Atividade Orientada a Ensino

Acadêmico: Victor Hugo Lima Bauer

RGA: 2020.1907.025-9

Professor: Carlos Alberto da Silva

Atividade: Segurança da Informação Aplicada a redes Wireless

INTRODUÇÃO

As atividades orientadas a ensino realizadas focaram no tema de Segurança da Informação focada em redes wireless (sem fio), com estudos direcionados a teste de intrusão explorando vulnerabilidades do protocolo WPS. As ferramentas estudadas e equipamentos utilizados estão listados a seguir, exibindo os comandos executados, resultados obtidos e vulnerabilidades encontradas e exploradas.

METODOLOGIA

Instituições investigadas

Oito instituições de ensino foram escolhidas para a aplicação dos testes, cobrindo diferentes níveis educacionais, tanto em instituições públicas quanto privadas. Para garantir a segurança desses locais, devido às suas vulnerabilidades, seus domínios serão ocultados durante a amostragem dos testes.

WPS

O Protocolo de Configuração Protegida Wi-Fi (WPS) apresenta uma falha conhecida como vulnerabilidade do PIN numérico. Essa vulnerabilidade permite que invasores descubram o PIN de 8 dígitos do WPS por meio de ataques de força bruta, ganhando acesso não autorizado à rede Wi-Fi em um curto período de tempo. Mesmo com algumas correções, muitos dispositivos continuam vulneráveis, tornando a desativação do WPS uma medida recomendada para garantir a segurança da rede.

Equipamentos utilizados

Kali Linux:

Por ser um sistema projetado com foco em testes de penetração e possuir nativamente diversas ferramentas otimizadas para essa finalidade, o Kali Linux foi selecionado como sistema operacional durante os testes.

Placa Wireless:

Para realizar os testes com sucesso, é vital usar uma placa wireless que suporte modo monitor e injeção de pacotes. Sem esse suporte, não será viável escanear as redes próximas e efetuar os ataques. O modelo de placa utilizado foi um TP-LINK TL-WN722N.

Técnica de intrusão

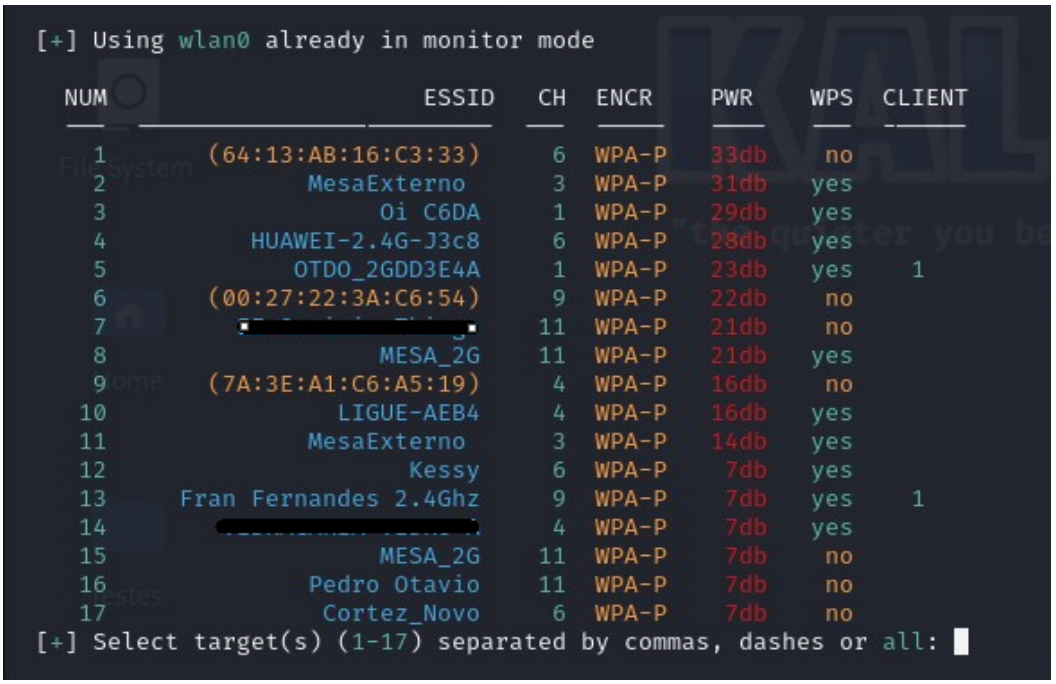
Como o foco do estudo foi em analisar as vulnerabilidades inerentes do uso do protocolo WPS, o tipo de ataque escolhido foi o Pixie-Dust, pois com ele é possível realizar o ataque de força bruta para descoberta do PIN de forma offline, evitando assim algumas contra medidas criadas por fabricantes de equipamentos roteadores. Pelo Wifite2 incorporar o Pixiewps em seu código, se torna fácil a utilização desse tipo de ataque para encontrar a chave PIN da rede.

Ferramentas

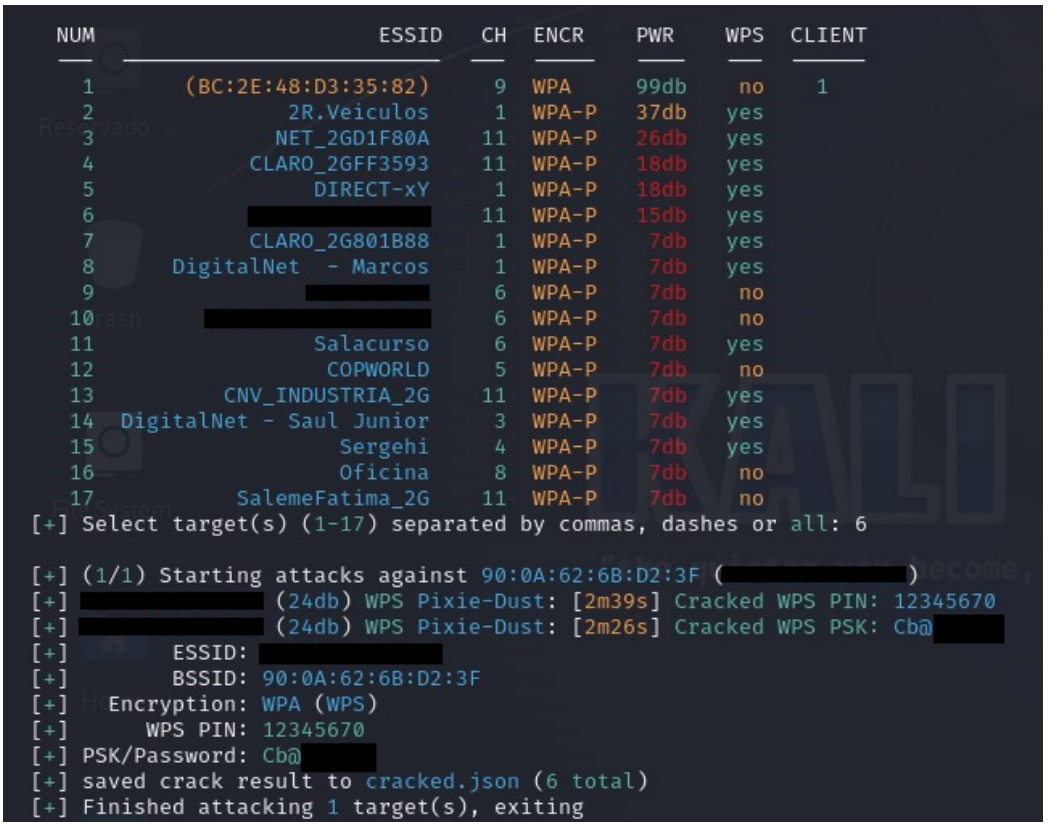
Wifite2

Foi utilizado Wifite2 para escanear as redes wireless das instituições, a fim de encontrar quais possuíam o protocolo WPS. Através do comando *$sudo wifite* foi iniciada a ferramenta e escolhida a placa da TP-LINK.

Após escolher a interface que representa nossa placa, a ferramenta começa a escanear as redes por perto, sendo possível identificar o ESSID, canal de comunicação, protocolo de segurança, potência do sinal, se está utilizando o protocolo WPS, e quantos clientes estão conectados no momento.



Dessa forma, é possível informar os IDs das redes para realização dos ataques.



Após a escolha da rede, a ferramenta executa o ataque Pixie-Dust, e ao obter sucesso, apresenta as informações de PIN e senha da rede obtidas. Dessa forma, quebrando a segurança da rede, e dos dados que por ela trafegam.

CONCLUSÃO

Na atividade orientada a ensino realizada, foi possível observar que por ser cada dia mais fácil ter acesso a equipamentos e ferramentas para realizar ataques a redes sem fio, concluímos que é necessário realizar o monitoramento de vulnerabilidades dos protocolos de segurança de maneira recorrente.

Conforme foi possível constatar nesta atividade, existem instituições que ainda possuem em suas redes vulnerabilidades referentes ao WPS. O que pode trazer diversos malefícios para a corporação, pois uma vez que um atacante não autorizado esteja dentro da rede da instituição, este pode iniciar diversos outros ataques, interceptando pacotes da rede, realizando exposição dos dados dos usuários, atacando outras instituições através da rede

invadida, e dependendo da configuração da a rede, realizar escaneamento de dispositivos conectados à rede através de softwares específicos.

Portanto, o estudo em segurança da informação focado em redes wireless foi fundamental para o entendimento que é recomendado que corporações optem por desabilitar recursos de WPS quando possível para trazer um nível maior de segurança à rede, evitando assim as vulnerabilidades que esse protocolo possa proporcionar.

Campo Grande, 30 de novembro de 2023.

gov.br
Documento assinado digitalmente
VICTOR HUGO LIMA BAUER
Data: 01/12/2023 09:04:16-0300
Verifique em https://validar.iti.gov.br

Victor Hugo Lima Bauer