

Digital Detective

Shashank Narayankar¹, Hitansh Kadakia², Sanket Kamble³, Aman Bharti⁴, Rasna Patel⁵

Students, Department of Computer Science and Engineering^{1,2,3,4}

Professor, Department of Computer Science and Engineering⁵

Parul University, Vadodara, India

Abstract: *The importance of cybersecurity cannot be neglected in today's digital world. These days the cyber threats are becoming more and more sophisticated, thus it is very important for organizations to conduct thorough and efficient information gathering and vulnerability assessments to protect their assets and sensitive data. To address this need, we have engineered an innovative solution: the Digital Detective. Digital Detective is made and designed as a one-stop solution that combines various tools from the Kali Linux ecosystem, making the information-gathering process very easy, more efficient and more effective reducing the resistance mainly faced by the cybersecurity professionals.*

Keywords: *Information gathering, Kali Linux, Automation Tool, Vulnerability Assessment, Reconnaissance, Scanning, Data Analysis, Security Assessment, Cybersecurity, Efficiency*

I. INTRODUCTION

The Digital Detective project is brilliant work done in cybersecurity to enhance the information-gathering process for professionals. As the digital infrastructures have become more difficult, the need for such effective tools to help and find vulnerabilities and prevent more and more cyber threats from happening. Our Digital Detective tool greatly helps this by integrating various tools available in the Kali Linux ecosystem. Kali Linux is widely known for its vast toolkit for penetration testing and security assessments, thus offering resources for reconnaissance, scanning, enumeration, and data analysis. By combining these tools into one project, the Digital Detective is made. Digital Detective makes the processes very easy and within the matter of minutes.

II. AIM

The aim of the Digital Detective project is to make a unified and efficient solution with is fully integrated within the Kali Linux ecosystem to streamline the information-gathering process for the cybersecurity professionals. The challenges which are faced by the cybersecurity professionals like: tool fragmentation, manual coordination, and potential human error, while prioritizing usability, reliability and security.

III. IMPORTANCE OF THE PROJECT

The **Digital Detective** project is of huge importance in the universe of cybersecurity due to its ability to revolutionize the information-gathering process. In today's increasingly complex digital infrastructure, the timely and accurate assessment of vulnerabilities is critical for organizations to make their defenses strong against evolving cyber threats. By consolidating disparate tools within the Kali Linux ecosystem into a unified platform, Digital Detective streamlines this process, enabling cybersecurity professionals to conduct thorough assessments efficiently. This consolidation not only enhances efficiency but also reduces the potential for errors inherent in manual coordination across multiple tools. Moreover, IGAT's emphasis on usability, reliability, and security ensures that it serves as a robust and trustworthy asset in the arsenal of cybersecurity defenses, ultimately contributing to the resilience of organizations in the face of cyber threats.

IV. USER INTERFACES

The user interfaces of the Digital Detective are totally designed to align with the Kali Linux's principals which prioritize a sleek and simple graphical interface alongside a dedicated command-line interface. Leveraging Kali Linux's standardized UI elements, Digital Detective 's GUI offers simplicity and efficiency, featuring clear navigation menus

and easily accessible tools. This GUI seamlessly integrates with Kali Linux's existing workflow, ensuring familiarity for users within the ecosystem. Additionally, Digital Detective provides a command-line interface consistent with Kali Linux's conventions, enabling advanced users to leverage its functionality through scripts and automation. Together, these interfaces offer a cohesive and user-friendly experience for cybersecurity professionals, enhancing productivity and effectiveness in information gathering tasks.

V. FUNCTIONAL REQUIREMENTS

1. **Scanning Module:** Digital Detective must include a scanning module capable of conducting port scanning, vulnerability scanning, and service enumeration to identify potential vulnerabilities and misconfigurations within target networks.
2. **Data Analysis Functionality:** The tool should provide robust data analysis capabilities, including packet sniffing, log analysis, and data correlation, to extract actionable insights and identify potential threats from gathered information.
3. **Automation and Scripting Support:** Digital Detective must support automation and scripting functionalities, allowing users to automate repetitive tasks, customize workflows, and integrate with external systems and APIs to enhance efficiency and productivity.
4. **Reporting and Logging Features:** The tool should generate comprehensive reports summarizing findings from information-gathering activities and maintain detailed logs for audit trails and forensic analysis, ensuring accountability and facilitating post-assessment analysis.
5. **User Authentication and Access Control:** Digital Detective must incorporate user authentication mechanisms and access control policies to ensure secure access to its functionalities and data, with role-based access control (RBAC) support for managing user permissions and ensuring data integrity and confidentiality.

VI. SYSTEM ARCHITECTURE

The system architecture of Digital Detective is a modular framework designed to automate information gathering within the Kali Linux environment. Comprising modules for reconnaissance, scanning, enumeration, data analysis, and reporting, this architecture fosters flexibility, scalability, and security. Each module is dedicated to specific tasks, facilitating efficient collaboration and interaction while adhering to well-defined interfaces. With a focus on modularity and interoperability, Digital Detective's architecture ensures seamless integration with external tools and systems, empowering cybersecurity professionals to conduct thorough assessments and strengthen organizational security effectively.

VII. TECHNOLOGIES AND FRAMEWORKS

Digital Detective harnesses a blend of Python's versatility along with Linux technologies to automate information gathering within the Kali Linux environment for cybersecurity assessments and threat detection. Python serves as the primary language for development, enabling flexibility and rapid prototyping. Complementing Python, the system integrates seamlessly with essential Linux tools such as Nmap, Metasploit, and Wireshark, providing comprehensive scanning, vulnerability assessment, and packet analysis capabilities. Furthermore, Digital Detective leverages Linux command-line utilities and shell scripting to automate tasks and streamline workflows, enhancing its functionality within the Kali Linux ecosystem. This fusion of Python's capabilities and Linux technologies forms a robust foundation for Digital Detective, ensuring efficient cybersecurity assessments and effective threat detection.

VIII. IMPLEMENTATION

The implementation of Digital Detective primarily involves the development of its CLI interface using Python. Python serves as the core language for building the tool's functionality, enabling seamless interaction with users through the command line. The focus is on designing a user-friendly CLI that allows users to input commands and receive relevant outputs efficiently.

```

root@kali: /home/kali/Desktop/digital_detective
File Actions Edit View Help
root@kali:~# python finalrecon.py --full https://paruluniversity.ac.in

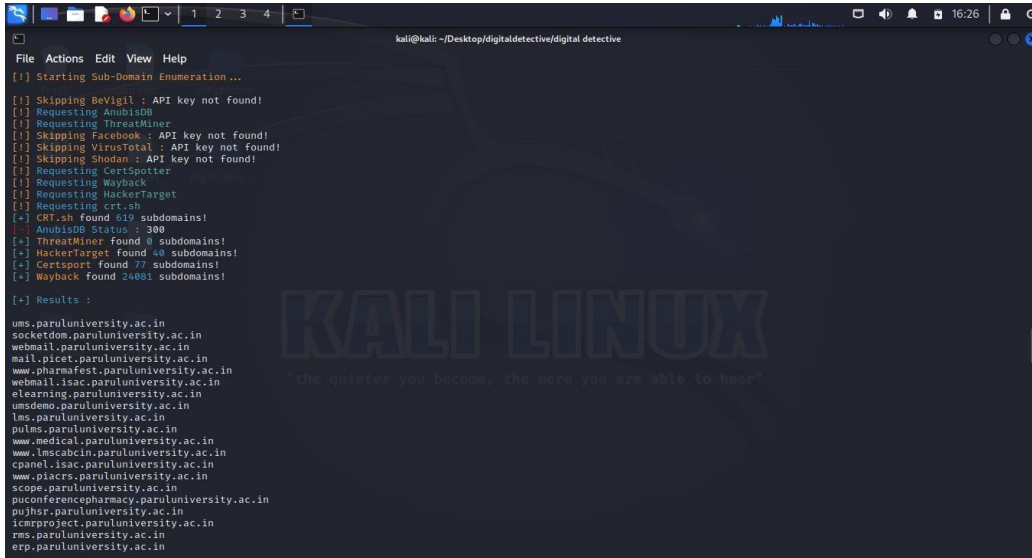
[+] Created By : Hitansh
[+] Target : https://paruluniversity.ac.in
[+] IP Address : 3.111.231.105
[!] Headers :
Server: nginx
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: no-cache, private
date: Sun, 07 Apr 2024 20:12:23 GMT
Set-Cookie: XSRF-TOKEN=eyJpdDI6IjQ2STFNUXVzak5WdWVnbE9IR2N2ZmM5PSIsInZhbnVlIjoia1ZlT2I2IjE5OTMhNS02MHNvSmdYmW1uMDQ2a0NyNDNqVFTaU1S1A2bkZcL2diaitZ7zJ3cVlQeVZmUWV0bisy2giltCjJlYWMiOjIhYmE5Y2UkNWEzYzUzNzAAN2YzODZlNzU2MmU3YTZmZmM4YzZlN2YzN2Y0YmI4YmM4MTg3NGI1NzFjMTg5In0%3D; expires=Sun, 07-Apr-2024 22:12:23 GMT; Max-Age=7200; path=/, parul_university_session=eyJpdDI6IjNuMm5EK3hGdnnN0aWhJNTZBdURBdWc9PSIsInZhbnVlIjoia1VW60MjB5ZmZ2aGpTIGNkVZQcld050NQtNzNkX9FeW5lY3huMmI3d2lWlRlMmQjVtSGJ4UnIwZUIyRTB3RG82RU81lCjYmM1O1lWmZmZlTlJNDQzNDMzY2lWMTJlY2ESMwJm0TE4NDNkMG5lYmNlNThlNmM4ODU0OGNlNmMkOTcwOTkYzA4ZjY4In0%3D; expires=Sun, 07-Apr-2024 22:12:23 GMT; Max-Age=7200; path=

```

```

root@kali: /home/kali/Desktop/digital_detective
File Actions Edit View Help
[!] SSL Certificate Information :
[+] protocol : TLSv1.3
[+] cipher
├─ 0: TLS_AES_256_GCM_SHA384
├─ 1: TLSv1.3
└─ 2: 256
[+] subject
├─ commonName: *.paruluniversity.ac.in
[+] issuer
├─ countryName: BE
├─ organizationName: GlobalSign nv-sa
├─ commonName: AlphaSSL CA - SHA256 - G4
[+] version : Version.v3
[+] serialNumber : 29410779615810757375797462
[+] notBefore : Apr 12 06:54:18 2023 GMT
[+] notAfter : May 13 06:54:17 2024 GMT
[+] subjectAltName
├─ 0: *.paruluniversity.ac.in
├─ 1: paruluniversity.ac.in
[!] Whois Lookup :
[-] Error : This domain suffix is not supported.
[!] Starting DNS Enumeration ...
paruluniversity.ac.in. 300 IN MX 10 alt4.aspmx.l.google.com.
paruluniversity.ac.in. 300 IN TXT "apple-domain-verification=G78RuFwQQR0tlZii"
paruluniversity.ac.in. 21600 IN NS tina.ns.cloudflare.com.
paruluniversity.ac.in. 1788 IN SOA curt.ns.cloudflare.com. dns.cloudflare.com. 2337877082 10000 2400 604800 1800
paruluniversity.ac.in. 3600 IN HINFO \n 9 075246433834383200
paruluniversity.ac.in. 21600 IN NS curt.ns.cloudflare.com.
paruluniversity.ac.in. 300 IN MX 5 alt1.aspmx.l.google.com.
paruluniversity.ac.in. 300 IN A 3.111.231.105
paruluniversity.ac.in. 1800 IN SOA curt.ns.cloudflare.com. dns.cloudflare.com. 2337877082 10000 2400 604800 1800
paruluniversity.ac.in. 300 IN TXT "globalsign-domain-verification=BRZutGSSdDuHGVRckG2pvk4xwZm4FcUyncjLON_3"
paruluniversity.ac.in. 300 IN MX 10 alt3.aspmx.l.google.com.
paruluniversity.ac.in. 3600 IN RRSIG x7k15Bq158wULXEkolj05UAL4lX2b0NB+Dg6Bg0DTEL
x7k15Bq158wULXEkolj05UAL4lX2b0NB+Dg6Bg0DTEL
paruluniversity.ac.in. 300 IN MX 1 aspmx.l.google.com.

```



```

File Actions Edit View Help
[!] Starting Sub-Domain Enumeration ...
[!] Skipping BeVigil : API key not found!
[!] Requesting AnubisDB
[!] Requesting ThreatMiner
[!] Skipping Facebook : API key not found!
[!] Skipping VirusTotal : API key not found!
[!] Skipping Shodan : API key not found!
[!] Requesting CertSpotter
[!] Requesting Wayback
[!] Requesting HackerTarget
[!] Requesting crt.sh
[+] CRT.sh Found 519 subdomains!
[+] AnubisDB status : 300
[+] ThreatMiner Found 0 subdomains!
[+] HackerTarget found 40 subdomains!
[+] Certspotter found 77 subdomains!
[+] Wayback found 24681 subdomains!

[+] Results :
ums.paruluniversity.ac.in
socketdom.paruluniversity.ac.in
webmail.paruluniversity.ac.in
mail.picet.paruluniversity.ac.in
www.pharmafest.paruluniversity.ac.in
webmail.isac.paruluniversity.ac.in
elearning.paruluniversity.ac.in
unsdemo.paruluniversity.ac.in
lms.paruluniversity.ac.in
pulms.paruluniversity.ac.in
www.medical.paruluniversity.ac.in
www.lscocabin.paruluniversity.ac.in
cpanel.isac.paruluniversity.ac.in
www.piacrs.paruluniversity.ac.in
scope.paruluniversity.ac.in
puconferencepharmacy.paruluniversity.ac.in
pujhsr.paruluniversity.ac.in
icrproject.paruluniversity.ac.in
iss.paruluniversity.ac.in
erp.paruluniversity.ac.in

```

IX. CONTINUOUS IMPROVEMENT

Continuous improvement is integrated into the development process of Digital Detective. Feedback from users and ongoing monitoring of performance and usability metrics inform iterative enhancements to the tool's functionality and user experience. Regular updates and refinements ensure that Digital Detective remains responsive to evolving user needs and technological advancements.

X. CONCLUSION

In conclusion, Digital Detective represents a significant milestone in the realm of cybersecurity automation. Its Python-based CLI interface streamlines information-gathering tasks, providing users with efficient and accurate insights into their targets within the Kali Linux environment. By leveraging the versatility of Python and integrating seamlessly with Linux technologies, Digital Detective offers a robust yet straightforward solution for cybersecurity assessments and threat detection. As it continues to evolve, guided by user feedback and technological advancements, Digital Detective remains committed to its mission of enhancing cybersecurity practices and safeguarding digital landscapes against emerging threats. With its dedication to innovation and adaptability, Digital Detective stands poised to play a pivotal role in addressing the ever-evolving challenges of cybersecurity in the years to come.

REFERENCES

- [1]. <https://www.cisco.com/c/en in/products/security/what-is-cybersecurity.html> by Cisco.
- [2]. https://www.researchgate.net/publication/336327385_Knowledge_Extraction_and_Integration_for_Information_Gathering_in_Penetration_Testing by AnisKothia and Bobby Swar.
- [3]. https://www.researchgate.net/publication/263779662_Network_Scanning_Vulnerability_Assessment_with_Report_Generation by Nikita Jhala.
- [4]. https://www.researchgate.net/publication/366366914_Security_Risks_in_Web_Penetration_Testing by Henry Brito, RaydelMontesino and Dainys Reyes.
- [5]. https://www.researchgate.net/publication/332106262_Penetration_Testing_Active_Reconnaissance_Phase_-_Optimized_Port_Scanning_With_Nmap_Tool by Sheeraz Ahmed and Hamayun Khan.
- [6]. https://www.researchgate.net/publication/382923793_Open_Port_Vulnerability_Assessment_For_Self-Defense_Using_Open-Source_Tool by SagarJambhorkar.
- [7]. https://www.researchgate.net/publication/266208072_A_Study_Of_Open_Ports_As_Security_Vulnerabilities_In_Common_User_Computers by Kuruvilla Mathew, MujahidTabassum, and Marlene Lu.