Learn-A-Thon!

Jesus Perez
Cybersecurity Architect
Advoqt Technology Group

Lead Instructor & Course Designer
CyberWarrior Academy

CTFd

Register to the CTF by connecting to:
ctf.aiseclabs.com
username/password = h4ck3r

advoqt

Agenda

09:00-10:00 Registration & VM Installation (60 min)

10:00-10:45 Tools & Techniques (45 min)

10:45-12:00 CTF Challenges (75 min)

12:00-01:00 Lunch Break (60 min)

01:00-02:00 CTF Challenges (75 min)

01:15-02:00 System Hacking (45 min)

02:00-02:30 Wrap-up & Prizes (30 min)

advoqt

Jesus Perez

Cybersecurity Architect & Instructor

Network Security

Vulnerability Management

Penetration Testing

Network & Security Training

Security Monitoring

Contact:
617-4156567
jesus@Advoqt.com
https://www.linkedin.com/in/jperezduerto/
https://github.com/japd06

Certifications:

2018

GIAC Web Application Penetration Tester (GWAPT)
Certified EC-Council Instructor (CEI)
Certified Ethical Hacker (CEH)
Certified Incident Handler (ECIH)
Certified Network Defender (CND)
GIAC Continuous Monitoring Certification (GMON)
GIAC Security Essentials (GSEC)
Fortinet Certified Network Security Professional (FCNSP) | (NSE4)
Fortinet Certified Network Security Administrator (FCNSA)
Cisco Certified Academy Instructor (CCAI)
Cisco Certified Network Associate Security (CCNA Security)

2009

Cisco Certified Network Associate (CCNA)

advoqt

Why do you want to be a pentester?

Penetration & Vulnerability Tester

CyberSeek™

AVERAGE SALARY

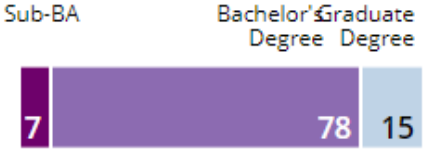
$97,000

Penetration & Vulnerability Tester

COMMON JOB TITLES

- Application Security Engineer
- Penetration Tester
- Security Analyst II
- Application Security Architect
- Application Security Analyst

REQUESTED EDUCATION (%)



TOP SKILLS REQUESTED

1. Information Security
2. LINUX
3. JAVA
4. Python
5. Information Systems
6. UNIX
7. Scanners
8. Software Development
9. SQL

TOTAL JOB OPENINGS

10,929

Penetration & Vulnerability Tester

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

Analyze

Protect and Defend

TOP CERTIFICATIONS REQUESTED

- GIAC
- CISA
- CISM
- Cisco Certified Network Associate
- Certified Ethical Hacker

https://www.cyberseek.org/

advoqt

Why Learning with CTF?

https://www.hackthebox.eu/
https://ctftime.org/
https://www.vulnhub.com/
https://github.com/WebGoat/WebGoat
https://sourceforge.net/projects/mutillidae/files/
http://overthewire.org/wargames/narnia/
https://github.com/CTFd/CTFd
https://github.com/facebook/fbctf

CTFd

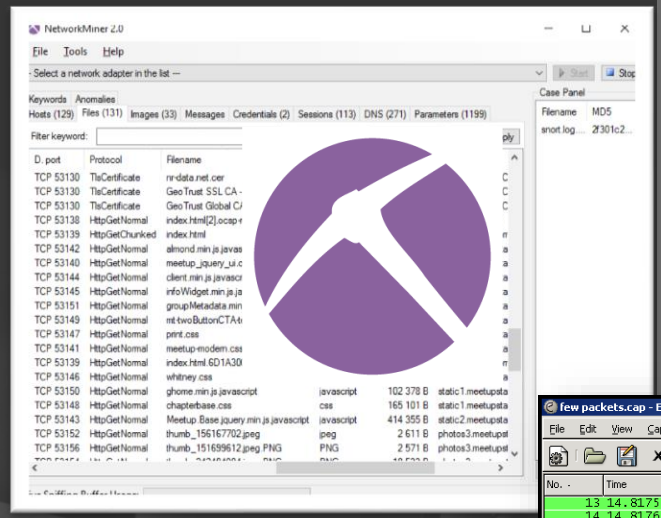
advoqt

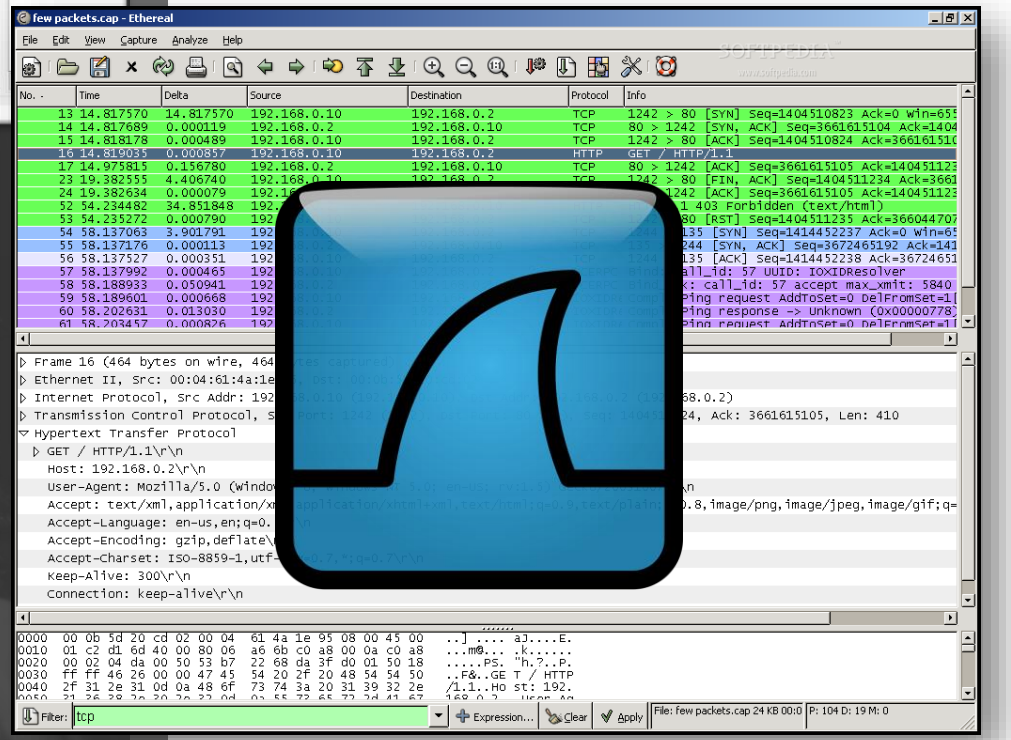
DISCLAIMER

Technology as a force for good!

We are teaching you so you can defend!

Packet analysis





Tools:

- Wireshark
- NetworkMiner
- Tcpdump
- Snort BRO
- Python Scapy

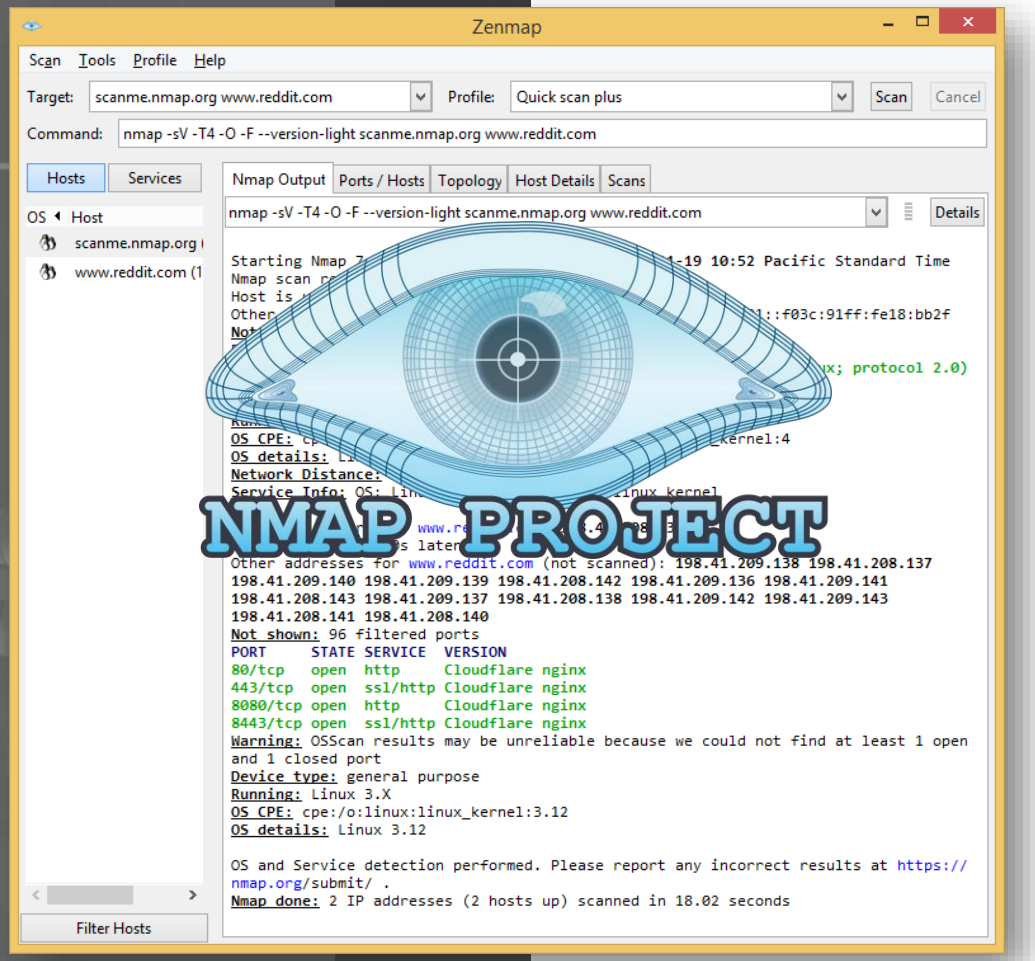
advoqt

Network Scanning

Tools:

- NMAP/Zenmap
- Masscan
- Xprobe2

- NMAP
  - Scan types
  - Scan speed
  - Output types



Python for Hackers!

Scapy

Sending Packets

Creating and sending a packet:

```
>>> packet =
IP(dst="4.5.6.7",src="1.2.3.4")/
TCP(dport=80, flags="S")
```

Send a packet, or list of packets without custom ether layer:

```
>>> send(packet)
```

Other send functions:

`sr()` sends and receives without a custom ether() layer
`sendp()` sends with a custom ether() layer
`srp()` sends and receives at with a custom ether() layer
`sr1()` sends packets without custom ether() layer and waits for first answer
`sr1p()` sends packets with custom ether() layer and waits for first answer

Send function options:

filter = <Berkley Packet Filter>
retry = <retry count for unanswered packets>
timeout = <number of seconds to wait before giving up>
iface = <interface to send and receive>

```
>>> packets = sr(packet, retry=5,
timeout=1.5, iface="eth0", filter="host
1.2.3.4 and port 80")
```

Port Scanning

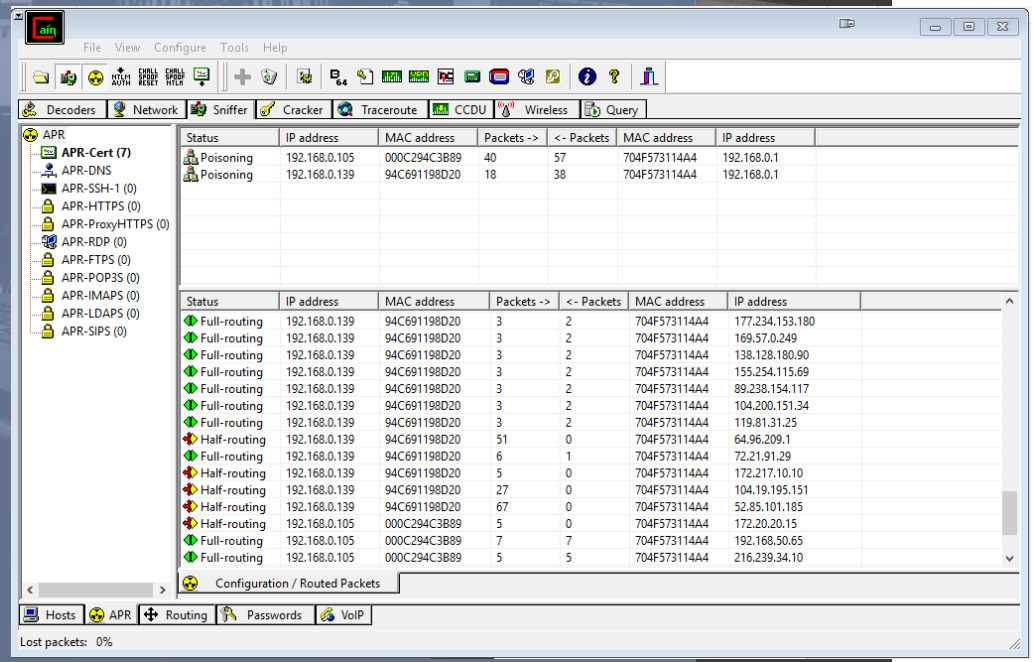
root@kali: ~/ViolentPython/CH1
root@kali: ~/ViolentPython/CH1 68x24

```
#!/usr/bin/python

import socket
socket.setdefaulttimeout(2)

ipaddress = '10.0.0.8'
int_ports = [21,25,80,445,3389]
banners = []

for port in int_ports:
    try:
        s = socket.socket()
        s.connect((ipaddress,port))
        banner = s.recv(1024)
        banner = banner.strip('\n').strip('\r')
        banners.append(banner)
        if banner == '':
            print 'Port open = '= port
    except:
        continue

## Read file
filename = 'vuln-banners.txt'
myfile1 = open(filename,'r')
```

Password Cracking

Tools:

- Cain & Able
- John the ripper
- Hydra
- Hashcat
- Responder



hashcat

advanced password recovery

John the Ripper

About the CTF

CTF Server: ctf.aiseclabs.com

Linux Webserver => 10.99.0.51
Linux DB Backend => 10.99.0.52
WinXP => 10.99.0.55
Windows10 => 10.99.0.54
Win2008 => 10.99.0.58
Windows 2012 => 10.99.0.12

Attacking Machine:
Hack&LearnVM DHCP
Username: student
Password: advoqt

CTFd

Register to the CTF by connecting to:
ctf.aiseclabs.com
username/password = h4ck3r