OST
Ostschweizer
Fachhochschule

Bind, Reverse, Web-Shells

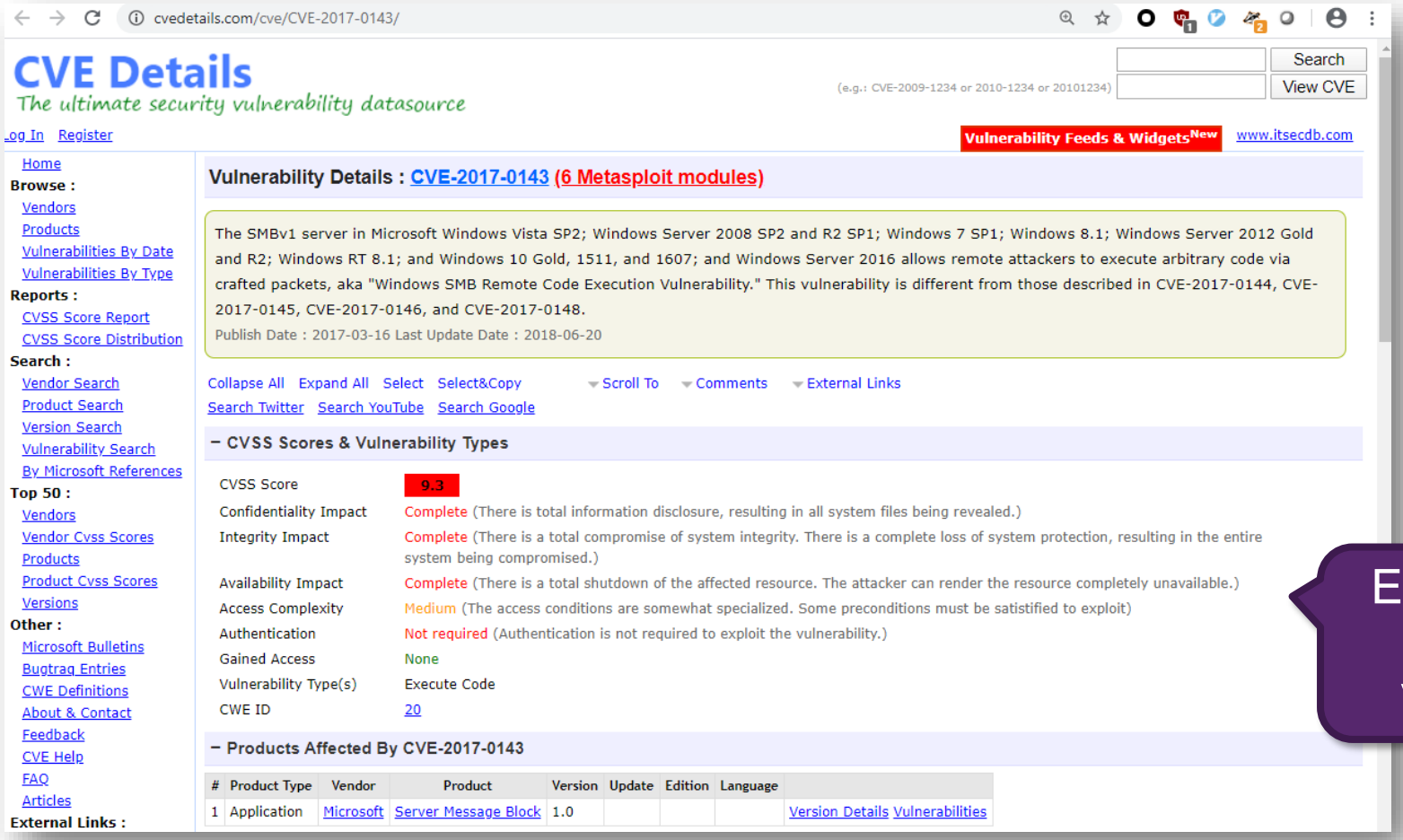
Einführung

Ivan Bütler

Abteilung Informatik, Rapperswil

Remote Code Execution (RCE)

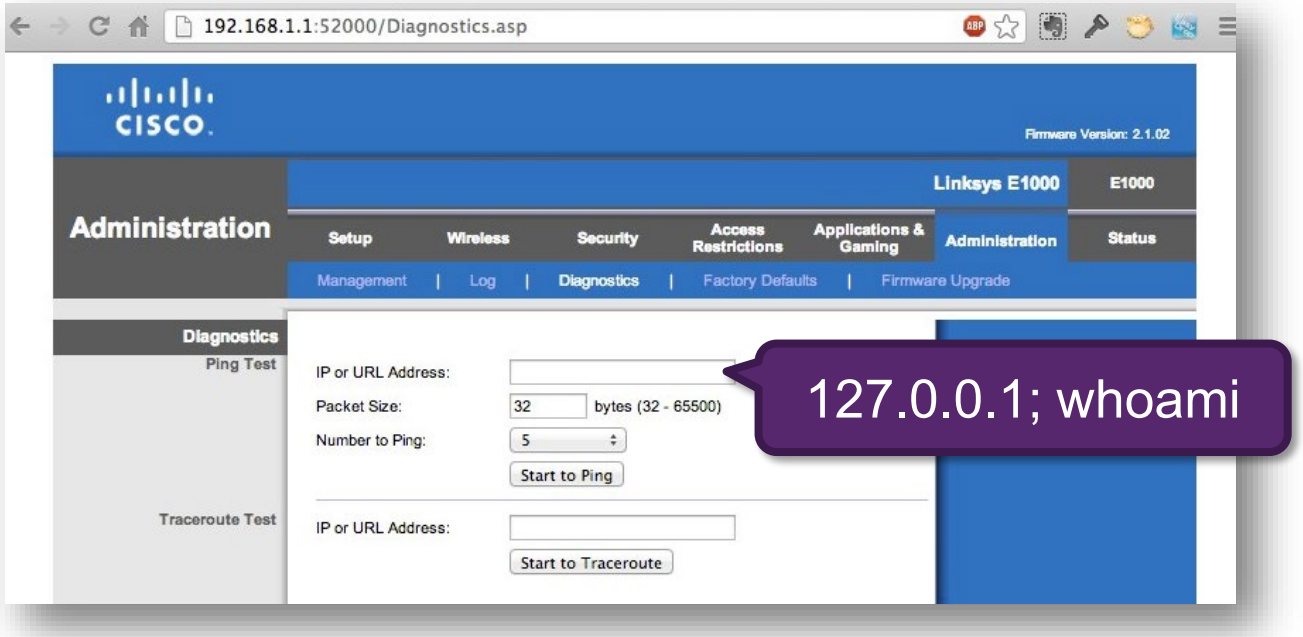
- Ability to trigger arbitrary code execution over a network.
- This is the holy grail an attacker wants on your system!



Example of the Eternalblue Vulnerability

How to get RCE?

- Command Injection
- File Upload (Upload a PHP file to a webserver)
- SQL Injections can sometimes be used to get RCE
- Buffer Overflow (write own instructions into the process memory and execute it)
- …

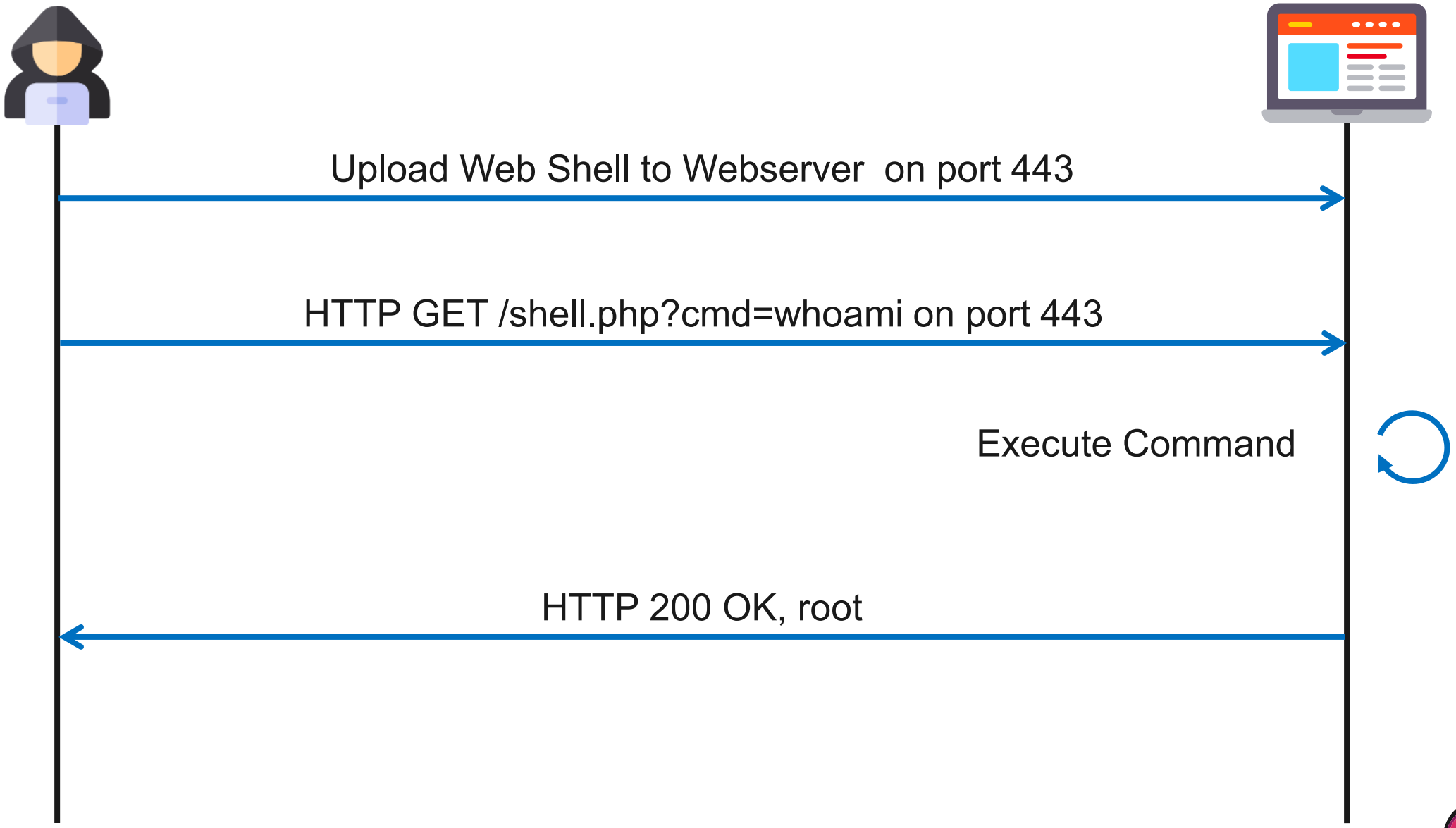


OST

Exploit Limitation

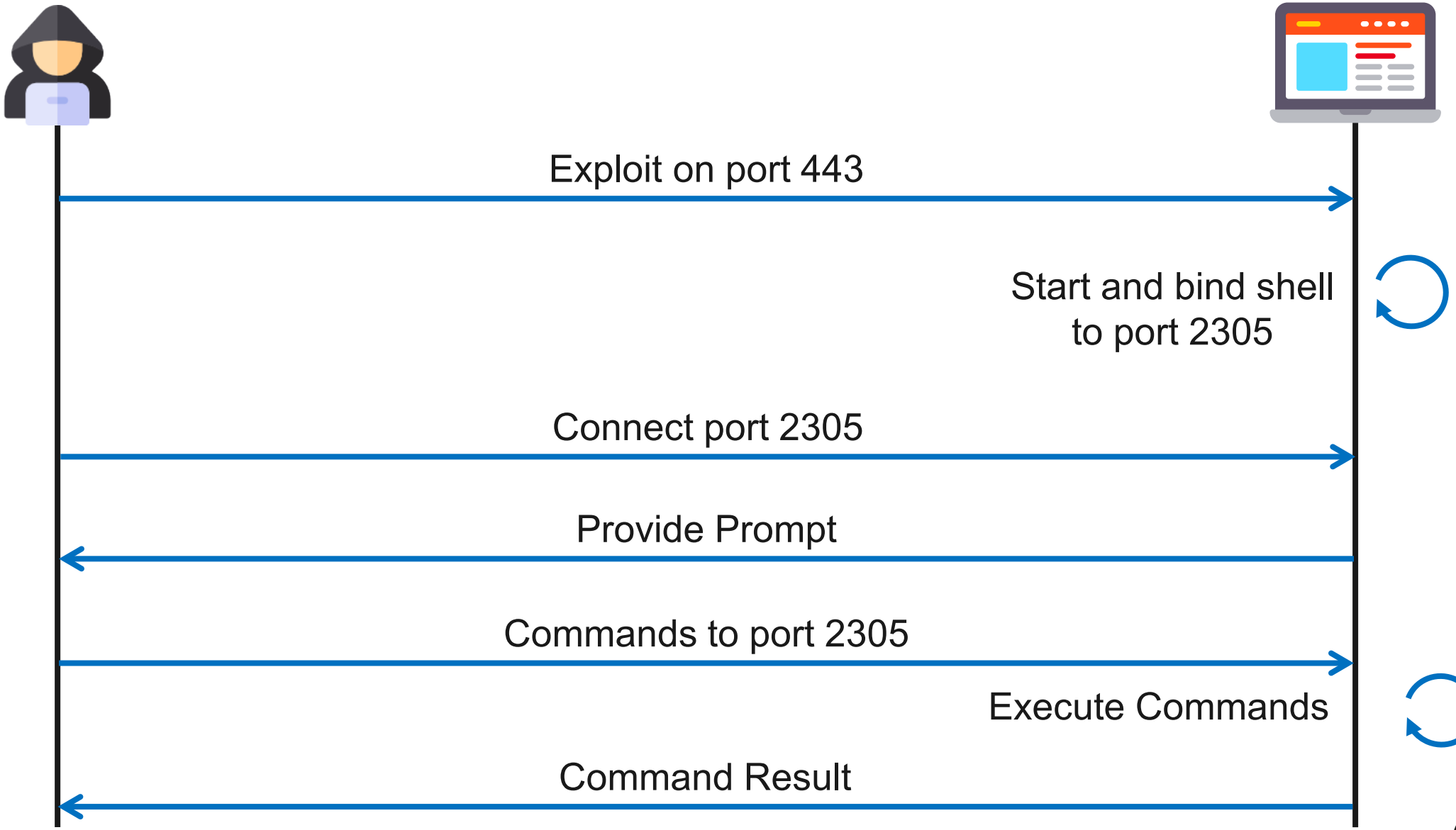
- Often, an exploit can only execute one command at a time
- Shells can be used to interactively execute commands on the system
- There are multiple types of shells
  - Web Shells
  - Bind Shells
  - Reverse Shells

Web Shell



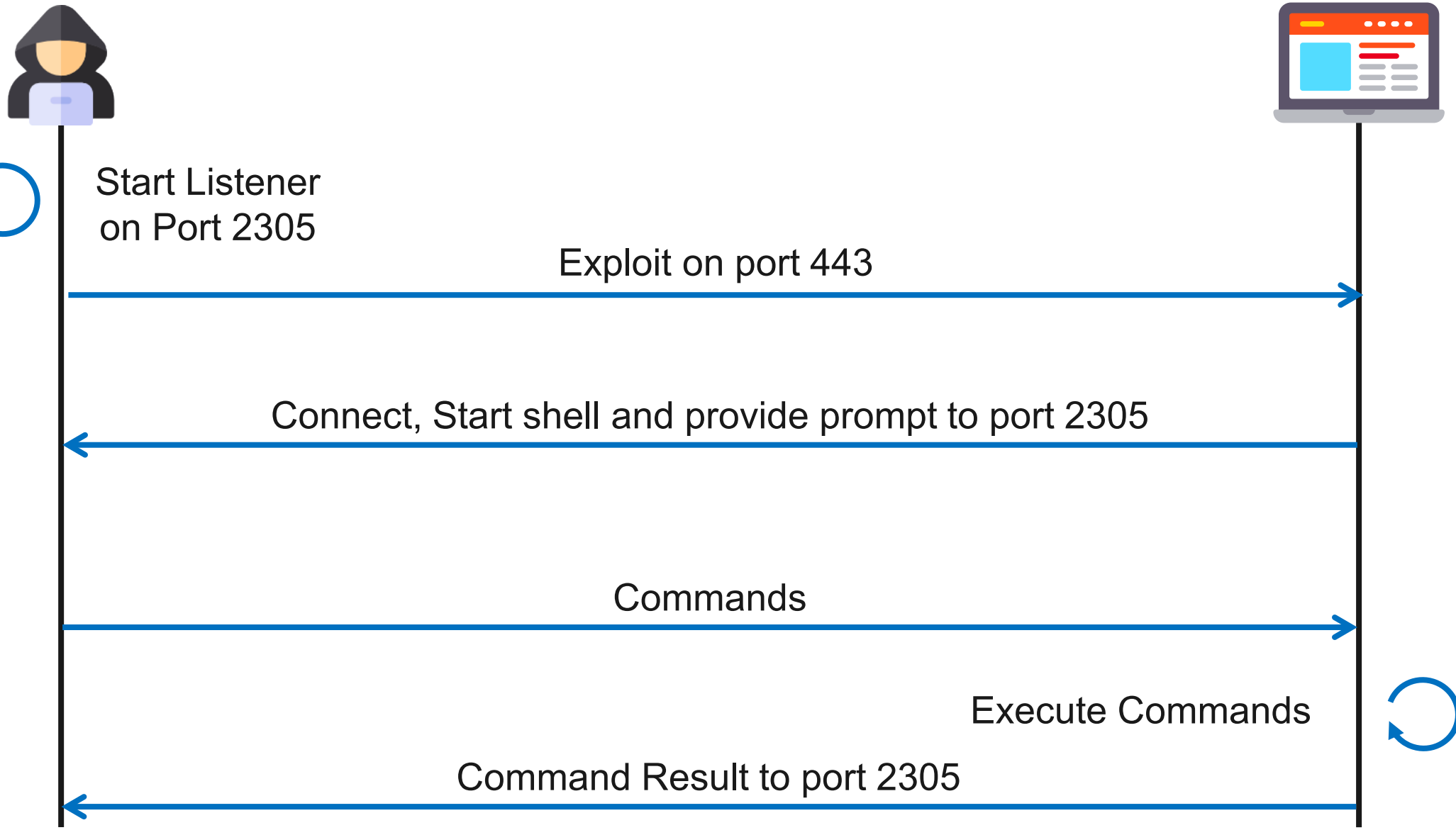
OST

Bind Shell



OST

Reverse Shell



OST