

Coding for Hackers

Andrea Draghetti



ERLUG



\$ whoami



Phishing Analysis and Contrast @ D3Lab



Team Member @ BackBox Linux



\$ Il coding è creatività e libertà

Il **Coding** non significa solo programmare al computer, ma imparare a pensare con metodo.

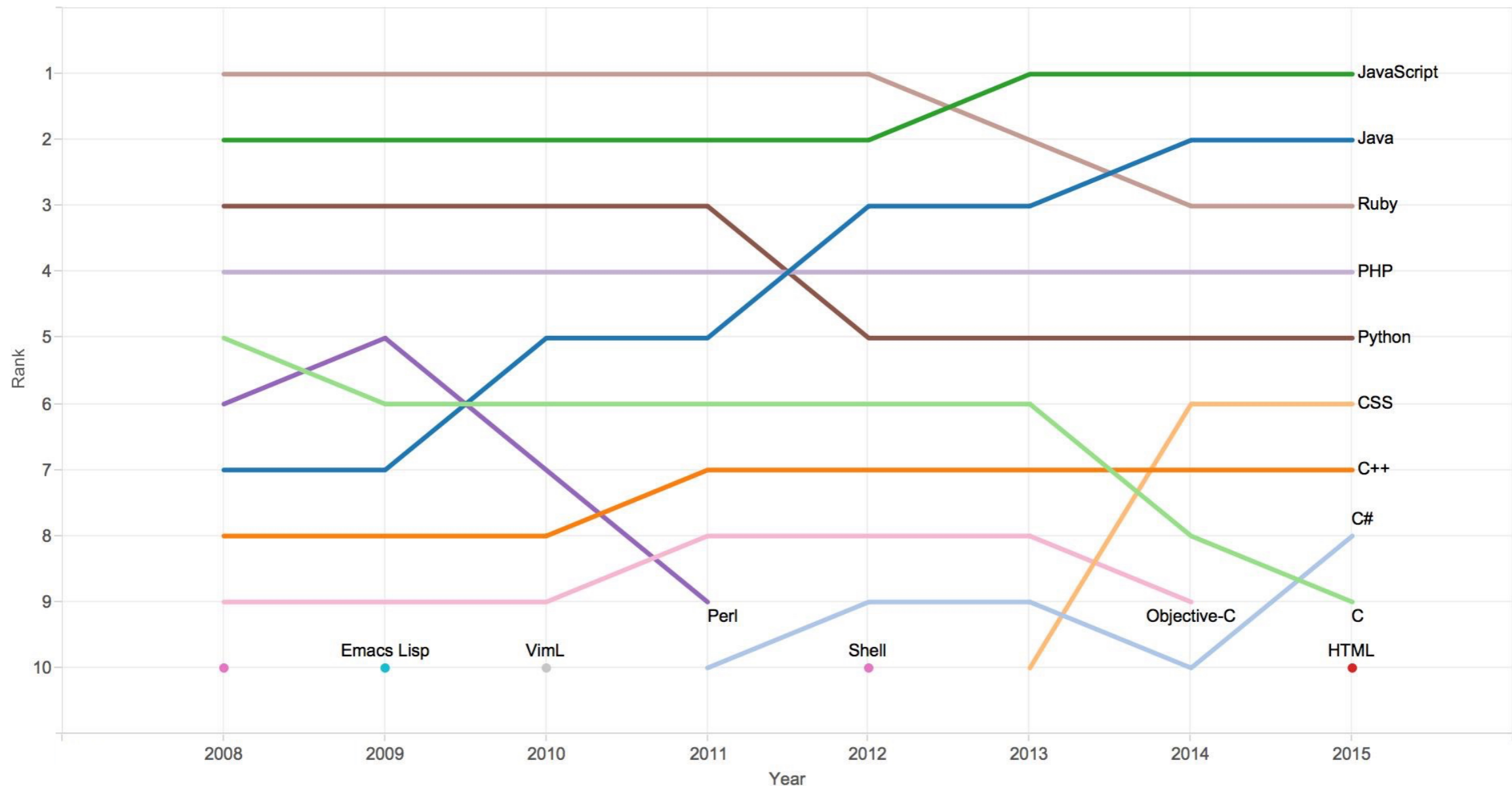
La libertà di immaginare o inventare qualcosa di nuovo.

Non è un talento ma una skill che può essere appresa.



\$ Top Languages in the World GitHub

Rank of top languages on GitHub.com over time

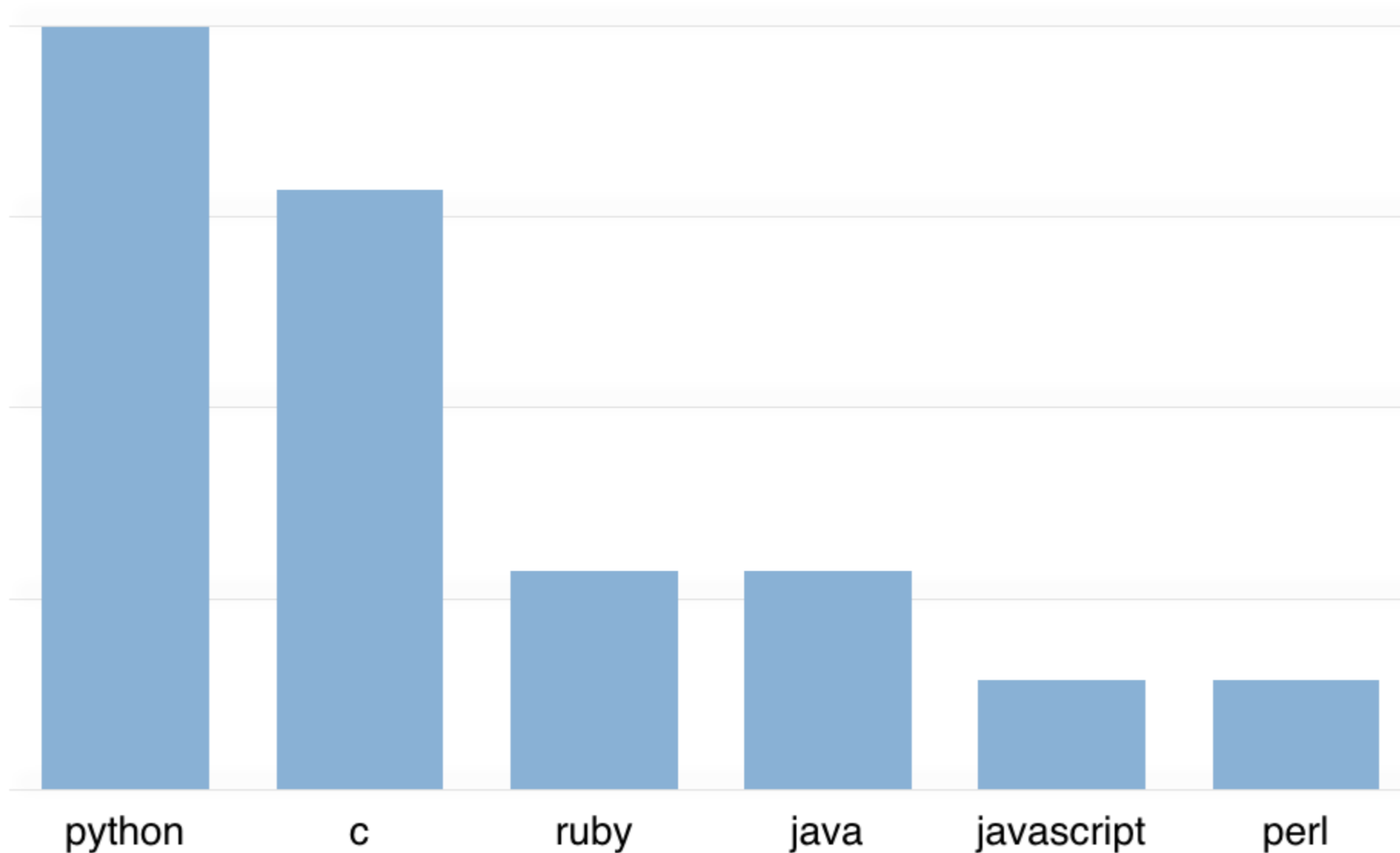


Source: GitHub.com

Open and Closed Source



\$ Top Languages for Hackers



Dati rilevati sui software Open Source inclusi in BackBox Linux



\$ Perché Python?

Free

Semplice

Collaborativo

Open Source

Trasportabile

Esprime il concetto di **Creatività** e **Libertà** del **Coding!**



\$ Indentazione ... ♥

```
if persona.anni < 18:
    print "Accesso negato"
    accesso = False
elif persona.anni > 80:
    print "Non è il caso..."
    accesso = False
else:
    accesso = True
    if persona.isUomo():
        print "Benvenuto"
    else:
        print "Benvenuta"
return accesso
```

```
if (persona.anni < 18) {
    printf("Accesso negato\n");
    accesso = 0; } else if (persona.anni > 80) {
    printf("Non è il caso...\n");
    accesso = 0; } else { accesso = -1;
    if (persona.isUomo == -1)
        printf("Benvenuto\n"); else
        printf("Benvenuta\n");} return(accesso);
```

Fonte: "Programmare in Python (Beri, Marco)"



\$ Indentazione ... ♥

```

if persona.anni < 18:
    print "Accesso negato"
    accesso = False
elif persona.anni > 80:
    print "Non è il caso..."
    accesso = False
else:
    accesso = True
    if persona.isUomo():
        print "Benvenuto"
    else:
        print "Benvenuta"
return accesso
    
```

```

if (persona.anni < 18) {
    printf("Accesso negato\n");
    accesso = 0; } else if (persona.anni > 80) {
    printf("Non è il caso...\n");
    accesso = 0; } else { accesso = -1;
    if (persona.isUomo == -1)
        printf("Benvenuto\n"); else
        printf("Benvenuta\n");} return(accesso);
    
```

Fonte: "Programmare in Python (Beri, Marco)"



\$ Hacker = Coding?! Are you sure?

L'Hacker accumula un insieme di tecniche e conoscenze per accedere e modificare un sistema Software o Hardware.

Un Hacker è in grado di aprirsi un varco nel codice, di riscriverlo riducendo la lunghezza e migliorandone la struttura. Ma è anche quella personalità che scrive codice per il solo gusto di riuscirci, per vedere una sua idea elaborare correttamente nel processore del computer.

L'Hacker NON è quella persona che fa due click su un software per “rubare” le credenziali dell'amico.



\$ SQL Map - Automatic SQL Injection

```

$ python sqlmap.py -u "http://172.16.120.130/sqlmap/mysql/get_int.php?id=1" --batch
[1.0.0.15#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsi
ble for any misuse or damage caused by this program

[*] starting at 21:00:27

[21:00:27] [INFO] testing connection to the target URL
[21:00:27] [INFO] heuristics detected web page charset 'ascii'
[21:00:27] [INFO] testing if the target URL is stable
[21:00:28] [INFO] target URL is stable
[21:00:28] [INFO] testing if GET parameter 'id' is dynamic
[21:00:28] [INFO] confirming that GET parameter 'id' is dynamic
[21:00:28] [INFO] GET parameter 'id' is dynamic
[21:00:28] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[21:00:28] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting attacks
[21:00:28] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [
Y/n] Y
[21:00:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:00:28] [WARNING] reflective value(s) found and filtering out
[21:00:28] [INFO] GET parameter 'id' seems to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[21:00:28] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[21:00:28] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause' injec
table
[21:00:28] [INFO] testing 'MySQL inline queries'
[21:00:28] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT - comment)'
[21:00:28] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[21:00:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT)'
[21:00:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[21:00:29] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[21:00:29] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[21:00:29] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[21:00:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[21:00:39] [INFO] GET parameter 'id' seems to be 'MySQL >= 5.0.12 AND time-based blind (SELECT)' injectable
[21:00:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'

```



\$ Zenmap - Nmap Security Scanner GUI

Scansione Strumenti Profilo Aiuto

Obiettivo: 213.254.12.146 Profilo: Quick scan Scansione Annulla

Comando: nmap -T4 -F 213.254.12.146

Hosts Servizi

SO	Host
	picard.linux.it (213.254.12.146)

Nmap output Porte / Hosts Topologia Dettagli host Scansioni

nmap -T4 -F 213.254.12.146

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-21 22:56 CEST
Nmap scan report for picard.linux.it (213.254.12.146)
Host is up (0.064s latency).
Not shown: 88 closed ports
PORT      STATE SERVICE
13/tcp    open  daytime
22/tcp    open  ssh
25/tcp    open  smtp
37/tcp    open  time
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
```

Dettagli

Filtra host



\$ Knock Subdomain Scan

```

Terminale - drego85@backbox: ~ (su backbox)
File Modifica Visualizza Terminale Schede Aiuto
drego85@backbox:~$ knockpy linux.it
Target information linux.it

Ip Address      Target Name
-----
: unknown linux.it
press [c] to continue to scan or [enter] to exit: c
Code           Reason
-----
Field          Value
-----

Loaded local wordlist with 1905 item(s)

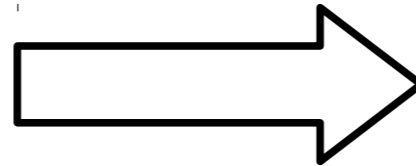
Getting subdomain for linux.it

Ip Address      Domain Name
-----
213.254.12.148  abc.linux.it
213.254.12.148  sulu.linux.it
77.43.112.34    ar.linux.it
213.92.8.5      dsl.linux.it
213.92.8.5      vlad-tepes.bofh.it
213.92.8.5      ftp.linux.it
213.92.8.5      vlad-tepes.bofh.it
85.94.204.146   gopher.linux.it
85.94.204.146   attila.bofh.it
213.92.8.5      irc.linux.it
213.92.8.5      vlad-tepes.bofh.it
213.254.12.146  lists.linux.it
    
```



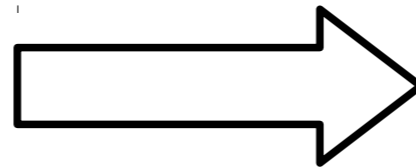
\$ Mondo Commerciale vs Open Source e Free

Nessus Vulnerability Scanner
Nexpose



OpenVAS

Burp Suite



Zed Attack Proxy



GRAZIE!

**Le slides e le riprese audio/video
dell'intervento saranno disponibili su:
<http://erlug.linux.it/linuxday/2016/>**



CC BY-SA 3.0 IT

