Intro, Nmap & THM

Coventry University Comsec

By Jack Orcherton

Welcome to Comsec!

- Weekly meeting every Wednesday at 18:30
- Learn & practise new cybersecurity skills
- CTF competitions
- Aimed at beginners to pro’s and open to people from other courses!
- Being led by second years: Jack Orcherton, Tiago Pascoal & Martin Schon

Legal

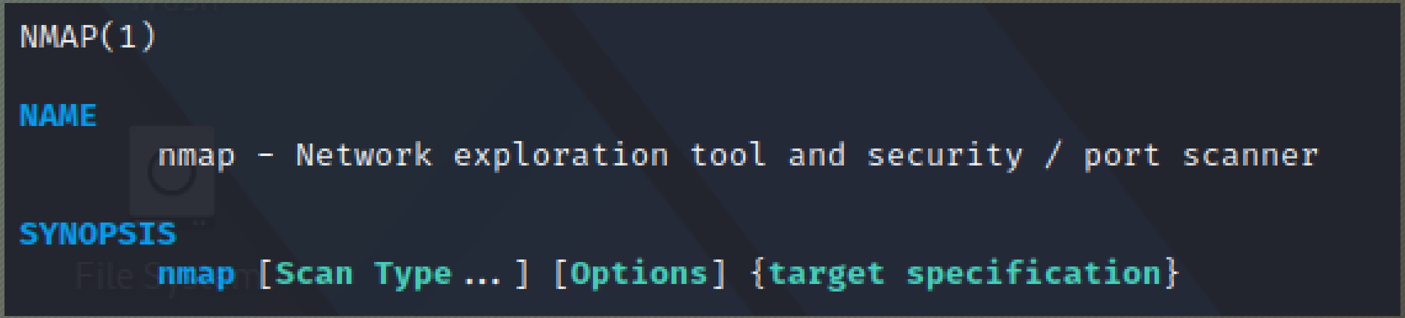
- As I’m sure you will have heard by now, there are some rules when it comes to hacking
  - These courses are to be used only **for ethical purposes**
  - Do **not attack anything**, unless you have written consent from the owner
  - If you’re unsure if you’re allowed to do something – you probably aren’t! So ask someone beforehand
  - We accept no responsibility
- For more information, please refer to the Computer Misuse Act 1990, or view your local equivalent.

Hacking Theory

- Reconnaissance
- Scanning & Enumeration
- Exploitation (Gaining Access)
- Maintaining Access
- Cover Tracks

Nmap

- Short for network mapper
- Most popular port scanning tool
- Installed by default on Kali



```
NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type ... ] [Options] {target specification}
```

- **NB:** Nmap scans are classed as a cyber attack under most laws. **DO NOT** scan anything without permission (especially on the uni network, as students have been expelled for this).

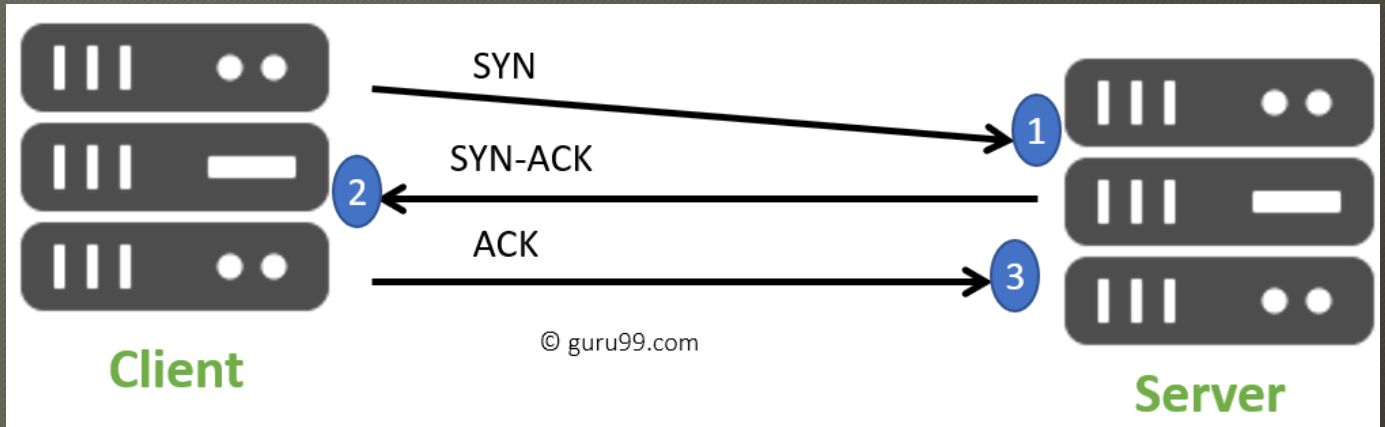
Why port scan?

- First step on most challenges
- Find programs running on devices
- Find program versions and find associated vulnerabilities
- OS detection
- Easy to do

- Disadvantages:
  - Can be ‘loud’ and detected on IDS/IPS

TCP Stealth Scan – Most Common

- The TCP handshake:
  - Syn – client device initiates and attempts to establish connection
  - Syn-ack – server acknowledges receipt of syn
  - Ack – client acknowledges receipt of syn-ack and communication will start
  - Fin – terminates connection
- A TCP scan uses this to its advantage, it sends a syn packet and if a syn-ack packet is received, the port is open. The connection is then dropped



© guru99.com

Other Types of Scan

- Ping Scan
  - Send an ICMP packet to specified hosts, if there is a response, you know its up
- UDP
  - Sends udp packet, if there is a response it is open, if there is no response it is open or filtered. If the port is unreachable it is closed
- ARP
  - Send an ARP request and wait for responses
- Listening
  - Just listen to network traffic & able to detect which devices are communicating
- TCP – see next slide

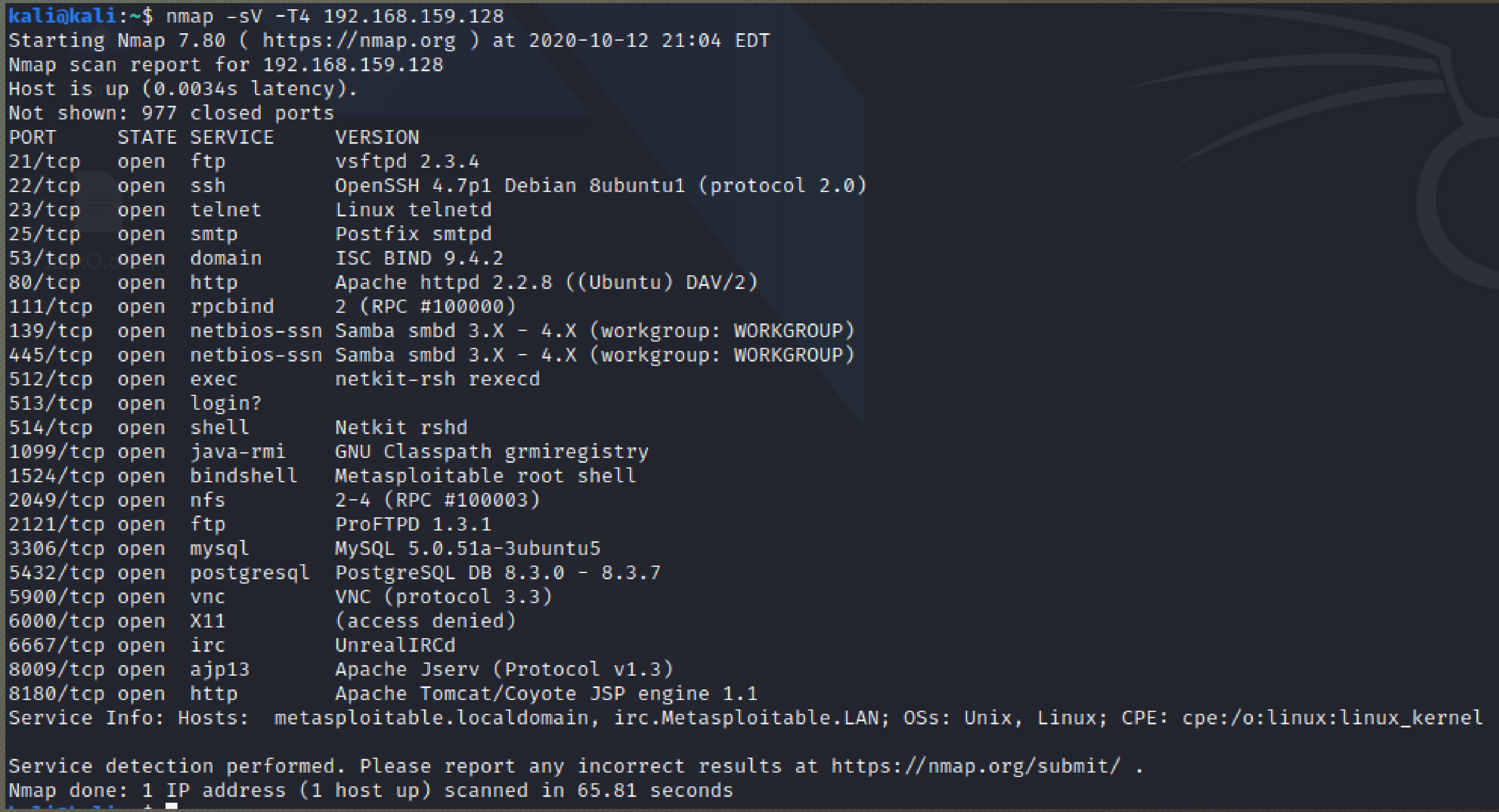
Common Commands

- -A – runs OS detection, version detection, script scanning & traceroute
- -T – set timing 0-5 (higher is faster but runs risk of being detected)
- -v/-vv – verbose mode – displays progress info in the terminal
- -pn – skip host discovery – sometimes useful when devices won't respond to ICMP
- -p – port selection (use –p- for all ports)
- -sV – find service & version running on the port
- -F – fast mode, scans fewer ports compared to a normal scan
- -O – OS detection
- For more options – run 'man nmap'

Example

- Common examples:
  - nmap -A -vv scanme.org
  - nmap -sV -vv scanme.org
  - nmap -A -p- -T4 scanme.org

- **NB:** scanme.org is a special site owned by nmap, that you can test the scanner on!

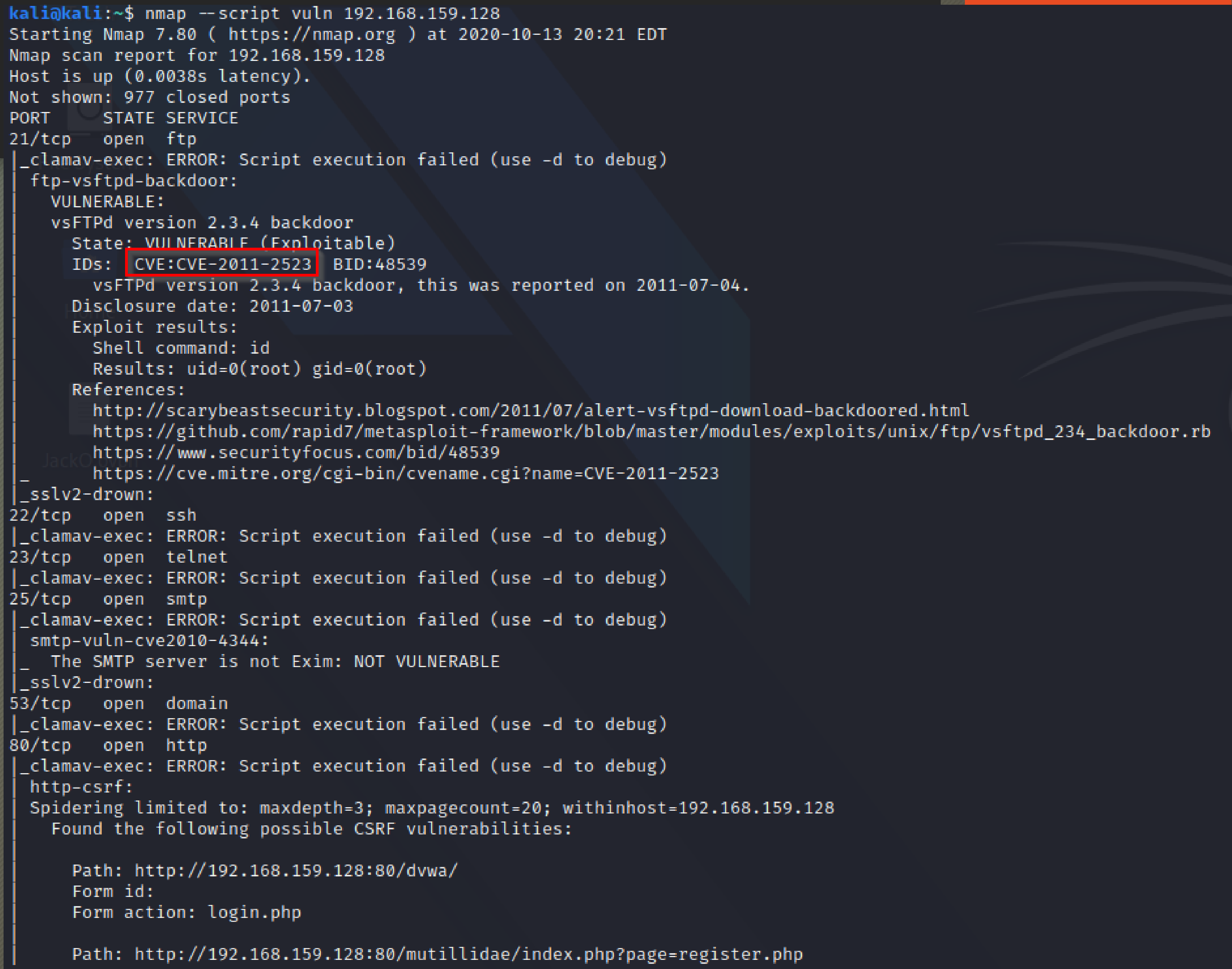


```
kali@kali:~$ nmap -sV -T4 192.168.159.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-12 21:04 EDT
Nmap scan report for 192.168.159.128
Host is up (0.0034s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.81 seconds
```

Nmap Scripts

- Nmap allows you to write your own scans, using the Nmap Scripting Engine
- Some built-in scripts
- nmap --script vuln



```
kali@kali:~$ nmap --script vuln 192.168.159.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-13 20:21 EDT
Nmap scan report for 192.168.159.128
Host is up (0.0038s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
22/tcp   open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
23/tcp   open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp   open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
53/tcp   open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.159.128
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.159.128:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.159.128:80/mutillidae/index.php?page=register.php
```

A Challenge from Dan

- 'sudo pip install docker-compose'
- Download the docker-compose.yaml from github
- 'docker-compose up' in the directory of the file
- You are ready to pw, start scanning.

Introduction to Try Hack Me

- Tryhackme is an online platform aimed towards beginners & gives guided walkthroughs on challenges (if you're more advanced you may to try HTB, more on this in the future)
- Go to https://tryhackme.com/ & create the free account!

Connecting to VPN

- https://tryhackme.com/room/hello
- Practical Demo (by Jack)

Homework Time!

- https://tryhackme.com/room/rpnmap
- If you get stuck remember man pages, -h & DuckDuckGo is your friend!

See you next Wednesday @ 18:30

Thank You!