Penetration Testing Toolkit - Output Report

1. Main Menu - Pen_Test_Toolkit (Main.py)

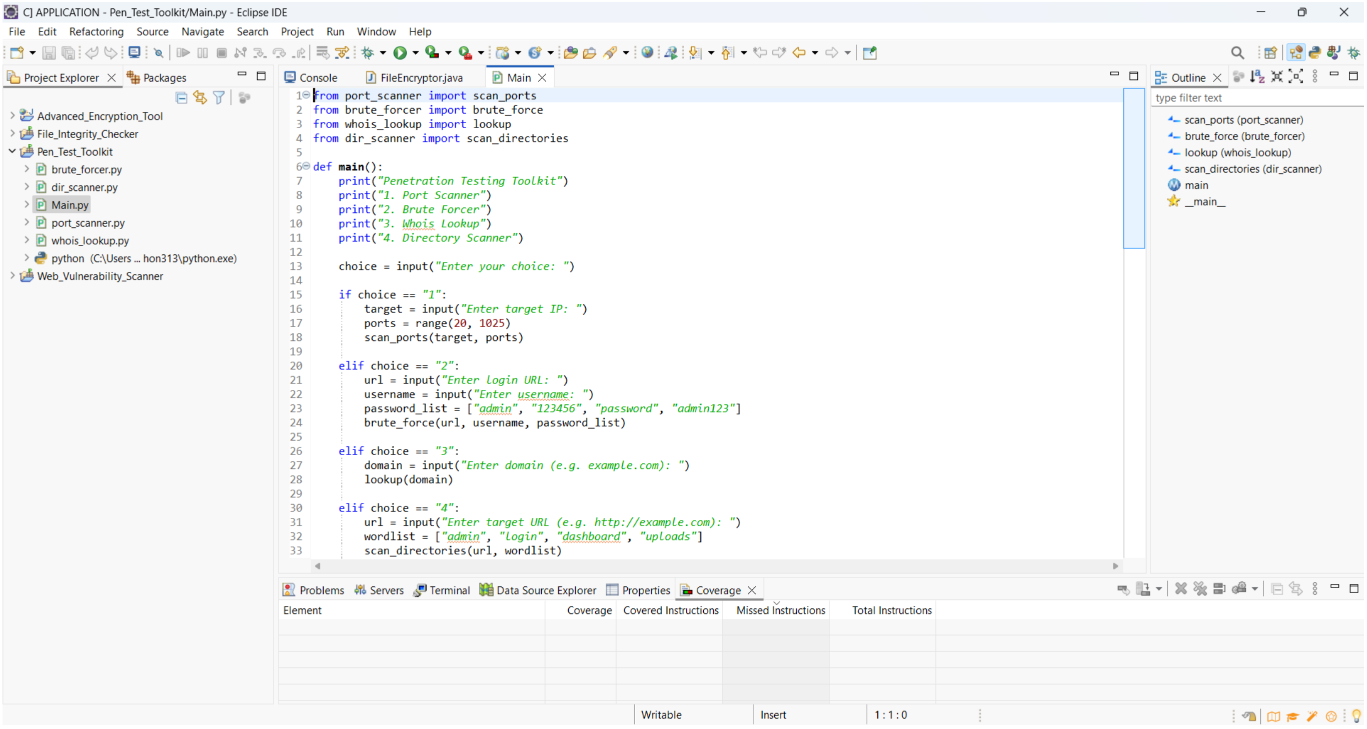
This is the main interface of your toolkit, offering 4 penetration testing tools:

1. Port Scanner

2. Brute Forcer

3. Whois Lookup

4. Directory Scanner



```python
from port_scanner import scan_ports
from brute_forcer import brute_force
from whois_lookup import lookup
from dir_scanner import scan_directories

def main():
    print("Penetration Testing Toolkit")
    print("1. Port Scanner")
    print("2. Brute Forcer")
    print("3. Whois Lookup")
    print("4. Directory Scanner")

    choice = input("Enter your choice: ")

    if choice == "1":
        target = input("Enter target IP: ")
        ports = range(20, 1025)
        scan_ports(target, ports)

    elif choice == "2":
        url = input("Enter login URL: ")
        username = input("Enter username: ")
        password_list = ["admin", "123456", "password", "admin123"]
        brute_force(url, username, password_list)

    elif choice == "3":
        domain = input("Enter domain (e.g. example.com): ")
        lookup(domain)

    elif choice == "4":
        url = input("Enter target URL (e.g. http://example.com): ")
        wordlist = ["admin", "login", "dashboard", "uploads"]
        scan_directories(url, wordlist)
```

Penetration Testing Toolkit - Output Report

2. Port Scanner

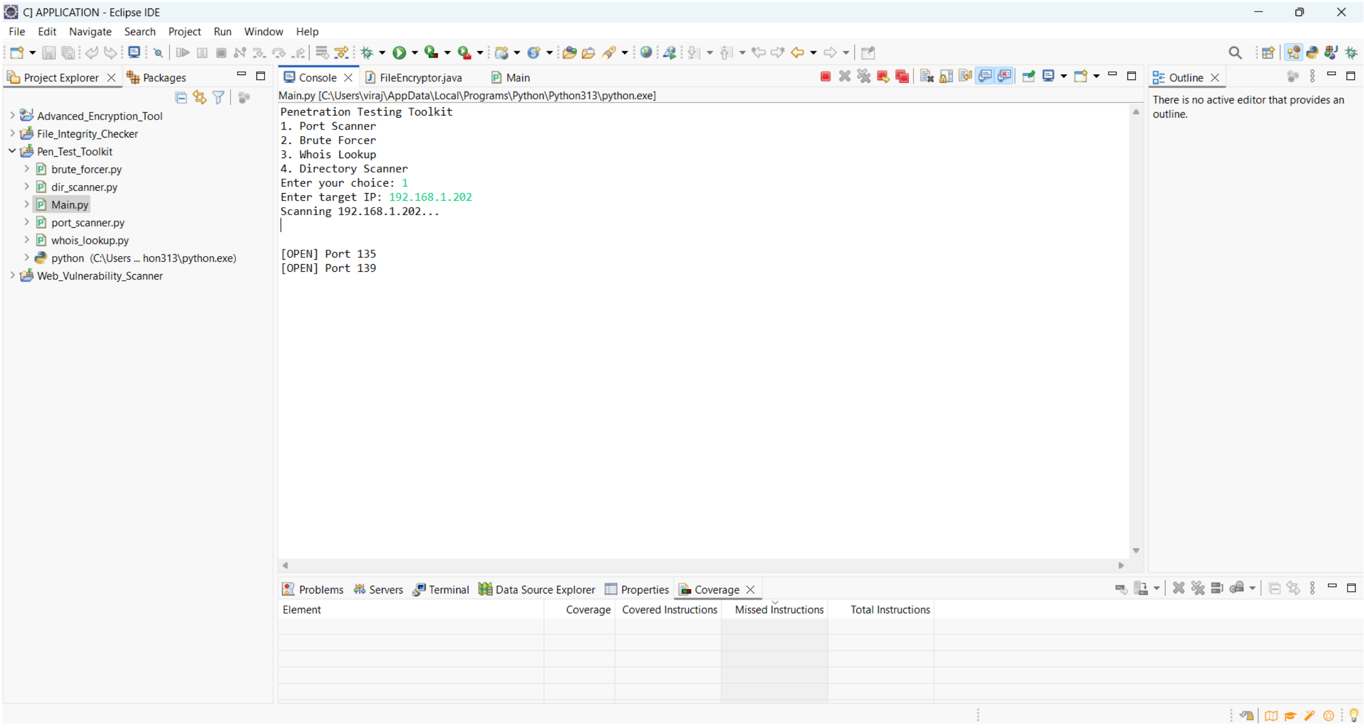
Input Target IP: 192.168.1.202

Result:

[OPEN] Port 135

[OPEN] Port 139

These ports are open on the target system, often used for Windows services like RPC and NetBIOS.



Main.py [C:\Users\viraj\AppData\Local\Programs\Python\Python313\python.exe]

```
Penetration Testing Toolkit
1. Port Scanner
2. Brute Forcer
3. Whois Lookup
4. Directory Scanner
Enter your choice: 1
Enter target IP: 192.168.1.202
Scanning 192.168.1.202...


[OPEN] Port 135
[OPEN] Port 139
```

Penetration Testing Toolkit - Output Report

3. Brute Forcer

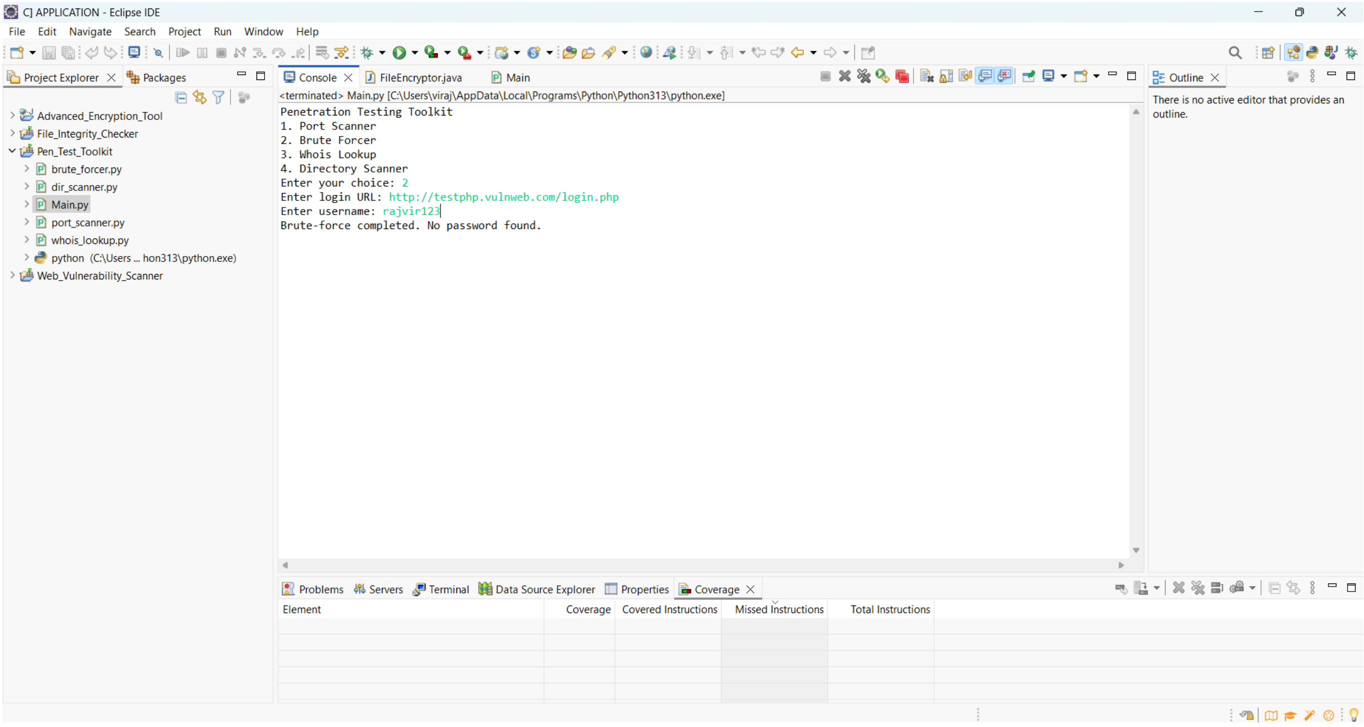
URL: http://testphp.vulnweb.com/login.php

Username: rajvir123

Tried passwords: admin, 123456, password, admin123

Result: No password matched the username.

This module simulates a login brute-force attack using a small wordlist.



```
<terminated> Main.py [C:\Users\viraj\AppData\Local\Programs\Python\Python313\python.exe]
Penetration Testing Toolkit
1. Port Scanner
2. Brute Forcer
3. Whois Lookup
4. Directory Scanner
Enter your choice: 2
Enter login URL: http://testphp.vulnweb.com/login.php
Enter username: rajvir123
Brute-force completed. No password found.
```

There is no active editor that provides an outline.

Element	Coverage	Covered Instructions	Missed Instructions	Total Instructions

Penetration Testing Toolkit - Output Report

4. Whois Lookup

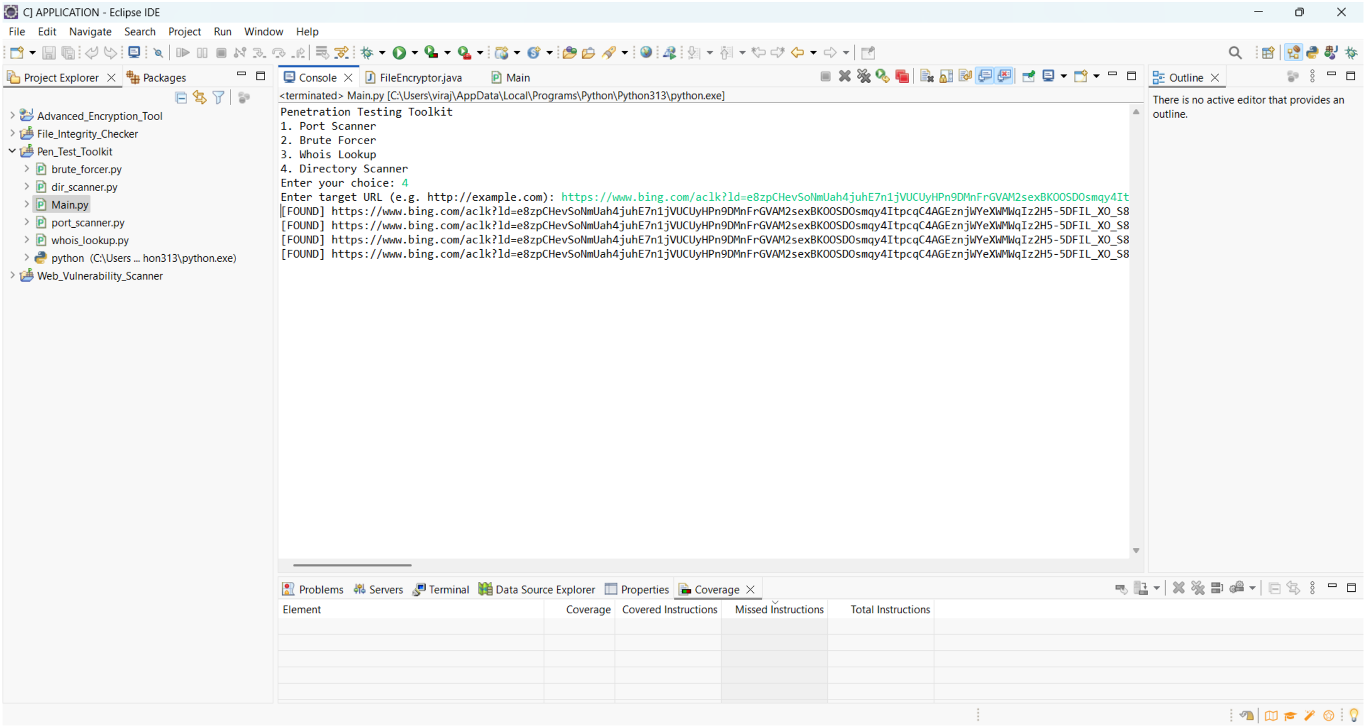
Domain: youtube.com

Registrar: MarkMonitor, Inc.

Creation Date: 2005

Expiry Date: 2026

Provides public registry information about the domain, useful for reconnaissance.



```
<terminated> Main.py [C:\Users\viraj\AppData\Local\Programs\Python\Python313\python.exe]
Penetration Testing Toolkit
1. Port Scanner
2. Brute Forcer
3. Whois Lookup
4. Directory Scanner
Enter your choice: 4
Enter target URL (e.g. http://example.com): https://www.bing.com/aclk?ld=e8zpCHevSoNmUah4juhE7n1jVUCUyHPn9DMnFrGVAM2sexBKOOSDOsmqy4It
[FOUND] https://www.bing.com/aclk?ld=e8zpCHevSoNmUah4juhE7n1jVUCUyHPn9DMnFrGVAM2sexBKOOSDOsmqy4ItpcqC4AGEznjWYeXWMWqIz2H5-5DFIL_XO_S8
[FOUND] https://www.bing.com/aclk?ld=e8zpCHevSoNmUah4juhE7n1jVUCUyHPn9DMnFrGVAM2sexBKOOSDOsmqy4ItpcqC4AGEznjWYeXWMWqIz2H5-5DFIL_XO_S8
[FOUND] https://www.bing.com/aclk?ld=e8zpCHevSoNmUah4juhE7n1jVUCUyHPn9DMnFrGVAM2sexBKOOSDOsmqy4ItpcqC4AGEznjWYeXWMWqIz2H5-5DFIL_XO_S8
[FOUND] https://www.bing.com/aclk?ld=e8zpCHevSoNmUah4juhE7n1jVUCUyHPn9DMnFrGVAM2sexBKOOSDOsmqy4ItpcqC4AGEznjWYeXWMWqIz2H5-5DFIL_XO_S8
```

Penetration Testing Toolkit - Output Report

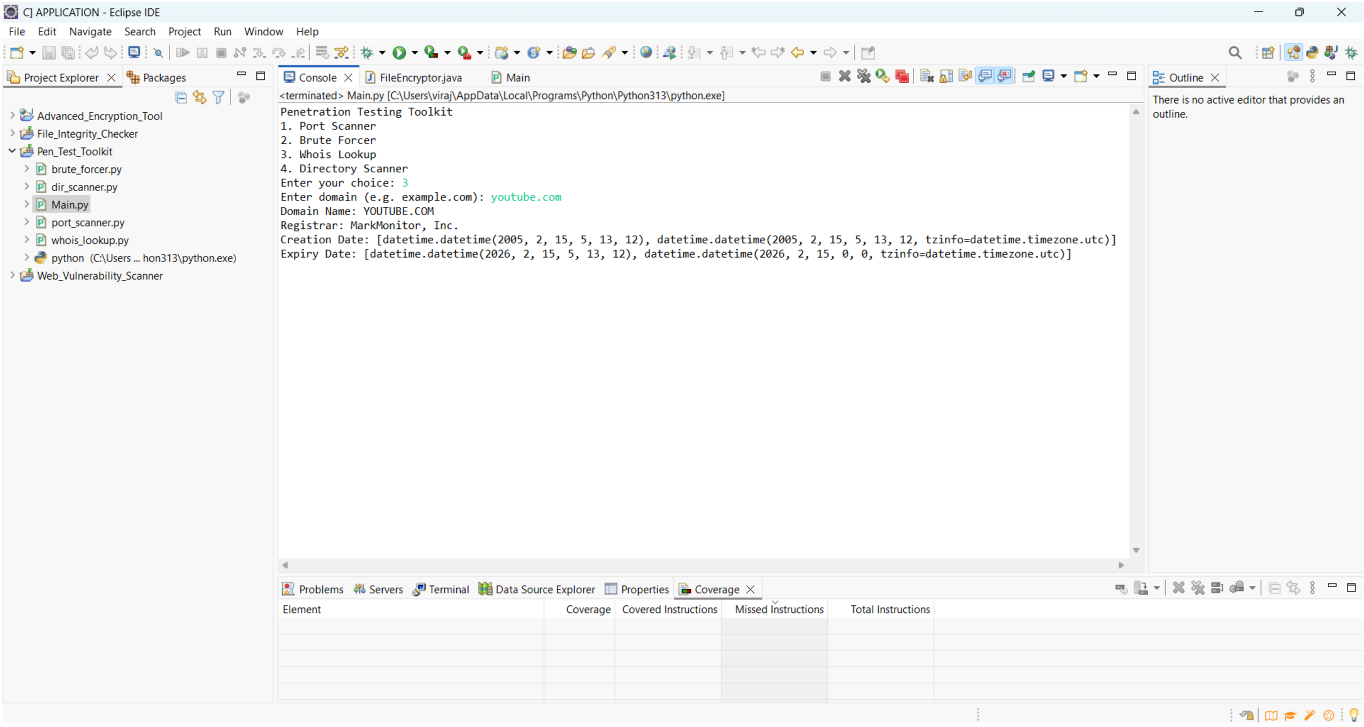
5. Directory Scanner

Target URL: https://www.bing.com/...

Common directories scanned: admin, login, dashboard, uploads

Result: Multiple login pages found.

Helps to identify sensitive endpoints that could be exploited.



```
<terminated> Main.py [C:\Users\viraj\AppData\Local\Programs\Python\Python313\python.exe]
Penetration Testing Toolkit
1. Port Scanner
2. Brute Forcer
3. Whois Lookup
4. Directory Scanner
Enter your choice: 3
Enter domain (e.g. example.com): youtube.com
Domain Name: YOUTUBE.COM
Registrar: MarkMonitor, Inc.
Creation Date: [datetime.datetime(2005, 2, 15, 5, 13, 12), datetime.datetime(2005, 2, 15, 5, 13, 12, tzinfo=datetime.timezone.utc)]
Expiry Date: [datetime.datetime(2026, 2, 15, 5, 13, 12), datetime.datetime(2026, 2, 15, 0, 0, tzinfo=datetime.timezone.utc)]
```