Intermediate Metasploit

d4rkm4tter

whoami

BS in Computer Science from SUU

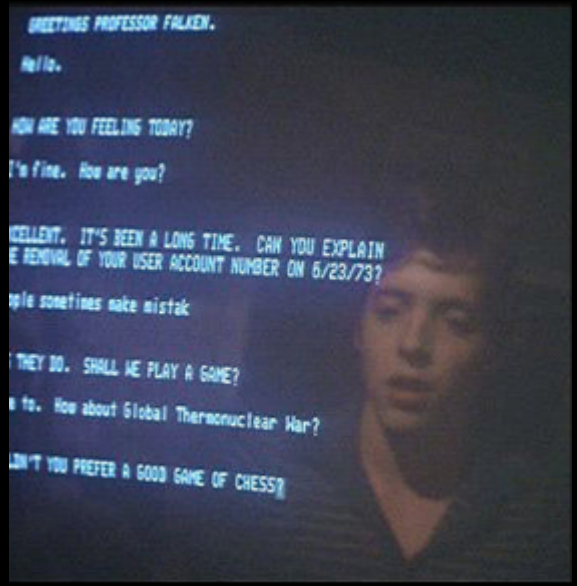
I hack stuff and sometimes get paid for it

I hang out with #dc801

Long history with *nix systems

Regularly compete in CTF competitions

(Defcon’s Qualifier starts May 16th @ 6:00 pm)



Disclaimer

Don’t do stuff you’re not supposta

Don’t be chaotic evil, be lawful evil

Yes these tools can do real damage, don’t be dumb

Don’t blame me because you are giving up your rights by listening to me

Any names or things referenced in this presentation are fiction and not any real person or thing

More Warnings

Most exploits works by crashing threads or processes.

Bad things will happen so expect this behavior, or don’t exploit.

Some MSF Basics

How to get help? msf> help [command]

More help? msf> [command] -h

Autocomplete is your friend! <TAB> everything!

MSF Directory on Kali - /usr/share/metasploit-framework

More Basics

msf> db_status

Kali doesn't start MSF nor Postgresql on boot

service postgresql start && service metasploit start

msf> db_rebuild_cache

More More Basics

Directory Structure:

auxiliary/[type]/[application]/[name]

encoder/[architecture]/[name]

exploits/[OS]/[type]/[exploit_name]

payload/[OS]/[architecture]/[meterpreter||shell_name]

nop/[architecture]/[name]

post/[OS]/[type]/[name]

Less More Basics

Example usage:

```
msf> use auxiliary/scanner/discovery/udp_probe
msf> use encoder/x86/alpha_upper
msf> use exploit/windows/smb/ms08_067_netapi
msf> set PAYLOAD windows/meterpreter/reverse_tcp
```

Less Basics

msf> workspace

msf> search [keywords]

msf> use [module]

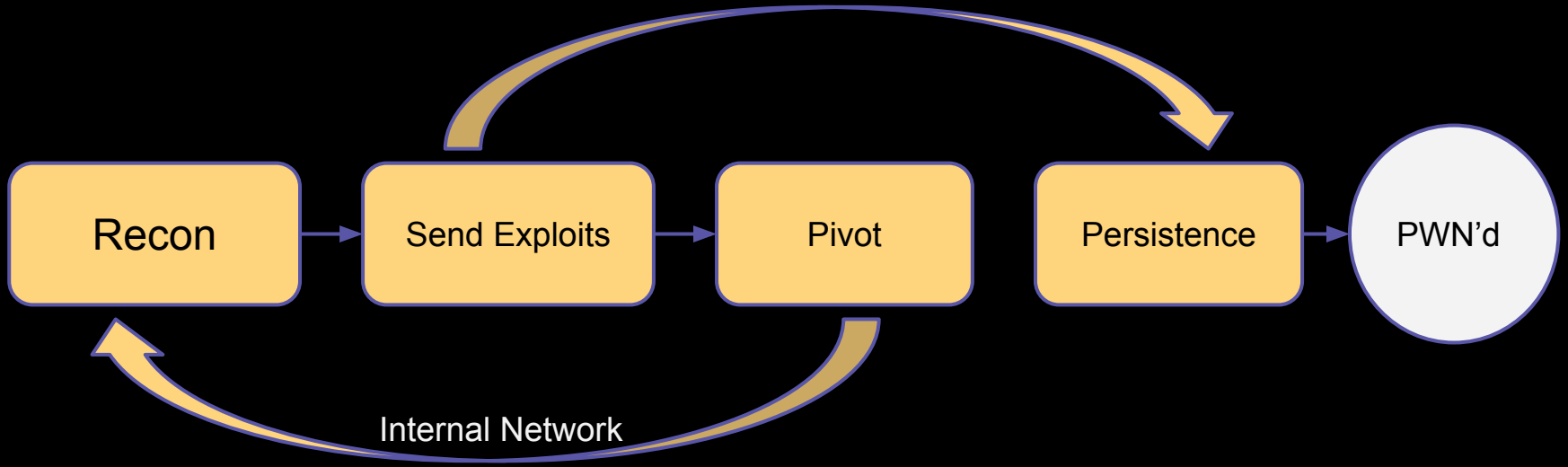
msf> set [variable/option] [value]

msf> show [all/options/modules/exploits]

msf> session -l

msf> session -i 1

Methodology



Setting the Scene

You are a hacker

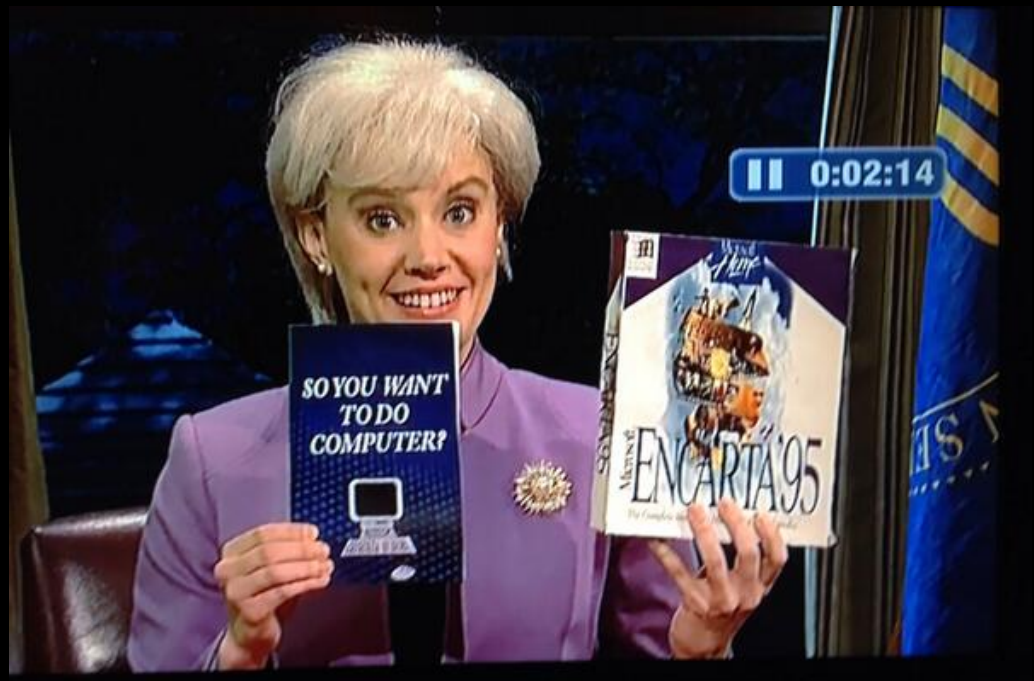
Target: lulzsec

Motive: They are suspected of taking a copy of your bosses' "special video"

Objective: Gain access to their internal servers and find evidence they accessed your servers and took the data.

TO THE CONSOLE!

msf>



OMG IT CRASHED!!

DO A BARREL ROLL!

[R or Z twice]

VERY DEMOTIVATIONAL .com

Finally, its over!

Questions?

Follow me: @d4rkm4tter

Blog: palshack.org

IRC: #DC801

Some Vidz: http://bit.ly/QhWNL2