

Hackers && Opensource

ra1nb0w & A6U

24 Ottobre 2009



Chi siamo?

- Studenti di Sicurezza Informatica presso l'Universita' degli Studi di Milano (DTI).
- ...

Di cosa parleremo...

- cos'e' l'opensource (potenzialita')
- chi sono gli hackers e i falsi miti
- falsa sicurezza(data retention)
- creativita' del codice
- oltre la finestra
- hacking
- living in the future

Di cosa non parleremo...

- exploit / 0days
- invadere la privacy altrui
- spiare la propria fidanzata
- cambiare i voti scolastici :D
- ...

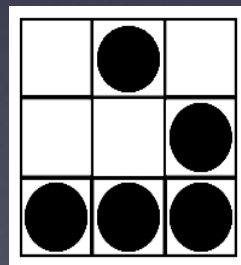


Cos'e' l'opensource?



Terminologia

- *hacker: colui che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte. (white-hat)*
- *cracker: colui che commette crimini informatici. (black-hat)*
- *script-kiddie <> lamer: colui che ricerca un'intrusione facile usando script altrui.*



Falsa sicurezza

- Data retention : archiviazione “sicura” dei dati
- Falsi hacker : uso di script pronti all'uso
- Profiling : raccolta di informazioni su qualcuno
- Privacy nei social network
- ...

IT Hackers activity

- fantasy coding
- debugging
- traffic analysis
- bug hunting
- hardening
- problem solving
- scrivere documentazione e diffonderla
- diffondere la liberta'
- lottare contro il controllo

< Paranoici >

- criptare tutto
- navigare anonimamente (tor - freenet)
- non lasciare nessuna traccia se non voluta
- capire tutto quello che si usa



Creativita' del codice

```
#include <stdio.h>
main(t,_,a)char *a;{return!0<t?t<3?main(-79,-13,a+main(-87,1-_,
main(-86,0,a+1)+a)):1,t<_?main(t+1,_,a):3,main(-94,-27+t,a)&& t==2?_<13?
main(2,_,+1,"%s %d %d\n"):9:16:t<0?t<-72?main(_,t,
"@n'+,#'/*{}w+/w#cdnr/+,{}r/*de}+,/*{*+,/w{%+,/w#q#n+,/{l,+,/n{n+,/+ #n+,/#\
;#q#n+,/+k#;*+,/'r : 'd*'3,}{w+K w'K: '+}e#';dq#'l \
q#'+d'K#!/+k#;q# 'r}eKK#}w' r}eKK{n l} '/#;#q#n') {) #}w' ) {) {n l} '/+ #n';d}rw' i;# \
) {n l} !/n {n #' ; r { #w' r nc {n l} '/# {l, +'K {rw' iK {; [{n l} '/w#q#n'wk nw' \
iwk {KK {n l} !/w { %' l ##w #' i; : {n l} '/* {q# 'ld; r' } {n lwb !/*de} 'c \
;; {n l' - { }rw] '/+, } ## '*' } #nc, ', #nw] '/+kd'+e}+; #'rdq#w! nr' / ' ) }+} {rl# '{n' ' ) # \
}' +} ## (!!/" )
:t<-50?_==*a?putchar(31[a]):main(-65,_,a+1):main((*a=='/')+t,_,a+1)
:0<t?main(2,2,"%s"): *a=='/' || main(0,main(-61,*a,
"!ek;dc i@bK'(q)-[w]*%n+r3#l,{ }:\nuwloca-0;m .vpbks,fxntdCeghiry"),a+1);}
```

http://en.wikipedia.org/wiki/Code_obfuscation

Creativita' del codice - result

On the first day of Christmas my true love gave to me
a partridge in a pear tree.

On the second day of Christmas my true love gave to me
two turtle doves
and a partridge in a pear tree.

On the third day of Christmas my true love gave to me
three french hens, two turtle doves
and a partridge in a pear tree.

On the fourth day of Christmas my true love gave to me
four calling birds, three french hens, two turtle doves
and a partridge in a pear tree.

On the fifth day of Christmas my true love gave to me
five gold rings;
four calling birds, three french hens, two turtle doves
and a partridge in a pear tree.
...

```

#
sub j(\$){($
@_;while($$P=-s:~
$V+=('('eq$1)?-32:31
$$P,0,1,""))-74} sub a{
;SI=int($I*$M/$Z);SK=int(
/$Z);SL=int($L*$M/$Z); $G=$
G)>=abs($F)?$G:$F;($E<0) and($
;for($i=0;$i<=abs$E;$i++){ $D->{$K
}->{$I+int($i*$G/$E)}=1}}sub p{$D={};$
$H=$_;SI=$N-j$H;SK=$O-j$H;while($H){$q=ord
substr($H,0,1,"");if(42==$q){$J=j$H;$L=j$H}else{$q-=43;$L=$q
%9;$J=($q-$L)/9;$L=$q-9*$J-4;$J-=4;$J+=SI;$L+=SK;a($I,$K,$J,$L);
($I,$K)=($J,$L)}a($I,$K,$N,$O)}@_;my$T;map{$y=$_;map{$T=$D->{$y}
->{$_}?$\'':$\''}(-59..59);$T.="\\n"}(-23..23);print "\\e[H$T"$w= eval{
require Win32::Console::ANSI};$b=$w?'1;7;':'';($j,$u,$s,$t,$a,$n,$o
,$h,$c,$k,$p,$e,$r,$l,$c)=split/\/, 'Tw*JSK8Iag*PJ[*J@wR}*JR]*QJ[*J'.
'BA*JQK8I*JC}KUZ}BAIJT}*QJ[R?-R[e]\'RI'. '}'Tn*JQ}wRAI*JDnR8QAU}wT8KT'.
']n*JEI*EJR*QJ}*JR*Dj@IQ[*JSe*JD[n]*JPe*'. 'JBI/KI}T8@?PcdnfgVCBRcP'.
'?ABKV]]}*JWe*JD[n]*JPe*JC?8B*JE};Vq*OJQ/IP[\''. 'wQ}*JWeOe{n*EERk8;'.
'J*JC}/U*OJd[OI@*BJ*JXn*J>w]U}CWq*OJc8KJ?O[e]U/T*QJP?}*JSe*JCnTe'.
'QIAKJR}*JV}wRAI*J?}T}*RJcJI[\\3;U]Uq*PM[wV]W}WCT*DM*SJ'. 'ZP[Z'.
'PZa[\\]UKVgogK9K*QJ[\\]n[RI@*EH@IddR[Q[ ]T]T]T3o[dk*JE'. '[Z\\U'.
'{T}*JPKTKK}*OJ[QIO[PIQIO[[gUKU\\k*JE+J+J5R5AI*EJ00'. 'BCB*'.
'DMKKJIR[Q+*EJ0*EK';sub h{($\\ = qw(% & @ x)[int rand
4];map{printf "\\e[\\$b;\\$dm",int(rand 6)+101-60* ($w
||0);system( "cls")}if$w ;($A,$S)= ($_[1], $
_[0]);($M, @,)= split ' ';for($z=256
;$z>0;$z --$S){$S*= $A;p @,} sleep$z
[2];while ($_[3]&&($ z+=$ S) <=256){
p@,}}{" ". "32}7D$j" ."}AG". "$u}OG"
."$s}WG" ."$t",". "24}{(" ."}IJ$a"
."}1G$n" ."}CO$so" ."}GG$t" ."}QC"
."$h}" ."}^G$e" ."}IG" ."}$r",
"32}?" ."}H$P}FG$e}QG$r" ."}ZC"
."$l", "28}{LC" ."" ."}"
."$h}:" ."}J$a}EG" ."}$c"
."}M" ."}C$K}ZG" ."}$e"
."}" ."}dG$r","18" ."}{"
."D;" ."}SC" )}{h(16 ,1,1,0
);h(8, .98,0,0 );h(16 ,1,1,1)
;h(8.0 ,0.98,0, 1); redo}###
#written
#liverpole
#eeeeeeeeeeeeee

```

guardare oltre
la GUI

■ ■ ■ ■

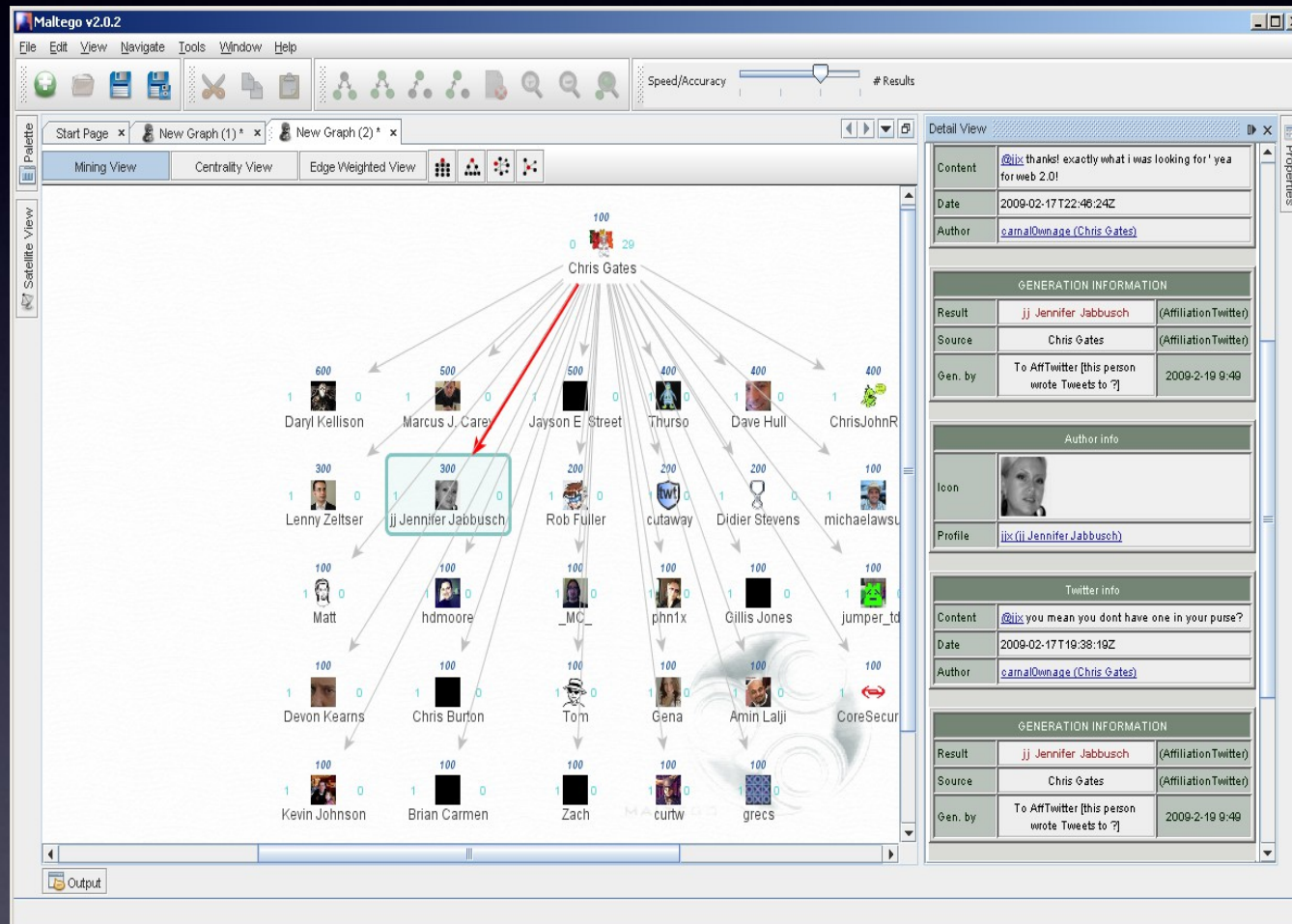
Driftnet

Visualizzare le immagini passanti per la rete (ethernet)



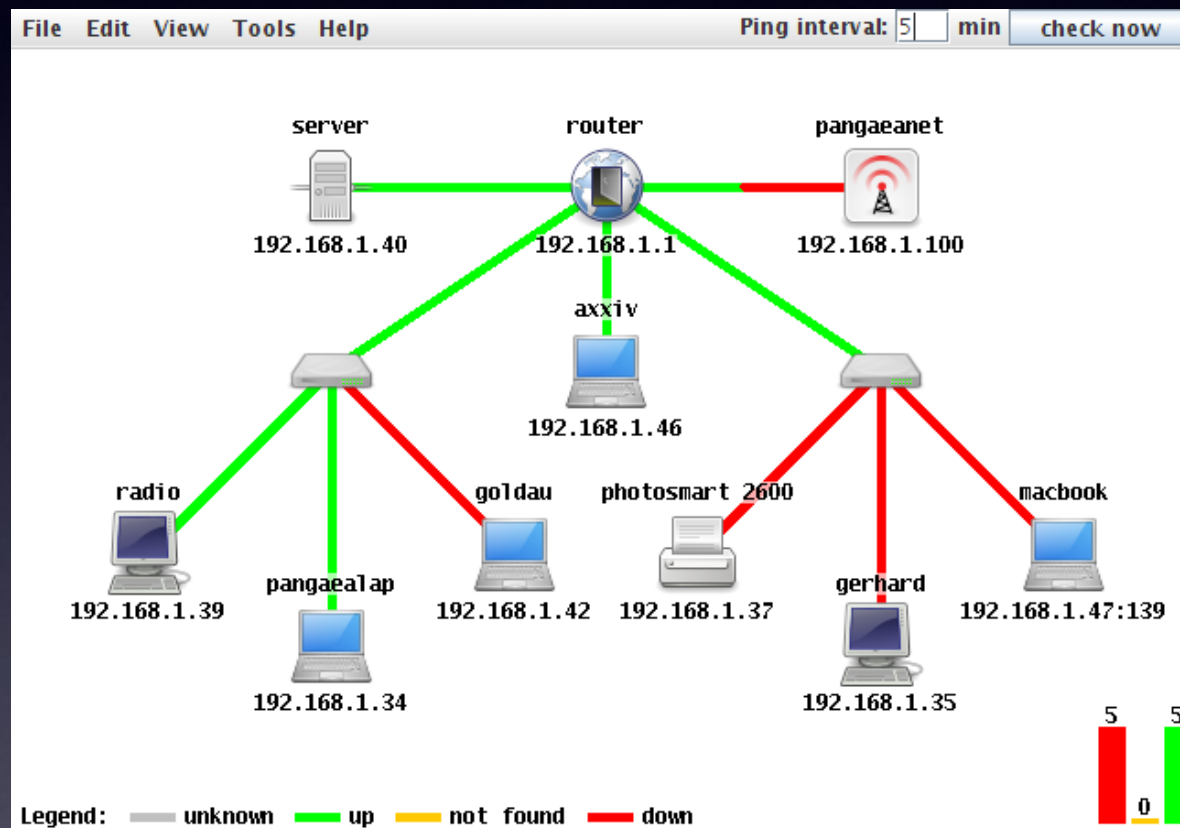
Maltego

Ci permette di fare data mining sulle persone



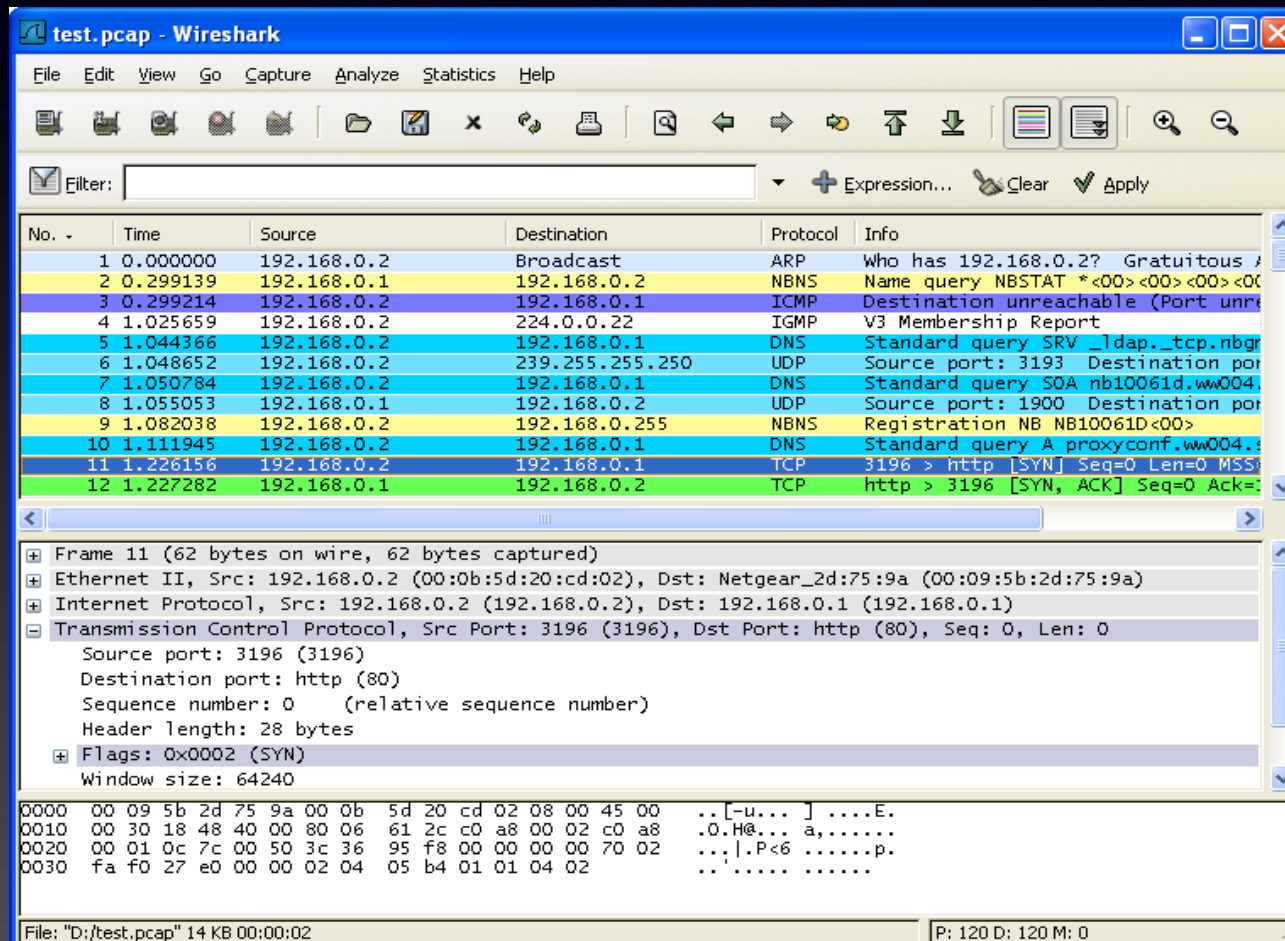
JnetMap - Radialnet

Ci permette di visualizzare il network map



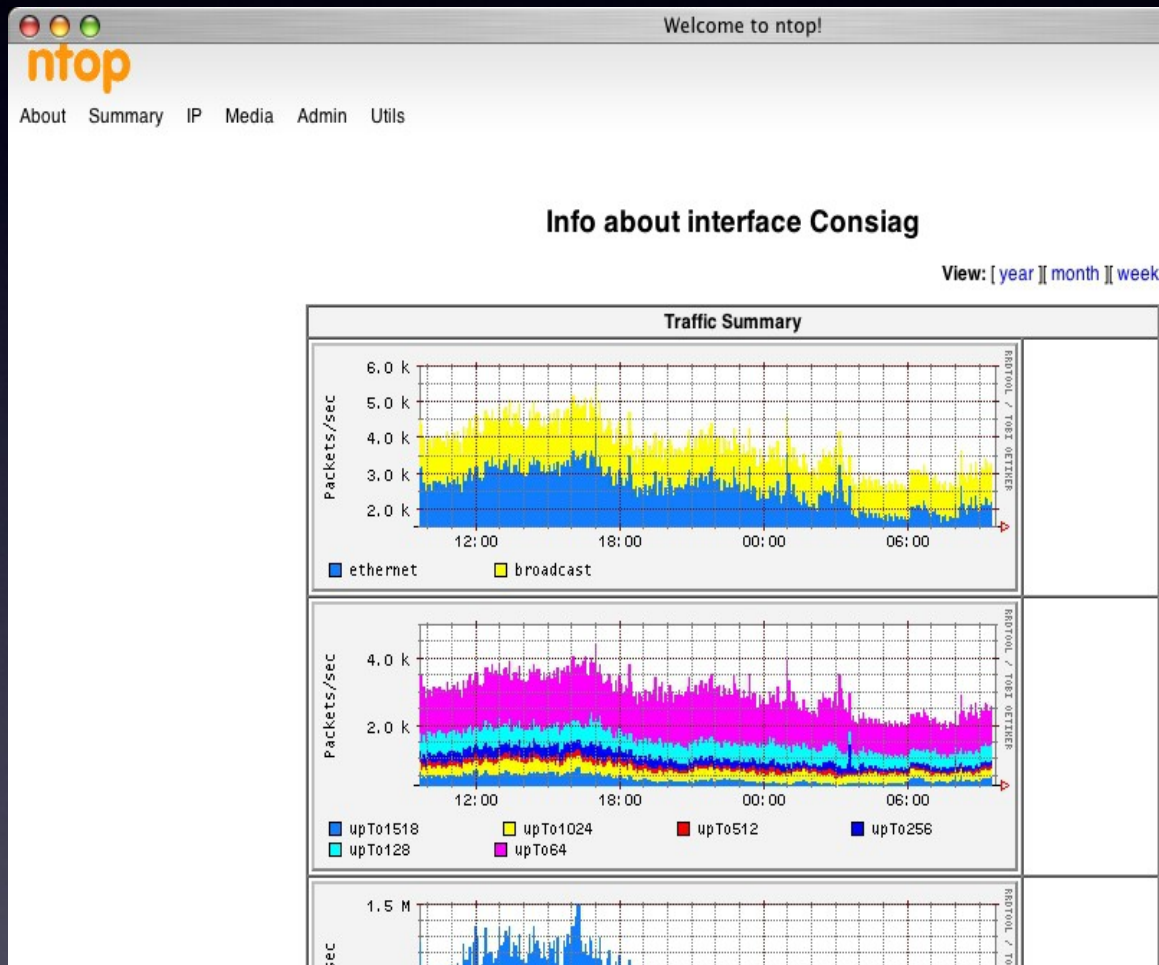
Wireshark

Ci permette l'analisi del traffico di rete



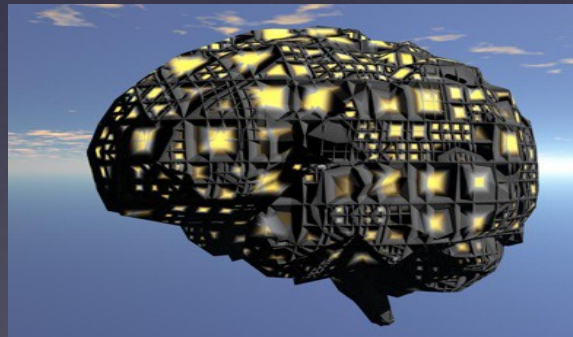
NTOP

Grafici sul traffico di rete

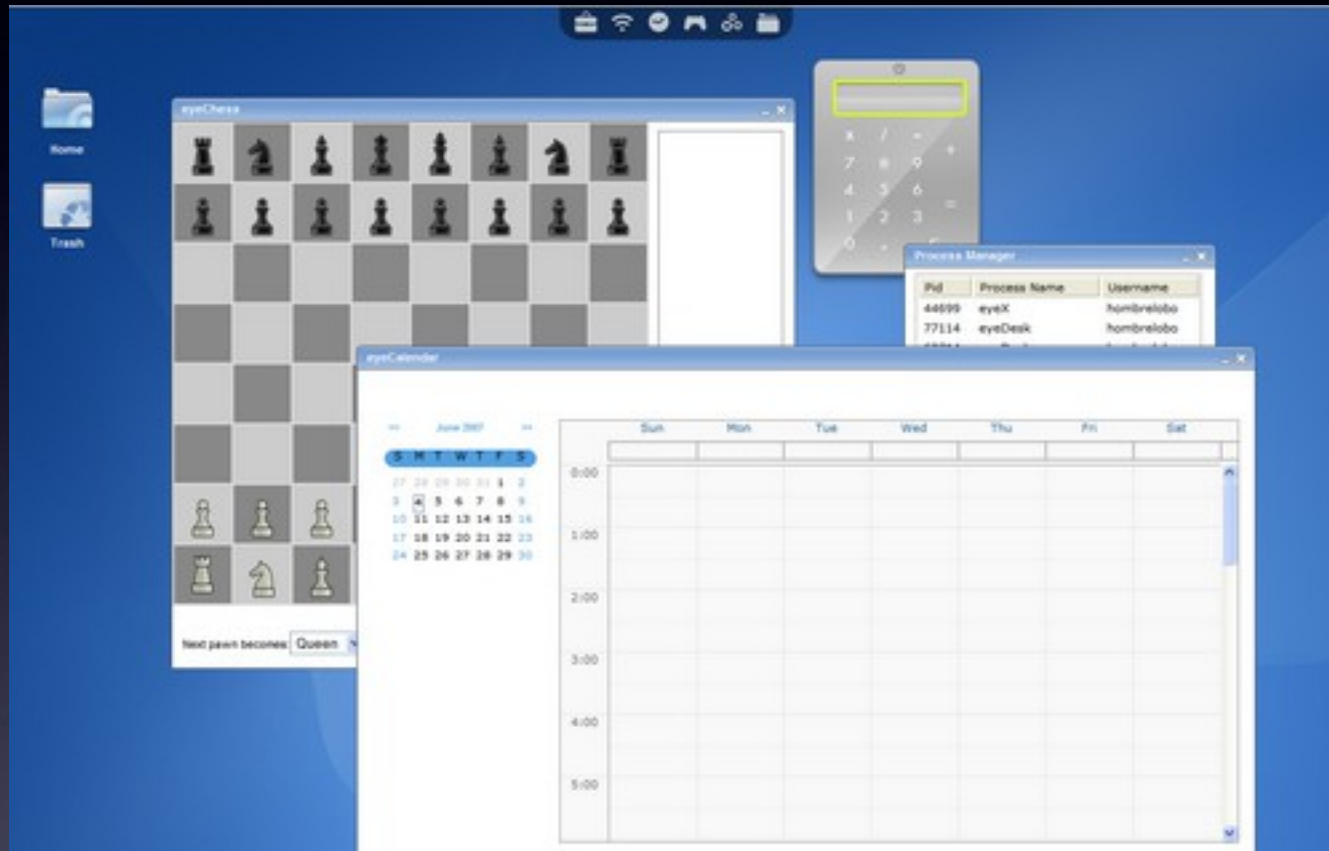


Living in the future

- world wide computer
- !=cybersfruttatori
- cloud computing
- grid computing
- distributed antivirus (immunet protect)
- AI = artificial intelligence
- ...



eyeOS example



References

- Il lato oscuro della rete (Nicholas Rucc)
- How to become a hacker (Eric S. Raymond) - *<http://www.catb.org/esr/faqs/hacker-howto.html>*
- Luca Carettoni, David Laniado "Etica Hacker: l'imperativo hands-on" - *<http://www.ikkisoft.com/stu/hackdoc.pdf>*
- Hackers Prolog - *<http://hpp.recursiva.org>*
- *internet's world*
- man - info - papers

Contact

- *Rainbow*
- vieni a trovarci su irc.freenode.net - canale #pnlug
- mail: rainbow@irh.it
- site: www.irh.it
-
- *A6U*
- mail: mail@teocolella.net
- Site: www.teocolella.net

License

Queste slide sono realizzate da Davide 'ra1nb0w' Gerhard e Matteo Colella e sono soggette alla licenza Creative Commons nella versione Attribution-ShareAlike 2.0; possono pertanto essere distribuite liberamente ed altrettanto liberamente modificate, a patto che se ne citi l'autore e la provenienza (sito-mail).

END

