VoIP (in)Security

strumenti OpenSource per il security assessment

Alessio L.R. Pennasilico
mayhem@recursiva.org
http://www.recursiva.org/

hackit_07
ten years nerdcore

$ whois mayhem

Security Evangelist @ 

Member / Board of Directors:

AIP, AIPSI, CLUSIT, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer, Sikurezza.org, Spippolatori, VoIPSA.

Core Team at:

CrISTAL, Hacker's Profiling Project, Recursiva.org

Come mi sento oggi

hackit_07

ten years nerdcore

mayhem

sono preoccupato

VoIP explosion

"IDC Anticipates 34 Million More Residential VoIP Subscribers in 2010"

Telecom

cronaca

CALEA

leggi

Spyware

interessi economici

tutti vogliono sapere

qualcosa di me

it’s none of your business

History

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

Benjamin Franklin, 1759

Telefoni

hackit_07

ten years nerdcore

Telefoni

intercettazioni

Telefoni

È possibile mettersi in ascolto da un altro apparecchio della stessa linea, da un altro interno.

Telefoni

È possibile collegare al cavo telefonico un qualche dispositivo di intercettazione con un paio di pinzette a coccodrillo.

Telefoni

È possibile mettersi in ascolto alla centralina telefonica.

Telefoni

È possibile intercettare le linee telefoniche primarie, mettersi in ascolto sui collegamenti telefonici via microonde o via satellite, ecc.

VoIP

hackit_07

ten years nerdcore

VoIP

economico

VoIP

semplice

VoIP

flessibile

VoIP

interoperabile

VoIP

efficace

VoIP

integrabile

VoIP

sicuro?

non di default

rispetto alla telefonia tradizionale

VoIP

può esserlo di più!

VoIP

non è il telefono che conosciamo

Rischi

hackit_07

ten years nerdcore

Telefonia tradizionale

“I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. The phone company is nothing but a computer.”

Captain Crunch, “Secrets of the Little Blue Box“, 1971

(slide from Hacker's Profile Project, http://hpp.recursiva.org)

Concorsi via radio...

"Each week, the station ran the "Win a Porsche by Friday" contest. In this contest, a $50,000 Porsche is awarded to the 102nd caller who calls after a particular sequence of songs announced earlier in the day is played.

... e phreaking

On the morning of June 1, 1990, businessmen, students, housewives, desperados, mere contest fanatics etc. jammed all the telephone lines with their auto-dialers and car phones. But Poulsen played the game differently. With the help of his almost equally talented accomplices stationed at their own computers, he seized full control of the station's 25 telephone lines, effectively blocking out all calls excluding their own. With careless ease, he made the 102nd call and collected his Porsche.“

Kevin Poulsen

His exploits did not end there. It is known that he wiretapped a number of intimate phone calls of a Hollywood actress, possibly with the intention of blackmailing her. He even conspired to steal classified military orders, and went so far as to crack an Army computer and snoop into an FBI investigation of former Philippine president Ferdinand Marcos.

http://library.thinkquest.org/04oct/00460/poulsen.html

I primi attacchi

"A brute-force password attack was launched against a SIP-based PBX in what appeared to be an attempt to guess passwords. Queries were coming in about 10 per second. Extension/ identities were incrementing during each attempt, and it appeared that a full range of extensions were cycled over and over with the new password. The User-Agent: string was almost certainly falsified."

John Todd on VoIPSA mailinglist, May 24th 2006

Frodi

"Edwin Andreas Pena, a 23 year old Miami resident, was arrested by the Federal government: he was involved in a scheme to sell discounted Internet phone service by breaking into other Internet phone providers and routing connections through their networks."

The New York Times, June 7th 2006

Intercettazioni

"Unknowns tapped the mobile phones of about 100 Greek politicians and offices, including the U.S. embassy in Athens and the Greek prime minister."

Bruce Schneier, his blog, 22th June 2006
Greek wiretapping scandal

e-mail

sappiamo gestire le e-mail?

VoIP

non è il telefono che conosciamo

SPIT

SPAM over Internet Telephony

Vishing

VoIP phishing

end point security

trojan, spyware, backdoor

intercettazione ambientale

microfono del computer

grande fratello

webcam

Rischi

rischi reali

Trunk ISP

Un trunk non protetto tra il nostro network ed un VoIP Provider mette molti tecnici del nostro ISP nelle condizioni di intercettare le credenziali di quel collegamento e di ascoltare tutte le conversazioni.

Road Warrior

Spesso per permettere agli utenti mobili di utilizzare i servizi VoIP da remoto, il centralino VoIP viene pubblicato su Internet, esponendolo a numerosi attacchi (enumeration, brute forcing, exploiting, etc).

Esempio di chiamata

hackit_07
ten years nerdcore

Accendo il telefono

I telefoni IP per funzionare eseguono diverse azioni preliminari vulnerabili a diversi attacchi:

- ✓ ottengono l'indirizzo IP da un server DHCP
- ✓ ottengono l'indirizzo di un TFTP server
- ✓ scaricano il firmware dal TFTP server
- ✓ scaricano la configurazione dal TFTP server
- ✓ si autenticano sul server VoIP

Chiamiamoci!

Completato lo startup il telefono conversa con il server in merito al proprio stato ed allo stato delle chiamate (signaling).

Quando si verifica una chiamata tra due telefoni, conclusa la fase iniziale di signaling, si instaura un flusso RTP tra gli end-point o tra ogni SIP-UA ed il proprio server VoIP.

Strumenti

hackit_07

ten years nerdcore

Strumenti

Sono decine gli strumenti disponibili, scaricabili gratuitamente da Internet, completi di codice sorgente, in grado di effettuare **attacchi specifici** ai protocolli che trasportano la voce.

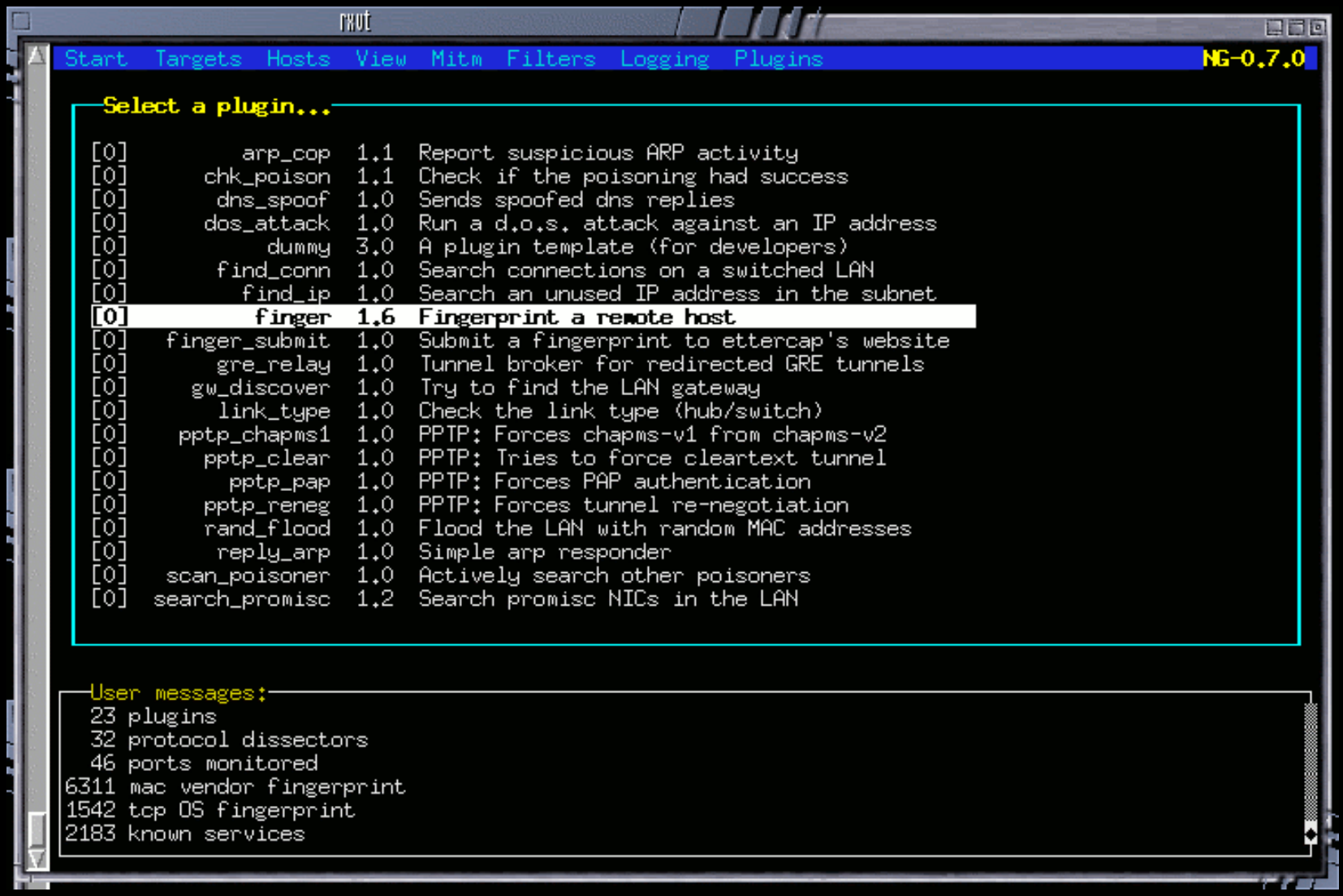
Ettercap

http://ettercap.sourceforge.net/

La suite per gli attacchi Man in the Middle. Multipiattaforma, da usare in console o in un windows manager, Ettercap permette di lanciare tutti quegli attacchi a Layer 2 che permettono di capire quanto la nostra rete switchata sia vulnerabile se non adeguatamente protetta.

Keywords: arp spoofing, arp poisoning, hijacking, sniffing, decoding, dns spoofing, dos, flood.

Ettercap (2)


root
Start Targets Hosts View Mitm Filters Logging Plugins NG-0.7.0
Select a plugin...
[0] arp_cop 1.1 Report suspicious ARP activity
[0] chk_poison 1.1 Check if the poisoning had success
[0] dns_spoof 1.0 Sends spoofed dns replies
[0] dos_attack 1.0 Run a d.o.s. attack against an IP address
[0] dummy 3.0 A plugin template (for developers)
[0] find_conn 1.0 Search connections on a switched LAN
[0] find_ip 1.0 Search an unused IP address in the subnet
[0] finger 1.6 Fingerprint a remote host
[0] finger_submit 1.0 Submit a fingerprint to ettercap's website
[0] gre_relay 1.0 Tunnel broker for redirected GRE tunnels
[0] gw_discover 1.0 Try to find the LAN gateway
[0] link_type 1.0 Check the link type (hub/switch)
[0] pptp_chapms1 1.0 PPTP: Forces chapms-v1 from chapms-v2
[0] pptp_clear 1.0 PPTP: Tries to force cleartext tunnel
[0] pptp_pap 1.0 PPTP: Forces PAP authentication
[0] pptp_reneg 1.0 PPTP: Forces tunnel re-negotiation
[0] rand_flood 1.0 Flood the LAN with random MAC addresses
[0] reply_arp 1.0 Simple arp responder
[0] scan_poisoner 1.0 Actively search other poisoners
[0] search_promisc 1.2 Search promisc NICs in the LAN
User messages:
23 plugins
32 protocol dissectors
46 ports monitored
6311 mac vendor fingerprint
1542 tcp OS fingerprint
2183 known services

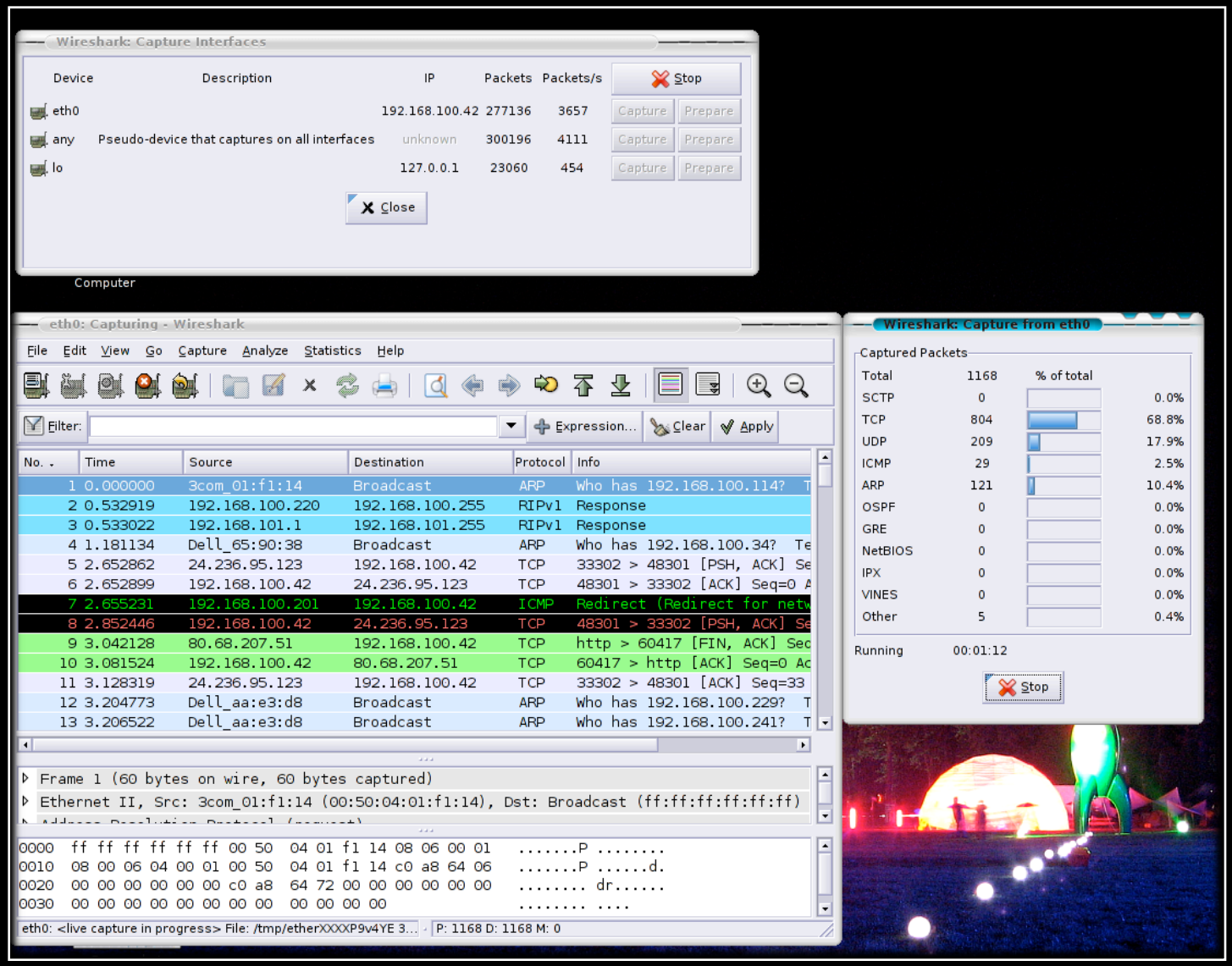
Wireshark

http://www.wireshark.org/

Sniffer multipiattaforma, corredato di molti decoder, che lo mettono in grado di interpretare il traffico intercettato.

Wireshark può interpretare tanto i flussi di signaling, quanto quelli RTP, ed estrarne tutte le informazioni necessarie per una successiva analisi.

Wireshark (2)


Wireshark: Capture Interfaces
Device
Description
IP
Packets
Packets/s
Stop
eth0
192.168.100.42
277136
3657
Capture
Prepare
any
Pseudo-device that captures on all interfaces
unknown
300196
4111
lo
127.0.0.1
23060
454
Close
Computer
eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 3com_01:f1:14 Broadcast ARP Who has 192.168.100.114?
2 0.532919 192.168.100.220 192.168.100.255 RIPv1 Response
3 0.533022 192.168.101.1 192.168.101.255 RIPv1 Response
4 1.181134 Dell_65:90:38 Broadcast ARP Who has 192.168.100.34?
5 2.652862 24.236.95.123 192.168.100.42 TCP 33302 > 48301 [PSH, ACK]
6 2.652899 192.168.100.42 24.236.95.123 TCP 48301 > 33302 [ACK] Seq=0
7 2.655231 192.168.100.201 192.168.100.42 ICMP Redirect (Redirect for
8 2.852446 192.168.100.42 24.236.95.123 TCP 48301 > 33302 [PSH, ACK]
9 3.042128 80.68.207.51 192.168.100.42 TCP http > 60417 [FIN, ACK]
10 3.081524 192.168.100.42 80.68.207.51 TCP 60417 > http [ACK] Seq=0
11 3.128319 24.236.95.123 192.168.100.42 TCP 33302 > 48301 [ACK] Seq=33
12 3.204773 Dell_aa:e3:d8 Broadcast ARP Who has 192.168.100.229?
13 3.206522 Dell_aa:e3:d8 Broadcast ARP Who has 192.168.100.241?
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 3com_01:f1:14 (00:50:04:01:f1:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
0000 ff ff ff ff ff ff 00 50 04 01 f1 14 08 06 00 01 .....P ....
0010 08 00 06 04 00 01 00 50 04 01 f1 14 c0 a8 64 06 .....P ......d.
0020 00 00 00 00 00 00 c0 a8 64 72 00 00 00 00 00 00 .... dr......
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
eth0: <live capture in progress> File: /tmp/etherXXXXP9v4YE 3...
P: 1168 D: 1168 M: 0
Wireshark: Capture from eth0
Captured Packets
Total 1168 % of total
SCTP 0 0.0%
TCP 804 68.8%
UDP 209 17.9%
ICMP 29 2.5%
ARP 121 10.4%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 5 0.4%
Running 00:01:12
Stop

Vomit

http://vomit.xtdnet.nl/

Voice Over Misconfigured Internet Telephones, a partire dal file di dump creato da uno sniffer, in formato tcpdump, vomit crea un file audio contenente la conversazione VoIP transitata sulla rete monitorata. Supporta il protocollo MGCP con codec G.711 e funziona solo con Linux.

```
./vomit -r elisa.dump | waveplay -S 8000 -B 16 -C 1
```

Oreka

http://oreka.sourceforge.net/

Distribuito per Windows e Linux, supporta i protocolli di Cisco CallMananager, Lucent APX8000, Avaya, S8500, Siemens HiPath, VocalData, Sylantro, Asterisk SIP channel.

Intercetta e registra le conversazioni basate su flussi RTP. Semplice, intuitivo, via web e con supporto per MySQL.

Scapy

http://www.secdev.org/projects/scapy/

Distribuito per Linux e per Windows, Scapy manipola i pacchetti VoIP, decodificandoli e forgiandoli in modo interattivo, combinando tra loro diverse tecniche di attacco.

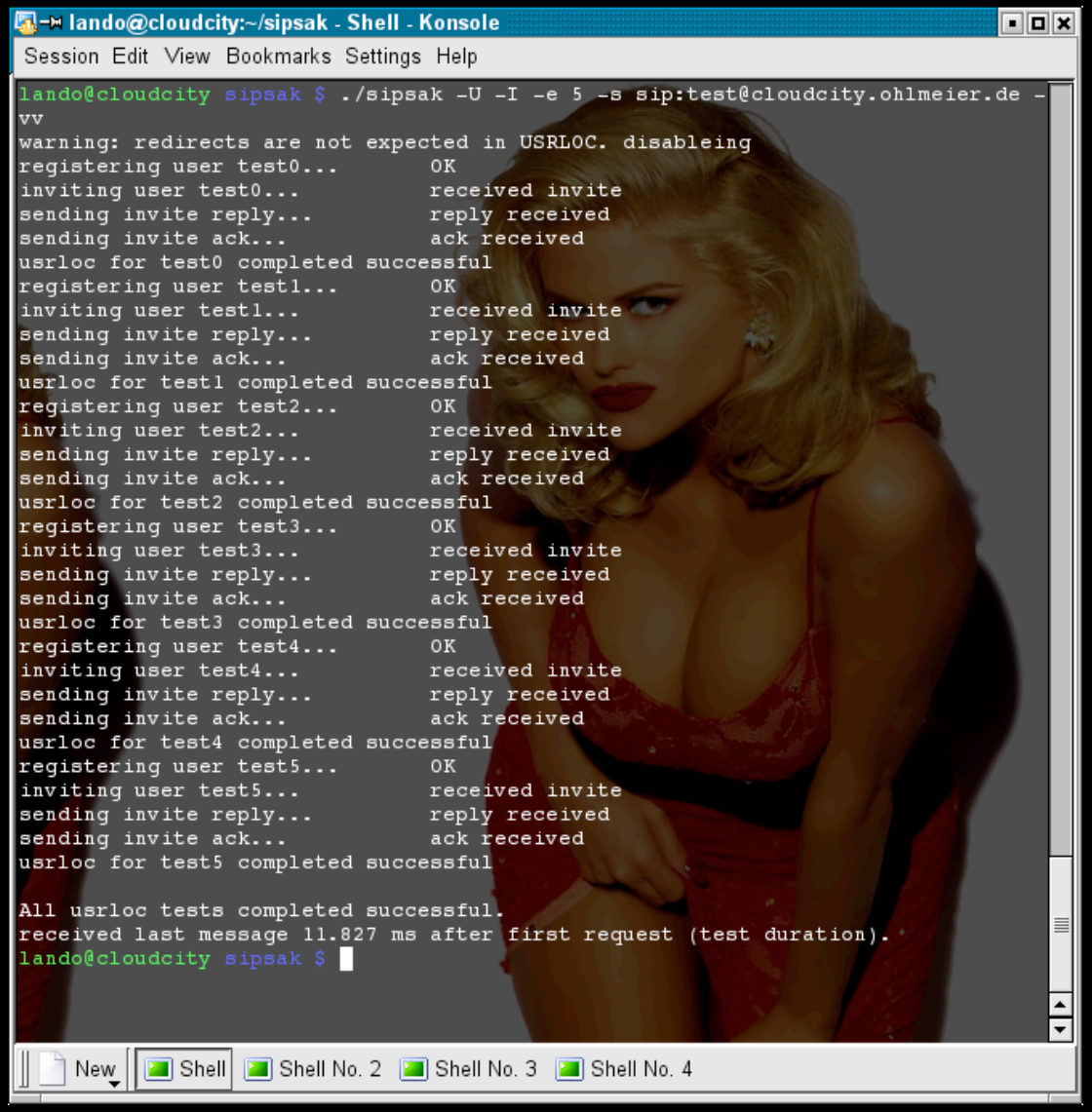
Keywords: send invalid frames, inject 802.11 frames
VLAN hopping, ARP cache poisoning, VOIP decoding,
WEP encrypted channel, combining technics

SipSak

http://sipsak.org/

Si tratta del coltellino svizzero del VoIPAdmin.
Permette di interagire con qualsiasi device SIP inviando traffico creato ad hoc per interagire con il server e verificare il suo comportamento in situazioni create da noi.

SipSak (2)


lando@cloudcity:~/sipsak - Shell - Konsole
Session Edit View Bookmarks Settings Help
lando@cloudcity sipsak $ ./sipsak -U -I -e 5 -s sip:test@cloudcity.ohlmeier.de -vv
warning: redirects are not expected in USRLOC. disableing
registering user test0... OK
inviting user test0... received invite
sending invite reply... reply received
sending invite ack... ack received
usrloc for test0 completed successful
registering user test1... OK
inviting user test1... received invite
sending invite reply... reply received
sending invite ack... ack received
usrloc for test1 completed successful
registering user test2... OK
inviting user test2... received invite
sending invite reply... reply received
sending invite ack... ack received
usrloc for test2 completed successful
registering user test3... OK
inviting user test3... received invite
sending invite reply... reply received
sending invite ack... ack received
usrloc for test3 completed successful
registering user test4... OK
inviting user test4... received invite
sending invite reply... reply received
sending invite ack... ack received
usrloc for test4 completed successful
registering user test5... OK
inviting user test5... received invite
sending invite reply... reply received
sending invite ack... ack received
usrloc for test5 completed successful
All usrloc tests completed successful.
received last message 11.827 ms after first request (test duration).
lando@cloudcity sipsak $
New
Shell
Shell No. 2
Shell No. 3
Shell No. 4

Ohrwurm

http://mazzoo.de/blog/2006/08/25#ohrwurm

Il “verme delle orecchie” è un RTP fuzzer. Il suo scopo è testare l'implementazione del protocollo SIP del device testato inviando una enorme quantità i richieste con diverse combinazioni di parametri, più o meno sensati, allo scopo di individuare eventuali comportamenti anomali.

Le anomalie riscontrate spesso si rivelano essere bug di implementazione.

Smap

http://www.wormulon.net/index.php?/archives/1125-smap-released.html

Unendo nmap e SipSak otteniamo uno strumento in grado di rilevare i device SIP, dedurre di che marca e modello di device si tratta dal fingerprint e creare una mappa della rete analizzata. E' inoltre possibile interagire direttamente con il device, fingendosi un apparato SIP, per ottenere maggiori informazioni.

SiVus

http://www.vopsecurity.org/html/tools.html

Si tratta di un SIP security scanner: verifica le caratteristiche del target dello scan rispetto ad un database di vulnerabilità conosciute.

SIPVicious

http://sipvicious.org/blog/

Suite che comprende uno scanner, un enumeratore ed un password cracker. Multipiattaforma, anche per MacOSX.

Altri strumenti

- Packet Gen & Packet Scan
- Shoot
- Sipness
- Sipshare
- Sip scenario
- Siptest harness
- Sipv6analyzer
- Winsip Call Generator
- Sipsim
- Mediapro
- Netdude
- SipBomber
- RTP Flooder
- Invite flooder
- RTP injector
- Sipscan
- reg. hijacker eraser/adder
- Fuzzy Packet
- Iax Flooder
- Cain & Abel
- SipKill
- SFTF
- VoIPong
- SipP

Il solito vecchio problema: le persone

hackit_07
ten years nerdcore

Social Engineering

Informazioni che riguardano la nostra infrastruttura possono essere ottenute dalle persone attraverso il telefono, questo proprio per la fiducia che questo strumento ha saputo acquisire nel tempo.

Su cosa basiamo la fiducia?

Viene spesso data per assodata la bontà di alcuni elementi, quali il numero chiamante, il tono e timbro di voce.

Forse iniziamo a sospettare di non dover credere al Caller ID, ma ...

Piccoli Accessori

In vendita su Internet per 25 € può essere collegato a PC, GSM e telefoni. Cambia il tono/“sesso” di chi parla.

Funzioni mancanti

Esiste un telefono senza la funzione “trasferisci chiamata”?

SI!

misconfiguration

```
081XXXXXXX
```

“Prema 1 per l’ufficio commerciale, 2 per il magazzino, 3 per accedere al menù di ricerca, 9 per parlare con un operatore”

```
3 0 0456152498
```

“Alba S.T. buon giorno, come posso esserle utile?”

Conclusioni

hackit_07

ten years nerdcore

Conclusioni

- **Corretta analisi del rischio e pianificazione**
- Separare la rete dati dalla rete voce (vlan)
- Gestire la priorità del traffico (QoS)
- Autenticazione ed Autorizzazione (AAA)
- Utilizzo di crittografia e certificati digitali (TLS, SRTP)
- Apparati configurati per prevenire gli attacchi IP conosciuti (mitm, garp, spoofing, flooding)
- Firewall a livello applicazione
- Evitare i single point of failure
- **Verifica periodica della sicurezza dell'infrastruttura**

sono preoccupato

VoIP explosion

"IDC Anticipates 34 Million More Residential VoIP Subscribers in 2010"

History

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

Benjamin Franklin, 1759

Conclusioni

il VoIP può essere sicuro

Conclusioni

più sicuro della telefonia tradizionale

Conclusioni

dipende da noi

Web-o-grafia

http://cavallette.autistici.org/2006/04/149

http://www.voipsa.org/

http://www.voip-info.org/

http://misitano.com/pubs/voip-ictsec.pdf

http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58.zip

http://www.schneier.com/blog/

http://arstechnica.com/news.ars/post/20060407-6552.html

http://www.sicurezzainformatica.it/archives/2007/01/voip_malware.html

http://www.skype.com/intl/it/

http://zfoneproject.com/

Web-o-grafia

http://www.it-observer.com/articles/1134/tackling_voice_security_threat

http://www.webcrunchers.com/crunch/esq-art.html

http://www.nytimes.com/2006/06/08/technology/08voice.html

http://www.cloudmark.com/press/releases/?release=2006-04-25-2

http://www.usdoj.gov/usao/nj/press/files/pdffiles/penacomplaint.pdf

http://www.usdoj.gov/usao/pae/News/Pr/2005/feb/Moore.pdf

Scholz - Attacking VoIP Networks

Domande?

Grazie per l'attenzione!

Alessio L.R. Pennasilico
mayhem@recursiva.org
http://www.recursiva.org

hackit_07
ten years nerdcore