Web Pentest 101

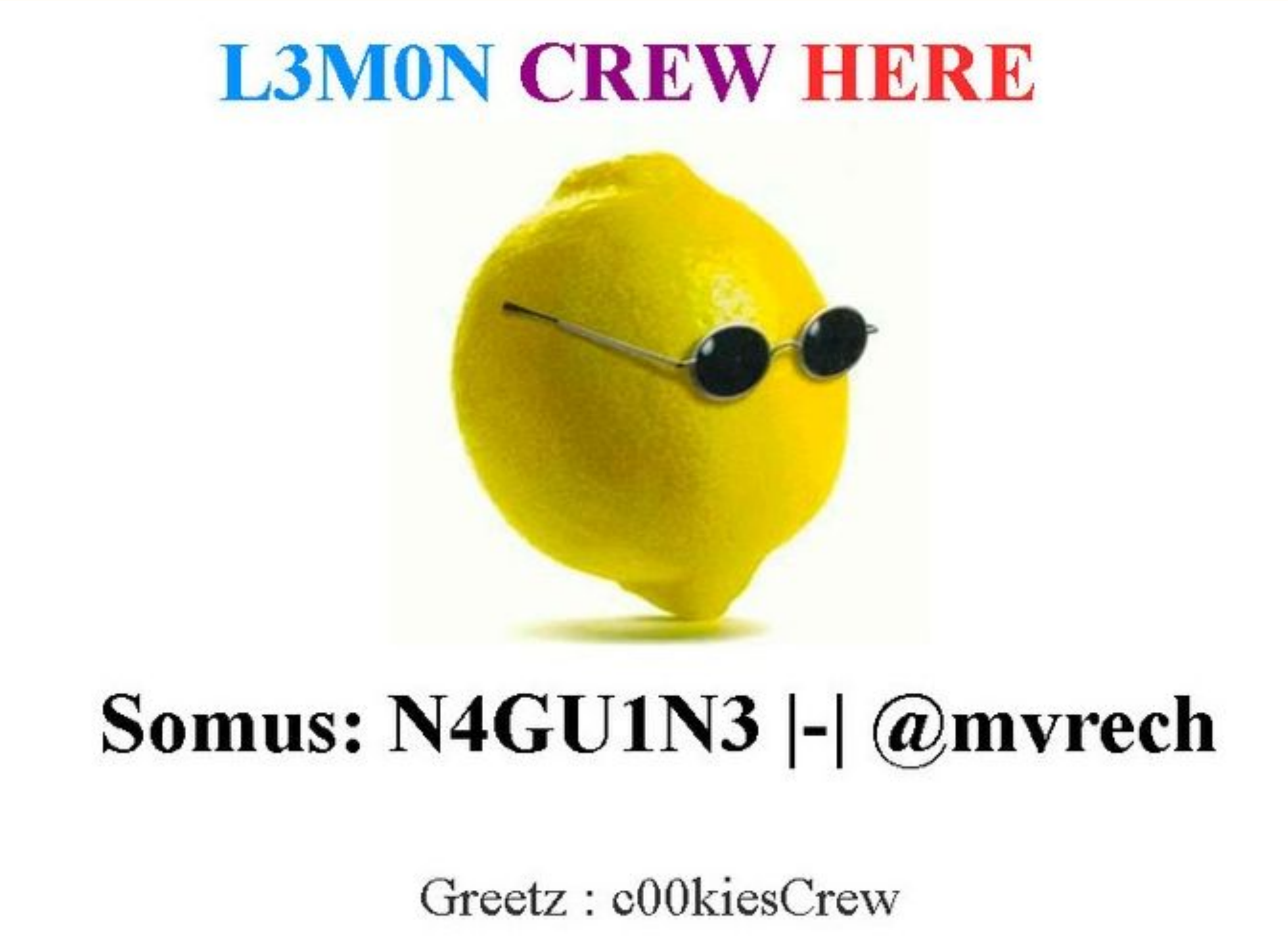
from abrasax to /dev/null

0x04: Defacement

Join the blackhat (noobie) force

- What is it
- Why people do it
- Post-exploitation
  - Web shells
  - Botnets
- What else can be done
- You never was there

Defacement what?



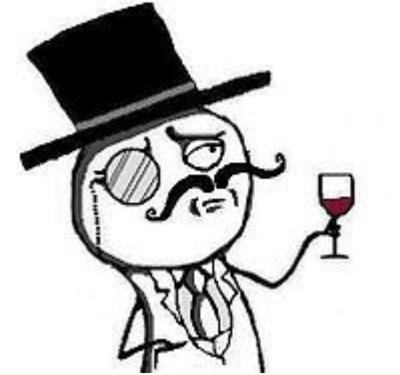
L3M0N CREW HERE

Somus: N4GU1N3 |-| @mvrech

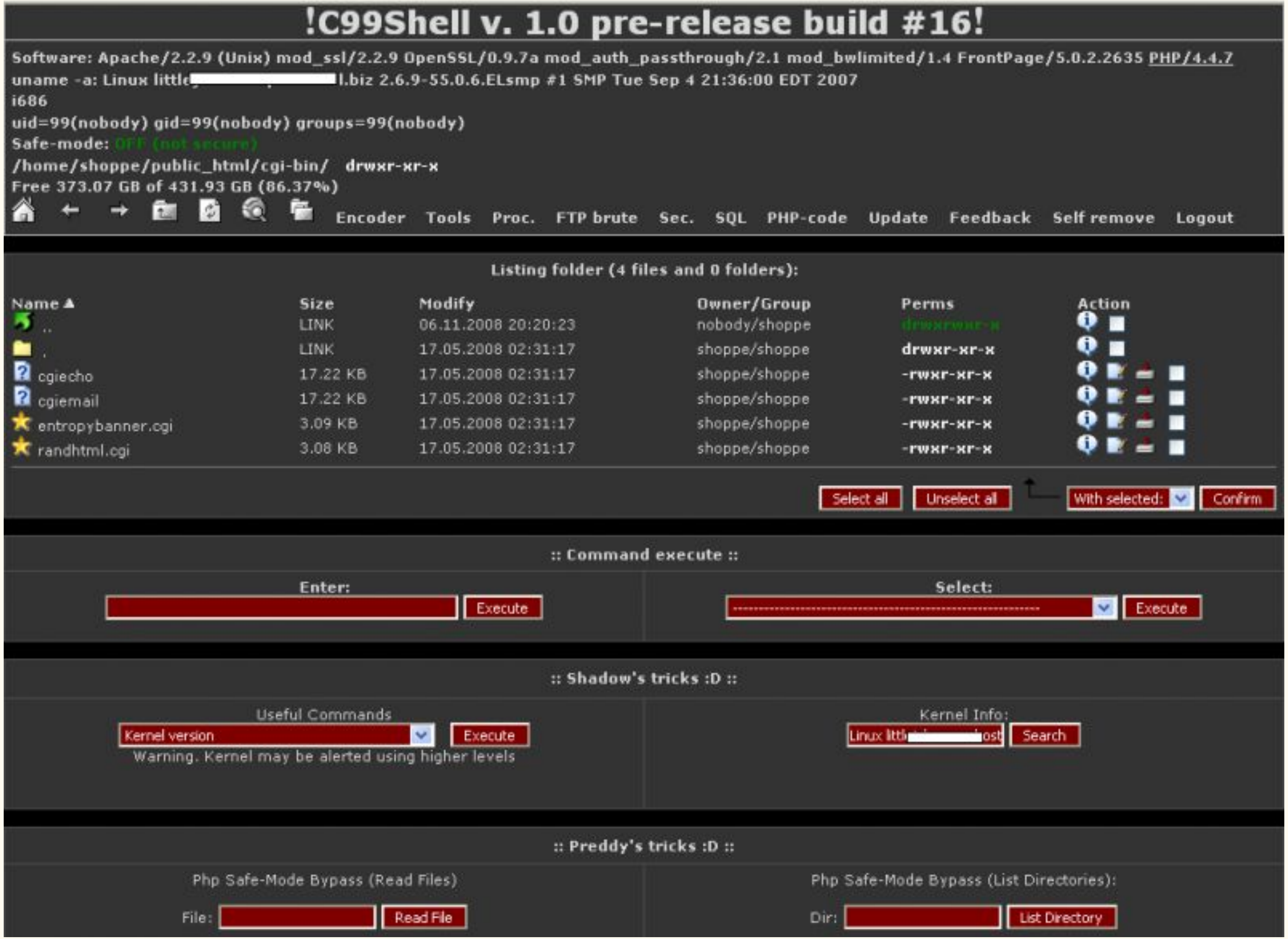
Greetz : c00kiesCrew

Why people do deface

- Protests
  - Anonymous
  - Lulzsec
- Power
  - Crews
  - Newbies
- Attention
  - Kids
    - me
- Damage
  - Enterprises



Web shells



!C99Shell v. 1.0 pre-release build #16!

```
Software: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/4.4.7
uname -a: Linux little[redacted]l.biz 2.6.9-55.0.6.ELsmp #1 SMP Tue Sep 4 21:36:00 EDT 2007
i686
uid=99(nobody) gid=99(nobody) groups=99(nobody)
Safe-mode: OFF (not secure)
/home/shoppe/public_html/cgi-bin/   drwxr-xr-x
Free 373.07 GB of 431.93 GB (86.37%)
```

Listing folder (4 files and 0 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
..	LINK	06.11.2008 20:20:23	nobody/shoppe	drwxrwxr-x	□
.	LINK	17.05.2008 02:31:17	shoppe/shoppe	drwxr-xr-x	□
cgiecho	17.22 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	□
cgiemail	17.22 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	□
entropybanner.cgi	3.09 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	□
randhtml.cgi	3.08 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	□

:: Command execute ::

:: Shadow's tricks :D ::

Useful Commands: Kernel version

Warning. Kernel may be alerted using higher levels

Kernel Info: Linux littl[redacted]ost

:: Preddy's tricks :D ::

Php Safe-Mode Bypass (Read Files)

Php Safe-Mode Bypass (List Directories):

How it happens?

- We already know some methods to get access to restricted pages like admin dashboard
- But, how to get TOTAL access into the server?

- We can write new recipes, but it’s not enough, we need to change entire pages, run programs and get a linux shell to have a more complex access. But how?

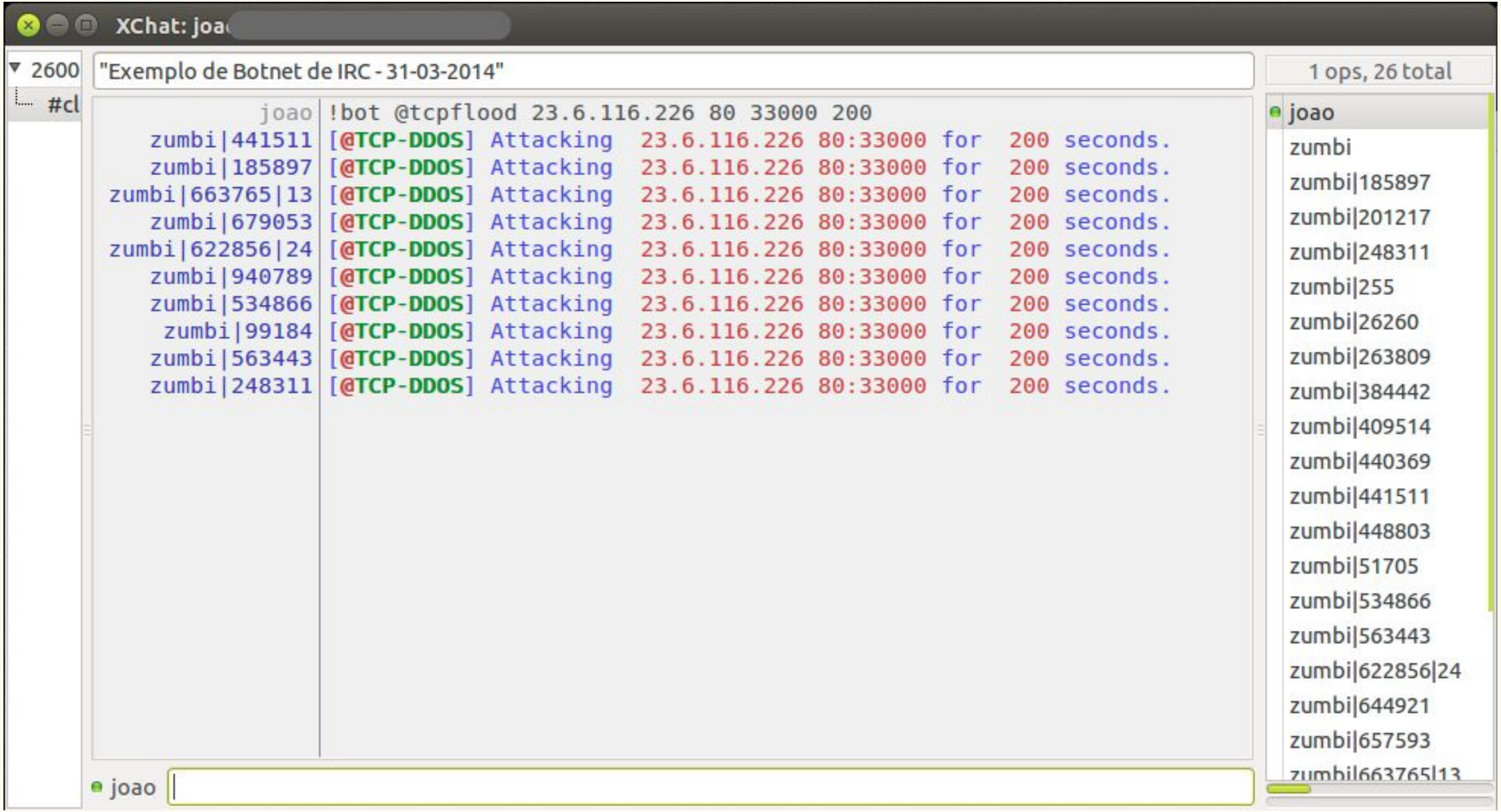
Shell upload

- The main way to get better access to the system is to find a field where administrators are allowed to upload photos, or other kind of documents. The challenge (in major cases not so challenging) is to upload a php shell (or asp) in a field that only accept image types or other kind of documents
- Of course, is not the only way, some good practices is to try the same user and password in ftp server or ssh server
- All this methods will be teached in other class designed only for this purpose
- Once you have a shell you can upload other kind of files such as programs and bots

Bots

Botnets

- A server is anything but a computer
- So you can upload programs that execute like in your computer
- As in your computer, you can execute programs that you can understand, so, you only can execute php if you have apache or some server that understand php (or php in your computer)
- So, many times you should be able to execute perl or python, not only php
- Just upload the file and execute as a shell
- So, as in your computer, you can execute commands, mine crypto coins or even try to access a website so many times that he won't be able to answer anyone for a while
- This servers are even better for this because sometimes they have a powerful internet to attack others systems, and more capability of process to mine crypto coins
- So people start to upload programs that put all website they hacked into the same irc channel or any other communication channel.



XChat: joa[redacted]

▼ 2600
#cl

"Exemplo de Botnet de IRC - 31-03-2014"

1 ops, 26 total

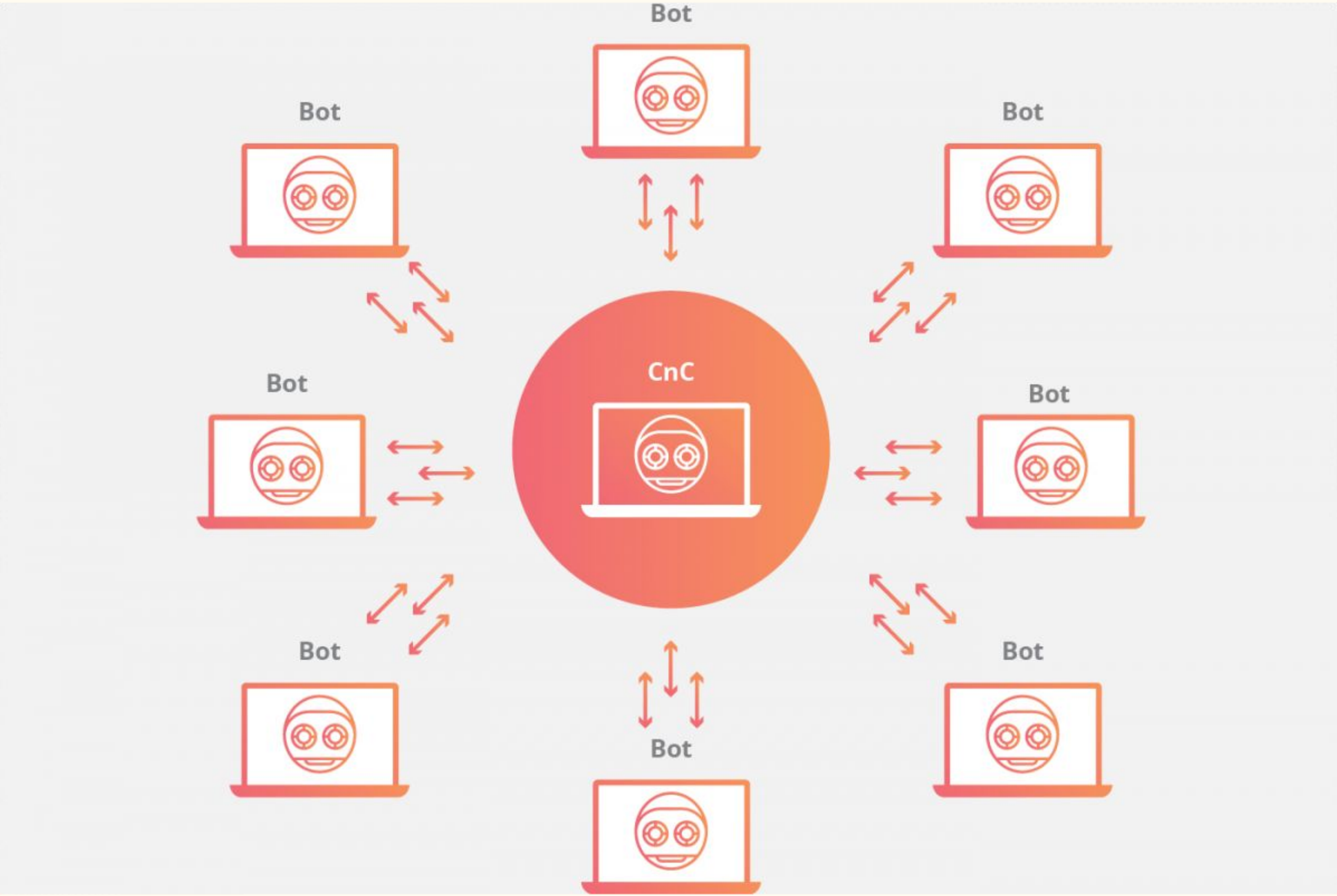
```
         joao !bot @tcpflood 23.6.116.226 80 33000 200
 zumbi|441511 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
 zumbi|185897 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
zumbi|663765|13 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
 zumbi|679053 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
zumbi|622856|24 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
 zumbi|940789 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
 zumbi|534866 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
  zumbi|99184 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
 zumbi|563443 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
 zumbi|248311 [@TCP-DDOS] Attacking  23.6.116.226 80:33000 for  200 seconds.
```

● joao
zumbi
zumbi|185897
zumbi|201217
zumbi|248311
zumbi|255
zumbi|26260
zumbi|263809
zumbi|384442
zumbi|409514
zumbi|440369
zumbi|441511
zumbi|448803
zumbi|51705
zumbi|534866
zumbi|563443
zumbi|622856|24
zumbi|644921
zumbi|657593
zumbi|663765|13

● joao

Botnets

- In this way they build entire networks of zumbi machines to perform more powerful attacks, execute massive or directed commands, perform spam, and things like that
- The place where the attackers control the bots is called command and control or C&C
- Some bots help hackers to automatize theirs attacks searching for more vulnerable websites


Bot
Bot
Bot
CnC
Bot
Bot
Bot
Bot
Bot
Bot

What else?

What else you want to

- Sometimes the server host a lot of websites, but each website has only permission to execute in it’s paste, so, if you find any vulnerability to get ROOT access in the server, you can use it’s full power or even deface each website of this server
- Some people hack servers to send SPAM, we call this programs mailers, they send the same message for a large number of emails, generally this contains spam to steal bank credentials
- Also sometimes (people don’t do this anymore) developers store user personal data like credit cards in the system database, this lead to more credit cards stolen
- If you can’t upload a shell, but can write in places like the index and also insert javascript you could change all the html and deface the page without get full access. Or redirect the page to one server that belongs to you with a pwned page
- If it is a site with a large amount of visitations you can insert javascript that use visitors computers to mine some crypto coins and make money
- And what else you can imagine
- Also, there is a site where people who defaces display their attacks, it’s called zone-h and they take like a picture of the actual state of the site, to comprove that you owned it once the admin fix the issue

To finish this section

- Remember to maintain only the necessary files in the server to not be detected so easy
- Some servers has their own protection systems, like anti-hackers. So many old php shells are detected by them and deleted, also, they alert the system administrator about the hack, so, use original and the more common possible code
- If you get root always remove your logs
- And the most important, always use proxy