Fake AP s OpenBSD

Vložil/a Merlyn [1], 4 Červen, 2010 - 08:58

- Hacking [2]
- Security [3]
- WiFi & Wireless [4]

S pomocí falešného wifi access pointu je možné provést Man in the Middle útok, při kterém útočník nastaví svůj vlastní access point tak, aby vypadal jako access point, na kterém je přihlášen, nebo na který se chystá přihlásit oběť. Počítač oběti se automaticky připojí k AP s větším signálem. Je tedy důležité, aby útočník byl buď blízko oběti nebo měl výkonnou anténu, která přebije anténu správného AP.

Ve chvíli, kdy je oběť připojena, vyžádá si od DHCP serveru IP adresu a s ní všechny potřebné informace o síti, mimo jiné i adresu DNS serveru. Když je oběť připojena na fake AP, putuje komunikace přes váš počítač a záleží jenom na vás, co s ní uděláte.

Sice existují sofistikovanější možnosti fake AP, třeba pomocí **fakeAP[6]** nebo **aircrack-ng[7]** (jeho airbase-ng), nicméně prvně jmenovaný program se mi nepodařilo najít jako OpenBSD verzi (ačkoliv prý existuje) a druhý mi prozměnu ani s jednou wifi kartou nefungoval (s Linuxem by ale měly oba programy fungovat bez problému). Kromě toho, způsob popsaný v tomto článku můžete použít s čistým OpenBSD, aniž byste cokoliv instalovali (s vyjímkou deauth, který ale není úplně nutný).

Princip Man in the Middle útoku je většině asi všeobecně známý. Pokud někdo neví, oč se jedná, doporučuji podívat se na wikipedii[1].

Co potřebujete?

* **dvě wifi karty** - jedna bude připojena k síti, a ta druhá bude slouzit jako fake AP
* **OpenBSD[2]** - hlavně nástroje ifconfig a pf[3]
* **DNS server** - třeba BIND, pro hraní si s DNS
* volitelne **deauth[4]**

Konfigurace:

Konfigurace sestává ze tří základních kroků a X dodatečných kroků (podle toho, co budete provádět). Tím prvním je nastavení wifi karty, která bude použita k připojení na správný AP.
Mějme například situaci, kdy wifi síť má:

```
SSID: Wifi
WEP Klic: 0xAB8921FD3A
MAC adresu: 00:21:AB:CD:78:A1
Kanal: 1
Subnet: 192.168.1.X.
```

Počítač má dvě wifi karty - iwn0 pro připojení na Wifi síť a rum0 pro vytvoření AP.

Kdybyste se rozhodli neměnit MAC adresu na svém fake AP (není to bezpodmínečně nutné), pak pomocí bssid parametru ifconfig můžete určit konkrétní AP, na které se připojíte, jinak doporučuji se nejprve připojit ke spravnemu AP, a pak až vytvořit fake.

Prvně zjistíme informace o AP pomocí ifconfig iwn0 scan. Zjistit WEP heslo se dá velice jednoduše. Zde na SP lze, tusim, najít článek. Takže jen zmíním, že tohle není omezené na sítě bez šifrování nebo sítě, ke kterým máte klíč. Většina lidí nebude očekávát nějaké nekalé jednání, když "to přece mají zaheslované".

```
nwid Wifi nwkey 0xAB8921FD3A chan 1 bssid 00:21:ab:cd:78:a1 184dB 54M
privacy,short_slottime
```

Připojíme iwn0 na Wifi.

```
ifconfig iwn0 nwid Wifi nwkey 0xAB8921FD3A bssid 00:21:ab:cd:78:a1 up
dhclient iwn0
```

Druhým krokem je nastavení druhé wifi karty (rum0) na parametry AP. Jednotlivě se jedná o - nastavení MAC adresy a nastavení nwid, nwkey, inet, netmask a chan přes ifconfig.

```
ifconfig rum0 lladdr 00:21:ab:cd:78:a1
```

Zde si dejte pozor, abyste nastavili použitelnou IP adresu (jinou podsíť, než na jaké je správný AP)

```
ifconfig rum0 inet 192.168.2.254 netmask 255.255.255.0 media autoselect mediaopt
hostap mode 11g nwid Wifi chan 1 up
```

Mode nastavte 11b nebo 11g. V závislosti na tom, co je nastaveno na správném AP, více vizte[5]

Třetím nutným bodem je rozběhání NATu. Tento bod není nutný, ale pokud NAT nenastavíte, oběť se bude moci dostat max k vám, takže si brzy začne stěžovat, že "nejede internet".

Do souboru /etc/pf.conf přidejte následující, případně podobné, řádky (zde doporučuji nastudovat si **pf.conf[5]**):

```
# Vn?jší za?ízení - p?ipojené k Wifi
ext_if=iwn0

# Vnit?ní za?ízení - náš fake AP
int_if=rum0

# Vynecháme za?ízení lo
set skip on lo

# Vytvo?ení NATu
nat on $ext_if inet from $int_if:network -> ($ext_if:0)

# Defaultní chování (nic dovnit?, cokoliv ven)
block in
pass out keep state

# Povolíme cokoliv na vnit?ním za?ízení
pass quick on $int_if

# Také je pot?eba net.inet.ip.forwarding nastavit na 1
sysctl net.inet.ip.forwarding=1
```

Nakonec nastavíme a spustíme DHCP server **dhcpd** pro přidělování IP adres.

V tuto chvíli můžeme počkat než se oběť přihlásí. Jistější ale bude situace, kdy použijeme **deauth**.

Tento prográmek slouží k deauthentifikaci všech připojených stanic, případně jedné stanice dle výběru. Použití je velice jednoduché:

```
./deauth iwn0 [bssid]
```

Co můžete provádět?

* sniffing

První věc, kterou můžete provádět, je sniffing. Klasika tcpdump [5] nebo wireshark [6]. Tohle je nejméně nápadná věc, ale s nejmenším ziskem/prospěchem (btw. všiml jsem si, že ICQ už (konečně) posílá hesla jako md5 hash).

* změna DNS

Nastavení a konfigurace DNS serveru by, myslím, byla nad rámec tohoto článku, takže vás jen odkážu na **[8]**.

* redirect pomocí pf (firewallu)

Redirect se do jisté míry podobá změně DNS.

* jakýkoliv přímý útok

Na AP může být firewall, který například blokuje/filtruje komunikaci mezi dvěma klienty. Tímto se takovému firewallu vyhnete.

* DoS

Další možnosti vy/zne-užití je DoS - prostým přidáním rdr pravidla můžeme všechny požadavky na port 80 a 443 přesměrovat na localhost.

Možná vás v tuto chvíli napadlo, proč to dělat takhle, když pomocí deauth můžete také provést DoS. Je to pravda, ale v případě použití deauth si uživatel všimne, že se mu "nejde připojit", ale takhle můžete na localhostu "spíchnout" stránku, např.: "Společnost Kavárna se omlouvá svým zákazníkům za nedostupnost internetu" nebo něco na tento způsob.

Možné nápadnosti:

* Pokud nemáte dostatečně silnou anténu (ale i když ji máte), hodně nápadným článkem jste vy sami. Když si například jdete sednout do internetové kavárny, abyste si pohráli, nezapomeňte si vzít sako mezi cool studenty a hadr alá homeless do vyšší společnosti :-P

* Uživatel od vašeho fake AP dostane jinou IP adresu z jiné podsítě. Toho si běžný uživatel nevšimne, ale stačí jeden zkušenější a paranoidnější a už se může ptát obsluhy na detaily (které stejně obsluha nebude vědět).
Tato nápadnost se dá obejít tím, že fake AP vytvoříte jako bridge. Pokud ale budete chtít podsunout nakažený DNS server, budete muset spustit dhcp server. Ovšem můžete mu nastavit přidělování stejných (ze stejného rozsahu podsítě) adres jako legitimní síť, díky absenci NATu při tomto řešení.

[1] http://en.wikipedia.org/wiki/Man-in-the-middle_attack [7]
[2] http://www.openbsd.org [8]
[3] http://www.openbsd.org/faq/pf/ [9]

[4] http://team.vantronix.net/~reyk/deauth.c [10]
[5] http://en.wikipedia.org/wiki/IEEE_802.11 [11]
[6] http://www.blackalchemy.to/project/fakeap/ [12]
[7] http://aircrack-ng.org [13]
[8] http://www.kernel-panic.it/openbsd/dns/ [14]

URL článku: https://security-portal.cz/clanky/fake-ap-s-openbsd

Odkazy:
[1] https://security-portal.cz/users/merlyn
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/security
[4] https://security-portal.cz/category/tagy/wifi-wireless
[5] http://www.tcpdump.org/
[6] http://www.wireshark.org/
[7] http://en.wikipedia.org/wiki/Man-in-the-middle_attack
[8] http://www.openbsd.org
[9] http://www.openbsd.org/faq/pf/
[10] http://team.vantronix.net/~reyk/deauth.c
[11] http://en.wikipedia.org/wiki/IEEE_802.11
[12] http://www.blackalchemy.to/project/fakeap/
[13] http://aircrack-ng.org
[14] http://www.kernel-panic.it/openbsd/dns/