Bezpečnost a Hacking WiFi (802.11) - 2. Nejslabší ochranné prvky

Vložil/a matej [1], 23 Červenec, 2009 - 19:05

- Hacking [2]
- Hacking method [3]
- Networks & Protocols [4]
- Security [5]
- WiFi & Wireless [6]

V předchozím díle se mluvilo o úplných základech. V tomto díle si ukážeme ty nejslabší "bezpečnostní prvky" a jak jednoduše je lze obejít.

3. Najslabšie ochranné prvky

Sieť WLAN je možné chrániť viacerými spôsobmi. Niektoré z nich sú dodnes v povedomí verejnosti považované za bezpečnostné (niekedy dokonca bezpečné), v skutočnosti sú však len „kozmetické“ a použiteľné len na ochranu pred nenakonfigurovanými zariadeniami.

3.1 Skrývanie SSID

Často používaným „zabezpečením“ je ukrytie identifikátoru siete SSID (Service Set Identifier, identifikátor sady služieb) – umožňuje to množstvo AP aj Host-AP. Identifikátor sa v „Beacon“ rámcoch nevysiela, resp. vysiela sa ako prázdny reťazec. Bez poznania tohoto identifikátoru nie je možné sa na sieť asociovať – samotné SSID slúži teda ako akási forma hesla.
Skrývanie SSID je možné použiť v kombinácii s ďalšími spôsobmi zabezpečenia.

3.1.1 Zistenie SSID

Rámec Association request obsahuje SSID siete, do ktorej sa stanica chce asociovať. Tento je prenášaný bez akéhokoľvek zabezpečenia. Probe request a response rámce, ktoré sa vysielajú počas vyhľadávania siete stanicou, taktiež obsahujú SSID.
Možné sú teda dva útoky:

A) pasívny – Monitorujeme prevádzku a čakáme, kým sa niektorá zo staníc bude asociovať, resp. vyhľadávať AP. V asociačnom aj probe rámci priamo vidno SSID.
B) aktívny – Management rámce nie sú nijakým spôsobom zabezpečené. Pošleme sfalšovaný disasociačný alebo deautentifikačný rámec niektorej stanici a monitorujeme prevádzku. Stanica sa vzápätí opäť asociuje, čím prezradí SSID.

Monitorovanie pre zistenie názvu SSID môžeme robiť pomocou programov wireshark, airodump-ng (z balíka Aircrack-ng [7]), airsnort, apod. Deautentifikačný rámec môžeme zostrojiť ručne a následne poslať cez framespam, alebo pomocou aireplay-ng (z balíka Aircrack-ng):

```
# ./aireplay-ng -0 1 -a 00:11:3b:07:00:14 -c 00:11:3b:0b:22:0c rausb0
23:07:23 Sending DeAuth to station -- STMAC: [00:11:3B:0B:22:0C]
```

-0 1 určuje typ útoku (deautentifikácia) a počet vyslaných rámcov (1),
-a ... určuje BSSID (Basic Service Set Identifier, identifikátor základnej sady služieb) (MAC adresa AP),
-c ... určuje MAC adresu deautentifikovanej stanice,
rausb0 je zariadenie použité na vyslanie rámca (musí byť v monitor mode).

V zápätí airodump-ng aj airsnort zobrazia zistené SSID, v prípade wireshark je treba prezrieť výpis alebo ho vyfiltrovať. Ak SSID nezachytíme, znamená to najskôr, že niektorý z rámcov sa stratil – buď náš deautentifikačný pri prenose (a treba poslať ďalší), alebo Probe/Association rámce (a treba pokus zopakovať).

V prípade, že deautentifikačných rámcov posielame väčšie množstvo, bude sa jednať o DoS útok (Denial of Service, zamietnutie služby) (viď. 6.4).

3.1.2 Ochrana voči zisťovaniu SSID

Žiadna. SSID nikdy nebolo určené ako bezpečnostný prvok, taktiež nikdy nemalo byť skrývané. Skrývanie SSID je teda vhodné len na zamedzenie asociovania sa nenakonfigurovaných staníc, príp. takých, ktoré sú nastavené na automatické pripájanie sa do ľubovoľnej dostupnej siete.

3.2 Filtrovanie podľa MAC adresy

Ďalším z možných spôsobov zabezpečenia je obmedzenie množiny MAC adries staníc (sieťových kariet), s ktorými bude AP komunikovať. Prístupový bod (AP) má nakonfigurovaný zoznam MAC adries zariadení, ktoré bude asociovať. Zariadenia s inými MAC adresami ignoruje, resp. odpovie záporne. Na svete by nemali existovať dve IEEE 802.11 sieťové rozhrania s rovnakými MAC adresami, a preto sa môže tento druh filtrovania pozdávať ako kvalitný druh zabezpečenia.

3.2.1 Zneužitie cudzej MAC adresy

MAC adresa je síce unikátna, na zariadení obvykle napálená vo flash pamäti, väčšinou je však softvérovo zmeniteľná – často dokonca pomocou pôvodného ovládača od výrobcu.
Pasívnym monitorovaním je možné jednoducho zistiť platné MAC adresy, ktoré v danej BSS (Basic Service Set, základná sada služieb) komunikujú.
Tie potom môžeme použiť pre vlastné účely:

· **posielanie falošných surových (raw) rámcov**
· **zneužitie MAC adresy pre „legitímne“ využívanie služby** – po odchode daného zariadenia zo siete, resp. po jeho vypnutí softvérovo zmeníme MAC adresu svojho zariadenia a naplno využívame služby poskytované danou sieťou;
· **ukradnutie MAC adresy** – vybranú stanicu odstavíme pomocou úzko nasmerovaného nízkoúrovňového DoS (viď. 6.1 Rušenie pásma, 6.3 RTS/CTS) a použijeme jej adresu, DoS útok však musíme úzko nasmerovať, aby sme odstavili iba vybranú stanicu a nie aj AP;
· **súčasné používanie MAC adresy v tom istom čase** – v prípade používania spojovo orientovaných protokolov (TCP (Transmission Control Protocol, protokol pre riadenie vysielania)) časté prerušenia; ak sa však obmedzíme len na bezspojovú komunikáciu (UDP (User Datagram Protokol, protokol pre používateľské datagramy), ICMP (Internet Control Message Protocol, protokol pre riadiace správy na internete), je možný bezproblémový chod.

Falošné rámce môžeme posielať v režime monitor napríklad pomocou aireplay-ng z balíka Aircrack-ng, ručne zostrojené rámce pomocou framespam, pomocou file2air alebo rôznymi inými utilitami.
Zmena MAC adresy vlastného zariadenia nie je náročná operácia, líši sa podľa typu OS, resp. ovládača. Niektoré WLAN ovládače podporujú zmenu MAC adresy iba v režime monitor. Je to možné urobiť ako root jedným z nasledujúcich spôsobov:

```
# ifconfig rausb0 hw ether 00:11:22:33:44:55 # pre Linux
# macchanger rausb0 –m 00:11:22:33:44:55 # pomocou utility macchanger
# wicontrol -i rausb0 –m 00:11:22:33:44:55 # pre FreeBSD
# ifconfig ed0 ether 00:11:22:33:44:55 # -II-
# ifconfig iwn0 lladdr 00:11:22:33:44:55 # OpenBSD
# ifconfig en0 lladdr 00:11:22:33:44:55 # Mac OS X - Leopard
```

V OS Windows je možné zmeniť MAC adresu ako administrátor v konfigurácii zariadenia pre konkrétne sieťové pripojenie, záložka Advanced (rozšírené), položka Network Address. Ak táto položka nie je prístupná, môžeme ju úpravou registrov „dorobiť“ – vytvorením kľúča `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\0001\Ndi\params\NetworkAddress`

a potrebných hodnôt pod týmto kľúčom. 0001 treba nahradiť číslom adaptéra, ktorému položku chceme pridať. Ukážka takejto úpravy registrov je na priloženom médiu v súbore NetworkAddress.reg.

3.2.2 Ochrana voči zneužitiu MAC adresy

Na sieti, kde je ľubovoľná prevádzka, prakticky nie je možné zabrániť odchyteniu platnej MAC adresy. Napriek tomu je tento spôsob ochrany často využívaný, pretože chráni pred neúmyselným zneužitím, resp. zneužitím laikom.
Ak chceme sťažiť, resp. zabrániť úmyselnému zneužitiu platnej MAC adresy s cieľom využívať služby poskytované sieťou, je potrebné na sieti použiť šifrovanie – viď. 4. WEP, 5. WPA a WPA2.

URL článku:
https://security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-2-nejslab%C5%A1%C3%AD-ochrann%C3%A9-prvky

Odkazy:
[1] https://security-portal.cz/users/matej
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/hacking-method
[4] https://security-portal.cz/category/tagy/networks-protocols
[5] https://security-portal.cz/category/tagy/security
[6] https://security-portal.cz/category/tagy/wifi-wireless
[7] http://www.aircrack-ng.org
[8] http://matej.sustr.sk/publ/dipl/
[9] http://creativecommons.org/licenses/by-nc/3.0/