ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

Bruno Souza do Nascimento Vicente

A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÕES

Resende
2022

	APÊNDICE III (TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL) AO ANEXO B (NITCC) ÀS DIRETRIZES PARA A GOVERNANÇA DA PESQUISA ACADÊMICA E DA DOUTRINA NA AMAN **TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL**	**AMAN 2022**

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

TÍTULO DO TRABALHO: A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÕES.
AUTOR: BRUNO SOUZA DO NASCIMENTO VICENTE.

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

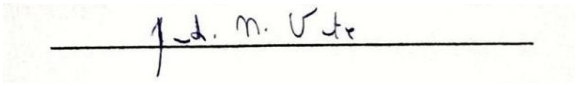
Autorizo a Academia Militar das Agulhas Negras a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulgá-lo por publicação em revista técnica da Escola ou outro veículo de comunicação do Exército.

A Academia Militar das Agulhas Negras poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou da Direção de Ensino da Academia Militar das Agulhas Negras.

Resende 3 Agosto de 2022



Bruno Souza Nascimento Vicente

Dados internacionais de catalogação na fonte

V633i VICENTE, Bruno Souza do Nascimento

A implementação de um servidor Radius para o incremento da segurança de redes sem fio em operações. / Bruno Souza do Nascimento Vicente – Resende; 2022. 45 p. : il. color. ; 30 cm.

Orientador: Anderson Henrique De Moura

TCC (Graduação em Ciências Militares) - Academia Militar das Agulhas Negras, Resende, 2022.

1.Segurança 2.Redes sem-fio. 3.Radius 4.Operações 5.Controle de acesso I. Título.

CDD**:** 355

Ficha catalográfica elaborada por Jurandi de Souza CRB-5/001879

A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÕES.

Monografia apresentado ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Orientador: Cap Com Anderson Henrique de Moura

Resende
2022

Bruno Souza do Nascimento Vicente

A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÃO.

Monografia apresentado ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Aprovado em 04 de JUNHO de 2022:

Banca examinadora:

Anderson Henrique de Moura, Capitão
(Presidente/Orientador)

Felipe Barcellos Brasil, Capitão

Júlio César Lacerda Do Nascimento, 1º Tenente

Resende
2022

DEDICATÓRIA

Dedico esse trabalho à Deus, por ter me abençoado com sabedoria e conhecimento, por ter me auxiliado para a conclusão dessa fase tão importante da vida. Também dedico à minha família, os quais bancaram meus estudos e me proporcionaram todo o apoio necessário para que eu me tornasse Oficial do Exército Brasileiro.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me ajudar nesse período árduo e longo de formação Acadêmica, por ter me abençoado com saúde e recursos para alcançar meus objetivos.

Agradeço aos meus pais, meus sustentáculos, dos quais me apoiaram em todas as minhas decisões e me orientaram sempre para meu bem.

Agradeço ao meu orientador, pela ajuda e disposição em me auxiliar e contribuir para que o resultado final desse trabalho de conclusão de curso fosse adequado.

Por fim, agradeço ao Exército Brasileiro pela oportunidade de fazer parte dessa instituição tão renomada e reconhecida no Brasil. Em especial à Academia Militar das Agulhas Negras pelo ensino oferecido com excelência tanto no conhecimento técnico científico quanto nos atributos da área afetiva.

RESUMO

A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÃO DO EXÉRCITO BRASILEIRO.

AUTOR: Bruno Souza do Nascimento Vicente.
ORIENTADOR:Anderson Henrique de Moura

Este trabalho visa executar a implementação de um servidor Radius para aumentar a segurança de redes sem fio, trazendo um serviço capaz de autenticar usuários para acesso de redes em operações. Nesse contexto, o trabalho esclarece a necessidade de segurança de redes sem fio, disponibiliza um tutorial de instalação e configuração de um servidor Radius, realiza a integração com serviços de DNS e o DHCP, apresenta as potencialidades desse servidor a partir da interface gráficaDaloRadius e por fim, promove a segurança da rede sem fio utilizando o software livre*Freeradius*. Nesta monografia, a utilização de livros, artigos e consultas com especialistas foramas principais fontes de levantamento de dados e consolidaram-se como metodologia do projeto. Como resultado, obteve-se com êxito a implementação do servidor Radius, o que aumentou a segurança de uma rede sem fio e comprovou-se a relevância do trabalho no que tange o controle de acesso, o projeto auxiliou na superação das vulnerabilidades de uma rede sem fio no que diz a respeito a autenticação de usuários e a importância da monografia, traduzido pelos questionários com especialistas da área. Por fim, concluiu-se queas redes sem fio em operação têm a necessidade de aprimoramento de segurança e que o referido projeto vem de encontro com essa demanda, sendo uma oportunidade de aprimoramento não apenas da segurança de redes sem fio, mas sim, de toda a operação.

Palavras-chave: Segurança. Redes sem fio. Radius. Operações. Controle de acesso.

ABSTRACT

THE IMPLEMENTATION OF A RADIUS SERVER FOR ENHANCING THE SECURITY OF WIRELESS NETWORKS IN OPERATION.

AUTHOR: Bruno Souza do Nascimento Vicente.
ADVISOR: Anderson Henrique de Moura

This work aims to perform the implementation of a Radius server to increase the security of wireless networks, bringing a service capable of authenticating users for network access in operations. In this context, the work clarifies the need for wireless network security, provides a tutorial for installing and configuring a Radius server, performs the integration with DNS services (which names all the IP addresses - hosts) and DHCP (server responsible for distributing the address ranges to the hosts), presents the potential of this server from the DaloRadius graphical interface and finally, promotes wireless network security using a Freeradius free software. In this monograph, the use of books, articles and consultations with experts were the main sources of data collection and were consolidated as the project's methodology. As a result, the Radius server was successfully implemented, which increased the security of a wireless network and proved the relevance of the work regarding access control, the project's help in overcoming the vulnerabilities of a wireless network regarding user authentication, and the importance of the monograph, translated by the questionnaires with experts in the field. Finally, it was concluded that wireless networks in operation have the need for security improvement and that this project meets this demand, being an opportunity to improve not only the security of wireless networks, but also the entire operation.

Keywords: Security. Wireless networks. Radius. Operations. Access control.

LISTADE FIGURAS

LISTADEABREVIATURAS E SIGLAS

Aseguir,todasasabreviaturasesiglasencontradasnestamonografia.Estasseapresentamem ordemalfabética,paramelhorvisualizaçãoe organizaçãodoleitor:

AAA	Authentication, Authorization and Accounting
AD	Active Directory
AMAN	Academia Militar das Agulhas Negras
AP	AccessPoint
BIND	BerkeleyInternet NameDomain
DHCP	Dynamic Host Computer Protocol
DNS	DomainNameSystem
EAP	ExtensibleAuthenticationProtocol
EPEX	Escritório de Projetos do Exército Brasileiro
ICS	Internet Connection Sharing
IETF	InternetEngineeringTaskForce
IP	InternetProtocol
LDAP	Lightweight Directory Access Protocol
MySQL	Structured Query Language
NAS	Network Attached Storage
OSI	Open System Interconnection
PHP	Hypertext Preprocessor
PPP	Pont-to-PointProtocol
PPPoE	Point Protocol over Ethernet
RADIUS	Remote Authentication Dial in User Service
RFC	Requestfor Comments
ROUTER	Roteador
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi ProtectedAccess

SUMÁRIO

1 INTRODUÇÃO

A tecnologia consolida-se diariamente como grande aliada do Exército Brasileiro para a realização de operações de diversos segmentos. Com agilidade e eficiência, tal ferramenta cresce em ritmo acelerado, haja vista que as novas gerações de pessoas possuem um viés facilitador para compreender os últimos avanços para o mundo da tecnologia.Com o crescimento tecnológico e consequentemente de pessoas conectadas, a segurança também deve crescer neste sentido.

Nesse contexto, as redes de computadores têm estado cada vez mais presentes nas Forças Armadas, sendo em ambientes internos como a projeção de um laboratório, quanto em atividades em campanha como em uma operação militar de grande porte. Conforme apresentado na Diretriz Geral do Comandante do Exército 2011 – 2014 (BRASIL, 2011a), a Ciência e Tecnologia (C&T) é fundamental para que a Força responda de forma eficiente às novas demandas.

De fato, em todos os lugares é possível observar as redes de computadores e quanto mais é explorado, maior é o número de vulnerabilidades que são descobertas e também exploradas. Quando foca-se dentro das Forças Armadas, mais em específico em atividades de campanha da área de comunicações, observa-se que muitas são as falhas de segurança e pontos sensíveis nas redes, principalmente se tratando de redes sem fio.

Uma grande vertente que necessita desta segurança são as redes *wireless*, recente cronologicamente, porém habitual em sua utilização, cuja infraestruturadispensa a utilização de cabos, o que facilita, mas a deixa mais suscetível, como se pode observar: “basta o usuário ligar seu equipamento sem fio ou notebook com placa wireless para que passe a ter acesso à Internet. No entanto, do mesmo modo que o acesso é facilitado para usuários legítimos, ele é facilitado também para possíveis hackers”. (Nakamura &Geus, 2007).

Em operações militares, a necessidade de segurança é ainda maior, pois muitas vezes se trata de informações sigilosas que trafegam nessa rede.Surge então a urgência de haver um sistema que reforce a segurança das redes em operações militares, alguma ferramenta, protocolo e doutrina que forneça a confiabilidade necessária para o tráfego de informações. Além disso, fornecer também potencialidades para registro de informações em caso de perda, como um serviço de backup e serviço de logs.

Buscando soluções para ampliar a segurança de redes sem fio em operações, destaca-se a proposta do referido trabalho, a implementação de um servidor *Radius* para o incremento da segurança. Uma ferramenta de simples utilização e configuração, que uma vez instalada e corretamente ajustada, fornece ao administrador de rede diversos caminhos para melhor controlar o acesso à rede, cadastrando usuários e fornecendo o controle necessário.

É essencial recomendar que todas as organizações militares sejam protegidas de ameaças. O conhecimento contigo neste espaço, proporcionará formas de defesa contra estes ataques com uma implementação positiva e benéfica disponível pelo autor.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Implementar um servidor *Radius* em uma rede de computadores simulada à operações militares de forma a complementar a segurança de redes sem fio.

1.1.2 Objetivo específico

Esclarecer a necessidade de segurança de redes sem fio em operações militares.

Instalar e configurar apropriadamente um servidor Radius.

Estabelecer a integração de um servidor *Radius*com o serviço de DHCP e DNS.

Realizar a gestão de usuários de uma rede sem fio a partir de um servidor *Radius*, a partir da interface gráfica DaloRadius.

Apresentar as funções básicas da interface de gerenciamento DaloRadius.

2 REFERENCIAL TEÓRICO

2.1 RADIUS

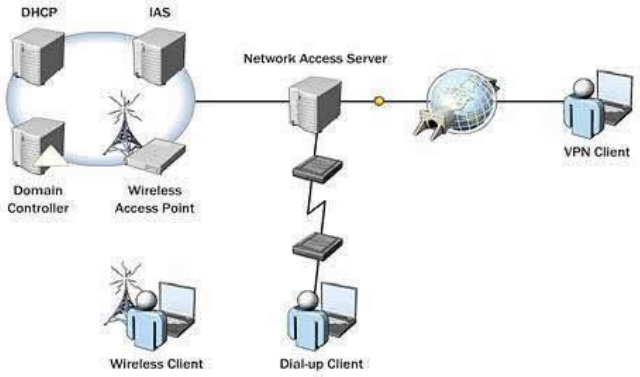
Remote Authentication Dial In UserSerivice(*RADIUS*), é um protocolo de autenticação (no contexto deste trabalho, também exercerá a atribuição de servidor/serviço). Inventado*pela Livinston na* metade dos anos 1990, a qual a*Internet EngineeringTask Force(IETF)* padronizou em 1996 na *Request for Comments (RFC)* 2139, visa executar a autorização e gestão de usuários, para acesso à rede ou serviços de rede. Baseia-se numa rede cliente/servidor. Esta ferramenta verifica a identidade digital do usuário de rede, permitindo com que o serviço conceda acesso autenticado aos usuários autorizados.

Após a autenticação, são determinados quais são os privilégios que o usuário está autorizado, nesse momento, é registrado o acesso deste no serviço *Radius*para que haja uma melhor gestão do controle de acesso aos recursos disponibilizados por esta ferramenta.

De acordo com o livro Segurança em Redes – Fundamentos, escrito pelo engenheiro da computação Alexandre Fernandes de Moraes, são características do serviço *Radius*:

> • Baseia-se no modelo cliente servidor, desta forma um mesmo servidor *RADIUS* pode ser utilizado para atender vários NAS ou clientes na rede ao mesmo tempo.
>
> • Um servidor *RADIUS* pode servir de Proxy para a autenticação em outros servidores *RADIUS*.
>
> • Autorização: existem mais de 50 opções no *RADIUS* que podem ser utilizadas para criar regras de filtragem NAS ou em outros equipamentos clientes *RADIUS*, possibilitando desta forma autorizarmos ou negarmos alguns tipos de acessos de usuários.
>
> • Auditoria e contabilidade: além da autenticação e autorização, o servidor *RADIUS* permite a contabilidade do acesso do usuário, ou seja, dados sobre a sessão do usuário são armazenados e contabilizados. Quando um usuário inicia uma sessão na rede, essa informação é passada ao servidor *RADIUS* por um pacote inicial. Quando termina, outro pacote informa que a sessão foi terminada e a quantidade de bytes trocados durante ela.
>
> • Vários equipamentos e dispositivos de rede podem ser cliente *RADIUS*, como roteadores, servidores, firewalls e switches de rede. (MORAES, 2008, p.65).

Figura 1 – Diversas ligações do servidor Radius



Fonte: Elements of a Network Access Infrastruture, 2009

2.2 STRUCTURED QUERY LANGUAGE (MYSQL):

Para que haja êxito neste projeto, é indispensável a utilização de um banco de dados para armazenamento de informações dos usuários e controle geral das aplicações que permitirão acesso a seus interessados. Para tanto, foi utilizado de um sistema de gerenciamento de banco de dados, conhecido por *MySQL*. Este sistema, criado na Suécia por David Axmark, Allan Larsson e Michael Widenius, permite "a fácil integração com o *Personal Home Page* (PHP). O *MySQL* é incluído, quase obrigatoriamente, nos pacotes de hospedagem dos sites da Internet oferecidos atualmente" (ABREU, Mauricio Pereira de; MACHADO, Felipe Nery Rodrigues. *Projeto de Banco de Dados:* Uma Visão Prática, 2009, p. 290).

A grandeza desta aplicação se consolida por: diversas empresas utilizam-se do *MySQL* para suas respectivas aplicações internas de banco de dados. Este, por sua vez, tem como principal característica a utilização do código aberto e, por ser um banco de dados relacional(que modela os dados de uma forma que eles sejam percebidos pelo usuário como tabela), permite que inúmeras pessoas desenvolvam projetos em diversos segmentos, como por exemplo, o *Radius*. A finalidade do *MySQL* consiste em armazenar usuários, função esta que está interligada com o servidor *Freeradius*, por meio da aplicação *DaloRadius*.

2.3 OVERVIEW DE FERRAMENTAS *(FRONTENDS):*

Abaixo, uma visão geral da ferramenta de possível utilização para o desenvolvimento do projeto que se interligam com o*Freeradius*.

-**DaloRadius**: Esta ferramenta está integrada ao servidor *Radius* e é disponibilizada a seus usuários por meio de uma plataforma web. Nela, existe a gestão de usuários, criação de relatórios, geo-localização e a área de *accouting*.

2.4 DOMAIN NAME SYSTEM (DNS):

Ao falar de integração na rede, é necessário que haja nomes para seus respectivos domínios. Inevitavelmente, praticidade e organização devem ser desenvolvidas em qualquer atividade computacional. O servidor *DNS* concede a oportunidade de digitar determinado nome, evitando assim, a necessidade de recordar do endereço *IP* a todo o momento em que estiver acessando determinado conteúdo.

Encontra-se, no livro Linux – Guia do administrador do sistema, de Rubem E. Ferreira, a seguinte definição:

> *DNS* é o serviço responsável por traduzir nomes em endereços *IP* (e vice-versa) de um determinado domínio internet. No Linux/Unix, o serviço DNS é implementado pelo software BIND. O BIND trabalha na arquitetura cliente-servidor. O resolvedor (resolver) é o cliente que faz perguntas sobre um determinado computador. O servidor de nomes (*nameserver*), implementado pelo *daemonnamed* no *BIND*, é o processo que responde às perguntas. (FERREIRA, 2008, p.441)

Neste trabalho, a função do *DNS* será de nomear todos os *hosts*, facilitando o gerenciamento do administrador, bem como o funcionamento geral da rede.

2.5 DYNAMIC HOST COMPUTER PROTOCOL (DHCP)

Mecanismos de praticidade nos serviços de rede são indispensáveis nos dias atuais. Em um ambiente de redes, requerem-se a todo instante a excelência na prestabilidade das funções, bem como procurar caminhos alternativos visando a ausência de falhas. Para isso, existe o servidor *DHCP*. Encontra-se, no livro Linux – Guia do administrador do sistema, de Rubem E. Ferreira, a seguinte definição:

> [...] tem como função principal fornecer (alugar) um endereço *IP* dinamicamente a um computador no momento de sua conexão à rede. O servidor de *DHCP* verifica qual o endereço *IP* disponível numa faixa cadastrada previamente em uma tabela dentro deste e informa ao solicitante esse endereço, tornando-o indisponível para outras solicitações. (FERREIRA, 2008, p.459).

Este protocolo consolida-se cada vez mais como solução eficiente para combater empecilhos como este, pois, de tal modo, toda aplicação desenvolve-se automaticamente, haja vista que este serviço em pequenas redes facilmente são executados, mas em grandes redes de computadores, as chances de falhas são maiores. Vale ressaltar que, com a aplicação automática do *DHCP*, não existirão problemas de conflito de rede, pois “quando a máquina solicitante sai da rede, o serviço *DHCP* torna o endereço *IP* dessa máquina disponível novamente”. (FERREIRA, 2008, p.459).

2.6 ROUTER

Com o avanço tecnológico e a alta demanda de serviços que as redes de computadores proporcionam a seus profissionais, deve-se ter ao alcance, ferramentas que permitam executar do melhor modo possível a interligação dos ambientes de rede: tal atribuição corresponde ao roteador, pois este dispositivo interliga diversas redes distintas. Seu objetivo é definir o melhor caminho para que os pacotes de dados trafeguem, proporcionando que os dados cheguem ao seu micro após passar por diversos roteadores.

O site Guia do Hardware indica que "roteadores vão desde PCs comuns com duas ou mais placas de redes compartilhando a conexão com a Web através do ICS do Windows ou outro proxy qualquer, a até grandes roteadores", em que estes são "capazes de unir os *backbones* da Internet e encaminhar milhões de pacotes de dados por segundo".

Encontramos, no livro Segurança em Redes – Fundamento, de Alexandre Fernandes de Moraes, a seguinte definição:

> São os equipamentos que trabalham na camada de rede do modelo OSI, camada 3, roteando os pacotes entre as redes. Os roteadores executam, além do roteamento, algumas tarefas essenciais da rede, como servir de filtro isolando protocolos não roteáveis e o tráfego de broadcast, evitando que eles se propaguem entre as redes. (MORAES, 2010, p.130).

O referido livro informa que os roteadores "são equipamentos essenciais também para garantir a segurança das redes, além de atuarem como filtros de pacotes indesejáveis". Neste mesmo segmento, "os roteadores de nova geração trabalham como um *Firewall StatefullInspection*, protegendo as redes de invasores".

2.7 PROTOCOLOS DE SEGURANÇA

2.7.1 Rede sem fio

Nos últimos anos, houve um grande crescimento na utilização de WLANs, principalmente, as baseadas nos padrões da família IEEE 802.11. Pensando em segurança, foi introduzido um protocolo denominado WEP (*WiredEquivalentPrivacy*). De acordo com Linhares e Gonçalves:

> O intuito desse protocolo era oferecer às WLANs IEEE 802.11 um nível de privacidade equivalente ao das redes locais (LANs – Local Area Networks) Ethernet. Uma LAN geralmente está protegida por mecanismos de segurança físicos (controle de acesso à salas, prédios, etc) que são eficazes em uma área física controlada. Contudo, essa abordagem não é efetiva para as WLANs, pois as ondas de rádio usadas para a comunicação não ficam necessariamente confinadas pelas paredes da área onde se encontram os dispositivos que compõem a rede. Usando criptografia de dados, o WEP consegue uma proteção similar à oferecida por mecanismos de segurança físicos. A criptografia de dados protege as informações

> que irão transitar pelo canal de comunicação entre o ponto de acesso e os clientes (e vice-versa).(LINARES; GONÇALAVES; 2010; p. 1-2).

Com a evolução, o protocolo foi atualizado e substituído por outros:

> Diversas pesquisas demonstraram problemas significativos de segurança no padrão IEEE 802.11. Em 2003, o WEP foi então substituído pelo WPA (Wi-Fi Protected Access) que por sua vez, devido a algumas falhas de implementação, foi substituído, em 2004, pelo padrão IEEE 802.11i ou WPA2.(LINARES; GONÇALAVES; 2010; p. 1-2).

2.7.2 WiredEquivalentPrivacy (WEP)

No livro Segurança em Redes – Fundamento encontra-se as seguintes diretrizes para o protocolo:

- Fornecer confidencialidade aos dados por meio de um algoritmo criptográfico de chave simétrica;
- Eficiente e confiável;
- Livre exportação;
- Todavia, estudos realizados pela Universidade de Berkeley na Califórnia e pela Universidade de Maryland provaram a existência de problemas envolvendo a segurança do WEP. (MORAES, 2010, p.251).

2.7.3 WI-FI ProtectAccess (WPA)

Em busca de um protocolo mais seguro nasceu o WPA, de acordo com Linhares e Gonçalves:

> Tendo em vista o grande número de vulnerabilidades apresentadas pelo protocolo WEP, um grupo de trabalho do IEEE 802.11 iniciou pesquisas para o desenvolvimento de um novo padrão de segurança denominado IEEE 802.11i. O intuito primordial era resolver todos os problemas de segurança encontrados no WEP. Enquanto o padrão estava sendo desenvolvido, a Wi-Fi Alliance11, para responder às críticas geradas pelo meio corporativo em relação ao WEP, apresentou em 2003 um padrão denominado Wi-Fi Protected Access (WPA). (LINARES; GONÇALAVES; 2010; p. 8).

Encontramos, no livro Segurança em Redes – Fundamento, de Alexandre Fernandes de Moraes, as seguintes nomeações para o protocolo:

> • WPA Personal: Usa uma chave preestabelecida, que deve ser configurada no *access point* e nas estações para a troca de chaves.
> • WPA Enterprise: É um protocolo de autenticação, que se baseia na utilização EAP (ExtensibleAuthenticationProtocol).(MORAES, 2010, p.251).

2.7.4 WI-FI Protect Access2 (WPA2)

Neste trabalho, utiliza-se a versão mais atualizada do prototocolo WPA, o WPA2:

> O padrão IEEE 802.11i, homologado em junho de 2004, foi desenvolvido com o objetivo de prover mais segurança na comunicação, visto que o protocolo de segurança então utilizado (WEP) apresentava diversas vulnerabilidades. O novo método de criptografia utilizado exige um maior poder computacional do NIC (Network Interface Card) durante o processo de codificação/decodificação,

> impossibilitando assim, apenas uma atualização de firmware. Os principais avanços do WPA2 em relação ao WPA são, basicamente, novos algoritmos de criptografia e de integridade. (LINARES; GONÇALAVES; 2010; p. 8).

2.8 ACCESS POINT

Com o advento da tecnologia, pontos de acesso estão se tornando extremamente populares e presentes no cotidiano da sociedade. A Rede *Wireless* oferece praticidade para seus usuários, justamente por não necessitar de uma estrutura cabeada.

Access Point (ponto de acesso, em português), consolida-se como um dispositivo que realiza a interconexão entre um ou vários dispositivos móveis, sendo possível também a ligação entre redes sem fio e redes cabeadas. Estes pontos de acesso se estabelecem por meio de roteadores ou pequenos modens, promovendo conexão à internet, sejam para pequenas ou grandes áreas. Há a possibilidade destes pontos de acesso estabelecer em grandes conexões, como por exemplo, a rede de acesso a Internet da Universidade de Taubaté: a área universitária (departamentos) é subdividida em áreas menores, sendo cada uma delas cobertas por um ponto de acesso. Entretanto, por mais que ocorram melhorias neste sentido, a vulnerabilidade cresce exponencialmente. Para tanto, surgiram duas aplicações: *WPA* e *WPA2*.

2.9 O QUE É E PARA QUE SERVE UMA REDE DE AUTENTICAÇÃO?

Encontra-se no livro Segurança em Redes, de Alexandre Fernandes de Moraes, a seguinte definição:

> Autenticação é o processo que determina se alguma pessoa, ou algo, é realmente quem diz ser. Os processos de autenticação são extremamente comuns em redes de domínio público, como a Internet, e em redes privadas (ambientes corporativos). Existem vários métodos de autenticação, todos baseados em três linhas diretas, “autenticação por algo que você sabia, autenticação por algo que você tenha e autenticação por algo que você seja”. (MORAES, 2008, p.47)

Os sistemas de autenticação foram pensados para confirmar se o usuário é autêntico, realizar a autorização e principalmente, a auditoria. Essas soluções ficaram conhecidas como *Authentification, AuthorizationandAccounting*(AAA). São vastamente utilizadas tanto na internet, no processo de controle de autenticação, como nas empresas de forma a controlar e contabilizar os acessos dos usuários a rede e as informações. Em geral, os equipamentos de rede, como servidores de acesso remoto e roteadores, trabalham com protocolos e soluções *AAA*.

O processo de autorização dentro da solução *AAA* define os direitos e serviços que o usuário poderá acessar na rede, o que pode incluir a definição do endereço *IP* do usuário e a aplicação de filtros que delimitam as aplicações e protocolos suportados para usuário.

2.10 BACKUP

Backup é um termo inglês que significa cópia de segurança. Para mostrar ao usuário da rede a existência de cópia de um ou mais arquivos guardados em seu repositório de armazenamento, utiliza-se deste termo na informática. Segundo Neto et al (2012, p.2) o backup pode ser definido como "cópia de segurança dos dados de determinado dispositivo de armazenamento que pode ser espelhado em outro dispositivo de forma a garantir a estabilidade dos arquivos e afastar a possibilidade de surpresas como a perda desses dados."

No entanto, seu grande benefício é a recuperação destes dados que, por ventura, venham a ser extraviados e/ou excluídos, seja por vírus, por engano, etc. Assim, o conteúdo original do arquivo que se perdeu, terá uma cópia que o dispositivo de armazenamento assim providenciará.As informações são cada vez mais importantes no dia-a-dia de todas as pessoas e empresas, e essas informações têm de aparecer para a pessoa certa na hora certa, sem que esteja corrompida ou inutilizável, e para isso são utilizadas algumas ferramentas como o backup (FONTES, 2012).

2.11 O QUE É UMA OPERAÇÃO MILITAR?

No Manual de Operações EB70-MC-10.223 do Exército Brasileiro, encontra-se a seguinte definição:

> Operação militar é o conjunto de ações realizadas com forças e meios militares, coordenadas em temo, espaço e finalidade de acordo com o estabelecido em uma diretriz, plano ou ordem para o cumprimento de uma atividade, tarefa, missão ou atribuição. É realizada no amplo espectro dos conflitos, desde a paz até o conflito armado/guerra, passando pelas situações de crise, sob a responsabilidade direta de autoridade militar competente. (Ministério da Defesa, 2017, p.8)

De acordo com essa definição, a operação militar será aquela que cumpre um objetivo específico. E é nesse contexto que se apresenta a necessidade de segurança das comunicações: acesso a redes de computadores.

2.12 IMPORTÂNCIA DA SEGURANÇA DAS REDES SEM FIO EM OPERAÇÕES.

A importância da segurança de redes sem fio é uma pauta crescente, com o crescimento de ataques cibernéticos em empresas, sites e personalidades da política, por exemplo, em operações militares não poderia ser diferente.

É importante constatar que em uma rede de computadores, todos os sistemas são interligados, ou seja, um servidor DHCP trabalha em conjunto com um servidor DNS e ambos trabalham ao mesmo tempo que um servidor *Radius* e um servidor web. Tal simultaneidade é

um facilitador de gerência e sinônimo de integração, contudo também é um complicador, pois um ponto de vulnerabilidade pode comprometer todo o sistema.

Em geral, a rede sem fio é um ponto visível e qualquer indivíduo por meio de um aparelho móvel, por exemplo, tem a possibilidade de encontrá-la, o que as torna mais vulnerável. Esse ponto de acesso pode ser também a entrada para toda rede de computadores, isso faz com que a sua segurança seja ainda mais importante.

De acordo com a portaria nº 004-DCT, 31 janeiro de 2007 do Departamento de Ciência e Tecnologia – Instruções Reguladoras Sobre Segurança Da Informação Nas Redes De Comunicação e de Computadores Do Exército Brasileiro IRESER – (IR 13-15), encontra-se o seguinte artigo:

> Art. 68. As redes sem fio são categorizadas conforme a abrangência da área de cobertura, cada qual com requisitos de segurança próprios, desta forma todas as soluções a serem adotadas para uso na Força devem ser previamente preparadas de tal modo que as configurações de segurança sejam adequadamente ajustadas, em particular, os aspectos de identificação e autenticação do usuário e da criptografia dos dados. (Departamento de Ciência e Tecnologia, 2007, p. 17-18).

Tal artigo vem para ressaltar a necessidade de preparação e adequação dos requisitos de segurança para o uso de redes sem fio. Além disso, o artigo 68 ainda abrange um ponto que vem ao encontro com o deste trabalho, que são os aspectos de identificação e autenticação do usuário.

2.13 O CRESCIMENTODA CIBERNÉTICANO EXÉRCITO BRASILEIRO.

A presente monografia aborda diversos assuntos interdisciplinares, como conhecimentos de informática, redes de computadores, emprego tático no que se trata de operações militares e o mais evidente, cibernética. Dessa maneira, fazer a avaliação e identificação do crescimento da cibernética no Exército Brasileiro enriquece a monografia.

De acordo com o site oficial do Escritório de Projetos Estratégicos do Exército a cibernética cresceu de importância a partir de 2009, assim como citado nos parágrafos abaixo.

O Governo Brasileiro publicou, em dezembro de 2008, na Estratégia Nacional de Defesa (END), estabeleceu o Setor Cibernético como um dos três setores de importância estratégica para a Defesa do País. Atendendo a determinação do Ministério da Defesa, o Exército Brasileiro (EB), em 2009, instituiu o Setor Cibernético no âmbito da Força Terrestre.

> Nasceu, nesse momento, o Projeto Estratégico de Defesa Cibernética. Quando da criação desse Projeto, logo se percebeu a necessidade da existência de um órgão que fosse encarregado de exercer a governança, de forma colaborativa, entre os vetores naturalmente vocacionados para compor a defesa no campo cibernético. Essa necessidade foi atendida com a criação, em 2010, do Centro de Defesa Cibernética (CDCiber). As premissas de trabalho deste novo órgão são coordenar e integrar os esforços dos vetores da Defesa Cibernética. Para atuar neste segmento tão específico, iniciou-se, entre outras atividades, o processo de capacitação de recursos humanos, possibilitando o domínio de temas multidisciplinares. Especial enfoque foi destinado ao desenvolvimento de doutrina de proteção dos próprios ativos, bem como na capacidade de atuar em rede, na de implementar pesquisa científica voltada ao tema e na indução da capacidade tecnológica nacional. (EPEX, 2020)

O Programa Estratégico do Exército de Defesa Cibernética possui atualmente seis projetos estruturantes, para potencializar a capacidade cibernética do país. O programa visa além de atender mais de 50 organizações militares ligadas a área, quer proporcionar defesa para as redes operacionais da Força Terrestre. (EPEX, 2020)

O crescimento da cibernética não se limita ao campo das Forças Armadas, ele também é acelerado no setor privado. Principalmente no setor de cibersegurança, o resultado é expressivo: o aumento na demanda por cibersegurança se traduz nos resultados do setor. Em 2020, o mercado de segurança da informação faturou US$ 156,2 bilhões no mundo, e deve alcançar US$ 352,2 bilhões em 2026, como mostra um levantamento da consultoria *MordorIntelligence*.

Dentro desse contexto, as redes sem fio também se destacam. Uma pesquisa realizada pela Deloitte, afirma que o ecossistema em torno das tecnologias sem fio avançadas é multifacetado, fluido e em constante crescimento. (DELOITTE, 2021)

2.14 CRESCIMENTO DOS ATAQUES CIBERNETICOS NO BRASIL.

Uma realidade no Brasil hoje são os ataques cibernéticos. Com o aumento da tecnologia, ao acesso a informação e à expansão da acessibilidade a internet, hoje tem se tornado cada vez mais comuns ataques cibernéticos, tanto em pessoas físicas quanto às instituições públicas e privadas, um exemplo disso foi o ataque ao aplicativo do ministério da saúde no início do ano de 2022 que o deixou indisponível por vários dias.

O Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021, um aumento de mais de 950% com relação a 2020 (com 8,5 bi), segundo a Fortinet. Em escala global, esse número é ainda maior, segundo Arturo Torres que é estrategista de segurança cibernética do FortiGuardLabs da Fontinet para América Latina e Caribe explica: “Quase 10% dos ataques globais foram direcionados ao Brasil, de acordo com nossos

sensores, o que fez do país o principal alvo e trouxe esses números surpreendentes".Os dados apresentados mostram que o crescimento dos ataques cibernéticos no Brasil é uma realidade, o que leva a concluir que defesa do espaço cibernético deve ser uma prioridade para o país.

3 REFERENCIAL METODOLÓGICO

3.1 METODOLOGIA

De acordo com Chizzotti (1991), o método científico é resultado de uma sequência de etapas que resulta em um processo de pesquisa. Não obstante, segundo Marconi (2003) também é um conjunto de regras em uma investigação científica que tornam os resultados mais confiáveis. Tais definições trazem a premissa de que cada trabalho acadêmico possui um método científico mais adequado para sua linha de pesquisa, trazendo ao autor a responsabilidade de escolher de acordo com seus objetivos a serem alcançados.

Nesse trabalho foi utilizado o método indutivo que tem por objetivo a análise de ideias a partir da observação, nesse sentido, chegar a um conclusão. O método indutivo de acordo com Monteiro Mezzaroba (2004) e por Lakatos Marconi (2007):

> "o método indutivo fundamenta-se na observação de um objeto ou fenômeno específico para que se alcancem, partindo dele, conclusões gerais ou universais. É que quando se parte da observação consistente do específico, proposições gerais ganham força e plausibilidade" (MEZZAROBA; MONTEIRO, 2004).

> "A indução, portanto, é um processo mental que parte de dados particulares e, na medida em que estes vão sendo "suficientemente constatados", permite-se inferir uma verdade mais ampla que aquela contida inicialmente nas partes examinadas. É um procedimento generalizador que tem como objetivo chegar a conclusões de conteúdo muito mais amplo que as próprias premissas que foram utilizadas de alicerce" (MARCONI; LAKATOS, 2007, p. 53).

No levantamento de dados do referido trabalho, os questionários e as pesquisas biográficas fundamenta-se como a observação de um fenômeno, ou seja, a insegurança de muitas redes sem fio e a necessidade de melhor protegê-las. Abrindo espaço para conclusões gerais e proposições de solução, como é o caso, do servidor Radius.

3.2 TIPO DE PESQUISA

De acordo com Antonio Carlos Gil, professor doutor da Universidade Federal de Pelotas, existe duas óticas pelas quais pode-se avaliar o tipo de pesquisa, quanto aos objetivos e quanto os procedimentos técnicos. Esta monografia, na ótica dos objetivos utiliza-se da pesquisa exploratória, que tem por objetivo citado abaixo:

> " proporcionar maior familiaridade com o problema (explicitá-lo). Pode envolver

> levantamento bibliográfico, entrevistas com pessoas experientes no problema pesquisado. Geralmente, assume a forma de pesquisa bibliográfica e estudo de caso.” (GIL, 2008)

De acordo com tal definição, o trabalho se encaixa com exatidão na pesquisa exploratória, a busca por dados deu-se pelo levantamento bibliográfico em livros, revistas e notícias e também questionário com especialistas no assunto, no caso, oficiais da arma de Comunicações do Exército Brasileiro.

Quanto ao procedimento, o tipo de pesquisa é o misto, utilizando-se a pesquisa bibliográfica e o estudo de campo. A pesquisa bibliográfica, para Fonseca (2002), é realizada da seguinte maneira:

> [...] a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta (FONSECA, 2002, p. 32).

A pesquisa bibliográfica foi utilizada em sua primazia para comprovar a importância da proteção de uma rede sem fio e também procedimentos eficientes de instalação, configuração e detalhamento da solução proposta, no caso, o servidor Radius.

Por outro lado, a pesquisa de campo como já citado, também foi utilizada, para Fonseca (2002):

> A pesquisa de campo caracteriza-se pelas investigações em que, além da pesquisa bibliográfica e/ou documental, se realiza coleta de dados junto a pessoas, com o recurso de diferentes tipos de pesquisa (pesquisa ex-post-facto, pesquisa-ação, pesquisa participante, etc.) (FONSECA, 2002).

Desse modo, a pesquisa de campo teve como objetivo avaliar a forma de segurança utilizada nas redes sem fio durante as operações militares. Esses dados são restritos às experiências de militares especialistas.Considerando que na maioria dessas redes de operaçõesfuncionavam serviços essenciais para uma operação militar, havendo informações sensíveis, os pontos observados na pesquisa foram principalmente o acesso de forma não controlada a esses pontos de acesso ea importância da proteção desses pontos de acesso.

3.3 INSTRUMENTOS DE PESQUISA

3.3.1 Questionário com especialistas e pesquisas bibliográficas

Esse levantamento de dados é feitaa partir de questionário com especialistas, no caso, militares da Arma de Comunicações. Capitães, Tenentes e Aspirantes a Oficial que já exerceram funções chaves em operações simuladas ou não.A pesquisa se refere a operações militares simuladas, as quais são realizadas na Academia Militar das Agulhas Negras e também de experiências da vida militar dos que responderam o questionário.

Esse levantamento de dados também é feita a partir de pesquisas nas mais diversas fontes, comorevistas, livros, artigos científicos, trabalhos de conclusão de curso e internet.

3.4 INSTRUMENTOS DE ANÁLISE

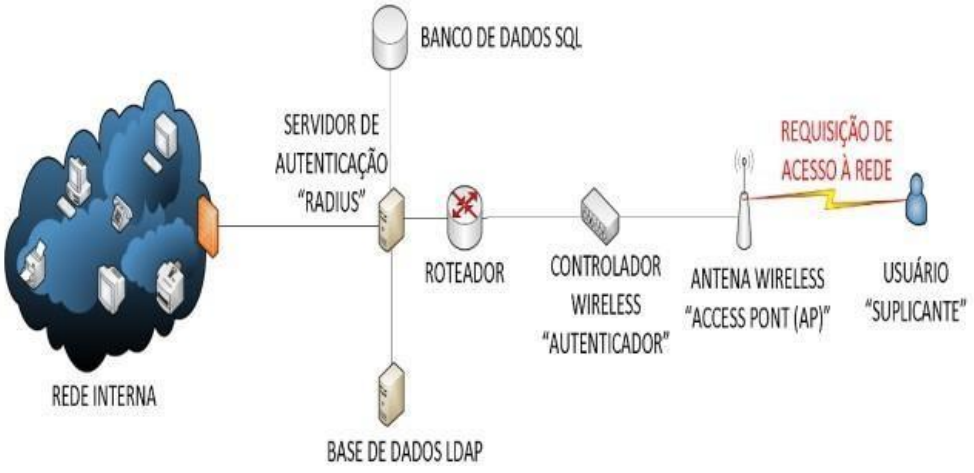
3.4.1 Apresentação do cenário

O cenário é realizado de modo simulado, utilizando máquinas virtuais, um ambiente que se assemelha as redes de computadores que ocorre em operações militares, dentro das limitações acadêmicas, será utilizado como referência à manobra escolar.Com instalação dos serviços de DHCP e DNS disponíveis em tais cenários e um ponto de acesso à rede sem fio.

3.4.2 Uso do Radius

A instalação do servidor Radiusé explorada em específico em sua potencialidade de autenticação de usuários. Dentro de um cenário já pronto, é comprovada a facilidade e aplicabilidade.Realiza-se a instalação do servidor Radius e sua integração com os serviços de DHCP e DNS.

Figura 2 – Infraestrutura do processo de autenticação por RADIUS



Fonte: Dulaney (2011)

A análise de dados nessa etapa ocorre ligando os pontos em comuns dos questionários e das facilidades obtidas com o serviço instalado. Esses pontos em comuns são essenciais para atingir os objetivos e também comprovar a necessidade combinada com eficácia do servidor Radius para o incremento da segurança de redes sem fio em operação.

4 PROCEDIMENTOS

4.1 AMBIENTE DE CONFIGURAÇÃO

Para execução desse trabalho, criou-se um ambiente simulado. A simulação foi gerada com a utilização de máquinas virtuais criadas a partir do software de virtualização VirtualBox. O sistema operacional Linux – Ubuntu Server 18.04 LTS foi o sistema operacional escolhido e é nele que é configurado o servidor Radius.

Esse ambiente também conta com servidores DHCP, DNS e web (utilizando o servidor apache).

Além dos requisitos de softwares, também fez-se presente recursos de hardware, entre eles o *Roteador Wireless N 450MbpsTp-Link*modelo No. TL-WR940N, versão do firmware 3.17.1 Build 161124 Rel.64003n. Em sua interface virtual foi configurada parâmetros necessários para a integração com o servidor Radius.

4.1.1 Instalação de pacotes essenciais

Os recursos a seguir são essenciais para criação do ambiente propício para a configuração do servidor Radius, sendo assim, apresenta-se:

- Servidor *Radius*.
- Servidor web - Apache.
- Banco de dados Mysql.
- PHP.

Antes de qualquer instalação faz-se necessário atualizar os pacotes disponíveis em seu repositório, os comandos utilizados foram "*sudoapt-get update*" e "*sudoapt-get upgrade*" para verificar se havia atualizações em aberto.

Após isso, instalam-se os recursos essenciais já citados, eles são diluídos em diversos pacotes. Para a instalação ser completa e integral, foi realizado da seguinte forma:

apt-getinstallapache2 mariadb-serverphp libapache2-mod-php php-mail php-mail-mime php-mysqlphp-gdphp-common php-pear oho-dbphp-mbstringphp-xmlphp-curlunzipwget –y

4.2 CRIAÇÃO DO BANCODE DADOSMYSQLPARAAUTENTICAÇÃO

Os dados de usuários que o servidor Radius consulta para realizar a autenticação, como dados de logins, senhas, são todas armazenadas em um banco de dados, no caso, o MySQL. Dessa maneira, após sua instalação no tópico anterior, é necessária sua configuração.

O primeiro passo é criar uma senha para o banco de dados:

Passo 1:*#mysql_secure_installation*

O segundo passo é criar um banco de dados chamado radius para o armazenamento:

Passo 2:*#mysql –u root*

CREATE DATABASE radius;

O terceiro passo é dar permissão para um usuário(rondon) para acessar todos os dados do banco de dados, criar a sua senha(AM@N) e habilitar os privilégios.

Passo 3:*GRANT ALL ON radius.* TO rondon@localhost IDENTIFIED by "AM@N";*

FLUSH PRIVILEGES;

EXIT;

4.3 INSTALAÇÃO E CONFIGURAÇÃO FREERADIUS

Nesse momento da configuração é instalado o servidor Radius, com a utilização do pacote FreeRadius e mais dois pacotes úteis:

Passo 1: *apt-get install freeradiusfreeradius-mysqlfreeradius-utils –y*

O modelo de tabela que é utilizado no freeradius foi instalado com o comando "*freeradius-mysql*", faz-se necessário agora importar esse modelo de tabela para o banco de dados mysql:

Passo 2: *mysql –u root –p radius < /etc/freeradius/3.0/mods-config/SQL/main/mysql/schema.sql/*

Após isso cria-se um link simbólico, ou seja, um atalho:

Passo 3:*ln –s /etc/freeradius/3.0/mods.available/sql /etc/freeradius/3.0/mods-enable/*

Nesse ponto, é modificado e descomentado os parâmetros como descrito no arquivo /etc/freeradius/3.0/mods/sql para que o freeradius seja habilitado para ser utilizado como banco de dados:

Passo 4:*nano /etc/freeradius/3.0/mods/sql*

driver = "rlm_sql_mysql"

dialect= "mysql"

#Connection info:

#

server = "localhost"

port = 3306

login = "radius"

password = "AM@N"

#Clients will ONLY be read on server on startup.

read_clients = yes

 # Table to keep radius client info

client_table = "nas"

Feito isso, o próximo passo é alterar o grupo e o dono a quem pertence o arquivo /etc/freeradius/3.0/mods/sql, isso é feito para que seja autorizada a consulta desse arquivo pelo servidor:

Passo 5 -*chgrp –h freerad /etc/freeradius/3.0/mods-avaible/sql/*

chown –R freerad:freerad /etc/freeradius/3.0/mods-enabled/sql

Reinicia-se o servidor para validar todas as configurações e verifica-se os status para apurar possíveis falhas:

Passo 6 -*systemctl restart freeradius*

systemctl status freeradius

4.4 INSTALAÇÃO ECONFIGURAÇÃO DALORADIUS

A plataforma DaloRadius é um frontend utilizado para o gerenciamento do FreeRadius. Sua instalação é feita a partir do arquivo baixado no site github:

Passo 1:*Wget http:/github.com/lirantal/daloradius/archive/master.zip*

E sua descompactação:

Passo 2:*unzip marter.zip*

É movimentado o arquivo daloradius-master que é foi resultado da descompactação para a pasta criado daloradius dentro do diretório proveniente do servidor web:

Passo 3:*mvdaloradius-master /var/www/html/daloradius*

É necessário configurar a comunicação do daloradius com o banco de dados. O primeiro passo é de dentro da pasta /var/www/html/daloradius importar os esquemas que estão na pasta daloradius para dentro do banco de dados do mysql:

Passo 4: *mysql –u root –p radius <contrib/db/fr2-mysql-daloradius-and-freeradius.sql*

Passo 5:*mysql –u root –p radius <contrib/db/mysql-daloradius.sql*

Deve-se alterar as permissões de acesso para a pasta alguns arquivos que estão em /var/www/HTML/daloradius/:

Passo 6:*chown –R www-data:www-data /var/www/html/daloradius/*

chown 664 var/www/html/daloradius/library/daloradius.conf.php

A partir agora, fazem-se algumas alterações no banco de dados do daloradius para que as configurações estejam alinhadas, ou seja, daloradius, servidor Radius e banco de dados mysql em sincronia:

Passo 7:*Nano /var/www/html/daloradius/library/daloradius.conf.php*

$configValues[‘CONFIG_DB_USER’] = ‘rondon’;

$configValues[‘CONFIG_DB_PASS’]= ‘AM@N’;

Reinicia-se os serviços:

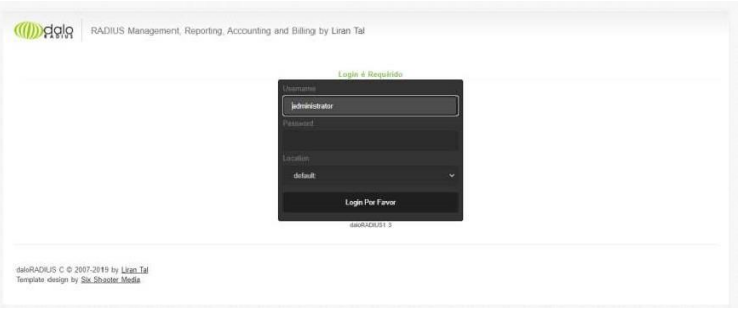
Sistemctlrestartfreeradius

Systemctlrestart apache2

No navegador, pode-se acessar a página web com o daloradius funcionando, nesse primeiro momento, enquanto não há um servidor DNS na rede, acessa-se pelo IP da máquina servidora. O username padrão é: “administrator”; a senha padrão é: “radius”.

Ip_do_servidor/daloradius

Figura 3 –Aba de login Daloradius



Fonte: Autoria própria

Figura 4 – Tela inicial Daloradius

Fonte: Autoria própria

4.5 APONTAMENTODOROTEADORPARA O SERVIDOR.

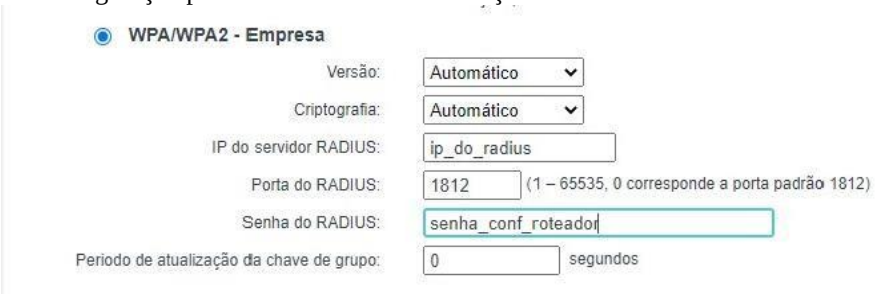
Quando um aparelho tenta se conectar em um ponto de acesso, é necessário buscar as credenciais de sse solicitante no banco de dados e verificar se o servidor Radius o reconhece, sendo assim, é necessário apontar o roteador para a máquina servidora.Essa configuração ocorre na barra lateral do roteador, na aba Wireless e Segurança do wireless. Deve-se

selecionar a forma de autenticação WPA2. Essa opção possibilita colocar o ip da máquina do servidor Radius, a porta padrão 1812 e a senha configurada no servidor Radius quando há o cadastramento do NAS por meio da plataforma Daloradius.

Figura 5 – Aba lateral de configuração do Roteador

Fonte: Autoria própria

Figura 6 – Configuração padrão WPA2 com autenticação Radius



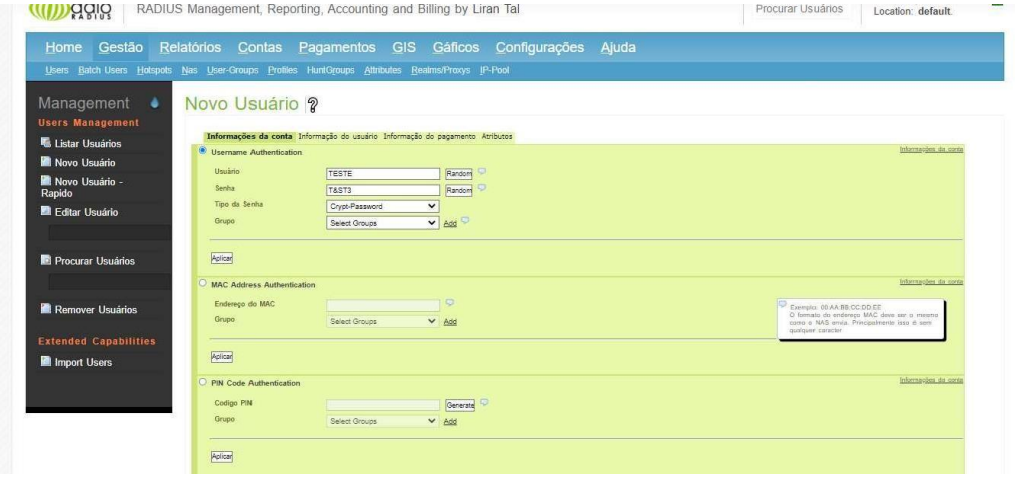
Fonte: Autoria própria

4.6 AÇÕESBÁSICAS UTILIZANDOAINTERFACEDALORADIUS

4.6.1 Criando usuários

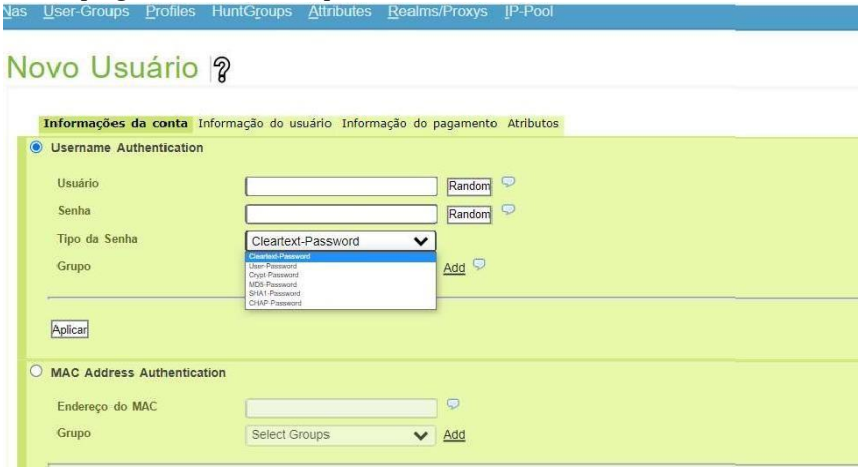
Uma das grandes funcionalidades da plataforma DaloRadius é adicionar o usuário através de uma interface intuitiva e de fácil gerenciamento. Na barra horizontal superior, selecionando Gestão, e novos usuários na barra vertical esquerda, é aberta opção de adicionar usuários. Pode-se fazer a inclusão de novas credenciais pela combinação nome de usuário e senha, MAC Address do aparelho ou PIN. O foco do trabalho é realizar a adição de usuários por “Username Authentication”, nessa opção escolhe-se um nome de usuário, a senha, tipo de criptografia e um grupo desejado.

Figura 7 – Adicionando um novo usuário



Fonte: Autoria própria

Figura 8 – Tipos de Criptografia de senhas disponíveis



Fonte: Autoria própria

4.6.2 Descrevendo algumas funções de gerência.

A plataforma DaloRadius possui diversas funções de gerências, das quais citar todas não é objeto de estudo do referido trabalho. Contudo, destaca-se a inserção de informações dos usuários, ao clicar em User Info torna-se possível o cadastramento do usuário, o que facilita a administração. É possível também a descrição de informações pessoais e empresarias, como departamento, companhia, telefones endereço empresa e outros.

Háem *Management*, a opção *List Users*, onde é possível verificar a lista de usuários disponíveis, sendo os verdes ativos e os vermelhos adicionados, porém, não ativos. É possível no superior da tela desabilitar, habilitar e remover usuários Na figura 10, os usuários que estão com ponto vermelho estão desabilitados e em verde, habilitados. Além disso, nessa mesma figura pode-se observar o hash da senha criada com criptografia.

Figura 9 – Informações de usuários

Fonte: Autoria própria

Figura 10 – Listando usuários

Fonte: Autoria própria

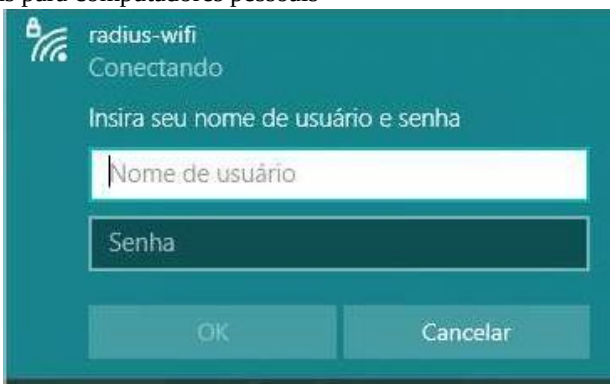
4.7 TESTE DE AUTENTICAÇÃO

Uma das grandes diferenças de quando esta se utilizando um servidor Radius, é a janela aberta para realizar a inserção da credencial do usuário, no caso, o nome de usuário e a senha. Isso acontece tanto nos celulares, quanto nos dispositivos de computadores pessoais. Na imagem, comprova-se que a conexão é bem sucedida.

Figura 11 – Página de login para celulares

Fonte: Autoria própria

Figura 12 – Página de logins para computadores pessoais



Fonte: Autoria própria

Figura 13 – Rede conectada

Fonte: Autoria própria

4.8 INTEGRAÇÃO AOS SERVIÇOS DA REDE

4.8.1 Integração DNS

Considerando que há no ambiente de trabalho um servidor DNS ativo e funcional, para realizar a integração Radius, basta configurar as zonas diretas e inversas de alguns arquivos específicos.

No arquivo /etc/bind/db.dominiolocal.locadiciona-se no final do arquivo a seguinte linha para criação da zona direta:

RADIUS IN A XXX_WWW_YYY_ZZZ(ip do servidor)

No arquivo /etc/bind/db.192 adiciona-se no final do arquivo a seguinte linha para criação da zona reversa:

Zzz IN PTR radius.dominiolocal.loc.

Para o teste de conectividade dá-se o comando:

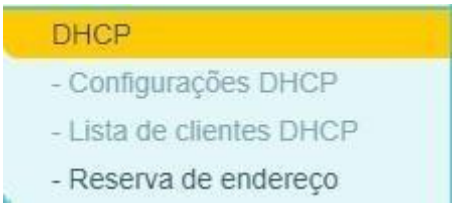
host ip_do_servidor

4.8.2 Integração DHCP

O cenário estabelecido para o trabalho, possui um ponto de acesso integrado a um servidor DHCP, oque facilita a integração com o servidor Radius. Uma ferramenta útil é reservar um endereço de ip específico para o servidor Radius, na aba DHCP e Reserva de endereço é possibilitada essa configuração, basta adicionar o endereço MAC da máquina servidora, o endereço de ip, ativar e salvar as configurações.

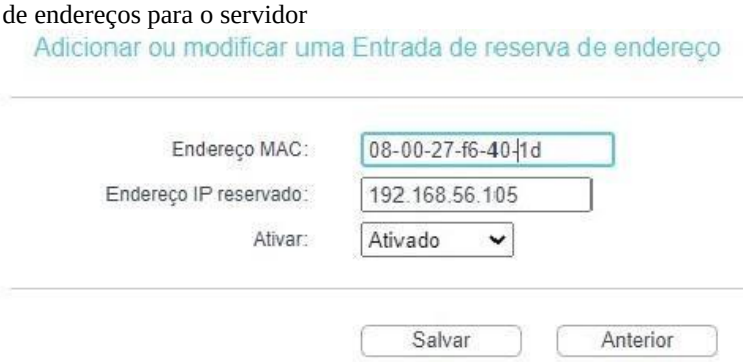
Após ativar essa configuração, o Servidor Radius trabalha normalmente e atinge o objetivo de integrar-se ao servidor DHCP.

Figura 14 - Aba de configurações lateral DHCP



Fonte: Autoria própria

Figura 15 – Reserva de endereços para o servidor



Fonte: Autoria própria

5 RESULTADO E DISCUSSÕES

No contexto de operações militares realizadas por tropa de qualquer natureza, quando há emprego de rede sem fio, observam-se as grandes vulnerabilidades que ela apresenta. Uma rede desprotegida pode permitir que pessoas indesejadas, ou até mesmo invasores, tenham acesso ilimitado aos serviços nela disponíveis. Com os questionários, foiafirmados aspectos principalmente no se relaciona a ter um sistema de proteção dessas redes.

Foi esclarecida a necessidade de segurança de redes sem fio em operações militares principalmente a partir dos questionários realizados, nos quais militares com experiência na área responderam perguntas em relação à importância do controle de acesso, como o servidor apresentado ajuda na superação das vulnerabilidades conhecidas de uma rede sem fio e qual a importância do trabalho nesse sentido. Como citado:

> O assunto sobre a autenticação é muito importante, pois dificulta o acesso não autorizado aos nossos sistemas corporativos. Com o servidor Radius instalado, o banco de dados criado, as permissões citadas de forma correta como banda de *upload*, *download*, mac para o usuário e ip, dificultam bastante a tentativa de acesso. (Tenente Villar; apêndice C)

Nesta monografia, a implementação do servidor Radius ocorreu de forma bem sucedida, apesar das potenciais complicações que a utilização de configuração por linha de comando pode apresentar, tal instalação e configuração não apresentou maiores complicações. A configuração possui alguns passos que exigiram o conhecimento do software linux, mas a eficiência atingiu um dos objetivo proposto.

Houve o estabelecimento da integração com o serviço de DHCP E DNS, pois para que o ambiente operacional fosse integrado era necessário que o servidor Radius também pudesse interagir com esses serviços, o que ocorreu de forma eficaz, comprovando que o servidor funcionaria em uma rede já estabelecida.

Após a instalação, configuração e exploração do servidor Radius, iniciou-se o processo de exploração da interface gráfica de gerenciamentoDaloRadius, na qual foi demonstrado como adicionar, resolver, excluir e realizar cadastro com os usuários de forma simplificada. Vale destacar que a plataforma possui outras potencialidades, contudo as abordadas cumprem os objetivos apresentados.

Por fim, houve a promoção da segurança de uma rede sem fio. Essa ferramenta é eficiente, de fácil aplicação e cumpre as determinações do Exército Brasileiro quanto ao uso de redes sem fio.

6 CONSIDERAÇÕES FINAIS

O estudo teve como objetivo implementar um servidor Radius de software livre para melhorar a segurança de redes sem fio no âmbito de operações e comprovar a importância da segurança das redes sem fio. Para alcançar esses objetivos, instalou-se um servidor Radius, integrou a serviços de DHCP e DNS, realizou a exploração desse servidor e a utilização de ferramentas de apoio, como o software Daloradius.

A base de dados *MySQL* foi fundamental para a realização deste procedimentoprático. Este, por sua vez, armazenou todos os dados que foram criados por meio doservidor, em seu banco. A grandeza desta aplicação se consolida cada vez mais porinúmeras de suas funcionalidades: diversas empresas utilizam-se do MySQLparasuasrespectivas aplicaçõesinternas de bancodedados.

Também foi utilizado a interface *Daloradius*,ferramenta esta que facilita a execução das atribuições do administrador de rede pormeio do bloqueio de acessos simultâneos, autenticação de usuários, exclusão deelementos indesejáveis, desativação temporária e a criação de cadastros dos queutilizarãooserviço.Devido à riqueza do servidor *Radius*, há vários tipos de frontends, contudo escolha foi coerente paraqueotrabalho viesseaser desenvolvidodamelhormaneirapossível.

A segurança cibernética é de grande relevância dentro do Exército Brasileiro e dentro do contexto de operações, muitos são os casos de invasões e de crescimento de ataques hackers, o que aumenta a relevância desse estudo. Isso levanta a necessidade de além de haver um software para esse fim, como o servidor Radius, também militares capacitados para operar o grande fluxo de informações e demandas de segurança.

A pesquisa levantou a importância da segurança de redes sem fio a partir de entrevistas com especialistas e também levantamento bibliográfico, trazendo como resultado o aumento da segurança da rede a partir da implementação do servidor proposto em um cenário adaptável para as operações. Com o servidor, é protegido tanto as redes diretamente quanto indiretamente com a proteção de todos os serviços estão disponíveis naquele ambiente.

Os questionários ressaltaram a importância de haver uma mentalidade de proteção das redes sem fio, levantaram pontos como a grande relevância de um servidor que proporcione o controle de usuários, para proteção de acessos indesejados, inibição de entrada na rede, dificuldade de exploração não requisitada e saturação da rede. As opiniões e alegações dos

especialistas da área: oficiais de comunicações; reforçaram as constatações bibliográficas previamente levantadas.

Para o aprimoramento do trabalho, deixa-se como sugestão que nas fileiras do Exército Brasileiro seja abordada a necessidade e importância da capacitação em segurança de redes sem fio, para que o conhecimento adquirido traga diversos benefícios para as Forças Armadas.

REFERÊNCIAS

BRASIL. Ministério da Defesa. **MD30-M-01: Doutrina de Operações Conjuntas**. 1ª ed. Brasília, DF.

BRASIL. Ministério da Defesa. **EB70-MC-10.223: Operações**. 1ª ed. Brasília, DF, 2017.

BRASIL. Ministério da Defesa. **EB70-MC-10.232:Guerra Cibernética.** 1ª ed. Brasília, DF, 2017.

BRASIL. Ministério da Defesa. **MD33-M-11: Manual de apoio de fogo em operações conjuntas**. 1ª ed. Brasília, DF, 2013.

CARDOSO NETO, Celso et al. BACKUP. REVISTA DE TRABALHOS ACADÊMICOS, 2014.

ESCRITÓRIO DE PROJETOS DO EXÉCITO BRASILEIRO**. Liberdade de Ação no Espaço Cibernético.** 2021. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/> Acesso em 11 fev. 2022.

FERREIRA, Ruben E. Linux: **guia do administrador do sistema.** 2 ed. São Paulo: Novatec Editora, 2008.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

GIL, Antonio Carlos. Como **elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

LINHARES, André Guedes; GONÇALVES, Paulo André da Silva. Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w. 2010. 17 - Universidade Federal de Pernambuco (UFPE), Recife - PE. 2010).

MACHADO, Felipe Nery Rodrigues; Maurício Pereira de Abreu. **Projeto de Banco de Dados: uma visão prática.** 16 ed. São Paulo: Erica, 2009.

MORAES, Alexandre Fernandes de. **Segurança em Redes: Fundamentos**. 1 ed. São Paulo: Erica, 2010.

OSSAMU, CARLOS. **Aceleram os investimentos em redes sem fio avançadas**. 2021. Disponível em: <https://inforchannel.com.br/2021/03/22/aceleram-os-investimentos-em-redes-sem-fio-avancadas/> Acesso em 08 mar. 2022.

PACETE, GUSTAVO. **5 ataques cibernéticos no Brasil em 2021 que geraram alerta.** 2021. Disponível em: <https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/> Acesso em 09 mar. 2022.

PINHEIRO, João Victor. **Autenticação com Freeradius - Instalação Apache + MySQL + PHP + Freeradius + Daloradius**. 16 de Agosto de 2020. Disponível em: <https://www.youtube.com/watch?v=qWTRLZFgaCA&list=PLnZhHJZsJ3UEBzk0BUGZZoXbQGz8uePsG&index=3>. Acesso em: 20 de Dezembro de 2021.

PINHEIRO, João Victor. **Autenticação com Freeradius - Instalação Apache + MySQL + PHP + Freeradius + Daloradius**. 16 de Agosto de 2020. Disponível em: https://www.youtube.com/watch?v=MvKnTf0cYKQ&list=PLnZhHJZsJ3UEBzk0BUGZZoXbQGz8uePsG&index=4. Acesso em: 20 de Dezembro de 2021.

SANTOS, 2010, p. 22-37 apud Teleco, Redes Sem Fio: **análise de vulnerabilidade.** Disponível em . Acesso em 13 de Julho de 2021.

THIOLLENT, Michel. **Metodologia da pesquisa - ação**. 2. ed. São Paulo: Cortez, 1986.

VALOR ECONÔMICO. **Cresce a demanda por segurança cibernética**. 2021. Disponível em <https://neweseguros.com.br/crsce-a-demanda-por-seguranca-cibernetica/> Acesso em 08 mar. 2022.

APENDICE A – QUESTIONÁRIO

O senhor está convidado a participar do questionário para levantamento de dados para o seguinte Trabalho de Conclusão de Curso: a implementação de um servidor Radius para o incremento da segurança de redes sem fio em operações. Esta pesquisa seguindo o tema acima é de interesse da Academia Militar das Agulha Negras com o objetivo de melhorar o processo ensino aprendizagem e compõe o TCC para bacharelado em Ciências Militares realizado pelo Cadete Bruno Souza do Nascimento Vicente, do 4º ano do Curso de Comunicações.

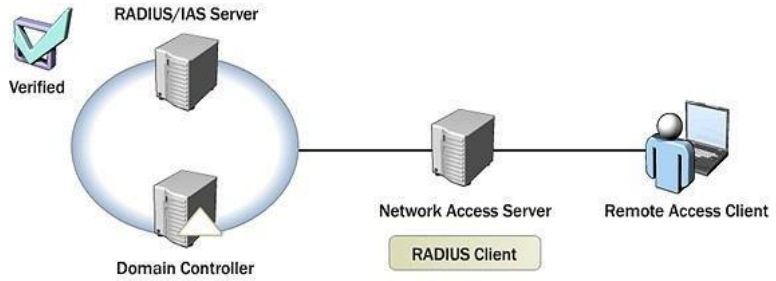
A participação é voluntária e consiste em preencher um questionário. É facultada a recusa a participar ou desistir de responder a qualquer momento. As informações serão utilizadas para fins exclusivamente acadêmicos, sendo as informações disponíveis no referido trabalho de conclusão de curso.

Para introdução ao trabalho, o autor disponibiliza um pequeno resumo sobre servidor Radius:

De acordo com Rigney et al. (2000) o servidor Radius tem três funções básicas: a de autenticar usuários, de autorizar a serviços providos pela rede e de contabilizar todo novo pedido de entrada na rede por parte do requisitante. Abaixo, é explicado como é a infraestrutra de uma rede com um servidor Radius.

O usuário ou aparelho envia um pedido para poder ter acesso a um recurso de uma determinada rede protegida a um Network Access Server (NAS). Para isso ele utiliza suas credenciais de acesso que, por sua vez, são passadas ao dispositivo NAS. Esta solicitação leva consigo as credenciais de acesso, que geralmente estão sob a forma de login e senha fornecidos pelo usuário. Estas credenciais serão comparadas em uma base de dados e o usuário pode ter acesso ou não à rede.

Figura 16 - Autenticação de Um Cliente Pelo Servidor RADIUS



Fonte: Centralize Network Access Authentication, 2009

1- Em uma operação militar, em muitos casos, há uma rede wi-fi interna disponível para militares que pode dar acesso aos serviços como SPED, EBNET e SisBol, tornando os pontos de acesso portas de entrada para serviços sensíveis à segurança da informação. No cenário proposto pelo trabalho, utiliza-se como um dos métodos de aprimorar a segurança, um ponto de acesso com protocolo de segurança WPA2 e a exigência de nome de usuário e senha próprio para cada militar promovida pelo servidor Radius. **Com base nas vulnerabilidades de uma rede sem fio conhecidas: como o controle de acesso fornecido pelo servidor Radius é capaz de auxiliar na superação dessas vulnerabilidades?**

2- De acordo com a portaria nº 004-DCT, 31 janeiro de 2007 do Departamento de Ciência e Tecnologia – instruções reguladoras sobre segurança da informação nas redes de comunicação e de computadores do Exército Brasileiro IRESER – (IR 13-15), Art. 68: determina-se que as redes sem fio devem possuir requisitos de segurança próprios, com configuração de segurança adequadamente ajustados, em particular, os aspectos de identificação e autenticação do usuário. **A partir disso, baseado em experiências em operações e fazendo uma avaliação sobre a segurança de redes sem fio: por que é importante o controle de acesso de uma rede sem fio no contexto de operações militares?**

3- De acordo com a portaria nº 004-DCT, 31 janeiro de 2007 do Departamento de Ciência e Tecnologia – instruções reguladoras sobre segurança da informação nas redes de comunicação e de computadores do Exército Brasileiro IRESER – (IR 13-15), Art. 41 determina: O acesso aos dados e serviços corporativos de rede no Exército, seja em conexões locais ou remotas, só pode ser concedido mediante a verificação da autenticidade da identificação do usuário por meio de técnicas de autenticação de rede. **Em relação a este trabalho, sabendo que visa a implementação de um servidor Radius para o incremento da segurança em redes sem fio, com enfoque em autenticação de usuários, qual a relevância que o senhor atribui ao mesmo? E quais aspectos isso pode auxiliar nas operações militares?**

APÊNDICE B – RESPOSTAS DO QUESTIONÁRIO (APÊNDICE A) COM O TENENTE LUIZ EDUARDO MARTINS SPOTTI

INSTRUMENTO DE COLETA DE DADOS – QUESTIONÁRIO COM ESPECIALISTA

TEMA: A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÕES

Questão 1. Resposta: Impondo uma autenticação do usuário que está conectando, dificultando a quebra da senha.

Questão 2. Resposta: Para evitar o acesso de usuários indevidos e restringir as permissões por usuário.

Questão 3. Resposta: Extrema relevância para a segurança das comunicações. O principal aspecto é na filtragem de acesso ao sistema, impedindo conexões indevidas a serviços e coleta de dados restritos aumentando o sigilo e a segurança das comunicações.

APÊNDICE C – RESPOSTAS DO QUESTIONÁRIO (APÊNDICE A) COM O TENENTE VICTOR MARTINS VILLAR

INSTRUMENTO DE COLETA DE DADOS – QUESTIONÁRIO COM ESPECIALISTA

TEMA: A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÕES

Questão 1. Resposta: O controle fornecido pelo servidor de autenticação Radius auxilia na segurança, pois cria um login e senha para cada usuário conseguir se conectar na rede wifi, desta forma, dificulta o ataque padrão de obtenção de hash e força bruta para quebrar a senha. Com esse método, o atacante precisará obter primeiramente um usuário válido para depois tentar craquear o hashdesde usuário.

Questão 2. Resposta: É importante o controle, pois previne o acesso de pessoas não autorizadas aos sistemas corporativos.

Questão 3. Resposta: O assunto sobre a autenticação é muito importante, pois dificulta o acesso não autorizado aos nossos sistemas corporativos. Com o servidor Radius instalado, o banco de dados criado, as permissões citadas de forma correta como banda de upload, download, mac para o usuário e ip, dificultam bastante a tentativa de acesso. Além disso, cabe ressaltar a importância da criação de uma senha segura, pois não adianta uma grande infraestrutura com uma senha fraca.

APÊNDICE D – RESPOSTAS DO QUESTIONÁRIO (APÊNDICE A) COM O TENENTEMATHEUS LOPES SALINAS

INSTRUMENTO DE COLETA DE DADOS – QUESTIONÁRIO COM ESPECIALISTA

TEMA: A IMPLEMENTAÇÃO DE UM SERVIDOR RADIUS PARA O INCREMENTO DA SEGURANÇA DE REDES SEM FIO EM OPERAÇÕES

Questão 1. Resposta: Tendo em vista que o servidor trabalha com a segurança WPA2, o gerenciador de sistema consegue com o auxílio do servidor limitar o acesso, garantindo maior segurança para a rede.

Questão 2. Resposta: Pois em caso contrário, qualquer indivíduo não autorizado poderia acessar a rede, saturá-la ou ter acesso a coisas não autorizadas.

Questão 3. Resposta: É de suma importância. Pode auxiliar no controle de acesso; pode reduzir e controlar a saturação da rede e inibi a utilização da rede por visitantes não integrantes da equipe de comando.