International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Systematic Review: Automation in Cyber Security

Nitin[1], Dr. Lakshmi J. V. N[2]

[1]MCA Computer Science Department, [2]Associate Professor, MCA Computer Science Department,
[1,2]Jain (Deemed-to-be) University, Bengaluru, Karnataka, India

ABSTRACT

Many aspects of cyber security are carried by automation systems and service applications. The initial steps of cyber chain mainly focus on different automation tools with almost same task objective. Automation operations are carried only after detail study on particular task (pre-engagement phase), the tool is going to perform, measurement of dataset handling of tool produced output. The algorithm is going to make use of after comparing the existing tools efficiency, the throughput time, output format for reusable input and mainly the resource's consumption. In this paper we are going to study the existing methodology in application and system pen testing, automation tool's efficiency over growing technology and their behaviour study on unintended platform assignment.

KEYWORDS: *Pentesting, Automation, Cyber chain, Vulnerabilities, 0day*

How to cite this paper: Nitin | Dr. Lakshmi J. V. N "Systematic Review: Automation in Cyber Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.388-391, URL: www.ijtsrd.com/papers/ijtsrd41315.pdf

IJTSRD41315

INTRODUCTION

As the population of internet devices exponentially grows without limits, respective regulatory bodies need a control with data being handled by whom, what, how and where. And it completely depends the service provider, but still the SP(service providers) irrespective of hardware or software need to agree with the rules and regulations introduced and applied by government data protection authorities. The idea behind automation in Cyber security is, increasing the efficiency and time saving. Most of the static based task are carried out by the service application itself, but here the explicit detection and prevention softwares takeover the static tasks like previously discovered contents, and later the systems keeps the records of it and starts comparing to the realtime service application operations. For dynamic tasks or completely new events some more level of human interaction is needed for decision making on particular event or some intelligence system that has more accuracy rate compare to usual detection and precaution based softwares.

Testing the compatibility of the tools with new concepts and algorithms, leading to some level of testing operation improvement. Knowing the different pentesting phases, and understanding on how to create a tool that automates the static and dynamic operations. Every phase has a tool that helps in pentesting life cycle, understanding the importance of documentation on every phase and report generation by specific tools. The known vulnerability can be blacklisted on the application or system by the service provider, using this set of prevention data, the preventative software or system can learn and can be used on the future for 0day vulnerabilities mitigation.

Necessity and Pentesting the Internal and External Assets, Services

Testing the consistency of the system or service is a must in growing technological population and which at the end the user is looking for the unique way or the secured way of interfacing each other. And this can be achieved by the continuous testing methodology and improvement to its efficiency, this is the key to hold a big part of market. The automated testing tools covers the known vulnerability scanning scope which helps in saving time and man power.

Need of pentesting in all organization irrespective of business scale:

A) Protecting the internal confidential data. B) Protecting the user shared data for service usage. B) Protecting the systems that gets the service running. These are the main categories where every organization need to invest in to get the business running in the competitive market. The subcategories will be organizational assets as well as owned external assets like the user data.

Pentesting Internal Assets: Intra-network, connected systems and networking devices, database hosting systems, computational servers, authentication management server and softwares that handle the work flow or operation management systems. These devices need to be tested their performance in uncomfortable zone to see the its efficiency and output it generates. The pentesting operation is carried out by the internal VAPT (Vulnerability Assessment and Pentration Testing) team if the organization has the budget according to their business objective. Every organization in global scale has an internal VAPT team apart from third party service provider, the team must be skillful to test the

assets, services and be on the same level as service provider in testing skill to check integrity of services the third party is offering, it might be a software irrespective of platform, network, common interface platforms for both employees as well customers. Mainly the internal team handles the day to day tasks like SOC, NOC etc. And these operations cannot easily be handover to third party due to cost matter and confidential operations period[1][9][10]. The first responder of any internal cause of threat would be internal VAPT team. The internal assets pentesting operations may get easier if the development practices throughout the deployment of any project is under high prioritization of security precautions, and this can be achieved with greater experience in specified operation development as well as in development model like Water Fall model, Iterative model, Spiral model, Agile model etc. The complexity resides on the network level, the complexity is must and it should be completely comprehensible to internal team, like virtual sub-networks, and their behaviour with preset of ACL(Access Control List). And this all depends on the network architecture efficiency, impact isolation strategy implementation in software and hardware parts[3].

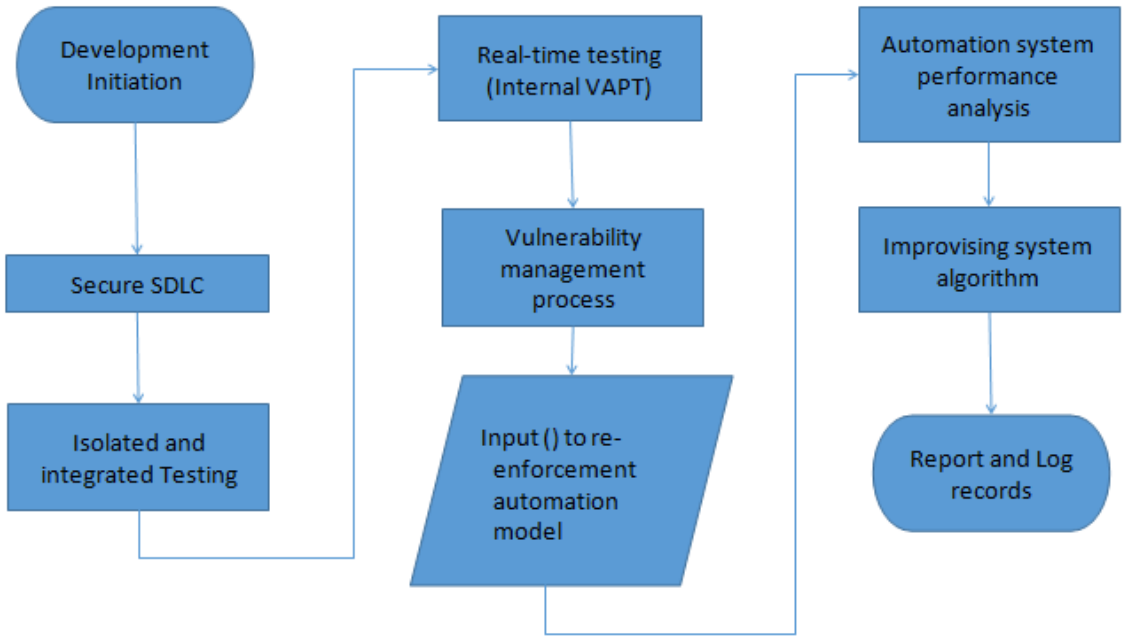

Fig 1.1 Generic Testing and Model Training Life Cycle Flow Chart

The necessity of internal pentesting to protect the internal data flow and privileged systems, and the intra-network is the one that challenges the attacker, how far the attack can be carried out. If the impact on the hosted services is leading and effecting to internal operation and architecture, that means the organization intra-network is not robust in nature. Sometimes the attack would not necessarily be initiated from outside the network, the organizational employee could use it for sabotaging the organization. The nodes under the intra-network has to be secured, before any attacker makes use of existing vulnerabilities on the nodes. It is also important to know how well the prevention systems works at worst situation like cyber attacks.

Pentesting Externally hosted services: This is the public exposed assets, that needs more attention with constant support, in short maintaining the consistency of any hosted services can reduce the impact and future loss. The services could be standalone software, internet services like web applications, mobile applications, IoT devices, hardware equipments or subscription based services etc. Every single services has a separate set of standards for pentesting methodologies and frameworks.

For web application pentesting standard methodology could be initial reconnaissance and OSINT(Open source Intelligence Gathering), threat modelling, vulnerability analysis, initial exploitation, post exploitation, and finally vulnerability assessment, report writing and auditing[4]. The methodology completely depends on the team or organization specific, and can design their own frameworks for set of service's pentesting. IoT pentesing general methodology includes isolation testing technique, later begins with communication protocols usage and testing its consistency, testing environmental interaction with other connected components to complete the task, testing its functionality using bottom-up or top to bottom approach, its hardware and firmware reconnaissance and testing, centralized management device or system testing[5]. The hardware equipment pentesting methodology is almost same as IoT device testing but with wider scope. The tools that are used throughout the process is completely depends on the organization choice, hired third party standard methodological based tools.

Generic Methodology And Existing System's Workflow

The workflow represents complete procedure that needs to fulfill all the pentesting and specific organization requirements. First the internal team is the only source for complete pentesting operations, secondly hiring a third party penetration testing team as a service. The higher authority and defined standards for SDLC inside the organization highly depends on the penetration testing plans with proper budget like when and how. The pentesting operation could take place on every month at lower scope, quarterly or yearly. The how defines the techniques, methodologies and standard frameworks and this lead to choosing an efficient tool matching the preset of criteria[6].

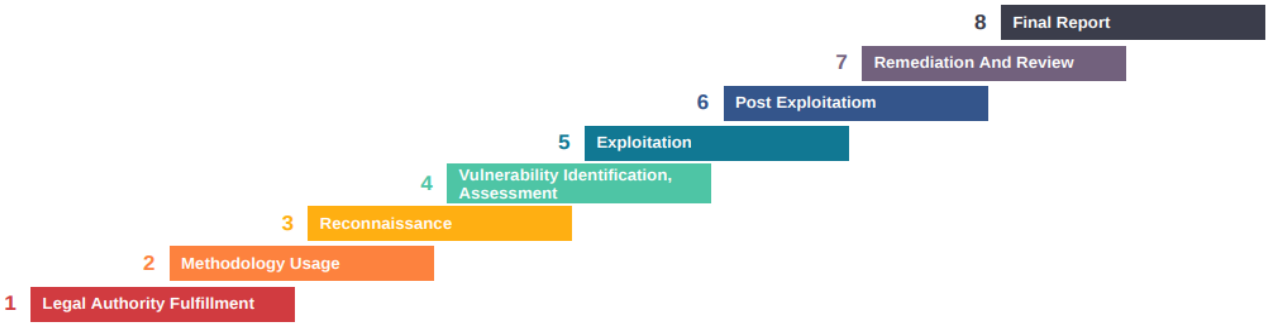

Fig 2.1 Generic Penetration Testing Phases

To begin with pentesting an asset irrespective of type based(period), it is must to acquire the legal grant from asset owner and non disclosure agreement, before starting the decision making process on type of methodology or framework going to be used. Testing any assets fall under these categories, white box, grey box and black box testing. White box testing include complete knowledge about internal structure and its mostly be performed by the internal VAPT team, and other testing includes little or no internal knowledge about the internal network and architecture of the asset and these testing is mostly be performed by the third party pentesting team. Every team follows above phases, and set of tools is must to note before usage on the assets. Every phase has at-least one tool that automates the part of the process; information gathering about the assets, finding the injectable end-points and even makes more comprehensive about the assets behaviour dynamically. The manual testing is needed where the efficiency and accuracy of the tool lacks behind.

Automated pentesting tools mostly work on the basis of static data format, either the result is exploitable or not, sometimes false positive. To overcome this problem, new and highly capable intelligence is being added like machine learning, AI leading to re-enforcement learning module[7] which is capable of performing the task dynamically. The rate of false positive decrease as the dataset input to the system is relevant and up to date. One automation tool in both offensive and defensive security management depends on the other micro based tools. The tool is designed to find the already specified vulnerable end point and try to inject the payload which is generated based on specific type of vulnerability or the new way of updating the tool is pushing the new trend exploits as a module to the tool, same way as security patch to the system but here as a newly found exploit with payload. And is not a dynamic way of pentesting any assets. Tool only works on dataset, payload, injectable end-points or form fields, or by checking the service or exploitable software version, attack takes place according to provided module based procedure with crafted payload. The most of re-enforcement learning based systems or tools are usually not open sourced[7] and it is not a good practice to completely depend on free tools cause, maintenance and its consistency is not guaranteed by the developer[8]. Mainly the micro or open source tools are not tested in all environments or situations. In defensive security operations, the person cannot handle the huge inspection of every operations on internal network or hosted service behaviour, the automated inspection and preventative tools plays the middle role of alerting any suspicious activity to privileged users, this leading to many advantage.

Benefit of Task Automation in Routine Security Operations

Pentesting automation tools play vital role in day to day operations independent of organizational scale and target scope. Tools are designed in reducing the user interaction after initiation with input. Below mentioned advantages are considered from both static and dynamic automation systems or tools.

Faster: Compare to manual pentesting the automated tools can able to surpass the speed of testing the targeted application with commonly known exploitation techniques. The tools which uses dynamic learning methodology, may take slightly more time compare to static, and the performance also depends efficient re-enforcement algorithm and the target asset scope.

Scope coverage: If the scope of testing application or system is large, the automated testing tools are able to cover all known tests, which a person might miss some part, module or features, this leading to cover and focus more on discovering new vulnerabilities.

Consistency: The tools are able to update and upgrade the testing techniques to keep up with new attack and payloads. New technologies are being developed and integrated into the existing systems or softwares, and it increases the scope and time on improving the dynamic testing systems with new datasets. Consistency depends on how well the accuracy and efficiency improves with every new tests.

Robust in Nature: Machine learning and AI based automation systems are robust in pentesting tasks. With trained intelligence system testing module would able to discovery new vulnerabilities like using Dijkstra algorithm etc[2].

Saves Time and Cost: Main purpose of including and usage of automation tools or systems is to save the test result generation time and cost. Investing in manual pentesting job is going to cost more but it is necessary to conduct a manual pentesting operations atleast once in a year. Manual pentesting over automation will lead to increasing the organization budget.

Less User Interaction: The tools need very less user interactions over specific tasks or no interactions at all. The manual pentesting requires user interaction on all stages while reconnaissance, scanning and information gathering, attacking phase, remediation and report generating phase. The automation tools are designed in such a way that, the user does not need to discover, attack and write the report at the end of test every time.

Report Generating: Almost all the open source and paid automation tools generate a complete scanning, fetched information, discovered vulnerabilities and their severity level, impact area and final recommended fixes after test in reusable format as well as for report documentation.

In defensive approach, more than half of the tasks are carried out by the automation systems or software; network and security operation centre. The system looks for malicious patterns in data and control flow based on pattern matching algorithm[10][11], system even tries to prevent it from completing the task but with all under human supervision. The pattern matching system generates alert on the basis of percentage of impact is going make on any part of asset in the organization. The alert contains detail report on specific application behaviour on which the pattern recognized, severity level, description of the attack or malicious task, all resources utilization and some level of recommendation to mitigate the continuation of the malicious task.

Conclusion and Future Scope

There's no control on restricting the growing technology and number of devices on the internet, billions of devices gets added to internet every year. Developers, manufacturers and service owners does not perform proper testing phase, this leading to creating new continuous maintenance department. The application, service or software system gets encountered on unsettled or completely new environment, this causes new issues on the overall application behaviour, finally leading to organizational loss or losing user trust. The automated testing and monitoring tools work to mitigate any future impact before any attacker discovers and leverages the vulnerability. It is important to maintain the tool consistency and reliability on highest priority. Mainly the algorithms in dynamic testing systems should get improved on accuracy, resource consumption should be decreased leading to less load on performance and get faster result on every test. This can be achieved by properly testing the overall performance at different environment and dataset before making it public.

Automated testing systems should mainly focus on other technology integration and working with different datasets. Systems efficiency is measured by improvements in its performance. This can be achieved by leveraging the neural network and deep learning algorithms with proper module implementation, and focusing and feeding manual pentesting methodology to the system. More accurate algorithms decreases the false positive alerts and vulnerability discoveries. Automated testing tool's main scope should be discovery the 0day loop holes.

Reference

[1] A. V. Erisa Karafili, "Automatic Firewalls' Configuration Using Argumentation Reasoning, "Springer, Cham, p. 15, 2020.

[2] J. Hoffmann, "Simulated Penetration Testing: From "Dijkstra" To "Turing Test++","ICAPS, p. 25, Apr 2015.

[3] G. S. J. H. M. S. Dorin Shmaryahu, "Simulated Penetration Testing As Contingent Planning," ICAPS, p. 28, Jun 2018.

[4] F. U. R. J. A. D. M. R. Insha Altaf, "Vulnerability Assessment And Patching Management, "International Conference On Soft Computing Techniques And Implementations (ICSCTI -IEEE), p. 5, Oct 2015.

[5] J. A. R. K. Archibald, "Refining The Pointer "Human Firewall" Pentesting Framework," Emerald Publishing Limited, p. 27, Sept 2019.

[6] N. Samant, "Automated Penetration Testing," San Jose State University, 2011.

[7] Stefan Niculae, Daniel Dichiu, Kaifeng Yang, Thomas Back, "Automating Penetration Testing Using Reinforcement Learning.," Experimental Research Unit Bitdefender & Natural Computing Group, Leiden Institute Of Advanced Computer Science., p. 13, 2015-2020.

[8] A. L. S. O. L. J. G. V. Esteban Alejandro Armas Vega, "Benchmarking Of Pentesting Tools," International Journal Of Computer And Information Engineering, p. 4, 2017.

[9] Matt Willems , "What Soc Automation Tools Can Do For Your Team," 28 Sep 2020. [Online]. Available: Https://Logrhythm.Com/Blog/What-Automation-Can-Do-For-Your-Soc/.

[10] P. N. Martti Lehto, Cyber Security: Analytics, Technology and Automation, Springer, Cham, 2015.

[11] M. S. V. K. B. Vibha Gupta, "Analysis Of Pattern Matching Algorithms In Network Intrusion Detection Systems," International Conference On Advances In Computing, Communication, & Automation (Icacca) - IEEE, p. 5, Oct 2016.