Cybersecurity Reconnaissance Project

Introduction

Reconnaissance is the initial phase of a cybersecurity assessment, where information about a target system or network is gathered. This project outlines **passive reconnaissance** (using Wappalyzer and Shodan) and **active reconnaissance** (using Nmap), explaining their methodologies, tools, and ethical considerations. The goal is to demonstrate how these techniques are used in penetration testing or threat intelligence while adhering to legal and ethical boundaries.

1. Passive Reconnaissance

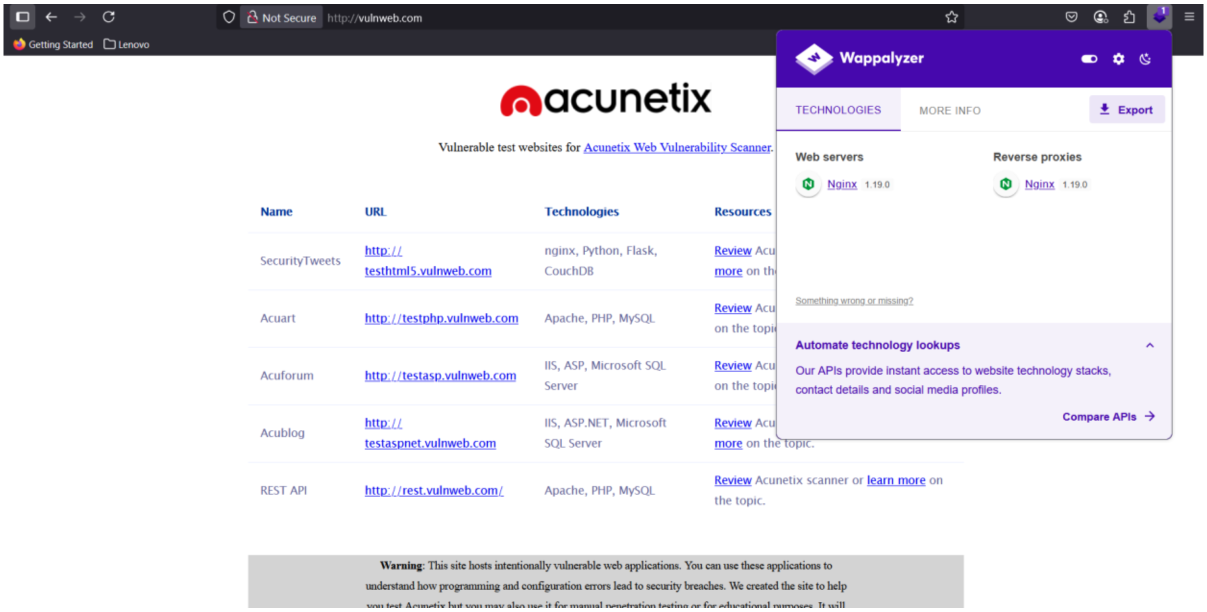
Passive reconnaissance involves gathering information about a target without directly interacting with it, minimizing the risk of detection. It leverages publicly available data or third-party services.

1.1 Wappalyzer

Overview: Wappalyzer is a browser extension that identifies technologies used on websites, such as content management systems (CMS), frameworks, and server software. It's ideal for understanding a target's web stack without sending requests directly to the server.

How to Use:

- **Installation**: Install Wappalyzer from the Firefox Add-ons store (`addons.mozilla.org`) or Chrome Web Store. Search for "Wappalyzer," add it to your browser, and pin the icon to the toolbar.
- **Usage**:
  - Visit the target website (e.g., **vulnweb.com)**.
  - Click the Wappalyzer icon in the browser toolbar.
  - Review the output, which lists technologies like WordPress (CMS), Apache (web server), or jQuery (JavaScript library).
- **Example**:

- 

Not Secure http://vulnweb.com

Getting Started Lenovo

acunetix

Vulnerable test websites for Acunetix Web Vulnerability Scanner.

Name	URL	Technologies	Resources
SecurityTweets	http:// testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acu more on th
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acu on the topi
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acu on the topi
Acublog	http:// testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acu more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help you test Acunetix but you may also use it for manual penetration testing or for educational purposes. It will

Wappalyzer

TECHNOLOGIES MORE INFO Export

Web servers	Reverse proxies
Nginx 1.19.0	Nginx 1.19.0

Something wrong or missing?

Automate technology lookups

Our APIs provide instant access to website technology stacks, contact details and social media profiles.

Compare APIs →

  - Use Case: Identifying outdated CMS versions (e.g., Drupal 8) to check for known vulnerabilities via CVE databases.

Advantages:

- No direct interaction with the target, reducing detection risk.
- Quick and easy to use via browser.
- Provides insights into web stack for further vulnerability research.

Limitations:

- Limited to web-based technologies.
- May not detect custom or obfuscated software.
- Dependent on browser compatibility (e.g., Firefox/Chrome).

Ethical Considerations:

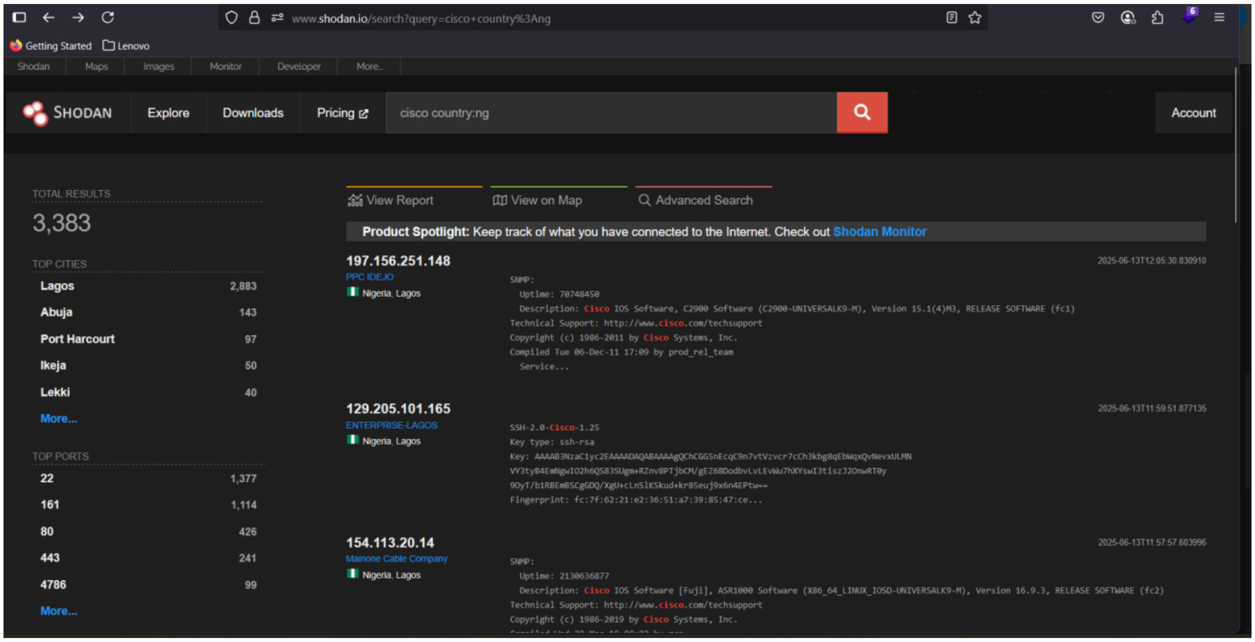
- Use Wappalyzer only on websites you have permission to analyze.
- Avoid sharing sensitive findings publicly to prevent exploitation by malicious actors.

1.2 Shodan

Overview: Shodan is a search engine for internet-connected devices, indexing servers, IoT devices, and more. It’s used for OSINT (Open-Source Intelligence) to identify exposed services without direct interaction.

How to Use:

- **Setup**: Register at www.shodan.io for a free or paid account. Free accounts have limited query credits.
- **Basic Search**:
  - Log in and use the search bar.
  - Enter queries like `port:80 city:New York` to find HTTP servers in New York or `os:Linux org:ExampleCorp` to find Linux systems in a specific organization.
- **Advanced Filters**:
  - Use filters like `net:192.168.0.0/24` for IP ranges or `vulnerability:CVE-2021-44228` for specific vulnerabilities.
  - Example: `apache country:US` lists Apache servers in the US.
- **CLI/API**: Install the Shodan CLI (`pip install shodan`) for terminal searches or use the API (paid feature) for automation.
- **Example**:



cisco country:ng

TOTAL RESULTS

3,383

TOP CITIES	
Lagos	2,883
Abuja	143
Port Harcourt	97
Ikeja	50
Lekki	40
More...	

TOP PORTS	
22	1,377
161	1,114
80	426
443	241
4786	99
More...	

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

197.156.251.148 2025-06-13T12:05:30.830910

PPC IDEJO

Nigeria, Lagos

```
SNMP:
  Uptime: 70748450
  Description: Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 06-Dec-11 17:09 by prod_rel_team
  Service...
```

129.205.101.165 2025-06-13T11:59:51.877135

ENTERPRISE-LAGOS

Nigeria, Lagos

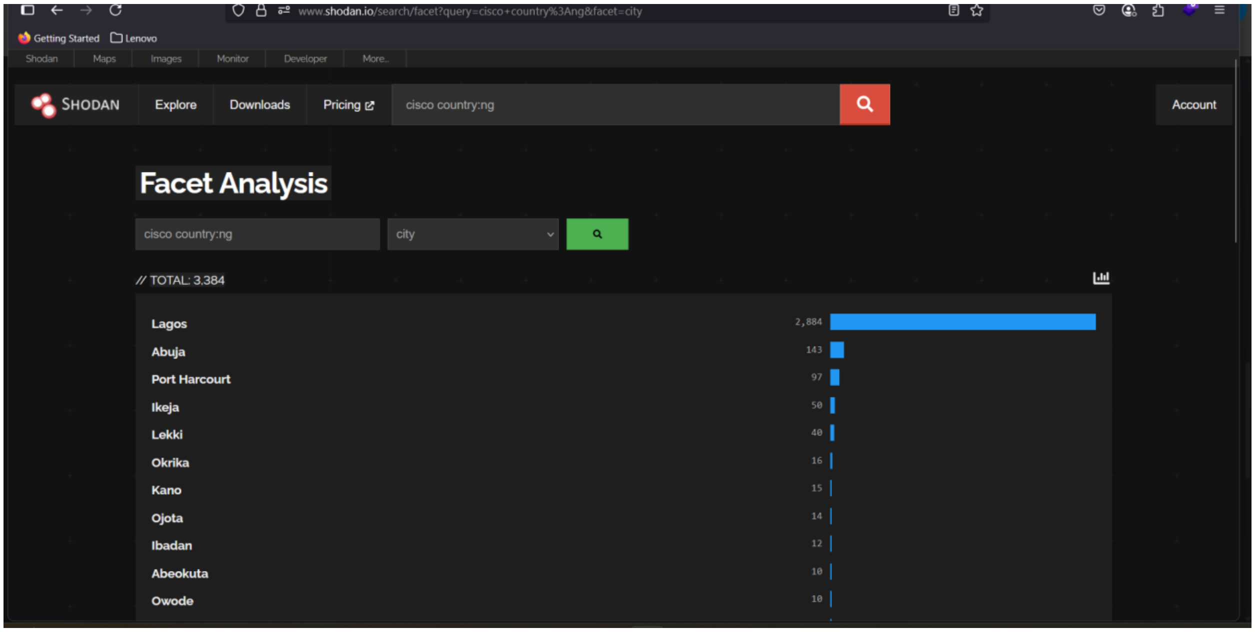
```
SSH-2.0-Cisco-1.25
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgQChCGG5nEcqC9n7vtVzvcr7cCh3kbg8qEbWqxQvNevxULMN
VY3tyB4EmNgwIO2h6QS83SUgm+RZnv8PTjbCM/gEZ68DodbvLvLEvWu7hXYswI3tiszJ2OnwRT0y
9OyT/b1RBEmBSCgGDQ/XgU+cLnSlKSkud+kr85euj9x6n4EPtw==
Fingerprint: fc:7f:62:21:e2:36:51:a7:39:85:47:ce...
```

154.113.20.14 2025-06-13T11:57:57.603996

Mainone Cable Company

Nigeria, Lagos

```
SNMP:
  Uptime: 2130636877
  Description: Cisco IOS Software [Fuji], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.9.3, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
```



Facet Analysis

cisco country:ng | city

// TOTAL: 3.384

Lagos	2,884
Abuja	143
Port Harcourt	97
Ikeja	50
Lekki	40
Okrika	16
Kano	15
Ojota	14
Ibadan	12
Abeokuta	10
Owode	10

- Query: cisco nigeria:ng
- Output: List of IP addresses, ports, and device details for webcams in London.
- Use Case: Identifying misconfigured IoT devices with open ports.

Advantages:

- Accesses a vast database of internet-facing devices.
- Supports complex queries for precise targeting.
- Useful for mapping an organization’s external attack surface.

Limitations:

- Free accounts have query and scan limits.
- Data may be outdated or incomplete.
- Requires careful query crafting to avoid irrelevant results.

Ethical Considerations:

- Only query devices or networks you’re authorized to analyze.
- Avoid scanning or exploiting devices without explicit permission, as this may violate laws like the Computer Fraud and Abuse Act (CFAA).

2. Active Reconnaissance

Active reconnaissance involves direct interaction with the target system, such as sending packets to probe for open ports or services. This increases the risk of detection but provides detailed insights.

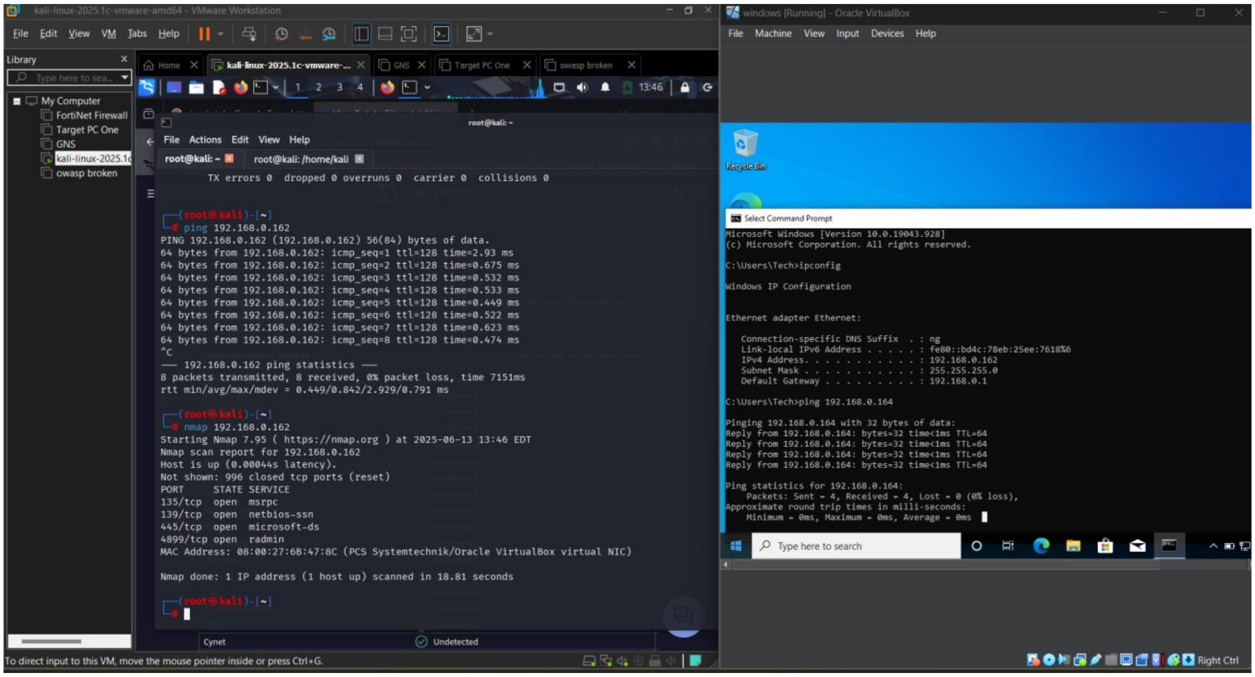
2.1 Nmap

Overview: Nmap (Network Mapper) is an open-source tool for network scanning and host discovery. It identifies open ports, services, operating systems, and vulnerabilities by sending crafted packets to the target.

How to Use:

- **Installation**: Install Nmap on Linux (`apt install nmap`), Windows, or macOS (`brew install nmap`). Download from `nmap.org`.
- **Basic Scan**:
    - Open a terminal and run: `nmap <target>`, e.g., `nmap 192.168.0.162`.
    - Output shows open ports, services, and states (e.g., port 80/tcp open, HTTP).
- **Common Commands**:
    - **Port Scan**: `nmap -p 1-1000 <target>` scans ports 1–1000.
    - **Service Detection**: `nmap -sV <target>` identifies service versions (e.g., Apache 2.4.41).
    - **OS Detection**: `nmap -O <target>` guesses the operating system.
    - **Aggressive Scan**: `nmap -A <target>` combines service, OS, and script scanning.
    - **Stealth Scan**: `nmap -sS <target>` uses SYN packets to reduce detection.

- **Example**:


kali-linux-2025.1c-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
FortiNet Firewall
Target PC One
GNS
kali-linux-2025.1c
owasp broken
Home
kali-linux-2025.1c-vmware-...
GNS
Target PC One
owasp broken
13:46
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: /home/kali
Cynet
Undetected
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
windows [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Select Command Prompt
Type here to search
Right Ctrl

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[~]
└─# ping 192.168.0.162
PING 192.168.0.162 (192.168.0.162) 56(84) bytes of data.
64 bytes from 192.168.0.162: icmp_seq=1 ttl=128 time=2.93 ms
64 bytes from 192.168.0.162: icmp_seq=2 ttl=128 time=0.675 ms
64 bytes from 192.168.0.162: icmp_seq=3 ttl=128 time=0.532 ms
64 bytes from 192.168.0.162: icmp_seq=4 ttl=128 time=0.533 ms
64 bytes from 192.168.0.162: icmp_seq=5 ttl=128 time=0.449 ms
64 bytes from 192.168.0.162: icmp_seq=6 ttl=128 time=0.522 ms
64 bytes from 192.168.0.162: icmp_seq=7 ttl=128 time=0.623 ms
64 bytes from 192.168.0.162: icmp_seq=8 ttl=128 time=0.474 ms
^C
--- 192.168.0.162 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7151ms
rtt min/avg/max/mdev = 0.449/0.842/2.929/0.791 ms

┌──(root㉿kali)-[~]
└─# nmap 192.168.0.162
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-13 13:46 EDT
Nmap scan report for 192.168.0.162
Host is up (0.00044s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
4899/tcp open  radmin
MAC Address: 08:00:27:6B:47:8C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.81 seconds

┌──(root㉿kali)-[~]
└─#
```

```
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Tech>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ng
   Link-local IPv6 Address . . . . . : fe80::bd4c:78eb:25ee:7618%6
   IPv4 Address. . . . . . . . . . . : 192.168.0.162
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\Tech>ping 192.168.0.164

Pinging 192.168.0.164 with 32 bytes of data:
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

  - Use Case: Identifying outdated Apache versions for potential exploits.

Advantages:

- Provides detailed, real-time data about the target.
- Highly customizable with scripts (NSE) for vulnerability scanning.
- Supports stealth options to minimize detection.

Limitations:

- Direct interaction risks detection by firewalls or IDS/IPS.
- May be blocked by network defenses.
- Requires root privileges for some scans (e.g., SYN or OS detection).

Ethical Considerations:

- Obtain explicit permission from the target's owner before scanning.
- Avoid aggressive scans on production systems, as they may cause disruptions.
- Comply with local laws and terms of service for cloud-hosted targets.

3. Practical Example: Reconnaissance Workflow

Scenario: You're tasked with assessing the external attack surface of a fictional company, `example.com`, with permission.

1. **Passive Recon with Wappalyzer**:
    a. Visit `example.com` and use Wappalyzer.
    b. Findings: WordPress 5.8 (outdated), Nginx server, Google Analytics.
    c. Action: Research CVEs for WordPress 5.8 to identify potential exploits.
2. **Passive Recon with Shodan**:
    a. Query: `org:Example hostname:example.com port:80`.
    b. Findings: IP `93.184.216.34` running Apache on port 80, located in the US.
    c. Action: Note the IP for further analysis and check for exposed services.
3. **Active Recon with Nmap**:
    a. Command: `nmap -sV -p 80,443 93.184.216.34`.
    b. Findings: Port 80 (Apache 2.4.29), port 443 (HTTPS, same version).
    c. Action: Cross-reference Apache version with CVE databases for vulnerabilities.

Outcome: Combine findings to create a report detailing the web stack, exposed services, and potential vulnerabilities, ensuring all actions are documented and authorized.

4. Ethical and Legal Guidelines

- **Authorization**: Always obtain written permission before performing reconnaissance, especially active scans.
- **Scope**: Stay within the defined scope of the engagement to avoid legal issues.
- **Data Handling**: Securely store and dispose of collected data to protect sensitive information.
- **Laws**: Comply with regulations like GDPR, CFAA, or local cybersecurity laws.
- **Responsible Disclosure**: Report vulnerabilities to the target owner promptly and confidentially.

5. Conclusion

Passive reconnaissance (Wappalyzer, Shodan) and active reconnaissance (Nmap) are complementary techniques for gathering intelligence about a target. Passive methods minimize detection risk, while active methods provide deeper insights at the cost of potential exposure. By combining these tools ethically and systematically, cybersecurity professionals can map attack surfaces and identify vulnerabilities effectively.

Resources:

- Wappalyzer: `wappalyzer.com`
- Shodan Help: `help.shodan.io`
- Nmap Documentation: `nmap.org/docs`
- TryHackMe: Shodan and Nmap modules
- YouTube: “Mastering Shodan.io” by InfoSec Pat, “Nmap Tutorial” by Hak5