MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO DE
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1T(QC-CA) RAFAEL CAVEARI GOMES

PROBLEMAS DE SEGURANÇA EM REDES DE COMPUTADORES NA MARINHA DO BRASIL: UMA ANÁLISE SOBRE A TÉCNICA ROGUE ACESS POINT

Rio de Janeiro
2018

1T(QC-CA) RAFAEL CAVEARI GOMES

PROBLEMAS DE SEGURANÇA EM REDES DE COMPUTADORES NA MARINHA DO BRASIL: UMA ANÁLISE SOBRE A TÉCNICA ROGUE ACESS POINT

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk (CIAW) como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações (C-ApA-SIC).

Orientadores:
Professor Anderson Oliveira da Silva
Professor Julio Cesar Ho

CIAW
Rio de Janeiro
2018

1T(QC-CA) RAFAEL CAVEARI GOMES

PROBLEMAS DE SEGURANÇA EM REDES DE COMPUTADORES NA MARINHA DO BRASIL: UMA ANÁLISE SOBRE A TÉCNICA ROGUE ACESS POINT

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações.

Aprovada em _____ /_____ / 2018

Banca Examinadora:

Anderson Oliveira da Silva, DSc – PUC Rio _____

Julio Cesar Ho – CIAW _____

Miriam Moraes Puerari, MSc – CIAW _____

CIAW
Rio de Janeiro
2018

A Deus, aos meus pais Lídia e Antônio (in memoriam) e a minha esposa Luana.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pela minha vida, família e saúde. Sem Ele nada disso seria possível. Agradeço a toda minha família pela dedicação e apoio incondicionais, em especial aos meus irmãos Rodrigo e Ronaldo que me ajudaram desde o início de minha carreira.

À minha mãe Fátima e minha avó Lenice pelo amor, carinho e preocupações constantes com o meu bem-estar.

À minha esposa Luana que sempre me apoiou e é exemplo de dedicação e perseverança para mim.

Aos professores orientadores Anderson e Júlio Ho pelas excelentes aulas ministradas e pelas orientações tão necessárias nesse momento de extrema insegurança que é o final do C-ApA-SIC. Aos demais professores e instrutores que me inspiraram a sempre buscar meus objetivos e acreditar que a dedicação em busca do conhecimento nunca é em vão.

Aos campanhas de turma que sempre tiveram uma palavra de conforto e motivação para seguir em frente. Sem eles essa jornada teria sido muito mais penosa.

Um muito obrigado especial ao meu pai Antônio Carlos (in memoriam) e ao meu avô Nininho (in memoriam) que sempre foram exemplos de seres humanos dignos e obstinados.

Obrigado por tudo.

“O insucesso é apenas uma oportunidade para recomeçar com mais inteligência.”

Henry Ford

PROBLEMAS DE SEGURANÇA EM REDES DE COMPUTADORES NA MARINHA DO BRASIL: UMA ANÁLISE SOBRE A TÉCNICA ROGUE ACESS POINT

RESUMO

Nenhuma rede ou sistema é cem por cento seguro. Entretanto, as redes sem fio acrescentam um fator extra na questão de segurança, quando comparadas à rede cabeada. Pelo fato de utilizarem ondas eletromagnéticas como meio de propagação e acesso, é muito mais difícil controlar a sua abrangência, podendo facilmente ultrapassar os limites físicos da instituição, possibilitando assim, a sua detecção ou sua tentativa de utilização por pessoas não autorizadas. A utilização de redes sem fio em instituições militares da Marinha do Brasil só é permitida mediante autorização formal da DCTIM. Contudo, uma rede sem fio autorizada pode ser alvo de um ataque do tipo Rogue Acess Point, onde outra rede ilegítima tenta se passar pela legítima. Além disso, mesmo se na organização militar não existir uma rede sem fio, um usuário mal-intencionado pode fazer uso dessa técnica para roubar informações de usuários mais incautos que por ventura venham a se conectar na rede falsa.

Um Rogue Acess Point é um ponto de acesso que foi instalado sem a autorização explícita do administrador da rede. Os pontos de acesso invasores representam uma ameaça à segurança porque qualquer pessoa com acesso às instalações pode, de forma maliciosa, instalar um ponto de acesso sem fio de baixo custo que induz usuários a se conectarem na rede falsa que tenta se passar pela rede legítima. Isso basicamente é realizado quando o Rogue Acess Point finge ser o ponto de acesso Wi-Fi da rede e também, o servidor DHCP, que fornece parâmetros de configuração falsos para o dispositivo solicitante. O dispositivo malicioso induz o cliente a entrar na rede Wi-Fi falsa e também responde a requisição DHCP do cliente informando ser o roteador da rede e o servidor DNS, além de fornecer um endereço IP falso para cliente. O cliente não tem como saber que o dispositivo malicioso não é o verdadeiro Access Point e servidor DHCP, logo, confirma o recebimento da resposta e configura sua interface de rede adequadamente. O cliente então rejeita qualquer outra resposta a sua solicitação.

Uma vez conectado na rede ilegítima, o usuário fica exposto a diversas ameaças: pode ser direcionado para um servidor web falso que coleta informações sensíveis, ter toda a sua comunicação inspecionada, etc.

Esse trabalho de conclusão de curso procura realizar uma análise da técnica de ataque Rogue Acess Point, assim como busca elencar possíveis soluções que mitiguem as ações de usuários mal-intencionados e que podem fazer uso desse ataque.

Palavras-chave: rogue, access point, ataque, wi-fi

LISTA DE FIGURAS

LISTAS DE SIGLAS E ABREVIATURAS

AC	Autoridade Certificadora
AMRJ	Arsenal de Marinha do Rio de Janeiro
AP	Access Point
ARPAnet	Advanced Research Projects Agency Network
BSSID	Basic Service Set Identifier
BSA	Basic Service Area
BSS	Basic Service Set
CIAW	Centro de Instrução Almirante Wandenkolk
C-ApA-SIC	Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ESA	Extended Service Area
ESS	Extended Service Set
HTTPS	Hyper-Text Transfer Protocol over SSL/TLS
IP	Internet Protocol
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
MAC	Media Access Control
MB	Marinha do Brasil
MIMO	Multiple-Input Multiple-Output
OM	Organização Militar
PAE	Port Access Entity
RADIUS	Remote Authentication Dial in User Service
RECIM	Rede de Comunicações Integradas da Marinha
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security

UDP	User Datagram Protocol
WI-FI	Wireless Fidelity
WIPS	Wireless Intrusion Prevention System
WPA	Wi-fi Protected Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

Na sociedade contemporânea, as informações são cada vez mais consideradas os principais patrimônios de qualquer organização, além disso estão constantemente sob risco. A sua perda ou roubo constitui um prejuízo para a organização e é um fator decisivo na sua sobrevivência nos dias atuais (MÉDICE, 2013).

Para garantir a segurança da informação de qualquer organização, seja ela civil ou do âmbito militar, é necessário que haja normas bem definidas e procedimentos claros que deverão ser seguidos piamente por todos os usuários. É um desafio fazer com que seus colaboradores conheçam e sigam corretamente as políticas de segurança, entendendo a sua importância (MÉDICE, 2013).

Ataques cibernéticos ocorrem na internet com diversos objetivos e usando variadas técnicas. De modo geral, qualquer serviço, computador ou rede que seja acessível através de uma rede pode ser alvo de um ataque, assim como qualquer computador que esteja conectado à uma rede pode participar de um ataque.

Os motivos que levam os atacantes a desferir ataques em redes de computadores são diversos, como demonstração de poder, prestígio, motivações financeiras, motivações ideológicas, motivações comerciais, entre outros.

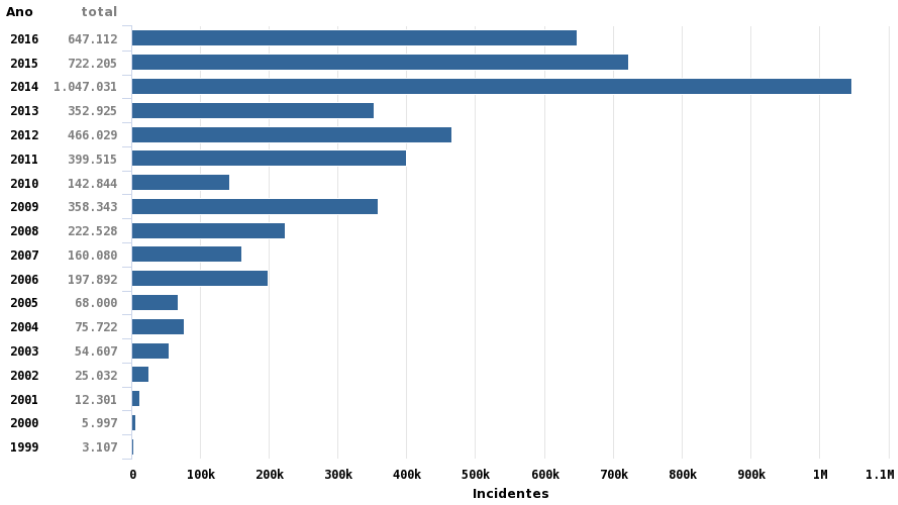
Podemos conceituar vulnerabilidade como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Essas vulnerabilidades podem estar em falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Basicamente, um ataque que explora as vulnerabilidades ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema ou acessar informações confidenciais, por exemplo, disparando ataques contra outros computadores ou tornando um serviço inacessível.

1.1 Apresentação do problema

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), o número de incidentes digitais informados no ano de 2016 foi de 647.112. Esse total de notificações, apesar de ser 10% menor que o total de 2015, demostra que os problemas relacionados à segurança das informações digitais encontram-se em grande evidência nos dias atuais. Observando a Figura 1, pode-se verificar a evolução do número de incidentes reportados com o passar dos anos (CERT, 2018).

Figura 1: Total de incidentes reportados ao CERT.br por ano.



Fonte: CERT (2018).

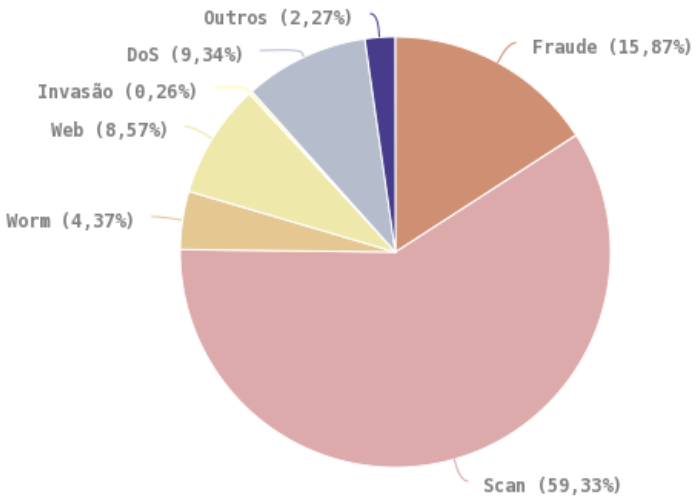
O total de ataques reportados no ano de 2016 podem ser desmembrados em sete categorias (CERT, 2018):

a) Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede;
b) Denial of Service (DoS): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede;
c) Invasão: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede;
d) Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na internet (pichação virtual);

e) Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por hackers para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;
f) Fraude: engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem; e
g) Outros: notificações de incidentes que não se enquadram nas categorias citadas anteriormente anteriores.

Os percentuais das categorias de ataques podem ser vistos na Figura 2.

Figura 2: Tipos de ataques reportados ao CERT.br no ano de 2016.



Fonte: CERT (2018).

Tendo em vista esse cenário do crescente número de ataques a redes de computadores e incidentes cibernéticos no Brasil, é de vital importância que uma instituição como a Marinha do Brasil (MB), invista em consideráveis esforços para mitigar essas vulnerabilidades.

Além dos ataques citados acima, um vem ganhando grande notoriedade nos últimos tempos pela disseminação no uso de redes sem fio: o *Rogue Acess Point* (AP). Um Rogue AP é um ponto de acesso wireless, não autorizado na rede, que tem como objetivo a captura de informações de seus utilizadores.

As redes sem fio vieram facilitar em muito o acesso à informação. Através de placas com tecnologia IEEE 802.11, mais popularmente conhecidas como placas Wireless Fidelity (Wi-Fi), que vem integradas tanto em smartphones como em

tablets. Os utilizadores desses equipamentos tentam, em qualquer lugar, ganhar acesso às redes wireless disponíveis.

Na Marinha do Brasil, a utilização de redes sem fio a princípio é vedada. Contudo, em casos excepcionais, as Organizações Militares (OM) da MB que tiverem interesse em instalar uma rede sem fio devem encaminhar um pedido formal a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) a fim de obter um parecer favorável a autorização. Nenhum dispositivo de rede sem fio deve ser implementado sem análise e autorização prévias da DCTIM (BRASIL, 2017).

Contudo, nos casos onde existe uma rede sem fio autorizada em determinada organização militar, um usuário mal-intencionado pode se utilizar de um Rogue AP para induzir os usuários legítimos a se conectarem na rede wireless falsa. Com isso, várias informações podem ser capturadas do usuário e diversas possibilidades ao atacante são facilitadas. Deve-se levar em consideração também que, mesmo não existindo uma rede sem fio oficial autorizada na OM, um atacante pode “iniciar sua oferta de serviço” através do Rogue AP e se beneficiar de usuários leigos que acessam essas redes, para roubar informações. Em ambas as situações as consequências podem ser graves.

1.2 Justificativa

A segurança em redes de computadores é um assunto muito discutido nos dias atuais, tendo em vista a constante divulgação pela mídia de ataques cibernéticos direcionados a grandes instituições privadas e governamentais pelo mundo.

Um ataque que foi bastante difundido e atingiu tanto organizações públicas como privadas (incluindo a MB) em maio de 2017, foi do tipo ransomware - que criptografa os arquivos do usuário, impedindo sua utilização, até o pagamento de um resgate (ransom). Foi usado também em combinação com uma funcionalidade de worms para que a infecção se espalhasse automaticamente. O alcance global foi sem precedentes. A contagem de máquinas infectadas chegou a mais de 200 mil em pelo menos 150 países (O GLOBO, 2017a).

Outro ataque de grande vulto atingiu a Europa em junho de 2017. O governo ucraniano afirmou que foi alvo de um ataque que atingiu bancos e

empresas e o classificou como o maior da história (O GLOBO, 2017b). Em um incidente que talvez possa estar relacionado a essa notícia, 350 pacientes deixaram de ser atendidos no Hospital do Câncer em Barretos (CORREIO 24 HORAS, 2017). Um ataque como esse poderia facilmente comprometer o atendimento do Hospital Naval Marcílio Dias (HNMD), onde vários exames de imagem e laboratoriais para serem realizados utilizam computadores com o sistema operacional Windows, alvo do ransomware.

Todos esses casos servem para demostrar o quanto somos alvos diários de ataques cibernéticos e nenhuma instituição está imune a eles. Tendo em vista a disseminação e utilização de redes sem fio, e a facilidade em se realizar um ataque do tipo Rogue AP, é de suma importância que a MB tome conhecimento da utilização dessa técnica e procure mitigar os seus efeitos, buscando métodos de proteção efetivos para resguardar os usuários da Rede de Comunicações Integradas da Marinha (RECIM), assim como os seus ativos de informação.

1.3 Relevância

A Marinha do Brasil, assim como qualquer outra instituição, está passível de ataques à suas redes de computadores. Por se tratar de uma Força Armada, onde constantemente informações sigilosas são trafegadas na rede e uma possível negação de algum serviço pode acarretar grande prejuízo à nação, fica ainda mais evidente a importância de se conhecer algumas técnicas de ataques utilizadas para garantir a melhor proteção disponível.

De acordo com Tanembaum (2003), a segurança em redes de computadores no início de sua existência não exigiu muitos cuidados, tendo em vista que sua utilização se limitava a pesquisas acadêmicas (correio eletrônico) e funcionários de empresas para o compartilhamento de recursos (impressoras, por exemplo). Contudo, com a popularização e disseminação do uso de computadores pessoais e a facilidade de conexão à internet, foi necessário aumentar o nível de segurança dessas redes.

Segundo Brasil (2017), define-se as propriedades fundamentais da segurança de redes como:

a) Confiabilidade: garantia de que um dado recurso irá desempenhar sua função, plenamente de acordo com as expectativas e conforme previsto em projeto, em um intervalo de tempo pré-determinado;
b) Rapidez nas respostas às solicitações: rápido acesso às informações;
c) Disponibilidade: garantir para os usuários o acesso contínuo aos recursos, aos serviços e aos aplicativos existentes;
d) Eficiência: satisfazer às expectativas dos usuários, com o menor dispêndio de recursos (materiais e humanos) possível; e
e) Segurança: requisito que visa, conforme a necessidade, garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações que trafegam pela RECIM.

Neste trabalho, será dado foco no requisito da segurança das redes de computadores na RECIM, buscando realizar uma análise da técnica de ataque Rogue AP.

1.4 Objetivos

Nesta secção, serão apresentados o objetivo geral e os objetivos específicos do presente trabalho.

1.4.1 Objetivo geral

O objetivo geral desse trabalho de conclusão de curso é estudar e propor novas medidas de proteções e procedimentos de segurança com o intuito de elevar o nível de segurança nas redes sem fio da Marinha do Brasil.

Contudo, além das ameaças externas, é importante atentar para as internas. De acordo com Power (1996), mais de 80% dos pesquisados no survey apontaram empregados como ameaças ou potenciais ameaças para segurança da informação.

Na técnica de ataque Rogue AP, um usuário interno legítimo teria conhecimentos privilegiados das características da intranet de sua OM. Com isso, seria extremamente fácil, por exemplo, criar uma página falsa do sistema de pagamento da MB e realizar a captura das credenciais de segurança do seu responsável.

O típico criminoso de computadores é um usuário autorizado e não-técnico do sistema que teve oportunidade e tempo suficiente para determinar que ações podem prejudicar o sistema ou causar uma auditoria. A principal ameaça para a proteção da informação ainda está associada a erros e omissões, sendo responsável por 65% dos problemas (POWER, 1996).

1.4.2 Objetivos específicos

O dual TCP/IP foi grande contribuinte na consolidação da implementação das comunicações em redes através de níveis de camadas. O TCP/IP é formado por um conjunto de protocolos nos quais os principais são o Transfer Control Protocol (TCP), que atua no nível de transporte, e o Internet Protocol (IP), que trabalha no nível de rede.

Inicialmente não havia preocupação na interceptação das informações utilizando esses protocolos e a segurança dos dados que trafegavam pela rede era inexistente, pois os pacotes que trafegavam não eram criptografados, podendo ser facilmente descobertos e as vulnerabilidades facilmente exploradas através de técnicas como (MITSHASHI, 2011):

a) IP Spoofing;
b) DoS e DDoS;
c) Trojan Horses;
d) TCP Hijacking;
e) Sniffing;
f) Flooding, etc.

Na Marinha do Brasil, assim como em qualquer outra instituição que provê serviços em rede aos seus usuários, os provedores desses serviços se tornam alvos de ataques.

Os objetivos específicos desse trabalho de conclusão de curso são: (i) realizar uma análise da técnica de ataque Rogue AP; (ii) demostrar como um ataque dessa natureza pode ser realizado; e (iii) elencar e analisar possíveis métodos de mitigação.

2 REFERENCIAL TEÓRICO

Esse trabalho de conclusão de curso utilizará principalmente o seguinte referencial teórico:

a) Brasil (2017): norma interna da MB referente a tecnologia da informação. O trabalho se balizou nessa publicação para não ir em desacordo com o que se espera do tratamento da tecnologia da informação na presente instituição;
b) Brasil (2013): As Normas para a Salvaguarda de Materiais Controlados, Informações, Documentos e Materiais Sigilosos na Marinha também foi utilizada para garantir que os procedimentos adotados durante a realização do trabalho não estivessem em desacordo com relação a salvaguarda das informações digitais geradas;
c) Brasil (2014): A DCTIMARINST Nº 30-13 (Uso de Redes Sem Fio na MB) tem como propósito principal estabelecer normas e procedimentos para o uso de redes sem fio seguras no âmbito da MB;
d) Mitshashi (2011): TCC que mostrou conceitos e a implementação de técnicas para conseguir o máximo possível de segurança dentro de uma rede de computadores, para maximizar a integridade e segurança dos dados de empresa;
e) Tanenbaum (2003) e Kurose e Ross (2010): estão entre as principais referências para o estudo de redes de computadores e da pilha TCP/IP. Apresentam fundamentos teóricos para o correto entendimento do trabalho como um todo;
f) Vleugels e Peeters (2010) e Colcher (1995): fundamentação teórica sobre redes sem fio.

Pelo fato da técnica de ataque Rogue AP ser extremamente recente e não existir um grande acervo de informação bibliográfica oficial, também foram

consultadas publicações em blogues de tecnologia, tutoriais no Youtube e fóruns na Deep Web[1].

[1] A deep web, também chamada de deepnet ou undernet, é uma parte da web que não é indexada pelos mecanismos de busca, como o Google, e, portanto, fica oculta ao grande público. É um termo geral para classificar diversas redes de sites distintas que não se comunicam.

3 METODOLOGIA

Neste capítulo, apresentam-se os procedimentos no desenvolvimento da pesquisa. A seção 3.1 trata da classificação da pesquisa quanto aos fins. Já a secção 3.2 discute a classificação da pesquisa quanto aos meios. E na seção 3.3, foram relacionadas as limitações a respeito dos métodos descritos.

3.1 Classificação quanto aos fins

Esse trabalho de conclusão de curso pode ser classificado quantos aos fins, no que se refere a metodologia, em (MALEBRANCHE, 2017):

a) Descritivo: uma vez que expõe as características das redes de computadores na Marinha do Brasil, assim como suas possíveis vulnerabilidades. Tal análise é de vital importância para demonstrar a técnica Rogue AP; e
b) Aplicado: pois é fundamentalmente motivado pela necessidade de resolver o problema concreto da possibilidade de instalação de um Rogue AP em uma organização militar com o objetivo de capturar informação do tráfego dos usuários.

3.2 Classificação quanto aos meios

Esse trabalho de conclusão de curso pode ser classificado quantos aos meios, no que se refere a metodologia, em pesquisa bibliográfica, uma vez que foi feito um estudo sistematizado desenvolvido com base em material publicado acessível ao público em geral, como teses, artigos, livros, entre outros (MALEBRANCHE, 2017). Contudo, foram utilizadas publicações disponíveis apenas para militares da Marinha do Brasil, buscando conciliar o que foi proposto com as normas internas da instituição.

3.3 Limitações do método

Pelo fato da utilização da técnica de ataque Rogue AP ser relativamente recente, existe uma certa dificuldade em se encontrar um bom referencial teórico para o estudo aprofundado. Dessa forma, foram utilizados muitos materiais não oficiais para o desenvolvimento desse trabalho, como a consulta a blogs de tecnologia e a vídeo tutoriais.

Será apresentado um estudo teórico de como um ataque AP Roque pode ser realizado. Contudo, devido ao tempo disponível para a realização desse trabalho, não será possível executar o referido ataque na prática. Essa limitação da metodologia poderia esconder possíveis dificuldades que um atacante encontraria ao realizar a referida técnica.

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Nesse capítulo serão apresentados os conhecimentos teóricos necessários para o completo entendimento da técnica de ataque Rogue AP. Em seguida, a técnica em si será apresentada, assim como um pequeno tutorial de como realizá-la e se proteger.

4.1 Redes sem fio

O conceito de redes de computadores teve início na década de 1960, quando a telefonia era a rede de comunicação dominante em praticamente todo o mundo. Devido ao alto custo e a sua importância, o conceito de interligar computadores com o intuito de compartilhar recursos entre usuário espalhados geograficamente pelo globo tornou-se de suma importância. Devido a esse fato, iniciaram-se estudos ao redor do mundo dando origem ao que conhecemos hoje como comutação de pacotes, sendo uma alternativa poderosa e eficiente à comutação de circuitos da telefonia (KUROSE; ROSS, 2010).

O principal legado dessas pesquisas foi a Advanced Research Projects Agency Network (ARPAnet) do Departamento de Defesa dos Estados Unidos da América, sendo a primeira rede de computadores operacional à base de comutação de pacotes e a precursora da Internet (KUROSE; ROSS, 2010).

Juntamente com o desenvolvimento e evolução acelerada da ARPAnet, no final da década de 1960, entrou em funcionamento a primeira rede de pacotes por radiodifusão chamada ALOHAnet, desenvolvida na Universidade do Hawaii, que deu início ao desenvolvimento de redes de computadores sem fio. Aliás, as técnicas de detecção de colisão e meio físico compartilhado da Ethernet foram adaptadas da rede de rádio ALOHAnet (KUROSE; ROSS, 2010).

Dessa forma, o conceito de interligar computadores foi extremamente difundido. O grande vilão em se utilizar redes de computadores cabeadas está relacionado ao custo da infraestrutura que cresce exponencialmente quando o número de usuários aumenta. Além disso, uma rede cabeada é de pouca

flexibilidade, necessitando uma reestruturação caso o número de clientes cresça ou um determinado host se desloque (KUROSE; ROSS, 2010).

As aplicações de uso não licenciado do espectro são dispensadas do licenciamento da estação e de autorização para uso de radiofrequência, e esse uso, no Brasil, é regido pelo Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita, aprovado pela Resolução nº 365 de 10 de maio de 2004 (COIMBRA, 2006). Dessa forma, a faixa de frequência utilizada pelo padrão IEEE 802.11 estará sujeita a diversos outros dispositivos que também utilizam essas frequências. Pode-se citar (APPLE, 2013):

a) Fornos micro-ondas;
b) Certas fontes elétricas externas, como linhas de alimentação, trilhos de ferrovias elétricas e estações de energia;
c) Telefones sem fios;
d) Aparelhos de vídeo (transmissores/receptores);
e) Alto-falantes sem fio;
f) Alguns monitores externos e monitores LCD;
g) Qualquer outro dispositivo sem fio que opere na largura de banda de 2,4 GHz ou 5 GHz, etc.

Como já se sabe, as redes sem fio são caracterizadas, principalmente, pelo seu meio físico de comunicação: o ar. Isso é possível graças às ondas eletromagnéticas devidamente moduladas com as informações que gostaríamos de trafegar pelo meio, permitindo que dispositivos se comuniquem sem qualquer tipo de cabeamento entre eles. Esse tipo de rede é utilizado em diversas situações, entre elas (KUROSE; ROSS, 2010):

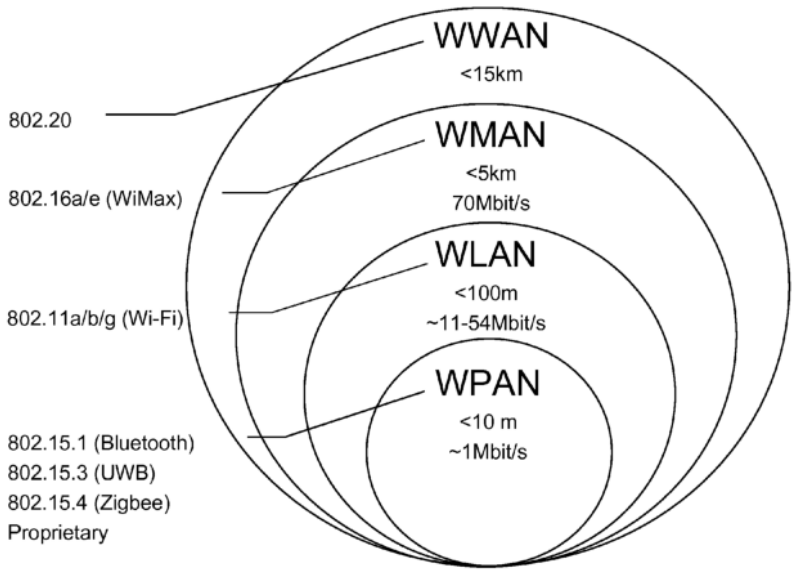
a) Quando não é possível instalar uma rede fixa (cabeada);
b) Quando há necessidade de se criar uma infraestrutura de rede temporária;
c) Quando se deseja estender uma rede já existente;
d) Quando necessitamos de mobilidade, etc.

Pensando nas questões relativas ao desenvolvimento, segurança e implementação de redes sem fio, o Institute of Electrical and Electronics Engineers (IEEE) criou padrões a partir de estudos já realizados sobre o conceito wireless, criando dessa forma, um padrão tecnológico. Em outras palavras, determinado equipamento pode ser configurado para determinado meio de atuação e, assim, ser

classificado como um padrão para determinada tarefa (VLEUGELS; PEETERS, 2010).

O padrão mais conhecido de redes sem fio é o padrão 802.11, que é o padrão das Wireless Local Area Network (WLAN). Contudo, existem também outros padrões que atendem a outros tipos de finalidade e necessidade: as Wireless Personal Area Network (WPAN), que são redes pessoais de curta distância; as Wireless Metropolitan Area Network (WMAN), que são redes que atendem a áreas metropolitanas; as Wide Area Network (WWAN), que estão no mesmo nível tecnológico que as WMANs, sendo que a diferença está apenas na sua área de abrangência. Na Figura 3, pode-se observar a abrangência dessas redes assim como as tecnologias envolvidas, conforme mostrado por Vleugels e Peeters (2010).

Figura 3: Tipos de redes sem fio.



Fonte: Vleugels e Peeters (2010).

4.1.1 Topologia

A topologia básica de uma rede sem fio pode ser vista na Figura 4, conforme informado por Kurose e Ross (2010). Nela, pode-se identificar os seguintes elementos de uma rede sem fio:

a) **Host (hospedeiro) sem fio.** Um hospedeiro sem fio pode ser um laptop, um smartphone ou um computador de mesa. Os próprios hospedeiros podem ser ou não móveis.

b) **Enlaces sem fio.** Um hospedeiro conecta-se a uma estação-base (definida logo em seguida) ou a um outro hospedeiro sem fio através de um enlace de comunicação sem fio. Existem diversos tipos de enlaces sem fio, cada um com suas características de taxas de transmissão, área de cobertura, etc.

c) **Estação-base.** A estação-base é parte essencial da infraestrutura de uma rede sem fio. Ela é responsável pelo envio e recebimento de dados (pacotes) de e para um hospedeiro sem fio que está associado a ela. Frequentemente, uma estação-base fica responsável pela coordenação da transmissão de vários hosts sem fio a ela associados. Estar associado a uma estação base significa que o hospedeiro está dentro do alcance de comunicação sem fio da estação-base e usa a estação-base para retransmitir os dados entre ele e a rede maior. No caso das WLANs, a estação-base é o AP (Access Point). Segundo Colcher et al. (1995), o ponto de acesso desempenha as seguintes funções:

– **Gerenciamento de potência:** permite que as estações operem economizando energia através de um modo chamado de *power save*.

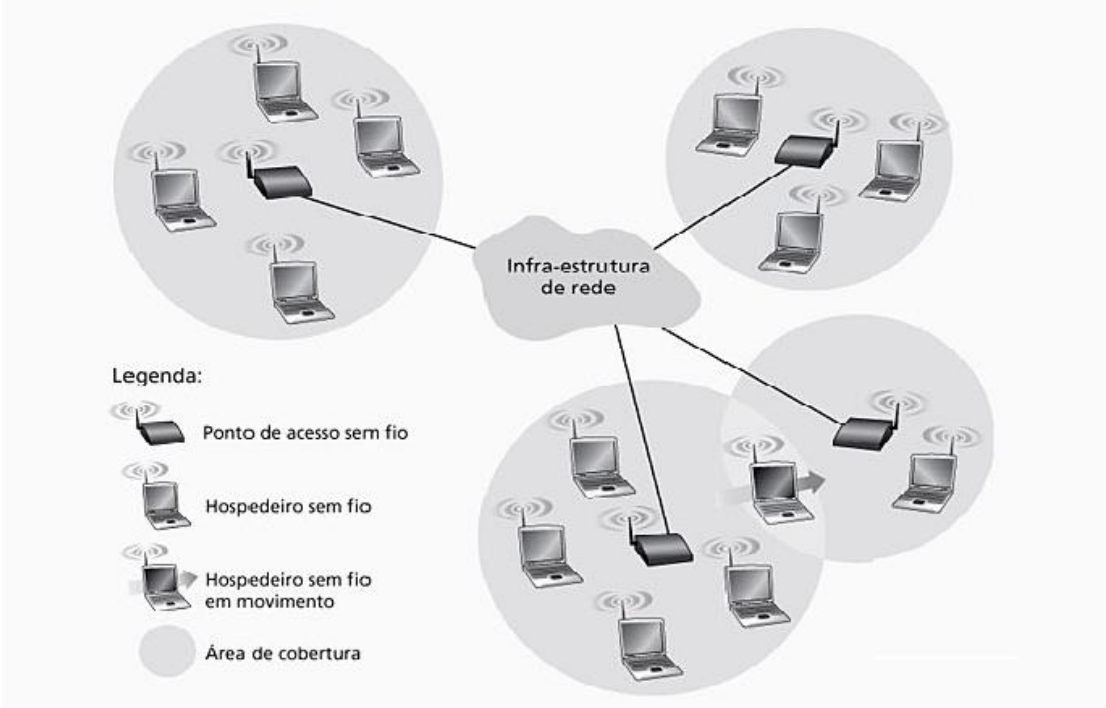
– **Sincronização:** garante que as estações associadas a um AP estejam sincronizadas por um relógio comum.

– **Autenticação, associação e reassociação:** permite que uma estação móvel, mesmo saindo de sua célula de origem continue conectada à infraestrutura e não perca a comunicação.

Quando um hospedeiro móvel se desloca para fora da faixa de alcance de uma estação-base e entra na faixa de uma outra, ele muda o seu ponto de conexão com a rede maior, isto é, muda o ponto de acesso com o qual está associado. Esse processo é denominado de *handoff* (transferência).

d) **Infraestrutura de rede.** É a rede maior com a qual um hospedeiro sem fio pode querer se comunicar, geralmente a internet.

Figura 4: Elementos de uma rede sem fio.



Fonte: Kurose e Ross (2010).

4.1.2 O Padrão IEEE 802.11

As Local Area Network (LAN) sem fio, ou WLANs, são uma das mais importantes tecnologia de rede de acesso à internet/intranet de hoje. Estão presentes nos mais diversos locais: em casas, universidades, cafés, aeroportos, esquinas, praças, e claro, em organizações militares da Marinha do Brasil. Conforme mencionado anteriormente, dentre os diversos padrões de rede sem fio desenvolvidos para WLANs o que mais se destacou foi o padrão IEEE 802.11, também conhecido como Wi-Fi (KUROSE; ROSS, 2010).

Existem diversas variações do padrão IEEE 802.11, entre eles os mais conhecidos são o IEEE 802.11a, o IEEE 802.11b, o IEEE 802.11g e o IEEE 802.11n. A Figura 5 ilustra um pequeno resumo desses padrões (KUROSE; ROSS, 2010).

Figura 5: Resumo de padrões IEEE 802.11.

Padrão	Faixa de frequência	Taxa de dados
802.11b	2,4-2,485 Ghz	até 11 Mbps
802.11a	5,1-5,8 Ghz	até 54 Mbps
802.11g	2,4-2,485 Ghz	até 54 Mbps
802.11n	2,4 GHz e 5 GHz	até 150 Mbps

Fonte: Adaptado de Kurose e Ross (2010).

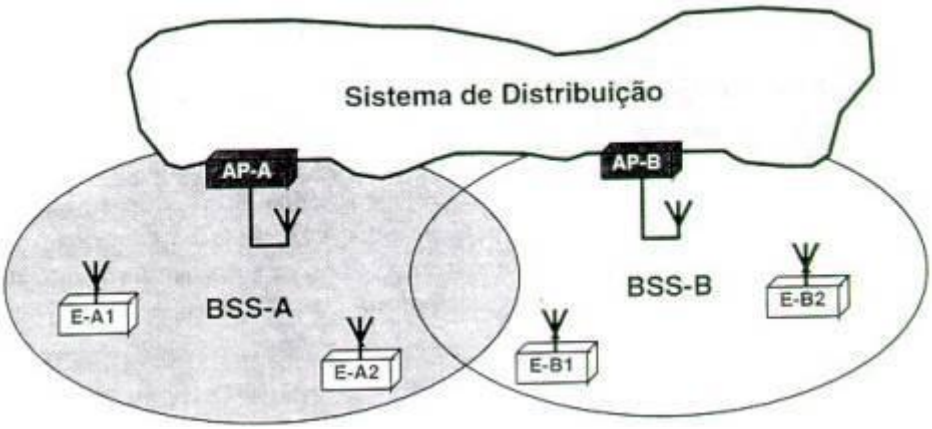
Conforme mostrado na Figura 5, o padrão 802.11b compete por espectro de frequência com telefones e fornos de micro-ondas de 2,4 GHz. Em frequências mais altas, as WLANs operando no padrão 802.11a podem funcionar com alta taxa de bits, entretanto a distância entre hospedeiro e ponto de acesso deve ser menor e, com isso, há uma influência maior dos múltiplos percursos (ALECRIM, 2013).

O padrão 802.11n tem como principal característica o uso de um esquema chamado de Multiple-Input Multiple-Output (MIMO) capaz de aumentar consideravelmente as taxas de transferência de dados por meio da combinação de várias vias de transmissão (antenas). Com isso, é possível usar dois, três ou quatro emissores e receptores para o funcionamento da rede, o que possibilita atingir taxas de 300 Mbps e 600 Mbps (ALECRIM, 2013).

O padrão 802.11 define uma divisão da área coberta pela rede em células. Essas células são comumente chamadas de Basic Service Area (BSA). O tamanho da célula depende das características do meio e da potência transmitida/recebida usado nas estações (ÉDIPO, 2010).

Na Figura 6, pode-se visualizar os principais componentes da arquitetura WLAN IEEE 802.11 (COLCHER et al., 1995):

Figura 6: Arquitetura da WLAN IEEE 802.11.



Fonte: Colcher et al. (1995).

a) **Basic Service Set (BSS).** É o bloco fundamental do padrão 802.11. Contém uma ou mais estações sem fio e um ponto de acesso. Na Figura 6 pode-se ver o AP-A no BSS-A e o AP-B no BSS-B.

b) **Ponto de acesso (AP)**. Como já mencionando, os APs são responsáveis pela captura das transmissões feitas pelas estações de sua BSA destinadas a estações localizadas em outras BSAs, retransmitindo-as usando um sistema de distribuição.

c) **Sistema de distribuição.** Interliga diversas BSAs para permitir a expansão da rede.

d) **Extended Service Area (ESA).** Representa a interligação de vários BSAs pelo sistema de distribuição através dos APs.

e) **Extended Service Set (ESS).** Representa um conjunto de estações formado pela união de vários BSSs conectados por um sistema de distribuição.

No padrão 802.11, cada dispositivo sem fio necessita se associar a um AP antes de poder enviar e receber quadros contendo dados de camada de rede. Ao instalar um AP, deve-se designar ao ponto de acesso um Service Set Identifier (SSID). Vulgarmente, o SSID é conhecido como o "*nome da rede*". Deve-se também escolher um número de canal para o AP. Dentro da faixa de operação do padrão IEEE 802.11b, por exemplo, definida entre 2,4 GHz à 2,485 GHz (faixa de 85 MHz) define-se 11 canais que se sobrepõem parcialmente. Para evitar essa sobreposição escolhe-se entre os conjuntos de canais 1, 6 e 11 (COLCHER et al., 1995).

Uma questão interessante que pode ser levantada é o modo como um dispositivo sem fio seleciona um AP a qual se deseja conectar num meio onde podem haver dezenas de pontos de acesso e, muito possivelmente, não pertencentes a mesma WLAN. O padrão IEEE 802.11 exige que o AP envie periodicamente quadros de sinalização, também chamados de *beacons*. Esses quadros de sinalização contêm o SSID e o endereço Media Access Control (MAC) do ponto de acesso. Dessa forma, o dispositivo em questão faz uma varredura dentre os 11 canais em busca desses beacons e mostra as redes disponíveis para o usuário de forma intuitiva. Pode-se agora escolher dentre os SSIDs listados para fazer a associação do dispositivo sem fio ao AP (KUROSE; ROSS, 2010).

Para que ocorra a associação entre o dispositivo sem fio e o AP é necessário que a estação se autentique. Há diversas formas para que isso ocorra, uma delas é permitir a associação através do endereço MAC de cada estação. Outra forma é solicitando um usuário e senha válidos. Em todos esses casos, é necessário que o AP se comunique com um servidor de autenticação, que é o real responsável por permitir ou não que à estação solicitante faça parte da rede (KUROSE; ROSS, 2010).

4.2 O DHCP

Atuando na camada de Aplicação da pilha TCP/IP, o Dynamic Host Configuration Protocol (DHCP) é utilizado pelos dispositivos que acessam a rede, cabeada ou sem fio, para obter informações sobre a configuração da mesma, como seu endereço IP, endereço IP do servidor Domain Name System (DNS)[2], o endereço IP do roteador, entre outros (RODRIGUES, 2015).

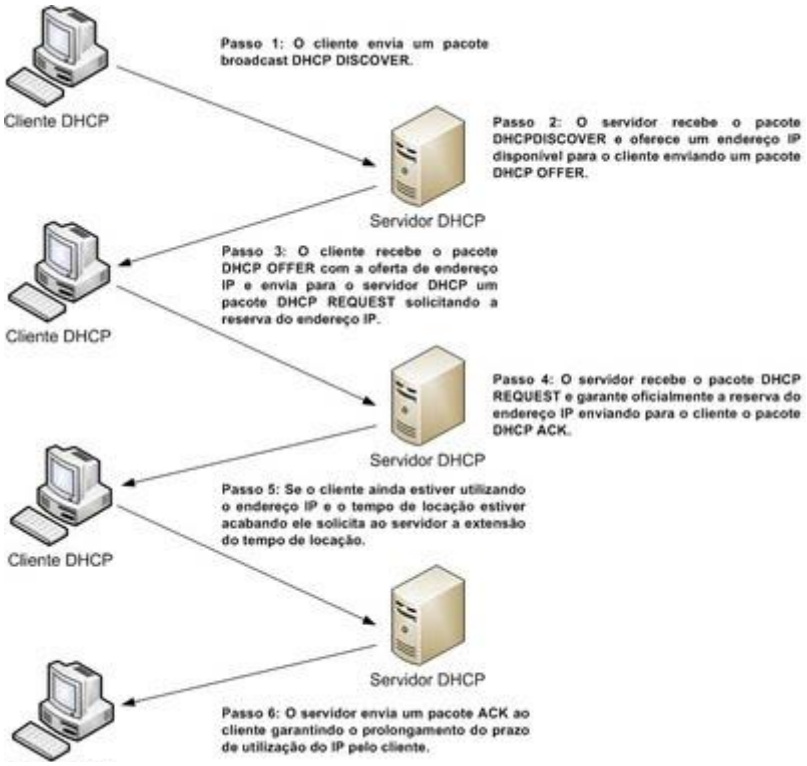
De uma forma bastante simplificada, o funcionamento normal de uma requisição DHCP é realizada da seguinte forma (RODRIGUES, 2015):

1) Determinado dispositivo acessa uma rede sem fio e necessita configurar suas informações próprias da referida rede (IP, DNS, gateway, etc). Essa máquina então, irá enviar um pacote DHCPDISCOVER usando o User Datagram Protocol (UDP) para o endereço de broadcast, ou seja, todos na rede receberão;
2) O servidor DHCP então, responde com um pacote DHCPOFFER, que oferece ao cliente as informações de configuração solicitadas;
3) Um pacote DHCPREQUEST é enviado ao servidor pelo cliente com a função de comunicar que aceita as informações oferecidas pelo servidor;
4) Enviando um pacote DHCPACK como resposta, o servidor confirma e registra as informações de configuração cedidas ao cliente.

[2] DNS é um sistema hierárquico e distribuído de gerenciamento de nomes para computadores, serviços ou qualquer máquina conectada à internet ou a uma rede privada. Realiza a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante. Em sua utilização mais convencional, associa nomes de domínios mais facilmente memorizáveis a endereços IP numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado resolução de nome (WIKIPÉDIA, 2018).

Na Figura 7, pode-se ver um resumo dos passos descritos.

Figura 7: Resumo de uma requisição DHCP.



Fonte: Rodrigues (2015).

Apesar de esse ser o funcionamento normal de uma requisição DHCP, um dispositivo malicioso que está na rede interna pode finge ser o servidor DHCP, ou seja, um Rogue DHCP Server que pode implementar um serviço de DHCP e fornecer parâmetros de configuração falsos para o dispositivo solicitante (SILVA, 2018).

O dispositivo malicioso responde a requisição do cliente e informa ser o roteador da rede e o servidor DNS, além de fornecer um endereço IP falso para cliente. O cliente não tem como saber que o dispositivo malicioso não é o verdadeiro servidor DHCP e confirma o recebimento da resposta e configura sua interface de rede adequadamente. O cliente rejeita qualquer outra resposta a sua solicitação (SILVA, 2018).

Uma vez que a vítima esteja dentro da rede sem fio falsa, o Rogue AP pode simular também ser um servidor DNS falso. Dessa maneira, quando o usuário realizar uma requisição web, a tradução de nomes é feita pelo servidor DNS falso e a vítima é direcionada para um servidor web falso que pode coletar informações sensíveis do usuário (SILVA, 2018).

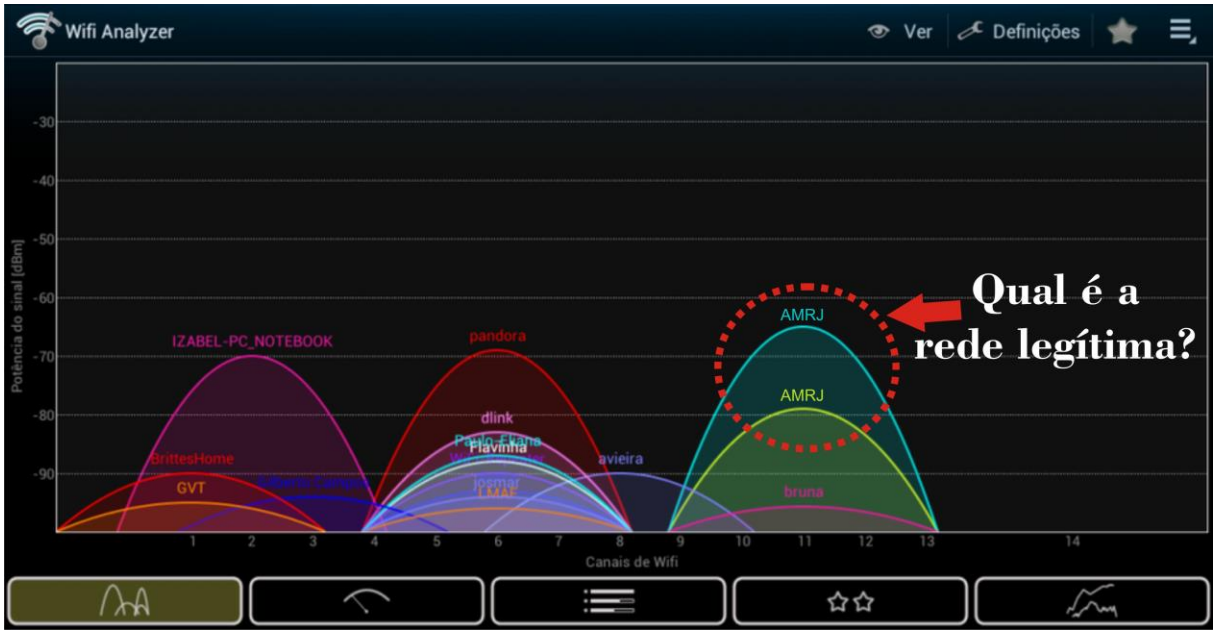
Além de poder ser direcionado para uma página web falsa, uma vez conectado na rede sem fio fornecida pelo Rogue AP, todo o tráfego da vítima é espionado pela entidade hostil (SILVA, 2018).

4.3 Rogue Acess Point

Como já mencionado, na técnica de ataque ao serviço de acesso à rede Wi-Fi Rogue Acess Point, o dispositivo malicioso procura forjar ser o acess point legítimo da rede verdadeira para induzir o usuário a se associar a rede falsa. O dispositivo mal-intencionado também finge ser um servidor DHCP para fornecer os parâmetros da rede falsa para a vítima. O objetivo principal é fazer o monitoramento do tráfego de rede da vítima que, necessariamente, passará pelo dispositivo malicioso (SILVA, 2018).

É extremamente difícil determinar qual o ponto de acesso legítimo da rede que se quer conectar. Com um simples aplicativo para smartphone é possível varrer o espectro de 2,4 à 5 GHz e encontrar as diversas redes sem fio disponíveis. Um exemplo pode ser visto na Figura 8, utilizando o aplicativo Wi-Fi Analyzer (WIFI ANALYZER, 2018).

Figura 8: Diversas redes sem fio sendo identificadas pelo aplicativo Wi-Fi Analyzer.



Fonte: Adaptado de Wi-Fi Analyzer (2018).

4.3.1 Medidas de proteção

Ao analisar a Figura 8 pode-se observar que existem duas redes sem fio com o mesmo SSID AMRJ. Contudo, apenas uma delas é a verdadeira rede do Arsenal de Marinha do Rio de Janeiro.

Infelizmente não há como o usuário ou seu dispositivo distinguir entre APs legítimos e forjados. Contudo, dentre os diversos métodos de controle de acesso, o mais indicado é o EAP, utilizado pelo padrão IEEE 802.1X, pois permite validar o certificado digital do servidor de autenticação da rede e usar criptografia. No entanto, se o Rogue AP usar um certificado digital emitido por uma Autoridade Certificadora (AC) legítima, o dispositivo aceitará o certificado sem contestar (SILVA, 2018).

Na verdade, apenas o provedor de serviço pode detectar e reagir contra Rogue APs. Contudo, essa ação requer uma infraestrutura de rede que implica em um significativo investimento, como a utilização de APs especiais e sistemas de monitoramento e de contra-ataque, conhecidos como *Wireless Intrusion Prevention System* (WIPS), que será discutido adiante (SILVA, 2018).

Outra forma de tentar mitigar o problema é sempre utilizar comunicação segura, Hyper-Text Transfer Protocol over SSL/TLS (HTTPS), entre cliente e o servidor (SILVA, 2018). Uma prática nem sempre adotada pelas organização militares da Marinha do Brasil (observação do autor).

4.3.1.1 O EAP

O Extensible Authentication Protocol (EAP) é um protocolo que possibilita que um usuário se autentique em um servidor específico a fim de receber mensagens provenientes do ponto de acesso. Este servidor trabalha com o uso do protocolo Remote Authentication Dial In User Service (RADIUS) e tanto pode ser representado pelo ponto de acesso quanto por uma outra máquina dedicada a este fim (PAIM, 2011).

O EAP possui basicamente quatro entidades:

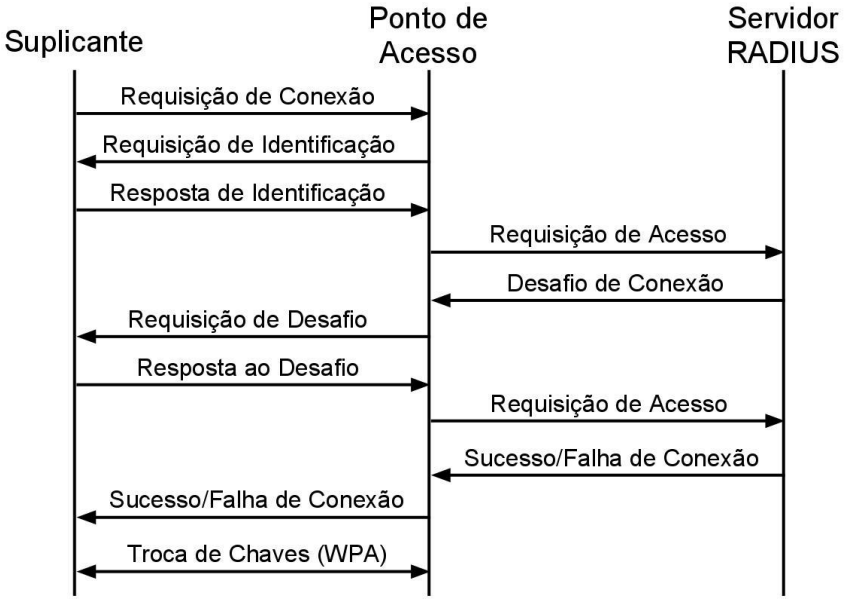
1) Autenticador: entidade que exige que a entidade na outra ponta do enlace seja autenticada;
2) Suplicante: entidade que é autenticada pelo Autenticador e que deseja acessar os serviços do Autenticador.

3) Port Access Entity (PAE): entidade de protocolo associada com uma porta. Pode suportar as funcionalidades do Autenticador, Suplicante ou ambos.
4) Servidor de autenticação: entidade que provê serviço de autenticação para o Autenticador. Pode fazer parte do Autenticador, mas normalmente é um servidor externo.

O EAP possui quatro tipos de mensagens básicas que são utilizadas durante o processo de conexão: Requisição, Resposta, Sucesso e Falha (PAIM, 2011).

O primeiro passo para a conexão em uma rede sem fio que utiliza o EAP é o envio de uma mensagem de Requisição para o AP. Este, por sua vez, retorna um pedido da identidade que o suplicante possui. Ao receber a resposta do suplicante o ponto de acesso a envia diretamente para o servidor RADIUS. O servidor, então, cria um desafio pelo qual o suplicante deve passar com o uso da senha que ele possui. Assim, caso este responda de maneira correta, terá acesso à rede sem fio; caso contrário, receberá uma mensagem de falha de conexão. Por fim, se o protocolo usado para encriptação for o Wi-Fi Protected Access (WPA) ou WPA2, ocorre o acordo entre o suplicante e o ponto de acesso a fim de decidir os valores de chaves temporais que serão usadas durante a comunicação. A Figura 9 apresenta uma versão simplificada deste processo (PAIM, 2011).

Figura 9: Diagrama de Autenticação EAP com Servidor RADIUS.



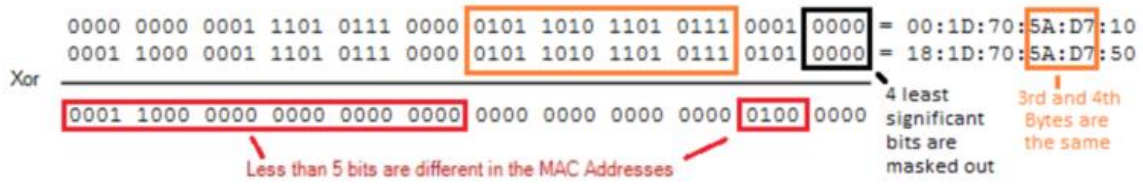
Fonte: Paim (2011).

4.3.1.2 WIPS

Para identificar um Rogue AP é necessária uma infraestrutura de WIPS em que todos os dispositivos possuem no mínimo duas antenas: uma para emitir e outra para monitorar continuamente o espectro de frequência. Os WIPS escutam os beacons 802.11 enviados por APs que estão visíveis[3]. Dessa forma, todos os Basic Service Set Identifier (BSSID)[4] identificados são listados e é possível fazer uma classificação dos Rogue SSID (HARRISON, 2017).

Para classificar um SSID como pertencente a um Rogue AP é necessário examinar os endereços MAC dos quadros da rede cabeada com os quadros recebidos pelo WIPS. Se o MAC da rede com fio e o BSSID forem iguais no terceiro e no quarto bytes do endereço MAC (geralmente os endereços MAC da LAN e da rede sem fio são contíguos) e o restante dos bytes diferirem por 5 bits ou menos, o AP será classificado como Rogue. Essa comparação é obtida aplicando uma operação XOR aos endereços MAC em formato binário, conforme mostrado na Figura 10 que indica um Rogue AP (HARRISON, 2017).

Figura 10: Operação XOR para determinar se BSSID pertence a um Rogue AP.

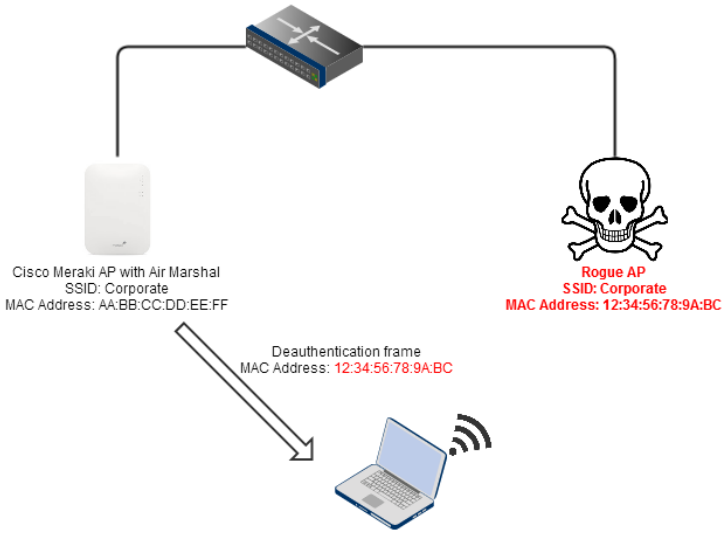


Fonte: Harrison (2017).

Com objetivo de proteger a infraestrutura corporativa de Rogue APs, o WIPS usa uma técnica chamada *contenção*. O WIPS basicamente pode transmitir quadros de desautorização 802.11. Ou seja, o WIPS falsifica o BSSID do AP falso e transmite uma desautorização 802.11 para o endereço MAC de broadcast (FF:FF:FF:FF:FF:FF). Resumidamente isso significa que o WIPS se passa pelo Rogue AP e informa a todos os clientes que estavam conectados ao AP falso e ao alcance do WIPS para se desconectarem, conforme pode ser visto na Figura 11.

[3] Visível, aqui, tem o sentido de estar no raio de alcance de uma antena.
[4] BSSID é o endereço MAC associado ao dispositivo transmitindo quadros de uma determinada rede sem fio, identificada por um SSID.

Figura 11: Rogue AP sendo alvo de “contenção”.



Fonte: Harrison (2017).

4.3.2 Como utilizar um Rogue AP

Existem diversas maneira de se implementar um Rogue AP. Contudo, já existem alternativas comerciais prontas que facilitam de sobremaneira ao atacante fazer uso dessa técnica para fins ilegais. A solução mais conhecida é o Wi-Fi Pineapple (WIFIPINEAPPLE, 2018). A imagem dos dispositivos comercializados pode ser vista na Figura 12.

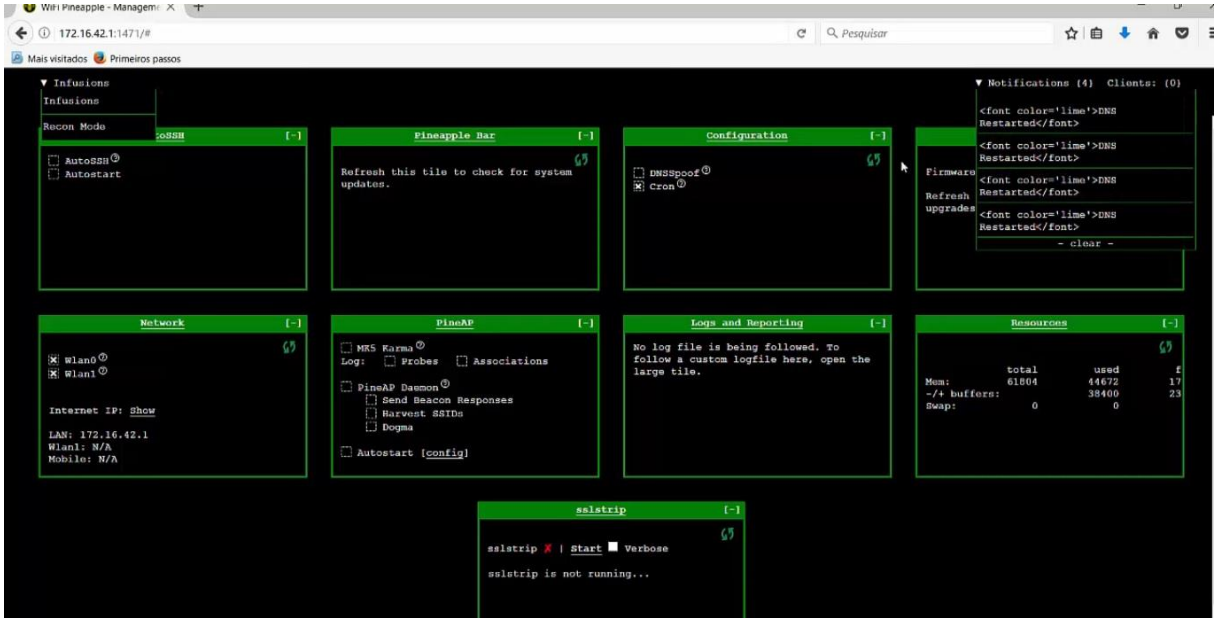
Apesar de ser vendida como uma alternativa para fins de auditoria de redes sem fio, um usuário mal-intencionado pode facilmente fazer uso do dispositivo para fins maléficos.

Figura 12: Wi-Fi Pineapple NANO ($100) e Wi-fi Pineapple TETRA ($200).

Fonte: Wifipineapple (2018).

Uma vez na interface web do Wi-Fi Pineapple, conforme pode ser visto na Figura 13, o usuário possui uma gama de opções e funcionalidades para explorar.

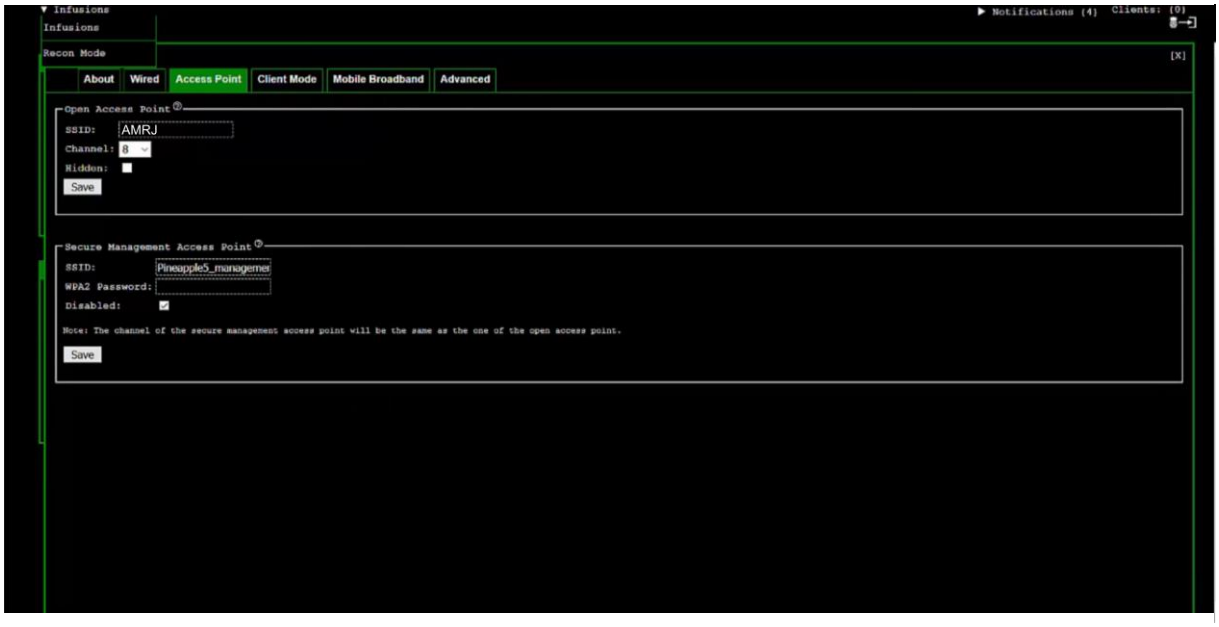
Figura 13: Interface web do Wi-Fi Pineapple.



Fonte: Wifipineapple (2018).

Indo na opção Network->Acess Point, o usuário pode configurar o SSID do Rogue AP, conforme pode ser visto na Figura 14. O importante aqui é definir o mesmo SSID da rede legítima.

Figura 14: Definindo um Rogue AP com SSID de nome AMRJ.

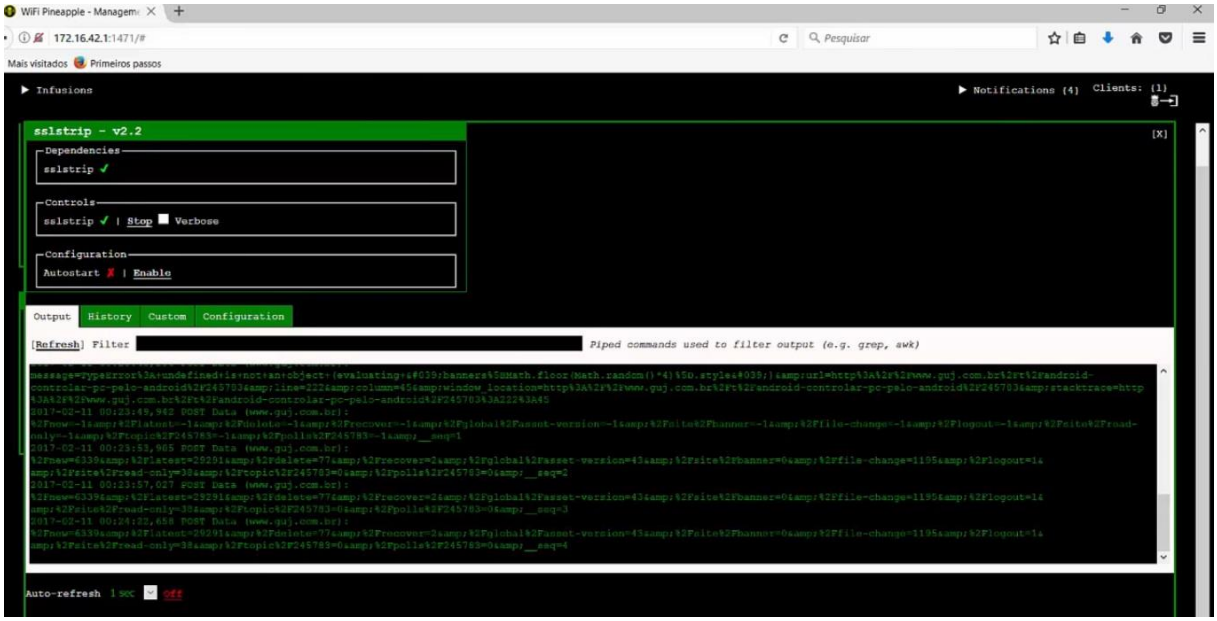


Fonte: Adaptado de Wifipineapple (2018).

Após realizar o procedimento descrito anteriormente, a rede AMRJ já estará disponível para acesso, competindo por usuários com a rede AMRJ legítima: se o sinal recebido da rede ARMJ falsa for mais intenso que o da rede legítima, muito provavelmente a conexão do usuário ocorrerá com o Rogue AP. Dessa forma, fica claro que o Rogue AP será mais eficiente quando este estiver distante do AP legítimo da rede.

Uma vez os usuários se conectando ao Rogue AP, pode-se utilizar a ferramenta sslstrip do Wi-Fi Pineapple para capturar todo o tráfego dos clientes, conforme pode ser visto na Figura 15.

Figura 15: Captura do tráfego do usuário através da ferramenta sslstrip do Wi-Fi Pineapple.



Fonte: Wifipineapple (2018).

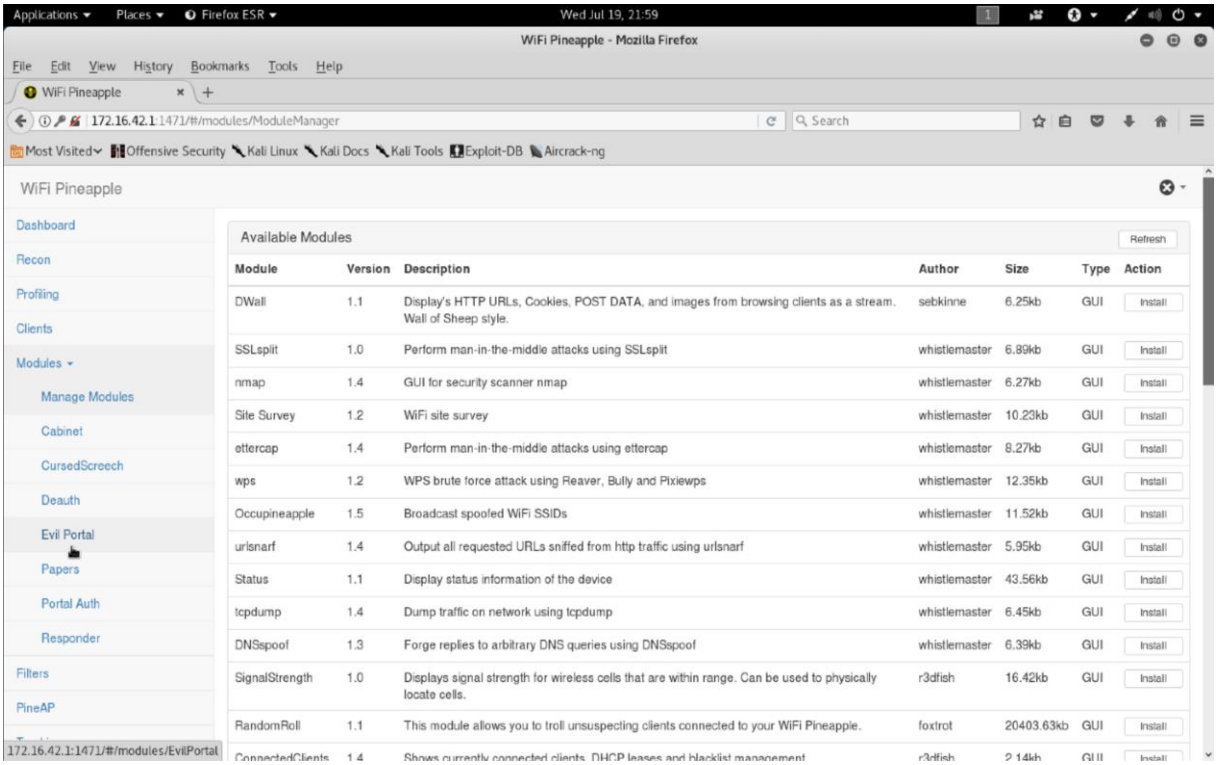
Usando o módulo ettercap do Wi-Fi Pineapple pode-se facilmente realizar um ataque de DNS Rogue e direcionar a vítima para um servidor DNS falso. Dessa forma, quando o usuário digitar em seu navegador o endereço do sistema web de pagamento da MB, por exemplo, será direcionado para uma página falsa e será vítima de phishing.

Em seguida, usando a ferramenta Evil Portal do Wi-Fi Pineapple, é possível criar uma página falsa do sistema de pagamento da MB e capturar as credencias de segurança do encarregado financeiro de uma organização militar.

A possibilidade de se instalar diversos módulos com centenas de funcionalidades no Wi-Fi Pineapple torna esse dispositivo extremamente flexível e de fácil utilização até para usuários menos experientes e com pouco conhecimento.

Um exemplo da diversidade de módulos disponíveis para o Wi-Fi Pineapple pode ser visto na Figura 16.

Figura 16: Exemplos dos diversos módulos que podem ser adicionados ao Wi-Fi Pineapple.



Fonte: Wifipineapple (2018).

5 CONCLUSÃO

Conforme foi possível demonstrar nesse trabalho, com pouco conhecimento técnico e a aquisição de um dispositivo relativamente barato, é possível criar um Rogue AP e capturar diversas informações dos usuários sem muito trabalho.

O fato de a priori a instalação de uma rede sem fio ser proibida pela administração Naval, dificulta, mas não impede por completo, a utilização dessas redes para fins maléficos, comprometendo os dados dos usuários e da própria RECIM.

Em se tratando de uma intuição militar, os dados trafegados pela rede sem fio são muitas vezes sensíveis e de carácter sigiloso, intensificando a necessidade de cautela na utilização dessas redes e da disseminação do conhecimento desse tipo de ataque para os usuários legítimos da rede.

É importante que os usuários tomem conhecimento da necessidade de nunca se conectar a um ponto de acesso desconhecido. Além do mais, todo o tráfego do usuário deve utilizar Transport Layer Security (TLS) na comunicação cliente-servidor, fato esse nem sempre observado, pois inúmeras páginas web da intranet da MB não utilizam comunicação segura.

Portanto, para mitigar o uso de Rogue AP, redes sem fio oficiais instaladas em organizações militares devem fazer uso de WIPS.

5.1 Sugestão para trabalhos futuros

A abordagem desse trabalho foi essencialmente teórica. Para trabalhos futuros, é importante realizar a aquisição de um Wi-Fi Pineapple pela administração Naval e realizar um ataque do tipo Rogue AP em uma OM de teste. O AMRJ, por ser uma organização militar de grande porte, com enorme concentração de pessoas e possuir uma rede sem fio para conexão dos navios docados à RECIM, seria um ambiente propício para utilização dessa técnica em campo.

Uma abordagem prática serviria para alertar os usuários da RECIM da enorme capacidade desse dispositivo e a necessidade constante de proteção, além de aumentar o nível do alerta situacional e da mentalidade de segurança dos militares e servidores civis da Marinha do Brasil no que se refere a utilização de redes sem fio.

REFERÊNCIAS

ALECRIM, E. **O que é wi-fi (IEEE 802.11)?** Disponível em: http://www.infowester.com/wifi.php#80211n, 2013. Acesso em 19 de maio de 2018.

APPLE. **Wi-fi e bluetooth: fontes potenciais de interferência sem fio**. Disponível em: http://support.apple.com/kb/HT1365?viewlocale=pt_BR, 2013. Acesso em 19 de maio de 2018.

BRASIL, Diretoria-Geral do Material da Marinha (DGMM). **Normas de Tecnologia da Informação da Marinha**. 2ª rev. Rio de Janeiro: MB, 2017.

_____, Estado-Maior da Armada (EMA). **Normas para a Salvaguarda de Materiais Controlados, Informações, Documentos e Materiais Sigilosos na Marinha.** 1ª rev. Brasília: MB, 2013.

_____, Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM). **DCTIMARINST Nº 30-13 (Uso de Redes Sem Fio na MB).** Rio de Janeiro: MB, 2014.

CERT.BR - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas Mantidas pelo CERT.br.** Disponível em: https://www.cert.br/stats/incidentes/. Acesso em 20 de fevereiro de 2018.

CORREIO 24 HORAS. **Novo ataque cibernético atinge empresas no Brasil; Hospital do Câncer suspende atendimentos**. Disponível em: http://www.correio24horas.com.br/noticia/nid/novo-ataque-cibernetico-atinge-empresas-no-brasil-hospital-do-cancer-suspende-atendimentos/. Acesso em 20 de fevereiro de 2018.

COIMBRA, T. R. **Regulação do espectro: Uso não licenciado**. http://www.teleco.com.br/tutoriais/tutorialespecradio/pagina_2.asp, 2006. Acesso em 19 de maio de 2018.

COLCHER, S.; SOARES, L. F. G. S.; LEMOS, G. **Redes de Computadores: Das Lans, Mans e Wans às Redes ATM**. Campus, 1995. Rio de Janeiro.

ÉDIPO, P. S. L. **Redes sem fio e redes móveis: Início e evolução.** Disponível em: http://lucianoedipo.wordpress.com/article/redes-sem-fio-e-redes-moveis-w98ptswyb0qd-3, 2010. Acesso em 19 de maio de 2018.

HARRISON, S. **Rogue Access Point**. Disponível em: https://meraki.cisco.com/blog/2017/09/rogue-access-point/. Acesso em 19 de maio de 2018.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: Uma abordagem top-down**. Pearson, 2010. São Paulo, trad. 5 ed. edição.

MÉDICE, Roney. **A importância da Segurança da Informação**: Visão Coporativa. 2013. Disponível em: https://www.profissionaisti.com.br/2013/07/a-importancia-da-seguranca-da-informacao-visao-corporativa/. Acesso em 19 maio de 2018.

MALEBRANCHE, H. **Metodologia do Estudo e Pesquisa**, 2017. 56 slides. Material apresentado para a disciplina MEP no Curso de Aperfeiçoamento Avançado Segurança da Informação e Comunicações do CIAW.

MITSHASHI, R. A. **Segurança de Redes**. Dissertação. FTSP. São Paulo, 2011.

O GLOBO. **Ataque cibernético atingiu 150 países e alcançou 200 mil alvos**. Disponível em: https://oglobo.globo.com/economia/ataque-cibernetico-atingiu-150-paises-alcancou-200-mil-alvos-21338738. Acesso em 20 de fevereiro de 2018.

_____. **Europa é alvo de ataque cibernético.** Disponível em: https://g1.globo.com/tecnologia/noticia/ucrania-e-empresas-da-europa-sao-alvo-de-ataque-cibernetico.ghtml. Acesso em 20 de fevereiro de 2018.

PAIM, R. R. **WEP, WPA e EAP**. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/eap.html. Acesso em 20 de maio de 2018.

POWER, R. **Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare**. Computer Security Institute. EUA, 1996.

RODRIGUES, B. **DHCP Starvation – Ataque de negação de serviço em rede local.** Disponível em: https://brenn0.wordpress.com/2015/01/24/dhcp-starvation-ataque-de-negacao-de-servico-em-rede-local/. Acesso em 20 de maio de 2018.

SILVA, Anderson O. **Fundamentos de Segurança da Informação**, 2018. 389 slides. Material apresentado para a disciplina FSI no Curso de Aperfeiçoamento Avançado Segurança da Informação e Comunicações do CIAW.

TANENBAUM, A. S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Elsevier, 2003.

VLEUGELS, K.; PEETERS, P. **Apparatus and method for integrating short-range wireless personal area networks for a wireless local area network infrastructure.** Disponível em: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US7826408.pdf, 2010. Acesso em 19 de maio de 2018.

WIKIPÉDIA. **Sistema de Nomes de Domínio**. Disponível em: https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio. Acesso em 20 de maio de 2018.

WIFI ANALYZER. **Site do desenvolvedor**. Disponível em: http://www.wifianalyzer.info/. Acesso em 21 de maio de 2018.

WIFIPINEAPPLE. **Pineapple Wireless Auditing Platform**. Disponível em: https://www.wifipineapple.com/. Acesso em 21 de maio de 2018.