ITSOLERA
PVT LTD

Summer Internship Task Report

Custom Reconnaissance Tool Development

Submitted By: Offensive Team Theta

1. **Objective:**
   The objective of this project is to design and develop a lightweight, modular reconnaissance tool that automates initial information gathering during penetration testing. This tool introduces offensive security interns to scripting, tool-building methodologies, and modular architecture in red team environments.

2. **Tool Overview**

- Tool Name: Theta Reconnaissance Tool
- Programming Language: Python
- Interface Type: Command-Line Interface
- Repository: [Tool Github Repository Link]

3. **Tool Architecture**
   Modules Implemented:
   - Modular structure with independent callable features.
   - Command-line flags for each recon module.
   - Logging with verbosity control.

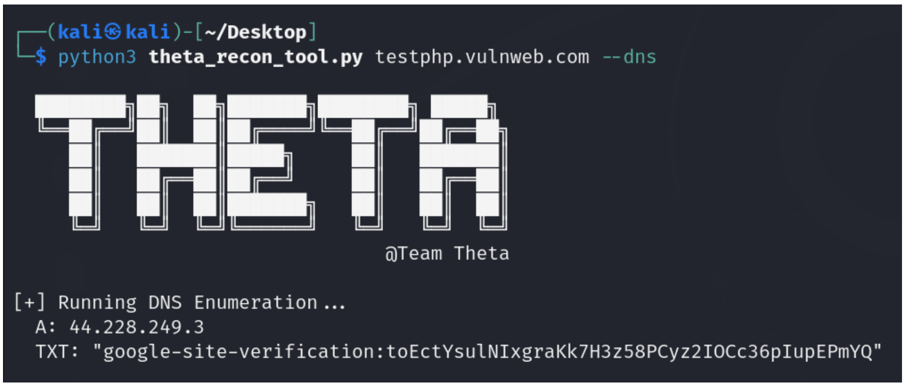
   Technology Stack:
   - Libraries used: e.g., requests, socket, argparse, nmap, whois, etc...

4. **Target**
   For the demonstration of this tool, the website `testphp.vulnweb.com` is used.

5. **Functional Modules**

5.1 Passive Recon

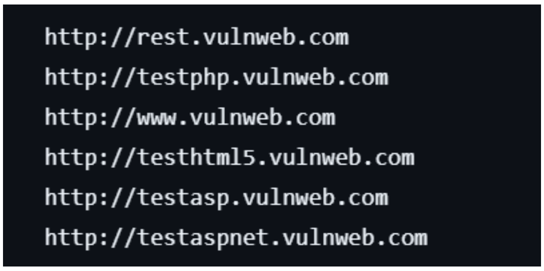
- **DNS Enumeration:**
  Description: Resolves A, MX, TXT, and NS records.
  Here we use the DNS module to find the DNS information about the target available publicly.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 theta_recon_tool.py testphp.vulnweb.com --dns

 THETA
                                   @Team Theta

[+] Running DNS Enumeration ...
  A: 44.228.249.3
  TXT: "google-site-verification:toEctYsulNIxgraKk7H3z58PCyz2IOCc36pIupEPmYQ"
```

- **Subdomain Enumeration:**
  Description: Uses APIs like crt.sh, AlienVault OTX.

  Here we get all the subdomains associated with our target.

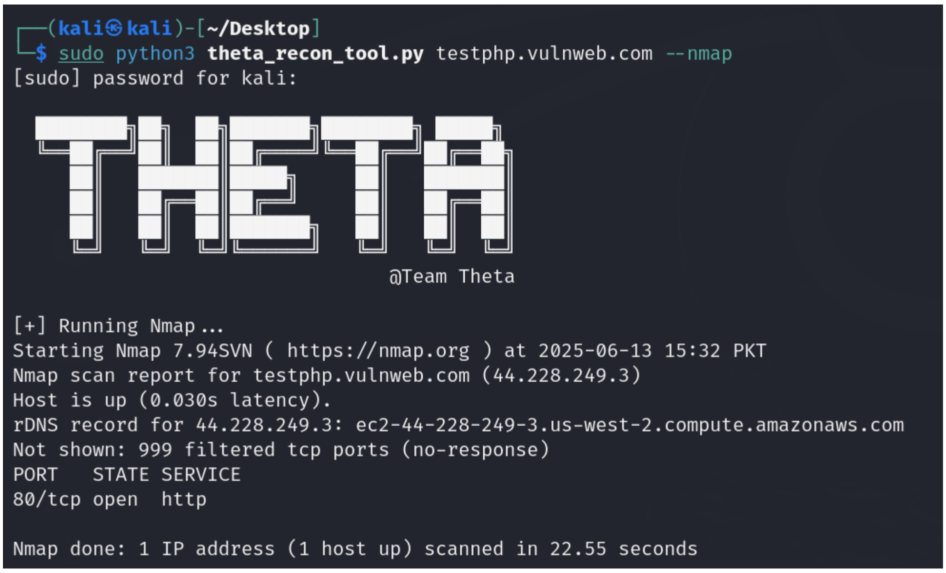


```
http://rest.vulnweb.com
http://testphp.vulnweb.com
http://www.vulnweb.com
http://testhtml5.vulnweb.com
http://testasp.vulnweb.com
http://testaspnet.vulnweb.com
```

5.2 Active Recon

- **Port Scanning:**
  Description: Conducts scans using raw sockets or Nmap wrapper.

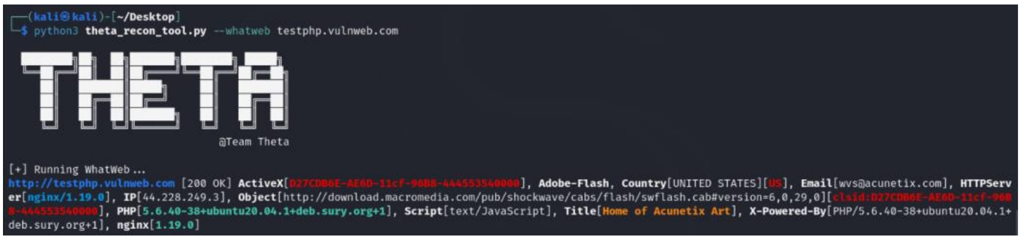
  By using NMAP we find one port open on our target which is port 80.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo python3 theta_recon_tool.py testphp.vulnweb.com --nmap
[sudo] password for kali:

  THETA
                                @Team Theta

[+] Running Nmap ...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-13 15:32 PKT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.030s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 22.55 seconds
```

- **Technology Detection:**
  Description: Uses APIs like WhatWeb, Wappalyzer.

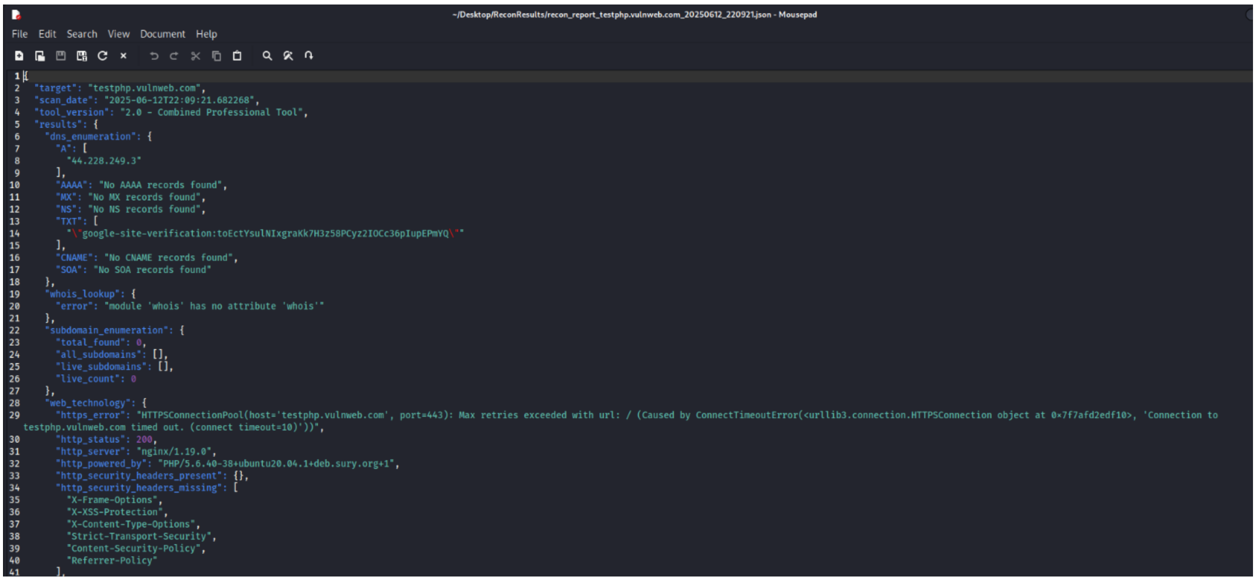
  Using the Whatweb module, we gain information about the owner and technologies used in our target. It is necessary because we can see vulnerabilities found earlier in the same technology.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 theta_recon_tool.py --whatweb testphp.vulnweb.com

  THETA
                                @Team Theta

[+] Running WhatWeb ...
http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPServ
er[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B
8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+
deb.sury.org+1], nginx[1.19.0]
```

6. Reporting

For later investigation purposes, we have saved our findings in a file, which can also be used for reporting purposes.


~/Desktop/ReconResults/recon_report_testphp.vulnweb.com_20250612_220921.json - Mousepad
File
Edit
Search
View
Document
Help

```
{
  "target": "testphp.vulnweb.com",
  "scan_date": "2025-06-12T22:09:21.682268",
  "tool_version": "2.0 - Combined Professional Tool",
  "results": {
    "dns_enumeration": {
      "A": [
        "44.228.249.3"
      ],
      "AAAA": "No AAAA records found",
      "MX": "No MX records found",
      "NS": "No NS records found",
      "TXT": [
        "\"google-site-verification:toEctYsulNIxgraKk7H3z58PCyz2IOCc36pIupEPmYQ\""
      ],
      "CNAME": "No CNAME records found",
      "SOA": "No SOA records found"
    },
    "whois_lookup": {
      "error": "module 'whois' has no attribute 'whois'"
    },
    "subdomain_enumeration": {
      "total_found": 0,
      "all_subdomains": [],
      "live_subdomains": [],
      "live_count": 0
    },
    "web_technology": {
      "https_error": "HTTPSConnectionPool(host='testphp.vulnweb.com', port=443): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0×7f7afd2edf10>, 'Connection to testphp.vulnweb.com timed out. (connect timeout=10)'))",
      "http_status": 200,
      "http_server": "nginx/1.19.0",
      "http_powered_by": "PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1",
      "http_security_headers_present": {},
      "http_security_headers_missing": [
        "X-Frame-Options",
        "X-XSS-Protection",
        "X-Content-Type-Options",
        "Strict-Transport-Security",
        "Content-Security-Policy",
        "Referrer-Policy"
      ],
```

7. Conclusion

This project helped bridge theoretical knowledge with practical offensive security tool development. The hands-on experience with recon techniques and Python scripting deepened our understanding of real-world red teaming and cybersecurity best practices.