem fio IEEE 802.11. O objetivo dessa pesquisa é de analisar as principais vulnerabilidades e ameaças que colocam em risco a segurança da informação em redes Wi-Fi de instituições de ensino superior de Belo Horizonte. Para isso, serão realizados Testes de Penetração para avaliar as fragilidades dessa infraestrutura. Os resultados a serem encontrados serão confrontados com os principais mecanismos de segurança descritos na literatura acadêmica e das normas técnicas que estão voltadas para essa temática.
Palavras-chave: Segurança da Informação, Wi-Fi, Teste de Penetração

ABSTRACT

With the technological evolution and convergence of next generation networks, the Wi-Fi infrastructure has become ubiquitous in enterprise environments. Although it brings the benefits of mobility, wireless networks are still something new for users and administrators and a number of risks, threats and vulnerabilities are associated with the IEEE 802.11 wireless networking standard. The objective of this research is to analyze the main vulnerabilities and threats that jeopardize the security of information in Wi-Fi networks of higher education institutions in Belo Horizonte. For this, Penetration Testing will be conducted to evaluate the fragilities of this infrastructure. The results will be confronted with the main security mechanisms described i the academic literature and technical standards that are focused on this theme.

Keywords: Information Security, Wi-Fi, Penetration Testing.

SUMÁRIO

1. Introdução

Com a evolução tecnológica e a convergência das redes de nova geração, as redes sem fio tornaram-se onipresentes nos ambientes corporativos. Cada vez mais, um número maior de pessoas e de dispositivos computacionais (*smartphone*, *tables*, *notebooks*, relógios, óculos, etc) adotam as redes sem fio (*Wireless*) Wi-Fi, definido pela IEEE (*Institute of Electrical and Electronics Engineers)* como padrão 802.11.

Os novos conceitos de Computação Pervasiva e Internet das Coisas têm como pilares os ambientes de rede sem fio, favorecendo assim a mobilidade e a facilidades no acesso a redes locais e a Internet. Em todo mundo, milhões de pessoas utilizam diariamente as redes sem fio em ambientes públicos e privados para acesso à Web e execução de atividades profissionais, pessoais, compras e entretenimento (RAMACHANDRAN, 2011).

As instituições de ensino, visando atender as necessidades de seus alunos, professores e funcionários, têm disponibilizado redes Wi-Fi para a comunidade acadêmica. Muitas vezes, essas redes apresentam boa velocidade de transmissão digital, grande área de cobertura e conexão com a rede cabeada da instituição.

As redes Wi-Fi, trouxeram uma grande praticidade para vida das pessoas, proporcionando grande liberdade no acesso, baixo custo de implementação, facilidade de instalação e configuração (RAMACHANDRAN, 2011; RUFINO, 2014). Entretanto, novos riscos surgiram com a adoção crescente e maciça dessa nova tecnologia. A frequência de tentativas de violação e ataques a essas redes tem se intensificado nos últimos anos (RAMACHANDRAN, 2011). Administradores sem muito conhecimento ou com desejo impulsivo de aderência rápida a essas novas demandas, deixam de lado as práticas de gestão e segurança das redes Wi-Fi (RAMACHANDRAN, 2011; RUFINO, 2014).

Dentro do contexto apresentado, coloca-se a pergunta que enseja a presente pesquisa.

No âmbito da segurança da informação, quais são as principais vulnerabilidades e ameaças presentes em redes Wi-Fi de instituições de ensino superior de Belo Horizonte?

1.1 Objetivo Geral

Analisar a presença de vulnerabilidades e ameaças que colocam em risco a segurança da informação em redes Wi-Fi de instituições de ensino superior de Belo Horizonte.

1.2 Objetivos Específicos

1- Discutir as vulnerabilidades e ameaças para a segurança da informação que estão presentes na arquitetura Wi-Fi, bem como seus principais mecanismos de segurança, a partir da literatura acadêmica e das normas técnicas que estão voltadas para essa temática.

2- Levantar as vulnerabilidades e ameaças que estão presentes em redes Wi-Fi por meio de teste experimental de invasão em ambientes acadêmicos.

3- Analisar os resultados do teste experimental e confrontá-los com a literatura acadêmica e normas técnicas pesquisadas.

1.3 Justificativa

O crescimento e expansão da área de cobertura das redes Wi-Fi se mostra cada vez mais necessário para o atendimento da demanda por mobilidade e integração de dispositivos moveis. Nesse sentido, umas das grandes preocupações para esse processo de massificação eficiente dos ambientes

Wi-Fi é a garantia da segurança no tráfego dos dados, privacidade dos usuários e disponibilidade da infraestrutura.

Para se alcançar essas garantias, mostra-se necessário um aprofundamento nas discussões acerca das principais ameaças e vulnerabilidades das redes Wi-Fi. Com isso, busca-se evidenciar as medidas de segurança que podem mitigar os riscos que essas redes trazem para seus usuários e para as empresas e instituições que são responsáveis por sua administração.

2. Referencial Teórico

[aqui você deve descrever em alguns parágrafos como está estruturado seu referencial teórico. Diga resumidamente quais os assuntos serão abordados, sequencialmente]

2.1 Segurança da Informação

A informação deve ser tratada como um ativo das empresas e, por ter esse nível de classificação, tem grande valor para as instituições. Seu gerenciamento é vital e muito importante para o sucesso e manutenção de qualquer organização. (ABNT NBR ISO/IEC 27001:2013; GIL, 2008)

Segundo a ABNT (2013), a Segurança da Informação está voltada para a proteção da informação contra vários tipos de ameaças, visando garantir a continuidade do negócio, minimizar riscos e maximizar os investimentos e as oportunidades de negócio.

A estrutura fundamental da segurança da informação está baseada em três pilares básicos:

. Confidencialidade – controles que busquem limitar o acesso a informação à quem se destine.

. Integridade – controles que busquem garantir a completeza das informações e dados, mantendo suas condições quando disponibilizados.

. Disponibilidade – controles que garantam o acesso à informação a qualquer momento que for solicitada. (SÊMOLA, 2003; MANOEL, 2014)

A identificação dos ativos físicos, tecnológicos e processos que estão atrelados ou manipulam as informações e suas classificações quanto aos possíveis riscos é um processo fundamental, haja vista a importância desses ativos para as instituições. A gestão do risco de cada ativo será um norteador para as ações da Segurança da Informação (ABNT, 2008)

A Segurança da Informação no nível corporativo sofreu duas grandes mudanças nas últimas décadas. A primeira trouxe a necessidade de implementação de controlos ao ambiente físico e dos processos institucionais. Nesse contexto, a segurança se preocupava exclusivamente com os arquivos em papel, entrada em locais restritos, arquivos e informações armazenadas nos computadores independentes, ou seja, esse pode ser considerado o período da **segurança do computador**. Já na segunda grande mudança, o surgimento das redes distribuídas e do uso das telecomunicações para comunicação e transmissão de dados entre usuários e computadores, trouxe uma necessidade de proteção mais abrangente. Assim nasce a Segurança de Rede (STALLINGS, 2008).

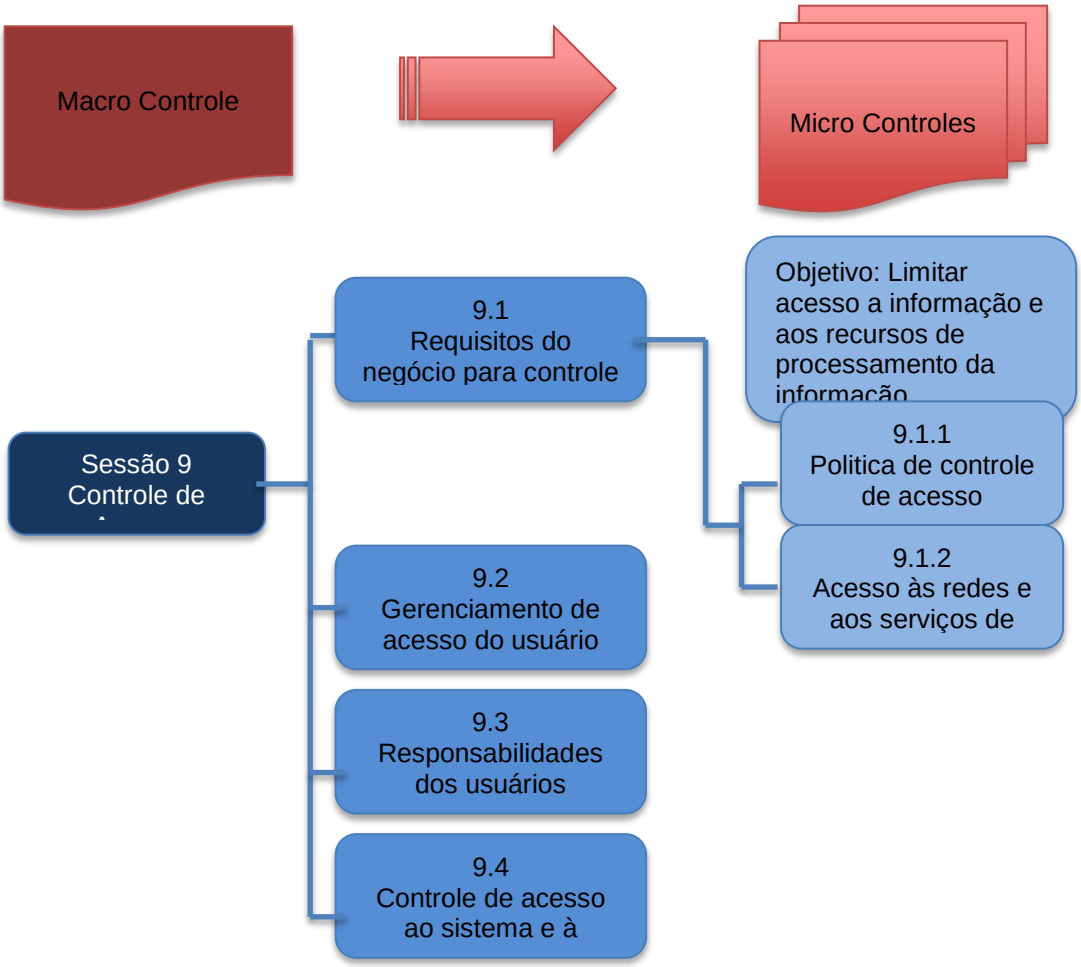
Atualmente, quase em sua totalidade, as instituições públicas e privadas têm seus ambientes de trabalho e sistemas de computadores conectados a redes, para diferentes propósitos e necessidades. Essas redes podem ser internas (redes locais) ou entre instituições parceiras remotas. Além disso, também podem estar ligadas à redes públicas e à Internet.

2.2 Norma ISO/IEC 27002

A norma ISO/IEC 27002 é um código de práticas que traz em sua estrutura um conjunto de controles de segurança bem abrangente que auxiliam na implementação e aplicação de um Sistema de Gestão de segurança da Informação. Essa norma busca um apontamento para as práticas de segurança da informação discutidas e sugeridas por comitês internacionais, mantido pela ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*).

Em sua última versão ISO/IEC 27002:2013 a norma traz uma proposta de 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles. A abordagem dessa norma vai da visão macro, onde estão as sessões de controle propostas, até a visão micro, onde estão os controles específicos a serem implementados. Essa pode ser melhor compreendida na figura 1.

Figura 1: Estrutura de controle da ISO/IEC:27002:2013



Fonte: elaborada pelo autor

A ISO/IEC 27002:2013 tem um caráter generalista, não aborda diretamente as características e necessidades especificas para as redes Wi-Fi. Para atender a esses propósitos específicos, uma nova norma para família ISO/IEC 27000 vem sendo projetada para um maior direcionamento às

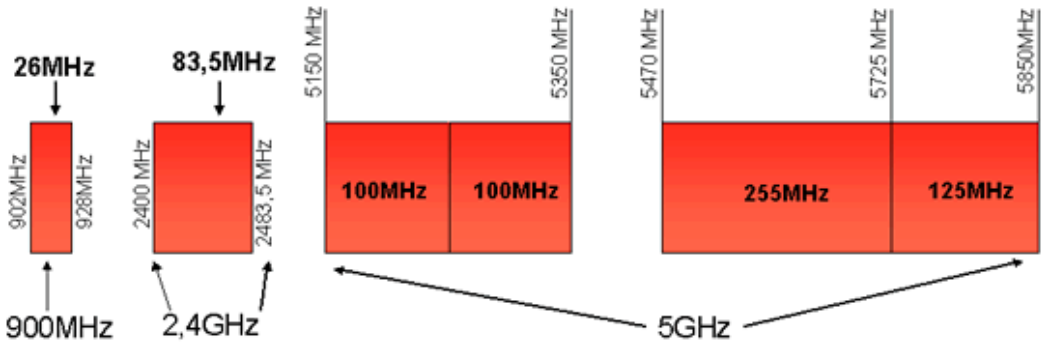
demandas na comunicação de redes sem fio, conhecida como ISO/IEC 27033-6.

2.3 Redes WLAN (*Wireless Local Area Network*)

Em meados dos anos 1980, a *Federal Communications Commission* (FCC), órgão regulador Norte Americano para telecomunicações e radiodifusão, atribuiu parte do espectro de frequência para desenvolvimento livre, sem a necessidade de licenciamento e pagamento para utilização de determinadas faixas de frequência. As faixas de frequências dedicas para *Industrial Sientific and Medical* (ISM) são bandas reservadas internacionalmente para o desenvolvimento industrial, científico e médico. Para isso, foram estabelecidas normas de limitação de potência de transmissão e técnicas de modulação dentro destas faixas.

Este padrão foi internacionalmente difundido e adotado em diversos países, e também no Brasil, com algumas ressalvas. No Brasil a legislação para este tipo de sistema foi inicialmente definida pela ANATEL, através da Norma 02/93, posteriormente pela Norma 012/96 (resolução 209 de Jan/2000) e atualmente pela resolução 506 de Jul/2008 – Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita. As faixas destinadas a WLAN no Brasil podem ser definidas na figura 2.

Figura 2: Faixas de rádio frequência destinada para WLAN no Brasil



Fonte: http://www.teleco.com.br/tutoriais/tutorialwlanx/pagina_3.asp

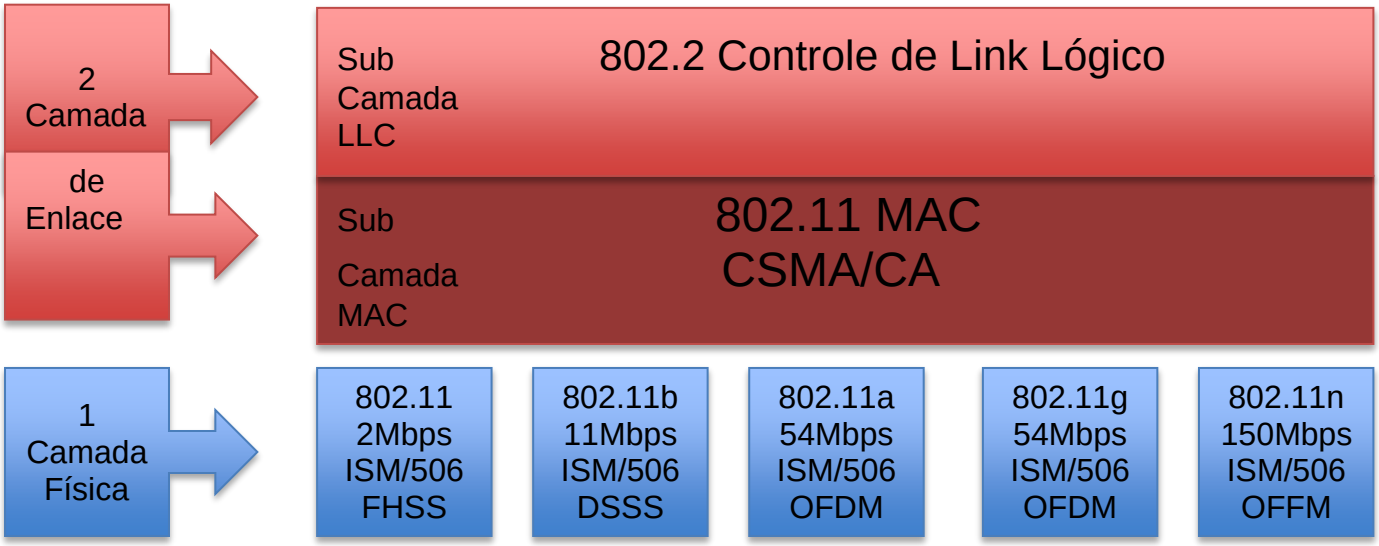
De acordo com GAST (2005), o padrão IEEE 802.11 pode ser referenciado por vários nomes como: Ethernet sem fio, justificando a ligação direta com o padrão de rede com fio IEEE 802.3. O nome Wi-Fi é definido pela organização Wi-Fi Alliance a partir do programa de certificação de interoperabilidade de produtos que utilizam as referências desse padrão. É Também é referênciada como WLAN (*Wireless Local Area Network*).

O IEEE desenvolveu diversos padrões e sub padrões para tecnologia de WLAN, entre eles se destacam os sub padrões 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac, Alguns desses padrões se diferem na frequência de operação, taxa de transmissão, largura de banda, na modularização utilizada para transmissão dos dados e nos recursos de segurança suportados.

2.3.1 Padrões IEEE 802.11 (WLAN`s)

O padrão IEEE 802 trabalha com as determinações da camadas 1 e 2 do modelo de referência ISO (*Open Systems Interconnection*). Ou seja, essa especificação trabalha a Camada Física (1) e Camada Enlace (2). O padrão 802.11 apresentado na figura 3 teve sua aprovação pela IEEE em 1997 e como um membro da família 802, o 802.11 traz definições para camada 1 e também para sub camada MAC (controle de acesso ao meio) na camada 2. Para a função de controle de link lógico LLC da sub camada 2, o 802.11 adota o padrão 802.2 como apresentado na figura: (GAST, 2005)

Figura 3: comparação entre Modelo OSI e padrão 802.11



Fonte: elaborada pelo autor

Na camada física, o 802.11 define uma série de padrões de transmissão e codificação para comunicações sem fio, sendo eles: FHSS (*Frequency Hopping Spread Spectrun*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*). É suas funções são:

. Codificação e decodificação de sinais

. Geração/remoção de parâmetros para sincronização

. Recepção e transmissão de bits

. Especificação do meio de transmissão

Na camada de enlace, o padrão 802 define duas sub camadas, o LLC (Logical Link Control) e o MAC (Media Access Control), para a camada de enlace de dados do modelo OSI. Mas o padrão 802.11 define funções somentes para a sub camada MAC, que tem como função:

. Aspectos de transmissão: reunir dados dentro de um pacote com endereços e campos detecção de erro.

. Aspectos de recepção: abre pacote e executa reconhecimento de endereços e detecção de erros

. Controle de acesso ao meio de transmissão LAN.

Já as funções de promover ligação para camadas superiores e executa controle de fluxo e erro de pacotes da camada LLC são herdadas do padrão 802.2 e incorporados ao 802.11.

Uma síntese cronológica dos padrões 802.11 usuais são apresentados na **tabela 1**

Tabela 1: cronologia dos padrões 802.11

Padrão	Ano	Frequência de Operação **GHz**	Taxa máxima de transmissão **Mbit/s**	Largura de Banda **MHz**	Modularização
802.11	1997	2.4	2	22	DSSS, FHSS
802.11a	1999	5	54	20	OFDM
802.11b	1999	2.4	11	22	DSSS
802.11g	2003	2.4	54	20	OFDM, DSSS
802.11n	2009	2.4 / 5	150	20 -40	OFDM
802.11ac	2013	5- 5.8	866.7	20 – 40 – 80 - 160	OFDM

Fonte: elaborada pelo autor

2.3.1.1 Padrão IEEE 802.11b

A IEEE evoluiu as capacidades do padrão 802.11 original e em 1999 foi crianda a especificação 802.11b. Esse padrão suporta taxa máxima de transmissão de até 11 Mbps, utiliza a mesma frequência de rádio (2,4 GHz) do padrão 802.11 original. Sofre maior interferências de outros dispositivos de mesma frequência como telefones sem fio e forno micro-ondas por em alguns casos operarem em mesmo canal gerando ruídos na comunicação.

2.3.1.2 Padrão IEEE 802.11a

Em paralelo ao desenvolvimento 802.11b, o IEEE criou uma segunda extensão para o padrão 802.11 definido como 802.11a, suporta largura de banda de até 54 Mbps e sinais em um espectro de frequência regulamentado de (5 GHz) . Esta maior frequência em comparação com 802.11b reduz o alcance de redes 802.11a e tem maior dificuldade de penetrar paredes e outros obstáculos. Como as arquiteturas 802.11b e 802.11a utilizam frequências diferentes, as duas tecnologias são incompatíveis. As maiores vantagens em relação ao padrão 802.11b são as maiores taxas de transmissão e menor interferência de outros dispositivos.

2.3.1.3 Padrão IEEE 802.11g

Com o intuito de buscas o melhor dos padrões 802.11 a e 802.11b, no ano de 2003, os fabricantes de produtos WLAN apoiaram um novo padrão definido com 802.11g pela IEEE. O 802.11g combina o melhor dos dois padrões anteriores, ou seja, suporte a velocidades de até 54 Mbps, e usa a frequência de 2,4 GHz para maior alcance. Esse padrão só é compatível com o 802.11b.

2.3.1.4 Padrão IEEE 802.11n

Com uma demanda crescente por redes Wi-Fi mais performáticas, maximizar a taxa de transmissão foi o principal motivador para o padrão 802.11n. Essa novas determinações melhoram a largura de banda, suportada pela utilização de múltiplos sinais de entrada e saída e antenas MIMO (*Multiple-Input Multiple-Output*). O conjunto de padrões 802.11n foi ratificado pela indústria em 2009, com especificações que prevê até 300 Mbit/s de taxa de transmissão e também oferece maior alcance do sinal, mais resistência a interferências e retro compatível com dispositivos 802.11b / g. Porém os dispositivos antigo SISO (*Single-Input Single-Output*) não tem benefício para novas melhorias.

2.3.1.5 Padrão IEEE 802.11ac

Homologado em janeiro de 2014, o novo padrão para WLANS o 802.11ac, trabalha na frequência de operação de 5 GHz, e pode chegar a taxa de transmissão de 1300 Mbit/s com o uso de antenas MU-MIMO (*Multi-User MIMO*). Utilizando tecnologia de banda dupla, com compatibilidade ao padrão 802.11n, suportando conexões simultâneas em 2,4 GHz e 5 GHz.

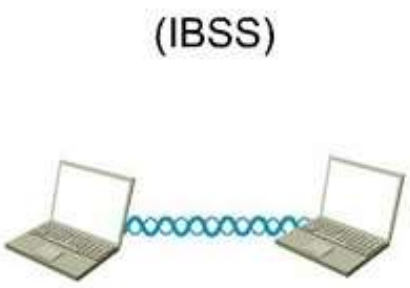
2.3.2 Arquitetura WLAN

As formas dos elementos se comunicarem e trocarem informações em uma infraestrutura WLAN podem variar em diferentes arquiteturas. As 3 principais formas para um enlace são:

. IBSS (*Independent Basic Service Set*), também referenciada com Ad-Hoc.
. BSS (*Basic Service Set*)
. ESS (*Extended Service Set*)

Na arquitetura IBSS ou Ad-Hoc, os elementos participantes dessa rede se comunicam diretamente uns com os outros, não existe a necessidade de um elemento concentrador e as equipamentos devem estar na mesma área de cobertura de sinal entre eles. Esse tipo de comunicação e restrita a poucos equipamentos e normalmente de uso domestico. A figura 4, representa essa rede.

Figura 4: arquitetura Ad-Hoc

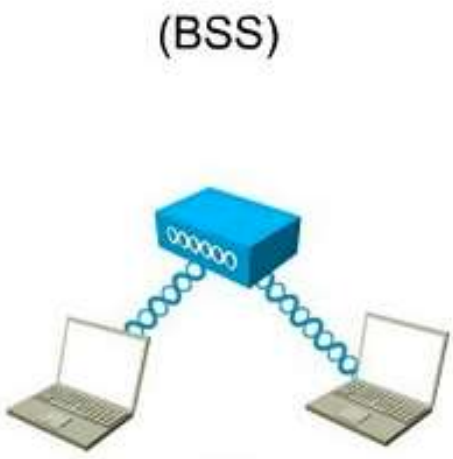


Fonte: http://www.learncisco.net/courses/icnd-1/wireless-lans/implementing-a-wlan.html

Para o enlace BSS, existe a necessidade de um equipamento concentrador, um ponto de acesso ou AP (*Access Point*). Também chamada de rede infra-estruturada, os elementos móveis participantes dessa rede devem se conectara ao elemento AP que está em seu raio de alcance. Atuando como um elemento de camada 1 (Física) do modelo OSI, o AP é semelhante ao Hub em uma rede cabeada, recebe o sinal de um dispositivo e propaga o para todos os elementos de sua área de cobertura em busca do receptor. Essa característica já demonstra uma vulnerabilidade dos ambientes Wi-Fi. Onde todos os dispositivos participantes daquela rede pode receber a comunicação uns dos outros mesmo não sendo o nó receptor da transmissão.

Para a arquitetura BSS, o AP pode atuar como uma ponte (*bridge*) entre a rede LAN e a WLAN. Dessa forma os equipamentos móveis (Wi-Fi) e fixo (Ethernet) pode se comunicar, formando uma mesma rede lógica. Mas um ponto de vulnerabilidade pode observado nessa ligação do mundo com e sem fio. Essa característica permite promover acesso de um dispositivo móvel sem fio a uma rede física. A figura 5 exemplifica uma rede BSS

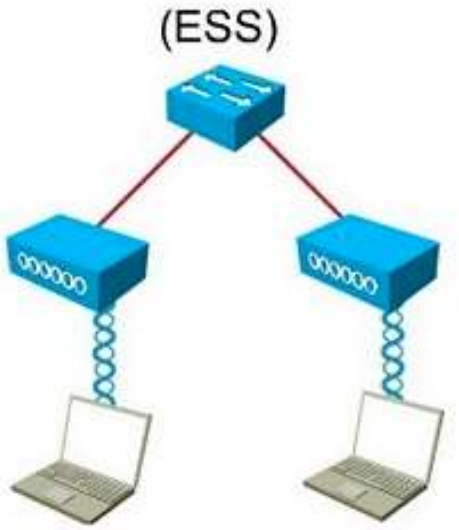
Figura 5: arquitetura BSS



Fonte: http://www.learncisco.net/courses/icnd-1/wireless-lans/implementing-a-wlan.html

As redes BSS são limitadas a um único elemento concentrador. Para resolver essa limitação, o enlace ESS estende o crescimento de uma WLAN através da ligação de várias BSS`s, possibilitando maior abrangência e área cobertura. Nesse cenário de múltiplas BSS, o protocolo WDS (*Wireless Distribution System*) compartilha as informações entre os AP`s, dando possibilidade dos dispositivos trocarem de BSS sem desconectar-se e possibilitado a criação de várias células para atendimento de grandes áreas geográficas como: universidades, fábricas, parques, praças, shoppings e até pequenas cidades. Uma representação de ESS pode ser exemplificada na figura 6

Figura 6: arquitetura ESS



Fonte: http://www.learncisco.net/courses/icnd-1/wireless-lans/implementing-a-wlan.html

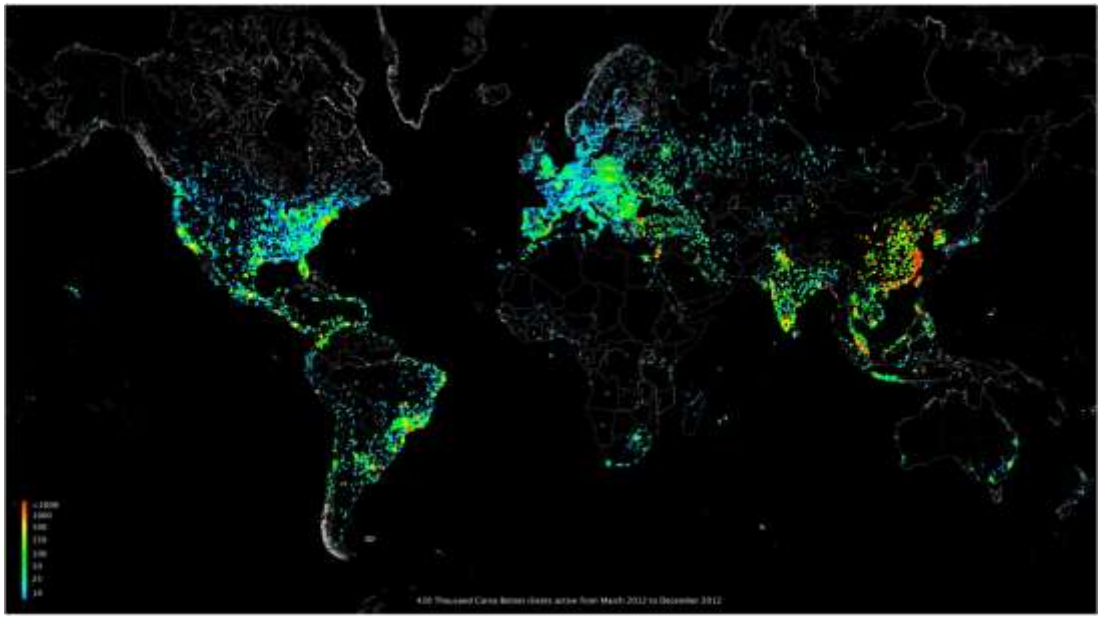
2.4 Ameaças e vulnerabilidades das redes Wi-Fi

Para o padrão Wi-Fi, uma grande variedade de ataques são descritos na literatura. Ataques que se aproveitam de falhas tecnológicas e deficiências do ambiente físico. Do ponto de vista humano, também se discute problemas e alternativas. Vasconcelos (2013) afirma que um problema importante na segurança das redes Wi-Fi está fortemente ligado ao desconhecimento e despreparo dos administradores e usuários na implementação e uso dos

recursos de segurança disponíveis. Gartner (2008) alega que 70% do sucesso dos ataques as redes Wi-Fi está amplamente relacionado a problemas de configuração de AP`s e também dos software de dispositivos clientes.

Pesquisa divulgada pela CNET (2013) mostrou que a ativação de dispositivos em redes com as configurações padrão de fábrica, como por exemplo, usuários e senhas já pré-configurandos pelos fornecedores, são muito comuns. A grande maioria de usuários e administradores não faz as alterações e configurações necessárias. Nessa pesquisa, foram feitas avaliações (varredura) de toda a Internet, e 420 mil dispositivos estariam sujeitos a exploração e invasão usando-se as configuração padrão disponibilizadas pelos fabricantes em manuais em sites. A figura 7 demostra a concentração desses dispositivos em nível global detectados pela ferramentas da pesquisa de Março a Dezembro de 2012.

Figura 7: Detecção global de dispositivos pela Carna Botnet



Fonte: CNET (2013)

Em relação as redes WLAN, CPP (2010) investigou por meio de teste de penetração em 40 mil redes Wi-Fi sendo elas: publicas, empresariais, *Hotspots*, SOHO (*Small Home/Home Office*) e residenciais em todo Reino

Unido. O estudo afirma que quase a metades dessas redes poderiam ser invadias em poucos segundos. A conclusão da pesquisa mostrou importantes resultados como:

- A maioria dos usuários acredita estar em segurança
- a grande maioria acredita que pessoas não autorizadas não acessam suas redes
- 17% das pessoas usam redes públicas regularmente
- Facilidade na implementação de AP`s maliciosos, levando os usuários a se conectarem em redes falsas.
- Redes WLAN são utilizadas para serviços sensíveis e com dados sigilosos como e-mails, serviços bancários e compras on-line.

2.4.1 Ataques ao protocolo 802.11

O padrão 802.11 trabalha sobres as camadas 1 e 2 do modelo OSI, identificadas respectivamente com camadas Física (PHY) e camada de Enlace (Data Link) sendo a segunda especificamente na sub camada MAC (controle de acesso ao meio). Por essas características especificas, esse protocolo possui ameaças e vulnerabilidades particulares.

Para Milliken (2010) podemos agrupar essa gama de ataques em, três macro categorias: ataques aos mecanismos criptográficos e de autenticação (*Encryption Bypass attacks*), ataques de negação de serviço (*Denial of Service attacks*), e ataques de falsificação de AP`s (*AP Masquerading attacks* ou *Rogue Access point attacks* - RAP). Yu e Liu (2007) também apresentam dois macro grupos de tipos de ataque as WLAN`s, os *Crypt Attacks* e os *Dos Attacks*.

Já Noor e Haasan (2013), apresentam como as principais ameaças e vulnerabilidades o escaneamento e quebra de senha, os ataques de MITM (*Man In The Middle*) e captura de pacotes (*Snniffing*), pontos de acesso falsos (*Rogue Access Point - RAP*), os ataques de negação de negação de serviço (*Denial of Service - DOS*) e por fim a própria engenharia social (*Social Enginnering*).

2.4.1.1 Ataques a Criptografia (WEP, WPA/WPA2)

Um dos princípios fundamentais nos processos de segurança de redes é a criptografia, definida como o estudo e a aplicação de tecnologias que vão possibilitar a transformação de informações legíveis e passiveis de entendimento em informações ilegíveis, entendidas somente por pessoas autorizadas ou que possuam credencias para isso. Senda assim a criptografia serve como base para garantia da integridade e confidencialidade dos dados transmitidos, dificultado algum acesso indevido a essa comunicação.

Na comunicação por rádio frequência, as dimensões físicas da rede são difíceis de serem determinas, e todos os dispositivos dentro da área de cobertura do sinal podem escutar e ter acesso as comunicações. Para as WLAN`s recursos criptográficos são fornecidos e seu uso muito recomentado, porém nem sempre são imunes a falhas e a quebra.

O primeiros ataques desferidos aos mecanismos criptográficos visaram o algoritmo WEP (*Wired Equivalent Privacy*), ele foi desenvolvido em 1999 com proposito de atender a demanda por segurança dos primeiros produtos comerciais.

Em 2001 foram descobertas graves falhas na estrutura desse protocolo, que se mostrou muito vulnerável e inseguro. Vulnerabilidade essas que permitiram um número elevando de ataques contra o WEP. Uma vasta referênciadiscute esses problemas, que podem ser concentrados nos seguintes pontos (FLUHRER, MANTIN e SHAMIR (2001); CHAABOUNI (2006); STOŠIĆ e BOGDANOVIĆ (2012); KUMKAR, et al (2012):

- Gestão e gerenciamentos das chaves criptográficas ruins
- *Inicialização Vector* (IV) pequeno e em testo-plano
- Função Hash CRC-32 é linear, imprópria para algoritimos criptográficos
- Cifra de fluxo RC4 deficitária
- Exploração RC4 para ataques estatísticos

• Mensagens forjadas para autenticação são aceitas
• Sem proteção aos quadros de gerenciamento

Com a exposição e demonstração sistemática das falhas do WEP em eventos de segurança, congressos e publicações científicas, uma atualização rapidamente foi apresentada.

No final de 2002, a Wi-Fi Alliance define com novo protocol de segurança, o WPA (*Wi-Fi Protected Access*). O WPA foi desenvolvido em caráter de urgência e utiliza como base as especificações do projeto IEEE 802.11i da própria IEEE.

Apesar de muitas melhorias como: evoluções dos algoritmos de criptografia, maior tamanho das chaves, metidos de autenticação com perfil pessoal (WPA-PSK) e coorporativo (802.1x), uso de chaves dinâmicas em contra partida as chaves estáticas do WEP e um novo código de verificação de mensagem MIC que é uma função *Hash* não-linear, bem mais consistente que o CRC-32. Muitos problemas para esse padrão foram encontrados e publicados cientificamente.

Para Beck e Tews (2008), Michael (2010), Beck (2010) e Caneill e Gilis (2010) o número de vulnerabilidades exploráveis ainda continua bem grande para as redes que adotam o WPA como medida de segurança:
• Ataques de dicionário para *Passphase* menores que 20 caracteres
• Captura de informações no processo de autenticação *four-way-handshak*
• Possibilidade de negação de serviço ao se detectar dois erros de MIC, gerando sucessivos cancelamentos de conexão.
• Ataque *Beck and Tews* que exploram o MIC e TKIP (*Temporal Integrity Protocol*)
• Possibilidade de ataque MTMI (OHIGASHI e MORII, 2009)
• Sem proteção aos quadros de gerenciamento

Em busca de um padrão mais bem elaborado e consistente de segurança, a IEEE trabalhou para evolução de um padrão avançado e mais seguro para as WLAN`s. Assim, em 2004 é finalizado o padrão IEEE-802.11i, que serviu como referência ao WPA e agora é homologado pela Wi-Fi Alliance como WPA2 (*Wi-Fi Protected Access 2*).

O WPA2 mantem compatibilidade ao WPA, e suas melhorias estão relacionadas diretamente aos algoritmos de criptografia e de integridade dos dados. Todas as melhorias propostas no padrão 802.11i foram implementados no algoritmo WPA2 (MILLIKEN, 2010).

Na atualização do WPA para WPA2 se incorpora a execução de um algoritmo AES *(Advanced Encryption Standard)* chamado CCMP (*Counter Mode CBC MAC Protocol*) para substituir o protocolo TKIP já comprometido. AES é a cifragem que substitui RC4, sendo uma cifra em bloco muito mais segura, operando em blocos de 128bits e também o uso de autenticação baseada em AAD (*Additional Authentication Data*).

Segundo Ahamad (2010), o WPA2 é considerado o padrão de segurança Wi-Fi mais seguro. No entanto este sistema ainda trás algumas vulnerabilidades que podem ser exploradas:

• Ataques de dicionário para *Passphase* menores que 20 caracteres
• Falsificação de endereços e dados no uso do GTK (*Group Temporal Key*) como possibilidade de ataque MITM (AHAMAD, 2010)
• Sem proteção aos quadros de gerenciamento
• Ataques de negação desserviço por desautenticação (LINHARES e GONÇALVES, 2010)

2.4.1.2 Ataques de negação de serviço (*Denial of Service* - Dos)

Uma vasta literatura discute os diversos problemas, procedimentos e métodos aplicados nos ataques de negação de serviço em redes Wi-Fi. Sharma e Barwal (2014) divide ataques de negação em 4 tipos de ataque os

relacionando as camada da arquitetura TCP/IP. Os 4 tipos são: Ataques a camada de aplicação, ataques a camada de Rede e Transporte, ataques a camada MAC e ataques a camada Física.
Em redes 801.11, os ataques Dos têm seu foco de ação nas camada Física e na sub camada MAC do nível de enlace.

Na sub camada MAC, o endereçamento das placas de rede (*MAC Addresses*) são um informação vital para o processo de comunicação e gerenciamento dos dispositivos e AP`s que participam de WLAN. Segundo Milliken (2010) há uma confiança grande na integridade de endereço MAC de origem. Esses endereços MAC são tratados com identificadores únicos, utilizados para distinguir um dispositivo do outro. No entanto, não há nenhum mecanismo de validação desses endereços. Um invasor pode clonar o endereço de qualquer cliente ou AP.

Um atacante pode transmitir pacotes usando um endereço MAC de origem clonado de um AP. O destinatário destes quadros falsificados não tem nenhuma maneira de identificar se os pacotes têm endereços MAC legítimos ou forjados. A capacidade de transmitir quadros de gerenciamento falsificados viabiliza vários ataques de negação a sub camada MAC.

Dois desses ataques na sub camada MAC são os ataques de inundação de autenticação/associação (*Authentication/Association flood attack*) e os ataques de inundação desautenticação/desassociação (*Deauthentication/Disassociation flood attacks*) (COMPTON, 2007; LIU e YU, 2007).

Durante um ataque de inundação de autenticação/associação, um atacante usa endereços MAC falsos para tentativas de autenticar e associar a um AP de destino. O atacante faz repetidos pedidos de autenticação/associação e, eventualmente, esgota a capacidade de memória e processamento do AP, deixando os clientes com pouca ou nenhuma chance de conexão com a rede Wi-Fi.

Ataques de negação de serviço aplicados a camada física de redes sem fio, buscam causar obstrução e interferência nas frequências de transmissão. Os ataques de interferência (*Jamming attacks*) são aplicados e discutidos há muitos anos, desde a segunda guerra mundial (SIMON et al, 2001) . Congestionamento de uma rede WLAN com sinais de ruído podem degradar o rendimento da rede. Interferência com outros transmissores de rádio de mesma frequência e potencia maior podem prejudicar o desempenho de uma rede Wi-Fi (KANDE e VANI, 2013; SHARMA e BARWAL, 2014).

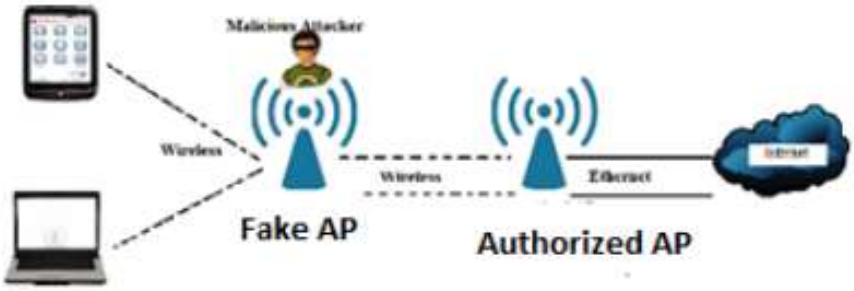
2.4.1.3 Ataques de AP falso (*AP Masquerading attacks* ou *Rogue Access Point attacks* - RAP)

Para Milliken (2010), embora a os mecanismos criptográficos tentem assegurar a conexão de cliente Wi-Fi para um AP, não existe a possibilidade de garantir totalmente que o próprio AP é legítimo. Existe um perigo real e crescente em redes sem fio modernas, a ameaça de *AP Masquerading*.
Este tipo de ataque ocorre quando um dispositivo AP falso ou mascarado se apresenta na rede tentando imitar é se passar como um AP legitimo existente. O grande objetivo desse ataque é levar os usuários a se conectarem sem perceber a esse AP falso, e à medida que se comunicam através do AP malicioso, tem seus dados capturados.

Para Thite, Vanjale e Mane (2014) os AP`s maliciosos podem ser divididos em dois grandes grupos: os *Fake Access Point* e *Rogue Access Point.* Nos casos de *Fake AP*, ilustrados na figura 8**,** ele é criado ou instalado por um atacante mal intencionado que não faz parte do grupo de usuários da rede. E o principal objetivo é realizar ataques MITM e Dos para roubo de informações e espionagem.

Já os *Rogue AP* podem ter caráter malicioso ou simplesmente serem implementados por usuário da própria rede, que se interessam em retirar maiores vantagem da infraestrutura.

Figura 8: Ataque MITM com *Fake AP*



Fonte: Thite, Vanjale e Mane (2014)

Ma, Teymorian e Cheng (2007) propõem uma taxonomia para os tipos de ataques explorados pelos *Rogue AP`s*. Essa taxonomia divide os AP`s falsos em quatro classes: *Improperly Configured AP, Unauthorized AP, Phishing AP* e *Compromised AP*

A tabela 2 apresenta a síntese da taxonomia com as quatro classes de *Rogue AP* e possíveis cenários de exploração proposto.

Tabela 2: Taxonomia dos *Rogue AP*

Classe de AP	**Senário de Exploração**
1- Configurações inadequadas	despreparo nas configurações de segurança, drivers e recursos físicos restritos e múltiplas placas de rede
2- Não autorizado	Ativação a rede interna sem autorização do administrador e conexão a redes vizinhas de maior proximidade e potência
3- Pescaria (*Phinshing*)	Fabricação de informações
4- Comprometido	Divulgação das credencias de segurança

Fonte: elaborada pelo autor

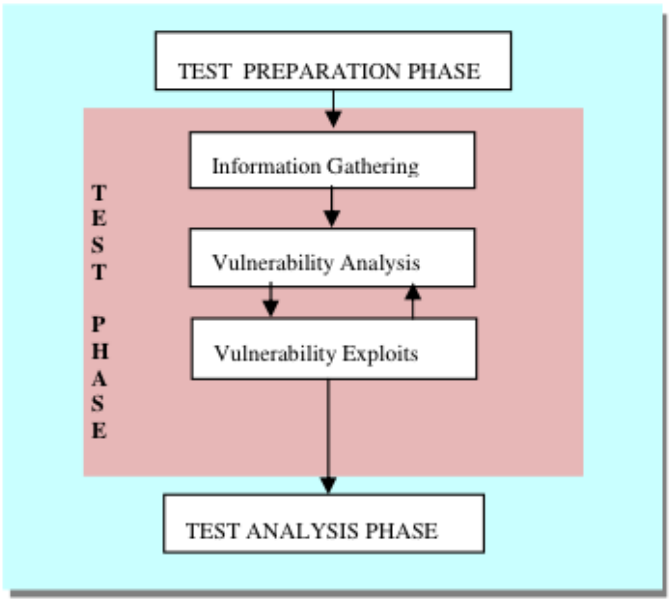
Um novo tipo de preocupação é apresentado na pesquisa de Nyathi e Nd lovu (2014). Os autores apresentam uma nova forma de ativação para um *Rogue AP*. Esse RAP (*Rogue AP*) é instalado e configurado de forma

maliciosa em um *SmartPhone* que possui o Sistema Operacional (SO) Android. O novo tipo é denominado como SRAP (*SmartPhone Rogue AP*). Sua facilidade de implementação e quantidade de dispositivos portadores desse SO, potencializam seu caráter malicioso.

2.5 Teste de Penetração (*Pentesting*)

Para Bacudio et al (2011) os Testes de Penetração ou *pentesting* são um conjunto de atividades realizadas para identificar e explorar falhas e vulnerabilidades de segurança. Eles ajudam a medir o nível robustez de segurança que foram implementadas. A metodologia do teste de penetração ilustrada na figura 9 inclui três fases: preparação da avaliação, testes e análise de teste. A fase de teste envolve as seguintes etapas: coleta de informações, análise de vulnerabilidade, e explorar de vulnerabilidade.

Figura 9: Fases de um teste de penetração



Fonte: Bacudio et al (2011)

Para um processo de levantamento desses riscos e também no intuito de criar um guia para melhoria de segurança nessas redes, as técnicas de Teste de penetração são um processo eficiente e muito utilizado em redes que já estão em produção ou querem passar por uma avaliação/auditora. O executor dos Testes de Penetração ou *pentester (Ethical Hacker)* pode

identificar problemas em um ambiente já em produção. Por meio de Teste de Penetração, busca-se evidenciar as falhas e vulnerabilidades que poderiam ser exploradas por possíveis invasores maliciosos (*Hackers*) (WEIDMAN, 2014; OSSTMM 3, 2010).

Em relação a estratégia do Teste de Penetração, podemos separá-los em três estratégias: Teste Caixa Preta (*Black Box*), Teste Caixa Branca (*White Box)* e Teste Caixa Cinza (*Grey Box*). Todas as três estratégias estão relacionadas a quantidade de informações previas recebidas pelo *pentester* (SHRAVAN, NEHA e PAWAN, 2014)

No Teste Caixa Preta o avaliador não receberá qualquer tipo de informação sobre o ambiente a ser analisado. O intuído é colocar o *pentester* em condições reais, onde um atacante externo, que não tem conhecimento algum de sua rede irá buscar uma forma de invasão.

No Teste Caixa Branca o avaliador recebe um grande quantidade de informações sobre o ambiente a ser analisado. Nessa estratégia o foco é simular um ataque interno, onde o atacante tem conhecimento sobre a rede, sistemas e pessoas. Essa metodologia é muito aplicada em testes específicos para uma aplicação, sistema Web, banco de dados ou rede.

No Teste Caixa Cinza o avaliador receberá algum nível de informação sobre o ambiente, informações que possivelmente são publicas ou fáceis de conseguir. O objetivo desse teste e ganhar tempo e analisar a efetividade da equipe de segurança e também ganhar experiência na aplicação de Teste de Penetração

Segundo Wilhelm (2013), manuais e *frameworks* consistentes e revisados por pares podem auxiliar na aplicação de Teste de Penetração efetivos e com resultados coerentes. Algumas opções como *Information System Security Assessment Framework* (ISSAF) e *Open Source Security Testing Methodology Manual* (OSSTMM) estão disponíveis e fornecem orientações sobre as etapas necessárias para realizar um completo Teste de Penetração.

Para Teste de Penetração em redes Wi-Fi, estão disponíveis muitas ferramentas de software, Sistemas Operacionais e hardware de grande capacidade e potência (ASSUNÇÃO, 2013). Sistemas operacionais como Kali Linux e Backbox Linux são completas suítes de ferramentas e *softwares* para *pentest* que auxiliam muito nos procedimentos e nas etapas de um Teste de Penetração

Todos esses recursos possibilitam uma avaliação muito apurada e precisa dos riscos e ameaças que podem acometer essas redes, ajudando na tomada de decisão para novos controles de segurança mais eficientes e robustos.

3. Metodologia

A natureza dessa pesquisa terá um enfoque qualitativo, onde o interesse principal é de expandir as informações. A abordagem qualitativa tem como ponto de partida uma realidade a ser desvendada e dá profundidade aos dados, contextualização do ambiente além dos detalhes desta realidade, sem abrir mão do rigor metodológico (SAMPIERI, COLLADO & LUCIO; 2006).

Neste tipo de abordagem, o pesquisador procura aprofundar-se na compreensão das ações dos indivíduos, grupos ou organizações em seu ambiente e/ou contexto – interpretando-os segundo a perspectiva dos participantes da situação enfocada, sem se preocupar com representatividade numérica e generalizações estatísticas. Desta forma, a interpretação, a consideração do pesquisador como principal instrumento de investigação e a necessidade do pesquisador de estar em contato direto com o cenário de pesquisa, para captar os significados dos comportamentos observados, revelam-se como características da pesquisa qualitativa (TERENCE & FILHO, 2006).

Nos estudos científicos qualitativos, a busca pela quantificação não é o foco de atenção. Há interesse em descrever e aprofundar sobre o tema, aplicando

modelos mais livres. O pesquisador tem como objetivo maior, descrever o fenômeno observado, entendendo sua ocorrência e correlaciona-lo a outros fatores envolvidos. (CASARIN; CASARIN, 2012)

Com base nos objetivos gerais e buscando uma maior aproximação conceitual, essa pesquisa se apresenta como descritiva. Seu objetivo primordial é descrever as características de uma determinada população (GIL, 2002). Para os estudos descritivos em uma pesquisa qualitativa, tem como ação principal coletar informações e descreve-las (SAMPIERI, COLLADO & LUCIO; 2006).

Para Gil (2002), análise dos fatos de um ponto de vista empírico, para uma comparação com a visão teórica, com os fatos reais, requer a definição de um modelo conceitual e operacional da pesquisa. Esse modelo recebe o nome de *design* ou delineamento.

O delineamento tem como base o planejamento da pesquisa em suas dimensão mais amplas, com foco nos procedimentos técnicos como: previsão de analise, interpretação e coleta dos dados (GIL, 2002).

Como base nesse delineamento, essa pesquisa se enquadra como pesquisa experimental.

> Um estudo experimental é uma atividade com o propósito de descobrir algo desconhecido ou de testar uma hipótese envolvendo uma investigação de coleta de dados e de execução de uma análise para determinar o significado dos dados. Isto cobre várias formas de análise e estratégias de pesquisa (LOPES, 2010, p. 9).

Nas pesquisas experimentais, o pesquisador exerce o papel de um agente ativo, não de um observador passivo. Essencialmente, é definido um objeto de estudo, determinando as variáveis de capazes de influenciar o cenário e definir as formas de controle e de observação causados pela manipulação dessas variáveis (GIL, 2002).

3.1 Coleta de Dados

A coleta de dados será feita por meio de Testes de Penetração adotando como referência a metodologia sugerida pela OSSTMM-3 (*Open Source Security Testing Methodology Manual*), através do método de Observação Não-Participante

Será utilizado o Sistema Operacional Kali Linux versão 1.1.0 e sua suíte de ferramentas de *Software Open Source* destinadas a Teste de Penetração Wi-Fi . Essa distribuição é bem amadurecida e vem se tornando um padrão de fato em processo de auditoria e Teste de Penetração em diversos padrões de rede, sistemas e ambientes computacionais. Para *pentest* em WLAN, esse Sistema Operacional disponibiliza em torno de trinta ferramentas com propostas de avaliações para diversos tipos de vulnerabilidades já apresentados no projeto.

3.2 População e Amostra

A população eleita será composta pelas maiores instituições de ensino superior localizadas de Belo Horizonte. Como critério de seleção dessa população, serão feitos testes experimentais nas instituições que possuem no mínimo 5.000 alunos regularmente matriculados, tendo como base no Censo da Educação Superior de 2013.

3.3 Tratamento dos Dados

Serão realizadas análises qualitativas e estatísticas dos dados a serem coletados na etapa experimental. Será realizado um confronto das vulnerabilidades e ameaças coletadas pelo Teste de Penetração com os controles de segurança sugeridos pela ISO/IEC 27002:2013.

4. CRONOGRAMA

Atividades/Mês	Fev 15	Mar 15	Abr 15	Mai 15	Jun 15	Jul 15	Ago 15	Set 15	Out 15	Nov 15	Dez 15
Revisão bibliográfica											
Definição do projeto de pesquisa											
Revisão do método											
Redação do projeto											
Redação do projeto											
Coleta dos dados											
Análise dos dados											
Análise dos resultados											
Redação da dissertação											
Defesa da dissertação											

5. REFÊRENCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/IEC Guia 73:2013. **Gestão de Riscos.** Vocabulário. Recomendações para uso em normas. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001. 20013. **Tecnologia da Informação.** Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos . Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: 2013; **Tecnologia da informação.** Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

ASSUNÇÃO, Marcos Flávio Araújo. **Wireless Hacking – Ataque e segurança de redes sem fio Wi-Fi**. São Paulo: Visual Books, 2013.

BACUDIO. Aileen G.; et al. An Overview Of Penetration Testing. **International Journal of Network Security & Its Applications (IJNSA)**, Vol.3, No.6, November 2011

CHAABOUNI. Rafik. Break Wep Faster with Statistical Analysis. Technical report, EPFL, LASEC, June 2006.

COMPTON. Stuart **802.11 Denial of Service Attacks and Mitigation.** Disponível em: http://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108, 2007, acesso em 15 mar 2015

CPP; UK Wireless Network Hijacking. Disponivel em: http://pt.slideshare.net/CPPUK/uk-wireless-network-hijacking-2010, 2010, acesso em: 15 mar 2015.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. Ed. São Paulo Atlas, 2008.

KANDE. Ramesh, VANI B.Madhura. Anti-Jamming Schemes To Prevent Selective Jamming Attacks. **International Journal of Computer Trends and Technology (IJCTT)** – volume 5 number 1 –Nov 2013

LIU. Chibiao, YU. James; A Solution to WLAN Authentication and Association DoS Attacks. **IAENG International Journal of Computer Science,** 34:1, IJCS_34_1_4 **August 2007**

NOOR,Mardiana Mohamad; HASSAN Wan Haslina. Wireless Networks: Developments, Threats and Countermeasures. **International Journal of Digital Information and Wireless Communications (IJDIWC)** 3(1): 119-134 The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2225-658X)

NYATHI. Thambo, ND LOVU. Siqabukile Beacon Frame Manipulation to Mitigate Rogue Access Points: Case of Android Smartphone Rogue Access Points. **COMPUSOFT, An international journal of advanced computer technology**, 3 (2), February-2014 (Volume-III, Issue-II)

RUFINO, Nelson Murilo de O. **Segurança em Redes sem Fio - Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth.** 4. Ed. São Paulo: Pearson, 2014.

SAMPIERI, Roberto Hernández; COLLADO, Carlos Hernández; LÚCIO, Pilar Baptista. **Metodologia de pesquisa**. 3. Ed. São Paulo: McGraw-Hill, 2006. 583 p.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma visão Executiva**. Rio de Janeiro: Campus, 2003.

SIMON. M.K., OMURAJ.K., SCHOLTZ. R.A., LEVITT. B.K.. SpreadSpectrum

Communications Handbook.McGraw-Hill, 2001.

SHARMA. Nisha, BARWAL. Paras Nath. Study of DoS Attacks on IEEE 802.11 WLAN and its Prevention/Detection. **International Journal of Engineering Science and Innovative Technology (IJESIT)** Volume 3, Issue 3, May 2014

SHRAVAN. Kumar,, NEHA. Bansal, PAWAN. Bhadana. Penetration Testing: A Review **COMPUSOFT, An international journal of advanced computer technology,** 3 (4), April-2014 (Volume-III, Issue-IV)

STALLINGS William. **Criptografia e Segurança de Redes – Princípios e Práticas**. 4. Ed. São Paulo: Pearson. 2008.
SVERZUT, José Umberto. **Redes GSM, GPRS, EDGE e UMTS**. São Paulo: Érica 2005.

TERENCE, Ana Cláudia Fernandes; FILHO, Edmundo Escrivão. Abordagem quantitativa, qualitativa e a utilização da pesquisa-ação nos estudos organizacionais. **XXVI ENEGEP**. Fortaleza, CE, Brasil. 9 a 11 de Outubro de 2006.

THITE. Sandip S., VANJALE. Sandeep, MANEP. B. A Novel Approach For Fake Access Point Detection and Prevention in Wireless Network. **International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)** ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 4, Issue 1, Feb 2014, 35-42

WEIDMAN, Georgia. **Teste de Invasão – Uma introdução prática ao hacking**. São Paulo: Novatec., 2014.
WILHELM. Thomas, Professional Penetration Testing: Creating and Learning in a Hacking Lab: 2.ed. Waltham, MA: Elsevier, 2013. 165 p.