X.25 Networks in the Arab world

Actual present, next future & field experiences analysis of an underestimated (and still actual) security issue.

Sheraton Dubai Creek,

Dubai, U.A.E.

April 5th, 2007

TRACK 1

Raoul "Nobody" Chiesa

Board of Directors Member at TSTF & ISECOM

INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES – ISECOM.ORG

TELECOM SECURITY TASK FORCE – www.TSTF.net

DISCLAIMER

- We **do not recommend** that you use this material for unauthorised access to telecommunications operators', private companies' or governments' infrastructures and/or systems.
- We cannot be held responsible if you decide nevertheless to explore such networks and systems, find them **fascinating**, start getting **sloppy** and leave **tracks** that finally gets you **in troubles** !
- The X.25 addresses used in the slides can be **sometimes real and sometimes fake**: in the first case they could be out-of-date, else they're still existing and they've been used for **clear example purposes**. In any case, the real X.25 addresses mentioned as evidences have been taken from **public or private (personal) sources** and their publication **does not mean in any case** an invitation to attack or test the connected systems.
- The information contained within this presentation **does not infringe** on any **intellectual property** nor does it contain **tools** or **recipe** that could be in breach with international and local laws known by the Author at the time of this publication for HITB 2007 Dubai.

AGENDA

- Intro
- Basic know-how
- Advanced know-how
- Arabic X.25 networks 2007 survey — **ONLY FOR HITB DUBAI**
- The Banner's Gallery ! — **FUNNIEST PART !**
- X.25 Hacking & Real-life Evidences
- Upcoming 0-day X.25 trends — **YEAH, UPCOMING FUTURE...**
- Conclusions
- References, contacts
- Q&A

INTRO

[This Talk]

[The Speaker]

[T.S.T.F.]

[Why are we talking about X.25 security in 2007 ?]

THIS TALK

- This talk will analyze nowaday's Arab X.25 networks from a security point of view, and detail its hacking evolution over the last decade.
- Suggested target audience includes CSOs, CTOs, Professional Penetration Testers, Security Auditors, Security Experts, CEOs, CIOs.
- After a **brief basic overview**, we will cover the following **key issues**:
  - **Arabic Countries overview (X.25 Addressing Format)**
  - **Customer's and Attacker's users typology**
  - **X.25 exploiting**
  - **Field experiences**
  - **Recent and upcoming 0-day X.25 security issues**

NOTE: This talk will **not** deeply analyze many X.25 topics: in you are interested in learning more, please refer to the talk I gave at Hack in the Box K.L. back in 2005, named "**X.25 (in)SECURITY in year 2005: What, Why, When, Who, How (not anymore) uncovered data networks,(yet) covered targets).**

(www.packetstormsecurity.org/**hitb**05/BT-Raoul-Chiesa-X25-Security.pdf)

THE SPEAKER

- Raoul “Nobody” Chiesa
- Board of Director’s Member at CLUSIT (Italian Computer Security Association, ITALY), ISECOM (Institute for Security and Open Methodologies, USA), OWASP Italian Chapter (Open Web Application Security Project, USA), TSTF (Telecom Security Task Force).
- X.25 hacker, when it wasn’t “a crime”
- Exploring X.25 security since 1986
- Official ISECOM OSSTMM Key Contributor (1.5, 2.0., 2.1, 2.2, 3.0
- Nowadays, Raoul is just a security professional, loving his job and runs a well-known security consulting firm in Europe.

About T.S.T.F.

Who's who

- 35 years combined GSM telecommunications experience;
- 50 years combined information security experience;
- A unique view on telco security – **nobody else does it**;
- Active research (papers, tools, forums);
- Experience in Europe, Asia, USA;
- Self-funded, no "business experts" running it, no VCs.

Networked structure

- Structure similar to the Global Business Network (http://www.gbn.org/);
- No central office, global coverage;
- Leverage on each individual's skills and services;
- Leverage on network effect.

T.S.T.F. Key People

- Emmanuel Gadaix (Thailand)
- Philippe Langlois (France)
- Fabrice Marie (Singapore)
- Raoul “Nobody” Chiesa (Italy)
- Stavroula “Venix” Ventouri (Greece)

WHY ARE WE TALKING ABOUT X.25 SECURITY IN 2007 ?

- Because of our **security testing** and **R&D experiences** on this protocol set, started back around the **late 80's**.

- Because X.25 has been the **first commercial global data network.** Widely used because it was the **only applicable choice** (Internet was only available for the academics and the government's employees; later, **embargo** in some countries of the world did the rest of the job) from 70's to 90's.

- During the '90 many commercial companies went to the Internet, **but they kept their X.25 access** and contracts (that, usually, are still active, even if **they forgot about it**!).

WHY SHOULD YOU BE INTERESTED IN THIS ?

- During the 90's we encountered a **huge number** of breaches on tested infrastructures, usually **getting access via the main X.25 company' links**. More than **90% of them was found insecure**.

- We kept on finding **open doors** while pentesting companies with X.25 leased lines (**1996->2007**); these doors always brought the Tiger Team to the **core of the target network**.

- New connections and new services that lay on X.25 communications **still get launched**, also when if you don't know it or even think it'd be possible...

- We are now in year **2007**, and hacking "news" are still upcoming.

BASIC KNOW-HOW

[What's this ?]

[How it works ?]

" X.25 is used in a Packet Switched Network and in 1964 was designed by Paul Baran of the RAND Corporation for use with the Public Data Network (PDN) and unreliable analog telephone services.

***The idea was to connect a dumb terminal to a packet-switched network*.**

In 1976 X.25 became a standard under the CCITT, now the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T)."

INTRODUCTION: WHAT'S THIS ?

- An International **P**acket **S**witched **D**ata **N**etwork (PSDN).
- A model **very similar** to Public Switched Telephone Networks (PSTN).
- 3 main packet type:
  - **Data**
  - **Control**
  - **Facilities**.
  - **International standards** (X.25/X.29, X.28, X.75, X.121) created by **ITU** (International Telecommunications Union, Switzerland) in the 70's.
- Each subscriber has an **international X.25 address** (N.U.A., Network User Address) assigned to a **leased line**, with one or more **logical channels**.
- X.25 networks owned both by national telcos (**mainly**) and private operators.
- Weird customers... wait until the end of this talk ☺

INTRODUCTION: HOW IT WORKS ?

- Subscriber A can call Subscriber B in order to establish a **switched virtual circuit** (SVC) call or a **permanent virtual circuit** (PVC).

- **Only the traffic is billed**, and customers don't pay the "connection-time".

- Both on SVCs and PVCs links is possible to talk over **many different protocols** (TCP/IP, host-to-host, SNA, proprietary, voice, Kermit....).

- X.3 PAD capabilities are implemented in **major OS**:

✓ most of *NIX flavours
✓ Cisco IOS
✓ DEC VAX & HP AXP VMS/OpenVMS
✓ AS400 (OS400)
✓ old stuff, just like the movie "Wargames"
✓ strange or unknown systems: really **A LOT** !!

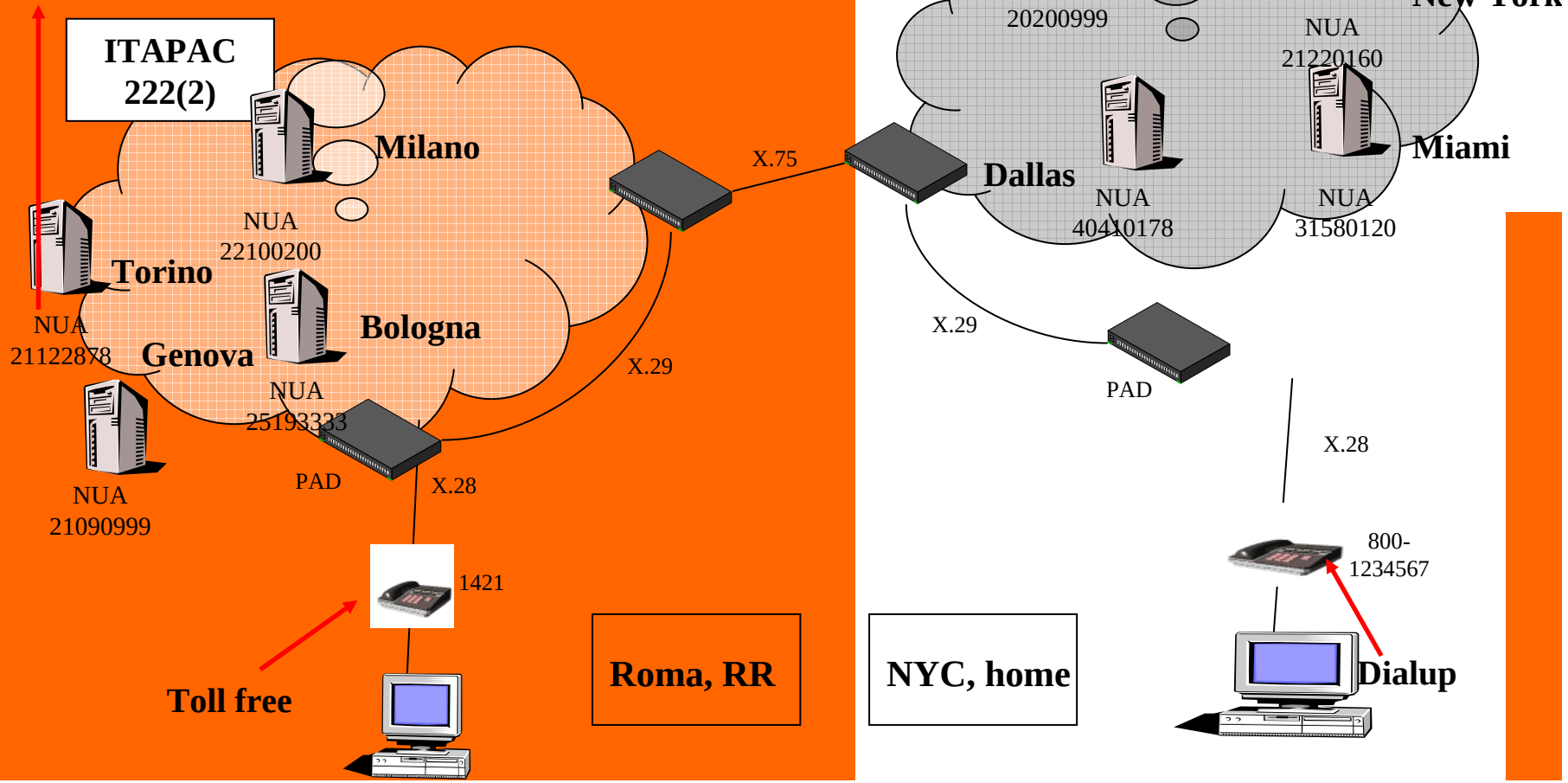
HOMEWORK

```
022221122878
|\ /|\_ _/|
| | | | | |____  22878: Network Port Address (NPA)
| | | |_|_____   11: Area Code for Torino
| | |___________ 2: ITAPAC Network (more networks)
| |_____________ 222: DCC assigned to Italy by ITU
```

Reading it both externally and locally:

0 222 2 11 22 878 from other networks;

21122878 from Italy/ITAPAC.



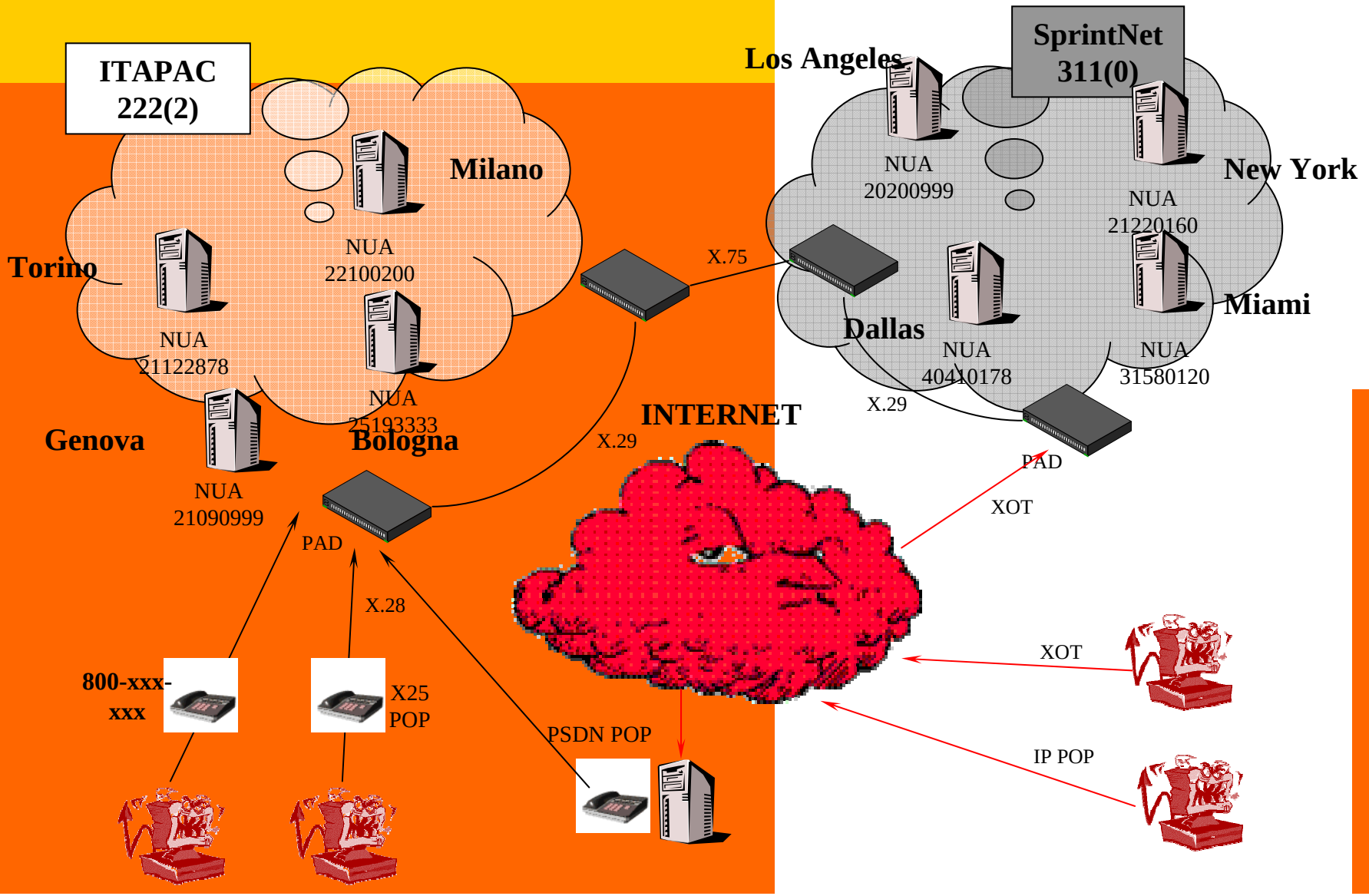
HACKWORK

Credits: Alfredo Andrés aka Slay

<tcpbgp@softhome.net>

Pablo Carretero aka Darkcode

<cmexec@kernelpanik.org>



ADVANCED KNOW-HOW

[NUA Addressing & DNICs]

[X.25 Scanning Examples]

[X.25 Survey: Analyzed Arab Networks]

X.25 ADDRESSING (1/2)

- X.25 hosts are **identified by**:
  - **NUA**s: one **device/system** could be configured in order to **manage different multiple assigned NUAs**, othwerwise could be **linked to more X.25 networks,** even with the **same NUA and a different DNIC** (USA/SprintNet->WW Partners, Bahrain/TymNet, ...).
  - ...but you may also find **more systems linked to a single NUA** (a.k.a. "***subaddressing***")
  - **Mnemonics**: only on some public network – eg Tymnet, SprintNet, Autonet, SITA, ...
  - ...think of 031069 Tymnet-gw - and those *one-step-ahead* private X.25 networks.

NOTE: X.25 addresses are reserved and should not be disclosed.

X.25 ADDRESSING (2/2)

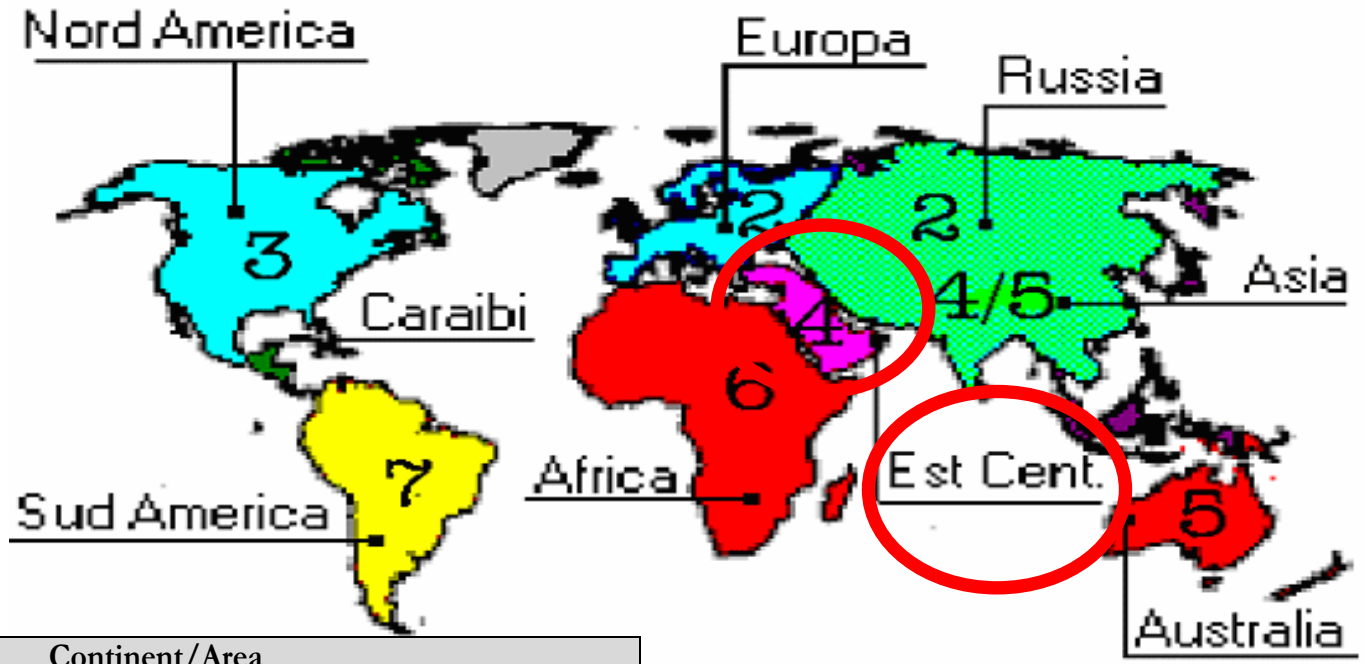
- X.121 address: **DNIC + NUA** = 15 digits max.
  - **DNIC** is a **4 digits** international code: **DCC** + **NCC**
  - **DCC** is assigned on a geographical basis by ITU (world's areas)
  - **NC**= Network Code (X.25 operators)

- (Local) NUA: **12 digits max** (typically 6->10). In many networks the is derived from the country itself national *PSTN numbering plan* (area codes referred to towns or areas of the country)

- For example:

	DNIC (4)	AC	NPA	
→	**311-0**	**212**	**10126**	**(USA, SprintNet, NYC)**
→	**280-2**	**21**	**229**	**(Cyprus, CytaPac, Limassol)**
→	**424-3**	**140**	**xx-yyy**	**(U.A.E., EMDAN, some town)**

DNIC WORLD AREAS



Zone	Continent/Area
1	Satellite connections for InmarSAT Voice/Dati(Atlantic, Pacific and Indian oceans)
2	Europe, Ex URSS
3	North America, Central America, some Carribean areas
4	Asia
5	Oceania
6	Africa
7	Part of Central America, Carribean and South America

Annex to ITU Operational Bulletin
No. 798 – 15.X.2003

INTERNATIONAL TELECOMMUNICATION UNION

TSB
TELECOMMUNICATION
STANDARDIZATION BUREAU
OF ITU

LIST OF DATA NETWORK IDENTIFICATION CODES (DNIC)
(According to ITU-T Recommendation X.121)

(POSITION ON 15 OCTOBER 2003)

Geneva, 2003

INDONESIA
INDONESIA.Annex to ITU OB 714-E – 11 – 15.04.2000
INMARSAT (OCEANI)
INMARSAT 111 1 Atlantic Ocean-East
111 2 Pacific Ocean
111 3 Indian Ocean
111 4 Atlantic Ocean-West
IRAN
IRAN (REPUBLIQUE ISLAMIQUE D') 432 1 IranPac
IRLANDA
IRLANDE 272 1 International Packet Switched Service
IRELAND 272 3 EURONET
IRLANDA 272 4 EIRPAC (Packet Switched Data Networks)
272 8 PostNET (PostGEM Packet Switched Data Network)
ISLANDA/ICELAND
ISLANDE 274 0 ISPAK/ICEPAC
ISRAELE
ISRAEL 425 1 ISRANET
ITALIA
ITALIE 222 1 Rete Telex-Dati (Amministrazione P.T. / national)
ITALY 222 2 ITAPAC X.25
ITALIA 222 3 PAN (Packet Network)
222 6 ITAPAC - X.32 PSTN, X.28, D channel
222 7 ITAPAC International
223 3 ALBADATA X.25
223 4 Trasmissione dati a commutazione di pacchetto X.25 (UNISOURCE ITALIA S.p.A.)
223 5 Trasmissione dati a commutazione di pacchetto X.25 (INFOSTRADA S.p.A.)
223 6 Trasmissione dati a commutazione di pacchetto X.25 (WIND Telecomunicazioni S.p.A.)
JAPAN/GIAPPONE
JAPON 440 0 GLOBALNET (Network of the Global VAN Japan Incorporation)
JAPAN 440 1 DDX-P (NTT Communications Corporation)
JAPON 440 2 NEC-NET (NEC Corporation)
440 3 JENSNET (JENS Corporation)
440 4 JAIS-NET (Japan Research Institute Ltd.)
440 5 NCC-VAN (NRI Co., Ltd.)
440 6 TYMNET-JAPAN (JAPAN TELECOM COMMUNICATIONS SERVICES CO., LTD.)
440 7 International High Speed Switched Data Transmission Network (KDD)
440 8 International Packet Switched Data Transmission Network (KDD)
441 2 Sprintnet (Global One Communications, INC.)
441 3 KYODO NET (UNITED NET Corp)
441 5 FENICS (FUJITSU LIMITED)
441 6 HINET (HITACHI Information Network, Ltd.)
441 7 TIS-Net (TOYO Information Systems Co., Ltd.)
441 8 TG-VAN (TOSHIBA Corporation)
JAPON 442 0 Pana-Net (MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.)
JAPAN 442 1 DDX-P (NTT Communications Corporation)
JAPON 442 2 CTC-P (CHUBU TELECOMMUNICATIONS CO., INC.)

DNIC/1

Each country has got at least one X.25 network (or more).

DNIC/2: THE AUSTRALIA CASE

Australian Network Identifiers:

Prefix	Allocation Date	Organisation
5052	30 June 1991	Telstra Corporation Ltd
5053	30 June 1991	Telstra Corporation Ltd
50541	6 September 1994	AAPT Ltd
50542	6 September 1994	AAPT Ltd
50543	6 September 1994	AAPT Ltd
50560	16 February 1994	SingCom (Australia) Pty Ltd
50568	16 February 1994	SingCom (Australia) Pty Ltd
50569	16 February 1994	SingCom (Australia) Pty Ltd
50573000	30 June 1991	Fujitsu Australia Ltd
50573500	19 February 1992	Department Of Defence
505790	17 November 1993	Department Of Defence
505791	17 November 1993	Department Of Defence
505799	23 February 1995	Telstra Corporation Ltd

Sub-carrier

Sub-carrier

Critical
(and shared !)

5052 = Austpac
5053 = Austpac International (formerly Midas / OTC Data Access)
5054 = Australian Teletex Network
5057 = Australian Private Networks

NB The allocation dates are official allocation dates, not necessarily actual dates. Austpac existed long before 1991.

The USA case

313 1	RCAG Telex Network
313 2	Compuserve Network Services
313 3	RCAG XNET Service
313 4	AT+T/ACCUNET Packet Switched Capability
313 5	ALASCOM/ALASKANET Service
313 6	Geisco Data Network
313 7	International Information Network Services - INFONET Service
313 8	Fedex International Transmission Corporation - International Document Transmission Service
313 9	KDD America, Inc. – Public Data Network
314 0	Southern New England Telephone Company - Public Packet Network
314 1	Bell Atlantic Telephone Companies - Advance Service
314 2	Bellsouth Corporation - Pulselink Servie
314 3	Ameritech Operating Companies - Public Packet Data Networks
314 4	Nynex Telephone Companies - Nyex Infopath Service
314 5	Pacific Telesis Public Packet Switching Service
314 6	Southwestern Bell Telephone Co. - Microlink II Public Packet Switching Service
314 7	U.S. West, Inc. - Public Packet Switching Service
314 8	United States Telephone Association - to be shared by local exchange telephone companies
314 9	Cable & Wireless Communications, Inc. - Public Data Network
315 0	Globenet, Inc. - Globenet Network Packet Switching Service
315 1	Data America Corporation - Data America Network
315 2	GTE Hawaiian Telephone Company, Inc. - Public Data Network
315 3	JAIS USA-NET Public Packet Switching Service
315 4	Nomura Computer Systems America, Inc. - NCC-A VAN public packet switching service
315 5	Aeronautical Radio, Inc. - GLOBALINK
315 6	American Airlines, Inc. - AANET
315 7	COMSAT Mobile Communications - C-LINK
315 8	Schlumberger Information Network (SINET)
315 9	Westinghouse Communications - Westinghouse Packet Network
316 0	Network Users Group, Ltd. - WDI NET packet
316 1	United States Department of State, Diplomatic Telecommunications Service Black Packet Switched Data Network
316 2	Transaction Network Services, Inc. -- TNS Public Packet-switched Network
316 6	U.S. Department of Treasury Wide Area Data Network

Data carriers & Telcos

Multinationals

Spy Game ? ;)

DNIC/4: THE U.A.E. CASE

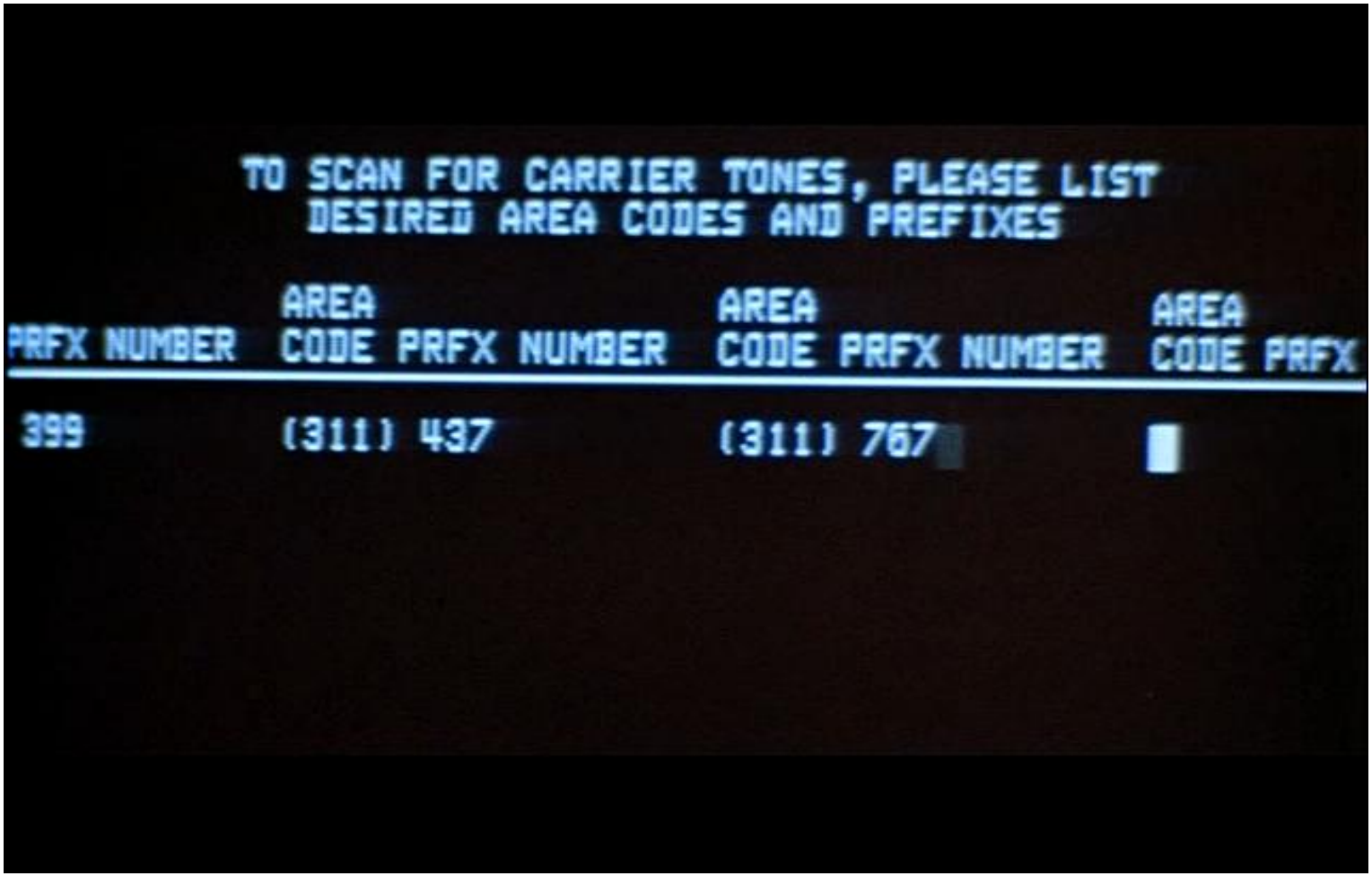
EMIRATS ARABES UNIS *UNITED ARAB EMIRATES* EMIRATOS ARABES UNIDOS	424 1 424 3	EMDAN Teletex Network EMDAN X.25 and X.28 Terminals

X.25 INTERNATIONAL ROUTING

- Since “once upon a time”, x.25 intl. routing has **never been reliable**.
- **Not all countries can call all networks.**
- **As a obvious consequence, X.25 scanning sometimes can suck a lot, if you’re not experienced enough:**
  - France/Transpac is good for scanning **Africa**.
  - Italy/Itapac is good for scanning **South America**.
  - Germany/DatexP is good for **Asia-Pacific** scanning.
- International routing issues have been noticed and observed in many countries, due to X.121 bandwidth limitations. Because of:
  - **poor countries**
  - **not enough budget**
  - **Few international X.25 links requests** (not a lot of subscribers making intl X.25 calls...except for hackers !

“WARGAMES” & SCANNING

WARDIALING…


TO SCAN FOR CARRIER TONES, PLEASE LIST
DESIRED AREA CODES AND PREFIXES
PRFX NUMBER
AREA CODE PRFX NUMBER
AREA CODE PRFX NUMBER
AREA CODE PRFX
399
(311) 437
(311) 767

X.25 WARDIALING: SCANNING FOR TARGETS 1/3 (Cyprus)


```
Scanning from NUA: 0280221000 started on 15-OCT-1994 15:29:30.75
0280221091  %COM        DROP STATION
0280221092  %COM        ECHO STATION
0280221093  %COM        TRAFFIC GENERATOR
0280221101  %CLR_OCC
0280221102  %CLR_DTE
0280221106  %CLR_DTE
0280221107  %COM
0280221108  %CLR_DTE
0280221117  %CLR_OCC
0280221118  %CLR_DTE
0280221121  %COM        MINISTRY OF HEALT, VAX/VMS
0280221122  %COM        IBM AIX UNIX
0280221125  %CLR_DTE
0280221147  %CLR_RPE SUBADDRESS 48 CYTA Pager via x.25
0280221199  %COM        CISCO
0280221206  %COM  LOGON: ??
0280221225  %COM        CISCO
0280221229  %COM  CISCO  BYBLOS  BANK  S.A.L.  -  LIMASSOL/CYPRUS  ACS-CYPRUS
LINE 6
0280221248  %COM        COM/DTE
0280221273  %CLR_DTE
0280221274  %CLR_OCC
0280221276  %CLR
Scanning ended with NUA: 0280221396 on 15-OCT-2000 15:46:36.32
```

X.25 WARDIALING: SCANNING FOR TARGETS 2/3 (Canada)


```
- 202 - ONTARIO  - Up to 700
20200115          VAX/VMS
20200116          VAX/VMS
20200156          Diand Information System
20200214          $ UNIX      (gtagmhs2)
20200230        METS Dial-In Server  Enter your login:
2020024098        Control Port on Node Ottawa 6505 PAD
20200286          $ VAX/VMS
2020032099        MPX.25102: PASSWORD
20200321          SunOS     Rel 4.1.3 (X25)
20200322          SunOS       ""
20200330          INETCO    Magicbank
20200342        ::
20200497          VAX/VMS
202005421         $ VAX/VMS
20200548          SunOS     Rel 4.1.3 (TMS470)
20200582          $ VAX/VMS   Production System
```

Who knows which OS is this ?

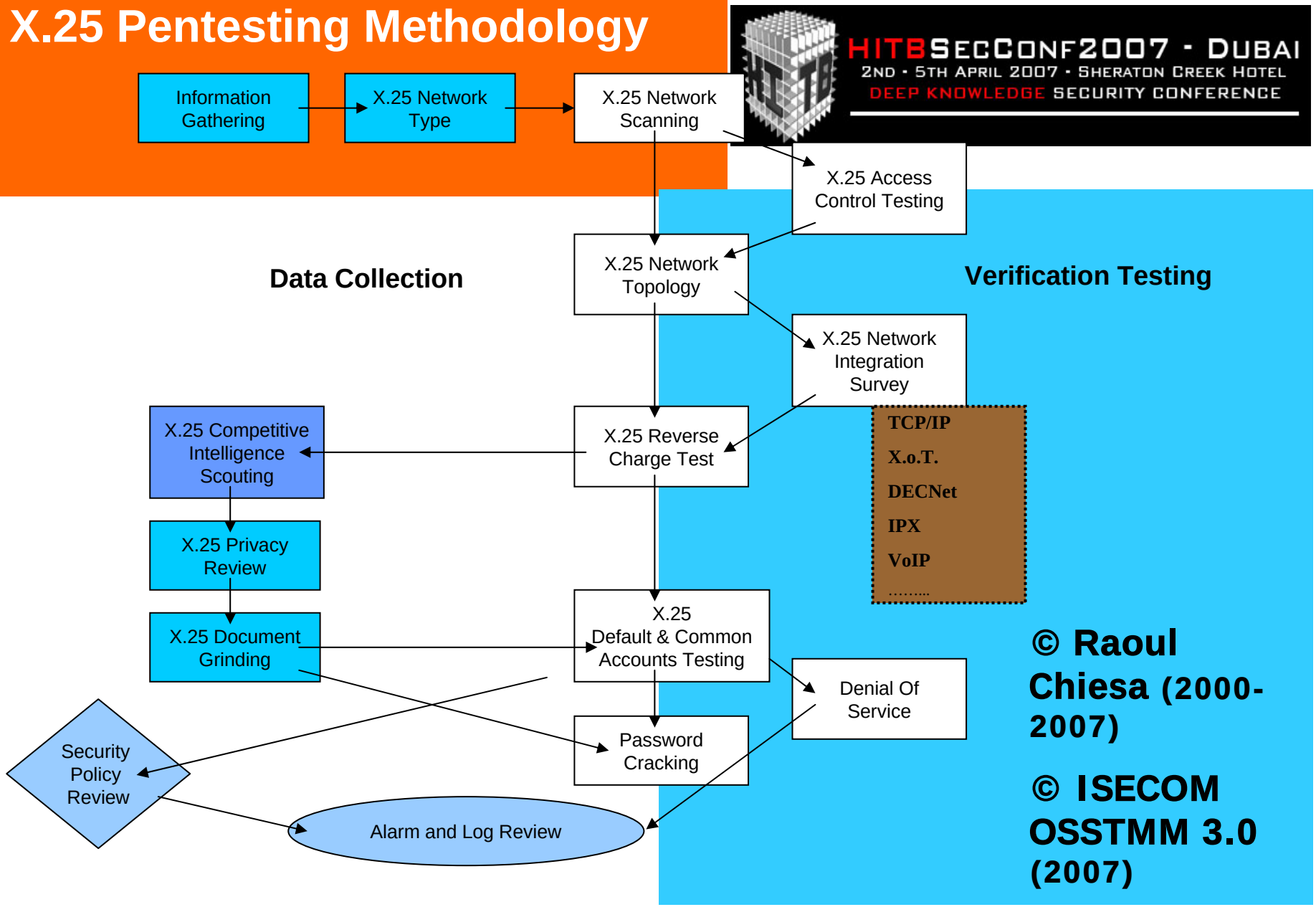
X.25 WARDIALING: SCANNING FOR TARGETS 3/3 (Luxembourg)

cat 027049xxxx
0270441057 busy (a few channels available)
0270442208 strange, crashes Putty
0270442187 yodette FTP READY
0270442207 com then hangs up
0270442308 **2 channels only, PAD** on subaddress 98
0270442317 **pad without password**, as for 0270442308
0270442299 **disconnects (DTE subscanning ??)**
0270449585 **SCO Unix** on subaddress 20 and 21: SCO OpenServer(TM) Release 5 (**umialt.transardenna.lu**) (ttyEt00)
0270449416 **CISCO with angry banner**
0270449530 **IBM AIX Unix**
0270449567 **IBM AIX Unix**
0270449529 **One more IBM AIX Unix**
0270449499 nothing (COM and drops)

2007 X.25 Survey on some Arab countries

- The following X.25 networks have been analyzed:
  - Bahrain
  - Brunei
  - Iran
  - Lebanon
  - Pakistan
  - Qatar
  - Saudi Arabia
  - UAE

X.25 Pentesting Methodology



Bahrain: information gathering/1

BAHRAIN - BASIC GLOBAL CONNECTION SERVICE
==========

(+3h GMT) **Last Update: May 18, 1993**

Bahrain Telecommunications Company (BTC) **Net. Name: BAHNET**
238 Road 1704 **DNIC: 4263**
Manama 317
Diplomatic Area
Bahrain

Contact Customer Services and Sales:
Mr. Ali Abdulla Algami **Tel: (973) 885312**
(973) 885274
Fax: (973) 885566 or 883451
Telex: (490) 8790
Tariff Dept.:
Khalil Ebrahim Fardan **Tel: (973) 885433**
Fax: (973) 885016
Telex: (490) 7892

Engineering:
Eng. - Yaqoob Sabt
Hardware Eng. - Mirza Aldurazi
Tel: (973) 883463
Fax: (973) 883461 or 252535
Telex: (490) 8000

Bahrain: information gathering/2

---------- OPERATIONAL/TECHNICAL INFORMATION ----------

1. FIRST LINE CUSTOMER SERVICE/TROUBLE REPORTING:
   Contact: Mr. Ali A. Aligami
   Hours of Operation: Sat-Wed 7am-2pm, Thur 7am-1pm
   Phone: (97.3)885312 and 885274
   Telex: (490) 8790
   Fax: (97.3)885566 or 883451
   Ontyme: INTL.BTCCOM
   Dialcom: INT.011

2. NETWORK INFORMATION ADDRESS: n/a

3. TEST ADDRESS: 4263007450004 Drop Host
   426300446921 Echo Host

4. ASYNC ACCESS PROCEDURES:

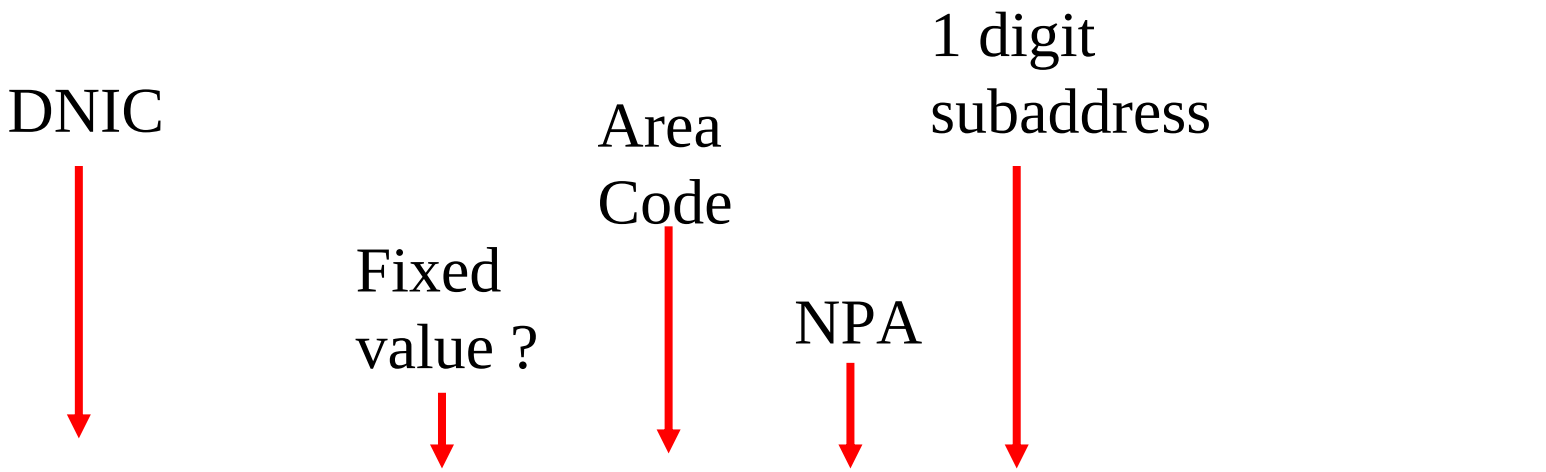
   1) Upon connection, type in a period (.) until it is echoed. Follow this by the (RETURN) key.

   2) A greeting message followed by an asterisk (*) will be printed.

   3) Enter your destination X.121 host address followed by the (RETURN) key, then enter your username and password to connect to your destination.

   4) At any moment, you may return to the asterisk prompt from the data mode by pressing (ctrl p) keys together. Pressing (RETURN) at the asterisk takes you back to data transfer mode.

Bahrain: NUA format guessing



This means that our scan format will be:

4263 00 xxx yyy z(z)

Brunei NUA Format & Scannings

0528220097	%COM	TRAFFIC GENERATOR
0528220098	%COM	ECHO STATION
0528220099	%COM	DROP STATION
0528220111	%COM	HANGS UP
0528220136	%COM	PAGER BY TELEKOM
0528220198	%COM	WELCOME TO JABATAN TELEKOM RAPID PAGE SERVICE
0528220228	%COM	HANGS UP

- ...Meaning that our scan format will be:

0	5282	20	xxx
0	5282	10	xxx
0	5282	xx	yyy

Iran NUA Format

- We obtained the following X.25 NUAs:

  0432121132297

  0432171000111

- So, our NUA scanning format could be:

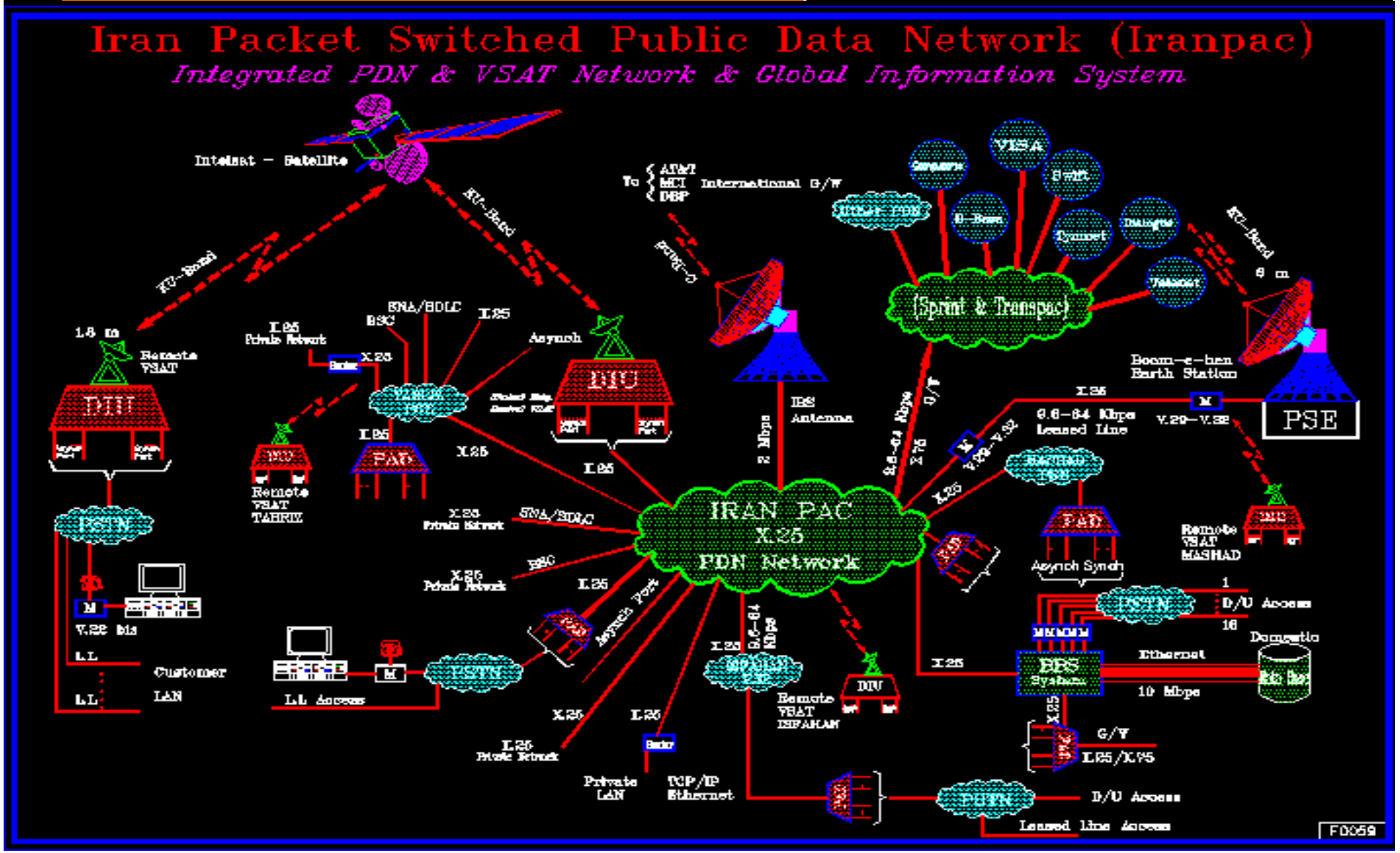
  0 4321 21 132 xxx

  0 4321 71 000 xxx

- Automatizing it...

  0 4321 xx yyy zzz

UNCOMMENTED



Lebanon NUA Format

- We obtained the following X.25 NUAs:

  041500880004 (COM + “Beep”, scan it from Germany/Datex-P in order to have good routing and no Network Congestion errors!)

  041500880047 (VAX/VMS)

- So, our NUA scanning format could be:

  0 4150 088 00 04

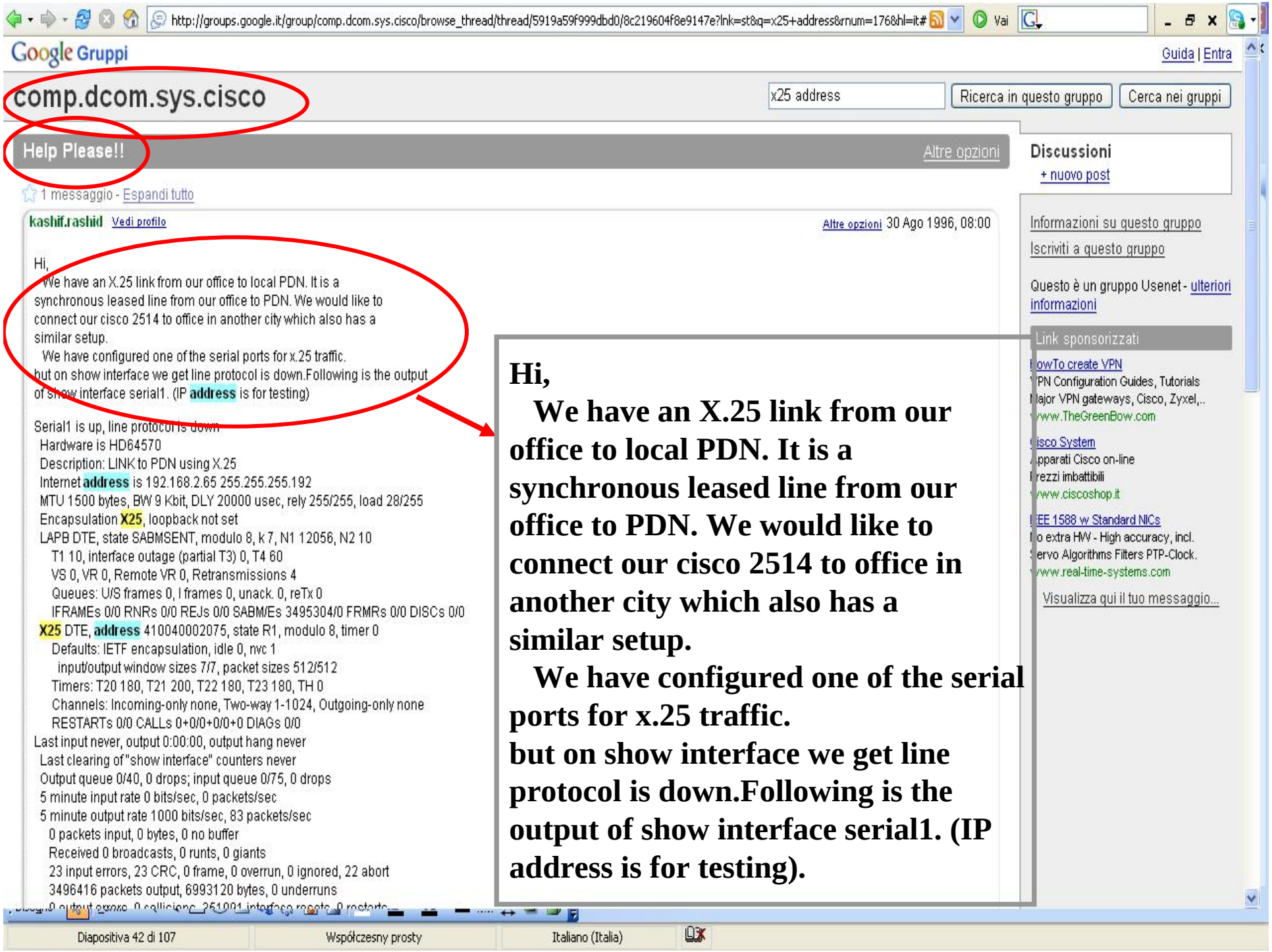
  0 4150 088 00 47

- Automatizing it...

  0 4150 xxx 00 yy

Pakistan NUA Format

- IT was near impossible to find a working NUA from Pakistan.
- Some years ago, “google hacking” became a standard approach
- You can’t imagine **how much** google can help you at finding unknown NUAs...
- http://groups.google.it/group/comp.dcom.sys.cisco/browse_thread/thread/5919a59f999dbd0/8c219604f8e9147e?lnk=st&q=x25+address&rnum=176&hl=it#8c219604f8e9147e


http://groups.google.it/group/comp.dcom.sys.cisco/browse_thread/thread/5919a59f999dbd0/8c219604f8e9147e?lnk=st&q=x25+address&rnum=176&hl=it#
Google Gruppi
Guida | Entra
comp.dcom.sys.cisco
x25 address
Ricerca in questo gruppo
Cerca nei gruppi
Help Please!!
Altre opzioni
1 messaggio - Espandi tutto
kashif.rashid Vedi profilo
Altre opzioni 30 Ago 1996, 08:00
Hi,
We have an X.25 link from our office to local PDN. It is a synchronous leased line from our office to PDN. We would like to connect our cisco 2514 to office in another city which also has a similar setup.
We have configured one of the serial ports for x.25 traffic.
but on show interface we get line protocol is down.Following is the output of show interface serial1. (IP address is for testing)
Serial1 is up, line protocol is down
Hardware is HD64570
Description: LINK to PDN using X.25
Internet address is 192.168.2.65 255.255.255.192
MTU 1500 bytes, BW 9 Kbit, DLY 20000 usec, rely 255/255, load 28/255
Encapsulation X25, loopback not set
LAPB DTE, state SABMSENT, modulo 8, k 7, N1 12056, N2 10
T1 10, interface outage (partial T3) 0, T4 60
VS 0, VR 0, Remote VR 0, Retransmissions 4
Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
IFRAMEs 0/0 RNRs 0/0 REJs 0/0 SABM/Es 3495304/0 FRMRs 0/0 DISCs 0/0
X25 DTE, address 410040002075, state R1, modulo 8, timer 0
Defaults: IETF encapsulation, idle 0, nvc 1
input/output window sizes 7/7, packet sizes 512/512
Timers: T20 180, T21 200, T22 180, T23 180, TH 0
Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
RESTARTs 0/0 CALLs 0+0/0+0/0+0 DIAGs 0/0
Last input never, output 0:00:00, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 1000 bits/sec, 83 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
23 input errors, 23 CRC, 0 frame, 0 overrun, 0 ignored, 22 abort
3496416 packets output, 6993120 bytes, 0 underruns
Discussioni
+ nuovo post
Informazioni su questo gruppo
Iscriviti a questo gruppo
Questo è un gruppo Usenet - ulteriori informazioni
Link sponsorizzati
owTo create VPN
PN Configuration Guides, Tutorials
ajor VPN gateways, Cisco, Zyxel,..
ww.TheGreenBow.com
isco System
pparati Cisco on-line
rezzi imbattibili
ww.ciscoshop.it
EE 1588 w Standard NICs
o extra HW - High accuracy, incl.
ervo Algorithms Filters PTP-Clock.
ww.real-time-systems.com
Visualizza qui il tuo messaggio...
Hi,
We have an X.25 link from our office to local PDN. It is a synchronous leased line from our office to PDN. We would like to connect our cisco 2514 to office in another city which also has a similar setup.
We have configured one of the serial ports for x.25 traffic.
but on show interface we get line protocol is down.Following is the output of show interface serial1. (IP address is for testing).
Diapositiva 42 di 107
Współczesny prosty
Italiano (Italia)

Luckness helps…

⌘ Uh, we got a tech guy looking for help here...

⌘ Let's have a closer look at his configuration example on the Cisco router !

Getting a Pakistan working NUA

http://groups.google.it/group/comp.dcom.sys.cisco/browse_thread/thread/5919a59f999dbd0/8c219604f8e9147e?lnk=st&q=x25+address&rnum=176&hl=it#

Google Gruppi — Guida | Entra

comp.dcom.sys.cisco — x25 address — Ricerca in questo gruppo — Cerca nei gruppi

Help Please!! — Altre opzioni

1 messaggio - Espandi tutto

kashif.rashid Vedi profilo — Altre opzioni 30 Ago 1996, 08:00

Hi,
We have an X.25 link from our office to local PDN. It is a synchronous leased line from our office to PDN. We would like to connect our cisco 2514 to office in another city which also has a similar setup.
We have configured one of the serial ports for x.25 traffic. but on show interface we get line protocol is down.Following is the output of show interface serial1. (IP address is for testing)

```
Serial1 is up, line protocol is down
  Hardware is HD64570
  Description: LINK to PDN using X.25
  Internet address is 192.168.2.65 255.255.255.192
  MTU 1500 bytes, BW 9 Kbit, DLY 20000 usec, rely 255/255, load 28/255
  Encapsulation X25, loopback not set
  LAPB DTE, state SABMSENT, modulo 8, k 7, N1 12056, N2 10
     T1 10, interface outage (partial T3) 0, T4 60
     VS 0, VR 0, Remote VR 0, Retransmissions 4
     Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
     IFRAMEs 0/0 RNRs 0/0 REJs 0/0 SABMEs 3495304/0 FRMRs 0/0 DISCs 0/0
  X25 DTE, address 410040002075, state R1, modulo 8, timer 0
     Defaults: IETF encapsulation, idle 0, nvc 1
       input/output window sizes 7/7, packet sizes 512/512
     Timers: T20 180, T21 200, T22 180, T23 180, TH 0
     Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
     RESTARTs 0/0 CALLs 0+0/0+0/0+0 DIAGs 0/0
Last input never, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 83 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     23 input errors, 23 CRC, 0 frame, 0 overrun, 0 ignored, 22 abort
     3496416 packets output, 6993120 bytes, 0 underruns
```

410040002075

Discussioni
+ nuovo post

Informazioni su questo gruppo
Iscriviti a questo gruppo

Questo è un gruppo Usenet - ulteriori informazioni

Link sponsorizzati

HowTo create VPN
VPN Configuration Guides, Tutorials
Major VPN gateways, Cisco, Zyxel,..
www.TheGreenBow.com

Cisco System
Apparati Cisco on-line
Prezzi imbattibili
www.ciscoshop.it

IEEE 1588 w Standard NICs
No extra HW - High accuracy, incl.
Servo Algorithms Filters PTP-Clock.
www.real-time-systems.com

Visualizza qui il tuo messaggio...

Diapositiva 42 di 107 — Współczesny prosty — Italiano (Italia)

Social Engineering could help as well ;)

http://groups.google.it/group/comp.dcom.sys.cisco/browse_thread/thread/5919a59f999dbd0/8c219604f8e9147e?lnk=st&q=x25+address&rnum=176&hl=it#

Following are the parameters provided by PDN and our **x25** config.
The ip numbers used are for testing purpose only.

```
interface Serial1
description Link to PDN using X.25
ip address 192.168.2.65 255.255.255.192
encapsulation x25
bandwidth 9
no keepalive
x25 default pad
x25 address 410040002075
x25 win 7
x25 wout 7
x25 ips 512
x25 ops 512
x25 ltc 1
x25 htc 1024
no cdp enable
lapb modulo 8
lapb k 7
lapb n1 2104
lapb n2 10
lapb T1 10
lapb T4 60
lapb N2 10
```

Following are the parameters given by PDN:

```
hardware mode: dte      duplex:full
clock config:normal     line speed: 9600 modem
timeout 5000msec        busyout: notallowed
modem capability: none  terminations: no

level2 charcteristics:
link proc:      labp dce
response timeout: 500 msec      retransmit limit:10
max bits in frame: 2104         frame window size:7
response delay timer: 200 msec  idle probe timer: 10000 msec
disconnect timer : 60sec        idle channel timer = off
octet data only
```

I will appreciate your help.
Thanx
Regards,
Kashif Rashid
kashif.ras...@cressoft.com.pk

Scegliere Guida in linea dal menu ? per visualizzare la Guida di Paint. 561,367

Pakistan NUA scanning

- We obtained the following X.25 NUA:

  0410040002075 (Thanks Rashid ! ;)

- So, our NUA scanning format should be...

  0 4100 4000 2 075

- Automatizing it...

  0 4100 x000 y zzz

Qatar: information gathering/1

QATAR - BASIC GLOBAL CONNECTION SERVICE

==========

(+4h GMT) **Last Update: July 7, 1990**

Qatar Public Telecommunications Corporation (QTEL)
PO Box 217
Doha, Qatar

Net. Name: DOHPAK
4270/4271
Tel: (974)426899
Fax: (974)426000
Telex: (497)4007 COMPOS DH

Contact Sales and Marketing:
Miss Maha Abdul Kader
Mr. Rashid Al Bader

1. ACCESS/SPEEDS: Asynchronous 300,1200 bps

2. PROTOCOLS: Asynchronous, Synchronous (X.25)

3. PRICING:

Subscription Charge: QR .550/month
Usage: QR 1.00/minute
QR 1.50/segment

4. COMMENTS: DOHPAK is a branch of the Hong Kong Network (Intelpack).

Qatar: information gathering/2

----------OPERATIONAL/TECHNICAL INFORMATION----------

1. FIRST LINE CUSTOMER SERVICE/TROUBLE REPORTING:
   Contact: Watch Keeper on Duty
   Hours of Operation: 24 hours a day, 7 days a week
   Phone: 433177
   Telex: 4007
   Fax: 410555

2. SERVICE INFORMATION ADDRESS: n/a

3. TEST ADDRESS: 04271 111 258

4. ASYNC ACCESS PROCEDURES:

   Upon modem connect . . .

   Receive: WELCOME TO DOHPAK X
   PLEASE TYPE YOUR CALLED NUMBER
   Send: <The full international number of the
   required distant computer><cr>
   Receive: PLEASE LOG-IN:
   Send: <enter username><cr>
   Receive: PASSWORD:
   Send: <password><cr>

   You are now connected to the service required

5. TYMUSA AVAILABLE: NO

6. DEFAULT PAD SETTINGS: n/a

Qatar: NUA format guessing

04271 111 258

DNIC → **4271**

Area Code → **111**

End-User Address → **258**

Test Address

This means that our scan format will be:

4271	**111**	**xxx**
4271	**xxx**	**yyy**

Saudi Arabia NUA Format

- We found some NUAs around...
  0420160014025
  0420140014017
  0420140014002 TEST ADDRESS

- So this should mean that our format would be:

04201	8010	xxxx
04201	40014	xxx
04201	60014	xxx
04201	40024	xxx
04201	40025	xxx
04201	40034	xxx

- Let's check if we're right: we'll **take the Test Address** (End-User Address) as **a suffix**, and we'll **play around the AC** (Area Code)

Saudi Arabia Areas Format

0420130100002 (OK) BURAYDAH
0420131100002 (OK) BAIL
0420140000002 (OK) RIYADH
0420140200002 (OK) MALAZ
0420140400002 (OK) MANFOUBA
0420140600002 (OK) ULAYAH
0420140700002 (OK) KHURAIS
0420140800002 (OK) MAATHAR
0420141100002 (OK) KHARJ
0420141200002 (OK) SHAFFA
0420141300002 (OK) AZIZIYAH
0420141400002 (OK) NASEEM
0420141600002 (OK) MURSALAT
0420141900002 (OK) NAS[illegible]
0420142100[illegible] (OK) [illegible]ERH
0420144400[illegible] (OK) SHQ[illegible]
0420149200[illegible] (OK) K.K.I.A.
0420154000002 (OK) BIBAN
0420157000002 (OK) BALAD
0420160000002 (OK) JEDDAH
0420160100002 (OK) BAB MAK
0420160200002 (OK) ROUWAIS
0420160300002 (OK) MAKKAH ROAD
0420160400002 (OK) NAZLAH
0420160500002 (OK) SALAMAH
0420160900002 (OK) MUSHRIFAH
0420161100002 (OK) SAHEFAAH
0420161200002 (OK) SHARAFIYAH
0420161300002 (OK) MAKKAH ROAD/52
0420161500002 (OK) SULAIMANIAH
0420165700002 (OK) K.A.I.A.
0420166100002 (OK) YAMBU
0420166200002 (OK) YAMBU
0420168100[illegible] (OK) [illegible]K
0420173[illegible] (OK) [illegible]
0421750[illegible] (OK) TAIF
0421800[illegible]002 (OK) DAMMAN
0420180100002 (OK) BAREED
0420180200002 (OK) LASILKI
0420180300002 (OK) MUTLAQ
0420180400002 (OK) ALKHOBAR
0420180700002 (OK) QATIF
0420180800002 (OK) DHARAHN
0420181200002 (OK) ARAF
0420182100002 (OK) SAKAKAH
0420183100002 (OK) JUBAIL
0420183200002 (OK) JUBAIL
0420186100002 (OK) HOFUF
0420190100002 (OK) ABHA
0420190600002 (OK) MUSHAIT

Scripted in 10 minutes !

UAE Scannings/1

CENSORED

You should have joined HITB DUBAI 2007…If you really wanted to see this slide ☺

UAE Scannings/2

NOTE: **X.25 call syntax on VOS:**

call_thru 255 -form -gateway mds-pdn -address
(insert X.121 NUA, e.g. 031069 for TymNet Gw)

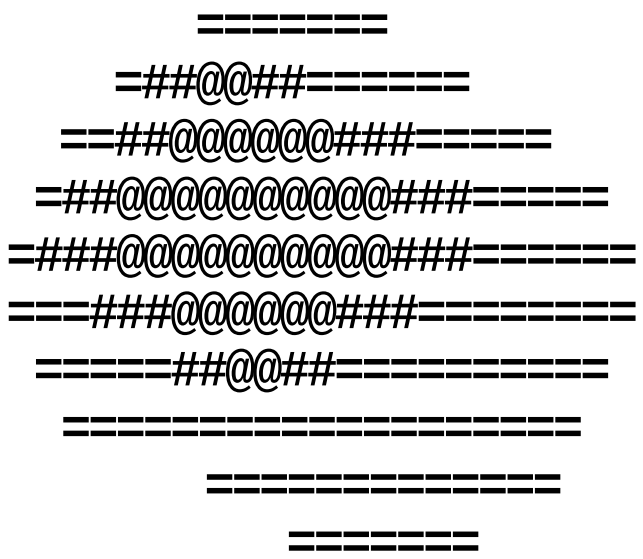
CENSORED

You should have joined HITB DUBAI 2007…If you really wanted to see this slide ☺

PAST AND RECENT TALES

- **90's**: NUA scanners available for PRIMOS (Electron), VMS (Nobody & Zibri), *NIX (Sentinel), AMIGA (Ncomm Scripts), DOS (Just Telix Salt Scripts), Windows (Scripts).
- **1994-95**: AT&T, GTE and others major US telcos got hacked via X.25
- **Recent years**: worldwide famous group released their own scanner (**ADMx25**).
- Recent years: **Multithread** and **Multichannel** Unix X.25 scanner available in the wild: it's **able to scan a whole country in a few hours**.
- **2003-07**: Russian crackers perform **mass huge scans** over SprintNet international networks and dialups (intl' reverse charge scans).

BANNER'S GALLERY



```
Welcome to At&T node attmail Unix System V/386 Release 3.2B

attmail login:
```

[TLC carriers have always been targets]
(and will always be)

BANNER'S GALLERY


```
Connected to 04201xxxxxxxx

INMARSAT-C Land Earth Station at INMARSAT C LES JEDDAH
KSA

WELCOME TO INMARSAT C LES JEDDAH KINGDOM OF SAUDI
ARABIA


Enter ?<CR> to get help information,
      C<CR> to cancel input.
```

[Land Earth Station *]

* See Jim Geovedi BCS and HITB 2006 presentation "Hacking a Bird in the Sky" !

BANNER'S GALLERY


```
$ pad 05057998210xxxx
Connected
Trying xxx.xx.xxx.xx ... Open
    **************************************************************
    * Access to this computer system is limited to authorised users only. *
    * Unauthorised users may be subject to prosecution under the Crimes   *
    *                        Act or State legislation                     *
    *                                                                     *
    *   Please note, ALL CUSTOMER DETAILS are confidential and must       *
    *                            not be disclosed.                        *
    **************************************************************

User Access Verification
Username:
```

[TLC carriers have always been targets/2]

BANNER'S GALLERY

Set h /x 0724xxx40xxx

COM

Welcome to Brasilsat Satellite Control System - node GVAX3

Username:

Satellites from Brazil

BANNER'S GALLERY


```
$ pad 0311077200704
Break-in sequence is '^Pa'

Connecting...
Connected

                                        ########
                                      ##############
                                    ##################
 ####  ##       ##           ##    ##   ###############
#    #  #        #            #    # ### ##############
#       #   ###  ####   ###   #    # ### #    ###   ###
#   ##  #  #   # #   # #   #  #    # ### # ### # ##  ##
 ##### ###  ###  ####   #### ###   ##  ## ### ##  ###
 ....................................###############.......................
                                        ########
    +++                        ####                      =#\
  ...|.  Deutsche            #### France Telecom      -==#### Sprint
     |   Telecom            ####                        -#/

#=========================================================================#
#                                WARNING!!                                #
# ACCESS TO AND USE OF THIS SYSTEM IS RESTRICTED TO AUTHORIZED INDIVIDUALS! #
#         Now we are start sending your addresses to the FBI / KGB!       #
#=========================================================================#

User Access Verification

Username:
```

[TLC carriers have always been targets/3]

BANNER'S GALLERY


```
-------------------------------------------------------------
 |ATTENTION: You have accessed a confidential and proprietary |
 |computing network.  Access  beyond this  point is  unlawful |
 |without  previous authorization from  BP and  MCI Security. |
 |TACACS+ account is required for access                      |
  ----------------------------------------------------------
 |WARNING: All  transactions  on this  router are logged 7x24 |
  ----------------------------------------------------------

ROUTER ID - BPAVMELR15C36


User Access Verification (Domain 10 - PDC)

The GNOC is in the process of cleaning up TACACS accounts. If your
account is disabled, you will require re-approval from the GNOC and
PSO WAN Service Line Leader.  Please send e-mail to
bpgnoc_tacacs_request@lists.wcom.com.

TACACS Username:
```

[TLC carriers have always been targets/4]

BANNER'S GALLERY


```
02624xxxxxxxxxx
Connecting...
Connected

                                C C
                               CC CC
                              CCC CCC
                              CCC CCC
                 CCC          CCC CCC          CCC
              CC  CCCC        CCC CCC        CCCC  CC
               CCC  CCCC      CCC CCC      CCCC  CCC
                CCCC  CCCC    CCC CCC    CCCC  CCCC
                  CCCC  CCCC  CCC CCC  CCCC  CCCC
                    CCCC  CCCCCC CCCCCC  CCCC
                      CCCC  CCC   CCC  CCCC
                        CCCC   CCC   CCCC
          CCCCCCCCCCCCCCCCCCCC  CCCCCCC  CCCCCCCCCCCCCCCCCCCC
         CCCCCCCCCCCCCCCCCCCCC  CCCCCCC  CCCCCCCCCCCCCCCCCCCCC

         C O M M E R Z B A N K   COPOS TEST Testsystem  TZK

System/32, VOS Release 14.2.2aa, Module %copost#m1
Please login  23:27:04
```

BANNER'S GALLERY


```
# pad 0487321873

          ______   _____    ____                       /\  /^\
       O |  ____! |  __ \  / __ \          O  _      ,'  /' /\`\
      /\/| !__    | !__) || !__! |        /|\/    ___/  /' /'  `\`\
     /   |  __!   |  ___/ |  __  | O  ,  / |     ____/' /' /^\  `\`\_
    /\   | !____  | |     | |  | | |\/   / \      -----'_/'   `\__`-
   /_/_  !______! !_!     !_!  !_! |/\_ _/___\_     _____________
     BUREAU OF ENVIRONMENTAL MONITORING & DATA PROCRSSING
           ENVIRONMENTAL PROTECTION ADMINISTRATION
             GOVERNMENT OF THE REPUBLIC OF CHINA


Username:
```

X.25 HACKING

[X.25 VS Internet]

[Attackers, Targets & Goals]

[What can I find ?]

[Evidences]

DIFFERENCES WITH THE INTERNET

- **X.25 Addressing is reserved**: scanning is the *mostly used way* to find new targets.
- WAN concept: a **single NUA** can **open a whole new world** to the attackers.
- No TCP/IP stack, **no "exploiting" concept** (well, until 2006...).
- Primarily **brute force attacks** on login (always works!).
- "Old school" hacking, social engineering and smartness **may help a lot**.
- There are a few X.25 walkers all over the world: **no kiddies, no "pink noise", no game's playing**.
- If he isn't a walker, he's an attacker: probably with a **very high skill level**.
- There are also just **a few X.25 security experts** all over the world...

ZOOMING THE DIFFERENCES: X.25 HACKING

- Mostly done via scanning and bruteforcing
- There are not “bugs” but “features”
  - ✓ PSI mail
  - ✓ CUD and FACILITY
  - ✓ XoT (x.25 over TCP)
  - ✓ IP over x.25
  - ✓ PPP

ATTACKERS, TARGETS AND GOALS

GOOD GUYS

- "X.25 Newbies" (South America scene)
- Lonely attackers, old school hackers
- Security researchers / Elite hackers (la crème)

BAD GUYS

- "X.25 Newbies" aka Real-Criminals! (Russia scene)
- Criminal organizations (w/insiders on target)
- High-Level Industrial spies (no "idiots")
- Intelligence (Foreign Agencies' agents)
- (cyber) Terrorists (?)

ATTACKERS, TARGETS AND GOALS

- **Subscribers**
  - X.25 subscribers did **always** run **huge data networks**.
  - It's like having an **open door to the world**, that directly brings up strangers into our bedroom.
  - Monitoring **isn't easy at all**, requires specific skills and the knowledge of high-level attackers' habits.
  - Attackers abuse of X.25 resources to **scan for new targets**: this means **money** that will be billed to you as well as **legal problems (**if someone will ever realize what happened).

- **Services**
  - **Telco Management Networks** (NMC, NE, Billing, etc..)
  - **GSM and 3G SMSCs/MMSCs**
  - **Bank to Bank transfers** (SWIFT); **E-payments** (POS)
  - **Local PTs offices** WAN
  - Worldwide Logistics & Transports
  - **Heavy Industry**
  - **Travelling** and **Hotels agencies**/environments (**airports** and **flight companies** as well)
  - **Chemical** and **Pharmaceutical**
  - **SAP**, **ORACLE** and similars (let's say "the big software houses")
  - **WHQ** -> **HQ** -> **Branches World Wide**
  - **Government** institutions and **Agencies**

ATTACKERS, TARGETS AND GOALS (The honey prize: OS for prime time)

- AOS/VS
- *BBS Systems*
- Bull PAD (Bull DPX/2)
- CICS/VTAM
- Cisco IOS
- CDC NOS
- DEC VAX/VMS, AXP/OpenVMS
- DEC Ultrix
- DEC Terminal Decserver
- DG/UX Aviion General
- DOS
- DRS/NX
- GS/1
- HP 3000
- HP/UX 9000
- IBM Aix
- IBM OS/400 (AS/400)
- IRIX SGI
- IRIS Operating System
- Linux
- Motorola XMUX (Gandalf)
- Northern Telecom PBXs
- PACX/Starmaster (Starmaster Gandalf)
- Pick Systems
- PRIMOS Prime Computer
- RSTS
- SCO
- Shiva LAN Router
- Sun Solaris
- TOPS 10/20
- Unknown systems (you will find many of them)
- VCX Pad
- VM/CMS
- VM/370
- XENIX
- WANG Systems
- ……

I'M SORRY BUT FRIENDS EXPLAINED ME IT'S BETTER I WON'T SHOW YOU THIS SLIDE, NEVER ☹

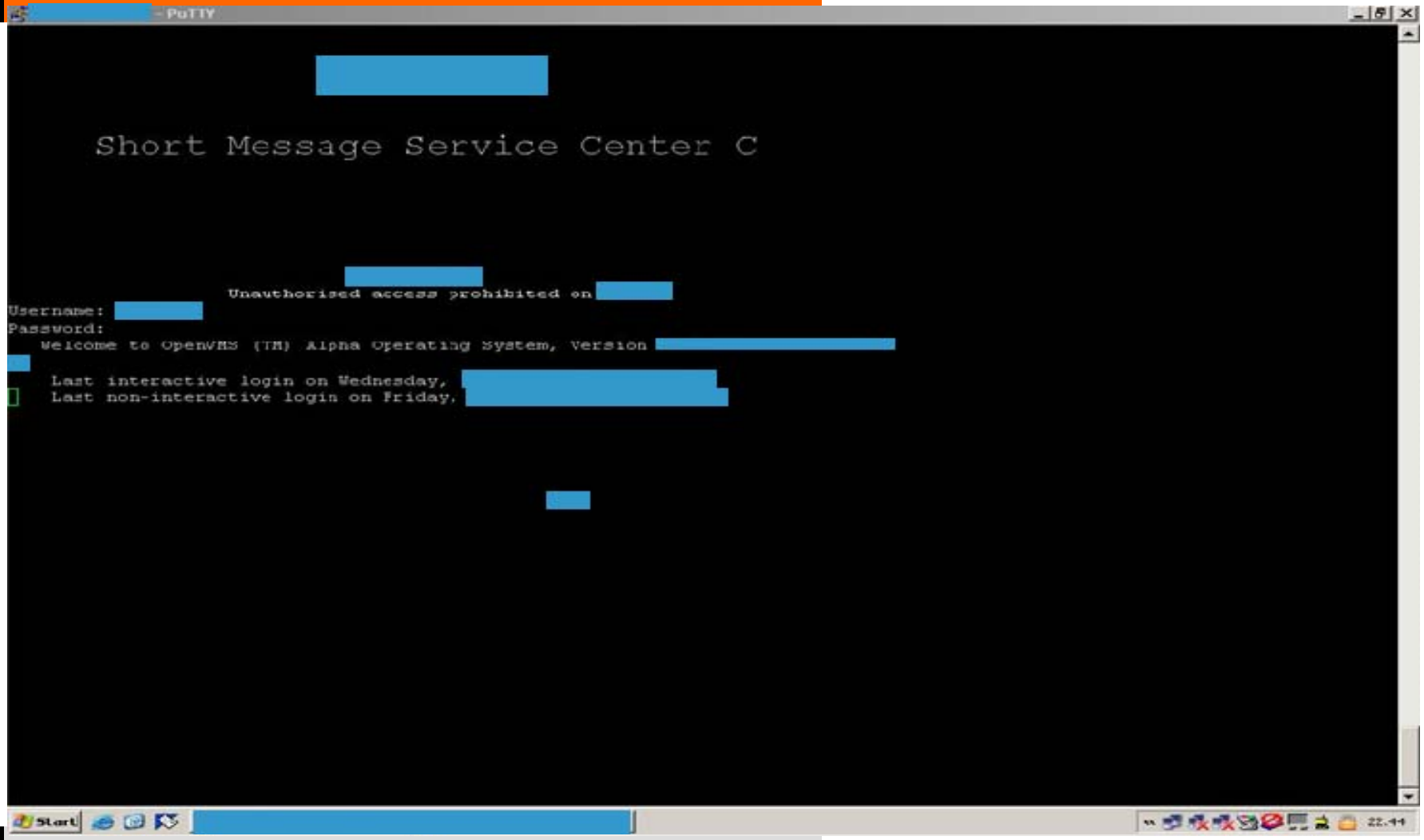
Censored for my personal life-assurance !

DIRECTORY SERVICE, PLEASE ! (India)

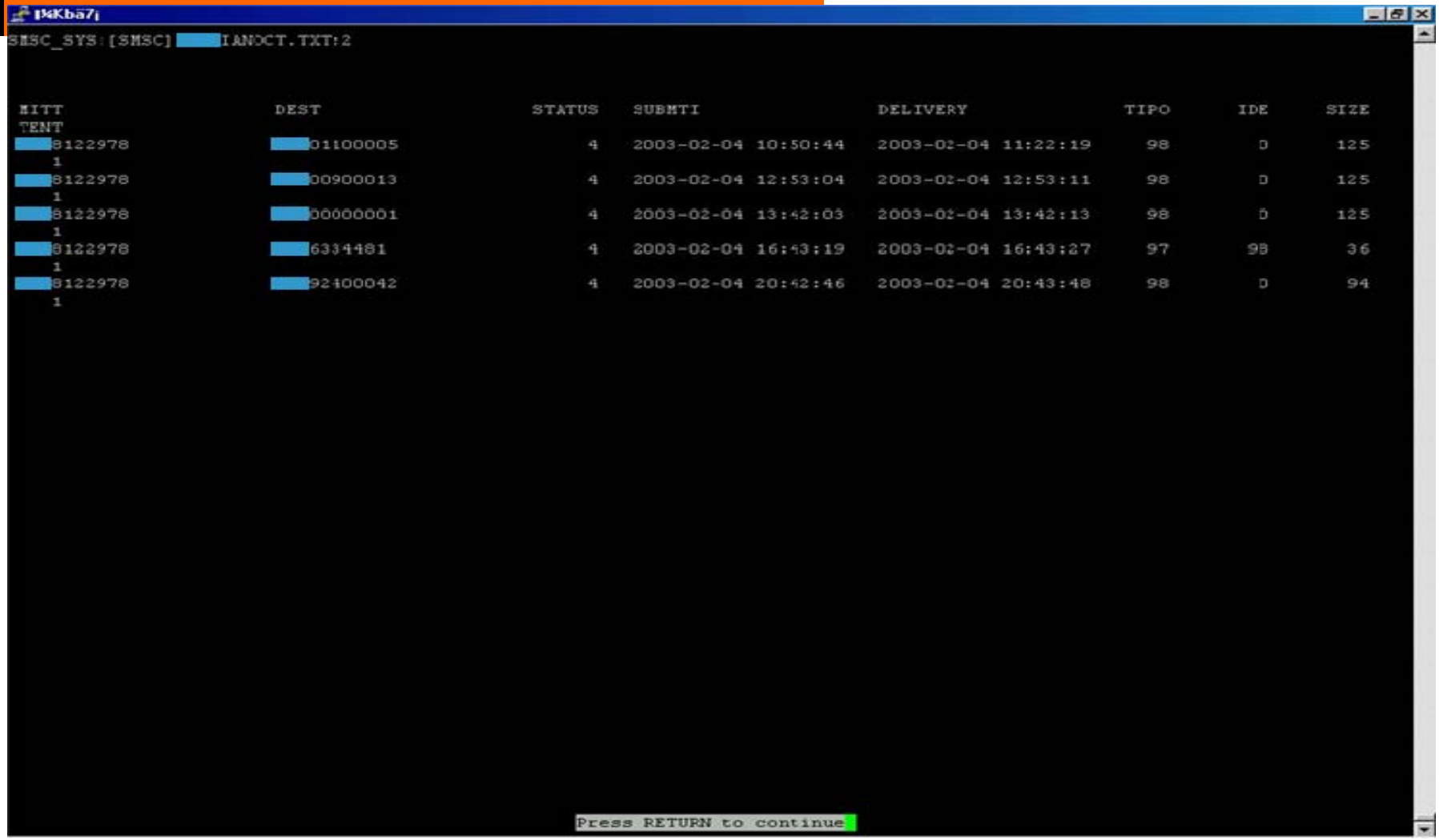
CENSORED

You should have joined HITB DUBAI 2007…If you really wanted to see this slide ☺

UH, IS THIS AN SMSC ?!?



PROCESSED SMSs: “FROM”, “TO”



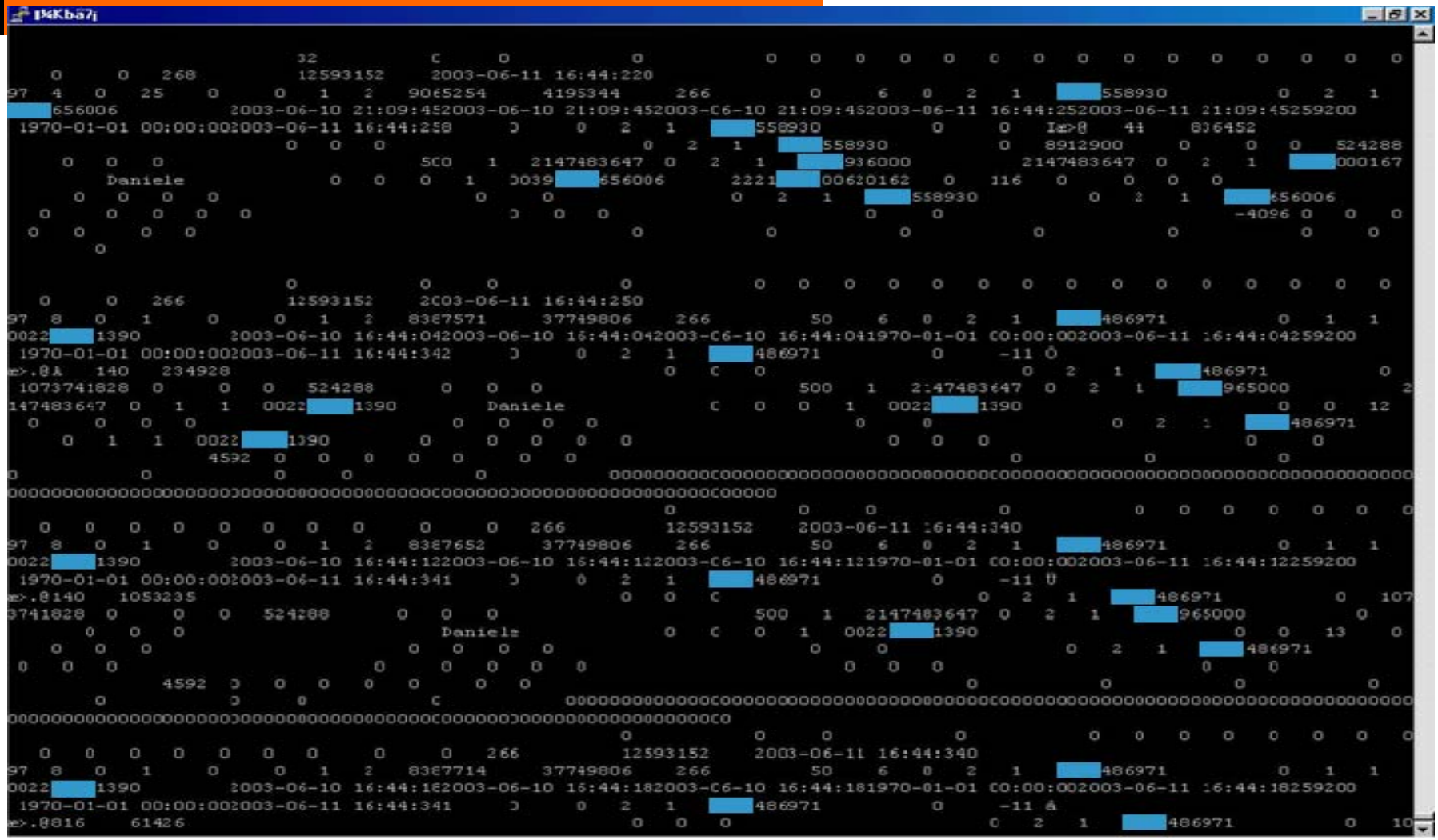
```
SMSC_SYS:[SMSC] [redacted]IANOCT.TXT;2

MITT                 DEST                 STATUS   SUBMTI              DELIVERY            TIPO    IDE     SIZE
TENT
[redacted]8122978    [redacted]01100005       4    2003-02-04 10:50:44  2003-02-04 11:22:19   98      0      125
   1
[redacted]8122978    [redacted]00900013       4    2003-02-04 12:53:04  2003-02-04 12:53:11   98      0      125
   1
[redacted]8122978    [redacted]00000001       4    2003-02-04 13:42:03  2003-02-04 13:42:13   98      0      125
   1
[redacted]8122978    [redacted]6334481        4    2003-02-04 16:43:19  2003-02-04 16:43:27   97     98       36
   1
[redacted]8122978    [redacted]92400042       4    2003-02-04 20:42:46  2003-02-04 20:43:48   98      0       94
   1

Press RETURN to continue
```

SMS PROCESSING QUE (!)


```
000C91[redacted]9180988FFFFFFFF 00000000000000000000000000 FFFFFF 9[redacted]69050000000000 000000 00000000000000000000
00000000000000000
15:55:02.18|04400403|MSISDN not found in cache
15:55:02.18|04400403|ISID inserted in cache
15:55:02.18|04400403|MSISDN inserted in cache
15:55:02.18|04400403|Context new 823
15:55:02.18|04400403|IOS received
15:55:02.18|04400403|SAD_DECODE_ADDR: Encoded address 000C91[redacted]185900FFFFFFFF -> address 0039[redacted]319500
15:55:02.18|04400403|SAD_DECODE_ADDR: Decoded address [redacted]819500 TELEPHONE NATIONAL
15:55:02.18|04400403|TP-MTI     ------01  SMS-SUBMIT (in the direction MS to SC)
15:55:02.18|04400403|TP-RD      -----0--  Accept duplicate message
15:55:02.18|04400403|TP-VPF     ---10---  TP-VP field present and integer represented (relative)
15:55:02.18|04400403|TP-SRR     --0-----  A status report is not requested
15:55:02.18|04400403|TP-UDHI    -1------  The beginning of the TP-UD field contains a header in addition to the short message
15:55:02.18|04400403|TP-RP      0-------  TP-Reply-Path parameter is not set in this SMS-SUBMIT/DELIVER
15:55:02.18|04400403|TP-MR      11100111  Message reference number 231
15:55:02.18|04400403|TP-DA      00001010  Address length 10
15:55:02.18|04400403|TP-DA      -000----  TON -> Unknown
15:55:02.18|04400403|TP-DA      ----0001  NPI -> ISDN/telephone numbering plan (E.164/E.163)
15:55:02.18|04400403|TP-DA      00110011  [redacted]
15:55:02.18|04400403|TP-DA      00100011  [redacted]
15:55:02.18|04400403|TP-DA      01100011  36
15:55:02.18|04400403|TP-DA      01111001  97
15:55:02.18|04400403|TP-DA      00010110  61
15:55:02.18|04400403|TP-DA                Address: [redacted]369761
15:55:02.18|04400403|TP-PID     00------  Protocol or Telematic interworking
15:55:02.18|04400403|TP-PID     --0-----  SME to SME protocol
15:55:02.18|04400403|TP-PID     ---00000  SM-AL protocol
15:55:02.18|04400403|TP-DCS     0000----  General Data Coding indication
15:55:02.18|04400403|TP-DCS     --0-----  Uncompressed
15:55:02.18|04400403|TP-DCS     ---0----  No message class meaning
15:55:02.18|04400403|TP-DCS     ----00--  Default alphabet
15:55:02.18|04400403|TP-VP      11111111  Validity period : 63 week(s)
15:55:02.18|04400403|TP-UDL     00110010  50
15:55:02.18|04400403|TP-UDHL    00000101  5
15:55:02.18|04400403|..IEI      00000000  Concatenated short messages, 8-bit reference number
15:55:02.18|04400403|..IEIDL    00000011  3
15:55:02.18|04400403|..IEDa      00110110  54  reference number
15:55:02.18|04400403|..IEDb      00000010  2  maximum number of short messages
15:55:02.18|04400403|..IEDc      00000010  2  sequence number
15:55:02.18|04400403|Event: 00, State: 00, Action: 01
15:55:02.18|04400403|Save PATIND data
15:55:02.18|04400403|NRT: recognised address as type EMPTY
15:55:02.18|04400403|SAD_RAW_ENCODE: Encoding [redacted]369761 as an TELEPHONE UNKNOWN address
15:55:02.18|04400403|SAD_RAW_ENCODE: Encoded address 000A81[redacted]637916FFFFFFFFFF
                                    Press RETURN to continue
```

SMS SNIFFING (IN REAL-TIME…)

HITB SECCONF2007 - DUBAI
2ND - 5TH APRIL 2007 - SHERATON CREEK HOTEL
DEEP KNOWLEDGE SECURITY CONFERENCE



X.25 INTERCEPTION AND REAL-TIME INVESTIGATION


```
================================================================================

10:15:16:56    10  A   outgoing       RcvR     3 octets    8       136
           LGN=0   LCN=10   LCI=10    P(R)=4
10 0a 81

Command line:  x25decode
Trace protocol: /dev/x25
Trace date: Tue Apr  7 10:14:54 BST 1998

Timestamp      VC  Snid  Direction   Pkt Type      Size     Mod  PacketId
================================================================================

10:15:16:98    10  A   outgoing       Data   126 octets    8       137
      D=0  LGN=0   LCN=10   LCI=10    P(S)=3    P(R)=4    M=0  Q=0
10 0a 86 56 2e 0d 56 48    48 47 2e 57 41 2f 45 31    * ...V..VHHG.WA/E1 *
42 54 55 4b 2f 49 31 31    47 49 41 2f 50 a0 25 d9    * BTUK/I11GIA/P.%. *
0d 56 47 59 41 0d 55 4e    42 2b 49 41 54 41 3a 31    * .VGYA.UNB+IATA:1 *
2b 31 47 2b 46 53 2b 39    38 30 34 30 37 3a 31 30    * +1G+FS+980407:10 *
31 35 2b 54 32 27 55 4e    48 2b 31 2b 48 53 46 52    * 15+T2'UNH+1+HSFR *
45 51 3a 39 34 3a 31 3a    49 41 27 4f 52 47 2b 46    * EQ:94:1:IA'ORG+F *
53 3a 4c 4f 4e 27 4c 54    53 2b 2a 52 27 55 4e 54    * S:LON'LTS+*R'UNT *
2b 34 2b 31 27 55 4e 5a    2b 31 2b 54 32 27          * +4+1'UNZ+1+T2'   *

================================================================================
```

UPCOMING X.25 0-DAY TRENDS

[DoSsing X.25 international links]

[Mass Scanning]

[CUD Fuzzying]

[Abusing XoT]

DOSsing X.25 INTERNATIONAL LINKS

- International links depend on agreements among countries.
- The # of lines is limited (usually << 1000).
- Some **very-small countries** are routed only by one country (San Marino via Italy/ITAPAC, Andorra via Spain/IBERPAC, ...)
- Pakistan, for example, manages its X.25 intl links with a 64 Kbit/s line (!)
- It might be theoretically possible to flood a whole country (with a **domino effect**).

MASS SCANNING

- **With multithreaded software scanning is really faaaast!**
- Depending on the number of available channels and on the network used to scan (some countries networks are faster than others).
- 32 available physical channels are enough to scan **10.000** x.25 NUAs in less than **3 minutes**.

Solaris example:

bash-2.02# grep "two_range" /etc/opt/SUNWconn/x25/config/link_config_0000.cfg
*two_range 1-**128***

bash-2.02#

XOT

- x.25 over IP (RFC **1613**)
- Because the legacy world **still needs x.25**, as Fabrice Marie explained us yesterday (Robbing Banks: easier done than said)
- For example, many ATM Bank networks (POS) transporting **SNA over X.25**, **have migrated to XoT**.
- This happens because it's really easy to add systems to the network without installing the whole x.25 stack

USING XOT: AN EXAMPLE

⌘ In order to play with XoT, you **don't need to have an X.25 link on your machine**: you can simply configure your own Cisco IOS to (ab)use another (remote) router's XoT facilities.

```
service pad to-xot
x25 routing
x25 route .* xot 196.xxx.xxx.196
```

PRIVATE X.25 NETWORKS VIA XOT

- A **new world** opens to you:
  - Not-routed networks, just local and “private”.
  - Mostly used by finance and telcos.
  - Needed by legacy applications.

```
root@darkstar:~# telnet 154.xx.233.xxx
Trying 154.xx.233.xxx...
Connected to 154.xx.233.xxx.
Escape character is '^]'.
Trying 1234555500...Open

PIN:
```

JUMPING FROM X.25 TO IP


```
bash-2.02# pad 025017722029600
Break-in sequence is '^Pa'

Connecting...
Connected
Trying 195.xxx.xx.xxx, 2001 ...Connect

Login:
```

NOTE: You can shell to the Cisco, with the correct escape sequence.

- See:
  http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080174a34.shtml

ABUSING XOT

- Auth is **not needed** ☺

- Easy to manipulate: (RFC **1613**)
  - **NUA spoofing**
  - **ACL bypassying**
  - **CUD fuzzying** (I will not cover this here, refer to my last HITB 2005 talk)

PRIVATE X.25 NETWORKS VIA XOT

- A lot of companies use PPP over x.25 to carry IP (where there is no Internet).
  - There is no Interactive Login, only PPP.
  - With XoT you can connect to the NUA and start PPPD (just some conversion problem, ie. 7E2 or 7E1 to 8N1).

PRIVATE X.25 NETWORKS VIA XOT


```
bash-2.02# /opt//SUNWconn/x25/bin/pad 025017725200468
Break-in sequence is '^Pa'

Connecting...
Connected
Entering PPP mode.
Virtual-Access2 interface address is unnumbered (Loopback0)
MTU is 1500 bytes
Header compression is on.

~ÿ}#À!}!}!} }8}"}&} }*} } }#}$À#}%}&ò}%uã}'}"}(}"EÄ~~ÿ}#À!}!}"}
}8}"}&} }*} } }#}$À#}%}&ò}%uã}'}"}(}"}/V~~ÿ}#À!}!}#} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"Æß~~ÿ}#À!}!}$} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"z~~ÿ}#À!}!}%} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"Có~~ÿ}#À!}!}&} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"})a~~ÿ}#À!}!}'} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"Àè~~ÿ}#À!}!}(} }8}"}&} }*} }
}#}$À#}%}&ò}%uã}'}"}(}"#~
```

XOT MANIPULATION

- X.25 spoofing
  - Make calls “nearly untraceable”
  - Fool system’s ACLs (not the – “HW” – telco’s ones)

- CUD
  - Used to ask for “application” (PSI MAIL on VAX/VMS & AXP/OpenVMS, “/bin/login” process on Sun Solaris, etc...)

X.25 EXPLOITING

- Really hard to perform
- Only a few, and not-standard services
- But it is **STILL POSSIBLE**... ☺
- Actually, we've developped the porting of the **Solaris remote telnet exploit** to X.25 environments and... **you know what ??**
- **It works** :)

X.25 EXPLOITING

- Looking for services and applications
  - (ALWAYS) **check for subaddresses**
  - Check **for CUD**
  - Es. Sunlink smnpx25d (http://www.securityfocus.com/bid/8882)
  - E.g.: customized applications.
  - Solaris login “telnet” exploit: http://wayreth.eu.org/padxploit.c

END

[Getting Help: take care]

[Conclusions]

[Bibliography]

[Greetings]

[Contacts]

TAKE CARE WHEN ASKING FOR HELP

- **Traditional security shops**: zero knowledge of X.25 security problems, telcos, poor understanding of global WANs logicals & procedures.
- **Traditional telcos consultants**: very poor knowledge of security issues.
- **X.25 carriers**: they'll try to sell you IP connections instead of fixing your X.25 and Frame Relay links security holes, and they'll suggest you to migrate everything you have onto the IP world.
- Customers' **loved and trusted security consultant**: in this case he probably doesn't even know what you are talking about.
- The **"Big 5" audit firms**: focused on policies, no real expertise (they outsource their jobs to companies like us).

CONCLUSIONS

Doing Nothing...

- ... with your PSDN infrastructure today is like doing nothing with your Internet hosts in the 90's: how many hackers played with your datas ? ☹
- ...in critical environments, this is an invitation for disaster.
- What can you do against this ?
- Ask for **professional** **X.25 Security Audits** and **Penetration Tests**

BIBLIOGRAPHY

Online material

- **I network X.25:Comprensione della struttura di rete, Tecniche di intrusione ed Identificazione degli attacchi**, by Raoul "Nobody" Chiesa and Marco "Raptor" Ivaldi, Italian Black Hats Technical Paper #1 (Italian only, 95 pages). http://www.blakhats.it/papers/x25.pdf/
- **Libnet-X.25**: The Preamble
- **Protocol Vulnerabilities within the X.25 Networking suite**.
- X.25 Standards and ITU Recommendations (http://www.itu.int/)
- X25zine (http://www.x25zine.org/)
- **X25 Trace: X.25 network tracing for Internet users**, by Dennis Jackson, JANET-CERT Coordinator, U.K.
- **A novice Guide to X.25 Hacking**, by Anonymous
- **Desktop Guide to X.25 Hacking in Australia**, by Epic Target
- **Accessing Telecom Australia's AUSTPAC service** - By Softbeard
- **The Force Files** - By The Force
- **Austpac.notes** - by Vorper VII
- **Globetrotter Ezine** - By The Force
- **Alt.2600 Hack** (90's posts) - By Simple Nomad

Literature

- **Underground** - By Suelette Dreyfuss (Australia)
- **The Cuckoo's Egg**, Clifford Stoll, Pocket Books, 1989 (USA)
- **Cyberpunks: Outlaws and hackers on the Computer Frontier**, Katie Hafner & John Markoff, Touchstone Books 1991 USA
- **Out Of The Inner Circle** - By Bill Landreth, McGraw Hill Internetworking Handbook
- **An Introduction To Packet Switched Networks Parts I and II**, Telecom Security Bulletin File by Blade Runner

BIBLIOGRAPHY

⌘ RFCs

- RFC 874 - A Critique Of X.25
- RFC 877 - Standard For Transmission Of IP Datagrams Over Public Data Networks
- RFC 1356 - Multiprotocol Interconnect On X.25 And ISDN In The Packet Mode
- RFC 1090 - SMTP On X.25
- RFC 1381 - SNMP MIB Extension For X.25 LAPB
- RFC 1382 - SNMP MIB Extension For The X.25 Packet Layer
- RFC 1461 - SNMP MIB Extensions For Multiprotocol Interconnect Over X.25

⌘ Tutorials

- RIM Remote System - Neurocactus Ezine
- Hacking UNIX Tutorial - By Sir Hackalot
- Advanced Hacking VAX's VMS - By Lex Luthor
- Guide to Gandalf XMUXs - By Deicide
- B4B0 Ezine #7 : Hacking The Shiva LAN-Rover - By Hybrid
- The Complete Hewlett Packard 3000 Hacker's Guide - By AXIS
- **X.25 And LAPB Commands For Cisco Routers**
- A Novice's Guide To Hacking - By The Mentor
- The Beginner's Guide To Hacking On Datapac - By The Lost Avenger and UPI
- **NEOPHYTE'S GUIDE TO HACKING** (1993 Edition) - By Deicide

GREETINGS

/X.25 gurus/

- **Machine**
- **Pengo**
- **Raist**
- **Freehunt from x25zine.org**
- **Emmanuel Gadaix from TSTF**
- **Vanja**
- **Raptor**
- **The Force (and the aussie scene)**

/Friends/

- **Venix**
- **Philippe Langlois from TSTF**
- **D0**
- **FX from Phenoelit**
- **Dialtone**
- **rpunk and people at #x.25 (efnet)**
- **Fyodor Yarochkin from TSTF**
- **Jim Geovedi from BellUA**
- **Anthony Zboralski from BellUa**
- **Fabrice Marie**
- **Dhillon Kannabhiran from HITB**
- **Sarah, just 'cause she's smart (and SO cute ;)**

/Telcos/

...just for being there :)

...And all of the Hack in the Box folks for this great event!

CONTACTS, Q&A

THANKS for your attention !

QUESTIONS ?

Raoul "Nobody" Chiesa

TELECOM SECURITY TASK FORCE, ISECOM

rc@TSTF.net
raoul@ISECOM.org