Ultra secret chat using Wi-Fi covert channel

Data exfiltration inside
802.11 protocol frames

HITBSecConf

AXPOSITIE

YAGO HANSEN

About @yadox

Ethical hacker, expert in network engineering and system administration, with extensive experience in network infrastructures of all sizes. During his professional career, he has carried out international projects for large corporations in the banking, insurance, telecommunications, and Government security sectors among others.

In recent decades he has specialized extensively in wireless technologies, successfully leading numerous projects for security planning, implementation and auditing. With his company (WiFense), he has developed an interception system for one of the largest global intelligence corporations based in Israel. In the field of cybersecurity, he carries out regular interventions for the press, as well as lectures and training cycles in various universities and congresses.

Co-founder of Mundo Hacker, a team with which he has broadcasted programs on radio, streaming, podcast, conferences, as well as shows on public TV (Telecinco, Discovery Max, TVE La Dos and Channel Trece in Colombia). He published numerous publications and articles in specialized magazines, also collaborating with Ra-Ma editorial, through which he has written and published several books on computer security. For some years now, he has been a regular security trainer for intelligence, defense and national security services for many international governments.

Definitions

Data exfiltration: *defines the act of extracting and transferring information from computer systems without authorization of the owners.*

- *Requires physical access or network access*
- *Used to steal or leak information*
- *Requires strict data access prevention and DLP techniques*
- *In Governments and secure corporate environment is difficult to succeed*
- *Used in recent data leaks*
- *Traditional methods and more creative methods*

Definitions

Covert Channel *[Wikipedia]: a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.*

- *When the main channels are secure, data exfitration gets difficult*
- *Information hiding using overt channels. Hidden channels*
- *Shared resource for sender and receiver. Synchronization.*
- *Elude standard hardware, firmware, software (drivers)*
- *Taking advantage of technology and standards.*
- *Channel undetectable / un-interceptable*
- *Sniffing and recognizing patterns*
- *Data obfuscation and encryption*

Requirements

Hardware

Wi-Fi monitor mode adapter. ALFA AWUS-036NHA

OS

Linux OS, Kali Linux (recommended)

Python (2-3)

Hacking language for excellence

Scapy python library

Dot11 class

Packet manipulation library

DEMO

A bit of theory

802.11 PROTOCOL (description)

Layer 2 protocol

Network protocols structure (frame struct)

802.11 PROBE REQUEST FRAME

Frame Control	DURATION	ADDR1 (DST)	ADDR2 (SRC)	ADDR3 (RA)	SC	ADDR4 (WDS)	FRAME BODY*	FCS
	x	remote	random	remote	sc	x	IE	x

FRAME CONTROL HEADER

VERSION	TYPE	SUB TYPE	TO DS	From DS	More FRAG	Retry	PWR MGMT	MORE DATA	PROT FRAME	ORDER
x	0	4	0	0	x	x	x	X	x	x

FRAME BODY: IE FIELDS (INFORMATION ELEMENTS)

TS	0	51	7	16	221	66
TIMESTAMP	SSID	APchannel report	Country	Meassurement transmission	Vendor WPS	Extended rates
X	empty	User UUID	ciphereduser + sc	remote	random	remote

What is 802.11?

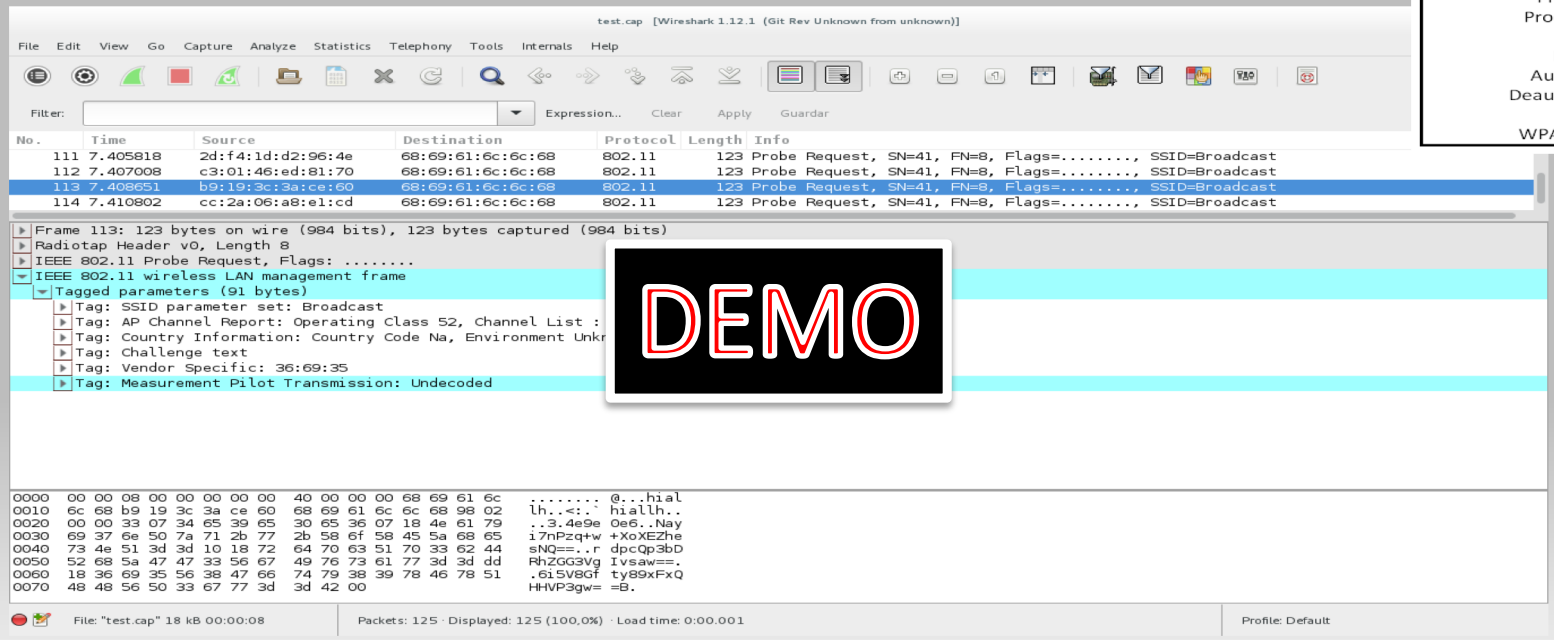
Wireshark reviewing packets

Using specific packet filters

Dissecting protocol

Checking for errors

Tipos de trama	Filtro Wireshark
Tramas de gestión	wlan.fc.type eq 0
Tramas de control	wlan.fc.type eq 1
Tramas de datos	wlan.fc.type eq 2
Association request	wlan.fc.type_subtype eq 0
Association response	wlan.fc.type_subtype eq 1
Reassociation request	wlan.fc.type_subtype eq 2
Reassociation response	wlan.fc.type_subtype eq 3
Probe request	wlan.fc.type_subtype eq 4
Probe response	wlan.fc.type_subtype eq 5
Beacon	wlan.fc.type_subtype eq 8
Disassociate	wlan.fc.type_subtype eq 10
Authentication	wlan.fc.type_subtype eq 11
Deauthentication	wlan.fc.type_subtype eq 12
WPA handshake	eapol



HITBSecConf

AXPOSITIE

Code revision

Protocol manipulation with Scapy

Type of frames to use

Channel, MAC, encryption key calculation

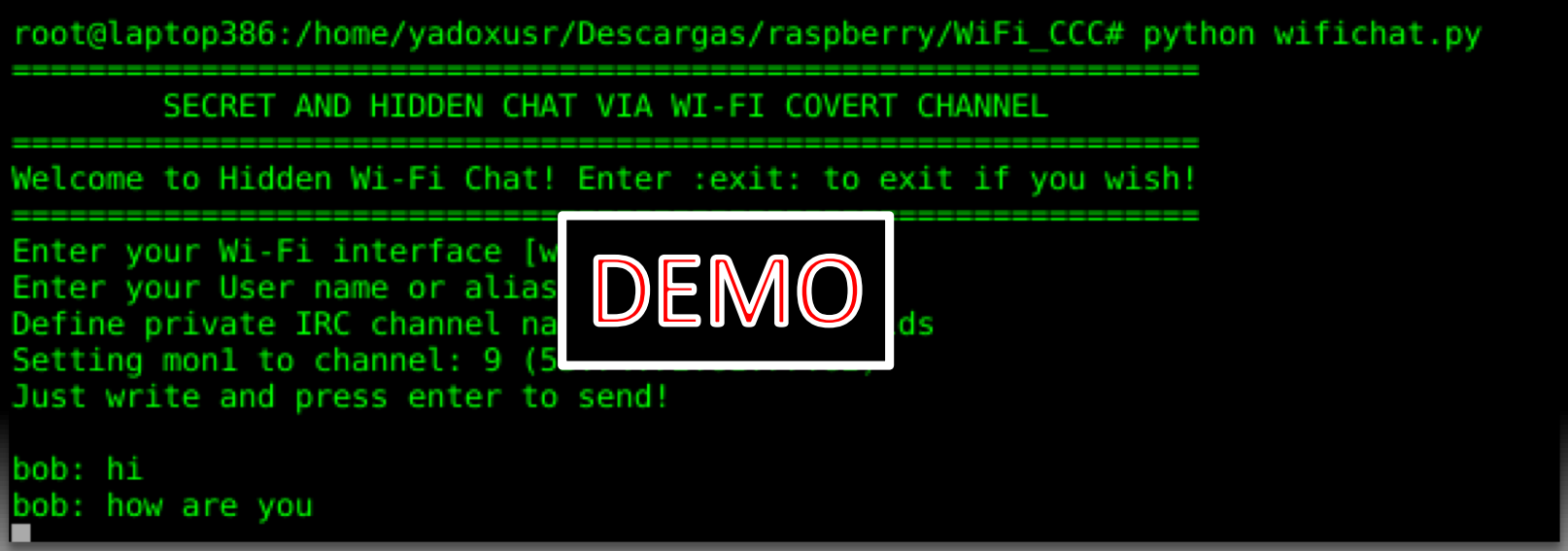
```
try:
        print "================================================================"
        print "       SECRET AND HIDDEN CHAT VIA WI-FI COVERT CHANNEL       "
        print "================================================================"
        print "Welcome to Hidden Wi-Fi Chat! Enter :exit: to exit if you wish!"
        print "================================================================"

        # Ask for monitor mode interface
    interface = raw_input("Enter your Wi-Fi interface [%s]: " %defaultinterface)
        if interface == '': interface=defaultinterface
    if not InitMon(interface): exit(-1)

        # Asks for the alias of the user
    username = raw_input("Enter your User name or alias: ")
        if username == '': exit()
        if username[0] == ":": exit()
        uuid = md5(getmac(intfmon))[7:14]
    userlist[uuid]=username
```

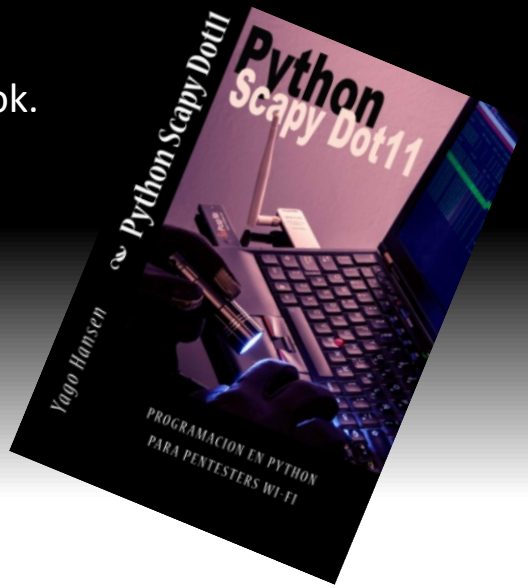
Demo time

https://github.com/yadox666/



Conclusions & Questions

- Detection and avoidance
- Difficulties
  Hardware, Drivers, Monitor mode, encryption
- Anti detection techniques
- Want more info?
  Ask for Python Scapy Dot11 book.



Don’t forget to visit our stand in the hacking armory section.

You’ll discover all thE Hacking tools you need

HITBSecConf