Penetração sem fio Kali Linux

Palavras de código em texto, nomes de tabelas de bancos de dados, nomes de pastas, nomes de arquivos, extensões de arquivos,

nomes de caminho, URLs fictícios, entrada do usuário e identificadores do Twitter são mostrados da seguinte maneira:

"Primeiro executamos o airmon-ng start wlan0 para colocar a interface no modo monitor"

Qualquer entrada ou saída da linha de comandos é escrita da seguinte forma:

# aireplay-ng --chopchop -b 08: 7A: 4C: 83: 0C: E0 -h 1C: 4B: D6: BB: 14: 06 mon0

Novos termos e palavras importantes são mostrados em negrito. Palavras que você vê no

tela, por exemplo, em menus ou caixas de diálogo, aparecem no texto assim: "Clique em

o botão Novo no menu da barra de ferramentas e o assistente é iniciado. "

Avisos ou notas importantes aparecem em uma caixa como essa.

Dicas e truques aparecem assim.

O processo de teste de penetração pode ser dividido em quatro fases principais ou estágios,

quais são como segue:

• Planejamento

• Descoberta

• ataque

• Relatório

Testando o adaptador para teste de penetração sem fio

Agora que configuramos o adaptador, podemos executar um pequeno teste para verificar se ele é realmente

adequado para testes de penetração sem fio, isto é, pode ser colocado no modo monitor e

suporta injeção de pacote. Para isso, usamos dois programas do pacote Aircrack-ng

Primeiro, executamos o airmon-ng start wlan0 para colocar a interface no modo monitor.

Se o comando for concluído com sucesso e o modo monitor estiver ativado no

recém criada interface mon0, isso significa que passou neste teste!

Em seguida, executamos o comando aireplay-ng -9 wlan0, onde a opção -9 significa que

é um teste de injeção (o formulário completo é --teste):

Aireplay-ng é uma ferramenta projetada para gerar e injetar quadros e vamos usá-lo para

realizar muitos dos ataques que abordaremos.

As ferramentas para varredura de redes sem fio incluídas no Kali Linux se enquadram na categoria

de scanners passivos. Nós cobrimos as duas mais populares dessas ferramentas neste capítulo,

airodump-ng e Kismet, mas também ferramentas como Fern Wi-Fi Cracker e Wifite podem

ser usado para este propósito.

Configurando o adaptador sem fio

modo monitor

No capítulo anterior, vimos como colocar a interface sem fio no monitor

modo, para verificar se é compatível com o sniffing de pacotes. Agora, analisamos o

detalhes deste procedimento.

Lembre-se que emitimos o comando airmon-ng start wlan0, como mostrado na

imagem seguinte:

A ferramenta airmon-ng também nos indica o chipset e o driver em uso pelo adaptador.

Observe que a interface mon0 é criada com o modo monitor ativado, enquanto o wlan0

interface está no modo gerenciado (que é o modo padrão para adaptadores sem fio)

A interface mon0 está escutando em todos os canais. Se quisermos ouvir em um específico

canal, podemos emitir o comando airmon-ng start wlan0 <channel>:

Vemos que outra interface chamada mon1 foi criada no modo monitor. Nós

pode criar várias interfaces de modo de monitor relacionadas a uma interface sem fio física.

Enquanto executamos o airmon-ng, notamos um aviso nos dizendo que alguns processos podem

Interferir com outras ferramentas da suíte Aircrack-ng. Para parar esses processos, podemos

execute o comando airmon-ng check kill.

Se quisermos parar a interface mon0, rodamos o comando airmon-ng stop mon0:

Agora que a interface está no modo monitor, podemos prosseguir com a varredura sem fio.

Digitalização sem fio com airodump-ng

A ferramenta airodump-ng é uma das muitas ferramentas incluídas no pacote Aircrack-ng.

É capaz de farejar e capturar quadros 802.11, além de gravar informações

em relação aos pontos de acesso e clientes descobertos. Airodump-ng verifica o Wi-Fi

faixa de freqüência, pulando de um canal para outro. Para usá-lo, depois de ter colocado o

interface sem fio no modo de monitor, como vimos anteriormente, corremos o airodump-ng

comando mon0. A captura de tela a seguir mostra sua saída:

A primeira linha mostra a última associação entre um AP e um cliente, com o atual

canal, o tempo de execução decorrido e o protocolo de segurança utilizado. Como podemos notar

na captura de tela anterior, a metade superior da tela exibe os APs enquanto o

metade inferior exibe os clientes.

Para cada AP encontrado, as seguintes informações são mostradas:

• O BSSID (endereço MAC)

• O nível de potência (PWR) e a qualidade de recepção (RXQ) do sinal

• O número de beacons enviados e o número de pacotes de dados capturados

• O canal (CH)

• A velocidade máxima suportada (MB)

• O algoritmo de criptografia (ENC), a cifra (CIPHER) e o

protocolo de autenticação (AUTH) usado

• O nome da rede sem fio ou SSID (ESSID)

Se <length: number> aparecer no campo ESSID, significa que o SSID está oculto

e o AP apenas revela seu comprimento (número de caracteres). Se o número for 0 ou 1,

significa que o AP não revela o tamanho real do SSID.

Na metade inferior, o campo STATION é sobre o endereço MAC dos clientes, que

pode ser associado a um AP. Se associado, o BSSID do AP é mostrado no

campo relativo; caso contrário, o estado não associado é exibido.

O campo Probes indica os SSIDs dos APs aos quais o cliente está tentando se conectar, se

não está associado no momento. Isso pode revelar um AP oculto quando responde a uma sonda

pedido ou a um pedido de associação de um cliente.

Existem outros métodos para obter um SSID oculto. Poderíamos forçar os clientes conectados

para reassociar com o AP enviando-os pacotes de autenticação, como veremos

no Capítulo 7, Ataques do Cliente Sem Fio. Poderíamos também analisar a associação capturada e

sondar pacotes de solicitação / resposta com o Wireshark para recuperar o SSID. Nós cobriremos

eliminação e análise de pacotes no Capítulo 4, Rachamento WEP e Capítulo 5, WPA / WPA2

Craqueamento, sobre cracking WEP e WPA / WPA2.

Podemos gravar a saída em um arquivo usando as opções -w ou --write seguidas pela

nome do arquivo. Airodump-ng pode salvar a saída em vários formatos (pcap, ivs, csv, gps,

kismet e netxml), compatível com as ferramentas de análise de pacotes e Kismet,

como Wireshark.

O Airodump-ng também permite selecionar canais específicos através do --canal ou

opção -c <ch\_nr1, ch\_nr2… ..n\_nrN>:

airodump-ng -c 1 -w saída mon0

Digitalização sem fio com Kismet

O Kismet é um poderoso scanner passivo disponível para diferentes plataformas e está instalado

por padrão no Kali. Não é simplesmente um scanner, mas também uma análise de quadros sem fio e

ferramenta de detecção de intrusão.

O Kismet é composto por dois processos principais: kismet\_server e kismet\_client.

O componente kismet\_server faz o trabalho de captura, registro e decodificação

quadros sem fio. Seu arquivo de configuração é kismet.conf e está localizado em / etc /

kismet / no Kali Linux. O frontend kismet\_client é uma interface baseada em ncurses

que exibe os APs detectados, estatísticas e detalhes da rede. Para executá-lo, digitamos

kismet na linha de comando ou navegue até o Kali Linux | Ataques sem fio | 802.11

Ferramentas sem fio | Kismet no menu do aplicativo:

A fonte do pacote é a nossa interface monomodo modo mon0 e a inserimos no Intf

campo no prompt subseqüente:

A fonte de pacotes também pode ser definida no arquivo kismet.conf, na diretiva ncsource,

como podemos ver na seguinte imagem:

**Esta é a maneira recomendada de configurar a fonte do pacote, evitando fazê-lo**

**manualmente toda vez que o Kismet é iniciado.**

**Fechamos o console do servidor e a interface do cliente é exibida. Para acessar o**

**menu na parte superior da janela, pressionamos a tecla ~ e movemos as entradas com**

**as teclas de seta. A interface e o comportamento do Kismet são personalizáveis navegando para**

**Kismet | Preferências:**

**A tela é dividida nas seguintes seções principais, de cima para baixo:**

**lista de redes, lista de clientes, gráfico de pacotes, status e painel lateral geral de informações**

**certo. Você pode escolher quais seções visualizar no menu Exibir:**

**Reconhecimento de WLAN**

Neste capítulo, vamos apresentar os conceitos básicos por trás das LANs sem fio

(Redes Locais) e ver como realizar o reconhecimento e informação

fase de coleta do nosso teste de penetração.

Este capítulo trata da varredura de redes sem fio e coleta de informações,

enumerando redes visíveis e ocultas, identificando os protocolos de segurança utilizados,

suas possíveis vulnerabilidades e os clientes conectados. Os tópicos abordados são

do seguinte modo:

• Introdução ao padrão 802.11 e LAN sem fio

• Introdução à digitalização sem fio

• Digitalização sem fio com airodump-ng

• Digitalização sem fio com Kismet

Introdução ao padrão 802.11 e

Rede sem fio

Antes de mergulhar na parte prática, vale a pena recordar os conceitos básicos da

Padrão 802.11 no qual as redes de área local sem fio são baseadas.

O 802.11 é o segundo padrão de camada (camada de enlace) para implementação de LAN sem fio

desenvolvido pelo IEEE. Dispositivos e redes que usam o padrão 802.11 são

comumente conhecido como Wi-Fi, uma marca comercial da Wi-Fi Alliance.

Houve especificações subseqüentes do padrão ao longo do tempo, o principal

são 802.11a, 802.11b, 802.11ge 802.11n.

[25] Reconhecimento de WLAN

802.11a opera na faixa de freqüência de 5 GHz enquanto 802.11b / g na freqüência de 2,4 GHz

faixa de freqüência, que é de longe a mais utilizada pelas redes Wi-Fi atualmente.

O 802.11n suporta ambas as bandas de frequência e é compatível com versões anteriores

as outras especificações do 802.11.

O alcance do sinal Wi-Fi depende do padrão utilizado, da potência do sinal

transmissor e na presença de obstáculos físicos e interferências de rádio.

Para dispositivos Wi-Fi comuns, normalmente varia de um máximo de 20 a 25 metros

dentro de casa a 100 metros e mais ao ar livre.

A taxa de transferência máxima, ou seja, a taxa de dados máxima, do padrão 802.11

varia de 11 Mbps dos padrões 802.11a / b para os 600 Mbps do 802.11n

padrão.

Cada banda de frequência é subdividida em múltiplos canais, que são subconjuntos que

incluir intervalos de frequência menores. A faixa de 2,4 GHz é subdividida em 14

canais, mas nem todos eles são sempre usados. A maioria dos países normalmente permite

apenas um subconjunto desses canais, enquanto alguns países permitem todos os canais.

Por exemplo, os Estados Unidos permitem canais de 1 a 11, enquanto o Japão permite todos os 14

canais. De fato, cada país estabeleceu seu próprio domínio regulatório (regdomain),

um conjunto de regras que define a alocação de espectro de rádio para transmissão sem fio. o

domínios regulatórios também definem a potência máxima de transmissão permitida.

A seção do cabeçalho MAC é dividida em vários campos, entre os quais o tipo

e Subtipo. O padrão 802.11 define três tipos diferentes de quadros:

•

Quadros de gerenciamento: esses quadros coordenam a comunicação entre

pontos de acesso e clientes em uma LAN sem fio. Quadros de gerenciamento incluem

os seguintes subtipos:

° quadros de beacon: Estes são usados ​​para anunciar a presença eo

configuração básica de um ponto de acesso (AP).

° ° Quadros de solicitação de sonda: Estes são enviados pelos clientes para testar a

presença de APs ou um AP específico para se conectar.

° ° Frames de resposta da sonda: Estes são enviados pelo AP em resposta a

solicitações de sondagem, contendo informações sobre a rede.

° ° Quadros de pedidos de autenticação: Estes são enviados pelos clientes para iniciar o

fase de autenticação antes de se conectar a um AP.

° ° Quadros de resposta de autenticação: Estes são enviados pelo AP para aceitar

ou rejeitar a autenticação do cliente.

° Quadros de solicitação de associação: são usados ​​pelo cliente para associar

com o AP. Deve conter o SSID.

° quadros de resposta da associação: estes são enviados pelo AP para aceitar ou

rejeitar a associação com o cliente.

• Quadros de controle: eles são usados ​​para controlar o fluxo de tráfego de dados no

rede. Os subtipos de quadros de controle são quadros Request-to-send (RTS)

e quadros Clear-to-send (CTS), que fornecem um mecanismo opcional para

reduzir as colisões de quadros e os quadros de Confirmação (ACK) enviados por

a estação receptora para confirmar o recebimento correto de um quadro de dados.

• Quadros de dados: contêm os dados transmitidos pela rede, com

pacotes de protocolos de camada superior encapsulados nos quadros 802.11.

Na próxima seção, vamos lembrar a estrutura e os blocos de construção de uma

rede sem fio.

Modo de infra-estrutura e acesso sem fio

pontos

As redes Wi-Fi usam o padrão 802.11 no modo de infra-estrutura. Neste modo, dispositivos

chamados pontos de acesso (APs) são usados para conectar as estações cliente sem fio a

LAN com fio ou com a Internet. Os pontos de acesso podem ser vistos como o análogo

switches para redes com fio, mas eles oferecem mais funcionalidades, tais como rede

roteamento de camadas, DHCP, NAT e recursos avançados de gerenciamento

console remoto ou no painel de administração da web.

Uma rede sem fio formada por um único AP é chamada de Basic Service Set (BSS)

uma rede com vários APs é conhecida como ESS (Extended Service Set). Cada AP

é identificado pelo BSSID (Basic Service Set ID), que normalmente corresponde a

o endereço MAC da interface sem fio no AP. Uma LAN sem fio é

identificado pelo ID do conjunto de serviços (SSID) ou ID do conjunto de serviços estendidos (ESSID),

que geralmente é uma string legível que é usada como o nome da rede.

Os pontos de acesso enviam periodicamente quadros de beacon de transmissão para anunciar

presença. Normalmente, os beacons também contêm o SSID do AP, de modo que é facilmente

identificáveis pelos clientes, que podem enviar solicitações de autenticação e associação para

o AP, para se conectar à rede sem fio.

Configurando modo monitor

airmon-ng start wlan0

airmon-ng start wlan0 <channel>

Vemos que outra interface chamada mon1 foi criada no modo monitor. Nós

pode criar várias interfaces de modo de monitor relacionadas a uma interface sem fio física.

Enquanto executamos o airmon-ng, notamos um aviso nos dizendo que alguns processos podem

Interferir com outras ferramentas da suíte Aircrack-ng. Para parar esses processos, podemos

execute o comando airmon-ng check kill.

Se quisermos parar a interface mon0, rodamos o comando airmon-ng stop mon0:

Wireless scanning with airodump-ng

The airodump-ng tool is one of the many tools included in the Aircrack-ng suite.

It is capable of sniffing and capturing 802.11 frames, besides recording information

relative to discovered access points and clients. Airodump-ng scans the Wi-Fi

frequency band, hopping from one channel to another. To use it, after having put the

wireless interface in monitor mode, as we saw previously, we run the airodump-ng

mon0 command. The following screenshot shows its output:

A primeira linha mostra a última associação entre um AP e um cliente, com o atual

canal, o tempo de execução decorrido e o protocolo de segurança utilizado. Como podemos notar

na captura de tela anterior, a metade superior da tela exibe os APs enquanto o

metade inferior exibe os clientes.

Para cada AP encontrado, as seguintes informações são mostradas:

• O BSSID (endereço MAC)

• O nível de potência (PWR) e a qualidade de recepção (RXQ) do sinal

• O número de beacons enviados e o número de pacotes de dados capturados

• O canal (CH)

• A velocidade máxima suportada (MB)

• O algoritmo de criptografia (ENC), a cifra (CIPHER) e o

protocolo de autenticação (AUTH) usado

• O nome da rede sem fio ou SSID (ESSID)

Se <length: number> aparecer no campo ESSID, significa que o SSID está oculto

e o AP apenas revela seu comprimento (número de caracteres). Se o número for 0 ou 1,

significa que o AP não revela o tamanho real do SSID.

Na metade inferior, o campo STATION é sobre o endereço MAC dos clientes, que

pode ser associado a um AP. Se associado, o BSSID do AP é mostrado no

campo relativo; caso contrário, o estado não associado é exibido.

O campo Probes indica os SSIDs dos APs aos quais o cliente está tentando se conectar, se

não está associado no momento. Isso pode revelar um AP oculto quando responde a uma sonda

pedido ou a um pedido de associação de um cliente.

Existem outros métodos para obter um SSID oculto. Poderíamos forçar os clientes conectados

para reassociar com o AP enviando-os pacotes de autenticação, como veremos

no Capítulo 7, Ataques do Cliente Sem Fio. Poderíamos também analisar a associação capturada e

sondar pacotes de solicitação / resposta com o Wireshark para recuperar o SSID. Nós cobriremos

eliminação e análise de pacotes no Capítulo 4, Rachamento WEP e Capítulo 5, WPA / WPA2

Craqueamento, sobre cracking WEP e WPA / WPA2.

Podemos gravar a saída em um arquivo usando as opções -w ou - -write seguidas pelo

nome do arquivo. Airodump-ng pode salvar a saída em vários formatos (pcap, ivs, csv, gps,

kismet e netxml), compatível com as ferramentas de análise de pacotes e Kismet,

como Wireshark.

Airodump-ng também permite selecionar canais específicos através do canal -channel

opção -c <ch\_nr1, ch\_nr2 ..... ch\_nrN>:

airodump-ng -c 1 -w saída mon0

Digitalização sem fio com Kismet

O Kismet é um poderoso scanner passivo disponível para diferentes plataformas e está instalado

por padrão no Kali. Não é simplesmente um scanner, mas também uma análise de quadros sem fio e

ferramenta de detecção de intrusão.

O Kismet é composto por dois processos principais: kismet\_server e kismet\_client.

O componente kismet\_server faz o trabalho de captura, registro e decodificação

quadros sem fio. Seu arquivo de configuração é kismet.conf e está localizado em / etc /

kismet / no Kali Linux. O frontend kismet\_client é uma interface baseada em ncurses

que exibe os APs detectados, estatísticas e detalhes da rede. Para executá-lo, digitamos

kismet na linha de comando ou navegue até o Kali Linux | Ataques sem fio | 802.11

Ferramentas sem fio | Kismet no menu do aplicativo:

Como podemos ver, o Kismet nos pede para iniciar o servidor e escolhemos Sim e depois

Comece no seguinte prompt. Em seguida, uma mensagem dizendo que não há fontes de pacotes

definido poderia aparecer e somos convidados a adicionar uma fonte de pacotes:

A fonte do pacote é a nossa interface monomodo modo mon0 e a inserimos no Intf

campo no prompt subseqüente:

A fonte de pacotes também pode ser definida no arquivo kismet.conf, na diretiva ncsource,

como podemos ver na seguinte imagem:

115/5000

Esta é a maneira recomendada de configurar a fonte do pacote, evitando fazê-lo

manualmente toda vez que o Kismet é iniciado.

263/5000

Fechamos o console do servidor e a interface do cliente é exibida. Para acessar o

menu na parte superior da janela, pressionamos a tecla ~ e movemos as entradas com

as teclas de seta. A interface e o comportamento do Kismet são personalizáveis navegando para

Kismet | Preferências:

A tela é dividida nas seguintes seções principais, de cima para baixo:

lista de redes, lista de clientes, gráfico de pacotes, status e painel lateral geral de informações

certo. Você pode escolher quais seções visualizar no menu Exibir:

[38] Capítulo 3

A lista de rede mostra as redes detectadas no modo de ajuste automático padrão.

Para selecionar uma rede e ver seus detalhes e os clientes conectados, precisamos mudar

o método de classificação para outro, por exemplo, usando Type ou Channel no Sort

cardápio. Então podemos selecionar uma rede na lista clicando nela com o mouse:

Navegue para o Windows | Detalhes da rede para obter informações mais detalhadas, como

BSSID, o canal, o fabricante, o nível do sinal, a taxa de pacotes e assim por diante:

[39] Reconhecimento de WLAN

Se selecionarmos as opções de clientes, podemos ver os clientes conectados à rede,

juntamente com informações úteis, como o endereço MAC, os pacotes trocados

e o fabricante do dispositivo do cliente.

No caso de redes com SSID encoberto, o Kismet mostra a string <HID SSID> em

lugar do nome da rede. Quando um cliente tenta se conectar à rede, o AP

envia o SSID em clear nos pacotes de resposta, permitindo que o Kismet o descubra,

já vi com Airodump-ng.

O Kismet gera os seguintes arquivos de log, por padrão, no diretório a partir do qual

foi iniciado (mas podemos mudar isso na diretiva logtemplate em kismet.conf):

• Um arquivo de captura de pacotes

• Redes em formato de texto (.nettxt)

• Redes no formato XML (.netxml)

• dados GPS no formato XML (.gpsxml)

Os arquivos de captura de pacotes podem ser examinados pelo Wireshark e podem conter

dados do espectro, níveis de sinal e ruído e dados GPS.

Enviar feedback

Histórico

Salvas