NAT Slipstreaming

Amir Mohamadi

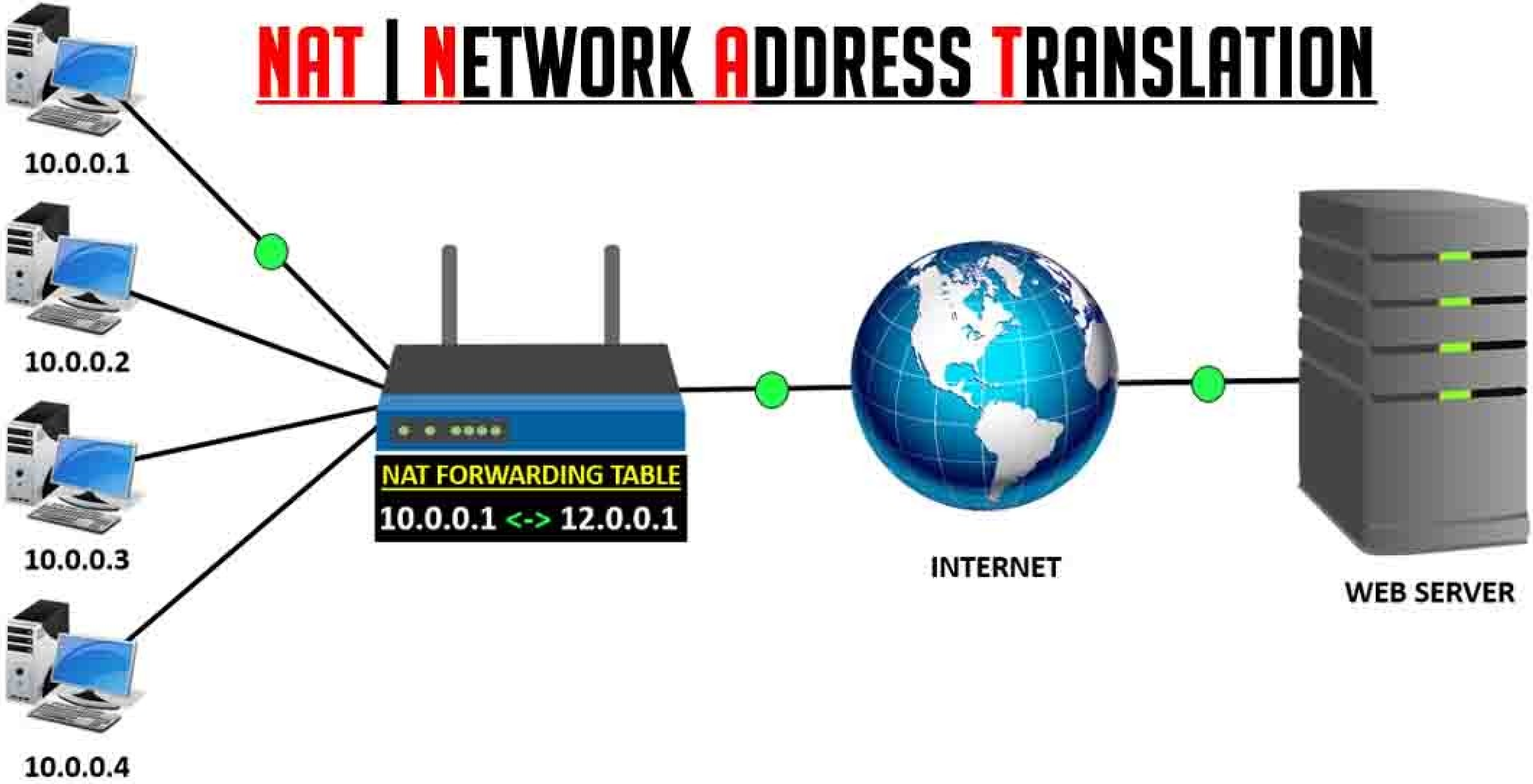
NAT SlipStreaming Explained

SAMY

NAT Slipstreaming Summary

- Goal: Attacker wants to access a service on a victim machine behind NAT (8080)
- Victim visits the attacker web server & downloads page
- Page makes a special malicious POST request to attacker
- Victim Router inspect packet and sees a SIP Message instructing to open port to victim
- Attacker access victim service on the opened port

NAT | NETWORK ADDRESS TRANSLATION



10.0.0.1

10.0.0.2

10.0.0.3

10.0.0.4

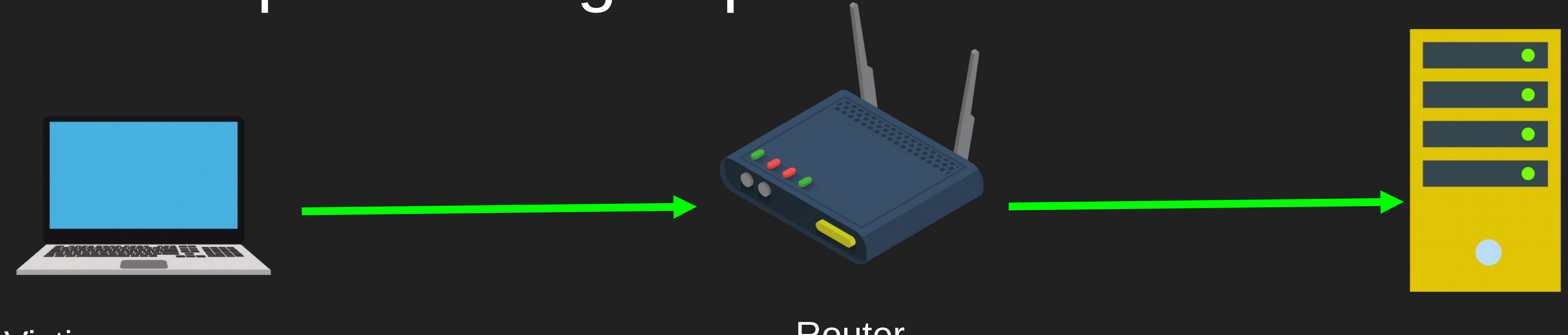
NAT FORWARDING TABLE

10.0.0.1 <-> 12.0.0.1

INTERNET

WEB SERVER

NAT Slipstreaming Explained



Victim
IP: 10.0.0.2
Running service on 8080

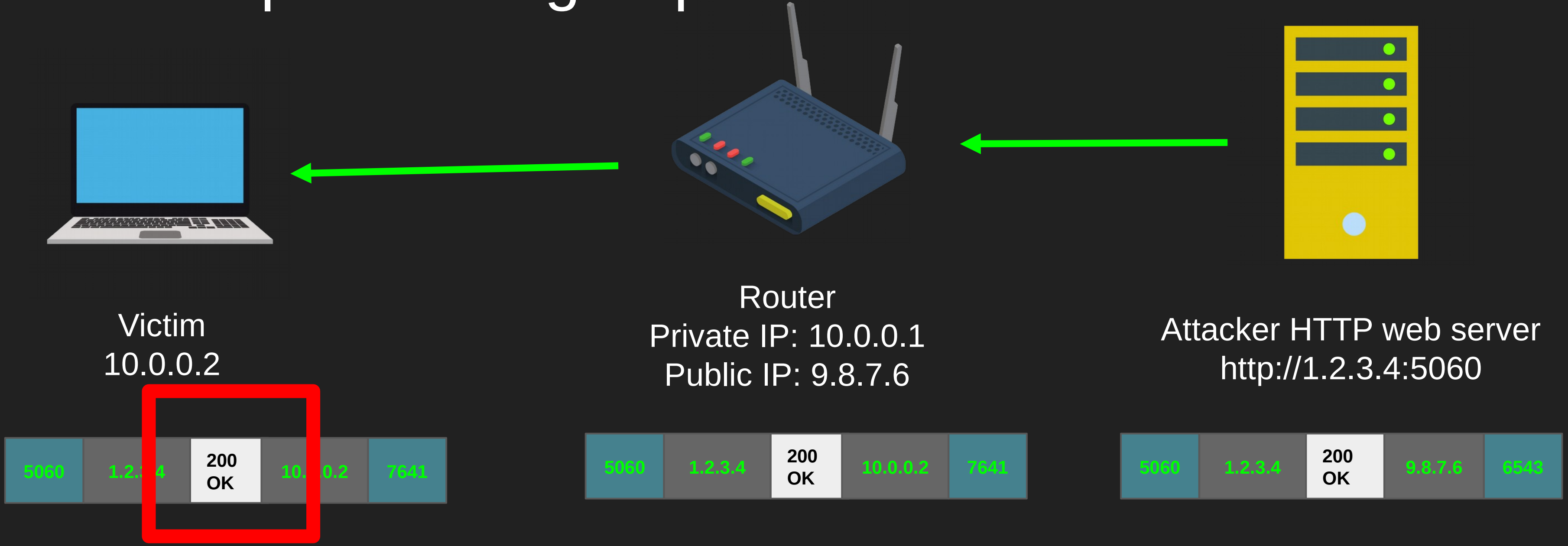
Router
Private IP: 10.0.0.1
Public IP: 9.8.7.6

Attacker HTTP web server
http://1.2.3.4:5060

7641	10.0.0.2	GET/	1.2.3.4	5060
6543	9.8.7.6	GET/	1.2.3.4	5060
6543	9.8.7.6	GET/	1.2.3.4	5060

Internal IP	Internal Port	Ext IP	Ext Port	Dest IP	Dest Port
10.0.0.2	7641	9.8.7.6	6543	1.2.3.4	5060

NAT Slipstreaming Explained



Victim
10.0.0.2

5060	1.2. 4	200 OK	10. 0.2	7641

Router
Private IP: 10.0.0.1
Public IP: 9.8.7.6

5060	1.2.3.4	200 OK	10.0.0.2	7641

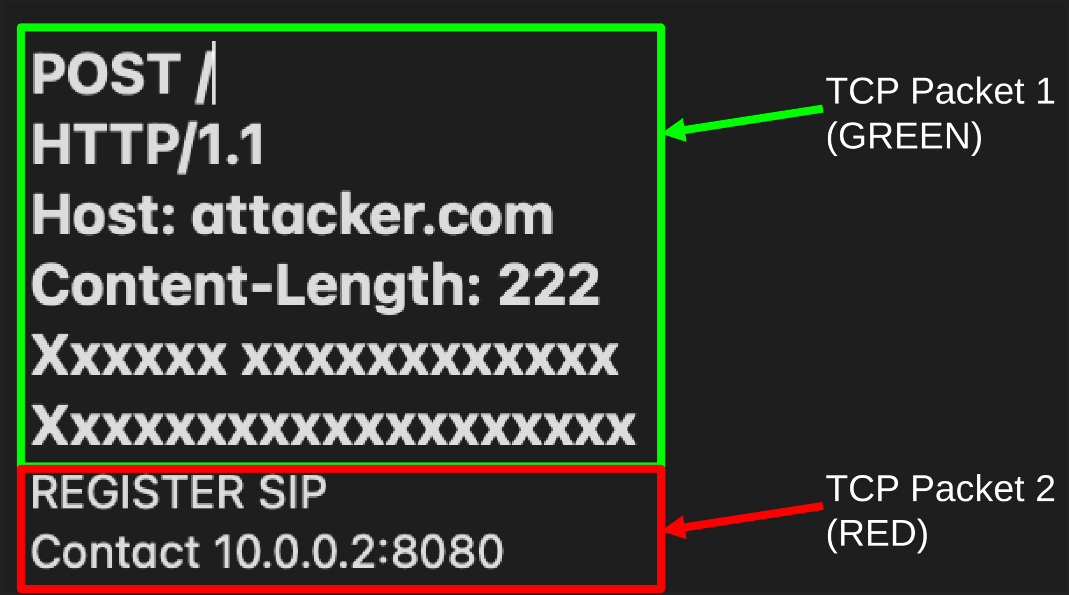
Attacker HTTP web server
http://1.2.3.4:5060

5060	1.2.3.4	200 OK	9.8.7.6	6543

Internal IP	Internal Port	Ext IP	Ext Port	Dest IP	Dest Port
10.0.0.2	7641	9.8.7.6	6543	1.2.3.4	5060

NAT Slipstreaming Explained

- Victim gets back malicious HTML Page
- Submits a special POST request to http://1.2.3.4:5060 with a malicious body

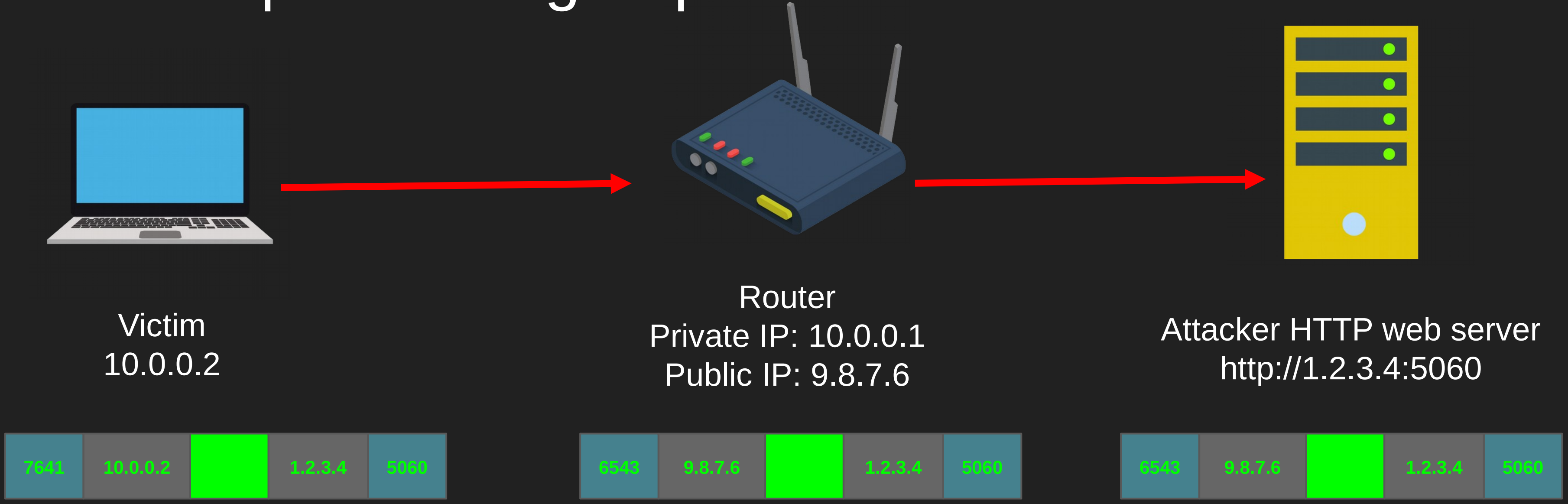


```
POST /
HTTP/1.1
Host: attacker.com
Content-Length: 222
Xxxxxx xxxxxxxxxxxx
Xxxxxxxxxxxxxxxxxxx
REGISTER SIP
Contact 10.0.0.2:8080
```

TCP Packet 1
(GREEN)

TCP Packet 2
(RED)

NAT Slipstreaming Explained



Victim
10.0.0.2

Router
Private IP: 10.0.0.1
Public IP: 9.8.7.6

Attacker HTTP web server
http://1.2.3.4:5060

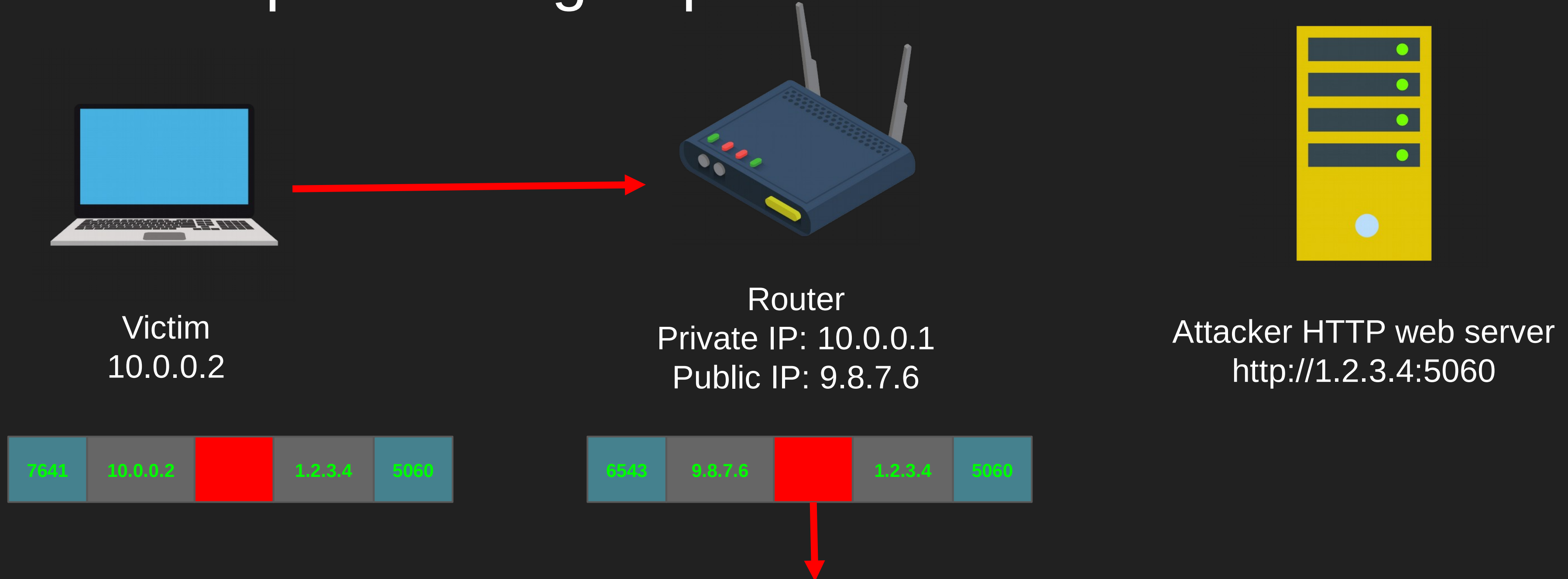
7641 | 10.0.0.2 | 🟩 | 1.2.3.4 | 5060

6543 | 9.8.7.6 | 🟩 | 1.2.3.4 | 5060

6543 | 9.8.7.6 | 🟩 | 1.2.3.4 | 5060

Internal IP	Internal Port	Ext IP	Ext Port	Dest IP	Dest Port
10.0.0.2	7641	9.8.7.6	6543	1.2.3.4	5060

NAT Slipstreaming Explained



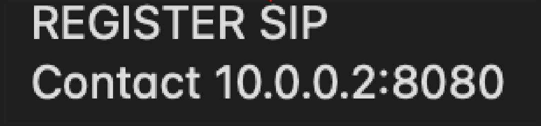
Victim
10.0.0.2

Router
Private IP: 10.0.0.1
Public IP: 9.8.7.6

Attacker HTTP web server
http://1.2.3.4:5060

7641	10.0.0.2	🟥	1.2.3.4	5060

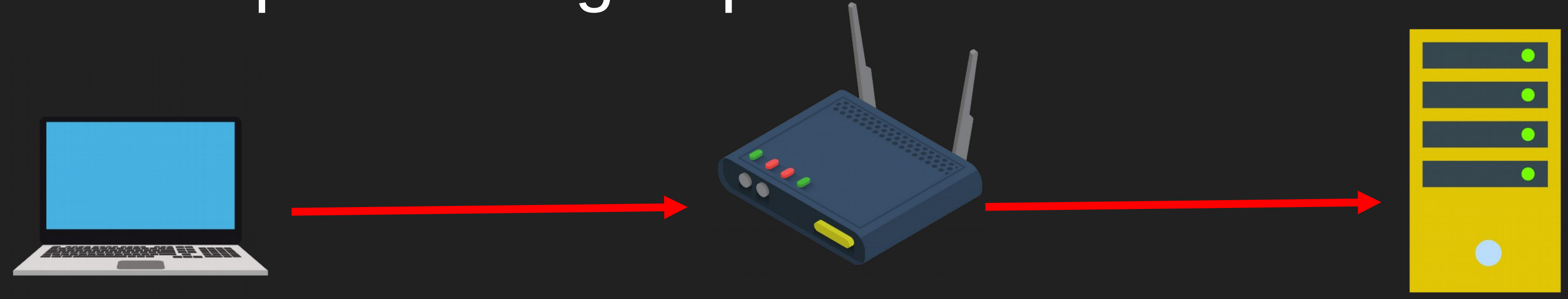
6543	9.8.7.6	🟥	1.2.3.4	5060



REGISTER SIP
Contact 10.0.0.2:8080

Router sees a packet targeted to 5060 and has REGISTER SIP, it thinks its a SIP message from the client and OPENS PORT 8080 and adds a NAT entry to allow external access (only if ALG SIP is enabled)

NAT Slipstreaming Explained



Victim
10.0.0.2

Router
Private IP: 10.0.0.1
Public IP: 9.8.7.6

Attacker HTTP web server
http://1.2.3.4:5060

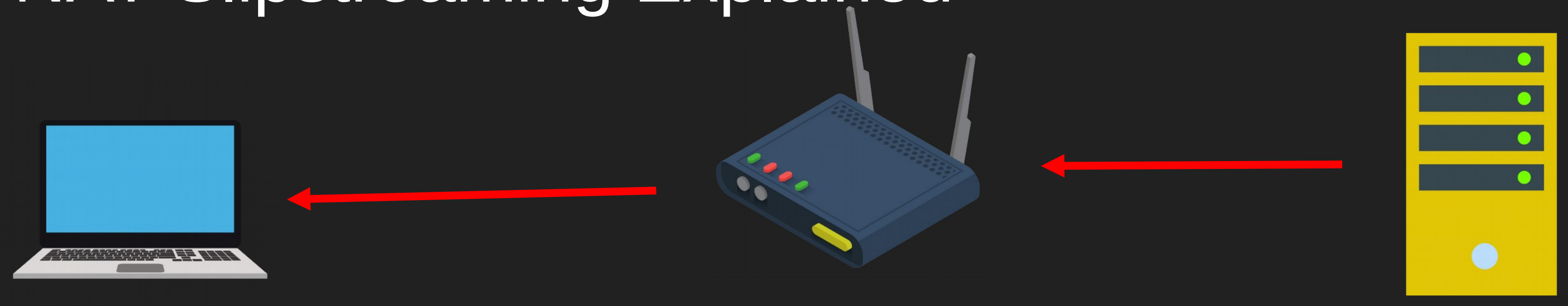
7641	10.0.0.2	🟥	1.2.3.4	5060

6543	9.8.7.6	🟥	1.2.3.4	5060

6543	9.8.7.6	🟥	1.2.3.4	5060

Internal IP	Internal Port	Ext IP	Ext Port	Dest IP	Dest Port
10.0.0.2	7641	9.8.7.6	6543	1.2.3.4	5060
10.0.0.2	8080	9.8.7.6	8080	1.2.3.4	5060

NAT Slipstreaming Explained



Victim
10.0.0.2

Router
Private IP: 10.0.0.1
Public IP: 9.8.7.6

Attacker HTTP web server
http://1.2.3.4:5060

5060	1.2.3.4	GET /	10.0.0.2	8080

5060	1.2.3.4	GET/	10.0.0.2	8080

5060	1.2.3.4	GET/	9.8.7.6	8080

Internal IP	Internal Port	Ext IP	Ext Port	Dest IP	Dest Port
10.0.0.2	7641	9.8.7.6	6543	1.2.3.4	5060
10.0.0.2	8080	9.8.7.6	8080	1.2.3.4	5060

- NAT Slip streaming by Samy Kamkar [https://samy.pl/slipstream/]
- POC [https://github.com/samyk/slipstream]
- RFC2766 – Network Address Translation
- RFC3261 – SIP [session initiation protocol]
- RFC7742 – Web RTC