Trabalho Prático 3

CET 8493 | UFCD 9196 - Cibersegurança Ativa | Formador: Paulo Vaz

Formando: João Rodrigo Mota da Costa

1. Descreva os diferentes tipos de redes WiFi, incluindo redes ad-hoc, infraestruturadas e mesh.

Redes ad-hoc: Também conhecidas como redes ponto a ponto, as redes ad-hoc são formadas por dispositivos sem fio que se ligam diretamente uns aos outros, sem a necessidade de um *access point* central. Estas redes são úteis em situações em que não há infraestrutura de rede disponível ou para estabelecer uma rede temporária.

Redes Infraestruturadas: São as redes mais comuns, nas quais os dispositivos sem fio se ligam a um *access point* central, como um *router*. O *access point* atua como um intermediário entre os dispositivos sem fio e a Internet, permitindo que os dispositivos comuniquem com a rede e acedam à internet.

Redes Mesh: São redes sem fio que utilizam vários pontos de acesso interligados para fornecer cobertura de rede numa área maior. Essas redes são úteis em áreas onde uma única rede infraestruturada não consegue fornecer cobertura adequada, como em grandes espaços ou em áreas ao ar livre.

2. Explique as diferenças entre esses tipos de redes, destacando as suas vantagens e desvantagens.

Ad-hoc

Vantagens

- Fácil de configurar e não requer hardware adicional
- Pode ser usado em situações em que não há uma rede existente disponível

Desvantagens

- Geralmente não é muito seguro, pois não há criptografia padrão e qualquer dispositivo pode ligar à rede
- Não é adequado para redes grandes, pois a capacidade de rede é limitada
- Não suporta roaming, o que significa que os dispositivos precisam de ligar manualmente a cada *access point*

Infraestruturadas

Vantagens

- Muito mais seguro do que as redes ad-hoc, pois há uma infraestrutura de segurança disponível
- Suporta roaming, o que significa que os dispositivos podem mover livremente e permanecer ligados
- Capacidade de rede escalável, podendo suportar redes grandes e muitos dispositivos

Desvantagens

- Pode exigir hardware adicional, como um *router* para configurar a rede
- A rede é centralizada, o que pode ser uma única falha de segurança e pode levar a problemas de desempenho
- Não é adequado para áreas externas, pois a cobertura do *access point* é limitada

Mesh

Vantagens

- Altamente escalável, com capacidade de cobrir grandes áreas e suportar muitos dispositivos
- Muito mais resiliente do que as redes infraestruturadas, pois não há um único ponto de falha
- Suporta roaming, permitindo que os dispositivos se movam livremente na rede

Desvantagens

- Requer hardware adicional para implementar
- Pode ser mais complexo para configurar e gerir
- Pode ser mais caro de implementar

3. Resuma os principais pontos abordados, incluindo os diferentes tipos de redes WiFi e os protocolos WiFi seguros e não seguros.

As redes ad-hoc permitem que os dispositivos se liguem diretamente uns aos outros sem a necessidade de um *access point*, enquanto as redes infraestruturadas dependem de um *access point* para ligar os dispositivos. Já as redes mesh são uma rede ad-hoc avançada em que cada dispositivo funciona como um *access point* para fornecer cobertura de rede.

Existem protocolos de segurança WiFi seguros e não seguros, sendo os protocolos WEP e WPA inseguros, enquanto o WPA2 é considerado seguro.

4. Explique por que é importante proteger as redes WiFi e quais são as principais medidas de segurança que podem ser adotadas para garantir a segurança das redes WiFi.

É importante proteger as redes WiFi para evitar que pessoas não autorizadas se liguem à rede e obtenham informações sensíveis ou danifiquem os dispositivos ligados. Além disso, uma rede WiFi não segura pode ser utilizada para atividades ilegais, como o *download* e partilha de conteúdo protegido por direitos de autor ou para disseminação de malware.

Algumas medidas de segurança que podem ser adotadas para garantir a segurança das redes WiFi incluem:

- Usar protocolos de segurança WiFi seguros, como WPA2.
- Usar *passwords* (ou *passphrases*) fortes e únicas para a rede WiFi.
- Manter o firmware do *router* atualizado.
- Desativar o SSID broadcasting, para evitar que a rede seja detectada facilmente.
- Usar criptografia para garantir a privacidade das informações transmitidas pela rede.
- Habilitar a autenticação de dois fatores para aumentar a segurança do acesso à rede.
- Limitar o acesso à rede apenas para os dispositivos autorizados.

Adotar essas medidas de segurança pode ajudar a proteger a rede WiFi contra ataques e invasões não autorizadas, garantindo que os dados transmitidos pela rede permaneçam seguros e protegidos.

5. O que é um Rogue AP?

Rogue AP é um termo que se refere a um *access point* (AP) falso ou não autorizado que é criado e utilizado sem a permissão ou conhecimento do administrador da rede. Este tipo de AP pode ser utilizado por um invasor para interceptar o tráfego de rede, roubar informações ou até mesmo comprometer a rede inteira.

Um Rogue AP pode ser configurado por um invasor próximo à rede que se deseja atacar, para atrair os dispositivos que tentam se ligar a ele, em vez de se ligar ao AP legítimo. Os utilizadores podem ser induzidos a se ligar a um Rogue AP por meio de técnicas de phishing ou engenharia social.

6. Como é que funciona?

O funcionamento de um Rogue AP é relativamente simples. O invasor cria um *access point* (AP) falso, geralmente em um local próximo à rede que deseja atacar, e o configura com o mesmo nome de SSID (Service Set Identifier) e canal do AP legítimo da rede. Isso faz com que os dispositivos que tentam ligar à rede sejam atraídos para o Rogue AP em vez de ligar ao AP legítimo.

Uma vez que um dispositivo se liga ao Rogue AP, o invasor pode capturar e monitorizar todo o tráfego de rede que passa pelo dispositivo, incluindo *passwords* (ou *passphrases*), dados pessoais e informações confidenciais. Além disso, o invasor pode lançar outros tipos de ataques, como ataques *Man-in-the-Middle*(MitM), para interceptar e manipular o tráfego de rede.

Rogue APs também podem ser configurados com protocolos de segurança fracos ou inexistentes, permitindo que os invasores acedam facilmente a rede e obtenham controlo total.

7. Como podem ser detetados?

Análise de espectro: Esta técnica é usada para detectar as frequências de rádio utilizadas pelos Rogue APs. Pode ser realizada com o uso de equipamentos especializados, como analisadores de espectro, que permitem identificar os sinais de rádio de diferentes dispositivos.

Verificação manual: Esta técnica envolve a verificação manual de todos os pontos de acesso em uma rede para verificar se todos eles estão autorizados. Isso pode ser feito por meio de um software de gestão de rede ou manualmente, verificando os logs de acesso de dispositivos ligados à rede.

Análise de tráfego: Esta técnica envolve a análise do tráfego de rede para identificar comportamentos suspeitos ou tráfego anômalo que possa indicar a presença de um Rogue AP. Isso pode ser feito por meio de ferramentas de análise de tráfego de rede, como o Wireshark.

Monitorização automatizado: Esta técnica envolve a implementação de soluções de segurança automatizadas que verificam continuamente a presença de Rogue APs na rede e emitem alertas quando são detectados.

8. Como é que nos podemos proteger?

Política de segurança: É importante ter uma política clara de segurança para a rede, que estabeleça as regras e procedimentos para a implementação e gestão dos pontos de acesso na rede. Isso pode incluir a proibição de pontos de acesso não autorizados e a exigência de autenticação para todos os dispositivos ligados.

Monitorização contínuo: Implementar uma solução de Monitorização contínuo que verifique a presença de Rogue APs e alerte os administradores de rede quando são detectados.

Atualização do firmware: É importante manter o firmware dos pontos de acesso atualizado com as últimas correções de segurança para garantir que eles estejam protegidos contra vulnerabilidades conhecidas.

Autenticação: Exigir autenticação para todos os dispositivos ligados à rede, por meio de *passwords* (ou *passphrases*) ou outras formas de autenticação, como certificados digitais.

Criptografia: Usar criptografia para proteger a comunicação na rede WiFi, como o protocolo WPA2.

Controlo de acesso: Limitar o acesso à rede WiFi apenas a utilizadores autorizados e restringir o acesso a partes específicas da rede, conforme necessário.

Formação de utilizadores: Educar os utilizadores sobre as políticas de segurança da rede e a importância de não utilizar Rogue APs na rede corporativa.

9. WiFi Pineapple é a solução?

O WiFi Pineapple é um dispositivo que pode ser usado para executar ataques de Rogue APs em uma rede. Embora possa ser útil para testar a segurança da sua própria rede, é importante ressaltar que o seu uso em redes sem autorização é ilegal e pode ter graves consequências legais.

Além disso, o WiFi Pineapple não é uma solução de segurança, mas sim uma ferramenta usada para testar e explorar vulnerabilidades em redes WiFi. Portanto, seu uso deve ser feito com cuidado e responsabilidade. É importante adotar as medidas de segurança mencionadas anteriormente para proteger uma rede contra ataques de Rogue APs.