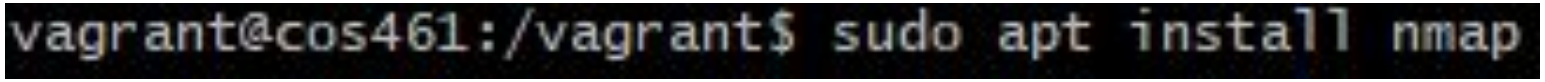
Port Scanning

Goals for today

- What is port scanning?
- How is it done?
- How do we prevent it?
- Breakout room questions:
  - How can you detect & defend against a port scan?
  - What are some ethical reasons to use port scans?

Setup for today

- Please open Vagrant
- SSH into two shells
- Install nmap



```
vagrant@cos461:/vagrant$ sudo apt install nmap
```

- Do not run it yet

Before we go any further…

- Don’t use pen test tools like nmap without permission
  - In 2017, students got a COS 432 server banned when using nmap
  - It’s illegal if you don’t have permission
    - Up to 20 years imprisonment, per 18 U.S.C § 1030

What is port scanning?

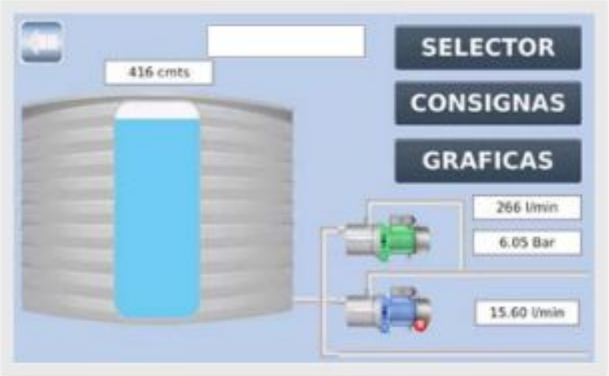
- Goal: identify open ports
- Why would we want to do this?
- How can we do this?

Why port scan?

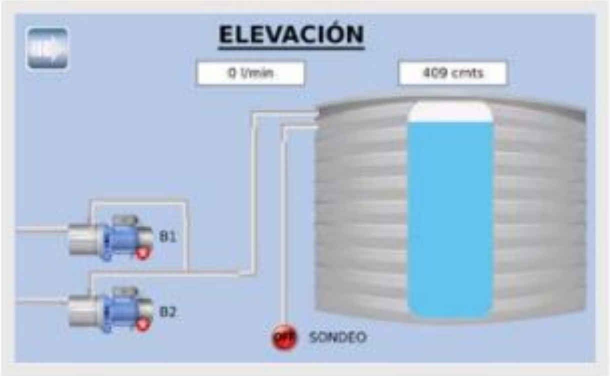
- Search for unprotected services
  - Open remote access controls
  - Hidden, unsecured, secret data
    - Open cameras
    - File servers
- Search for vulnerable services
- Check open services against known vulnerabilities

Open services are everywhere

- Critical infrastructure is left open
- Outdated software i used
- Vulnerability fixes ca be slow



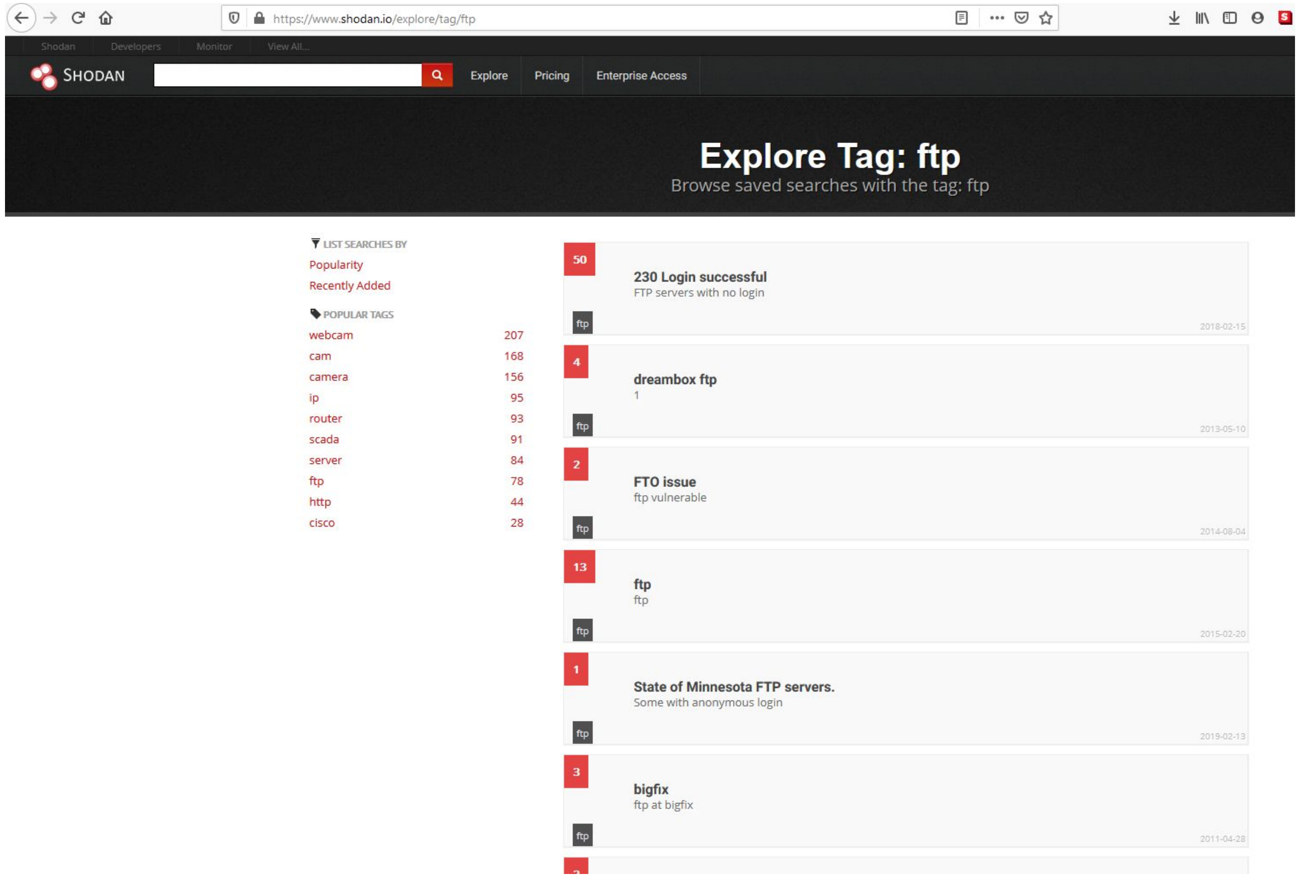
A monitor for a water pumping system. Top-level menu displays the available submenus: Selector, Readings, and Graph. This page shows one of the pumps is pumping water at 266 L/min, while the second pump is mostly inactive and pumps at 15.6L/min.



Another overview page shows both pumps are currently deactivated.

Open services are everywhere

- Shodan.io
  - Global port scan service
- Freely available



Explore Tag: ftp

Browse saved searches with the tag: ftp

LIST SEARCHES BY

Popularity

Recently Added

POPULAR TAGS

webcam	207
cam	168
camera	156
ip	95
router	93
scada	91
server	84
ftp	78
http	44
cisco	28

50 **230 Login successful**
FTP servers with no login
ftp 2018-02-15

4 **dreambox ftp**
1
ftp 2013-05-10

2 **FTO issue**
ftp vulnerable
ftp 2014-08-04

13 **ftp**
ftp
ftp 2015-02-20

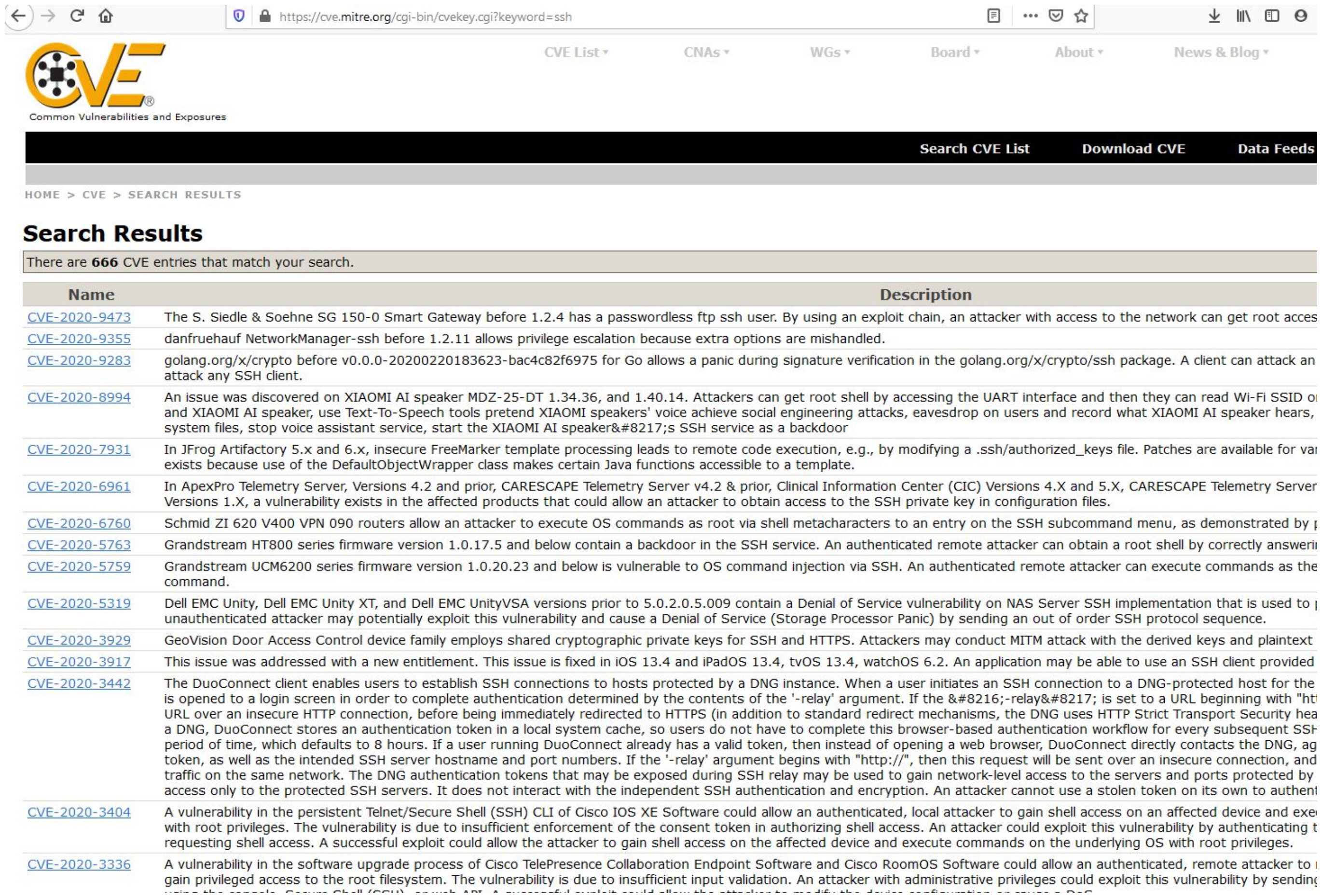
1 **State of Minnesota FTP servers.**
Some with anonymous login
ftp 2019-02-13

3 **bigfix**
ftp at bigfix
ftp 2011-04-28

Vulnerabilities are common

- Legally available:
  - CVE database
  - Zerodium
- Purchased on the black market

zerODIUM



https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ssh
CVE List ▾
CNAs ▾
WGs ▾
Board ▾
About ▾
News & Blog ▾
CVE®
Common Vulnerabilities and Exposures
Search CVE List
Download CVE
Data Feeds
HOME > CVE > SEARCH RESULTS

Search Results

There are **666** CVE entries that match your search.

Name	Description
CVE-2020-9473	The S. Siedle & Soehne SG 150-0 Smart Gateway before 1.2.4 has a passwordless ftp ssh user. By using an exploit chain, an attacker with access to the network can get root acces
CVE-2020-9355	danfruehauf NetworkManager-ssh before 1.2.11 allows privilege escalation because extra options are mishandled.
CVE-2020-9283	golang.org/x/crypto before v0.0.0-20200220183623-bac4c82f6975 for Go allows a panic during signature verification in the golang.org/x/crypto/ssh package. A client can attack an attack any SSH client.
CVE-2020-8994	An issue was discovered on XIAOMI AI speaker MDZ-25-DT 1.34.36, and 1.40.14. Attackers can get root shell by accessing the UART interface and then they can read Wi-Fi SSID o and XIAOMI AI speaker, use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, eavesdrop on users and record what XIAOMI AI speaker hears, system files, stop voice assistant service, start the XIAOMI AI speaker&#8217;s SSH service as a backdoor
CVE-2020-7931	In JFrog Artifactory 5.x and 6.x, insecure FreeMarker template processing leads to remote code execution, e.g., by modifying a .ssh/authorized_keys file. Patches are available for va exists because use of the DefaultObjectWrapper class makes certain Java functions accessible to a template.
CVE-2020-6961	In ApexPro Telemetry Server, Versions 4.2 and prior, CARESCAPE Telemetry Server v4.2 & prior, Clinical Information Center (CIC) Versions 4.X and 5.X, CARESCAPE Telemetry Server Versions 1.X, a vulnerability exists in the affected products that could allow an attacker to obtain access to the SSH private key in configuration files.
CVE-2020-6760	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by
CVE-2020-5763	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answeri
CVE-2020-5759	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute commands as the command.
CVE-2020-5319	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.
CVE-2020-3929	GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext
CVE-2020-3917	This issue was addressed with a new entitlement. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to use an SSH client provided
CVE-2020-3442	The DuoConnect client enables users to establish SSH connections to hosts protected by a DNG instance. When a user initiates an SSH connection to a DNG-protected host for the is opened to a login screen in order to complete authentication determined by the contents of the '-relay' argument. If the &#8216;-relay&#8217; is set to a URL beginning with "ht URL over an insecure HTTP connection, before being immediately redirected to HTTPS (in addition to standard redirect mechanisms, the DNG uses HTTP Strict Transport Security hea a DNG, DuoConnect stores an authentication token in a local system cache, so users do not have to complete this browser-based authentication workflow for every subsequent SS period of time, which defaults to 8 hours. If a user running DuoConnect already has a valid token, then instead of opening a web browser, DuoConnect directly contacts the DNG, ag token, as well as the intended SSH server hostname and port numbers. If the '-relay' argument begins with "http://", then this request will be sent over an insecure connection, and traffic on the same network. The DNG authentication tokens that may be exposed during SSH relay may be used to gain network-level access to the servers and ports protected by access only to the protected SSH servers. It does not interact with the independent SSH authentication and encryption. An attacker cannot use a stolen token on its own to authen
CVE-2020-3404	A vulnerability in the persistent Telnet/Secure Shell (SSH) CLI of Cisco IOS XE Software could allow an authenticated, local attacker to gain shell access on an affected device and exe with root privileges. The vulnerability is due to insufficient enforcement of the consent token in authorizing shell access. An attacker could exploit this vulnerability by authenticating t requesting shell access. A successful exploit could allow the attacker to gain shell access on the affected device and execute commands on the underlying OS with root privileges.
CVE-2020-3336	A vulnerability in the software upgrade process of Cisco TelePresence Collaboration Endpoint Software and Cisco RoomOS Software could allow an authenticated, remote attacker to gain privileged access to the root filesystem. The vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sendin

How do you port scan?

- General idea: brute force
  - For each computer:
    - For each port:
      - Test if the port is open

TCP Scans

- TCP connect scan:
  - Complete a three-way handshake.
- **TCP SYN scan**: (This is on your assignment)
  - **Half-open scanning.**
    - **A SYN packet is sent.**
    - **A listening target respond with a SYN+ACK.**
    - **A non-listening target respond with a RST.**
- TCP FIN scan:
  - Scanner sends a FIN packet.
    - Closed ports reply with a RST.
    - Open ports ignore the packet entirely.

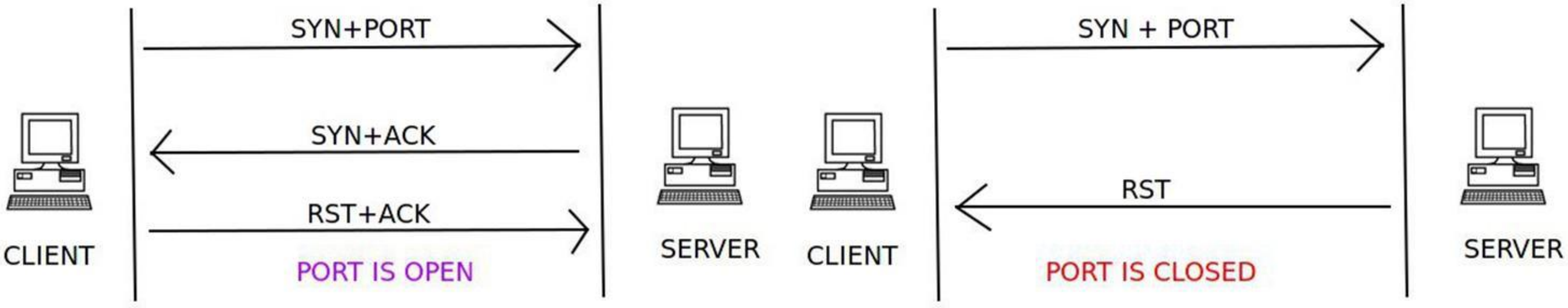
From Yiqian Zhang’s slides

UDP Scanning

- In order to find UDP ports, the attacker generally sends empty UDP datagrams. If
  - The port is listening, the service should send back an error message or ignore the incoming datagram.
  - The port is closed, then most operating systems send back an "ICMP Port Unreachable" message. Thus determine which ports are open.
  - Neither UDP packets nor the ICMP errors are guaranteed to arrive, so UDP scanners must also implement retransmission of packets that appear to be lost.

From Yiqian Zhang’s slides

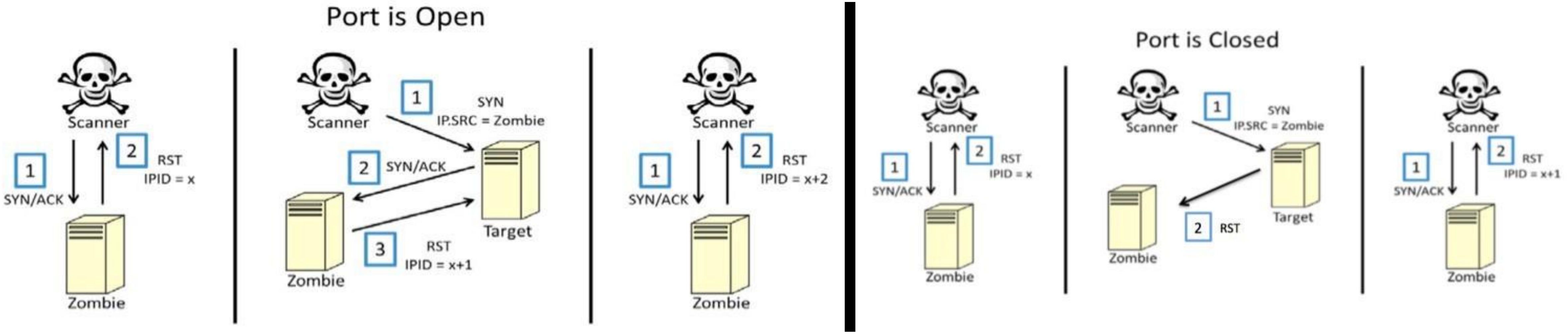
TCP SYN Scan



Images from https://resources.infosecinstitute.com/port-scanning-using-sc

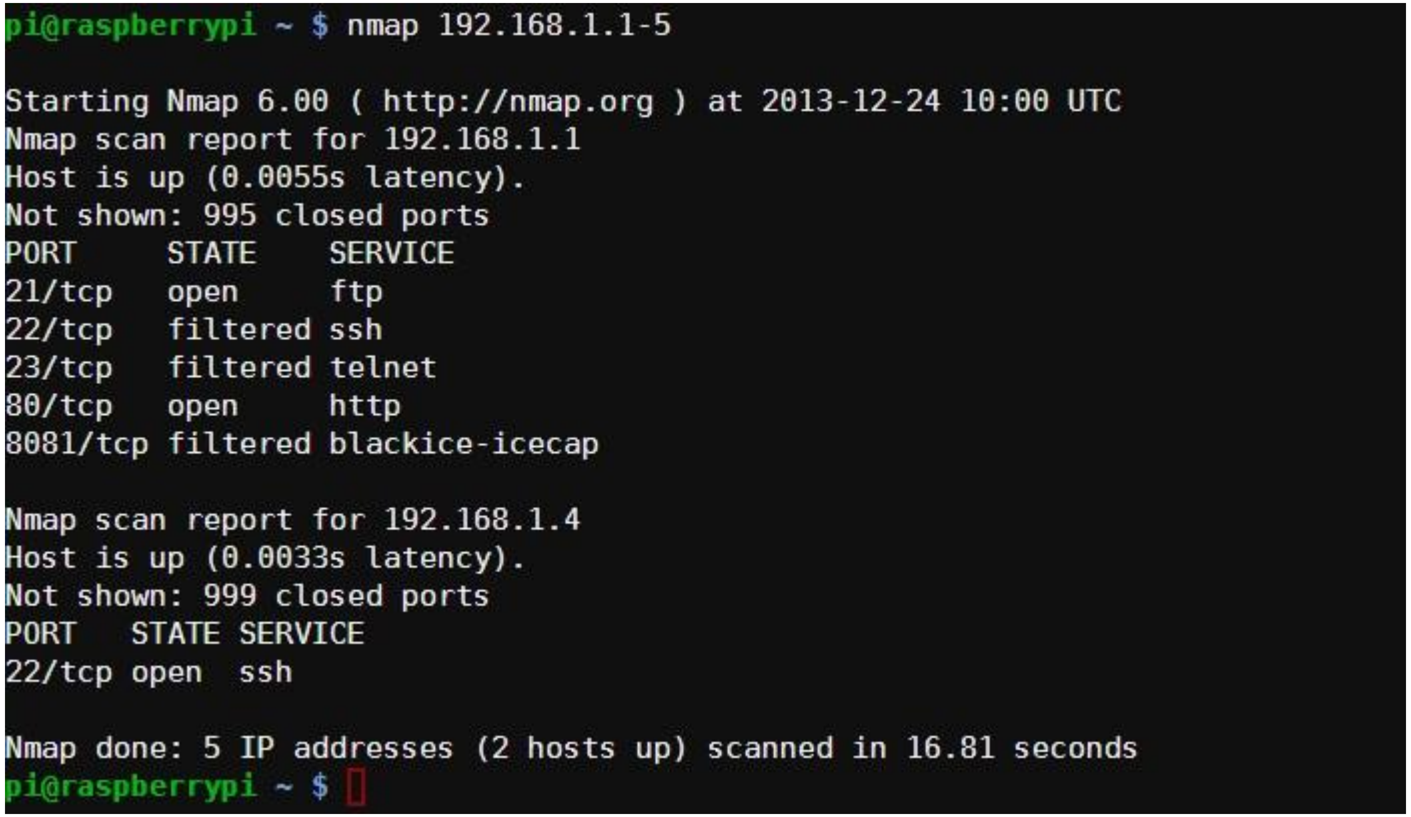
Zombie/idle scanning

- Check an idle machine’s connection count (Zombie machine)
- Scan the target, spoof the Zombie’s IP
- Check if the connection count has incremented by 1 (closed) or 2 (open)



nmap

- Common tool for port scanning
- Try it if you want!
  - (instructions on next slide)

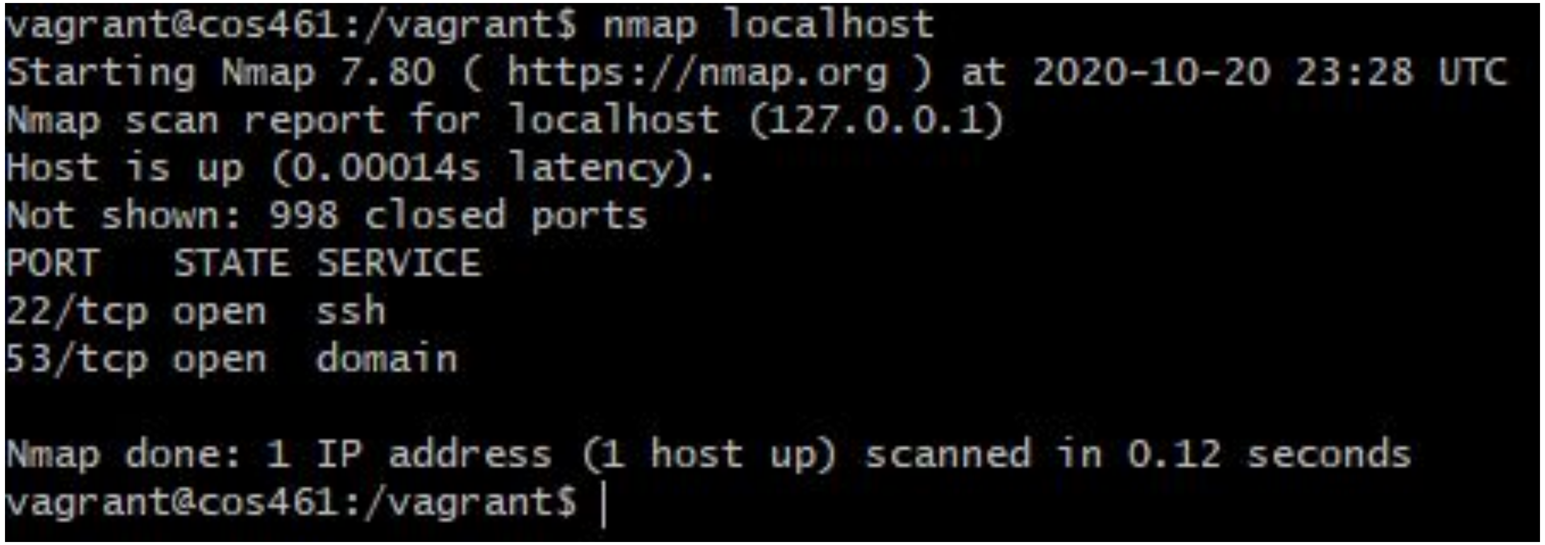


```
pi@raspberrypi ~ $ nmap 192.168.1.1-5

Starting Nmap 6.00 ( http://nmap.org ) at 2013-12-24 10:00 UTC
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
8081/tcp filtered blackice-icecap

Nmap scan report for 192.168.1.4
Host is up (0.0033s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 5 IP addresses (2 hosts up) scanned in 16.81 seconds
pi@raspberrypi ~ $ 
```

https://www.maketecheasier.com/assets/uploads/2013/12/nmap-range-scan.jpg

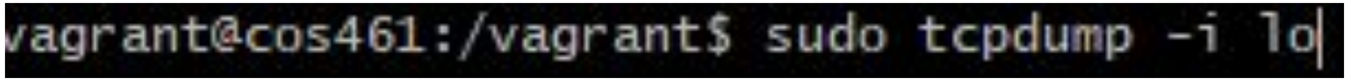
Trying nmap

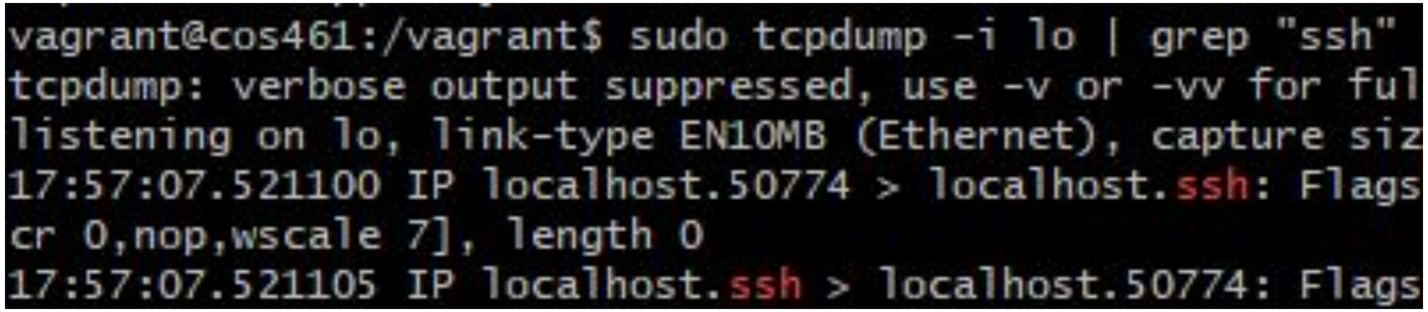
- nmap yourself on localhost
  - Also try against your public IP address (get permission from network owner)
- Try opening an HTTP server
  - python –m SimpleHTTPServer
  - Does the output change?



```
vagrant@cos461:/vagrant$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-20 23:28 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
vagrant@cos461:/vagrant$ 
```

Trying nmap

- Monitor the traffic
  - SSH into vagrant from two shells
  - 

    ```
    vagrant@cos461:/vagrant$ sudo tcpdump -i lo
    ```
  - Run nmap
  - Try to identify one open and one closed port
  - grep might help: 

    ```
    vagrant@cos461:/vagrant$ sudo tcpdump -i lo | grep "ssh"
    tcpdump: verbose output suppressed, use -v or -vv for ful
    listening on lo, link-type EN10MB (Ethernet), capture siz
    17:57:07.521100 IP localhost.50774 > localhost.ssh: Flags
    cr 0,nop,wscale 7], length 0
    17:57:07.521105 IP localhost.ssh > localhost.50774: Flags
    ```

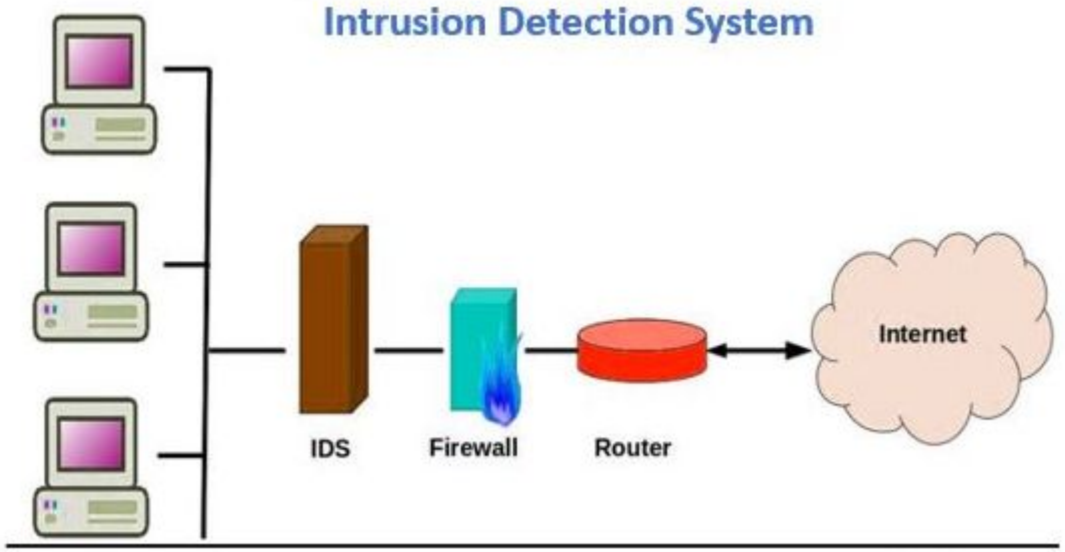
An ounce of prevention

- Firewalls block traffic based on rules
  - Usually blacklists and whitelists
  - Block all traffic on certain ports
  - To or from certain IPs

https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/

A pound of cure

- Network Intrusion detection systems
  - Scans for known malicious patterns
  - Identifies anomalous traffic
  - Typically cannot block traffic



Problems with port scanning

- Creates an obvious access pattern
  - Zombie scanning helps
- Can burden the network
  - Solution: target most common ports, esp. more vulnerable ones
    - e.g. Remote Desktop Protocol, SSH, FTP
- Usually requires follow-up work to find vulnerabilities

Breakout room questions

- What features can you use to detect a port scan?
- How can you defend against a port scan?
- What are some ethical reasons to use port scans?

Breakout room questions

- What features can you use to detect a port scan?
  - Packet sequence
  - Frequent, changing access
  - Short connections
  - Bursts of traffic to many local destinations
- How can you defend against a port scan?
- What are some ethical reasons to use port scans?

Breakout room questions

- What features can you use to detect a port scan?
- How can you defend against a port scan?
  - Firewalls block most ports
  - Disconnect attacker from network
  - Filter traffic from attackers
- What are some ethical reasons to use port scans?

Breakout room questions

- What features can you use to detect a port scan?
- How can you defend against a port scan?
- What are some ethical reasons to use port scans?
  - Testing a network, with permission, to check for vulnerabilities
  - For educational purposes, with permission