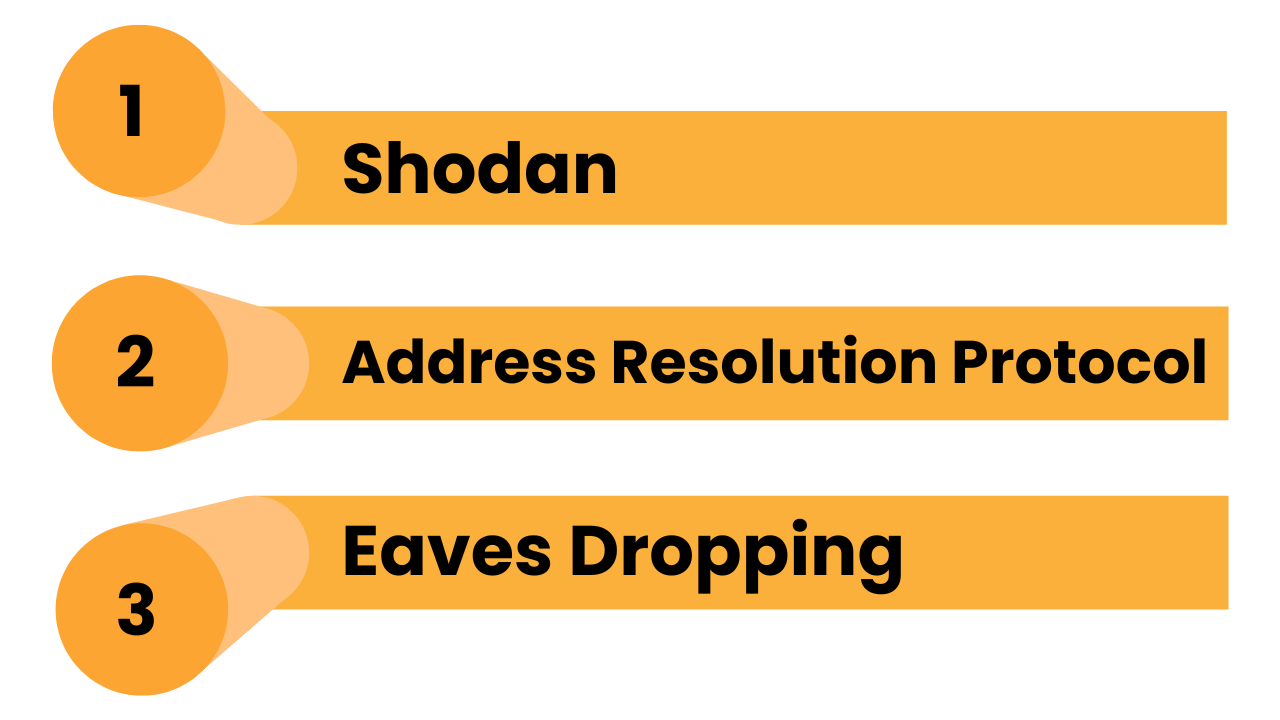


# Lesson 03: Tools for Footprinting (Shodan, Address Resolution Protocol, Eaves Dropping)



## Lesson Objectives

By the end of this lesson, you will be able to:

* Understand how to find connected devices and networks.
* Use tools to gather information from your own or test networks.
* Know the risks and limits of each tool.
* Use this data safely and legally in ethical hacking or cybersecurity testing.

## 1. What Are These Tools Used For?

## 

## 

## 

## 

## 1.1 Shodan – Search Engine for Devices



### What It Does:

Shodan is like Google — but for **internet-connected devices** (cameras, routers, servers, etc.).

### Website:

[shodan.io](https://www.shodan.io/)

### How to Use:

* Go to Shodan.io
* Type in search terms like:  
    
   apache country:"US"
* webcam port:554

### What You Can Find:

* Devices online (IoT, servers, etc.)
* Open ports and running services
* Device types and locations

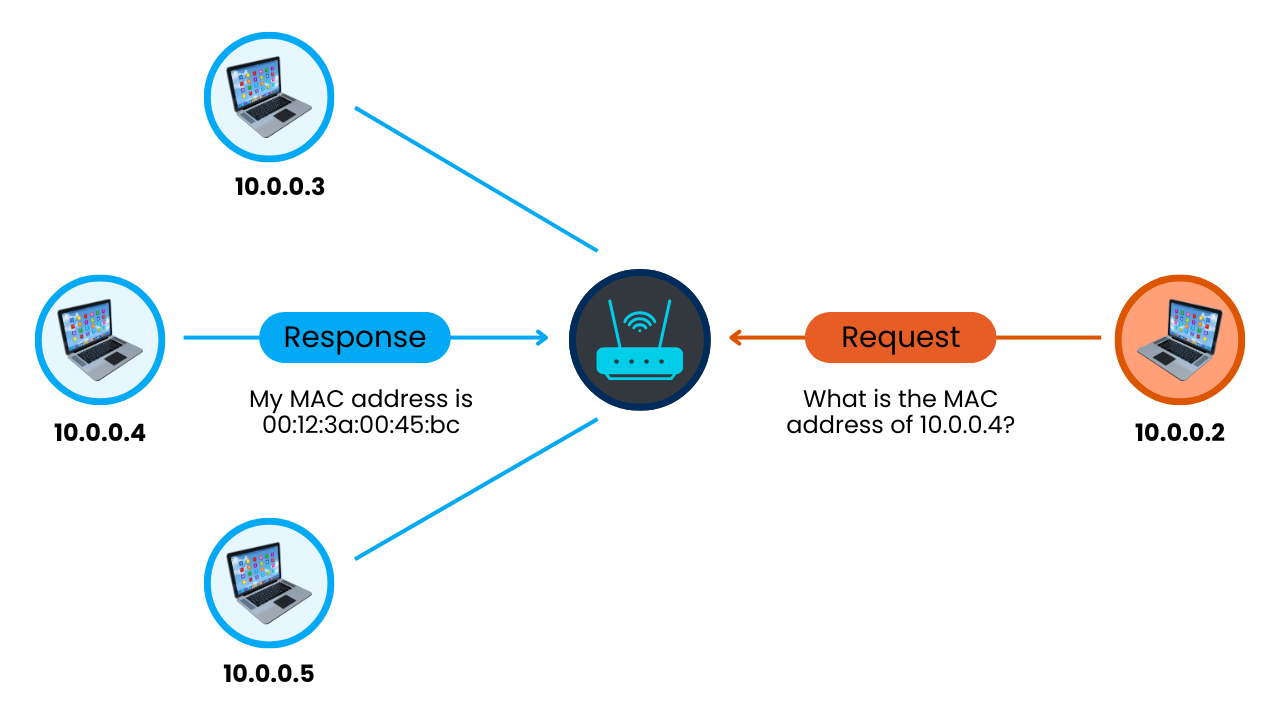
### Good For:

* Finding unsecured devices
* Researching exposed services

### Limitation:

* Only shows what’s publicly exposed
* Can be misused — so always **get permission**

## 1.2 ARP (Address Resolution Protocol)



### What It Does:

**ARP maps IP addresses to MAC addresses** (device IDs) on local networks.

### How to Use:

On Windows:

* arp -a

On Linux:

* sudo arp-scan --localnet

### What You See:

* Devices connected to your local network
* IP and MAC addresses
* Device manufacturer (sometimes)

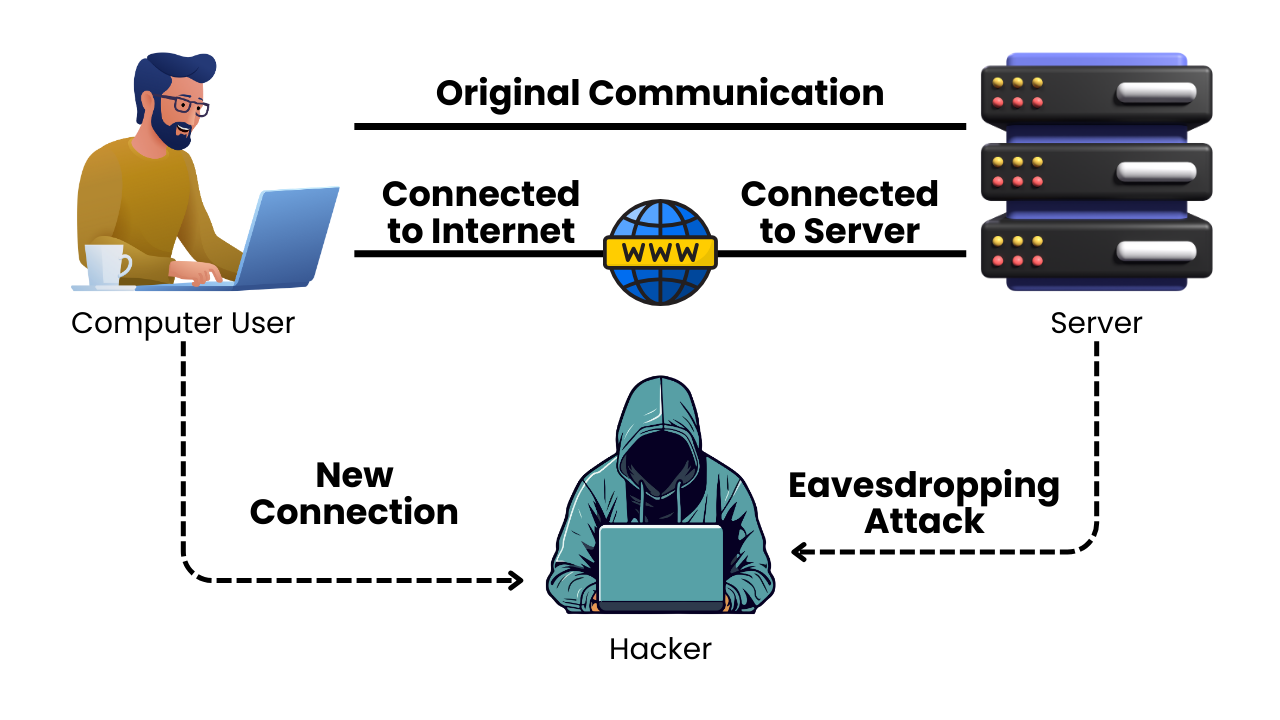
### Good For:

* Finding all active devices on your local network
* Mapping small internal networks

### Limitation:

* Works only on the same local network
* Doesn’t work across the internet

## 1.3 Eavesdropping (Network Sniffing)



### What It Does:

Captures and shows **network traffic** (data being sent and received).

### Tools You Can Use:

* **Wireshark** (GUI)
* **Tcpdump** (command line)

### How to Use:

Example (Tcpdump):

* sudo tcpdump -i eth0 port 80

In Wireshark:

* Select your network interface
* Start capture
* Filter by protocol (e.g., HTTP, DNS)

### What You See:

* Packets going through your network
* Websites visited, data sent (if unencrypted)

### Good For:

* Analyzing traffic
* Spotting insecure data (like passwords over HTTP)

### Limitation:

* Can only capture data on networks you’re connected to
* **Ethical rules apply** — never sniff traffic on networks you don’t own or control

## 3. Be Ethical!

* **Only sniff or scan your own network** — or get written permission.
* **Never connect to or control devices without approval**.
* **Respect privacy** — don’t view personal data.
* Follow **legal rules** — especially for public devices.

## 4. Key Takeaways

* **Shodan** helps you search for internet-exposed devices.
* **ARP** maps devices on your local network.
* **Eavesdropping tools** like Wireshark let you monitor network traffic.
* These are powerful tools — use them responsibly and with permission.
* Learn in safe labs or test environments only.