CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Post-Midterm Review and Nmap

Chris Samayoa

Week 12 – 1st Lecture
4/5/2022

Course Information

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- Post-Midterm Review
- Nmap Refresh

NMAP

- Main objectives
  - Identify information regarding the scanned target
- What can be found?
  - Existence of network device
    - Ping scans
  - Running services (http, https, smtp, etc)
    - Determined by finding open ports and gathering data
  - Host information
    - Hardware manufacturer
    - Operating system
    - Firewall detection

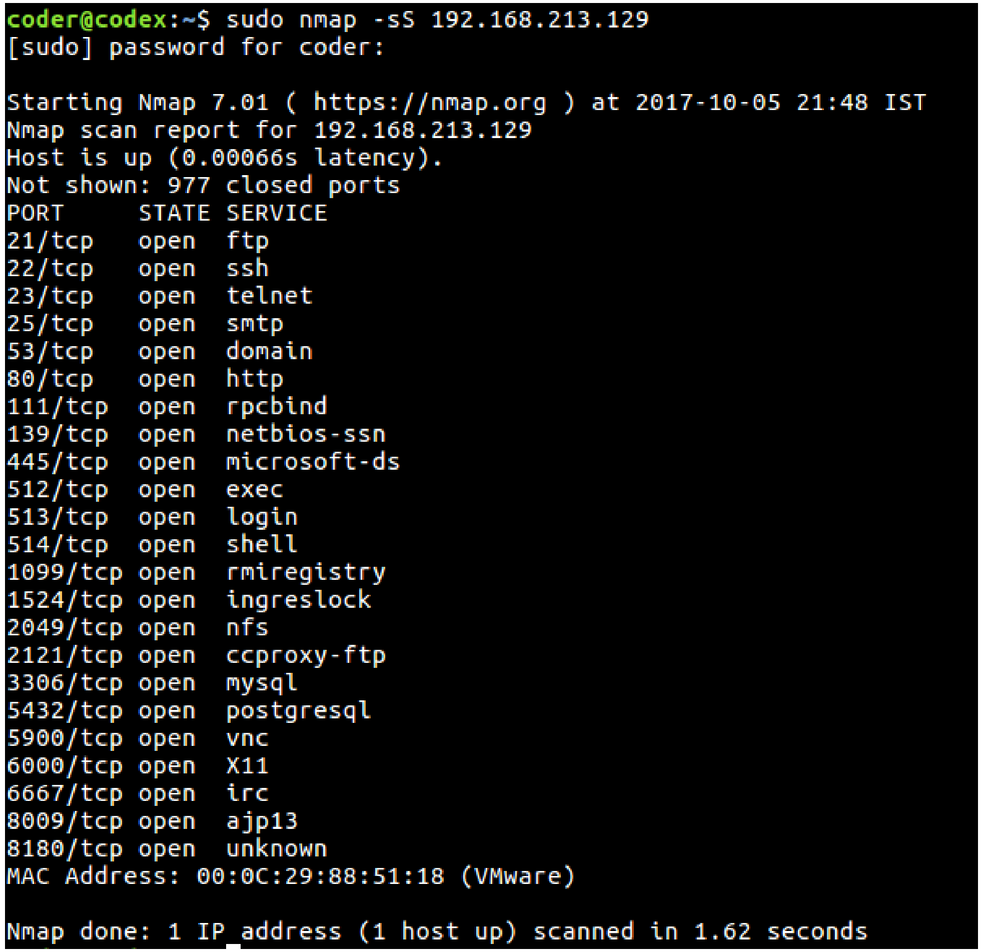
NMAP (cont’d)

- GUI Available
    - Zenmap
- Options
    - Port Scanning
        - Default: Scans the most common 1,000 ports for each protocol
        - Fast flag: Scan the 100 most common
    - Ping Scanning
        - IP address ranges
        - Subnet masks
        - Single IPs
    - Host Scans
        - Sends ARP requests (MAC address collection)
        - DNS queries
        - Latency information
    - Output to files

NMAP (cont'd)

- Port scans
  - TCP SYN: TCP handshake is not completed (avoids suspicion)
  - TCP connect: TCP handshake is completed (more reliable)
  - UDP: Identify DNS, SNMP, and DHCP ports
    - Frequently targeted by hackers
- OS Scans
  - Uses TCP and UDP Ports
  - Compares responses to database of over 2500 operating systems
    - Can return information about OS and version for each host

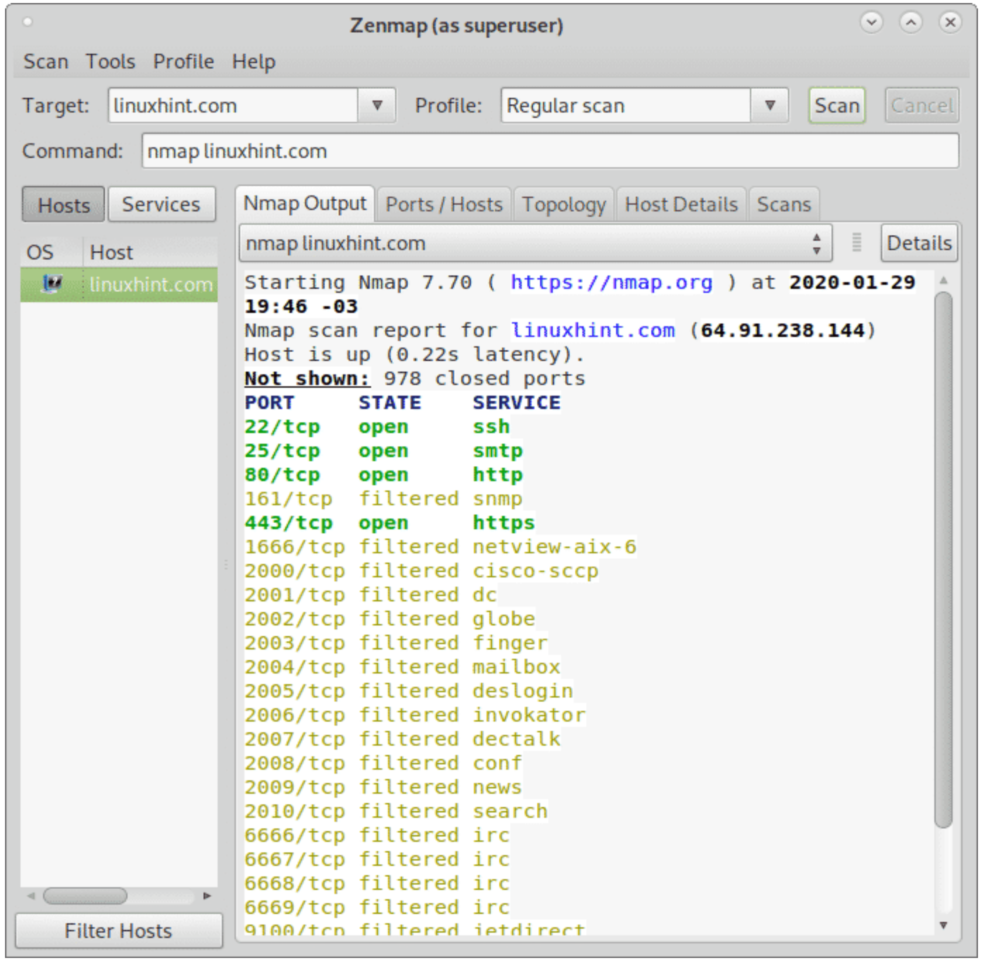
NMAP vs Zenmap



```
coder@codex:~$ sudo nmap -sS 192.168.213.129
[sudo] password for coder:

Starting Nmap 7.01 ( https://nmap.org ) at 2017-10-05 21:48 IST
Nmap scan report for 192.168.213.129
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:88:51:18 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```



Target: linuxhint.com

Profile: Regular scan

Command: nmap linuxhint.com

nmap linuxhint.com

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-29
19:46 -03
Nmap scan report for linuxhint.com (64.91.238.144)
Host is up (0.22s latency).
Not shown: 978 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
80/tcp    open     http
161/tcp   filtered snmp
443/tcp   open     https
1666/tcp filtered netview-aix-6
2000/tcp filtered cisco-sccp
2001/tcp filtered dc
2002/tcp filtered globe
2003/tcp filtered finger
2004/tcp filtered mailbox
2005/tcp filtered deslogin
2006/tcp filtered invokator
2007/tcp filtered dectalk
2008/tcp filtered conf
2009/tcp filtered news
2010/tcp filtered search
6666/tcp filtered irc
6667/tcp filtered irc
6668/tcp filtered irc
6669/tcp filtered irc
9100/tcp filtered jetdirect
```

NMAP (cont’d)

- Linux installation commands:
  - sudo apt update
  - sudo apt install nmap -y
- Common commands
  - Regular Scan
    - ➢ nmap [host URL or IP address]
  - Quick Scan
    - ➢ nmap -T4 -F [host URL or IP address]
  - Intense Scan
    - ➢ nmap -T4 -A –v [host URL or IP address]
  - Intense Scan – All TCP Ports
    - ➢ nmap –p 1-65535 -T4 -A –v [host URL or IP address]
  - Intense Scan – With UDP Ports
    - ➢ nmap –sS –sU -T4 -A –v [host URL or IP address]

NMAP References

- Nmap – Quick Port Scanning Tutorial
  - https://nmap.org/book/port-scanning-tutorial.html
- Nmap – All Options
  - https://svn.nmap.org/nmap/docs/nmap.usage.txt
- Nmap – Cheat Sheet
  - https://www.stationx.net/nmap-cheat-sheet/