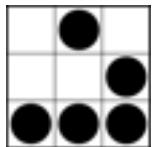


Basta Hacker in TV!

Come la percezione distorta della realtà influenza negativamente la nostra capacità di giudizio



<http://www.alba.st/>
Verona, Milano, Roma
Phone/Fax +39 045 8271202



Alessio L.R. Pennasilico
a.pennasilico@alba.st

\$whois -=mayhem=-

Security Evangelist @



Committed:

AIP Associazione Informatici Professionisti, CLUSIT

AIPSI Associazione Italiana Professionisti Sicurezza Informatica

Italian Linux Society, Sikurezza.org, Spippolatori, AIP/OPSI, IISFA

Hacker's Profiling Project, CrISTAL





Mia nonna diceva...

Non credere a tutto quel che vedi in televisione...

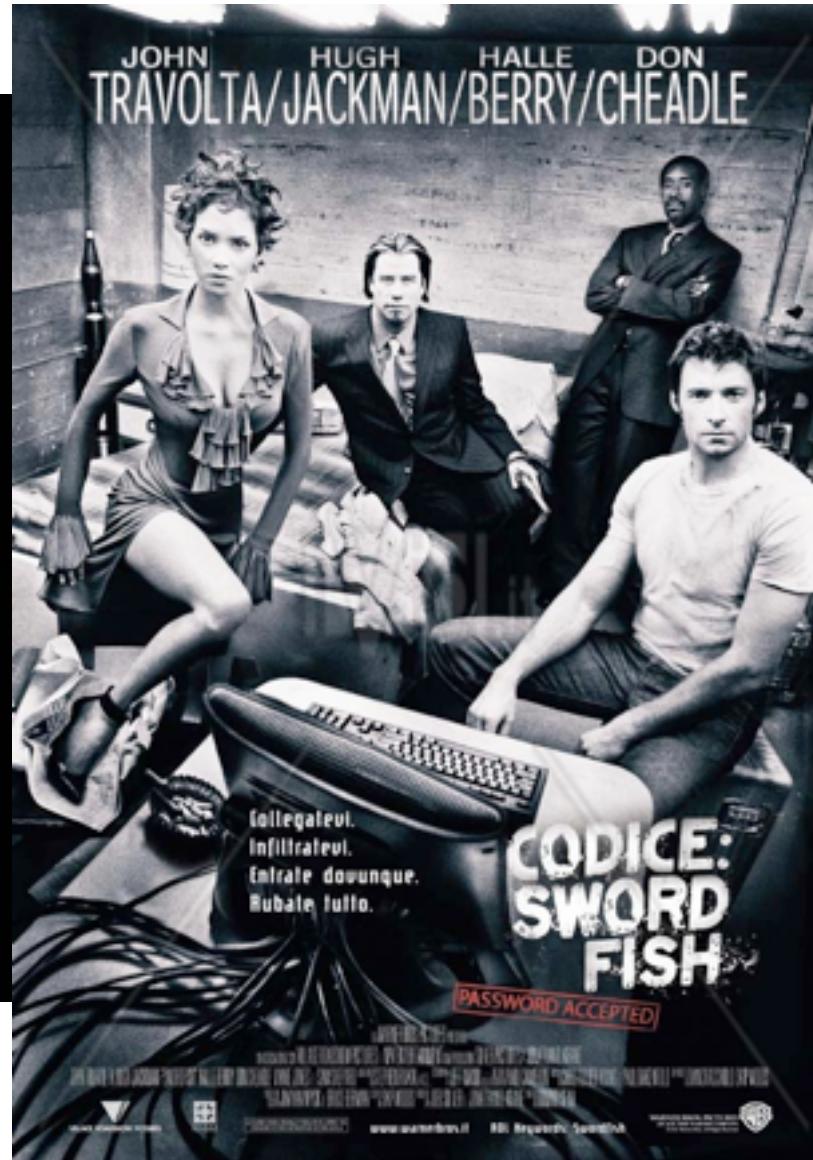


La tecnologia dei desideri...





Manca il realismo





Linguaggio ed immagini





Brute Forcing?

```
CHECKFSYS  
DAEMON  
ADM  
UUCP  
BIN  
SYS  
123  
ADDUSER  
ADMIN  
ANON  
ANONYMUS  
ASG  
AUDIT  
AUTH  
BACHAPPL  
BACKUP  
BATCH  
BBH  
BLAST  
BUPSCHED  
CBM  
CBMTEST  
ROOT
```

```
SUPPORT  
CUSTSUP  
DATABASE  
CATALOG  
USER  
GUEST  
TOUR  
SYSDIAG  
SYSDIAGS  
DIAGS  
TEST  
DIAG  
FLD  
SERVICE  
SUPPORT  
VISITOR  
ADMIN  
SYSADM  
SYSADMIN  
OPERATOR  
MANAGER  
SAVE  
TAR  
DEVICE  
DEVADMIN  
ANON  
ANONYMOUS  
UUCP  
NUUCP  
ADM  
NET  
MAN  
MGR  
NETMGR  
NETWORK  
INSTALL  
JOURNAL  
JOURNALS  
HTML  
LEARN  
LIB  
LIBRARY  
RSM  
RSMADM  
RUSR  
SALES  
SAS  
SAVE  
BACKUP  
SAVEP  
SERVICE  
FIELD  
SETUP  
SHUTDOWN  
SMTP  
MAIL  
SOFTWORK  
SPACE  
STARTUP  
SU  
SUNDING  
SUOPER  
SUPER
```



Anonimizzare le informazioni

The terminal window has a dark blue background and a light blue header bar. The title 'COMPILER' is in white capital letters. In the top right corner of the header is a small white square icon. The main area contains the following text:

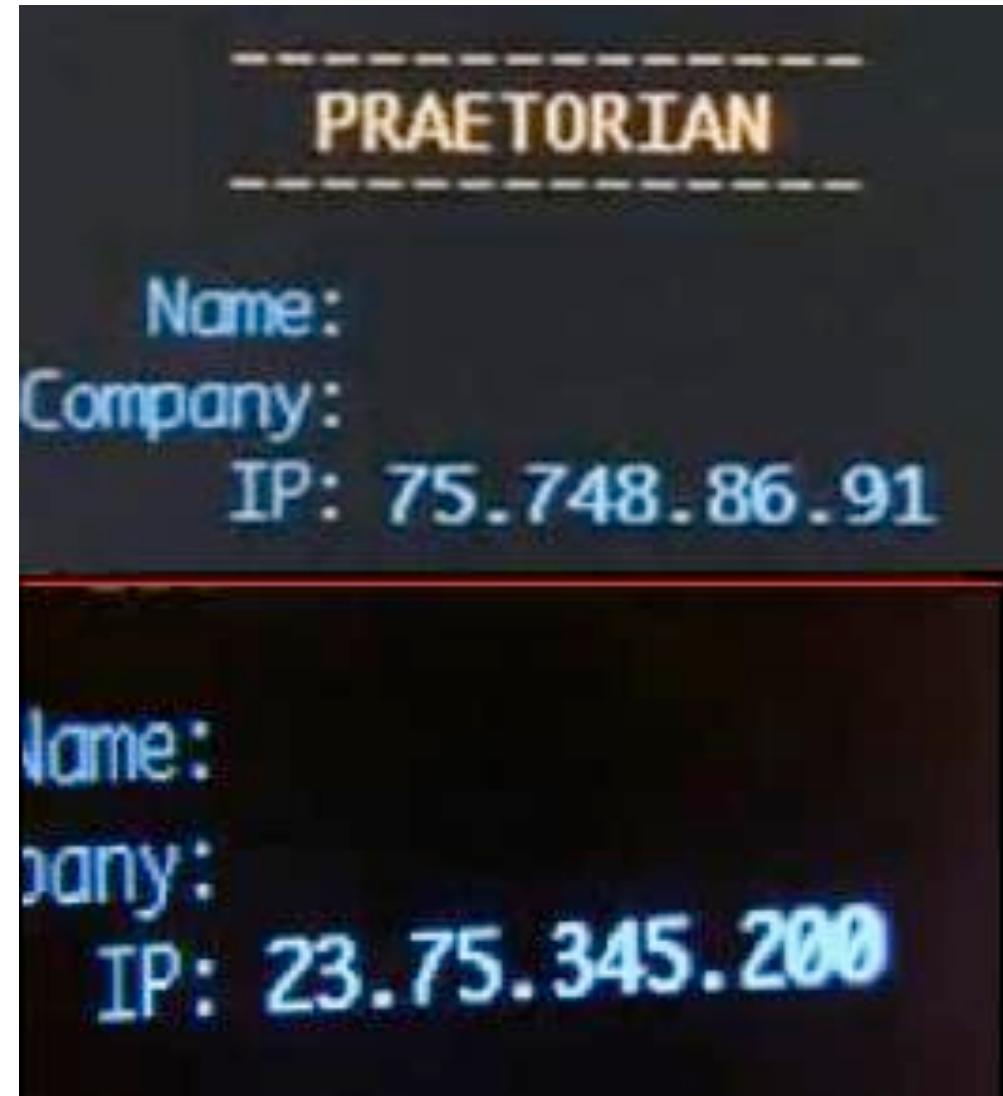
```
long ReadConfig(char *configFileSpec)
char buffer[200];
int basePort = -1;
int board, chip, unit, t
int lastBoard = -1, lastChip = -1;
long totalUnits = 0;
chipcth -c
```

To the right of the code, there are five IP addresses listed vertically:

Line of Code	Output IP Address
long ReadConfig(char *configFileSpec)	213.225.312.5
char buffer[200];	312.5.125.233
int basePort = -1;	232.12.10.362
int board, chip, unit, t	125.323.12.30
int lastBoard = -1, lastChip = -1;	291.12.112.323
long totalUnits = 0;	151.268.115.65
chipcth -c	

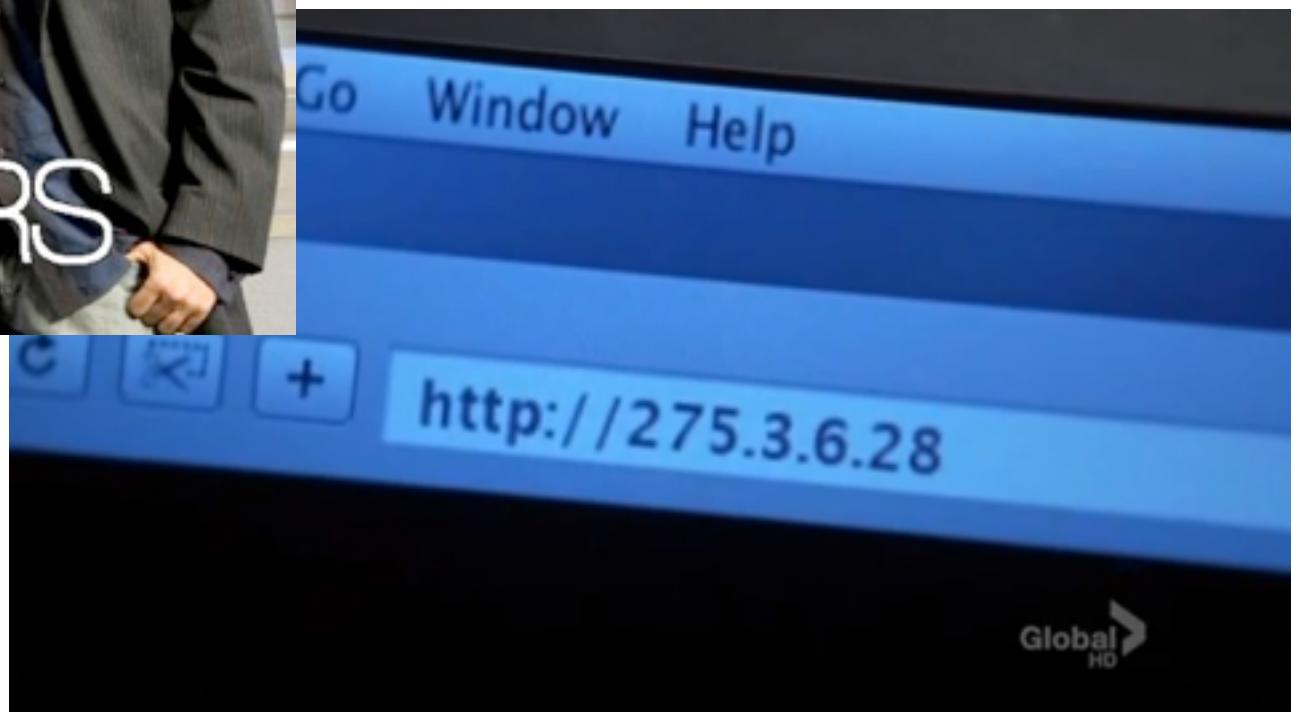
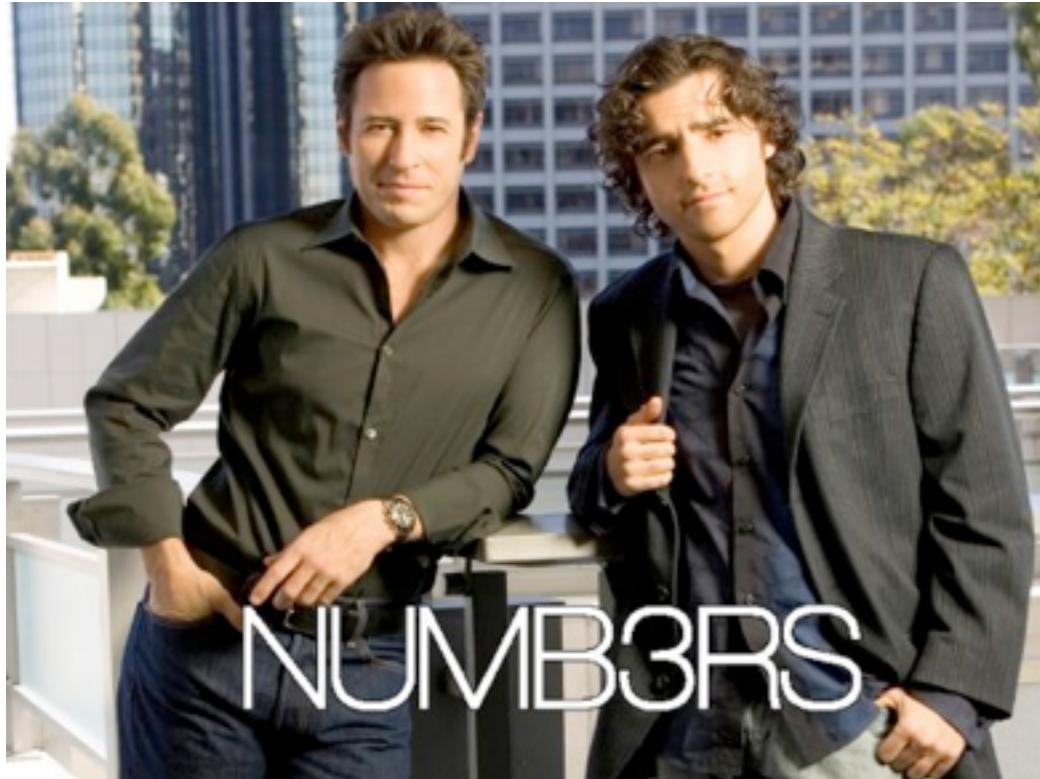


Prassi...





Prassi...





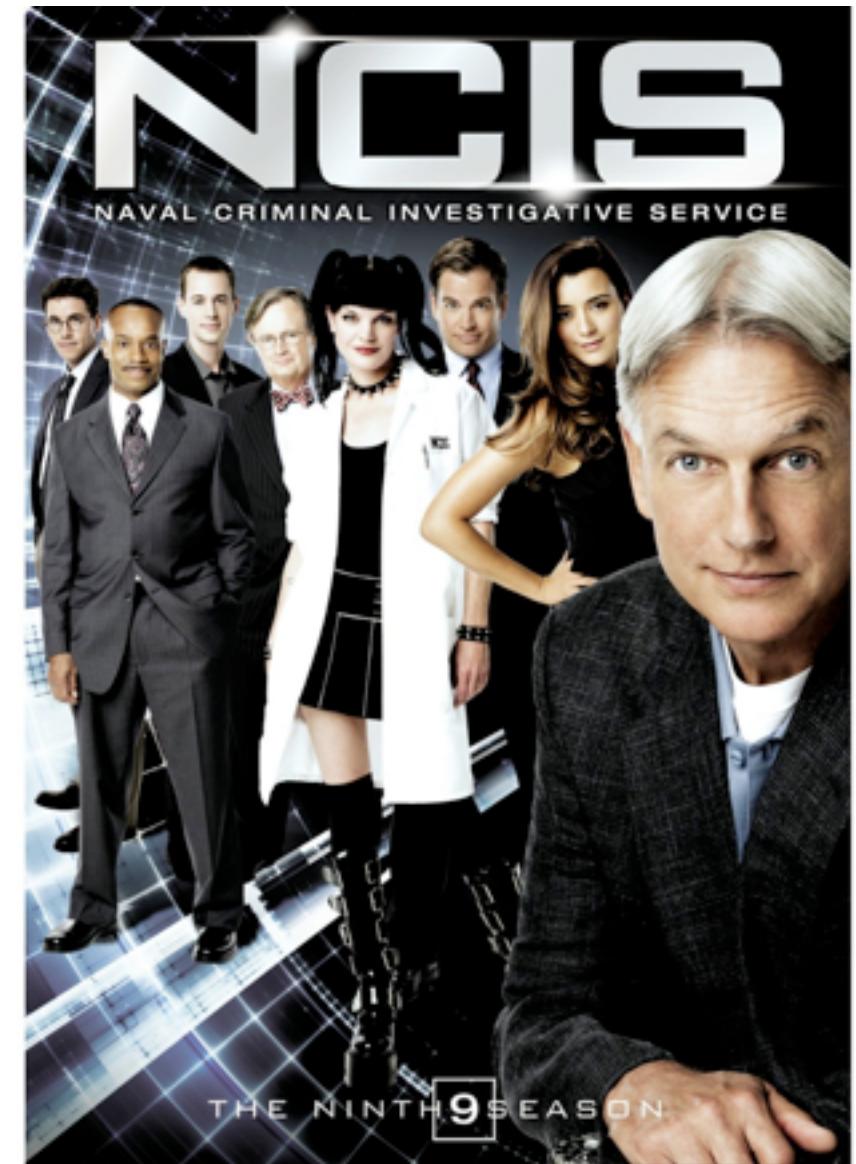
Visualroute?



Chi di voi lo usa per determinare la sorgente
di un attacco?



Forensics?



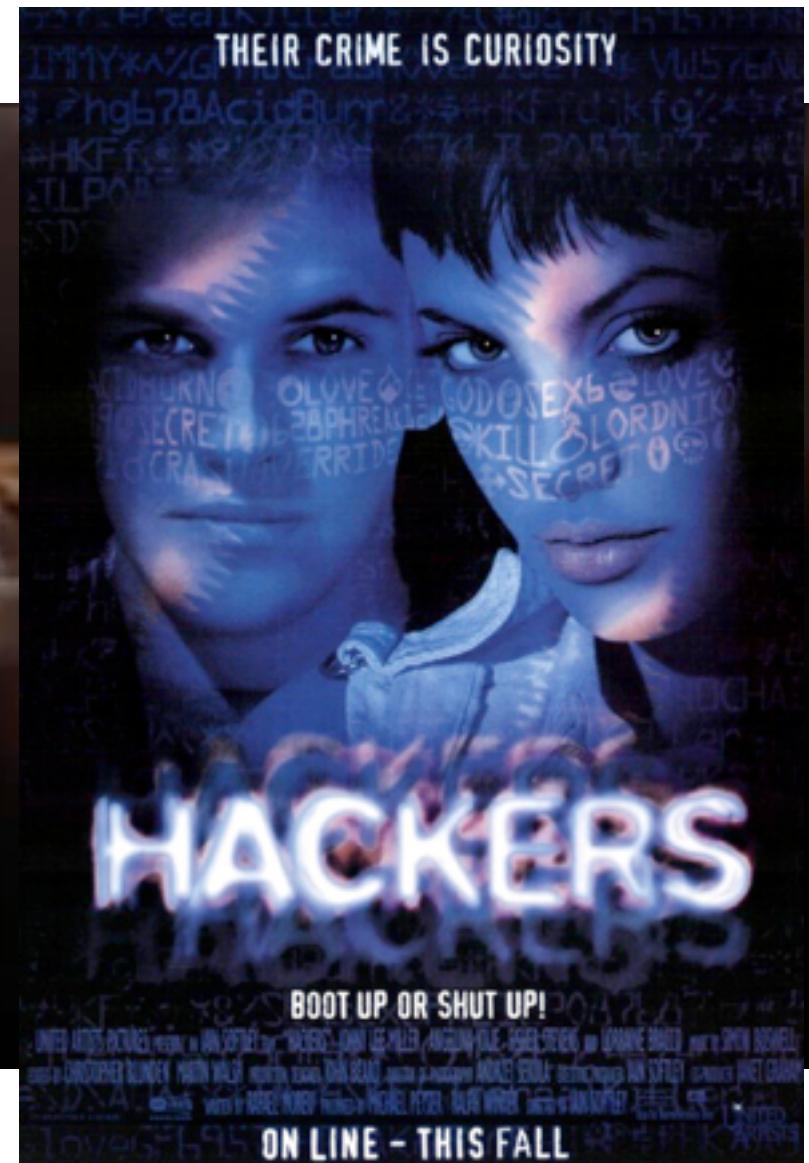


Reagire “velocemente”



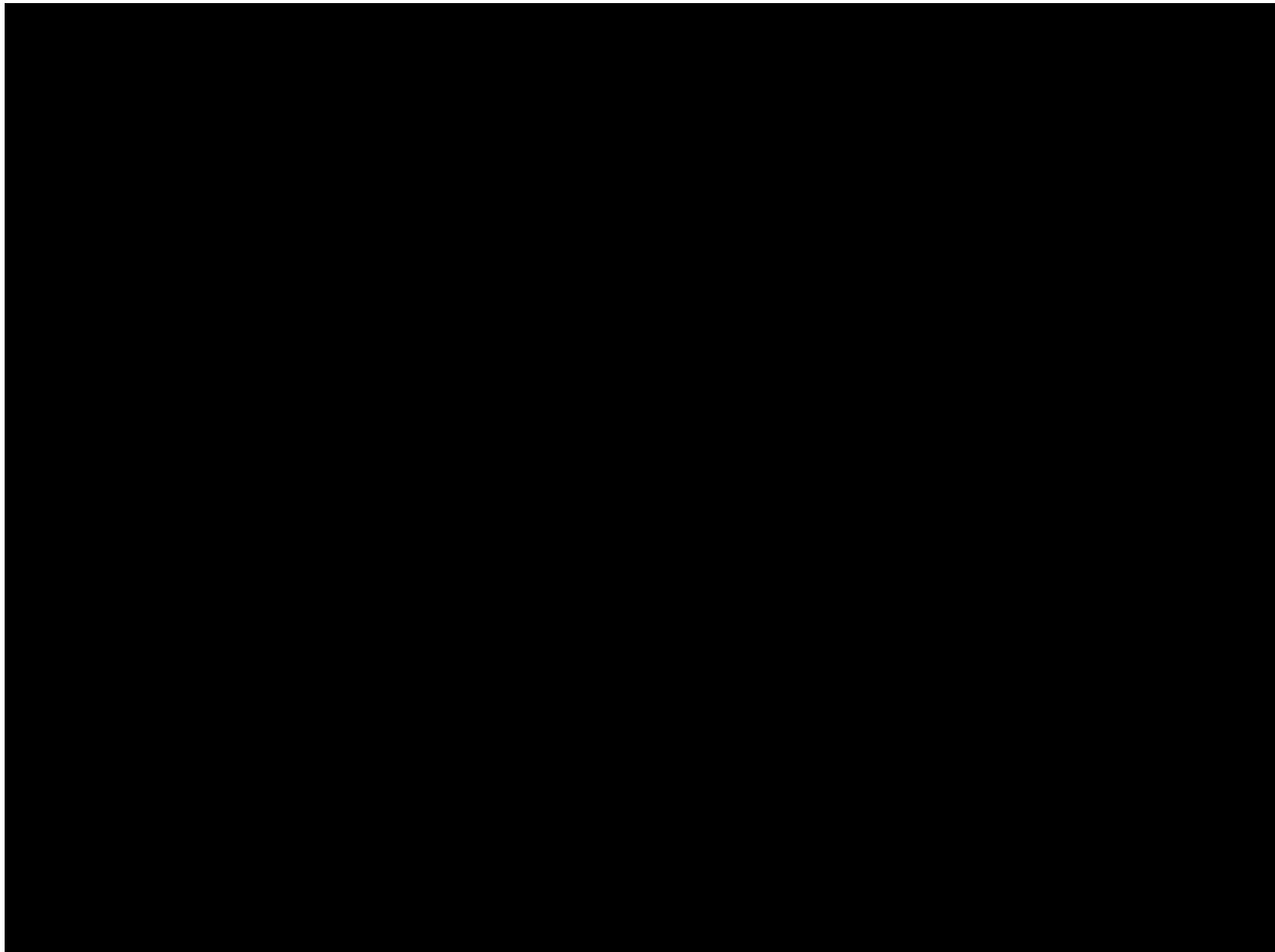


Le origini



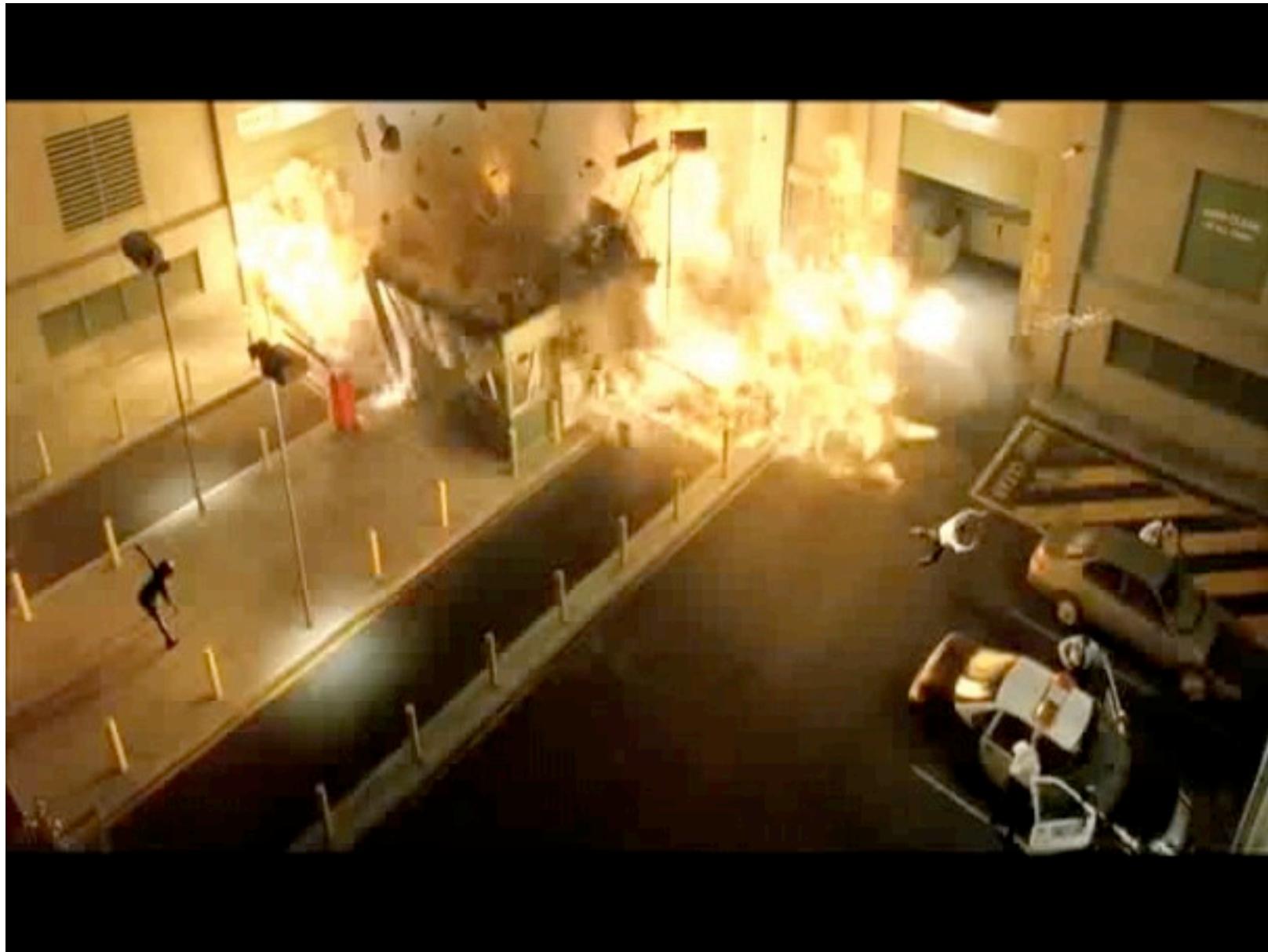


Matrix Reloaded





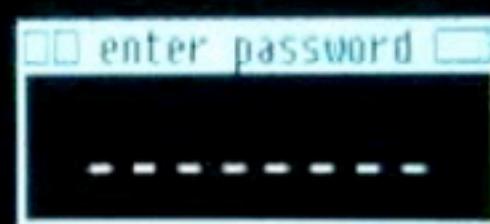
Physical Security





nmap

```
1 Port      State       Service
1 22/tcp    open        ssh
8
8 No exact OS matches for host
8
4 Nmap run completed - 1 IP address (1 host up) scanned
u # ssimuke 10.2.2.2 -rootpw="Z10H0101"
e Connecting to 10.2.2.2:ssh ... successful.
e Attempting to exploit SSHv1 CRC32 ... successful.
P Resetting root password to "Z10H0101".
System open: Access Level <9>
n # ssh 10.2.2.2 -l root
root@10.2.2.2's password: 
```





SSHv1 CRC32

```
1 Port      State      Service
1 22/tcp    open       ssh
8
8 No exact OS matches for host
8
8 Nmap run completed -- 1 IP address (1 host up) scanned
8 # sshnuke 10.2.2.2 -rootpw="210N0101"
e Connecting to 10.2.2.2:ssh ... successful.
e Attempting to exploit SSHv1 CRC32 ... successful.
P Resetting root password to "210N0101".
System open: Access Level <9>
n # ssh 10.2.2.2 -l root
root@10.2.2.2's password:  enter password
```

The terminal output shows the results of a Nmap scan, the execution of sshnuke, and a successful SSH session. A red box highlights the password reset command and the password entry field. An inset image shows a password entry dialog box with the placeholder 'enter password' and a masked password field.



Zoom?

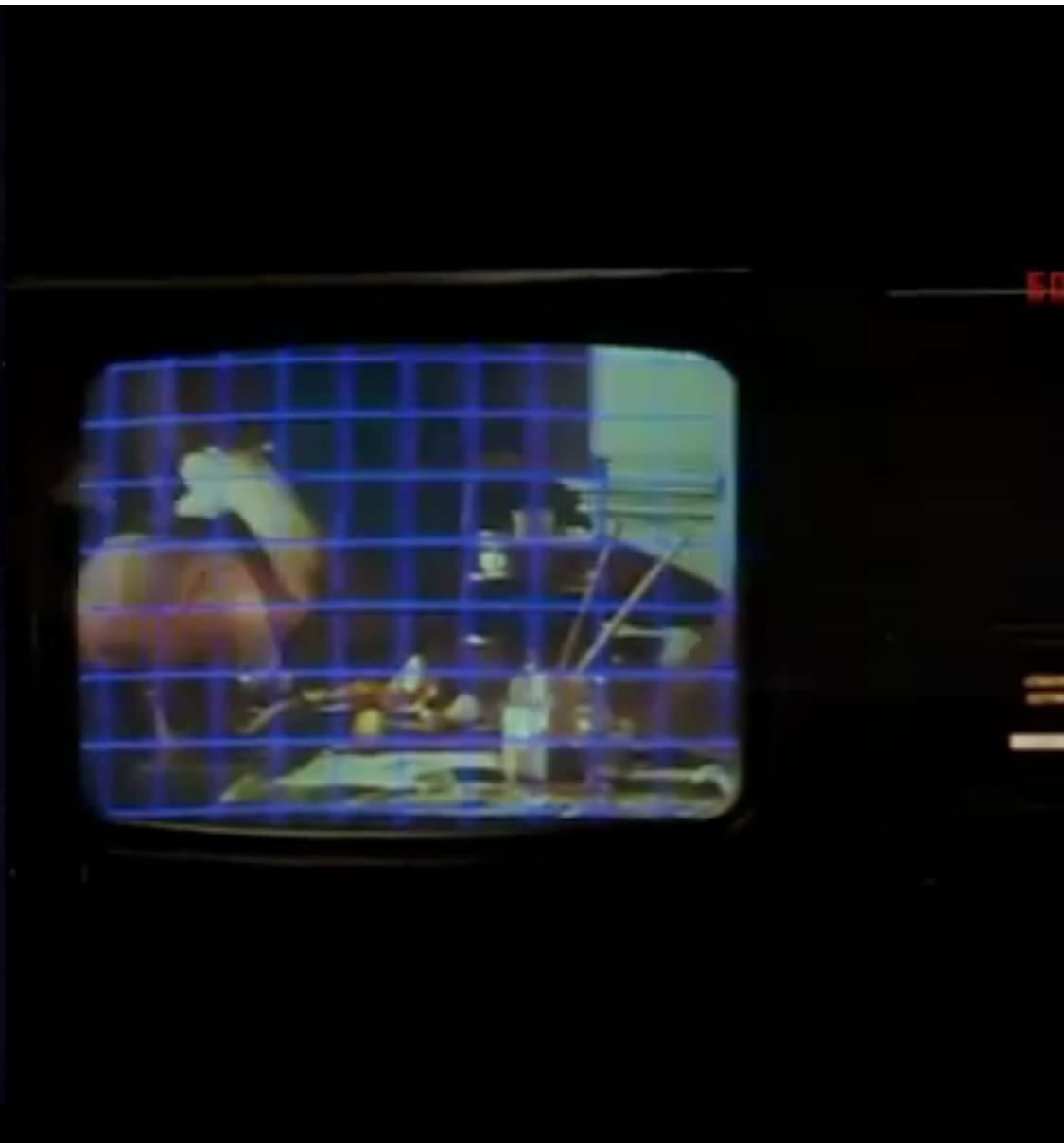
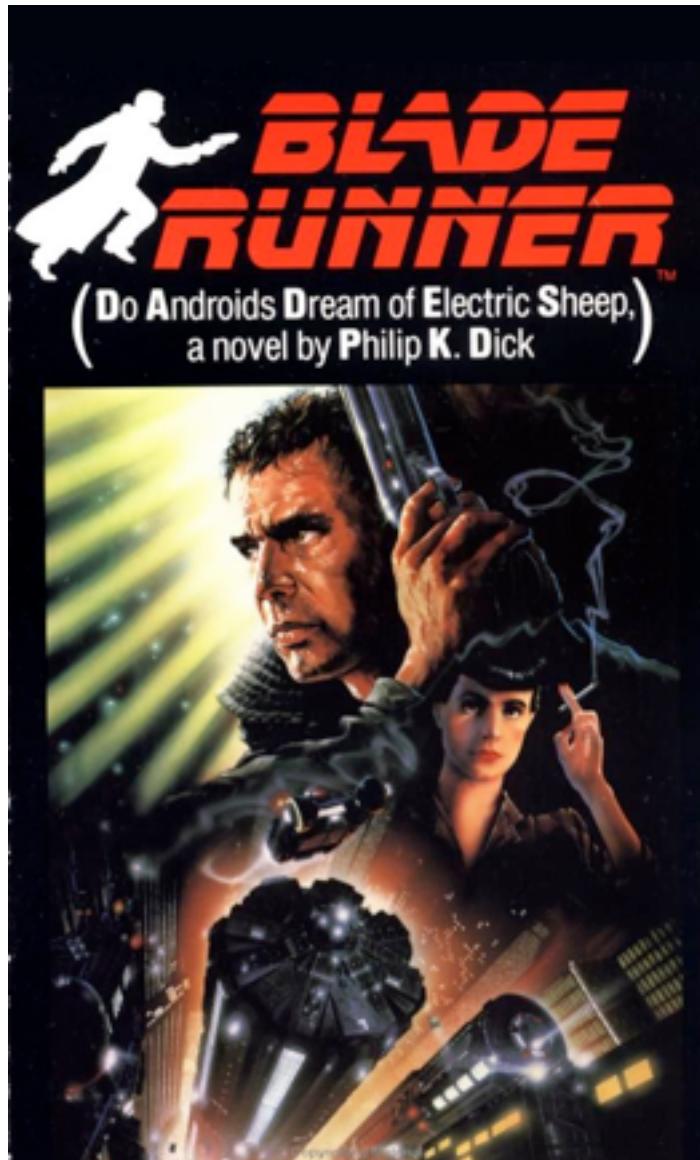




Zoomare con iPhone...

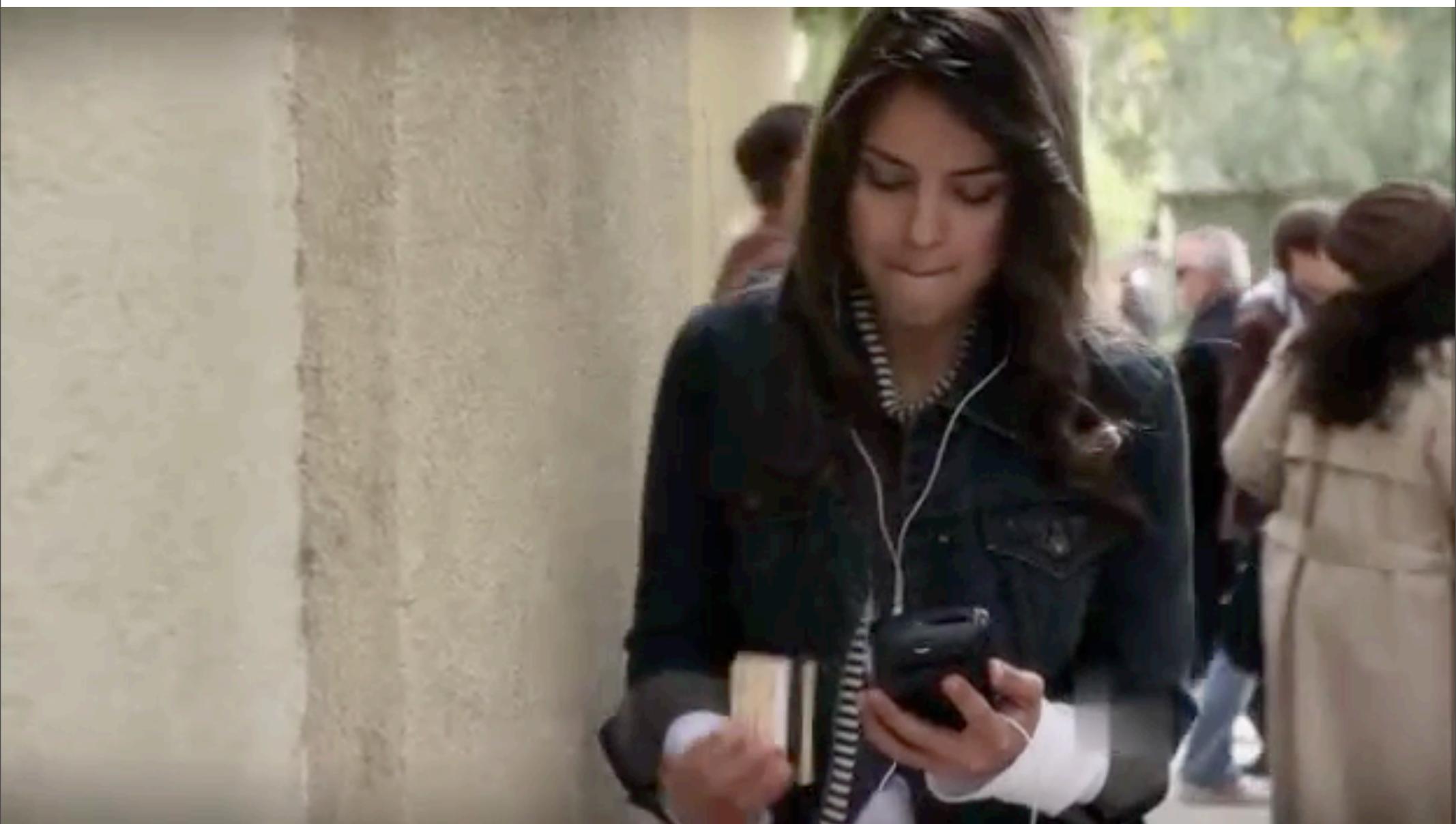


Le origini





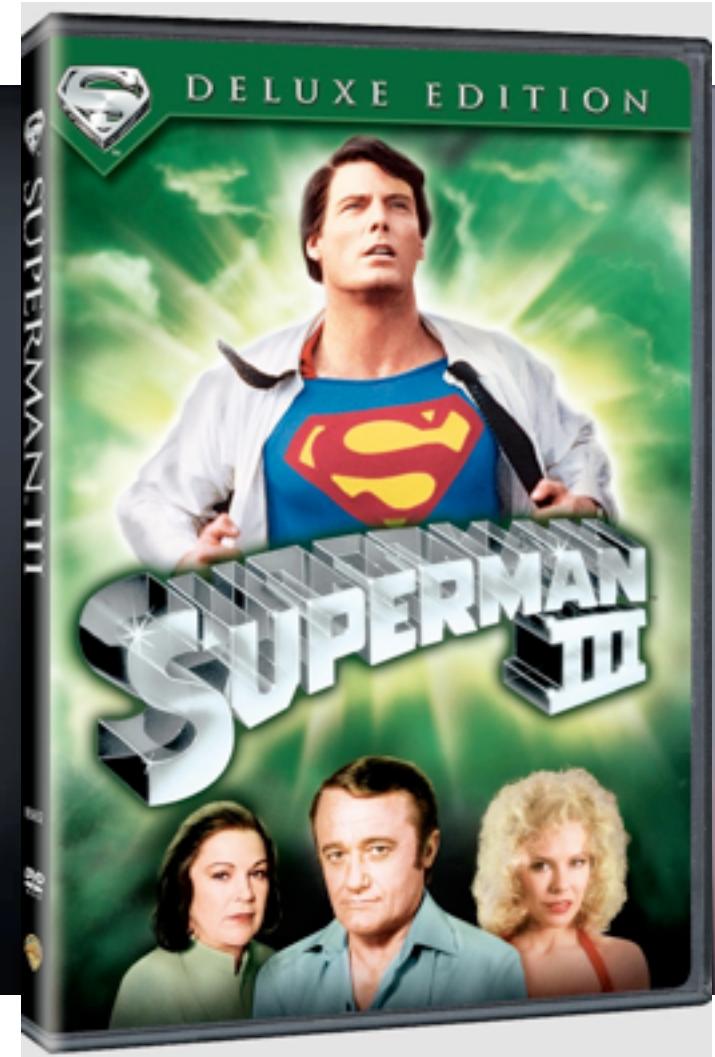
Rubare con NFC





Frodi

HELLO
WEBSOCE PAYROLL DIVISION
GIVE SECURITY CODE
OVERIDE ALL SECURI





Person of Interest

RECORDING

DATA RATE 757.48 GBS

CH1

CH2

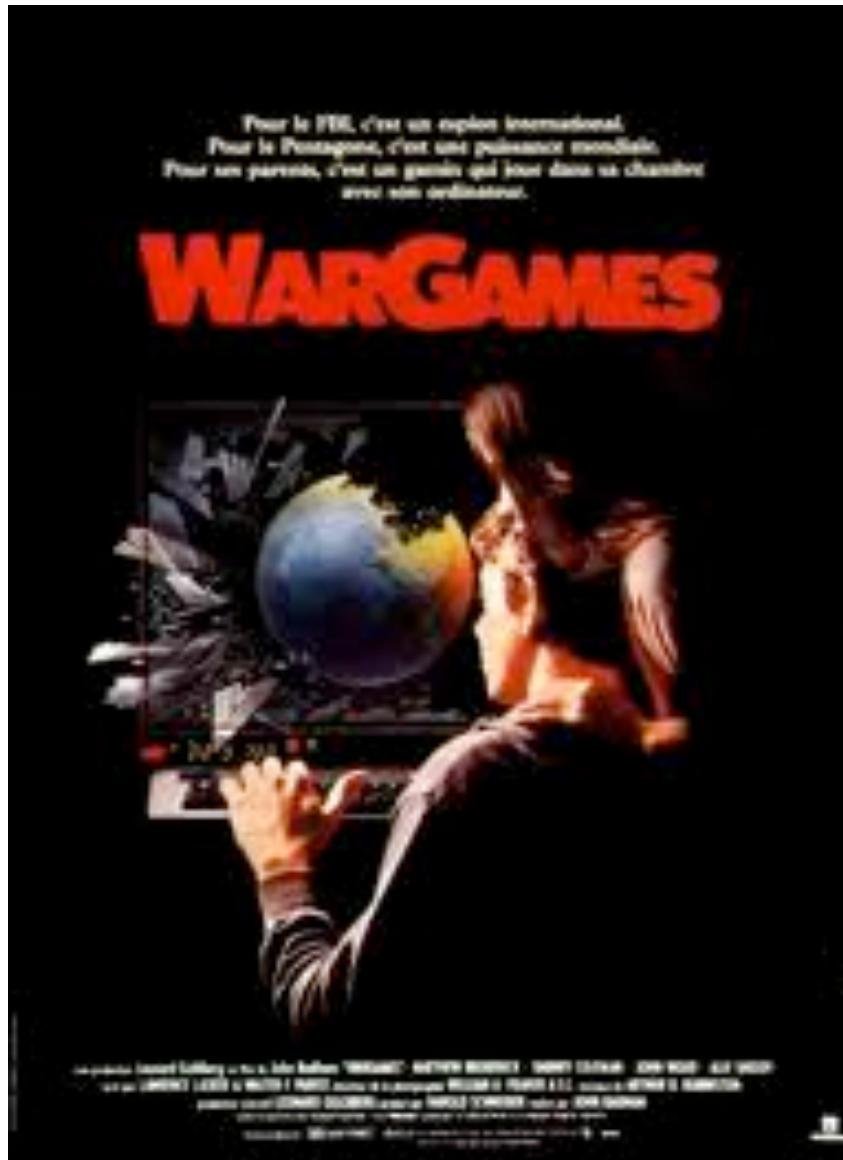


I social network





Il più realistico?





Wardialing

TO SCAN FOR CARRIER TONES, PLEASE LIST DESIRED AREA CODES AND PREFIXES					
A E PRFX NUMBER	AREA CODE PRFX NUMBER	A REA PRFX NUMBER	AREA CODE PRFX NUMBER	AREA CODE PRFX NUMBER	AREA CODE PRFX NUMBER
1) 399	(311) 437		(311) 767		



Gli hacker sono sexy?





Wardialing



⚠ Mai parlare della backdoor!



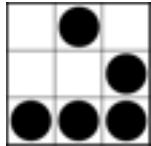


Economia “digitale”





La realtà?





Economia “reale”



The Associated Press

@AP



Following

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

3,146
RETWEETS

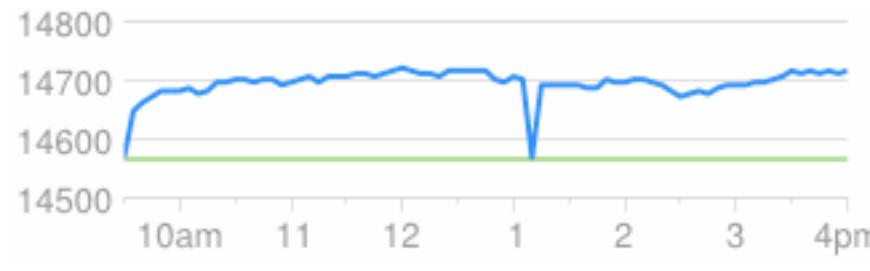
149
FAVORITES



Dow Jones Industrial Average 2 Minute
Dow Jones Indices: .DJI - Apr 23 4:37pm ET

1:07 PM - 23 Apr 13

14719.46 +152.29 (1.05%)



1d 5d 1m 6m 1y 5y max

Open	14567.17
High	14721.42
Low	14554.29
Volume	137,301,977
Avg Vol	N/A
Mkt Cap	N/A



SQL Injection

The screenshot shows a web browser window with the URL `sql.alba.st/index.php`. The page displays the **AIS Group** logo and the tagline "30 anni di esperienza al tuo servizio!". Below the logo is a login form titled "AUTENTICAZIONE UTENTI". The form has three fields: "SEDE" (dropdown menu set to "Verona"), "INTERNO" (text input field containing a value), and "PASSWORD" (text input field). A yellow "LOGIN" button is at the bottom. The "INTERNO" field is highlighted with a cursor, indicating it is the target for an injection attack. At the bottom of the page, there are links for **PROGECCO**, **Accord**, **ATTUA**, and **Alba**.

Video su SQL Injection



Altri rischi?

Posso interrogare il DB e ottenere tutti i dati contenuti:

```
' UNION ALL SELECT NULL,username,password,NULL FROM utenti WHERE 'x'='x
```



Password in cleartext

The screenshot shows a web browser window with the title "Sql Injection" and the URL "sql.alba.st/ricerca.php". The page header features the FIS Group logo and the tagline "30 anni di esperienza al tuo servizio!". Below the header, there are two search forms: "Ricerca di un numero di telefono" and "Chiamata di un numero di telefono". The "Ricerca di un numero di telefono" form includes an input field for "Inserire il nome:" and a "Ricerca" button. The "Chiamata di un numero di telefono" form includes an input field for "Inserire il numero/contatto skype:" and a "Chiama" button. At the bottom of the page, a note states: "I numeri preceduti da un asterisco (*) appartengono alla rubrica personale." followed by a table of contacts:

Nome	Cognome	Numero	Azione
* Mario	Rossi	045112233	Ch. Da
* Giuseppe	Verdi	098123	Ch. Da
* Paolo	Bianchi	01111234	Ch. Da
cyrax		superstrongpassword	Ch. Da
johndoe		cleartextpasswordaresafe	Ch. Da
admin		guest	Ch. Da



Come mi proteggo?

Evito di processare i caratteri speciali come ‘

Prevedo il processo che si chiama “normalizzare
l’input”



Cross site scripting

The screenshot shows a web browser window with the title bar "Sql Injection" and the URL "sql.alba.st/rubrica.php". The page content is from the "Albast" website, featuring the "Albast" logo at the top. Below it is a navigation link "[<< Pagina principale](#)". A red "Filtrra" button is prominently displayed. Below the button is a search form with fields for "Nome" and "Contiene", and buttons for "Invia" and "pulisci". A red "Gestione Rubrica" button is also present. At the bottom of the page are links for "Aggiungi Nuovo Contatto" and "Condividi rubrica", and a row of buttons for "Rag. Sociale", "N. Telefono", and "Cont. Skype". A red "[<< Pagina principale](#)" link is located at the very bottom. The overall layout is that of a standard web application's contact management section.

Video su XSS



Le informazioni



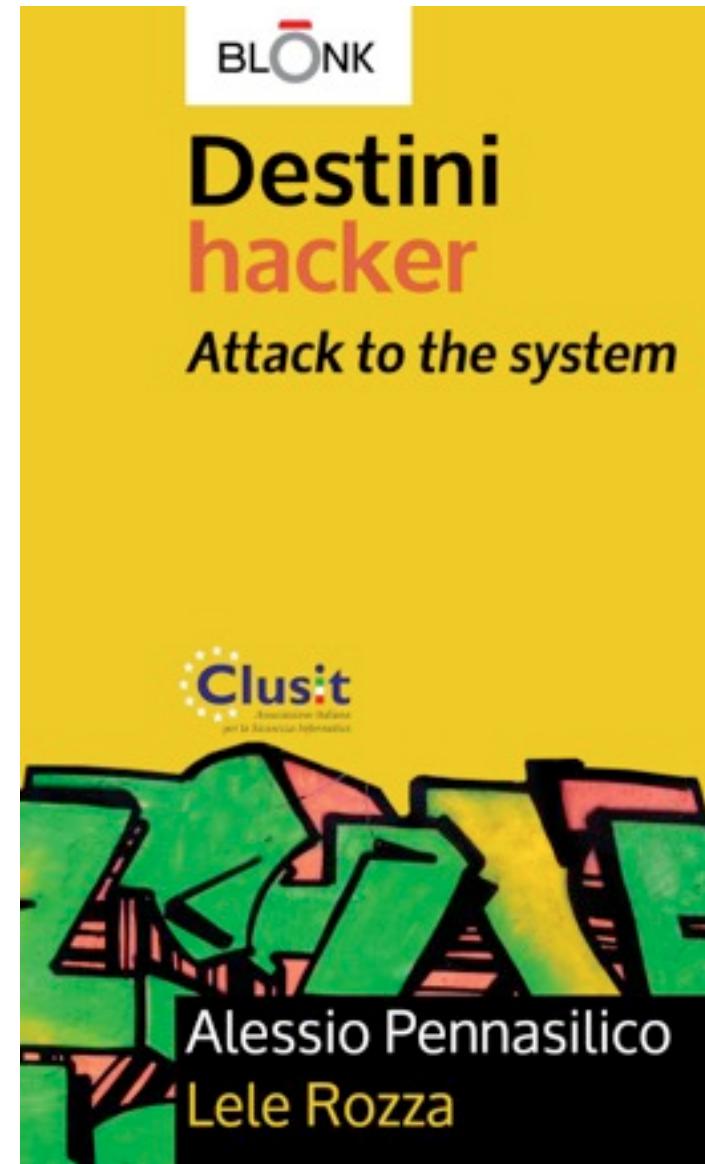


Lieto fine?



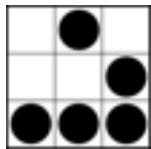


Awareness





Conclusioni





Tecnologia aliena?





Cosa dobbiamo affrontare?

Rischi

reali, concreti

semplici da trasformare in incidenti

alta probabilità di conversione in incidenti

grande impatto sul business

Rischi

facili da prevenire

difficili da mitigare a posteriori



Security by Design

Emergency exit



Se costruisco una casa
senza progettare
uscite di sicurezza
costruirle a lavori finiti
sarà disastroso



Grazie dell'attenzione!

Domande?

<http://www.alba.st/>
Verona, Milano, Roma
Phone/Fax +39 045 8271202



Alessio L.R. Pennasilico
a.pennasilico@alba.st

These slides are written by Alessio L.R. Pennasilico aka mayhem. They are subjected to Creative Commons Attribution-ShareAlike 2.5 version; you can copy, modify or sell them. "Please" cite your source and use the same licence :)