RESEARCHERID
THOMSON REUTERS

*[Arora,* 6(1): January 2019]
DOI: 10.5281/zenodo.2549713

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

# AN EFFECTIVE AND EFFICIENT PENTEST FRAMEWORK TO IDENTIFY VULNERABILITY

**Nitin Arora[1], Nikhil Srivastava[2], Sai Sagar Peri[3], Sumit Kumar[4] & Alaknanda Ashok[5]**
[1,2,3,4] School of Computer Science
[1]Department of Informatics
[2,3,4] Department of Systemetics
[1,2,3,4]University of Petroleum and Energy Studies
[5]Department of Electrical Engineering
[5]G. B. Pant University of Agriculture and Technology, Pant Nagar

## ABSTRACT

The tremendous growth in the field of computer science and information technology has given birth to a new line of system application securing which has become increasingly difficult with the intrusions becoming devious and adaptive. With threats becoming highly user adaptive there is a need to educate oneself about security.It has been found that when it comes to securing an organization and cyberspace we have a lot of work to do. Since the advancement in cyber-attacks are an imminent threat vector, it a necessity to have advance defensive mechanism to not only stop the known attack but should predict the zero days and applying relative mitigations in real time.Achieving the end goal of securing the end user's CIA is not an easy task, but the process can be optimized for giving better and efficient outcomes. For Information Security processes like Vulnerability Assessment, Penetration testing and Risk management plays an important role for protecting infrastructure and machines processing data.Optimizing the above processes can improve overall performance and can bring value to any new day industry. But if these processes are not executed or aligned with the business goals properly, can have a direct impact to the organization in the form of data breaches, DDOS, hacking of internal networks etc.Penetration testing is a process of finding and exploiting vulnerabilities before malicious users and warning the organization of existing vulnerabilities and risks. A Pentest framework will help the organization to easily identify a vulnerability in an effective and efficient way. A framework consists of tools and scripts that can be used by the penetration tester's team for testing the software and identifying their limitations and breaking point. A pen test framework helps simulate cyber-attacks on the organization's critical infrastructures and help the organization identify their existing risk that can be exploited to gain profit by someone with malicious intents.

***Keywords:*** *Penetration testing, Pentest framework. Exploit, payloads, IDS/IPS Evasion, AV bypass, Smart Pentest Framework.*

## I. INTRODUCTION

A penetration Test is an authorized simulated attack on a network or a system to find loopholes into that infrastructure. Hacking security of an organization can sometimes provide us with the potential ways a malicious individual or group of people can take-up for affecting the organization and its data.With the increase in attack paradigm, more complex attacks are introduced on a regular basis.To prevent organizations from cyber-attacks following things are really important: -

- Correct security measures.
- Awareness.

While preventing organization from cyber-attacks one try to find and mitigate the risks involved that can affect the organization's functionality.

For achieving the security goals penetration testing plays an important role and needs to be done with consistency. Below is a typical flow of penetration testing of an organization-

- Find an exploitable vulnerability.
- Design an attack around it.
- Test the attack.
- Seize a line in use.
- Enter the attack
- Exploit the entry for information recovery.

Based on the end result proper security actions takes place including risk acceptance and mitigation. A Penetration Testing Framework help to automate the process of pen testing in an effective and effortless way.There are tools like metaplasia and Canvas which are the industry standards for testing the infrastructure.

***1.1 Why is penetration testing important?***

To know your vulnerability before attacker exploits it. It's always good to take prevention then to take cure later and so by knowing you potential threats, it can help you model your business and its risk better and aligned to business growth.

## II. LITERATURE REVIEW

Penetration testing remains a required practice for the security-mindful expert for surveying the security of their infrastructure. Learning and making research in penetration testing is a troublesome errand, one must have the capacity to introduce the objective framework, reproduce its utilization and after that plan and test the apparatuses for assaulting this objective [1]. In the ongoing years, a couple of arrangements we outlined that remember a set of data gathering methods, exploitation and an incorporated database to help the penetration tester with his activity. We planned a suite that ties a genuine penetration testing system with a system recreation device that will permit its clients a practical affair of pen testing differed arrange designs. This suite enables cyber experts to examine certain parts of penetration testing with negligible arrangement and readiness necessities.[2].

Web server fingerprinting is a critical task for the Penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing. The simplest and most basic form of identify a web server is look at the server field in the HTTP response header with netcat[3]

All aspects of a penetration testing programmed (which includes determining requirements, acting the actual tests and carrying out follow up activities) need to be well managed. For example, by establishing an assurance process to oversee the testing, monitoring performance against requirements and ensuring appropriate actions are being taken[4].

The purpose of the Penetration Testing Guide is to help you to:

- Understand objectives for conducting a penetration test
- Gain an overview of the key components of an effective penetration testing approach
- Develop an appropriate penetration testing program
- Identify what needs to be considered when planning for and managing penetration tests
- Learn about the penetration testing process – and associated methodologies
- Determine criteria upon which to base selection of appropriate service providers.

## III. PROBLEM STATEMENT

- We proposed a smart pen test framework that test the organization's security to their core and help organization from various threats including Advanced Persistent Threats.
- We intend to solve various cyber-attacks happening on a daily basis including the zero days.

- To utilize the full potential of our framework one doesn't need to be a cyber-ninja, it is easy, fast and effective solution to the real world cyber security complications and limitations.
- With this framework what we intend to achieve is not just exploitation but also present the pen testers out there with an educational experience.

## IV. OBJECTIVES

- **Prepare for penetration testing** as part of a technical security assurance framework; managed by an appropriate penetration testing governance structure; considering the drivers for testing; the purpose of testing and target environments; and appointing suitable suppliers to perform tests
- **Conduct penetration tests enterprise-wide**, approving testing style and type; allowing for testing constraints; managing the testing process; planning for and carrying out tests effectively; as well as identifying, investigating and remediating vulnerabilities
- **Carry out appropriate follow up activities**, remediating weaknesses, maintaining an improvement plan and delivering an agreed action plan.

## V. METHODOLOGY

To implement the above goals, the following methodology needs to be followed: A web interface needs to be implemented using PHP on the backend and HTML+JS blend on the front end. This web interface will help our framework to be easily accessible, deployable, and manageable and have a direct impact on the usability of the product. On the backend, there will we use RPC involving our python script for triggering the events like Vulnerability Scanning and exploitation. Since we will be working with a lot of exploits ruby and perl will be used wherever it is required. Advance attacks like pivoting, dual pivoting, privilege escalation and data exfiltration will be available by the framework and will be implemented using the same process described above. At the end a smart pen test framework will be produced which will be capable of simulating real world cyber-attacks over an organization's network.

**Flow Diagram**

Figure 1 represents the complete flow graph of our proposed system. In this different stages are there. The complete flow graphs contains 7 stage.

ISSN 2348 – 8034
Impact Factor- 5.070

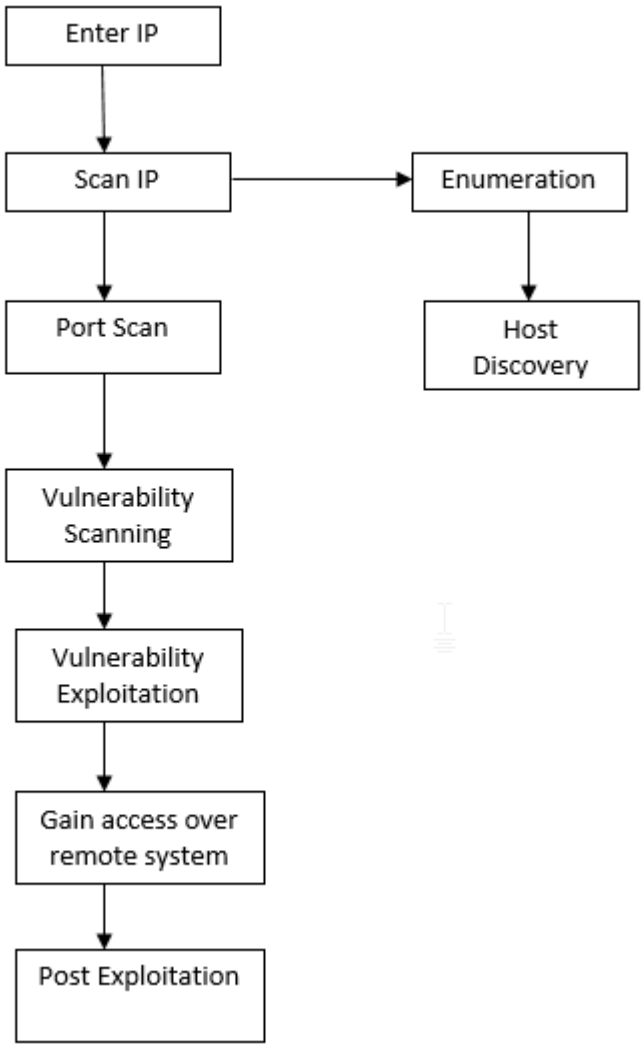


*Figure 1: Flow diagram of proposed system*

**Outputs and discussion**

Figure 2 shows the Hex-Ploit homepage. This page containing many entries like enter IP address, enter user name, and enter password and then click button to submit the entries.

ISSN 2348 – 8034
Impact Factor- 5.070


*Figure 2: Hex-PloitHomepage containing many entries*

ISSN 2348 – 8034
Impact Factor- 5.070


***Figure 3: Represents the system vulnerable and port number***

ISSN 2348 – 8034
Impact Factor- 5.070

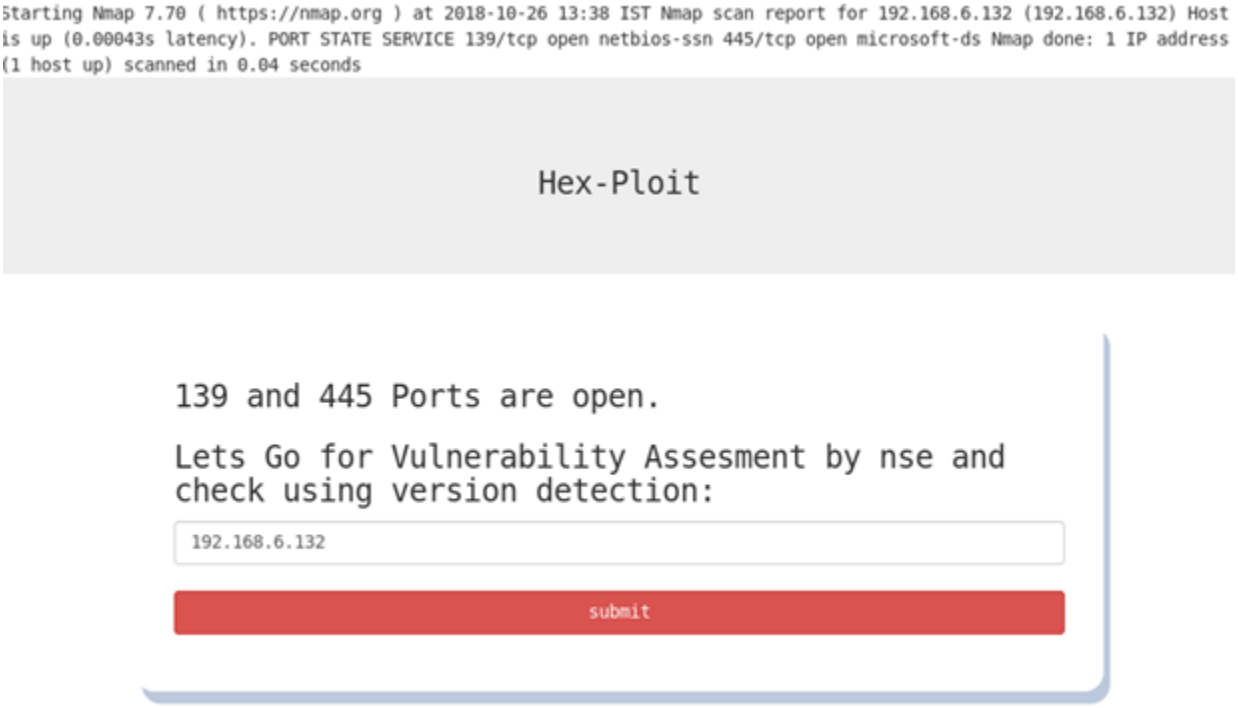


***Figure 4: shows the open ports***

## VI. CONCLUSION

This paper is completed as targeted.
By implementing above stated methodology, we achieved our goals:

- **Prepared for penetration testing**, as part of a technical security assurance framework; managed by an appropriate penetration testing governance structure; considering the drivers for testing; the purpose of testing and target environments; and appointing suitable suppliers to perform tests
- **Conducted penetration tests enterprise-wide**, approved testing style and type; allowed for testing constraints; managed the testing process; planned for and carried out tests effectively; as well as succeeded in identifying, investigating and remediating vulnerabilities
- **Carried out appropriate follow up activities**, remediating weaknesses, maintaining an improvement plan and delivering an agreed action plan.
- At the end, a smart pentest framework produced which is capable of simulating real world cyber-attacks over an organization's network i.e. HEXPLOIT.

## REFERENCES

1. *Overview and open issues on penetration test*
   https://link.springer.com/article/10.1186/s13173-017-0051-1
2. *web-application-security-testing.pdf*
   www.exploit-db.com/docs/english/44319-web-application-security-testing.pdf
3. *A Penetration Testing Research Framework*
   www.coresecurity.com/corelabs-research/projects/penetration-testing-research-framework
4. *CREST-Penetration-Testing-Guide.pdf*
   https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf