A.L.R.Pennasilico

Penetration Test

28 Maggio 2007

Strumenti per il security assessment

Fiorenzo Ottorini
f.ottorini@attua.it

Alessio L.R. Pennasilico
mayhem@alba.st

Fiorenzo Ottorini

CEO @

http://www.alba.st/
mayhem@alba.st

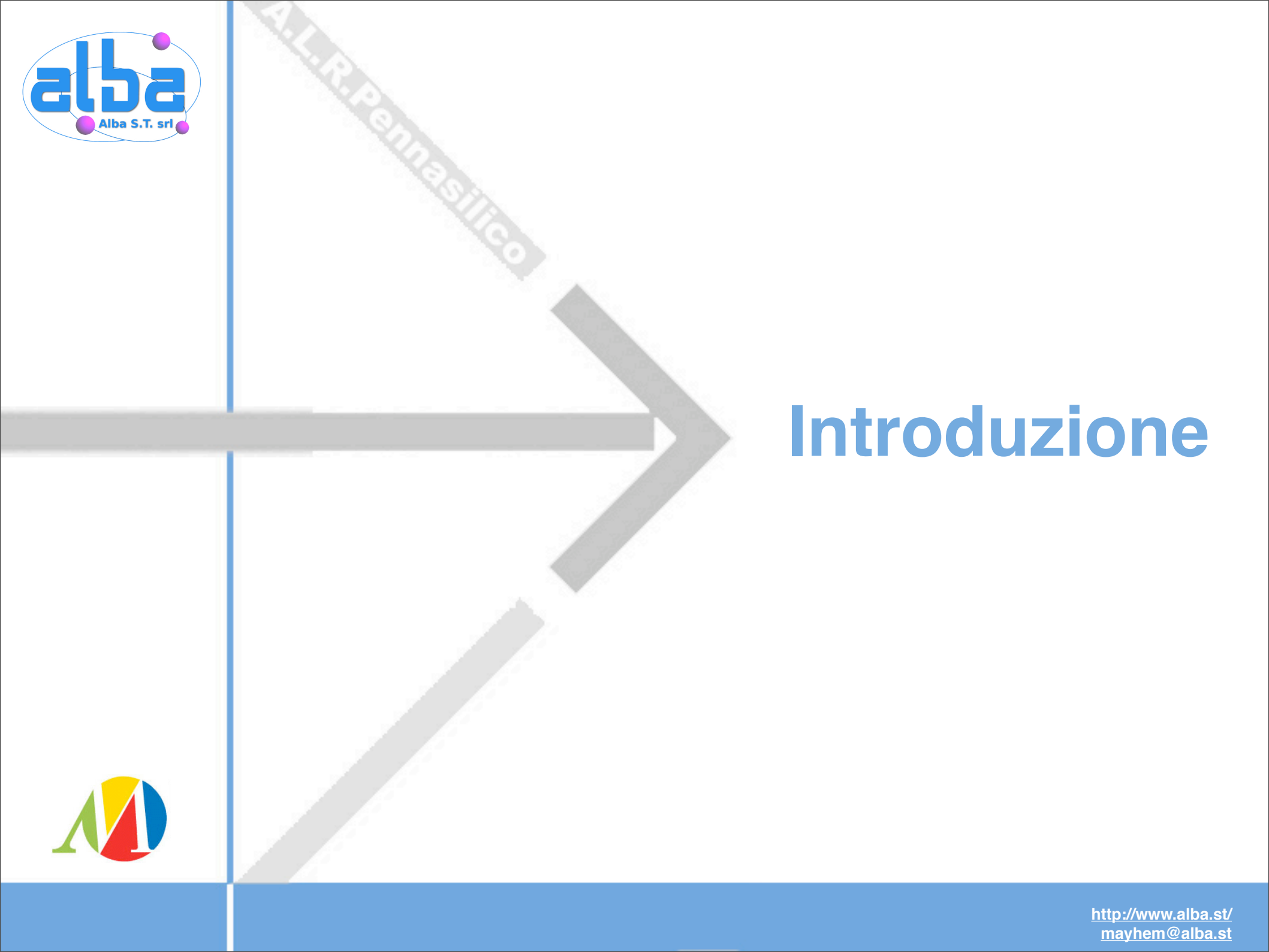
$ whois mayhem

Security Evangelist @ 

Member / Board of Directors:

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

http://www.alba.st/
mayhem@alba.st



Introduzione

Finalità

Conoscere gli strumenti disponibili e le loro funzionalità

Capire come interpretare i dati e correlarli

Ottenere una visione d'insieme della rete da verificare

Ringraziamenti

Queste slides sono nate quasi per caso, durante un pranzo a webbit, grazie ad alcuni cari amici, impegnati da anni nella diffusione della cultura informatica. Grazie a

fusys@s0ftpj.org

naif@s0ftpj.org

zen@kill-9.it

con i quali è nata l'idea di presentare questi strumenti in questo modo ed in questo ordine.

Disclaimer

Lo scopo di questo workshop è fornire agli amministratori di rete strumenti e metodi utili per rendere più sicura le loro rete.

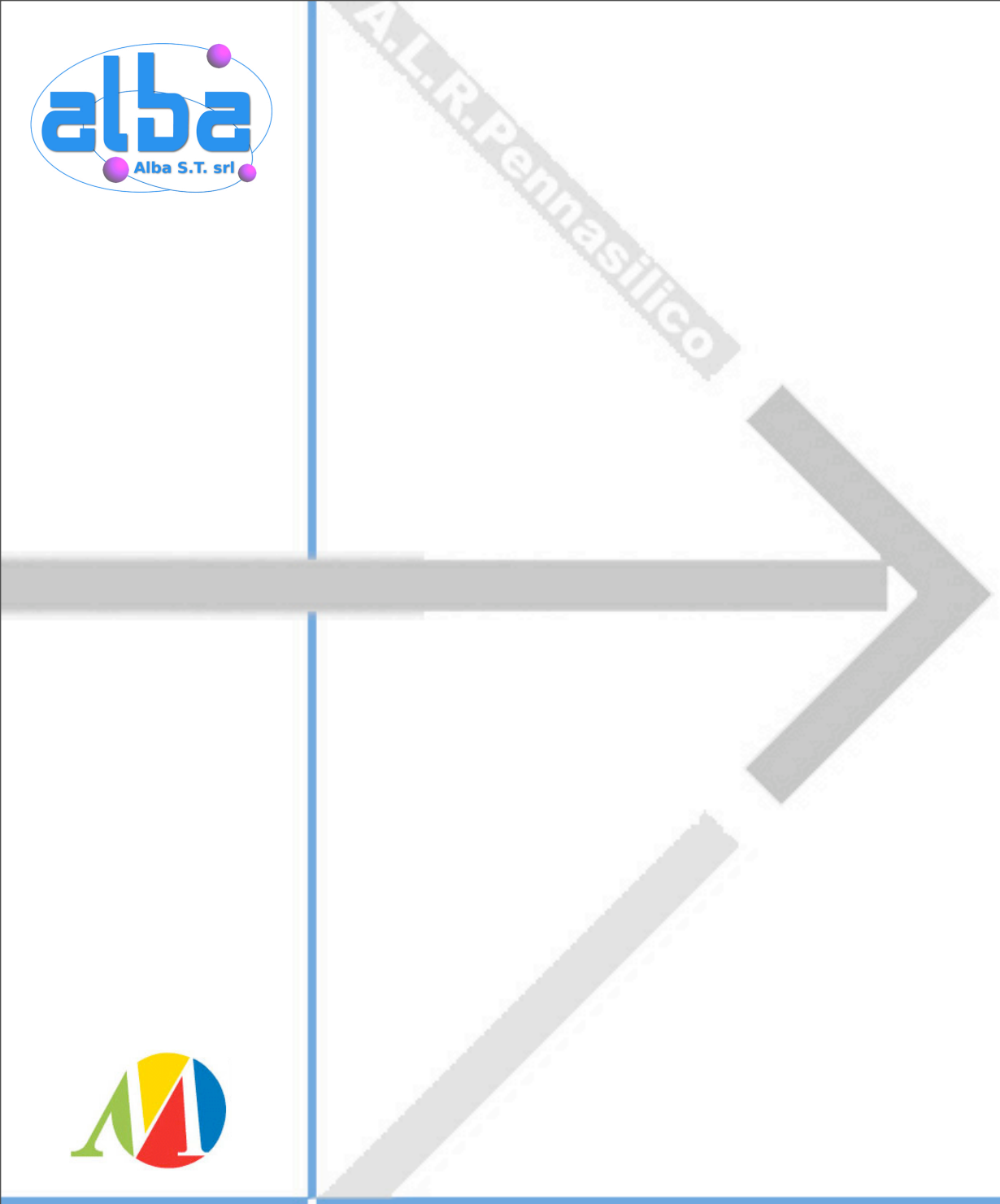
Si declina ogni responsabilità per danni causati da questi strumenti o dal loro utilizzo per scopi illeciti.

Vulnerability Assessment

Il primo passo di un pen-test è creare una mappa degli host e dei device che compongono la rete, dei servizi pubblicati e delle loro possibili debolezze; viene definito Vulnerability Assessment.

Penetration Test

A partire dai dati raccolti durante il vulnerability assessment, attraverso ulteriori test, molto più complessi ed invasivi, dovremo scoprire le reali debolezze della rete in esame.



DLGS 196/03

http://www.alba.st/
mayhem@alba.st

Legge sulla privacy

Esiste in Italia una norma che regola il come vanno gestiti i dati che si possiedono su altre “entità”.

Indicazioni

La norma prevede l'adozione di alcuni accorgimenti organizzativi e di alcuni accorgimenti tecnici.

Aspetti organizzativi

Redigere un documento, DPS, che individui che dati vengono trattati, da chi, in che modo.

http://www.alba.st/
mayhem@alba.st

Allegato tecnico

Cambio password

Backup dei dati

Aggiornamenti software

Antivirus aggiornato

Verifica del firewall

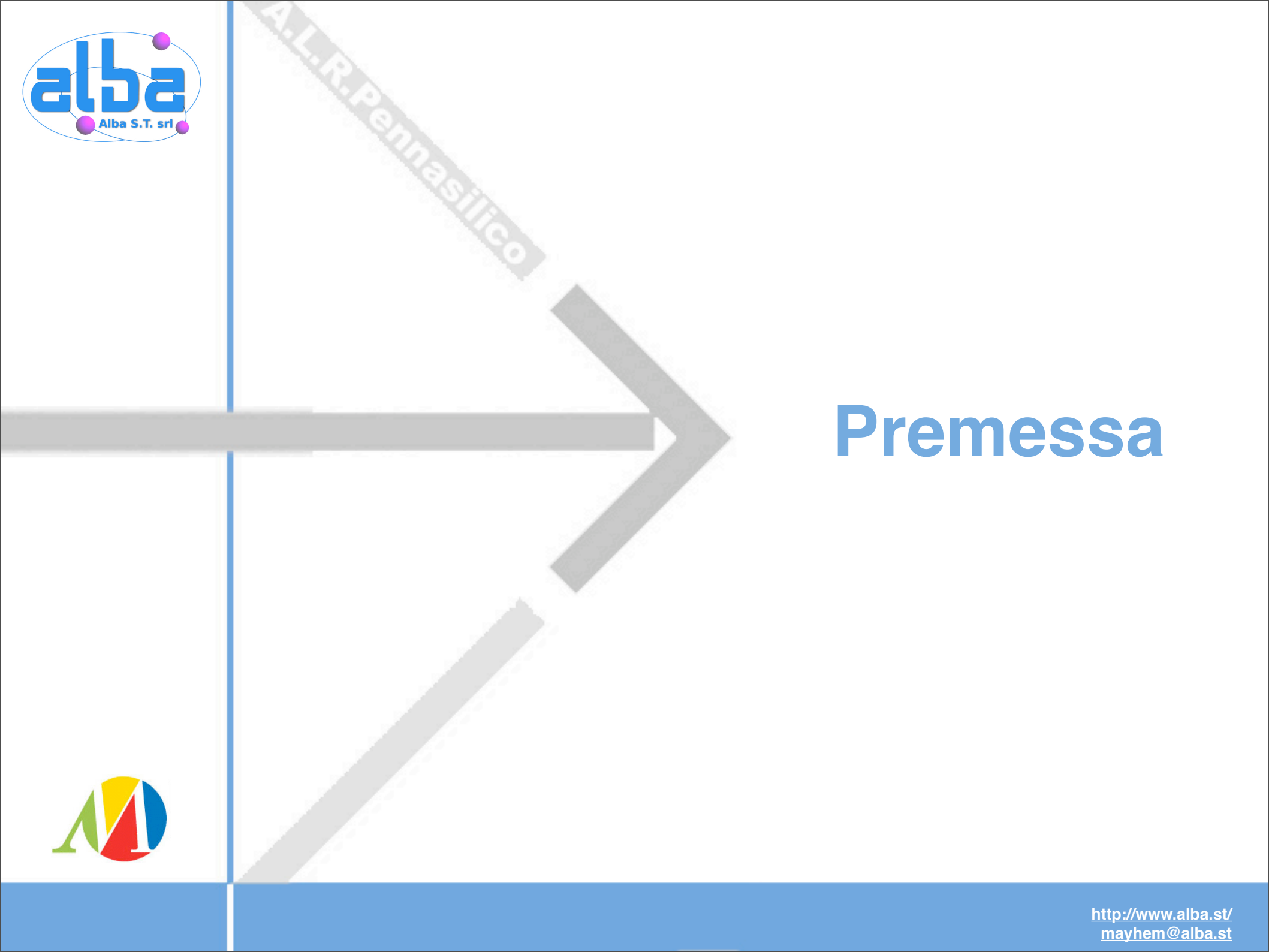
Verifiche periodiche

Grande attenzione viene posta nel tenere aggiornati e coerenti gli strumenti utilizzati.

http://www.alba.st/
mayhem@alba.st

Gestione dei processi

Tutto questo perché la sicurezza è un processo, non un prodotto.



Premessa

Premessa

Partiamo da alcuni concetti di base necessari a comprendere il funzionamento degli strumenti che poi andremo ad illustrare.

Porte Server

Un singolo host può offrire più servizi. Ogni servizio si rende disponibile su una porta “server”: una porta identificata da un numero ben preciso (es. Http=80).

Storicamente i servizi stanno in ascolto sulle porte inferiori a 1024, chiamate well-known-ports.

Porte Client

Un client invece può stabilire più comunicazioni contemporanee verso diversi servizi su diversi server.

Per questo il client, per accedere ai servizi, utilizza una porta diversa per ogni connessione, scelta “casualmente” tra 1024 e 65535.

Pila ISO/OSI

7	**Application**	Telnet, HTTP, SMTP
6	**Presentation**	JPEG, ASCII, EBCDIC
5	**Session**	RPC, Netbios, NFS
4	**Transport**	TCP,UDP, SPX
3	**Network**	TCP/IP, IPX/SPX
2	**Data-Link**	IEEE 802.2/802.3
1	**Physical**	RJ-45, V-35, FDDI

http://www.alba.st/
mayhem@alba.st

TCP & UDP

Layer 3: IP - Layer 4: TCP,UDP,ICMP

TCP è orientato alla connessione, è “affidabile”.

UDP è connectionless, più leggero ma meno “affidabile”.

ICMP gestisce “errori” e test.

Servizi

I servizi che noi andremo a studiare sono il layer più alto della pila, il settimo.

Applicazioni come http, ftp, server sql o ssh si posizionano a questo livello.

TCP Flags

SYN = serve a stabilire una connessione

ACK = conferma la corretta ricezione

FIN = termina la connessione

URG = marca il pacchetto come urgente

PUSH = chiede ancora dati

RST = chiude la connessione

Three way handshake

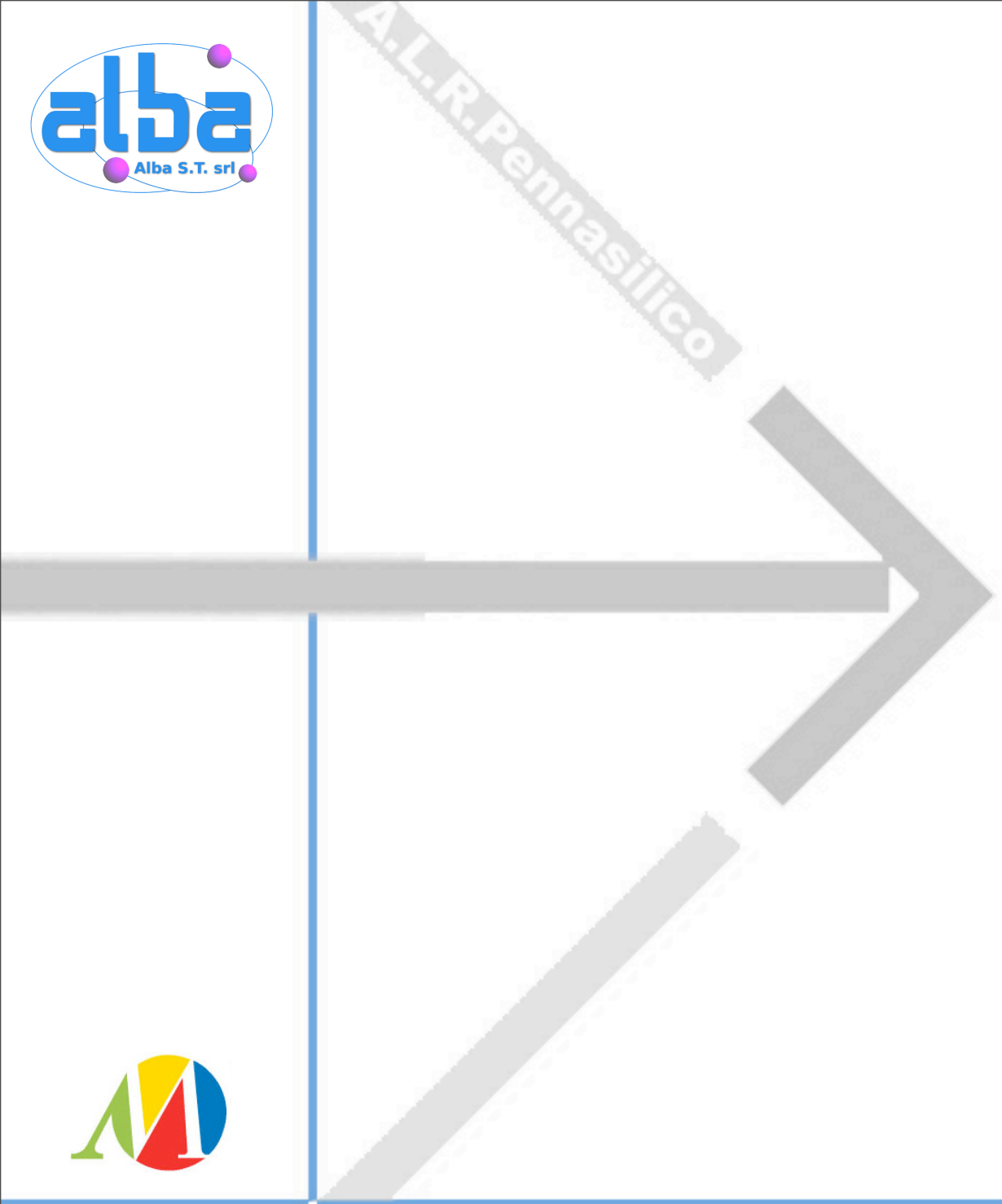
Vale solo per le connessioni TCP

Client – SYN=1 -> Server

Client <- SYN=1,ACK=1 – Server

Client – ACK=1 -> Server

Abbiamo stabilito la connessione, non abbiamo ancora scambiato nessun “dato”



Information Gathering

Prime Informazioni

La nostra prima necessità e conoscere quali servizi sono attivi sulla macchina che vogliamo testare.

whois

whois interroga dei server su Internet al fine di ottenere informazioni sulle persone fisiche e sull'ISP che gestisce una certa classe di indirizzi o un certo dominio.

$ whois recursiva.org

Domain ID:D104300355-LROR

Domain Name:RECURSIVA.ORG

Created On:03-May-2004 18:16:04 UTC

Last Updated On:03-Jul-2004 03:55:15 UTC

Expiration Date:03-May-2005 18:16:04 UTC

Sponsoring Registrar:R120-LROR

Status:OK

Registrant ID:GODA-06456516

$ whois recursiva.org

Registrant Name:Alessio Pennasilico

Registrant Street1:Via Labriola, 16

Registrant City:Villafranca

Registrant State/Province:Verona

Registrant Postal Code:37069

Registrant Country:IT

Registrant Phone:+39.348xxxxxxx

Registrant Email:mayhem@spippolatori.org

dig

Interrogare i server DNS per ottenere informazioni circa la presenza e la dislocazione dei server e dei servizi di una rete è spesso un buon punto di partenza.

$ dig mx recursiva.org

```
; <<>> DiG 9.2.3 <<>> mx recursiva.org

;; QUESTION SECTION:
;recursiva.org.                 IN      MX

;; ANSWER SECTION:
recursiva.org.          86400   IN      MX   10 mail.recursiva.org.

;; ADDITIONAL SECTION:
mail.recursiva.org.     86400   IN      A    217.133.6.188
```

traceroute

Conoscere quale strada compiono i nostri pacchetti, per raggiungere i diversi host della rete che stiamo analizzando, ci permette di avere ulteriori informazioni sulla topologia della rete.

traceroute www.recursiva.org

traceroute to www.recursiva.org (217.133.6.188), 64 hops max, 40 byte packets

```
 3  host25-114.pool8018.interbusiness.it (80.18.114.25)  9.126 ms  7.580 ms  8.16 ms
 4  r-pd48-pd70.opb.interbusiness.it (151.99.101.229)  9.904 ms  7.812 ms  7.865 ms
 5  r-mi258-pd48.opb.interbusiness.it (151.99.101.97)  12.654 ms  10.468 ms  10.337 ms
 6  151.99.75.226 (151.99.75.226)  13.294 ms  14.258 ms  13.195 ms
 7  gw-mix-mi257-a.opb.interbusiness.it (151.99.98.142)  11.512 ms  12.374 ms  10.821 ms
 8  ge-4-0-0.mil10.ip.tiscali.net (213.200.68.165)  12.740 ms  12.82 ms  12.227 ms
 9  pos-2-0.cag20.ip.tiscali.net (213.200.82.49)  27.943 ms  27.780 ms  29.493 ms
10  213.205.4.116 (213.205.4.116)  29.682 ms  27.40 ms  27.248 ms
11  * * *
```

tcptraceroute

traceroute utilizza pacchetti di tipo UDP o ICMP ECHO.

Questi pacchetti potrebbero essere filtrati.

tcptraceroute è uno strumento analogo, ma che lavora con pacchetti di tipo TCP.

tcptraceroute www.recursiva.org

root@coniglio ~ # tcptraceroute www.recursiva.org 80

Selected device eth0, address 10.0.0.137 for outgoing packets

Tracing the path to www.recursiva.org (217.133.6.188) on TCP port 80

[...]

8 ge-3-0-0.mil10.ip.tiscali.net (213.200.68.161) 56.870 ms 57.669

9 pos-2-0.cag20.ip.tiscali.net (213.200.82.49) 74.900 ms 73.260 ms

10 213.205.4.116 (213.205.4.116) 72.567 ms 72.911 ms 74.482 ms

11 www.recursiva.org (217.133.6.188) [closed] 145.409 ms 145.211

hping

hping2 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. Hping2 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping2 you are able to perform at least the following stuff:

- Test firewall rules
- Advanced port scanning
- Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
- Path MTU discovery
- Traceroute-like under different protocols.
- Firewalk-like usage.
- Remote OS fingerprinting.
- TCP/IP stack auditing.
- A lot of others.

nmap

Nmap è un port-scanner che ci permette di analizzare una rete per sapere quali host sono attivi e quali servizi pubblicano.

nmap -h

* -sS TCP SYN stealth port scan (default if privileged (root))

  -sT TCP connect() port scan (default for unprivileged users)

* -sU UDP port scan

  -sP ping scan (Find any reachable machines)

* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)

  -sV Version scan probes open ports determining service & app names/ versions

Some Common Options (none are required, most can be combined):

* -O Use TCP/IP fingerprinting to guess remote operating system

  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'

  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)

  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy

* -S <your_IP>/-e <devicename> Specify source address or network interface

Perchè diverse tecniche?

- ✓ tentare di non essere rilevati da un eventuale IDS
- ✓ tentare di “imbrogliare” un eventuale firewall
- ✓ tentare di sfruttare cattive implementazioni dello stack TCP/IP o del servizio per ottenere maggiori informazioni

nmap -sP

Ping Scan

Verifica quali host sono raggiungibili tramite un ping

(icmp echo request)

Questo strumento è disponibile al semplice utente.

nmap -sT

Esegue un 3way handshake completo per ogni porta da verificare.

E' il metodo di default dell'utente senza privilegi di root, poiché utilizza la connect() di sistema.

nmap -sS

SYN scan

Invia solamente il primo pacchetto con SYN=1, senza mai spedire il pacchetto con SYN=1 ed ACK=1.

E' necessario possedere i privilegi amministrativi per utilizzarlo.

nmap -sF

FIN scan

E' necessario possedere i privilegi di root per utilizzarlo.

Invia un pacchetto anomalo, con FIN=1, e resta in attesa di una risposta.

nmap -sN & -sX

E' necessario possedere i privilegi di root per poterli utilizzare. Entrambi generano pacchetti “inesistenti”.

Null scan invia un pacchetto con tutte le flag impostate a 0.

Xmas tree scan invia un pacchetto con le flag FIN, URG e PUSH impostate ad 1.

nmap -sU

UDP scan

La natura di UDP rende il risultato di questa verifica estremamente incerto.

E' necessario possedere i privilegi di root per utilizzarlo.

-P0 & -O

-P0 esegue la verifica anche per gli host che non rispondono al ping

-O genera una serie di pacchetti che hanno lo scopo di determinare il sistema operativo dell'host che stiamo verificando.

Nmap -sV

L'opzione di Service Scan serve a determinare la natura del servizio in ascolto, nel qual caso sia di tipo “binario”.

E' una ottima alternativa ad amap.

Output di nmap

```
root@coniglio:~# nmap -sS -n -O 127.0.0.1

PORT     STATE SERVICE

25/tcp   open  smtp

631/tcp  open  ipp

1241/tcp open  nessus

3306/tcp open  mysql

Running: Linux 2.4.XI2.5.X

OS details: Linux 2.5.25 - 2.5.70 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)

Uptime 0.057 days (since Sat Jun 26 10:03:54 2004)
```

Tipo di servizi

Dopo avere scoperto quali porte sono aperte vogliamo determinare quali servizi rispondono su quelle porte, quale versione del servizio viene utilizzata e quali funzionalità sono disponibili.

Banner “in testo”

Collegandoci alla porta 25/TCP scopriamo quale programma, in quale versione, è in ascolto su quella porta:

```
mayhem@coniglio:~$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 coniglio.recursiva.org ESMTP Postfix (2.1.1)
```

Banner Modificati

E' tuttavia possibile modificare il banner per diffondere meno informazioni:

```
mayhem@coniglio:~$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 eat.koalas.org ESMTP mayhem loves blowfish
helo spippolatori.org
250 coniglio.recursiva.org
```

Richiesta Informazioni

```
mayhem@coniglio:~$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
help
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
<p>help to /index.html.en not supported.<br />
</p>
<hr />
<address>Apache/2.0.49 (Gentoo/Linux) mod_ssl/2.0.49 OpenSSL/0.9.7d PHP/4.3.7
</body></html>
Connection closed by foreign host.
```

Servizio “binario”

Collegandoci alla porta 3306 invece non ricaviamo alcuna informazione utile circa il servizio che la tiene aperta:

```
mayhem@coniglio:~$ telnet 127.0.0.1 3306
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
'

4.0.200HYg{Uul,
Connection closed by foreign host.
```

netcat

netcat è un'ottima alternativa a telnet, grazie alle sue molte opzioni.

In questo contesto ci interessa notare che permette di connettersi a porte UDP ed a servizi che utilizzano encryption.

nc -h

```
[v1.10] connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -A algorithm           cast256, mars, saferp, twofish, or rijndael
        -k password             AES encrypt and ascii armor session
        -g gateway             source-routing hop point[s], up to 8
        -G num                source-routing pointer: 4, 8, 12, ...
        -l                   listen mode, for inbound connects
        -o file               hex dump of traffic
        -p port                local port number
        -s addr                local source address
        -u                   UDP mode
```

nmap lavora per noi

root@coniglio:~# nmap -sV -n -O 127.0.0.1

PORT STATE SERVICE VERSION

25/tcp open smtp Postfix smtpd

631/tcp open ipp CUPS 1.1

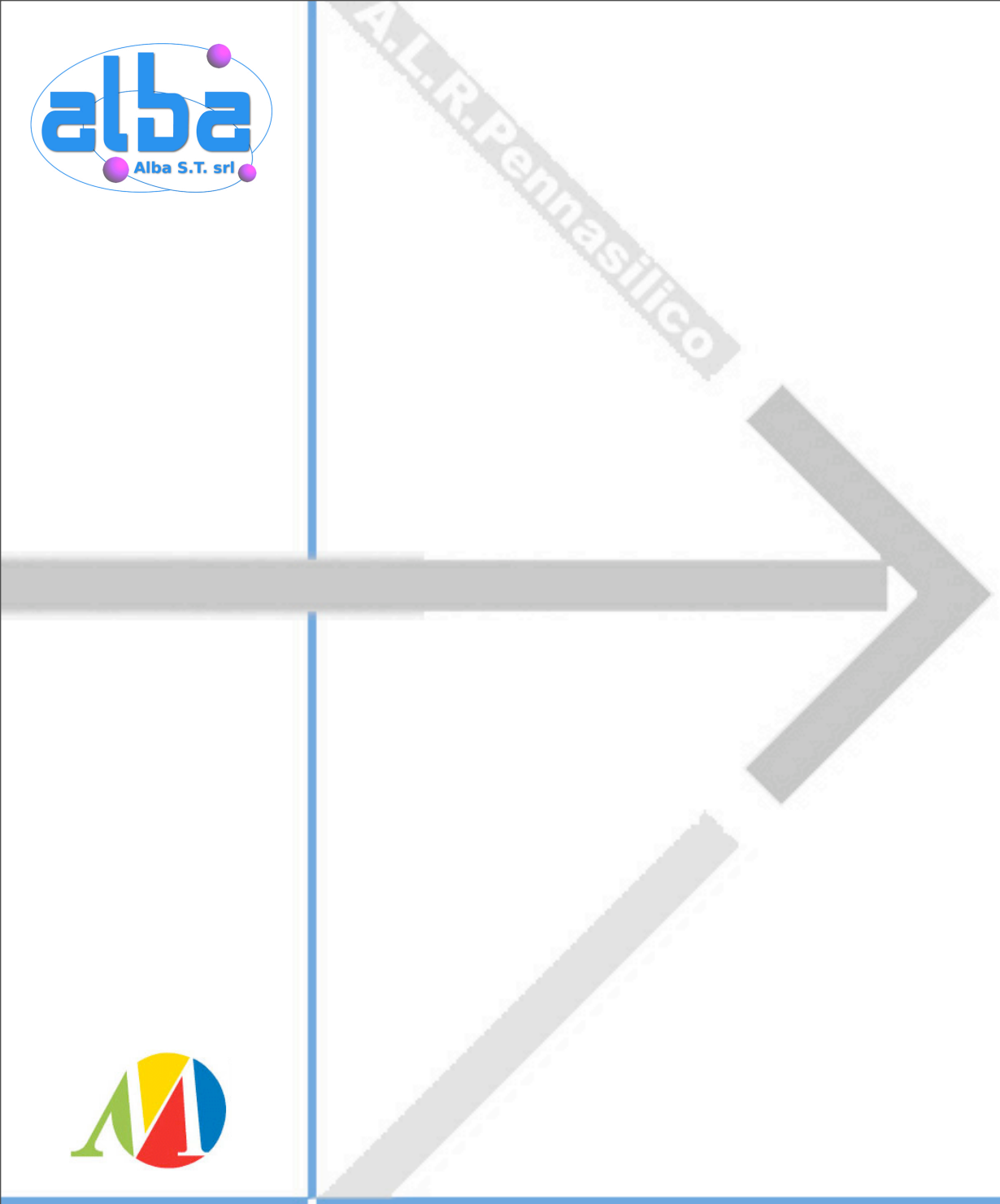
1241/tcp open nessus?

3306/tcp open mysql MySQL 4.0.20

Running: Linux 2.4.XI2.5.X

OS details: Linux 2.5.25 - 2.5.70 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)

Uptime 0.060 days (since Sat Jun 26 10:03:54 2004)



Vulnerabilità

Ricerca Vulnerabilità

Ora dovremmo cercare delle informazioni relative ad eventuali bug o misconfiguration dei servizi trovati.

Fortunatamente la maggior parte del lavoro, rispetto a servizi standard, può essere affidata ad appositi programmi.

nikto

nikto verifica la configurazione di un webserver, testa i bug noti e ci fornisce un report abbastanza dettagliato, un ottimo punto di partenza per ottenere importanti informazioni attraverso una procedura automatica.

nikto -h (1)

```
-Cgidirs      Scan these CGI dirs: 'none', 'all', or a value like '/cgi/'
-evasion+     ids evasion technique (1-9, see below)
-generic      force full (generic) scan
-host+        target host
-id+          host authentication to use, format is userid:password
-mutate+      mutate checks (see below)
-output+      write output to this file
-port+        port to use (default 80)
-root+        prepend root value to all requests, format is /directory
-ssl          force ssl mode on port
-useproxy     use the proxy defined in config.txt
```

nikto output

```
mayhem@coniglio:~$ nikto -host 127.0.0.1 -evasion 2 -mutate 1
---------------------------------------------------------------------------
- Nikto 1.32/1.19     -     www.cirt.net
+ Target IP:       127.0.0.1
+ Target Hostname: coniglio.recursiva.org
+ Target Port:     80
+ Using IDS Evasion:    Directory self-reference (/./)
+ Start Time:      Sat Jun 26 12:35:01 2004
---------------------------------------------------------------------------
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Apache/2.0.49 (Gentoo/Linux) mod_ssl/2.0.49 OpenSSL/0.9.7d PHP/4.3.7
+ IIS may reveal its internal IP in the Content-Location header. The value is
"index.html.en". CAN-2000-0649.
+ Allowed HTTP Methods: GET,HEAD,POST,OPTIONS,TRACE
+ HTTP method 'TRACE' is typically only used for debugging. It should be disabled.
+ mod_ssl/2.0.49 appears to be outdated (current is at least 2.8.15) (may depend on
server version)
+ mod_ssl/2.0.49 OpenSSL/0.9.7d PHP/4.3.7 - mod_ssl 2.8.7 and lower are vulnerable to
a remote buffer overflow which may allow a remote shell (difficult to exploit).
CAN-2002-0082.
+ /~root - Enumeration of users is possible by requesting ~username (responds with
Forbidden for real users, not found for non-existent users) (GET).
```

hydra

Lo scopo di hydra è trovare un account, username e password, valido per un particolare servizio, procedendo per tentativi (dictionary based).

hydra

Hydra v4.1 [http://www.thc.org] (c) 2004 by van Hauser / THC <vh@thc.org>

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns]
[-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV]
server service [OPT]

Options:
-R restore a previous aborted/crashed session
-S connect via SSL
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-e ns additional checks, "n" for null password, "s" try login as pass
-C FILE colon seperated "login:pass" format, instead of -L/-P options
-M FILE server list for parallel attacks, -T TASKS sets max tasks per host
-f exit after the first found login/password pair (per host if -M)
-t TASKS run TASKS number of connects in parallel (default: 16)
-w TIME defines the max wait time in seconds for responses (default: 30)
server the target server (use either this OR the -M option)
service the service to crack. Supported protocols: [**telnet ftp pop3 imap smb smbnt http https http-proxy cisco cisco-enable ldap mssql mysql nntp vnc rexec socks5 icq pcnfs sapr3 ssh2**]

hydra output

```
mayhem@coniglio:~$ hydra -L uid.txt -P pwd.txt /
        127.0.0.1 ftp -f

Hydra v4.1 (c) 2004 by van Hauser / THC
use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2004-06-26 13:21:37
[DATA] 16 tasks, 1 servers, 132 login tries (l:12/p:11), ~8 tries per task
[DATA] attacking service ftp on port 21
[21][ftp] host: 127.0.0.1   login: luser   password: pippo
[STATUS] attack finished for 127.0.0.1 (valid pair found)
Hydra (http://www.thc.org) finished at 2004-06-26 13:21:44
```

nessus

Nessus è un network security scanner.

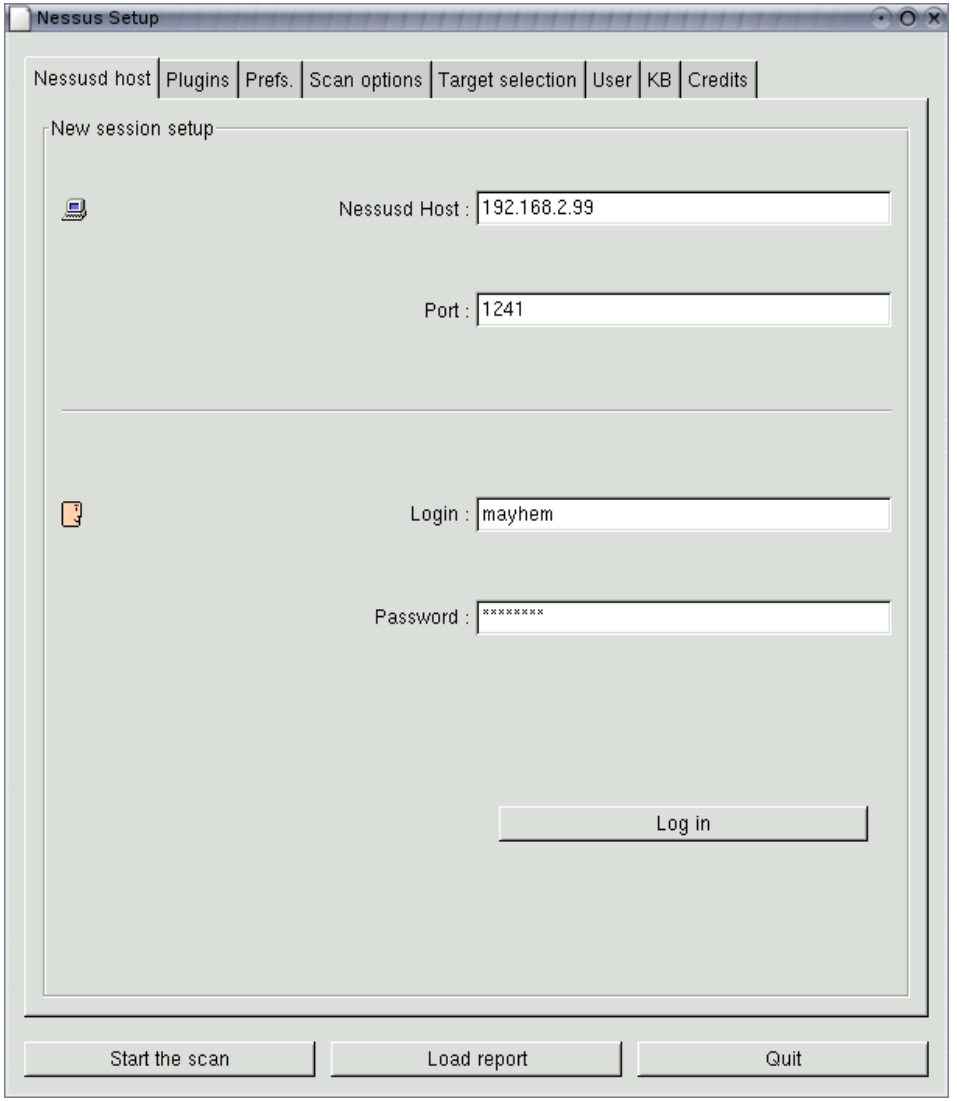
Lavora in modalità client/server e supporta la multiutenza.

Integra un proprio database di vulnerabilità e le potenzialità degli strumenti visti precedentemente.

Nessus - Autenticarsi

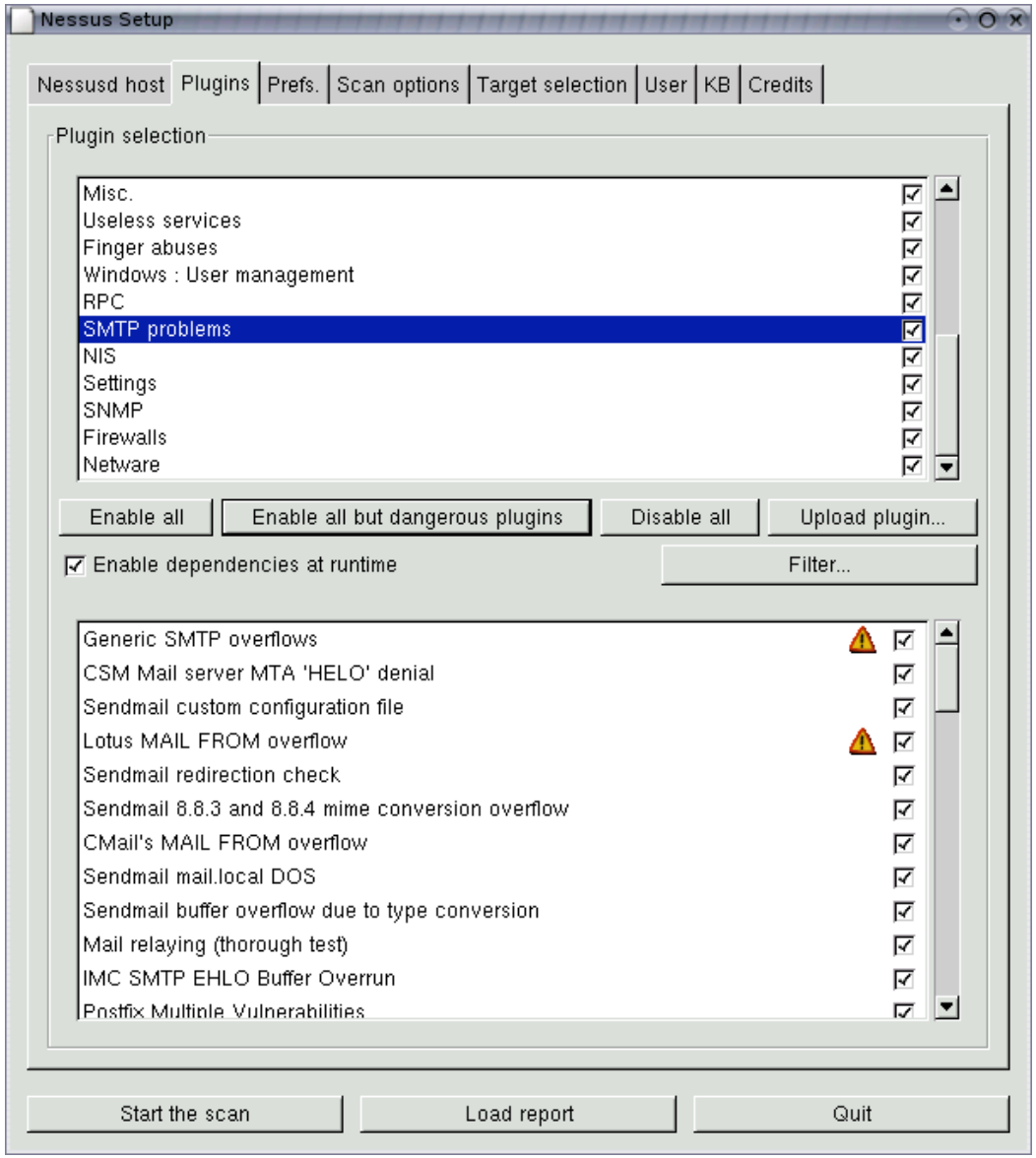
E' necessario autenticarsi per poter utilizzare il servizio

A diversi utenti possono corrispondere diverse autorizzazioni



Nessus - Test

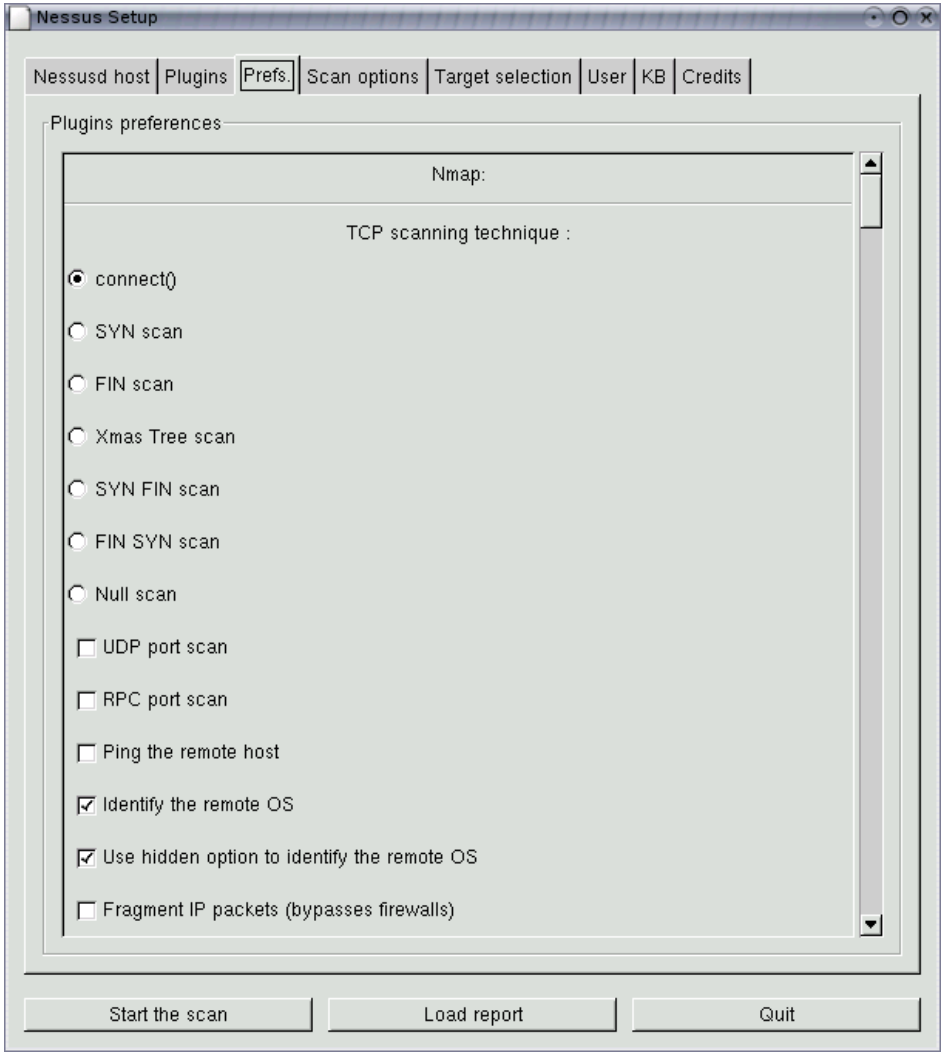
E' ora necessario specificare quali tipi di test desideriamo vengano effettuati.



http://www.alba.st/
mayhem@alba.st

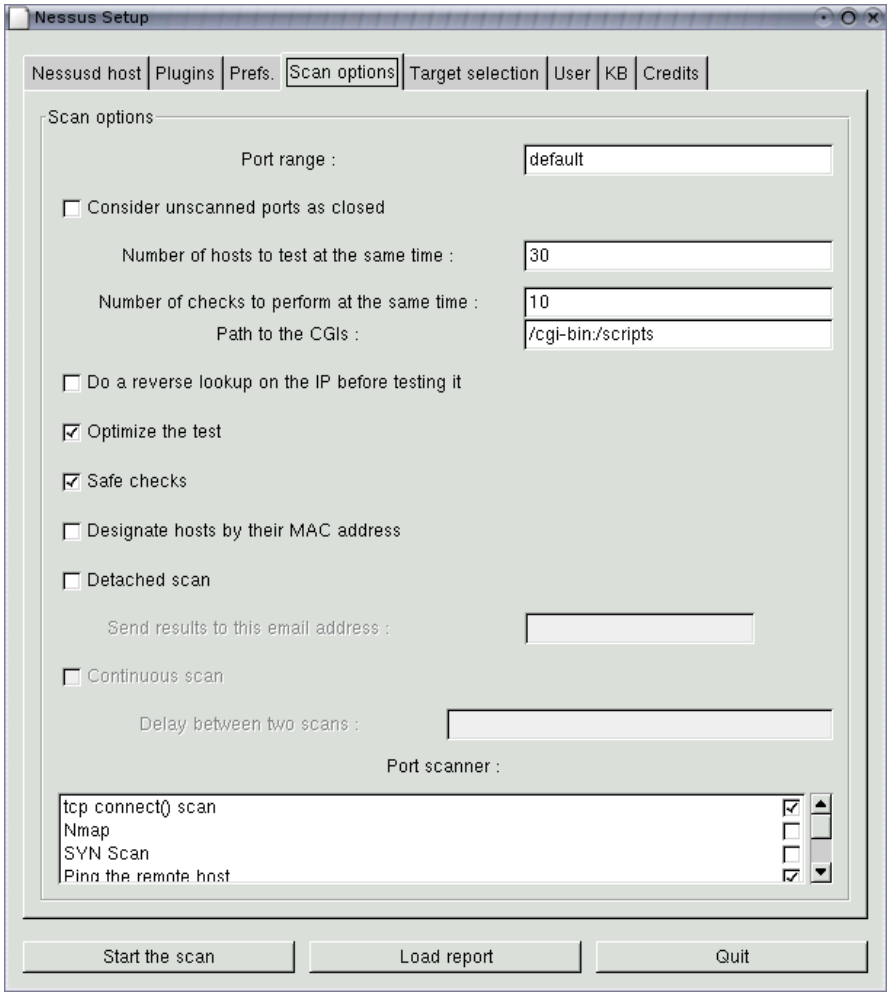
Nessus - Preferences

Possiamo selezionare in questa schermata le diverse opzioni per programmi esterni a cui nessus si può appoggiare.



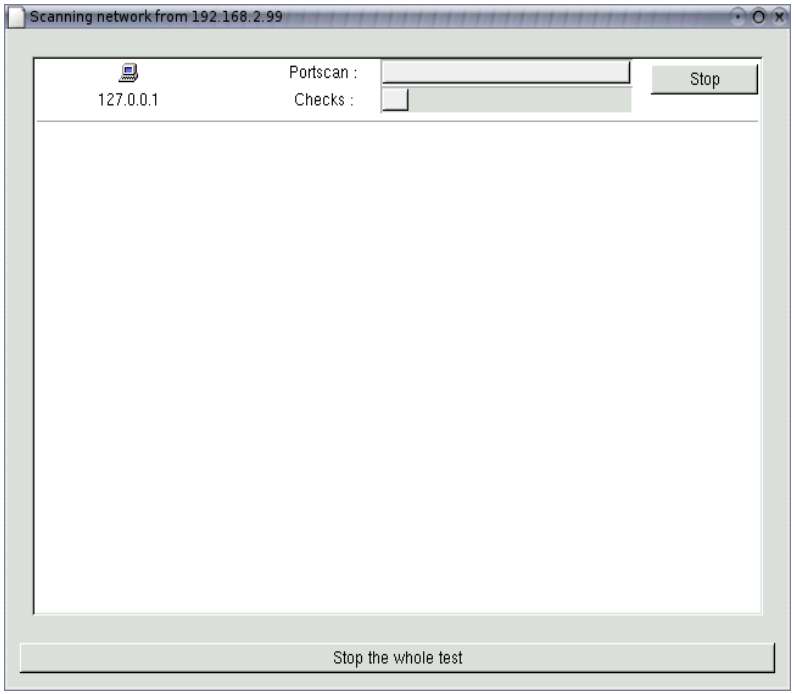
Nessus - Options

L'ultima operazione necessaria è la scelta delle opzioni e del target del security-scan.



Nessus - scanning

Non ci resta a questo punto che gustare un'ottima birra ed una sigaretta nello spazio a noi (fumatori) riservato.



Nessus - Report

Vulnerability found on port www (80/tcp)

The remote host is using a version of mod_ssl which is older than 2.8.18.

This version is vulnerable to a flaw which may allow an attacker to disable the remote web site remotely, or to execute arbitrary code on the remote host.

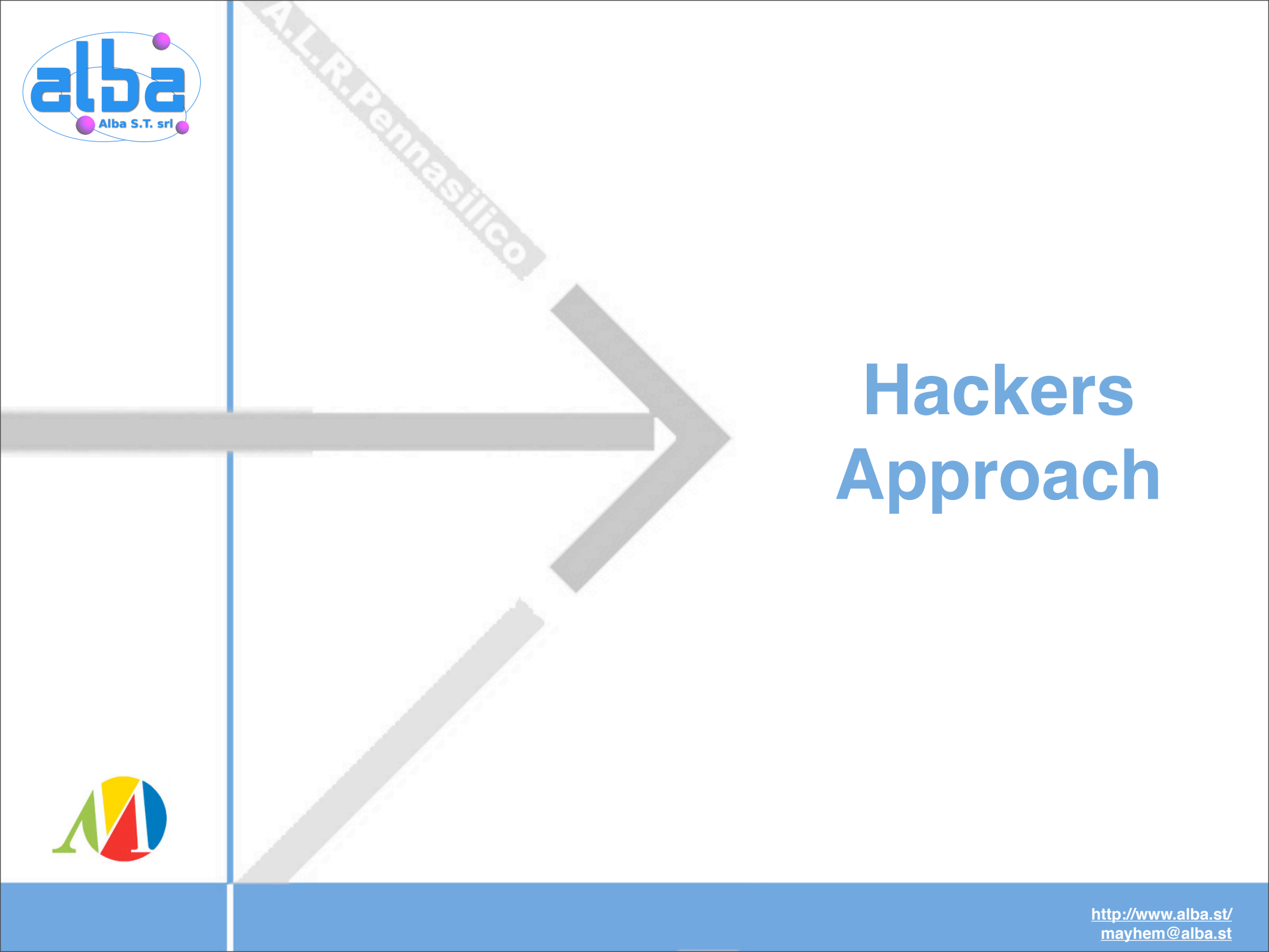
*** Note that several Linux distributions patched the old version of
*** this module. Therefore, this alert might be a false positive.
*** Please check with your vendor to determine if you really are
*** vulnerable to this flaw

Solution : Upgrade to version 2.8.18 or newer
Risk factor : Low
CVE : CAN-2004-0488
BID : 10355
Nessus ID : 12255

Risultati

I risultati di nessus non sono l'arrivo,
ma un punto di partenza.

Il report deve essere interpretato da un esperto, e non accettato acriticamente.



Hackers Approach

Ulteriori test

Con i risultati raccolti possiamo procedere a testare manualmente, o con strumenti più specifici, magari creati appositamente, ulteriori servizi peculiari del network esaminato.

Es. snmpwalk

snmpwalk fa parte del kit net-snmp e permette, conosciuta la community, di ottenere un elevato numero di informazioni (tra cui statistiche, configurazione hw e sw, etc etc) circa l'host che ha il demone snmpd attivo ed accessibile.

Diverso approccio

Effettuati questi ed altri test attraverso Internet potremmo considerare il test concluso.

Un elenco di server aggiornati e ben configurati potrebbe indurci a dire “la vostra rete per ora e' sicura”.

Altre tecniche

Altre tecniche

Un buon pen-tester non si ferma ai primi risultati, cerca una strada “alternativa”.

Ad esempio verificare accessi wireless, dial-up o la possibilità di ottenere informazioni dagli utenti.

kismet

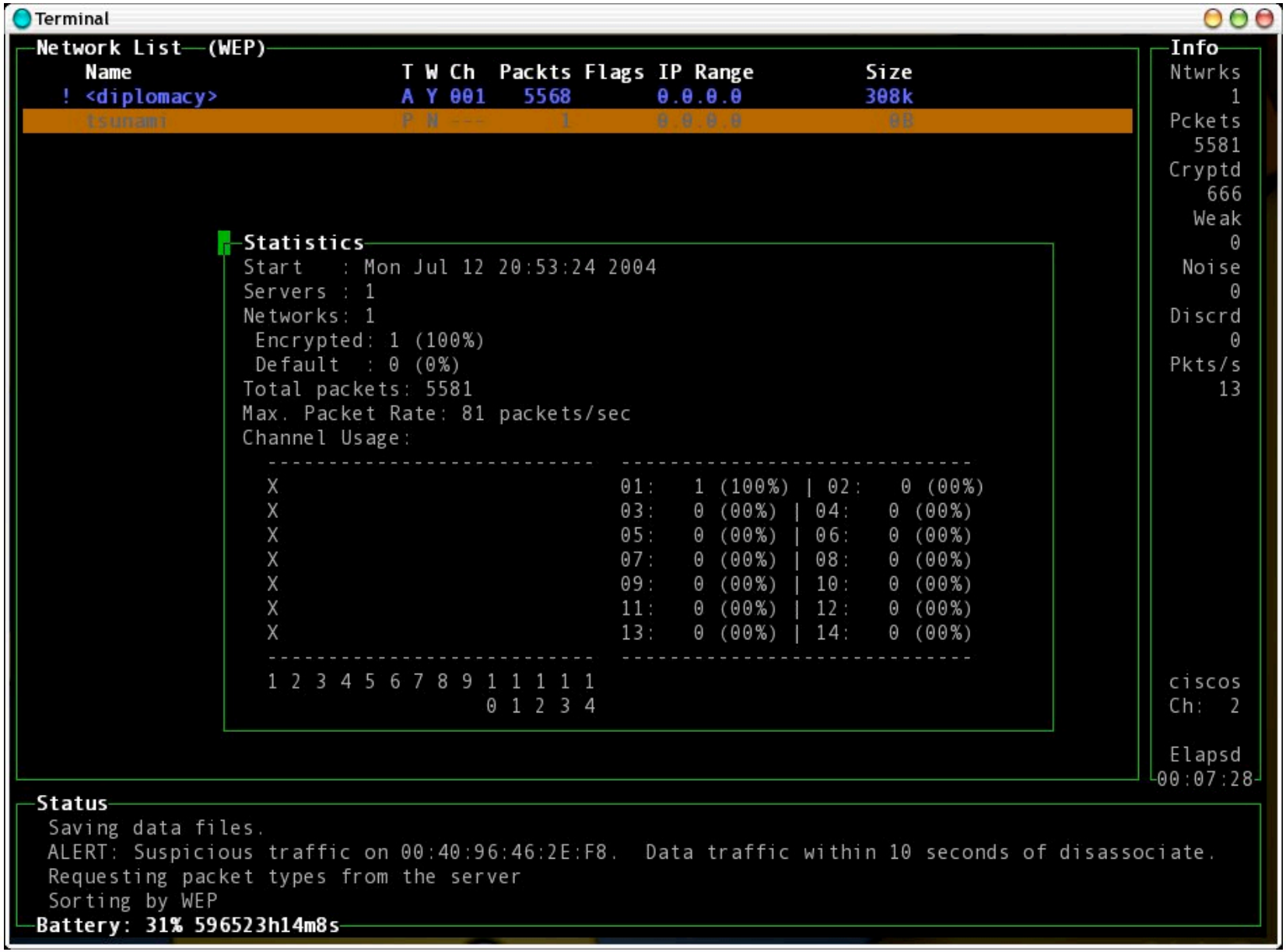
Kismet è uno sniffer orientato a rilevare reti wireless e collezionare i dati necessari per forzare l'eventuale chiave WEP.

Come lavora kismet

Questo strumento imposta la scheda wireless in RFMON, l'equivalente della modalità promiscua.

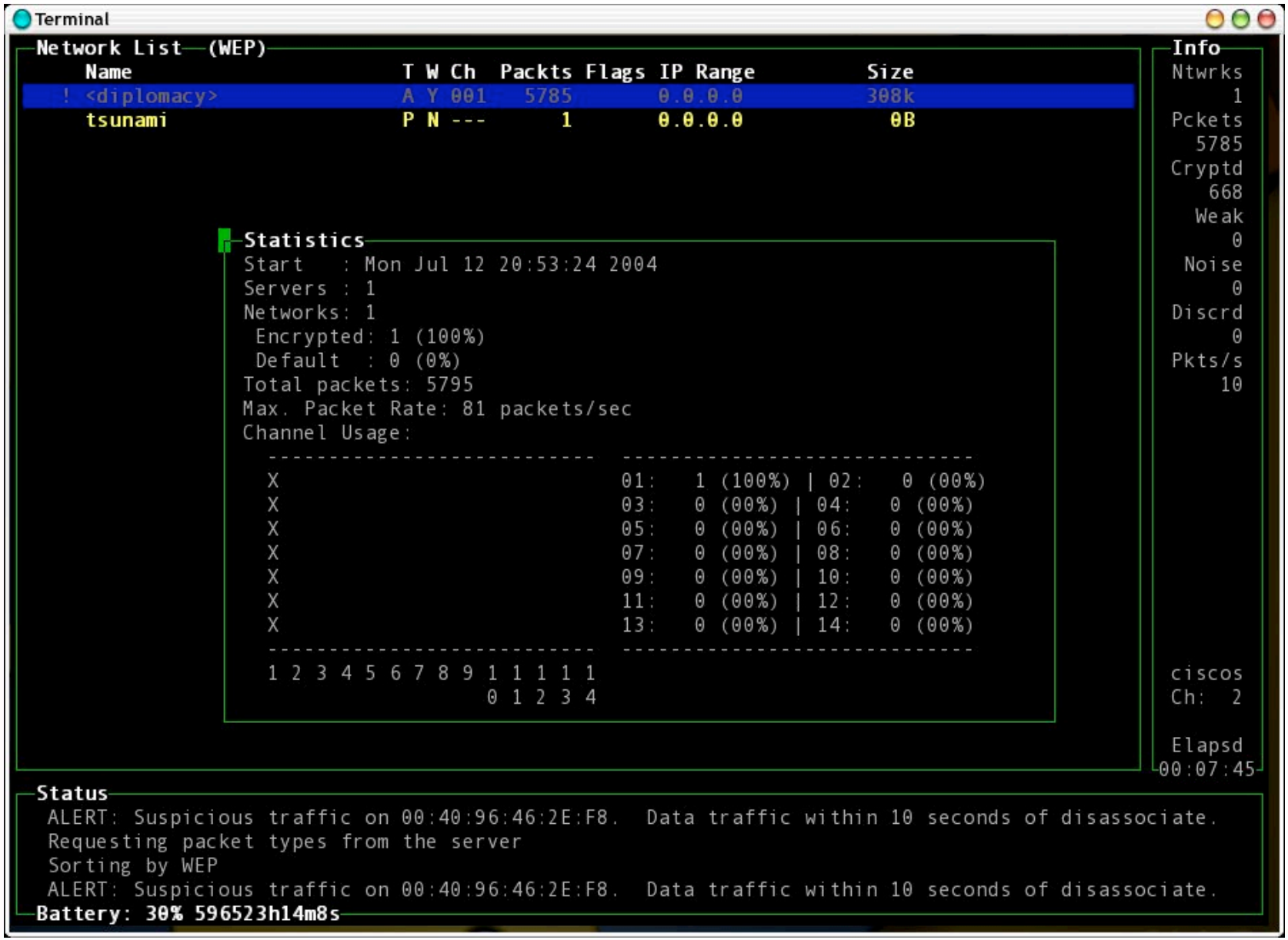
Saltando di canale in canale verifica se è possibile ricevere qualche segnale 802.11a/b/g e quali proprietà presenta.

Kismet



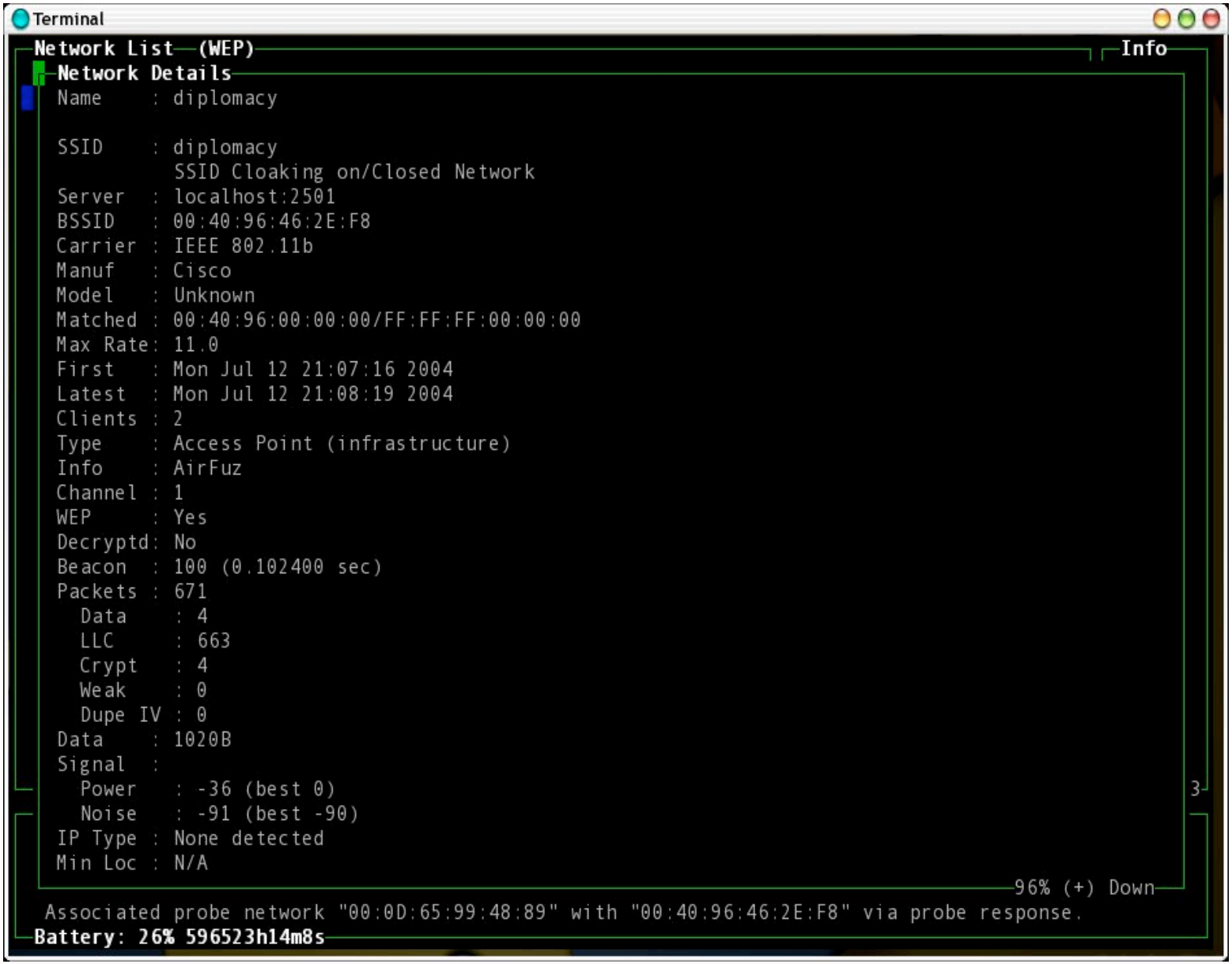
http://www.alba.st/
mayhem@alba.st

Kismet

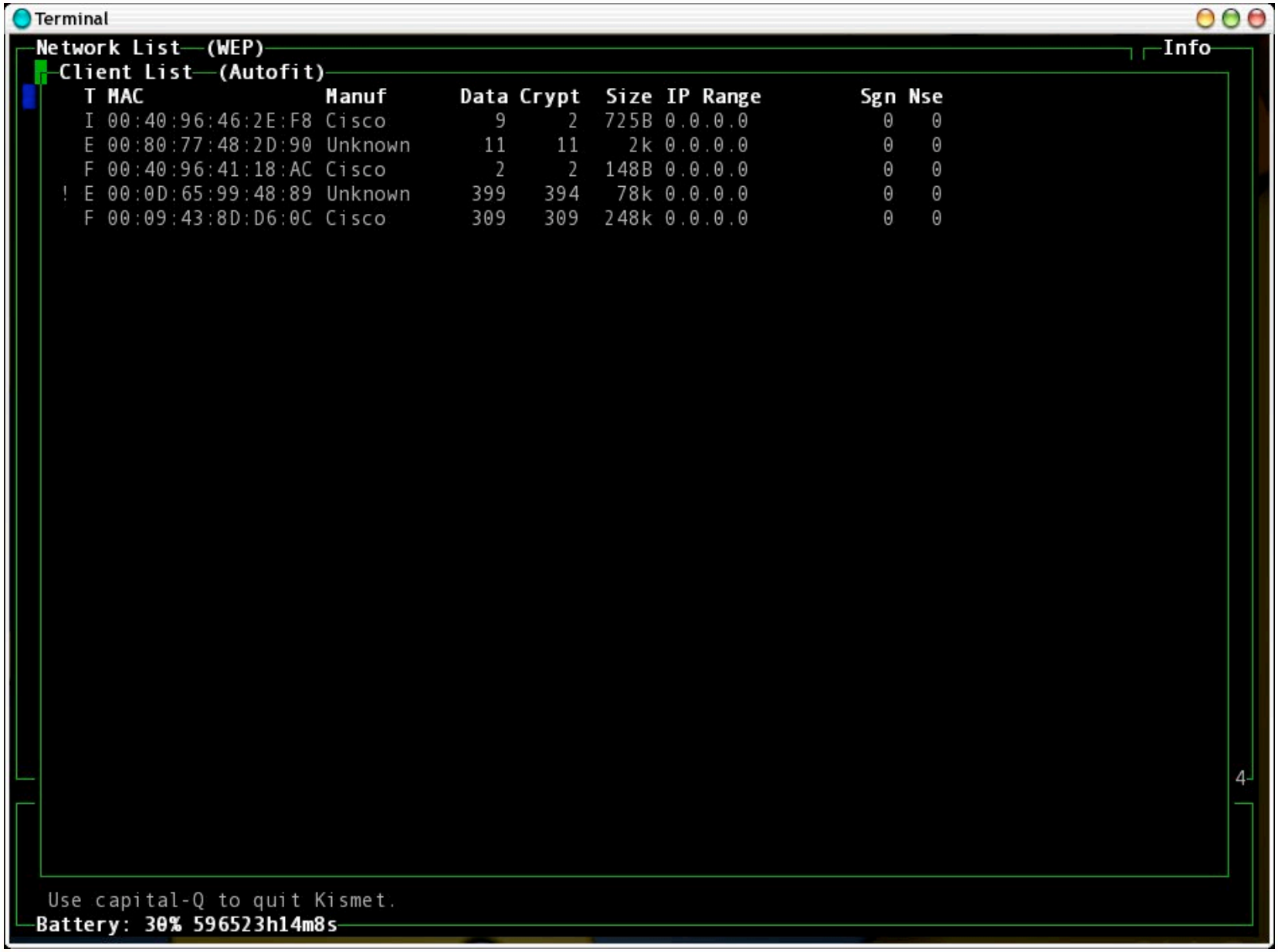


http://www.alba.st/
mayhem@alba.st

Kismet

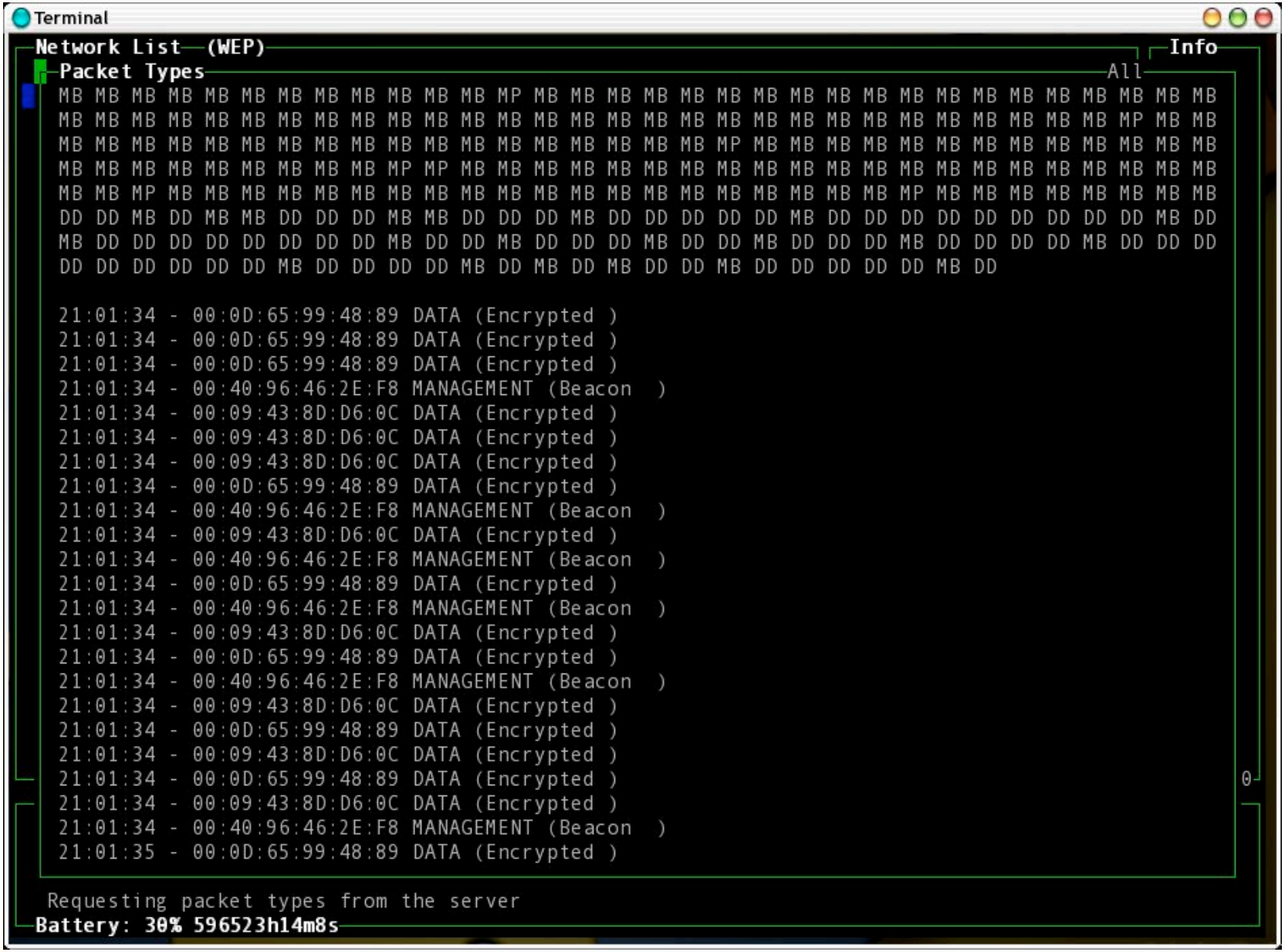

Terminal
Network List (WEP)
Info
Network Details
Name : diplomacy
SSID : diplomacy
SSID Cloaking on/Closed Network
Server : localhost:2501
BSSID : 00:40:96:46:2E:F8
Carrier : IEEE 802.11b
Manuf : Cisco
Model : Unknown
Matched : 00:40:96:00:00:00/FF:FF:FF:00:00:00
Max Rate: 11.0
First : Mon Jul 12 21:07:16 2004
Latest : Mon Jul 12 21:08:19 2004
Clients : 2
Type : Access Point (infrastructure)
Info : AirFuz
Channel : 1
WEP : Yes
Decryptd: No
Beacon : 100 (0.102400 sec)
Packets : 671
Data : 4
LLC : 663
Crypt : 4
Weak : 0
Dupe IV : 0
Data : 1020B
Signal :
Power : -36 (best 0)
Noise : -91 (best -90)
IP Type : None detected
Min Loc : N/A
96% (+) Down
Associated probe network "00:0D:65:99:48:89" with "00:40:96:46:2E:F8" via probe response.
Battery: 26% 596523h14m8s

Kismet



http://www.alba.st/
mayhem@alba.st

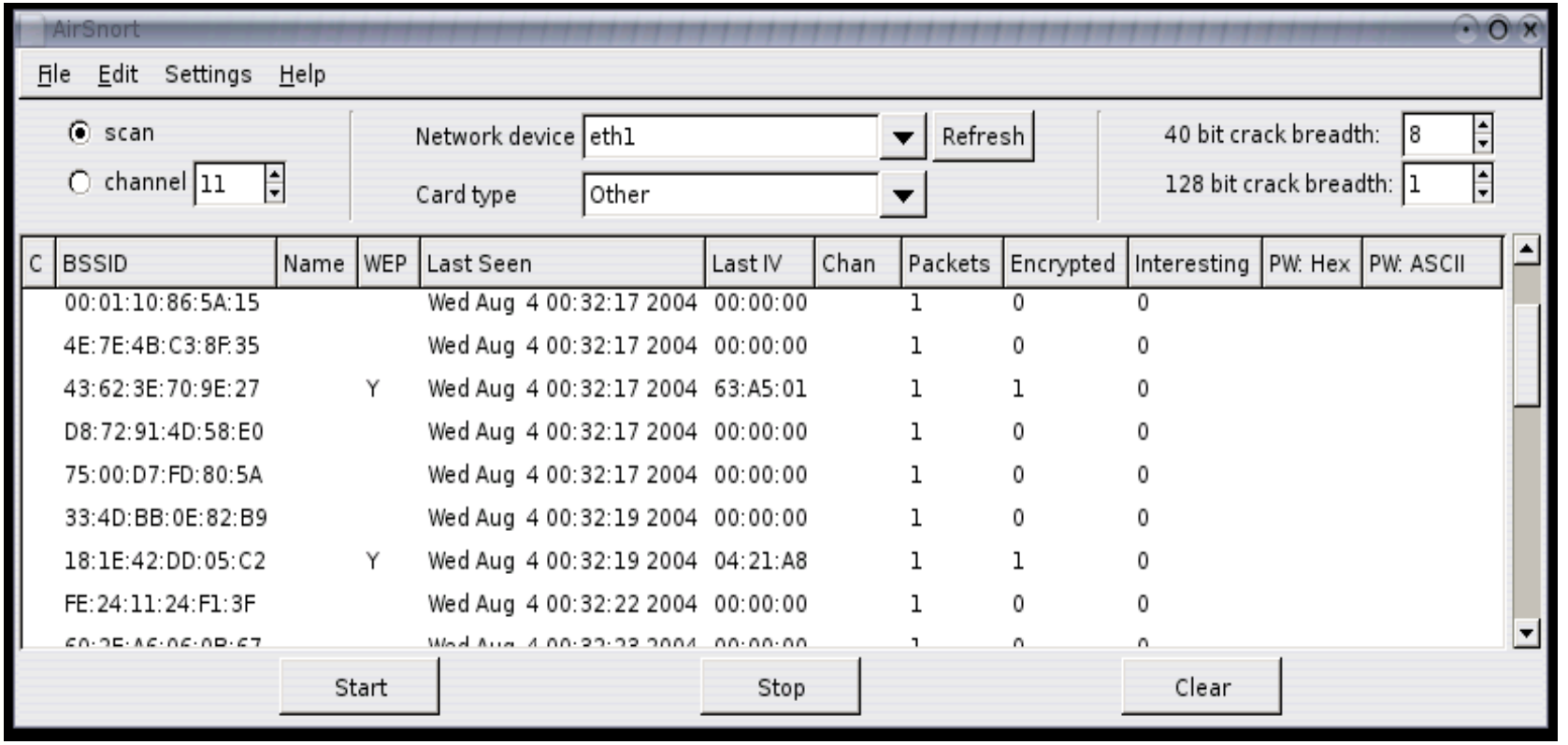
Kismet


Terminal
Network List (WEP)
Info
Packet Types
All
MB MB MB MB MB MB MB MB MB MB MB MP MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MP MB MB
MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MP MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MB MB MB MB MB MB MB MP MP MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB
MB MB MP MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MB MP MB MB MB MB MB MB MB MB
DD DD MB DD MB MB DD DD DD MB MB DD DD DD MB DD DD DD DD DD MB DD DD DD DD DD DD DD DD MB DD
MB DD DD DD DD DD DD DD DD MB DD DD MB DD DD DD MB DD DD MB DD DD DD MB DD DD DD DD MB DD DD DD
DD DD DD DD DD DD MB DD DD DD DD MB DD MB DD MB DD DD MB DD DD DD DD DD MB DD
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:40:96:46:2E:F8 MANAGEMENT (Beacon)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:40:96:46:2E:F8 MANAGEMENT (Beacon)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:40:96:46:2E:F8 MANAGEMENT (Beacon)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:40:96:46:2E:F8 MANAGEMENT (Beacon)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:40:96:46:2E:F8 MANAGEMENT (Beacon)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:0D:65:99:48:89 DATA (Encrypted)
21:01:34 - 00:09:43:8D:D6:0C DATA (Encrypted)
21:01:34 - 00:40:96:46:2E:F8 MANAGEMENT (Beacon)
21:01:35 - 00:0D:65:99:48:89 DATA (Encrypted)
0
Requesting packet types from the server
Battery: 30% 596523h14m8s

AirSnort

Individuata una rete su cui transita traffico criptato, sarà possibile utilizzare airsnort per trovare la corretta chiave WEP, che ci permetterà di accedere alla rete wireless analizzata.

AirSnort al lavoro



Accessi Dial-up

Spesso le moderne reti aziendali permettono comunque degli accessi

dial-up, per consentire connessioni remote ai propri dipendenti.

Ricerca di un RAS

Ricercare una connessione dati, sia in analogico che in digitale, su tutti i numeri di proprietà del cliente si rivela spesso fruttuoso.

Spesso username/password banali permettono una connessione “amministrativa”.

Modem “pirata”

Non è raro il caso di dipendenti che collegano al proprio PC aziendale, all'insaputa dell'ufficio IT, modem che permettono un collegamento dall'esterno, per garantirsi un accesso da casa.

Cain&Abel

Durante i nostri test potremmo venire in possesso di password criptate o avere accesso alla LAN. In questi casi Cain&Abel si rivelerà uno strumento indispensabile.

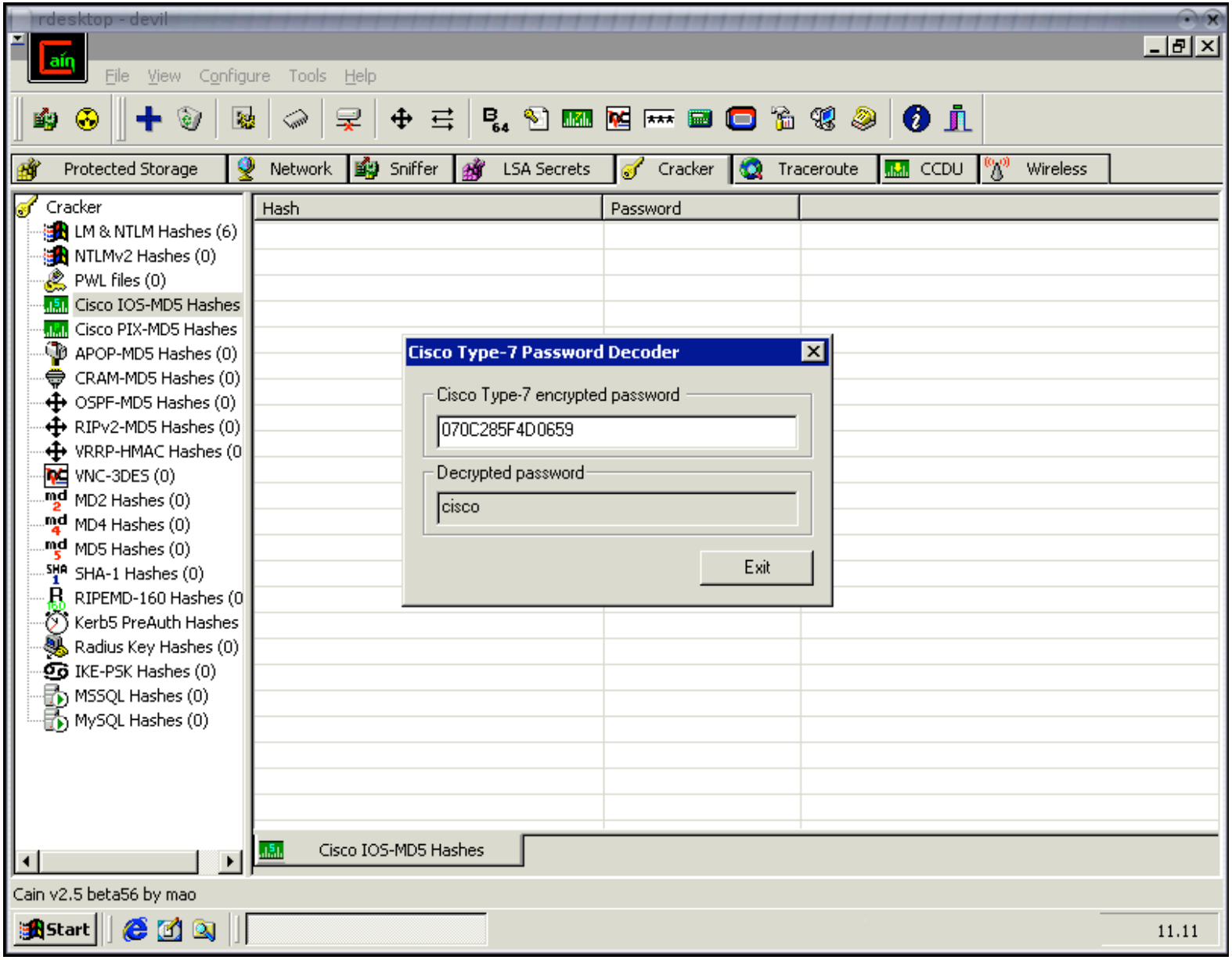
Cain&Abel

Questo tool permette di raccogliere gli hash Lan Manager, in transito su una rete che possiamo “osservare”, di fare il dump del SAM o di caricarne una copia da un file. Colleziona inoltre le password in chiaro che passano sul nostro segmento di rete.

http://www.alba.st/
mayhem@alba.st

Cain&Abel

E' possibile decifrare le password così raccolte, oltre a quelle di innumerevoli altri servizi, ad esempio le password di tipo 7 e di tipo 5 di Cisco.

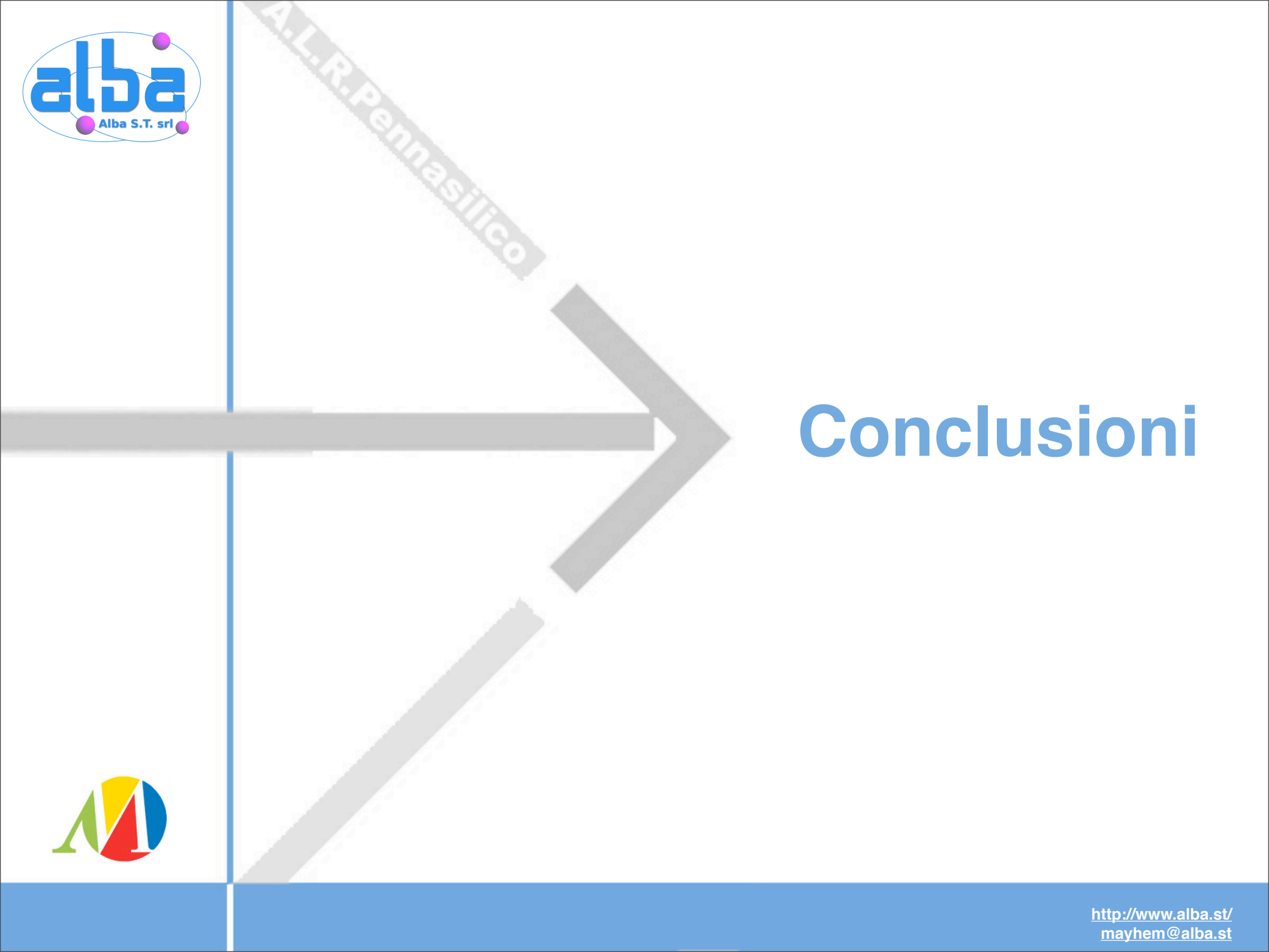

rdesktop - devil
File View Configure Tools Help
Protected Storage
Network
Sniffer
LSA Secrets
Cracker
Traceroute
CCDU
Wireless
Cracker
LM & NTLM Hashes (6)
NTLMv2 Hashes (0)
PWL files (0)
Cisco IOS-MD5 Hashes
Cisco PIX-MD5 Hashes
APOP-MD5 Hashes (0)
CRAM-MD5 Hashes (0)
OSPF-MD5 Hashes (0)
RIPv2-MD5 Hashes (0)
VRRP-HMAC Hashes (0
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
RIPEMD-160 Hashes (0
Kerb5 PreAuth Hashes
Radius Key Hashes (0)
IKE-PSK Hashes (0)
MSSQL Hashes (0)
MySQL Hashes (0)
Hash
Password
Cisco Type-7 Password Decoder
Cisco Type-7 encrypted password
070C285F4D0659
Decrypted password
cisco
Exit
Cisco IOS-MD5 Hashes
Cain v2.5 beta56 by mao
Start
11.11

Social-Engineering

Un'altra tecnica redditizia è tentare di impersonare qualcuno per ottenere informazioni direttamente da persone collegate all'azienda.

Social-Engineering

Possiamo spacciarci per l'amministratore di rete e chiedere ad un fornitore di servizi di comunicarci la password o fingerci un tecnico per farci comunicare informazioni da un dipendente o accedere ai locali dell'azienda.



Conclusioni

Abbiamo il firewall!

Attacchi alle reti wireless, ad accessi dial-up e social-engineering troppo spesso consentono di ottenere un accesso ad una rete effettivamente sicura rispetto ad attacchi provenienti da Internet.

Conclusioni

Questi strumenti sono molto utili per verificare un grande numero di host

per verificare con metodo le vulnerabilità note.

In un penetration test vengono tuttavia utilizzati strumenti creati ad-hoc, molta “creatività” e viene applicata una approfondita conoscenza dei servizi.

Etica Professionale

Non dimentichiamo comunque che i nostri test devono **sempre** essere effettuati secondo i tempi ed i modi **preventivamente** concordati con il cliente.

Test inutilmente dannosi vanno evitati, così come il terrorismo psicologico.

http://www.alba.st/
mayhem@alba.st

Web-o-grafia

- http://www.hping.org
- http://www.insecure.org/nmap/
- http://www.cirt.net
- http://www.thc.org
- http://www.nessus.org
- http://www.kismetwireless.net
- http://airsnort.shmoo.com
- http://www.oxid.it
- http://www.packetstormsecurity.org
- http://www.securityfocus.com
- http://www.sikurezza.org
- $ apropos && man :)

Sabato 16 Giugno 2007

Linux e la Sicurezza Personale

Relatori da tutta italia

Una giornata incentrata sul software
OpenSource e la Sicurezza

Domande?

Queste slide sono disponibili su:
http://www.alba.st

Per domande o approfondimenti:
mayhem@alba.st

Domande?

Grazie per l'attenzione!

Queste slide sono disponibili su:
http://www.alba.st

Per domande o approfondimenti:
mayhem@alba.st