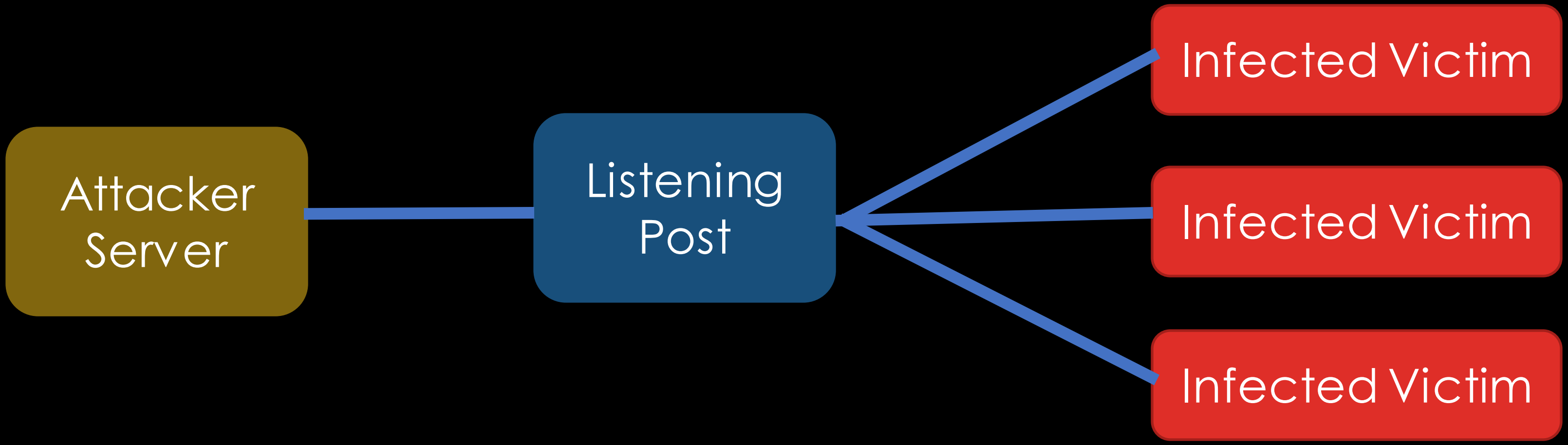
2021 NSA CODEBREAKER CHALLENGE

2021 SCENARIO

- NSA was investigating a foreign cyber actor
- We identified suspicious IP address and captured network traffic going towards it
- We suspect the machine is one of the actor's listening posts

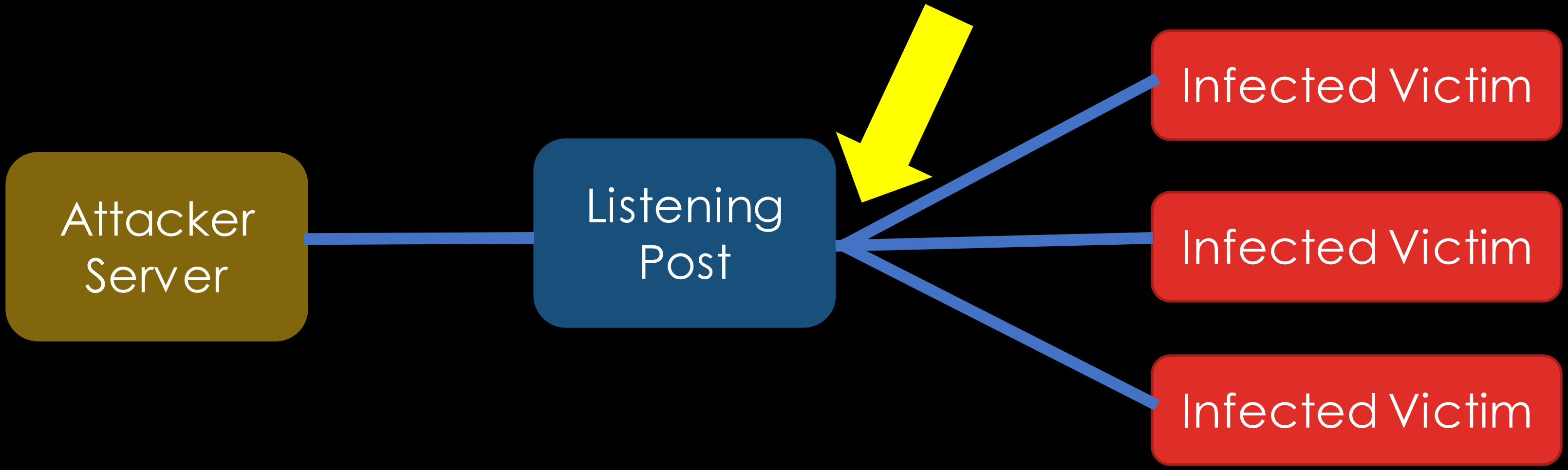
ASIDE: LISTENING POST

- Synonym for "command and control server"
- Attacker-controlled server, communicates with attacker's malware



ASIDE: LISTENING POST

- Synonym for "command and control server"
- Attacker-controlled server, communicates with attacker's malware



MISSION

- **Identify** scope of compromise
- **Analyze** actor's comms protocols and tradecraft
- **Gain** access to actor infrastructure
  - ➢Uncover additional tradecraft, tools
  - ➢Swim upstream

TASKS

- Tasks 1 – 4: Identify Scope of Compromise
  - ➢Task 1: Which Defense Industrial Base (DIB) companies? (Network Forensics)
  - ➢Task 2: Which user account? (Log Analysis)
  - ➢Task 3: What was the attack vector? (Email Analysis)
  - ➢Task 4: What was compromised? (Powershell, Registry Analysis)

TASKS

- Tasks 5 – 8: Analyze tradecraft and protocols
  - Task 5: Locate malicious artifact (Docker analysis)
  - Tasks 6 & 7: Reverse engineer malware (RE, Protocol Analysis)
    - Understand comms implementation
  - Task 8: Crack other comms sessions (Cryptanalysis)

TASKS

- Tasks 9 – 10: Gain access to actor infrastructure
  - Task 9: Connect to LP and identify registered clients (Protocol Analysis, Software Development)
  - Task 10: Expand LP access and identify data exfil path (Exploit Development)

SKILLS LEARNED

- Forensics (network, host)
- Binary Reverse Engineering
- Protocol Analysis / Reverse Engineering
- Cryptanalysis
- Software Development
- Vulnerability Research and Exploitation

WHAT'S NEW?

- Piloting Codebreaker Community of Practice
  - ➢Discord Room
  - ➢Wiki

- Interactive infrastructure

- New web infrastructure

TECHNICAL BACKGROUND

- Network Traffic Analysis
- Docker
- Host Forensics
- Binary Reverse Engineering
- Binary Protocol Analysis

NETWORK TRAFFIC ANALYSIS

- IP Addresses and Subnets
  - IP Address contains both a *network prefix* and a *host identifier*

- CIDR Notation: how many bits in the IP are part of the network prefix?
  - `192.168.1.142/24    ==>`
  - `10.0.0.0/8          ==>`
  - `172.16.150.123/32   ==>`

- Recommended Tools: Wireshark, Python

NETWORK TRAFFIC ANALYSIS

- IP Addresses and Subnets
    - IP Address contains both a *network prefix* and a *host identifier*

- CIDR Notation: how many bits in the IP are part of the network prefix?

```
➢192.168.1.142/24    ==> 192.168.1.0 - 192.168.1.255
➢10.0.0.0/8          ==>
➢172.16.150.123/32   ==>
```

- Recommended Tools: Wireshark, Python

NETWORK TRAFFIC ANALYSIS

- IP Addresses and Subnets
  - IP Address contains both a *network prefix* and a *host identifier*

- CIDR Notation: how many bits in the IP are part of the network prefix?

```
➢192.168.1.142/24    ==> 192.168.1.0 - 192.168.1.255
➢10.0.0.0/8          ==> 10.0.0.0 - 10.255.255.255
➢172.16.150.123/32   ==>
```

- Recommended Tools: Wireshark, Python

NETWORK TRAFFIC ANALYSIS

- IP Addresses and Subnets
  - IP Address contains both a *network prefix* and a *host identifier*

- CIDR Notation: how many bits in the IP are part of the network prefix?
  - `192.168.1.142/24   ==> 192.168.1.0 - 192.168.1.255`
  - `10.0.0.0/8         ==> 10.0.0.0 - 10.255.255.255`
  - `172.16.150.123/32  ==> 172.16.150.123`

- Recommended Tools: Wireshark, Python

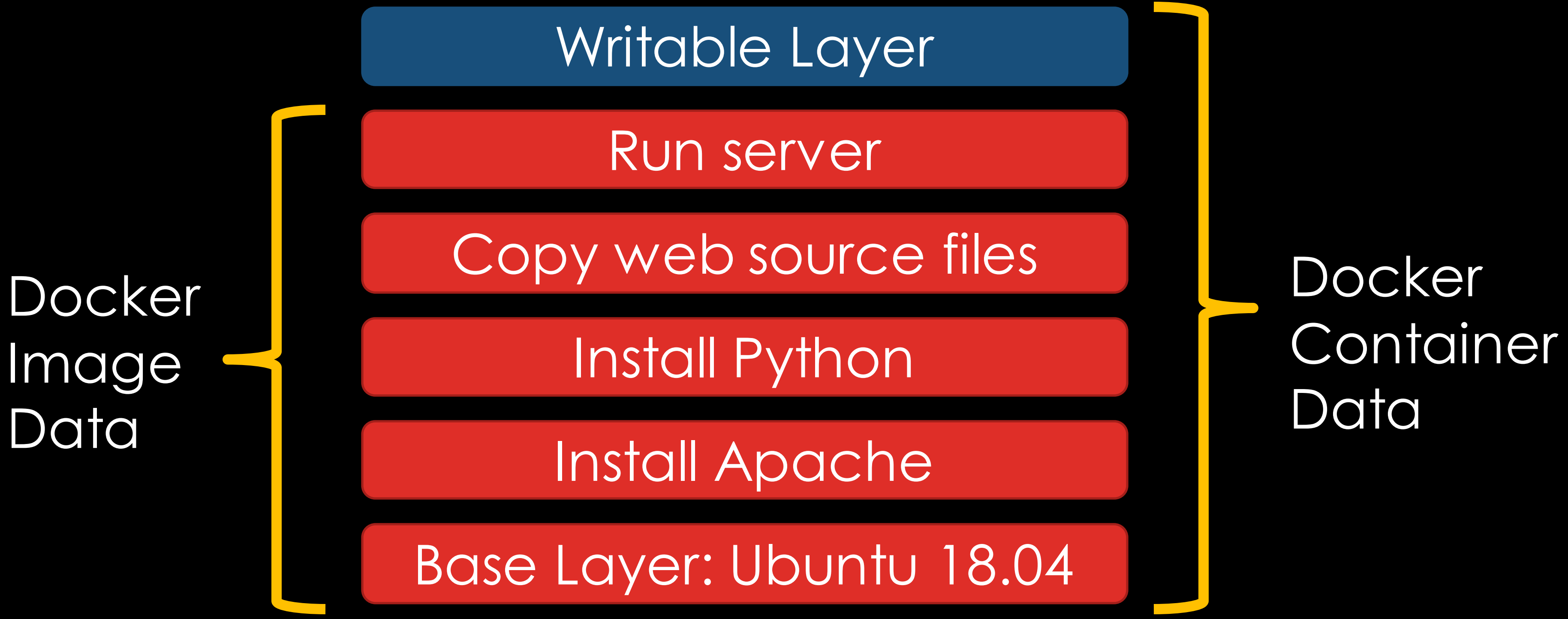
DOCKER

- Container:
  - Encapsulate an application + dependencies
  - Easy to run, minimal assumptions about host operating system

- Docker is a containerization platform
  - Docker *images* can be used to launch *containers*

WHAT'S IN AN IMAGE

- Docker images are a series of layers



Writable Layer

Run server

Copy web source files

Install Python

Install Apache

Base Layer: Ubuntu 18.04

Docker Image Data

Docker Container Data

IMAGE ANALYSIS

- Docker daemon can display image metadata, individual layers
  - ➢
    ```
    $ docker inspect
    ```

- Changes to a layer can be hidden by exporting the modified layer and re-importing

HOST FORENSICS

- Log Analysis
  - Unsure about format? Look for documentation!
  - Parsing manually is painful. Use scripts.

- Files that stick out
  - Too big
  - Too small
  - Weird permissions
  - Odd modification date
  - Differs from known good hash
  - Strange strings

BINARY REVERSE ENGINEERING

- Recommended Tool: Ghidra

- Reverse Engineering Tips
  - ➢Interesting strings?
  - ➢System calls? (Network sockets, file I/O)
  - ➢Linked libraries
  - ➢Exported symbols
  - ➢Debug symbols, if you're lucky

- Best way to get better is to practice!
  - ➢Lots of resources / tutorials online.
  - ➢Codebreaker "Resources" page; Ghidra tutorials

BINARY PROTOCOL ANALYSIS

- Look for patterns in transmitted data
  - Repeated bytes
  - Fixed message lengths
- Get in the mindset of the protocol designer
  - What messages would I need to do <X>?
  - What purpose does this message serve?
- Type / length / value format common
  - Especially if fields can have variable lengths
- Have access to a binary that generates comms? Analyze it!

GET STARTED

- Visit `nsa-codebreaker.org`
- Sign up with your school email address
- Learn and have fun!

THANKS!

nsa-codebreaker.org

codebreaker@uwe.nsa.gov

www.intelligencecareers.gov/nsa

- Student Programs / Summer Internships: Open until Oct 31