ACADEMIA DA FORÇA AÉREA
DIVISÃO DE ENSINO

ANÁLISE DA EFICÁCIA DA TECNOLOGIA *WPA2-ENTERPRISE* SEM CERTIFICAÇÃO COMO PROTOCOLO DE SEGURANÇA DE UMA REDE SEM FIO[1]

ERICK JULIO PIRES DA SILVA[2]
GUILHERME AUGUSTO SPIEGEL GUALAZZI[3]

RESUMO

Os ataques cibernéticos no Brasil estão aumentando muito com o passar dos anos. No ano de 2020 foram reportados mais de 600 mil ataques dessa natureza ao Centro de Estudos, Repostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Esses ataques possuem diversos objetivos diferentes, como uso das máquinas alvo para “minerar” criptomoedas, realizar ataques DDoS ou roubar dados de uma organização (DINIZ; MUGGAH; GLENNY, 2014, p. 9). Geralmente, os atacantes buscam ganhar dinheiro com esses ataques, extorquindo empresas com ameaças de deletar seu banco de dados ou vazar informações sensíveis (SUTTO, 2021). Entretanto, também há aqueles que querem apenas danificar o sistema do alvo, por motivos pessoais relacionados a crenças, inclinação política, vingança, entre outros. A popularização da *internet*, agregada com a velocidade e facilidade com que a informação é disseminada, permite que um maior número de pessoas possua os conhecimentos e práticas necessárias para realizar ataques cibernéticos. Apesar da rápida evolução dos métodos de segurança da informação, é comum que ainda existam falhas e vulnerabilidades que possam ser exploradas. Dessa forma, este artigo, tem por objetivo analisar o nível de dificuldade de se conseguir acesso à rede *wi-fi* de uma organização que utiliza o protocolo WPA2-Enterprise sem certificação para autenticação dos seus usuários. Para isso, foi utilizada a técnica *evil-twin* e analisados os seus resultados.

Palavras-chave: Cibernética. Segurança. *Wi-fi*. *Pentest*.

1 Artigo apresentado para Avaliação Final do Trabalho de Conclusão de Curso, como pré-requisito para a conclusão do Curso de Formação de Oficiais Aviadores da Academia da Força Aérea de Pirassununga/ SP.

2 Cadete do 4º Esquadrão do Curso de Formação de Oficiais Aviadores da Academia da Força Aérea – Pirassununga/ SP.

3 Professor Doutor da Academia da Força Aérea – Pirassununga/ SP.

ANALYSIS OF THE EFFECTIVENESS OF WPA2-ENTERPRISE WITHOUT CERTIFICATE AS A WIRELESS NETWORK SECURITY PROTOCOL

ABSTRACT

Cyber attacks in Brazil are increasing a lot over the years. In 2020, more than 600 thousand attacks of this nature were reported to Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br). These attacks have a number of different goals, such as using the target machines to "mine" cryptocurrencies, carry out DDoS attacks, or steal data from an organization (DINIZ; MUGGAH; GLENNY, 2014, p. 9). Attackers often seek to make money on these attacks by extorting companies with threats of deleting their database or leaking sensitive information (SUTTO, 2021). However, there are also those who just want to damage the target's system, for personal reasons related to beliefs, political inclination and revenge. The popularization of the internet, combined with the speed and ease with which information is disseminated, allows a greater number of people to have the knowledge necessary to carry out cyber attacks. Despite the fast evolution of information security methods, there are still flaws and vulnerabilities that can be exploited. Thus, this article aims to analyze the level of difficulty of gaining access to the wi-fi network of an organization that uses WPA2-Enterprise without certification protocol for authentication of its users. For this, the evil-twin technique was used and its results were analyzed.

Keywords: *Cybernetics. Security. Wi-fi. Pentest.*

INTRODUÇÃO

Este trabalho analisa as dificuldades de acessar uma rede wi-fi protegida pelo protocolo *WPA2-Enterprise*, por meios de testes de penetração (*pentest*). É notório que há algum tempo a segurança cibernética vem ganhando a atenção de todo o mundo, especialmente a do Brasil (CEREWTA; LEITE; FILHO, 2022). Nos últimos anos, diversos documentos foram registrados acerca do uso desse espaço, definindo suas doutrinas, seus cuidados e suas potencialidades, como o Manual de Campanha - Guerra Cibernética, criado pelo Exército Brasileiro em 2017 e o Decreto nº10.222, que aprova a Estratégia Nacional de Segurança Cibernética (BRASIL, 2017, 2020). Para tanto, a segurança da tecnologia da informação precisa ser constantemente aperfeiçoada e reforçada.

O uso do espaço cibernético mostrou-se cada vez mais inevitável por todas as organizações mundiais, logo tornou-se essencial o investimento na área de defesa cibernética (CORREA, 2021?). Em 1998, o Departamento de Defesa dos Estados Unidos criou a Força-Tarefa Conjunta de Defesa de Redes de Computadores com a finalidade de manter a segurança dos seus sistemas de informação (USA, 2018). Estamos nos tornando cada vez mais dependentes da Rede mundial de computadores e de dispositivos eletrônicos conectados, entretanto apesar de possuir diversas consequências positivas, a introdução da cibernética trouxe mais um problema: os ataques cibernéticos.

A segurança da rede é de extrema importância para qualquer instituição, especialmente as governamentais, que trabalham com documentos sensíveis. A constante verificação dos procedimentos de segurança da informação adotados é essencial para a manutenção da seguridade do sistema. Caso seja constatada alguma vulnerabilidade, é necessário que as atualizações e correções sejam feitas tão breve quanto possível, pois quanto maior o tempo que a vulnerabilidade existir, maior será a exposição do sistema a um possível ataque.

O objetivo deste trabalho é identificar as dificuldades de conseguir acesso não autorizado a uma rede *wireless.* Esse propósito será conseguido através de experimentos de testes de penetração em uma rede *wireless* que utiliza o protocolo *WPA2-Enterprise* sem certificação, utilizando técnicas e *softwares* específicos para esse fim.

Quanto ao método de abordagem, será qualitativa, em que será feito uma análise dos dados obtidos na fase experimental.

Por fim, esse trabalho também reafirma a necessidade de manter todos os sistemas digitais atualizados no que diz respeito às tecnologias de segurança disponíveis, a fim de mitigar os riscos de um possível ataque cibernético.

1 REFERENCIAL TEÓRICO

Redes sem fio de instituições que utilizam o protocolo *WPA2-Enterprise* sem certificação estão constantemente sob a possibilidade de um ataque do tipo *evil-twin*, visto que são poucas as barreiras que impedem esse tipo de ataque nessas redes (NUSSEL, 2010). De acordo com Pinto e Stuttart (2011) “Muitas aplicações web empregam pouco ou nenhum controle sobre a qualidade das senhas de seus usuários”. O mesmo se aplica à qualquer tipo de senha digital, como senhas de acesso a redes sem fio.

1.1 Características de rede *wi-fi*

Segundo o modelo OSI, os protocolos para redes de computadores se divide em sete camadas:

- 7. Camada de aplicação;
- 6. Camada de apresentação;
- 5. Camada de sessão;
- 4. Camada de transporte;
- 3. Camada de rede;
- 2. Camada de enlace de dados;
- 1. Camada física.

Os dados em redes *wireless* trafegam pela camada de enlace, ou seja, na camada 2. Mais especificamente, esses dados trafegam através do protocolo padrão IEEE 802.11. Desde 1997, esse padrão evolui aumentando a taxa, alterando a frequência de transmissão e a modulação (MORENO, 2016).

As redes de computadores podem ser classificadas conforme seu ambiente. Segundo Moreno (2016), podem ser:

> ***LAN* (*Local Area Network*)** – Rede de área local. Nesse tipo de topologia há um pequeno número de ativos (computadores) interconectados e sua abrangência é pequena (redes domésticas, pequenas redes empresariais, redes de hotéis etc.).
> ***WLAN* (*Wireless Local Area Network*)** – Redes *LAN* que utilizam *wireless* como forma de comunicação e troca de dados (em vez de cabos), sendo categorizados como *WLAN*.
> ***MAN* (*Metropolitan Area Network*)** – Rede de área metropolitana. Interligação das *LANs*/*WLANs* de uma mesma área geográfica, formando uma MAN.

> ***WAN* (*Wide Area Network*)** – Rede de longas distâncias. Redes *WAN* são a interligação das *MANs*. A internet é um exemplo de *WAN*. O seu endereço *WAN* pode ser consultado visitando o site http://www.meuip.com.br.

Portanto, as redes *wi-fi* de instituições podem ser caracterizadas como *WLAN*, pois são redes locais *wireless*, limitadas aos limites da organização.

1.2 Conexão a uma rede *wireless*

Uma conexão *wireless* é composta, geralmente, por um Cliente (STA) a um Ponto de Acesso (AP). O Ponto de Acesso é o dispositivo que interconecta os dispositivos conectados a ele, configurando assim uma rede local. O Cliente é o dispositivo que se conecta ao ponto de acesso. Segundo Moreno (2016), “Todo e qualquer dispositivo *wireless* (computadores, smartphones e outros) é um cliente ou *Station*.”.

Para entender como uma conexão *wireless* é feita, é necessário conhecer os conceitos a seguir. A comunicação entre o ponto de acesso e o cliente é feita de *frames*. Os *frames* responsáveis por essa conexão são:

- ***Beacon*** – *frame* constantemente enviado pelos APs para manter a rede *wireless* ativa;
- ***Probe Request*** – frame que conecta automaticamente o STA ao AP, caso essa conexão já tenha acontecido no passado;
- ***Probe Response*** – Resposta do AP ao STA que enviou um *probe request;*
- ***Authentication*** – *frame* que comunica algum tipo de autenticação;
- ***Association Request*** – uma vez realizada a autenticação, o pedido para associação é feito à rede;
- ***Deauthentication/Disassociation*** – *frame* que desconecta o cliente do AP; e
- ***Reassociation Request* e *Reassociation Response*** – *frame* enviado pelo cliente ao encontrar um AP com um sinal mais forte, a fim de se conectar a ele.

A conexão *wi-fi* ocorre na seguinte sequência:

1. Cliente envia *probe request;*
2. AP responde com um *probe response;*
3. Cliente envia um a*uthentication request*, e ocorre o processo de autenticação com o AP;
4. AP responde com um *authentication response; e*

5 Finalmente, o cliente envia um a*ssociation request,* que é respondido pelo AP por um *association response*.

Para garantir a segurança da rede, foram desenvolvidas criptografias que impedem de clientes indesejados se conectarem aos pontos de acesso, ou que dificultam a captura e leitura de pacotes que circulam na rede. São eles: OPN, WEP, OPN/SKA, WPA/WPA2 PSK, WPA Enterprise e o protocolo WPS. A OPN não apresenta um sistema de criptografia, portanto não ocorre nenhum processo de autenticação durante a conexão. Esse tipo de acesso não requer senha, portanto qualquer dispositivo pode entrar na rede. A WEP (*Wired Equivalent Privacy*), acrescenta criptografia apenas aos pacotes que circulam na rede. Dessa forma, caso os pacotes sejam capturados, eles não serão facilmente lidos, por estarem criptografados. Entretanto o algoritmo utilizado nessa criptografia pode ser quebrada em minutos, segundo Moreno (2016). A WPA (*wifi protected access*), criptografia que será explorada neste trabalho, utiliza um protocolo em que cada pacote contém uma chave diferente. Cada comunicação feita entre o AP e o cliente deve ser autenticada por ambas as partes.

A autenticação da conexão de rede pela criptografia WPA2-Enterprise acontece por um fenômeno chamado 4-*way handshake*. Esse mecanismo ocorre da seguinte forma:

> Na primeira fase, ambas as partes, o AP e o cliente, concordarão com a política de segurança (método de autenticação, protocolo para tráfego *unicast*, protocolo para tráfego *multicast* e método de pré-autenticação) para usar o que é suportado pelo AP e pelo cliente. Na segunda fase (aplicável apenas ao modo Enterprise) a autenticação 802.1X é iniciada entre o AP e o cliente usando o método da autenticação para gerar uma MK (chave mestra comum). Na terceira fase após uma autenticação bem-sucedida, chaves temporárias (cada chave tem vida útil limitada) são criadas e atualizadas regularmente; o objetivo geral desta fase é geração e troca constantes da chave. Na quarta fase todas as chaves geradas anteriormente são usadas pelo protocolo CCMP para fornecer confidencialidade e integridade aos dados (ARANA, 2006, tradução nossa).[4]

Na WPA *Enterprise* a geração e distribuição de uma chave mestra é gerada por um servidor chamado Radius. Essa autenticação é chamada de *Extensible Authentication*

4 In the first phase the parties, AP and the client, will agree on the security policy (authentication method, protocol for unicast traffic, protocol for multicast traffic and pre-authentication method) to use that is supported by the AP and the client. In the second phase (applicable to Enterprise mode only) 802.1X authentication is initiated between the AP and the client using the preferred authentication method to generate an MK (common Master Key). In the third phase after a successful authentication, temporary keys (each key has limited lifetime) are created and regularly updated; the overall goal of this phase is key generation and exchange. In the fourth phase all the previously generated keys are used by the CCMP protocol to provide data confidentiality and integrity.

Protocol (EAP). EAP é o protocolo que propicia a autenticação do usuário através de um servidor. Dessa forma, os protocolos WPA que utilizam EAP podem ser chamados de WPA-EAP. Nas redes WPA/WPA2 PSK, a chave mestra é gerada e distribuída pelo próprio AP (PAIM, 2011?).

Segundo Nussel (2010), a conexão do cliente com o AP através do servidor Radius com certificação é feita através de um “túnel” utilizando o protocolo de segurança TLS ou SSL. Esses protocolos codificam as informações passadas de um ponto a outro, nesse caso as informações de usuário e senha do cliente para o servidor. No caso de uma autenticação via servidor Radius, esses protocolos permitem a autenticação segura do cliente com o servidor.

1.3 Vulnerabilidades do protocolos *WPA2-ENTERPRISE*

As vulnerabilidades de conexão em redes WPA podem acontecer em qualquer ponto da sequência de conexão descrita anteriormente. Os invasores podem, por exemplo, tentar capturar os dados da comunicação entre o cliente e o servidor, e tentam os descriptografar o usuário e senha obtidos. Em caso de sucesso, o atacante consegue a senha de acesso à rede sem fio alvo.

Em geral, o protocolo WPA2 é vulnerável a ataques de DoS (negação de serviço), interferência de rádio frequência, *data flooding*, sequestro de sessão no que diz respeito à disponibilidade da rede. Esses ataques deixam a rede indisponível para uso. Além disso, nenhum protocolo de segurança impedirá ataques físicos aos APs bem como não impedirá falhas eventuais. O WPA2 também é vulnerável contra desautenticação. O atacante pode forçar a desautenticação do dispositivo cliente, de forma que ele possa controlar os *frames* usados para autenticação e imitar o MAC *Adress* do alvo, se passando por ele (ARANA, 2006).

Esser (2017) diz que há três tipos de WPA-EAP. O WPA-EAP com certificação do servidor, o WPA-EAP com certificação do servidor e do usuário e o WPA-EAP sem certificação. O primeiro faz com que o dispositivo cliente autentique o servidor por uma certificação via TLS. Com isso, o cliente garante que está acessando o servidor verdadeiro para então enviar os dados de conexão. O segundo faz com que tanto o cliente quanto o AP necessitem da autenticação um do outro por meio de uma certificação via TLS. Dessa forma, mesmo que o atacante intercepte os dados, ele não conseguiria as informações de conexão, pois ele somente receberia essas informações após o cliente ter certeza que está conversando com o servidor correto através da certificação, porém essa

nunca viria. Portanto, nesse caso, as informações obtidas pelo atacante seriam irrelevantes. A conexão WPA-EAP sem certificação não possui qualquer tipo de meio para que o cliente ou o servidor confirmem se são legítimos. Dessa forma o cliente sempre enviará os dados de conexão àquele AP com qual tente se conectar, mesmo que seja um AP falso.

Segundo Esser (2017), a falta de uma encriptação na comunicação entre o cliente e o AP possibilita que o atacante monitore o tráfego e capture facilmente a autenticação *challenge-response,* pois o cliente enviará as informações de conexão (usuário e senha) para o AP sem certificação de que esse AP é o correto. Por essa razão, essas redes são altamente suscetíveis a ataques utilizando a técnica *evil-twin.* Essa técnica consiste na criação de um AP falso por parte de atacante, de forma que o dispositivo do usuário tentará se conectar nesse AP enviando o usuário e senha criptografados como se fosse par ao AP da rede verdadeira, pois não haverá uma forma de autenticação entre o cliente e o servidor.

> É importante notar que, em um cenário onde o objetivo do atacante é obter acesso à rede corporativa, o invasor faria um ataque numa maior área, pois haveria muitos clientes com credenciais diferentes e o invasor precisaria apenas quebrar uma das credenciais para obter acesso. Novamente o comportamento do cliente é o elo mais fraco para manter a própria rede segura (ESSER, 2017, p. 33).

Uma área em que há várias pessoas utilizando a rede corporativa da organização, pode ser um grande alvo para os atacantes. Uma vez criada o AP falso, há uma possibilidade de que alguns dispositivos se conectem a essa rede, enviando as informações de acesso codificadas ao atacante sem que ninguém saiba, pois nenhuma notificação é enviada ao dispositivo alvo além da falha da conexão. Após isso, o trabalho do atacante é apenas descriptografar os dados obtidos.

1.4 Criptografia como barreira de ataques

A criptografia é o ato de codificar mensagens, de tal modo que somente é possível decodificá-la com a chave certa. Foi importante desde a antiguidade para transmitir mensagens secretas entre generais durante guerras, ou entre governadores. Durante a 2ª Guerra Mundial, por exemplo, a máquina Enigma foi usada para comunicação entre as tropas e diplomacia alemã. Essa máquina foi criada em 1918 por Arthur Scherbius e aperfeiçoada até o uso pelos alemães (FIGUEIREDO, COSTA, 2010).

O protocolo WPA2 a ser analisado neste trabalho utiliza o AES (Advanced Encryption Standard) como padrão de segurança. O AES é um algoritmo de chave simétrica, ou seja, a chave usada tanto para codificar quanto para descodificar é a mesma, e a principal vantagem desse método é que ele é simples tanto para o destinatário quanto para o remetente. Porém essa também pode ser uma desvantagem já que caso alguém indesejado obtenha essa chave, também será simples para ele decodificar a mensagem (OLIVEIRA, 2012).

Cada camada de segurança utilizada acrescenta uma barreira para dificultar uma invasão. Pode-se fazer um paralelo com a Teoria do Queijo Suíço de Reason (1997), que dizia que os acidentes acontecem devido à existência de falhas nas diferentes barreiras que impedem que o acidente aconteça, de forma que o improvável alinhamento dessas falhas leva ao acidente. Quanto mais barreiras, menor a probabilidade de que os buracos, ou falhas, se alinhem. Do mesmo modo, quanto mais barreiras que dificultem o ataque a uma rede sem fio, menor a probabilidade de que esse ataque seja bem-sucedido.

1.5 Força de senha

Uma senha forte é uma das melhores maneiras de se manter um sistema seguro. A segurança da informação é basicamente baseada em um sistema de autenticação (com uma senha), de forma que aquele que sabe a senha possui acesso àquela informação, conteúdo ou privilégio. Porém como se analisa uma senha para dizer que ela é forte? De forma geral, os ataques a senhas tentam diferentes combinações de caracteres para se chegar à senha correta. Para isso, os atacantes utilizam *wordlist* públicas, *brute force* ou podem até mesmo criar as próprias *wordlists* com base em informações do alvo, por exemplo. Dessa forma a *worlist* se tornaria mais eficiente e precisa contra aquele alvo. Uma senha segura seria aquela que possui no mínimo 8 caracteres, sendo no mínimo 3 caracteres especiais e um alfanumérico (MA; CAMPBELL; TRAN; KLEEMAN, 2010).

2 METODOLOGIA

Conforme se salientou na introdução, foi analisado o nível de segurança contra acessos de pessoas não autorizadas em uma rede sem fio de computadores. Para isso, foram usadas situações criadas através da manipulação do objeto de estudo por meio de técnicas e softwares específicos.

O objeto de estudo é a rede *wi-fi* de uma instituição que utiliza o *WPA2-Enterprise* sem certificação como método de autenticação. Os testes foram feitos utilizando uma

rede simulada, através da configuração de um ponto de acesso falso com as mesmas características de conexão dos *"Access Points"* legítimos dessa instituição.

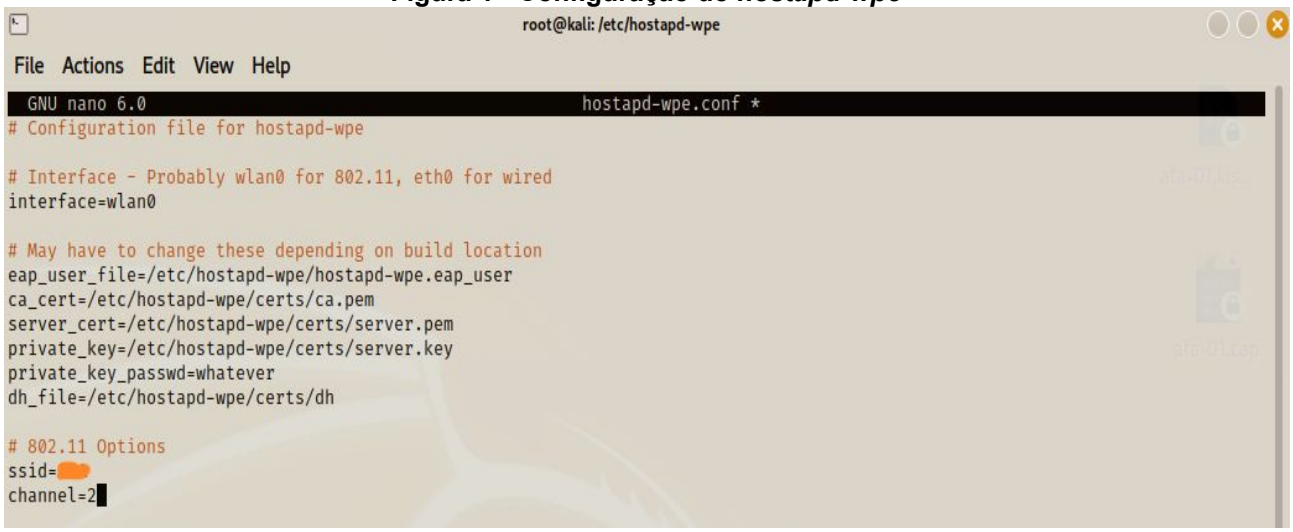
Para a execução dos experimentos, foram necessários *notebook* e *smartphone* pessoais com o sistema operacional *Kali Linux* e *Android* instalado, respectivamente, que foram usados como máquinas "atacante" e "alvo". No *Kali Linux*, foram instalados ferramentas que auxiliaram direta ou indiretamente nos ataques, como *aircrack-ng*, *hostapd-wpe*, e *John the Ripper*. O *notebook* com o sistema *Kali Linux* utilizado foi um *Dell G3 3590 a60p*, e o *smartphone* foi um *Samsumg Tab E SM-T560* com o sistema operacional *Android* 7.1.2.

O *Kali Linux* é um sistema operacional (SO) derivado do Linux, criado pela empresa Offensive Security. Essa distribuição foi criada para servir como um sistema de *pentest*, possuindo de forma nativa diversas ferramentas desenvolvidas para esse fim, como aquelas já citadas no parágrafo anterior. Esse sistema operacional foi escolhido por já possuir todas as ferramentas necessárias para os experimentos. Entretanto qualquer distribuição Linux poderia ser utilizada, desde que as ferramentas fossem instaladas. Ressalta-se que essas ferramentas foram desenvolvidas exclusivamente para o Linux, portanto na presente data não são compatíveis com outros sistemas operacionais.

A técnica de teste de penetração de redes *wi-fi* foi o *evil-twin,* que consiste na criação de um ponto de acesso falso para que o alvo se conecte a ele e envie as chaves de autenticação *challenge-response*, que posteriormente são descriptografados para conseguir a senha de acesso à rede.

Inicialmente, o *software hostapd-wpe* foi configurado para a criação de uma rede de mesmo nome da rede alvo, conforme Figura – 1. A captura de tela na íntegra encontra-se no Anexo A. Por questões de segurança o nome da rede foi censurado. O canal *wi-fi* utilizado na criação dessa rede foi o canal 2.

Figura 1 - Configuração do *hostapd-wpe*

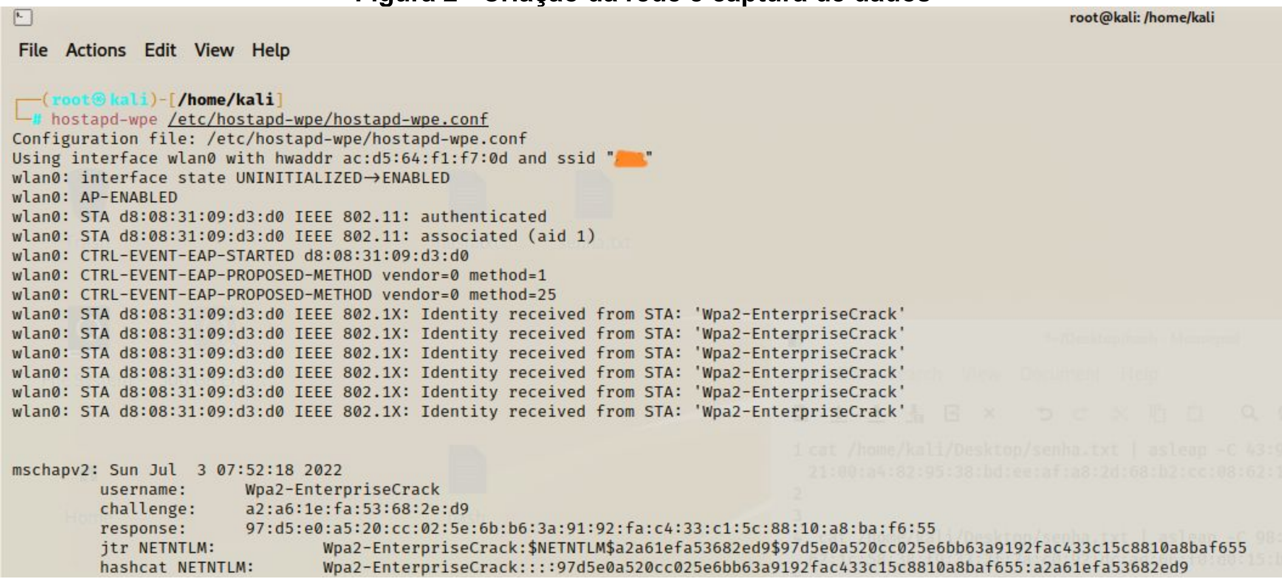


Fonte: O próprio autor.

A rede falsa foi criada com o mesmo nome da rede legítima para simular uma situação real, em que o atacante o faria para confundir o usuário, para que esse tentasse se conectar à rede falsa ao invés da rede verdadeira. Além disso, a rede verdadeira utiliza o canal 11 para operação. Para a rede falsa foi escolhida o canal 2 inicialmente. Caso houvesse conflito de canais no decorrer do experimento, outros canais poderiam ser utilizados para os testes. Ressalta-se que a rede legítima era uma rede 802.11n que utiliza a banda 2,4 GHz, portanto os canais disponíveis para o experimento seriam do 1 ao 13, com exceção do 11 que já é utilizado pela rede verdadeira.

Em seguida, o mesmo *software* foi utilizado para a criação do ponto de acesso falso através do comando "*hostapd-wpe /etc/hostpad-wpe/hostapd-wpe.conf*" no terminal do *Kali Linux*. Percebeu-se, nesse momento, que automaticamente a máquina alvo, que já estava configurada para acessar a rede verdadeira, tentou se conectar à rede falsa. A máquina alvo tentou se conectar à rede falsa utilizando um usuário e senha criados unicamente para o teste, e não correspondem a nenhum usuário legítimo da rede da instituição em questão. Assim que o cliente se comunicou com a rede falsa criada, a ferramenta hostapd-wpe capturou as informações de nome de usuário e a chave *challenge-response*, conforme observado na Figura 2. A captura de tela na íntegra encontra-se no Anexo B.

Figura 2 - Criação da rede e captura de dados

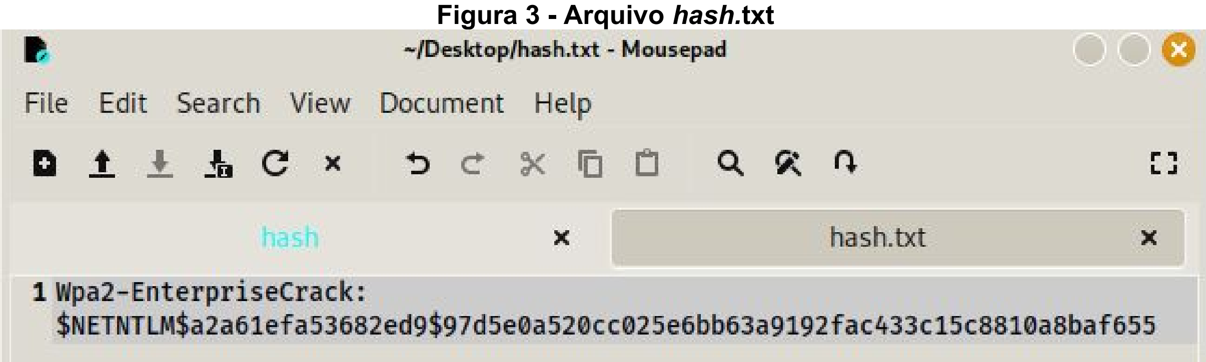


Fonte: O próprio autor.

Observa-se que a chave *challenge-response* foi capturada criptografada com a tecnologia mschapv2, que é a criptografia comumente utilizada em redes WPA-EAP sem certificação.

Após, foi criado um arquivo de texto de nome *hash*.txt e nele foi colocado o texto à frente de "*jtr NETNTLM*" capturada no passo anterior, conforme Figura 3. Em "jtr NETNTLM", jtr se refere à ferramente Jhon The Ripper, e NETNTLM se refere ao tipo de hash que foi capturado. O NETNTLM é derivado do hash NT, que criptografa a senha do usuário utilizando o algoritmo MD4, junto ao algoritmo de *challenge/response*.

Figura 3 - Arquivo *hash*.txt

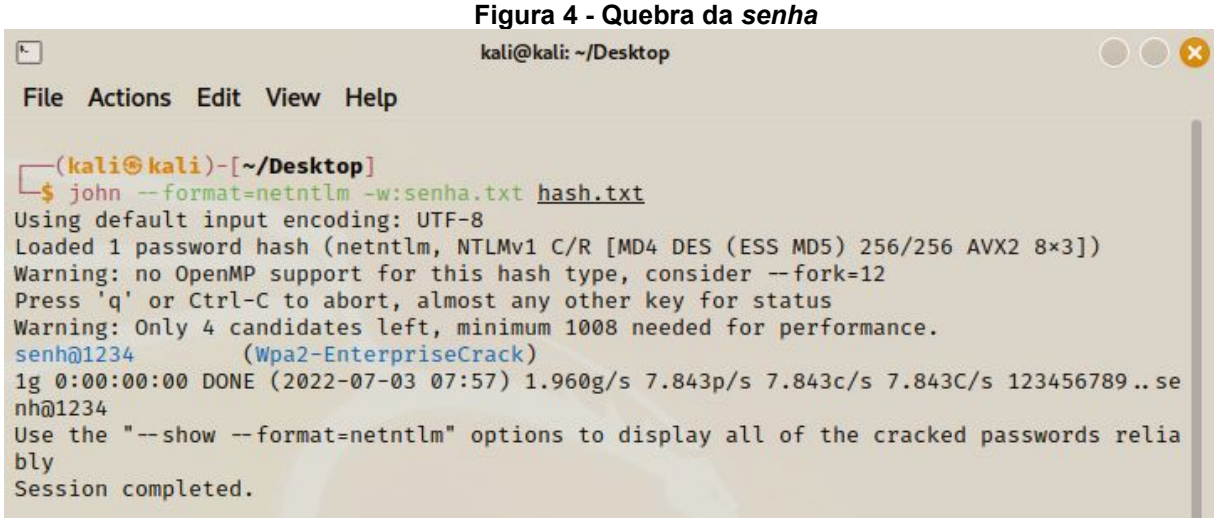


Fonte: O próprio autor.

Feito isso, uma *wordlist* foi utilizada através do *software John The Ripper* para a quebra da *hash.* Por fins de experimento, uma *wordlist* de nome senha.txt foi especificamente criada para esse teste. Essa *wordlist* continha apenas 5 combinações de possíveis senhas, sendo 4 delas aleatórias e uma a senha que foi utilizada para o teste. O comando utilizado para a quebra da senha foi "*john –format=netntlm* -w*:*senha.txt *hash*.txt", no terminal do *Kali Linux*. Rapidamente a senha foi quebrada e mostrada na tela

do computador, conforme Figura 4. O usuário é “Wpa2-EnterpriseCrack” e a senha é “senh@1234”.

Figura 4 - Quebra da *senha*



Fonte: O próprio autor.

3 RESULTADOS E DISCUSSÃO

As Figuras 1, 2, 3 e 4 representam cronologicamente os passos seguidos desde o início do ataque até o seu sucesso. Desconsiderando o tempo de instalação dos sistemas operacionais e *softwares* necessários nas máquinas atacante e alvo, foram gastos cerca de 20 minutos desde a configuração *hostapd-wpe* até a quebra da senha.

Os conhecimentos observados necessários para a realização desse tipo de ataque foram como funciona do protocolo de segurança de redes sem fio utilizada neste experimento, o funcionamento do sistema de autenticação desse protocolo, uso do sistema *Kali Linux* como meio para testes de penetração, princípios de criação de rede sem fio, princípios de criptografia e descriptografia e utilização dos *softwares hostapd-wpe* e *John The Ripper.*

Não foi necessário o uso de *softwares* de negação e/ou desautenticação, como o *aireplay-ng*, pois imediatamente após a criação do ponto de acesso falso a máquina alvo se desconectou da rede verdadeira e iniciou tentativas de conexão à rede falsa, enviando o nome de usuário sem qualquer tipo de criptografia e a chave *challenge-response*, criptografada pelo método *mschapv2*, que foi automaticamente transformada no formato *NETNTLM* pela ferramenta *hostapd-wpe.* O formato da chave necessária para a realização desse tipo de criptografia pelo *John The Ripper* é o NETNTLM.

Não foi observado qualquer tipo de resistência contra esse ataque nem por parte do cliente (máquina alvo), nem por parte do servidor. Nesse caso, o único obstáculo enfrentado foi a descriptografia da chave para obtenção da senha. Como a senha a ser

obtida era simulada e conhecida do autor, e a *wordlist* usada foi criada especificamente para esse fim, a quebra da chave foi facilmente realizada e a senha rapidamente conseguida. Em um ataque verdadeiro utilizando os mesmos equipamentos utilizados nesse experimento, o sucesso, ou não, bem como a velocidade da obtenção da senha em caso de sucesso, dependeria unicamente da força da senha do usuário.

> O nível de segurança das senhas está relacionado ao quão rápido elas podem ser quebradas. Com relação a ataques brute force (tentativa e erro) e de dicionário (o mesmo que brute force, porém com palavras pré-selecionadas) quanto mais caracteres e variações de caracteres, mais difícil será quebrá-la. Então, pode-se dizer que senhas fortes têm as seguintes características: São longas, acima de 8 dígitos. Possuem letras maiúsculas e minúsculas (sistema deve diferenciá-las), números e outros caracteres. Não são palavras, nomes ou datas comumente usadas. (AOKI, 2011)

Além disso, senhas vazadas na *internet* também não são seguras, uma vez que são frequentemente incluídas em *wordlists* populares, como a *rockyou.*txt, disponibilizada no sistema *Kali Linux* no ato da instalação desse sistema. Essa *wordlist* possui mais de 14 milhões de senhas, usadas em mais de 32 milhões de contas.

4 CONSIDERAÇÕES FINAIS

Este estudo descreveu uma análise da eficácia da tecnologia *WPA2-Enterprise* como protocolo de segurança de uma rede sem fio. Para isso, um experimento do tipo teste de penetração foi realizado em uma rede sem fio de uma instituição verdadeira. Este estudo teve como objetivo identificar as dificuldades de conseguir acesso não autorizado a uma rede *wireless.*

Comprovou-se, por meio do experimento realizado, que a rede *WPA2-Enterprie,* apesar de todos os recursos de criptografia e segurança utilizados por essa tecnologia, pode facilmente ser alvo de um ataque do tipo *evil-twin* se não possuir processo de certificação entre cliente e servidor. Foi observado que, após a sobtenção da chave *challenge-response,* a ação de descriptografar é facilmente realizada através de um único comando, e o seu sucesso depende unicamente da força da senha do usuário.

Portanto, para uma melhor segurança contra invasões em redes sem fio configuradas com o *WPA2-Enterprise*, sugere-se que sejam usadas certificações na conexão entre cliente e AP, para que hajam mais barreiras contra possíveis ataques na rede. Além disso, os usuários devem ser conscientizados a utilizar senhas mais fortes e originais, de forma que seja improvável que essas senhas estejam presentes em *wordlists* e que torne mais difícil o sucesso de um *brute force*.

Assim, conclui-se que a tecnologia *WPA2-Enterprise* sem certificação não é eficaz como protocolo de segurança de uma rede sem fio, pois é altamente dependente da força da senha do usuário para que seja segura.

A principal contribuição deste experimento foi a conscientização de administradores e usuários de redes de computadores que a segurança da rede dependem tanto do algoritmo utilizado na configuração da rede quanto da força das senhas utilizadas para acesso. Os administradores devem buscar implementar sempre a melhor tecnologia disponível e acessível nas suas redes, bem como os usuários devem atentar-se à segurança de suas senhas.

REFERÊNCIAS

ARANA, Paul. **Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)**. INFS 612, 2006.

AOKI, Eric. **Práticas de segurança para o desenvolvimento de sistemas web**. Iniciação Científica (Curso de Bacharelado em Análise de Sistemas e Tecnologia da Informação), FATEC-São Caetano do Sul. São Caetano do Sul, 2011.

BRASIL. **Decreto nº10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, 2020.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 01 de jul. de 2022.

BRASIL. Exército Brasileiro. **EB70-MC-10.232 - Manual de Campanha – Guerra Cibernética**. 2017. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf. Acesso em 17 de ago. de 2021.

CEREWUTA, Pollyanna; LEITE, Roniel; MARTINS FILHO, Rogério. **A Ascensão dos Crimes Cibernéticos no Contexto Contemporâneo**. JNT – Facit Business and Technology Journal. QUQLIAS B1. FLUXO CONTÍNUO. 2022.

CORREA, José. **Defesa e Segurança Nacional no Espaço Cibernético**. Centro de Defesa e Segurança Nacional. 2021?. Disponível em: https://cedesen.com.br/defesa-e-seguranca-nacional-no-espaco-cibernetico/. Acesso em: 17 de ago.de 2022.

COSTA, Celso José; FIGUEIREDO, Luiz Manoel. **Criptografia Geral**. 2 ed. Rio de Janeiro, 2006.

DINIZ, G; MUGGAH, R; GLENNY, M. **Desconstructing Cyber Security in Brazil: threats and responses**. Strategic Paper 11: Instituto Igarapé. 2014. Disponível em: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf. Acesso em: 17 de ago. de 2022.

ESSER, André. ***Framework Evil-Twin* - Um teste de intrusão *wi-fi* para *pentesters***. Tese (Mestrado em Telecomunicações e Engenharia da Computação) - Departamento de Ciência da Informação e Tecnologia, Instituto Universitário de Lisboa. Lisboa, 2017.

ESTADOS UNIDOS DA AMÉRICA. **U.S. Cyber Command**. U.S. Cyber Command History. Washington DC, [2020?]. Disponível em https://www.cybercom.mil/About/History/. Acesso em 01 de jul. de 2022.

HOSTAPD-WPE. **hostapd-wpe Usage Example**. Disponível em: https://www.kali.org/tools/hostapd-wpe/. Acesso em: 04 de jul. de 2022.

JOHN THE RIPPER. **John The Ripper password cracker**. Disponível em: https://www.openwall.com/john/. Acesso em: 04 de jul. de 2022.

KALI LINUX DOCUMENTATION. **What is Kali Linux?**. Disponível em: https://www.kali.org/docs/introduction/what-is-kali-linux/. Acesso em: 10 de ago. de 2022.

KAN, Ahmed. **Atacando rede sem fio WPA Enterprise**. Pentest.blog, 2016. Disponível em: https://pentest.blog/attacking-wpa-enterprise-wireless-network/. Acesso em: 26 de jun. de 2022.

MORENO, Daniel. **PENTEST em redes sem fio**. São Paulo: Novatec Editora, 2016.

NUSSEL, Ludwig. **The Evil Twin problem with WPA2-Enterprise**. SUSE Linux Products GmbH, 2010.

OLIVEIRA, Ronielton. **Criptografia simétrica e assimétrica: os principais algoritmos de decifragem**. Revista Segurança Digital, 2012.

OFFENSIVE SECURITY. **What is Kali Linux?**. Disponível em: http://docs.kali.org/introduction/what-is-kali-linux. Acesso em: 26 de jun. de 2022.

PAIM, Rodrigo. **WEP, WPA E WEP**. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2011?. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/index.html. Acesso em 17 de ago. de 2022.

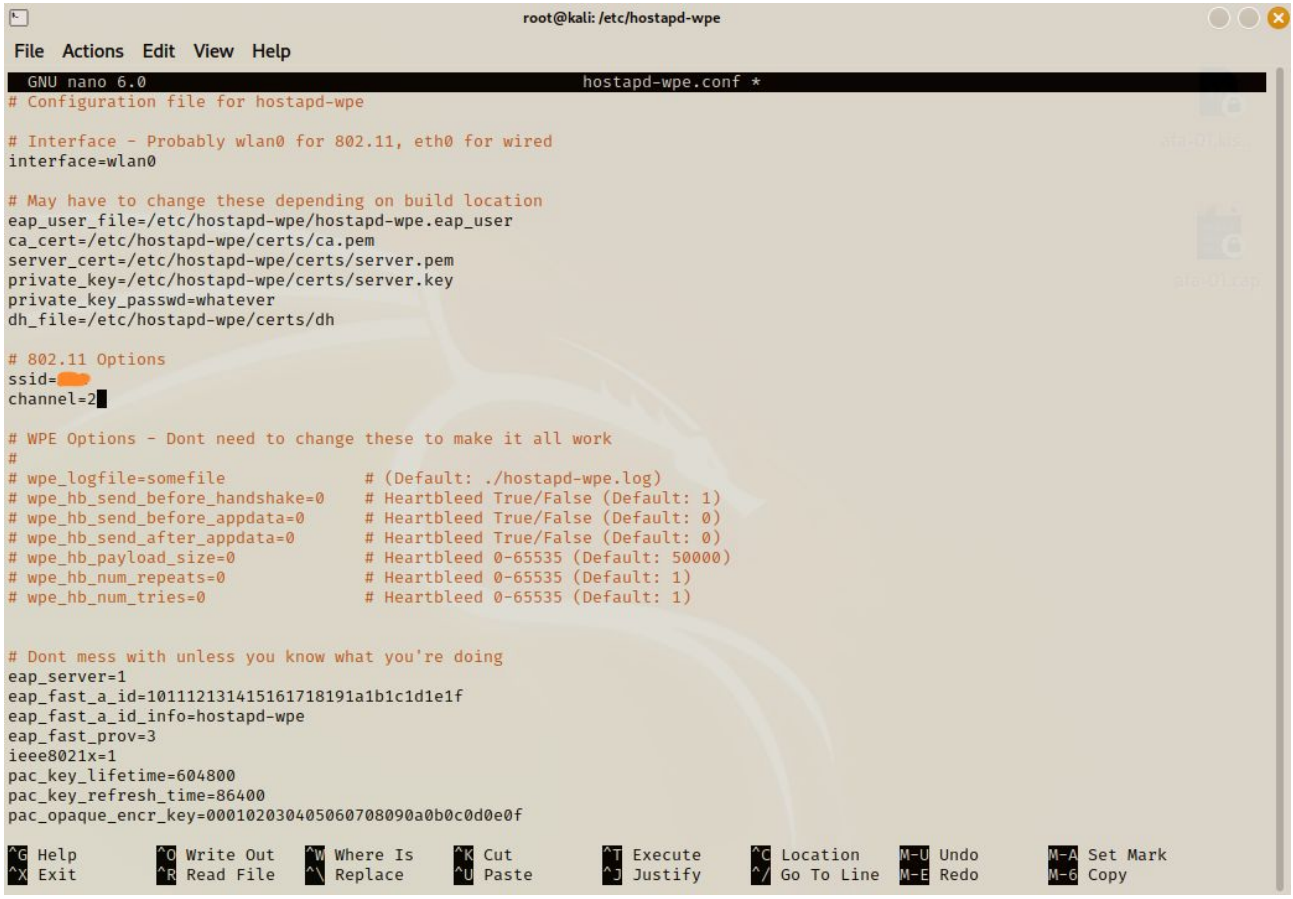
PINTO, Marcus; STUTTARD, Dafydd. **The web application Hacker's Handbook: Finding and Exploiting Security Flaws**. Estados Unidos da América: Wiley Publishing, Inc, 2011.

ROCKYOU.TXT. **Rockyou.txt**. Disponível em: https://www.kaggle.com/datasets/wjburns/common-password-list-rockyoutxt. Acesso em: 04 de jul. de 2022.

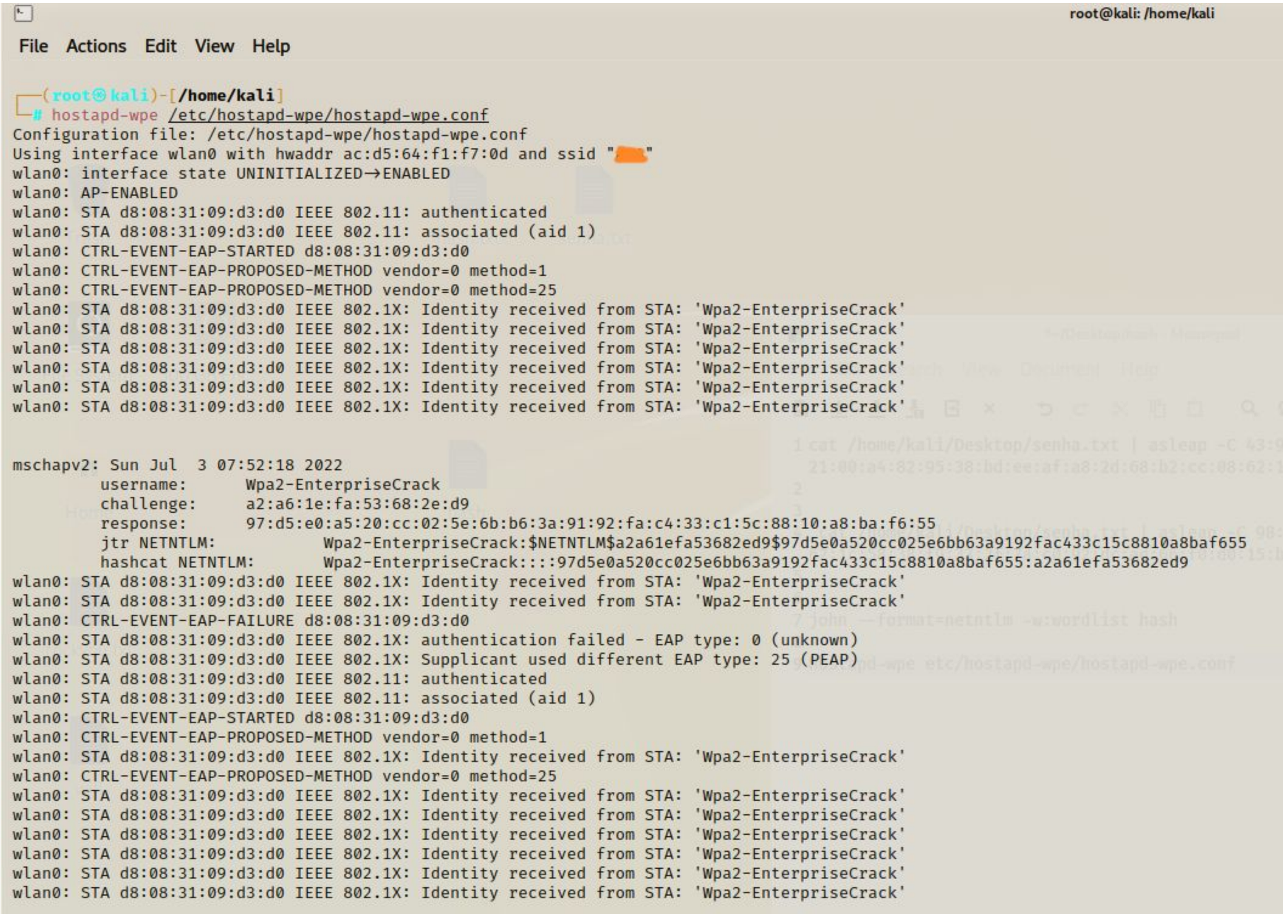
REASON, James. **Managing the Risks of Organizational Accidents**. Aldershot: Ashgate, 1997.

SUTTO, Giovanna. **Ataques cibernéticos sequestram dados para extorsão de empresas: o que fazer?**. Infomoney, 2021. Disponível em: https://www.infomoney.com.br/minhas-financas/ataques-ciberneticos-sequestram-dados-para-extorsao-de-empresas-o-que-fazer/. Acesso em: 17 de ago. De 2022.

ANEXO A – Configuração do *hostapd-wpe*



ANEXO B – CRIAÇÃO DA REDE E CAPTURA DE DADOS



```
root@kali: /home/kali
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan0 with hwaddr ac:d5:64:f1:f7:0d and ssid "[redacted]"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.11: authenticated
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED d8:08:31:09:d3:d0
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'


mschapv2: Sun Jul  3 07:52:18 2022
         username:      Wpa2-EnterpriseCrack
         challenge:     a2:a6:1e:fa:53:68:2e:d9
         response:      97:d5:e0:a5:20:cc:02:5e:6b:b6:3a:91:92:fa:c4:33:c1:5c:88:10:a8:ba:f6:55
         jtr NETNTLM:           Wpa2-EnterpriseCrack:$NETNTLM$a2a61efa53682ed9$97d5e0a520cc025e6bb63a9192fac433c15c8810a8baf655
         hashcat NETNTLM:       Wpa2-EnterpriseCrack::::97d5e0a520cc025e6bb63a9192fac433c15c8810a8baf655:a2a61efa53682ed9
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: CTRL-EVENT-EAP-FAILURE d8:08:31:09:d3:d0
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.11: authenticated
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED d8:08:31:09:d3:d0
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
wlan0: STA d8:08:31:09:d3:d0 IEEE 802.1X: Identity received from STA: 'Wpa2-EnterpriseCrack'
```