Avaliação de Segurança de Redes sem Fio com Foco em WPS

Aluno: Carlos Daniel da Silveira Santos (MATRÍCULA:20189022361)
E-mail: cdanielss1973@outlook.com; Período da Graduação: VI
Orientador: Fredison Muniz de Sousa

17 de setembro de 2020

Resumo

Contexto: O *Wi-Fi Protected Setup* (WPS) é um padrão definido pela Wi-Fi AllianceTM, para segurança de redes sem fio (Wi-Fi). Foi introduzido em 2006 e vinha para fornecer uma configuração mais fácil e substituir padrões obsoletos. Apesar de trazer novas funcionalidades, também trouxe consigo algumas vulnerabilidades. Como a principal falha do WPS, que é ser composto por um PIN (Número de identificação pessoal) de apenas 8 dígitos, suscetível a ataques de força bruta.

Problema: Com o avanço e o grande aumento dos serviços online, as redes de computadores estão cada vez mais vulneráveis. Hoje, quase todos os computadores e dispositivos móveis estão conectados à grande rede da Internet, onde problemas podem ocorrer, seja por próprio descuido do usuário, deixando sua máquina exposta ou por falhas de segurança da rede. Por isso, faz-se necessário o estudo das vulnerabilidades e falhas dos equipamentos de redes, para uma utilização adequada de acordo com o usuário.

Proposta: Este pré-projeto visa avaliar redes domésticas que estão vulneráveis, principalmente por conta do protocolo WPS, utilizando como cenário o município de Picos do Estado do Piauí (Picos - PI). A coleta de dados será feita com o auxílio do método de *WarDriving*, para a captura e análise de dados como: Protocolos de Segurança e configurações WPS. A análise dos dados visa contribuir para o desenvolvimento de métodos sistemáticos que possam auxiliar no desenvolvimento de novas soluções de segurança.

Palavras-chaves: Wi-Fi, WPS, Segurança, Internet, Protocolo.

1 Introdução

As redes de computadores são formadas por computadores autônomos que trocam informações entre si. Essa conexão pode ser feita de várias formas como fios de cobre, fibra óptica e ondas de rádio. Nestes sistemas são utilizados equipamentos concentradores denominados *switches*, para interligação dos computadores em uma rede e cliente-servidor que é uma estrutura que distribui as tarefas entre os fornecedores de um recurso (servidores) e os requerentes dos serviços (clientes) (TANENBAUM; WETHERALL, 2011).

A estrutura de uma rede conta com uma estrutura lógica para se comunicar, denominada protocolo de comunicação. Os protocolos são conjuntos de regras que visam estabelecer a comunicação entre as camadas do modelo OSI (*Open Systems Interconnection*). Os mesmos realizam o controle do formato e o significado das informações passadas (TANENBAUM; WETHERALL, 2011). O *Wi-Fi Protected Setup* (WPS) é usado como padrão de segurança para redes sem fio (Wi-Fi), que visa fazer a conexão entre um dispositivo e uma rede sem fio de maneira rápida e fácil. Essa tecnologia funciona em redes sem fio com uma senha criptografada.

Embora o WPS seja comercializado como uma forma segura de configurar um dispositivo sem fio, existem projetos e falhas de implementação que permitem a um invasor obter acesso a uma rede sem fio protegida (VIEHBÖCK, 2011). As duas das principais formas de atacar um dispositivo Wi-Fi com WPS são: A primeira é um ataque de força bruta offline que usa desequilíbrio no registro do protocolo. Este ataque requer ação do usuário, mas é o mais eficiente. A segunda forma de ataque usa fraquezas no implementação de WPS e fornece um *evil twin*. Este ataque mostra que mesmo desabilitando completamente o WPS nos roteadores, todas as vulnerabilidades não são cobertas (MOHTADI; RAHIMI, 2015).

1.1 Objetivos Gerais e Específicos

O objetivo geral deste pré-projeto é levantar dados que mostrem o atual cenário do nível de segurança das redes Wi-Fi no município de Picos do Estado do Piauí (Picos - PI). Os objetivos específicos deste trabalho são:

- Identificar o perfil das redes Wi-Fi da cidade de Picos;
- Demonstrar o atual nível de segurança das redes identificadas;
- Criar métodos sistemáticos que auxiliem na segurança das redes Wi-Fi.

2 Justificativa

A tecnologia das redes sem fio obteve um grande salto na quantidade de utilizadores pela conveniência e praticidade na utilização dos dispositivos móveis (TANENBAUM; WETHERALL, 2011). Dessa forma, criaram-se novos riscos aos dispositivos e usuários e consequentemente novos desafios às empresas desenvolvedoras. Portanto foram necessários investimentos para o desenvolvimento de tecnologias que aliem mais segurança e qualidade na utilização dessas redes.

O interesse no assunto surgiu da necessidade de entender os riscos a que as pessoas estão expostas ao utilizar as redes sem fio e de verificar se existe algum mecanismo que realmente garantam a segurança neste ambiente. Diversas tecnologias são desenvolvidas e adicionadas às redes sem fio para melhorar a experiência do usuário final, permitindo que este possa, por exemplo, instalar um roteador *wireless* em casa e conectar seus dispositivos com pouco ou nenhum conhecimento técnico (SILVA, 2014).

Diante da grande quantidade de usuários das redes sem fio, e tendo as mais diversas formas de ataques a vulnerabilidades, é necessário uma utilização consciente das ferramentas e dispositivos, pois a segurança é necessária em várias camadas de uma arquitetura de rede para proteção contra atacantes, que têm à mão um grande arsenal de ataques possíveis

(KUROSE; ROSS; ZUCCHI, 2007). Uma boa alternativa para lidar com os tais problemas seria sempre a atualização do software do dispositivo e uma configuração apropriada.

Mantendo o WPS ativo pode ser um fator de risco alto, ou seja, permitir um acesso não autorizado na rede e possivelmente ao restante do ambiente, quer seja para usá-lo como ponte para outros ambientes, quer seja para capturar informações que trafegam para outros ambientes Wi-Fi. Mesmo que a senha não seja exposta, e o PIN do WPS for descoberto já é suficiente para ter acesso a rede (RUFINO, 2019).

O presente trabalho visa solucionar um dos grandes problemas, para se desenvolver soluções por meio de métodos sistemáticos, para a segurança de redes. Sendo ele a falta de informações sobre o estado da rede. Além de fornecer conhecimentos na aplicação das contramedidas de segurança necessárias para mitigar os riscos e uma utilização devida dos equipamentos.

3 Referencial Teórico

Esta Seção apresenta os conceitos fundamentais para a compreensão do pré-projeto. Na Subseção 3.1 descreve as Redes sem Fios, abordando os seus conceitos de criação. Já a Subseção 3.2 contextualiza sobre os protocolos, adentrando nas falhas e vulnerabilidades.

3.1 Redes sem Fios

A tecnologia *wireless* significa "sem fio" (em livre tradução), e possibilita a transmissão da conexão entre pontos distantes sem precisar usar fios (como telefones sem fio, rádios ou o seu celular) (CANCELA et al.,). Essa tecnologia engloba uma série de outras, sendo a mais comum delas a Wi-Fi. Podem ser consideradas *wireless*, como o IrDA (*Infrared Data Association*) que transmite através de um adaptador infravermelho, há também o *bluetooth* muito utilizado em *smartphones*, porém sua distância é relativamente curta, dentre outros (ENGST; FLEISHMAN, 2005).

O *Institute of Electrical and Electronic Engineers* (IEEE) constituiu um grupo de pesquisa para criar padrões abertos que pudessem tornar a tecnologia sem fio cada vez mais realidade, tendo como objetivo desenvolver padrões técnicos de acordo com fabricante, definindo como dará a comunicação entre fabricante e cliente de rede. Ao longo do tempo, foram desenvolvidos diversos padrões, a qual destacou e melhor desenvolveu foi o padrão 802.11, conhecido como Wi-Fi (*Wireless Fidelity* ou fidelidade sem fio) (RUFINO, 2019).

O comitê apresentou o padrão IEEE 802.11 que foi inicialmente definido como uma especificação de nível físico e de *enlace* do modelo OSI para redes locais sem fio WLAN. A WLAN funcionava a 1 Mbps (megabits por segundo) ou 2 Mbps (TANENBAUM, 2003). Com o passar do tempo outros padrões foram criados, de acordo com a necessidade do mercado, o último padrão apresentado é o 802.11ax, que foi ratificado no segundo semestre de 2019, vindo para fornecer um desempenho mais previsível para aplicações avançadas, como vídeo 4K ou 8K (LÓPEZ-PÉREZ et al., 2019).

3.2 Protocolos de Segurança

Todas as atividades na *Internet* que envolvem duas ou mais entidades remotas comunicantes são governadas por um protocolo. Por exemplo, protocolos executados no hardware de dois computadores conectados fisicamente controlam o fluxo de bits no "cabo" entre as duas placas de interface de rede; protocolos de controle de congestionamento em

sistemas finais controlam a taxa com que os pacotes são transmitidos entre a origem e o destino; protocolos em roteadores determinam o caminho de um pacote da origem ao destino (KUROSE; ROSS; ZUCCHI, 2007).

3.2.1 Protocolo WEP (*Wired Equivalent Privacy*)

O protocolo IEEE 802.11 WEP foi criado em 2009 para fornecer autenticação e criptografia de dados entre um hospedeiro e um ponto de acesso sem fio (ou seja, a estação-base) usando uma técnica de chave compartilhada simétrica. A WEP não especifica um algoritmo de gerenciamento de chave, então supomos que o hospedeiro e o ponto de acesso sem fio de alguma forma concordam sobre a chave através de um método fora da banda (KUROSE; ROSS; ZUCCHI, 2007).

O WEP trabalha com chaves simétricas, ou seja, a mesma chave é sempre utilizada para encriptar e desencriptar as informações que serão trafegadas na rede. O WEP possui uma série de problemas e a incapacidade de garantir a confidencialidade dos dados neste protocolo foi comprovada em (FLUHRER; MANTIN; SHAMIR, 2001). O WEP pode ser quebrado através de ataques probabilísticos que foram otimizados em diversos programas específicos para isso (como o software *WEPCrack* e *Airsnort*). O atacante necessita capturar alguns milhares de pacotes e executar a análise via software para obter o segredo compartilhado.

3.2.2 Protocolo WPA (Wi-Fi *Protected Access*)

Para corrigir as vulnerabilidades apontadas no WEP, foi criado o WPA, protocolo de criptografia mais robusta do que o anterior. A criação do WPA tinha como o foco manter a compatibilidade com o WEP, mas ampliando suas características de segurança. O WPA não fornece apenas criptografia de dados forte para corrigir os pontos fracos do WEP, ele adiciona autenticação do usuário que estava faltando WEP (ALLIANCE, 2003).

Com o WPA foi apresenta uma nova tecnologia de chave denominada TKIP (*Temporal Key Integrity Protocol*), na qual a chave de criptografia é trocada periodicamente, sua autenticação é por trocas de chaves dinâmicas, prevenindo ataques de retransmissão de pacotes. Mesmo diante dessas melhorias do WPA, se um atacante obtiver os quadros trocados durante o processo de autenticação, é possível que realize um ataque de força bruta (FLEISHMAN; MOSKOWITZ, 2003).

3.2.3 Protocolo WPA2 (Wi-Fi *Protected Access2*)

O protocolo WPA2 foi desenvolvido para a obtenção de um nível de segurança ainda maior que no padrão WPA, que para isso substitui o método criptográfico do WPA (STANGARLIN; FILHO, 2017). O WPA2 introduz um novo algoritmo criptográfico, que é considerado completamente seguro, mas traz o inconveniente de não poder se comunicar com algumas interfaces de rede mais antigas. O WPA2 é considerado o padrão de segurança Wi-Fi mais seguro, pois apresenta componentes que são cruciais para a segurança da rede sem fio, Autenticação, Cifragem e Integridade (KUMAR; GAMBHIR, 2014).

Porém mesmo sendo considerado o padrão de segurança mais seguro, o WPA2 não está livre de falhas, foi constatada uma falha batizada de KRACK (*Key Reinstallation Attacks*) que expôs quase todas as redes *wireless*. O ataque consiste em enganar a criptografia da rede permitindo que os dados sejam interceptados pelo atacante. Felizmente para que

isso aconteça o atacante deve estar no alcance de sua rede, o que torna um pouco menos provável que aconteça em determinadas ocasiões (VANHOEF; PIESSENS, 2017).

3.2.4 Protocolo WPS

O WPS é um programa de certificação opcional, que é projetado para facilitar a tarefa de instalar e configurar a segurança em redes locais sem fio (VIEHBÖCK, 2011). Introduzido no início de 2007, o programa fornece um conjunto de soluções de configuração de rede. A principal e única vantagem do uso do recurso, é eliminação da necessidade de utilização e memorização de senhas. O WPS pode ser implementado nos concentradores de três formas diferentes:

- PIN: Neste método, um número de identificação pessoal (*Personal Identification Number* - PIN) é configurado no concentrador e utilizado no momento da conexão inicial. Este número vem, em muitos casos, informado em uma etiqueta colada ao concentrador. A autenticação via PIN no WPS é feita através da troca de mensagens entre o cliente e o concentrador sem fio. Nesta fase são trocadas oito mensagens;
- Botão WPS: Neste método, o usuário tem que pressionar um botão (físico ou lógico) no concentrador e iniciar a procura no cliente. Alguns clientes podem vir com um botão WPS também;
- NFC (*Near Field Communication*): Funciona por uma aproximação mínima de 10 centímetros de distância entre os dispositivos. Pelo fato da transmissão de informações via NFC ser instantânea, sem a necessidade de inserir senhas ou códigos de acesso, o contato entre os dois dispositivos deve ser mesmo bastante próximo para evitar o envio (ou recebimento) de dados de modo acidental, após posicionados bem próximo a conexão já é estabelecida.

O WPS é considerado uma técnica de autenticação fraca, pois vários ataques foram sucessivos contra o WPS. Um sistema que utilize a autenticação WPS por meio de PIN, pode ser facilmente quebrado por um ataque de força bruta, mesmo sendo usado junto com padrões WPA ou WPA2 e uma senha forte (SILVA, 2014). A melhor opção para manter as redes sem fio seguras é, aparentemente, desabilitar a função WPS nos roteadores.

4 Trabalhos Relacionados

Esta Seção explana sobre os trabalhos relacionados ao tema encontrados na literatura, especificamente sobre a exploração da vulnerabilidade do WPS. Todavia, a abordagem do pré-projeto objetiva investigar a infraestrutura de redes domésticas neste problema, contudo, não há estatísticas da quantidade de aparelhos que utilizam o WPS. Dessa forma, os trabalhos foram divididos da seguinte forma: trabalhos que exploram a vulnerabilidade do WPS e trabalhos que exploram vulnerabilidades em outros protocolos como WPA e WPA2.

4.1 Trabalhos que utilizam o WPS para exploração de Vulnerabilidades

Em Lindell e Lagerholm (2019), investiga a razão que causa o WPS um método inseguro, trazendo uma indagação sobre esse método ser seguro o suficiente para ser usado em redes corporativas. O trabalho aborda fraquezas e riscos de segurança, embora

não aborda outras informações importantes, como se a tecnologia pode ser aprimorada. Também não há informações sobre como o usuário, pode se proteger contra esses ataques, que também é uma parte importante da segurança da rede.

O artigo (NIKOLOV, 2018), faz uma avaliação e ataques de vulnerabilidades, dois tipos de ataque foram realizados nesta pesquisa, um através da troca de senha WPA2, e outro ataque para o roteador com WPS ativado, explorando a troca de PIN. O artigo descreve um modelo de senhas, com maior nível de segurança, ideal para usuários comuns. Durante os experimentos foram encontradas senhas que levam um tempo infinito de serem quebradas, por meio do método de força bruta, essas senhas eram compostas de letras aleatórias, números e símbolos especiais.

Em (VALCHANOV; EDIKYAN; ALEKSIEVA, 2019) apresenta uma metodologia e pesquisa baseada na cidade de Varna, que é a terceira maior cidade da Bulgária, utiliza o método de *WarDriving* para coleta de informações. Tendo como principal objetivo saber qual o atual nível de segurança em Varna. Os dados coletados incluem informações de um total de 19136 redes, os resultados obtidos foram analisados sistematicamente, com um total de 53% das redes com o WPS ativado.

4.2 Trabalhos que exploram vulnerabilidades em WPA e WPA2

Em (KOHLIOS; HAYAJNEH, 2018), faz um levantamento de todos os ataques disponíveis em uma rede Wi-Fi usando WPA2 de maneira organizada. Busca criar uma pesquisa abrangente que reitera pontos-chave para fornecer informações suficientes para a compreensão dos esquemas de criptografia. Conclui que o WPA2 permite que as informações do sistema, conhecidas como frames de gerenciamento, sejam enviadas em pacotes de texto simples do cliente para o ponto de acesso. Com essa vulnerabilidade, um adversário pode falsificar os pacotes para fazer com que pareçam vir do cliente alvo e realizar ataques, como a desautenticação. Também informa sobre o *Krack Attack*, esse processo explora o handshake de quatro vias que os protocolos de segurança sem fio usam para autenticar seus usuários ao se conectar à rede.

Já no artigo (KISSI; ASANTE, 2020), usa uma metodologia diferente dos demais, aplica testes em um laboratório de rede experimental. O estudo considerou utilizar o laboratório da rede de forma a não comprometer nenhuma rede individual ou organizacional devido à privacidade e legalidade de informações do usuário. Este artigo visa usar testes de penetração para avaliar vulnerabilidades e conduzir ataques em redes sem fio. Faz testes de ataque ativo, que são caracterizados por o invasor não apenas obter acesso a informações, mas fazer alterações nas informações da rede e até mesmo injetar pacotes fraudulentos na rede. Um atacante pode iniciar comandos para interromper as operações usuais do rede, como negação de serviço (DoS), sequestro de sessão, ataque de força bruta, ataque de resposta.

No trabalho de Soares e Moraes (2019) foi realizado uma pesquisa, para a avaliação dos mecanismos de segurança, são efetuados experimentos de ataques ativos, como o de dicionário e força bruta para obtenção das senhas das redes. A vulnerabilidade *Krack Attack* também é explorada com o objetivo de verificar se os dispositivos com Wi-Fi estão vulneráveis. Registrando que 31,6% das redes analisadas foram invadidas, por meio de força bruta. Já na exploração do *Krack Attack* quase 50% está propensa a sofrer ataques. Ainda discorre sobre a importância de atualizar sempre os dispositivos de redes, aliado com senhas bem elaboradas e boas práticas do usuário.

Tabela 1 – Comparação de trabalhos a partir dos modelos, diferenciando os objetivos e métodos de ataque.

Trabalhos	Objetivos	Ataques Ativos	Ataques Passivos
(LINDELL; LAGERHOLM, 2019)	Abordar falhas no padrão WPS	Não	Sim
(NIKOLOV, 2018)	Identificar vulnerabilidades por meio de ataques	Sim	Sim
(VALCHANOV; EDIKYAN; ALEKSIEVA, 2019)	Localizar vulnerabilidades por meio de uma pesquisa de campo	Não	Sim
(KOHLIOS; HAYAJNEH, 2018)	Abordar todas as possíveis falhas no protocolo WPA2	Sim	Sim
(KISSI; ASANTE, 2020)	Fornecer resultados de falhas por meio de ataques	Sim	Sim
(SOARES; MORAES, 2019)	Realizar uma pesquisa em busca de falhas	Sim	Sim
Este Trabalho	Localizar vulnerabilidades por meio de uma pesquisa de campo	Sim	Sim

5 Esboço da Proposta

Nesta seção será feita uma breve descrição da proposta deste pré-projeto. A proposta visa através do método *WarDriving*, levantar o perfil das redes sem fio da cidade de Picos no que diz respeito aos métodos de segurança aplicados às redes sem fio. A proposta visa realizar um estudo de campo para identificar o nível de segurança das redes de Picos.

Para realizar a análise serão encontrados e demarcados os pontos onde os ataques passivos serão feitos, onde será aplicado o *WarDriving*. Em seguida será feito os ataques ativos, nas redes com o WPS ativado ou utilize protocolos vulneráveis, o ataque será feito por meio de força de bruta. Os experimentos realizados servirão como guia prático para demonstrar o nível atual da seguranças das redes, para os usuários e administradores de redes, para que possam melhorar sua infraestrutura.

Para avaliar as vulnerabilidades das redes, serão usados métodos de ataques passivos e ativos. Ataques passivos são feitos por meio do método *WarDriving*, que irá identificar protocolos que estão sendo usados, para assim serem feitos os ataques ativos. Os ataques ativos serão feito por meio do método de força bruta, testando combinações de senhas mais utilizadas e senhas consideradas fracas.

6 Metodologia e Cronograma

Nesta seção será mostrada a metodologia planejada para o estudo de caso proposto. A metodologia usada nesse projeto para a obtenção dos resultados consiste em: pesquisa bibliográfica; estudo das técnicas de ataques; análise dos resultados.

Pesquisa bibliográfica: Essa é a primeira fase, nela será feito um levantamento com vários trabalhos para identificar problemas. A pesquisa também serve para coletar informações e possivelmente métodos e métricas que possam ser usados.

Estudo das técnicas de ataques: Nessa fase busca-se compreender como vai funcionar os ataques, escolhendo algoritmos específicos e ferramentas para obtenção de resultados. Como por exemplo, é necessário uma ferramenta para realizar o *sniffing* dos protocolos.

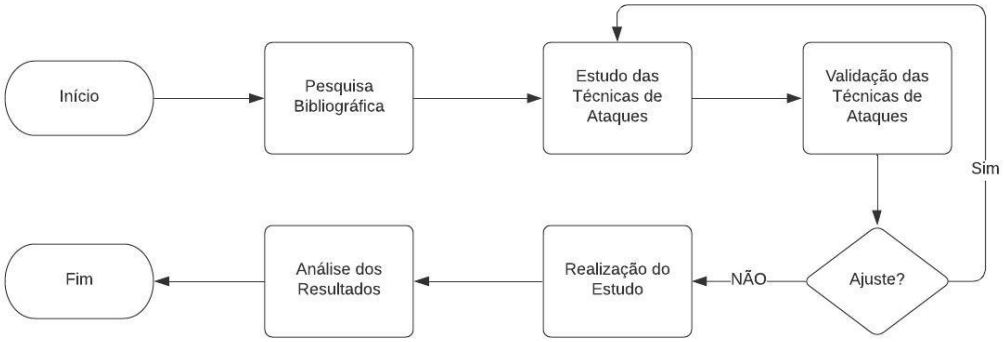

Figura 1 – Metodologia do projeto

Validação das técnicas de ataques: Nesta etapa, será feito um estudo e releitura das técnicas propostas, visando utilizar as mais novas tecnologias, para uma obtenção de resultados mais satisfatórios.

Realização do estudo: Após escolhido os parâmetros, métodos e métricas desejadas o modelo do estudo pode ser gerado. Nesse projeto serão escolhidas redes sem fio que possibilitam ataques ativos e ataques passivos.

Análise dos resultados: É a última fase do projeto. Nessa fase os resultados obtidos serão analisados e serão feitas conclusões acerca deles. Os resultados normalmente são apresentados com gráficos ou tabelas.

Por fim, a Tabela 2 apresenta o cronograma planejado para execução do projeto.

Tabela 2 – Cronograma de atividades.

Atividades	Mês 1 - 2	Mês 3 - 6	Mês 7 - 8	Mês 9 - 10	Mês 11 - 12
Pesquisa bibliográfica	X	X			
Desenvolver técnicas de ataques	X	X			
Realizar testes das técnicas		X	X		
Escrita de artigos científicos			X	X	
Redação da monografia			X	X	
Defesa da monografia					X

Referências

ALLIANCE, W.-F. Wi-fi protected access: Strong, standards-based, interoperable security for today's wi-fi networks. *White paper, University of Cape Town*, p. 492–495, 2003. Citado na página 4.

CANCELA, L. B. et al. A importância da segurança da informação em redes wi-fi. Citado na página 3.

ENGST, A.; FLEISHMAN, G. *Kit do iniciante em redes sem fio: o guia prático sobre redes Wi-Fi para Windows e Macintosh*. [S.l.]: São Paulo. Ed.: Pearson Makron Books, 2005. Citado na página 3.

FLEISHMAN, G.; MOSKOWITZ, R. Weakness in passphrase choice in wpa interface. *Wi-Fi Networking News. Acessado 21 de dezembro de 2006 em URL: http://wifinetnews. com/archives/002452. html*, 2003. Citado na página 4.

FLUHRER, S.; MANTIN, I.; SHAMIR, A. Weaknesses in the key scheduling algorithm of rc4. In: SPRINGER. *International Workshop on Selected Areas in Cryptography*. [S.l.], 2001. p. 1–24. Citado na página 4.

KISSI, M. K.; ASANTE, M. Penetration testing of ieee 802.11 encryption protocols using kali linux hacking tools. *International Journal of Computer Applications*, v. 975, p. 8887, 2020. Citado 2 vezes nas páginas 6 e 7.

KOHLIOS, C. P.; HAYAJNEH, T. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, Multidisciplinary Digital Publishing Institute, v. 7, n. 11, p. 284, 2018. Citado 2 vezes nas páginas 6 e 7.

KUMAR, U.; GAMBHIR, S. A literature review of security threats to wireless networks. *International Journal of Future Generation Communication and Networking*, v. 7, n. 4, p. 25–34, 2014. Citado na página 4.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. *Redes de Computadores ea Internet: uma abordagem top-down*. [S.l.]: Pearson Addison Wesley, 2007. Citado 2 vezes nas páginas 3 e 4.

LINDELL, J.; LAGERHOLM, F. *WPS-WiFi Protected Setup: En studie om Wi-Fi Protected Setup som autentiseringsmetod*. 2019. Citado 2 vezes nas páginas 5 e 7.

LÓPEZ-PÉREZ, D. et al. Ieee 802.11 be extremely high throughput: The next generation of wi-fi technology beyond 802.11 ax. *IEEE Communications Magazine*, IEEE, v. 57, n. 9, p. 113–119, 2019. Citado na página 3.

MOHTADI, H.; RAHIMI, A. New attacks on wi-fi protected setup. *Advances in Computer Science: an International Journal*, v. 4, n. 5, p. 127–132, 2015. Citado na página 2.

NIKOLOV, L. G. Wireless network vulnerabilities estimation. *Security & Future*, Scientific Technical Union of Mechanical Engineering"Industry 4.0", v. 2, n. 2, p. 80–82, 2018. Citado 2 vezes nas páginas 6 e 7.

RUFINO, N. M. d. O. *Segurança em redes sem fio: aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth*. [S.l.]: Novatec Editora, 2019. Citado na página 3.

SILVA, C. d. S. *Vulnerabilidade do WPS (Wi-fi Protected Setup) nas redes sem fio*. 2014. Citado 2 vezes nas páginas 2 e 5.

SOARES, L.; MORAES, I. Uma avaliação de vulnerabilidades em protocolos de autenticação para redes sem fio ieee 802.11. In: SBC. *Anais da III Escola Regional de Informática do Rio de Janeiro*. [S.l.], 2019. p. 37–40. Citado 2 vezes nas páginas 6 e 7.

STANGARLIN, D. P.; FILHO, W. P. *Análise de desempenho de redes sem fio com diferentes protocolos de criptografia*. 2017. Citado na página 4.

TANENBAUM, A. S. Redes de computadores. ed. *Campus-Tradução da Terceira Edição, Rio de Janeiro*, 2003. Citado na página 3.

TANENBAUM, J.; WETHERALL, D. *Redes de computadores. Tradução: Daniel Vieira.* [S.l.]: Pearson Prentice Hall: São Paulo, 2011. Citado 2 vezes nas páginas 1 e 2.

VALCHANOV, H.; EDIKYAN, J.; ALEKSIEVA, V. A study of wi-fi security in city environment. In: IOP PUBLISHING. *IOP Conference Series: Materials Science and Engineering*. [S.l.], 2019. v. 618, n. 1, p. 012031. Citado 2 vezes nas páginas 6 e 7.

VANHOEF, M.; PIESSENS, F. Key reinstallation attacks: Forcing nonce reuse in wpa2. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. [S.l.: s.n.], 2017. p. 1313–1328. Citado na página 5.

VIEHBÖCK, S. Brute forcing wi-fi protected setup. *Wi-Fi Protected Setup*, v. 9, 2011. Citado 2 vezes nas páginas 2 e 5.

Avaliação Final de TCC 01

ESTE DOCUMENTO DEVE SER PREENCHIDO PELO PROFESSOR AVALIADOR.

Este formulário será entregue junto com o pré-projeto impresso. Tal avaliação mais detalhada ajudará o aluno a evoluir seu trabalho futuro.

Professor, favor preencher antes da defesa apenas os nomes e a tabela de Avaliação Sobre o Documento.

Nome do Aluno: _____

Nome do Professor Avaliador:_____

Marque com um X a opção que melhor corresponde à sua avaliação.

Avaliação Sobre o Documento:

PARTE AVALIADA	RUIM	BOM	ÓTIMO
RESUMO			
INTRODUÇÃO			
OBJETIVOS			
REFERENCIAL TEÓRICO			
TRABALHOS RELACIONADOS			
PROPOSTA			
AVALIAÇÃO			
CRONOGRAMA			
ESCRITA EM GERAL			

Avaliação Sobre a Apresentação:

PARTE AVALIADA	RUIM	BOM	ÓTIMO
SEGURANÇA			
CLAREZA DE ARGUMENTAÇÃO			
TEMPO DE APRESENTAÇÃO			
SLIDES			

Nota :