Penetration Testing

nmap

```
nmap -sV -O -Pn 192.168.1.2

Nmap scan report for 192.168.1.2
Host is up (0.0041s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE   VERSION
22/tcp   open  ssh       OpenSSH 6.0p1 Debian 4
80/tcp   open  http      nginx 1.2.1
```

Gathering Hunting Exploiting Reporting

python-libnmap

```
ip = ifconfig.get_ip('wlan1')
targets = ip + '/24'

nm = NmapProcess(targets, '-sV -O -Pn')
rc = nm.run()

report= NmapParser.parse(nm.stdout)

db = NmapMongodbPlugin(dbname='scan')

report.save(db)
```

CVE Search

```
def get_cve_ids(vconfig):
    cve_ids = []

    for item in collection.find(
             {"vulnerable_configuration":
             {'$regex' : vconfig}}):

        cve_ids.append(item['id'])

    return cve_ids
```

vFeed

```
def find_exploits(cve_ids):
    exploits = []

    for id in cve_ids:
        vfeed = vFeed(id)
        cve_info = vfeed.get_cve()
        cve_info['id'] = id
        cve_info['msf'] = vfeed.get_msf()
        cve_info['score'] = vfeed.get_cvss()

        exploits.append(cve_info)

    return exploits
```

Gathering Hunting Exploiting Reporting

vFeed

```
CVE ID: CVE-2010-2550
-------------------------
The SMB Server in Microsoft Windows does not
properly validate fields in an SMB request, which
allows remote attackers to execute arbitrary code
via a crafted SMB packet.

[cvss_base]: 10.0
[cvss_impact]: 10.0
[msf_id]: ms10_054_queryfs_pool_overflow.rb
[msf_title]: Windows SrvSmbQueryFsInformation
[msf_file]: metasploit-
framework/modules/auxiliary/dos/windows/smb/ms10_
054_queryfs_pool_overflow.rb
```

My Happy Place

DirBuster, BurpSuite, Wfuzz, … mine

My Happy Place

```
DirBuster, BurpSuite, Wfuzz, … mine

*.bak
*.~
#*#
*.off
*.zip
*.tar.gz
*.tgz
*.tbz
*.git/
/tmp
etc ...
```

My Happy Place

`http://project-dev.example.com/project.zip`

And

`http://project-dev.example.com/.git/`

And

`http://project.example.com/.git/`

The End Game

Gaining Root Access → The cycle repeats

Gathering

Hunting

Exploiting

Good Guys vs Bad Guys

Obligatory disclamer ...