IJNRD.ORG ISSN : 2456-4184

International Research Journal IJNRD Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

AUTOMATED PENETRATION TESTING FRAMEWORK(APT FRAMEWORK)

Gundeti Manisai, Gondi Annie Spoorthi, Savaram Akhil Babu,Gidollu Naveen Reddy, Mrs. C. Surekha
Student/Scholar, Student/Scholar, Student/Scholar, Student/Scholar, Assistant Professor
Computer Science and Engineering
(Cyber Security)

Hyderabad Institute of Technology and Management (HITAM), Gowdavelly(V), Medchal(M),
Medchal-Malkajgiri Dist. 501401, Telangana, India

Abstract: **:**

"APT Framework" is a versatile tool which makes the manual penetration testing into automated penetration testing which is very essential in the world of security. It is crucial to make sure web applications are secure and resilient in the quickly changing digital world of today. This urgent need is met by the "APT Framework" project, which focuses on continuously carrying out dynamic reconnaissance, vulnerability assessment, and exploitation of any security flaws in target systems.

This paradigm provides a proactive and adaptable approach to threat identification and mitigation in light of the always evolving nature of cyber threats. Organizations can take a continuous, watchful posture against possible vulnerabilities rather than depending just on evaluations that are done on a regular basis. The architecture of the Automated Penetration Testing Framework places a high priority on flexibility and versatility. The framework is capable of thoroughly identifying potential holes because it incorporates a broad range of security testing approaches, including vulnerability scanning, code analysis, and network reconnaissance. characterized by an increase in cyberthreats,

In conclusion the APT Framework is mainly adopted in the field of security for the sole reason to find, exploit and mitigate the vulnerabilities found in the applications.

***IndexTerms*:**

Security flaws, vulnerability analysis, fuzzing of urls, scan of the network, threat modeling passive reconnaissance, Active Reconnaissance, OSINT(Open Security Intelligence) modules, Remote Code Execution(RCE), Cross site scripting(XSS), Website information.

INTRODUCTION

The APT Framework is an advanced and all-inclusive collection of tools, scripts, and techniques that have been painstakingly created to automate and expedite the process of penetration testing and security assessments in computer systems, networks, and applications. This framework is an example of an advanced technique, combining several functionalities designed to uncover vulnerabilities, simulate cyberattacks, and strengthen security postures in a variety of digital environments. The APT Framework is essentially a reliable system that coordinates a variety of automated testing approaches and strategies. It reflects a holistic approach to security, enabling security experts to conduct in-depth analyses with a great deal less manual labor than is usually required for such projects. The Framework frees up security teams to concentrate on strategic analyses by automating repetitive operations. They can then use the extra time to investigate important vulnerabilities.

The versatility and scalability of the framework, in addition to its extensive functions, are what make it so strong. Constructed with adaptability in mind, it offers flexible choices for customizing evaluations to meet the unique subtleties and demands of various contexts. Because of its flexibility, security testing may be done in a way that takes into account the particular settings and nuances of every target system or application.

Its ability to seamlessly integrate and orchestrate different tools, techniques, and scripting capabilities is essential to its usefulness. Through this integration, the framework's capabilities to address changing threats are increased and it can now incorporate pre-existing security utilities. Its capacity to combine these various components into a single, automated system solidifies its standing as an all-encompassing and essential instrument.

Furthermore, the APT Framework promotes thorough reporting rather than only identification. It carefully compiles and organizes data, generating comprehensive reports that list vulnerabilities found, indicate how serious they are, and suggest ways to mitigate them. These reports are extremely helpful since they provide security teams and other stakeholders with a clear plan on how to prioritize remediation operations and strengthen defenses against possible threats. Organizations will be able to approach security evaluations pro-actively thanks to the APT Framework. Penetration testing becomes a vital component of the proactive defense against complex cyber attacks by automating and systematizing it. This helps to preserve digital assets and promote resilience in a constantly changing threat landscape. The APT Framework is essential for improving security postures because of its automation and accuracy, which enable enterprises to foresee vulnerabilities.

LITERATURE SURVEY

For the development in the field of automated web application penetration testing , the APT framework is crucial. APT was created primarily to improve security assessments. It simplifies the process of finding vulnerabilities and taking advantage of them, giving security experts and penetration testers a reliable option.

Fundamentally, APT provides automated scanning features that let testers quickly find typical web application vulnerabilities including directory traversal, SQL injection, and cross-site scripting (XSS). Because of this automation, the detection process is accelerated, freeing up testers to concentrate on identifying and resolving serious security vulnerabilities.

APT offers a full suite of exploitation modules that cover a large number of attack methods and vectors. With the help of these modules, testers may replicate actual attack scenarios.

APT's customisation and flexibility are among its main advantages. The testing procedure can be customized by testers to meet the unique needs of the target environment by changing the attack plans, exploit payloads, and scanning parameters as necessary. Its adaptability guarantees that the testing methodology will continue to work in a variety of settings and scenarios.

Practically speaking, APT is used in many different fields, such as continuous security monitoring, red team exercises, and security assessments. APT is a useful tool for improving the security posture of online applications, whether it is integrated into continuous monitoring processes or utilized by security experts to undertake thorough evaluations.

With the APT framework, automated penetration testing has advanced significantly and now has a potent tool for locating and fixing security flaws in web applications**.**

PROBLEM STATEMENT

The ever-evolving nature of cybersecurity attacks poses serious hazards to sensitive data and digital assets within enterprises. The efficacy of conventional manual penetration testing approaches in pinpointing vulnerabilities present in systems, networks, and applications is frequently compromised. These assessments' manual process not only uses a lot of resources but also lacks the flexibility and scalability needed to keep up with the quickly changing landscape of cyber threats.

Moreover, the intricacy of contemporary IT infrastructures, varied applications, and cloud-based settings intensifies the difficulty of detecting and addressing such security weak points. An all-encompassing Automated Penetration Testing (APT) framework is desperately needed, one that can automate security assessments, use automation to find vulnerabilities quickly, and give organizations proactive steps to strengthen their defenses against ever-evolving cyber threats.

By creating an APT framework that combines customization, scalability, human expertise, and automated testing capabilities, this project seeks to overcome these issues. By empowering security practitioners to do thorough, effective, and fast security assessments, the framework aims to help them proactively uncover vulnerabilities and strengthen their cybersecurity posture.

PROPOSED SOLUTION

By utilizing automation, integration, and customization, the suggested solution seeks to build a thorough framework that improves the effectiveness, precision, and scope of security testing procedures.

Fundamental Elements: Automated Testing Modules: A variety of automated testing modules will be included in the framework, allowing for features like vulnerability discovery, exploitation simulation, active and passive scanning, and thorough reporting.

Customization and Integration: The framework's flexibility and modularity enable security professionals to modify tests to fit a range of settings.Compatibility and scalability are guaranteed through integration with a broad range of security tools and frameworks.

Important characteristics:

Efficiency and Scalability: The approach puts efficiency first, guaranteeing quick and resource-efficient testing without sacrificing performance, accuracy, or scalability.

Security and Compliance: During testing, the framework guarantees secure data handling and compliance with regulatory standards by adhering to strict security measures and ethical norms.

User-Friendly Interface(CLI): A user-friendly interface improves accessibility and convenience of use. It comes with an intuitive dashboard and is accessible on several platforms.

METHODOLOGY

The APT framework is built using advanced python scripts which will allows us to scan, enumerate, exploit the vulnerabilities. As there are many modules in the framework the basic outline of methodology as follows:

a)Reconnaissance(OSINT): The first step in any penetration testing or security assessment project is reconnaissance. To find possible weaknesses and attack routes, it entails obtaining intelligence about the target systems, networks, and infrastructure. Within the framework of the APT, reconnaissance techniques are essential for setting up later testing operations. They help testers comprehend the target environment, delineate the attack surface, and efficiently prioritize their testing efforts. There are two types they are

i) Passive Reconnaissance :

The information about the target is gathered without directly approaching the target, for example searching the linkedin profiles for the list of employees in a target company falls under Passive Reconnaissance.

ii) Active Reconnaissance:

In difference with the Passive Reconnaissance the tester will directly himself either physically or via his own personnal machine approach the target to gather the information

b)Scanning And Enumeration: The Scanning Phase involves the scanning of the network and assessing the potential vulnerabilities in the network layer as most of the information is passed in the network layer the security measure for the network layer has to be taken strictly without any leakage of information. After scanning the enumerating the potential threats is done in the enumeration module.

c)Vulnerability Analysis: After the completion of the scanning phase and assessing the potential threats the analysis for the vulnerability is taken care of. The exploitation of the vulnerability is done in this phase through which we can know the severity of the vulnerability discovered. As the impact and the severity of the vulnerability is crucial for any web application or website or for any company it should be analysed carefully and if the impact is severe the company will be informed with the top priority in which in turn results in the welfare of the company.

d)Reporting: At last the reporting phase which is very essential in preparing the detailed information which is found by the APT Framework each and every detail has to be reported by the client to the vendor this is done manually as the direct report the penetration testing is not possible for any scenario we take. After the reporting the client or the individual person will take care for the patching and removing the vulnerabilities from their respective applications.

e)Documentation : For the installation and usage of the Framework the complete document and report is already been prepared which includes installation of the framework, the penetration testing methodology, the modules in the framework, test cases which show the usage of the framework.

Requirements and installation

SOFTWARE REQUIREMENTS

The requirements for the APT framework are very minimal i.e, we need only python scripting language which is very reliable and fast when compared to other scripting languages and most of the modules which are integrated in the framework are well suitable with the Python language.

Furthermore, All the libraries will be installed through a reqirements.txt file which will be mentioned in the documentation and framework repository.

HARDWARE REQUIREMENTS

The following hardware components are required for the APT Framework:

a) Processor: A dual-core processor (e.g., Intel Core i3 or AMD Ryzen 3) with sufficient processing power to handle heavy load of requests which will be sent multiple times..

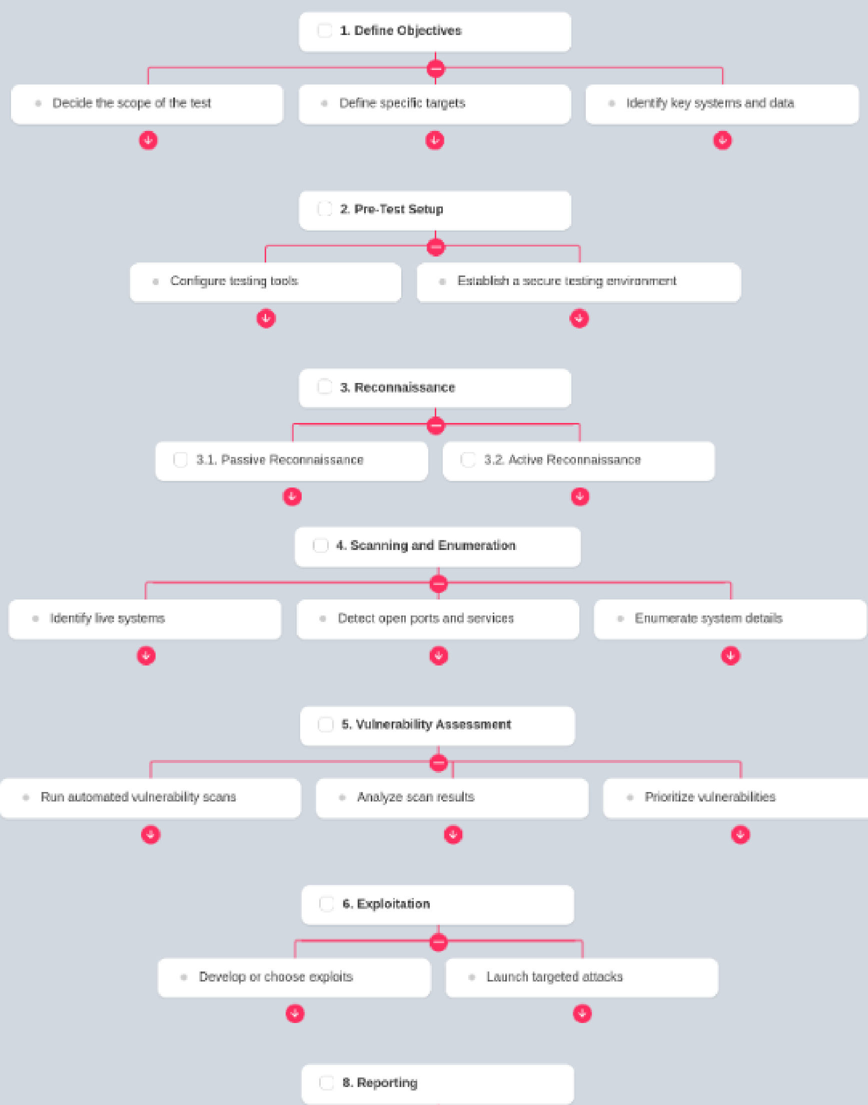
b) Memory (RAM): At least 2 GB of RAM to ensure smooth operation and adequate memory allocation for scanning processes and data storage.

c***) Storage:*** Storage space of 20 GB is recommended as the modules are to store every information gathered in the harddisk, with HDD or SSD are recommended for the Framework.

d) Network Connectivity: A stable internet connection is required for accessing websites, web applications and conducting vulnerability scans. This framework also works with the minimal bandwidth internet.

e) Operating System(OS): Linux is recommended to run the framework, to run the framework in windows we need to install linux environment in windows like ubuntu.

MODEL AND ARCHITECTURE


1. Define Objectives
Decide the scope of the test
Define specific targets
Identify key systems and data
2. Pre-Test Setup
Configure testing tools
Establish a secure testing environment
3. Reconnaissance
3.1. Passive Reconnaissance
3.2. Active Reconnaissance
4. Scanning and Enumeration
Identify live systems
Detect open ports and services
Enumerate system details
5. Vulnerability Assessment
Run automated vulnerability scans
Analyze scan results
Prioritize vulnerabilities
6. Exploitation
Develop or choose exploits
Launch targeted attacks
8. Reporting

WORKING

The working steps for the framework are very simple, the steps are as follows:

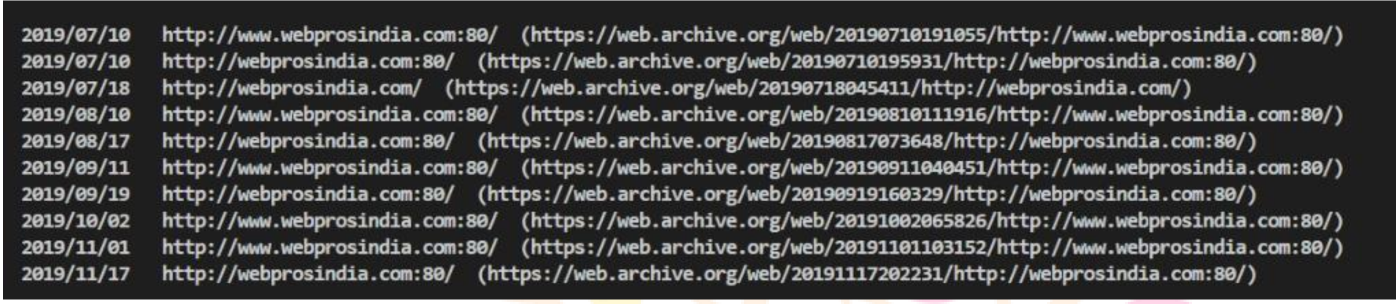
Install Python 3.11 and run the command "pip3 install –r requirement.txt" to install the required libraries for the framework.

1. Open the directory where the framework file is downloaded and open the terminal in that directory.
2. Then type the command "python3 APT.py" and run the command.
3. The framework will run and the command interface will be prompted to enter the command.
4. Enter help to know the various commands we can give to know the exact details.
5. After running the command help we will see some options as clear, attack, victim add, victim delete, victim list, list all modules, info of the module, load module, leave module.

6. Then enter the command list all modules which will show us all the modules namely passive reconnaissance, active reconnaissance, vulnerability analysis.
7. Enter 1 or 2 or 3 with respect to the module we need to select and after that the list of modules will be prompted in the terminal.
8. Now enter the command “load <modulename>” to load the module.
9. Now enter the command “victim add <target url>” and run the command
10. At last run the command “attack” to implement the script from the selected module to the target which will show us the results as per the selected modules.

RESULTS

Below is the result from performing passive reconnaissance with the Wayback Machine:



```
2019/07/10   http://www.webprosindia.com:80/  (https://web.archive.org/web/20190710191055/http://www.webprosindia.com:80/)
2019/07/10   http://webprosindia.com:80/  (https://web.archive.org/web/20190710195931/http://webprosindia.com:80/)
2019/07/18   http://webprosindia.com/  (https://web.archive.org/web/20190718045411/http://webprosindia.com/)
2019/08/10   http://www.webprosindia.com:80/  (https://web.archive.org/web/20190810111916/http://www.webprosindia.com:80/)
2019/08/17   http://webprosindia.com:80/  (https://web.archive.org/web/20190817073648/http://webprosindia.com:80/)
2019/09/11   http://www.webprosindia.com:80/  (https://web.archive.org/web/20190911040451/http://www.webprosindia.com:80/)
2019/09/19   http://webprosindia.com:80/  (https://web.archive.org/web/20190919160329/http://webprosindia.com:80/)
2019/10/02   http://www.webprosindia.com:80/  (https://web.archive.org/web/20191002065826/http://www.webprosindia.com:80/)
2019/11/01   http://www.webprosindia.com:80/  (https://web.archive.org/web/20191101103152/http://www.webprosindia.com:80/)
2019/11/17   http://webprosindia.com:80/  (https://web.archive.org/web/20191117202231/http://webprosindia.com:80/)
```

CONCLUSION

The APT framework is a simplified cybersecurity experience that is accessible and helpful for amateurs and professionals alike. APT framework provides organizations with the tools and insights they need to satisfy auditors, regulators, and other external stakeholders, ensuring peace of mind and regulatory adherence. It encourages proactive, intelligence-driven security measures and has the potential of leveraging technologies like AI and machine learning to anticipate and mitigate threats in real-time. Its adaptive nature ensures continuous improvement and compliance with regulatory standards. As the cybersecurity landscape evolves, APT is open to innovate and adapt, so users can customize their penetration testing as per their requirements.

REFERENCES

1. "A Survey of Web Application Security Testing Tools" by L. Correa and A. F. Vasconcelos
2. "Web Application Vulnerabilities and Security Threats: A Literature Review" by M. Hasan and M. Zulkernine
3. "A Survey of Vulnerabilities in Web Application Security" by P. A. Balaji, S. Sujatha, and R. Chandrasekaran
4. https://owasp.org/
5. https://www.mitre.org/
6. https://www.sans.org/
7. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto
8. "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman