# PROACTIVE PENETRATION TESTING FRAMEWORK FOR FINDING UNKNOWN VULNERABILITIES

[1]*KUDIKALA SATHYANARAYANA,* [2] *MADDURU SAMBASIVUDU*
[1]M. Tech, CSE Dept, MRCET, Hyderabad.
Email: sathyanarayana546@gmail.com.
[2] M.Tech, Assistant Professor, CSE Dept, MRCET, Hyderabad.
Email: samba.siva57@gmail.com.

**ABSTRACT-** *Enterprise infrastructures in modern world are interest to attach network which was multilayer architectures and environment which was server heterogeneous in order to know and fulfill each organization's goals and objectives completely. The increase in demands of information security measures is a result of complex network architectures. Dealing with this major security concerns as well as developing a myth of privacy based upon features and items is very essential that each organization needs to be effective in progress. An efficient security policy must be proactive which was opposite a different of recognized and unrecognized attacks and cases in order to provide sufficient defense layers. This approach which was proactive is normally admitted not in correct way that software and hardware are updated perfectly. Find outing for updates regularly and updating them alone will not be enough, because potential misconfigurations and locating as well as patching of design flaws becomes difficult; in turn that makes the whole network vulnerable. Trough this paper we present an idea how a comprehensive security level can be attained through extensive Penetration Tests. We present a Penetration Test methodology and also Penetration Test framework that is capable to explain all possible exploitable vulnerabilities. In addition, we conducted to the mentioned study we performed an analysis which was extensive in a network test of penetration case study on a setup that is present in the network simulation lab, revealing common network misconfigurations and their security which also implies the same to the whole network and its users.*

***Indexing Words:*** *penetration testing, network security, ethical hacking, and proactive security policy.*

## 1. INTRUDUCTION

Today's leading enterprises utilize state of the art ICT integrated solutions and technologies into their business operational processes, in an attempt to obtain the largest market share, locally or internationally. On the other hand, trailing and middle scale organizations cannot afford such costs resulting into partially adopting a subset of these high ends ICT feature. Despite their different levels of ICT integration, every modern organization has to effectively deal with the security issues that arise from these technologies. Multilayer network architectures, scalable web services, custom applications, distributed services and heterogeneous server platform environments, form a small sample of the infrastructure's complexity in modern organizations. These complex architectures in the core network infrastructure, result in large and more difficult than ever security demands in order to keep data and information assets secure. Additionally to this recently added system and network complexity, criminal organizations have formulated their hacking procedures in a try to break into corporate networks and harm the organization with every possible way. Most companies and institutes work diligently to maintain an effective security policy, implementing the latest products and services to prevent fraud, sabotage, information leakage, vandalism and denial of service attacks. However this proactive up-to-date approach does not result in a successful security policy.

The problem is that they still do not know whether and where they are vulnerable. They just take it on faith that the vendors' fixes will keep their network safe. Unfortunately, the up-to-date security approach is not adequate because it does not detect mis-configured settings or network infrastructure design flaws that can put the network under great risk. An organization that truly wants to adopt a proactive approach, aggressively seeks out all types of vulnerabilities by using relevant methods with the actual hackers. This process of systematically and actively testing is done on a deployed network to determine potential vulnerabilities is called Penetration Testing, and is also known as Ethical Hacking. A network penetration test is conducted using specific tools and processes to scan the network for vulnerabilities and discover exploitation mechanisms taking advantage of the discovered security holes. These exhaustive tests can be conducted either by the organization's internal IT security department or by an external certified penetration testing and security auditing organization. Each organization's management must continuously seek for the maximum information input and reevaluate their security policy in an endless loop, as shown in *Fig.1*. This approach will form a truly proactive security policy which is carefully redefined in a regular basis, taking into account every possible parameter (social, technical, environmental) might affect it. The remainder of the paper is organized as follows. Network attack taxonomy, by dividing the threats into classes according to their operational model. We present the proposed penetration testing methodology and working framework in. In we analyze the case study scenario and the lab setup where the penetration test was conducted. Test results and its effects in contrast to a real network setup are shown in.

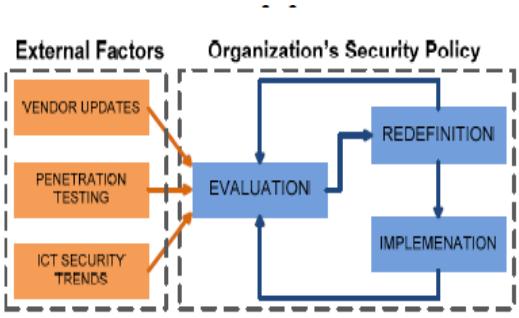


**Figure 1. Interaction between security policy and input from external factors.**

## 2. MODULES

- **GUI protocol specification:** In GUI protocol for the quantity reduction of information transactions between the front-end and the server with the help of compression methods. It is mainly used for the sake of network connections which were slow. The algorithm is developed based on standard ZLIB library which belongs to the system. While utilizing the Genero Web Client, algorithm compression is not get utilized and is gets disabled automatically. Compression detects network connectivities which were slow. Compression algorithm is a waste time for fast connectivity networks.

- **Generator of attack:**

We have to develop a simulated network which was aware of getting attacks and threats information for the sake of security. Those were possible of attack generator which was aware of all published and unpublished vulnerabilities. These are of also capable of getting information when the software fails. These alerts have to rise before security breaches. Based on or using metadata we have to get threats alert attack which were recognized or unrecognized.


**Figure 2: Penetration Testing Methodology Diagram**.

- **Attack injector:**

Approaches for restricting TCP data injection threats are blocked all the in packet-switched networks. Initial approach gives for the sake of leaving received segments that maintains ACK values which are smaller size than the another unknown sequence count number guessed minus the highest size of window. This way of approaching supports to maintain injected spurious segments vary from the TCP re-assembly buffer. In a another approach, heuristics came under utilization to test the sequence count of a recent attached segment, while sequence count is the next guessed, then the recently arrived segment is utilized and the segments of the re-assembly buffer are not considered.

- **Target system and monitor:**

The effected part is where the attack was formed will be visible to the user. This is cause of continuously monitoring.

**Algorithm 1**: Check rule (IPS_id, I, rate I, cap i)
If bi □ **(**IPS_id≠null) then
bi=false;
return
else
ratei← ratei + Fi
if ratei□ capi then
bi=false;
raise DDOS alert;
return
else
next IPS.checkRule(IPS_id,i,rate,cap;)
end if
end if
else
bi=true;
next IPS.checkRule(my ID, i,o,capi)
end if

## 3. RELATED WORK

In today's business environment a vital role is played by Information Communication Technology (ICT) services. Organizations with in adequate resources and skilled employee, started outsourcing their ICT projects to vendors. But outsourcing of these services may also contribute to some risks such as risk with respect to information security that could expose particular organizational information assets directly associated with ICT services at risks. An appropriate information security risk management (ISRM) in place of ICT while outsourcing the services in order to facilitate the management of information security risks in ICT outsourcing. The main objective of this research is to conduct a detailed study on the relationship between consequences and practices of ISRM in ICT Outsourcing. Queries were distributed among a sample of private companies selected from various industry and government agencies in Malaysia for the study. Findings in this study indicate that the difficulty of ISRM process influences its practices in ICT outsourcing. By the findings, influence strength between difficulties and practices of information security risk management approach in ICT outsourcing project has been discovered. Risk treatment planning task was considered as the most difficult and risk control task was considered the least difficult in ISRM cycle. However the management of the organization should plan their risk treatment measures while selecting a plan that could ensure more effective information security risk management implementation. Finally we conclude that by observing the difficulties of organizations in using the ISRM for ICT Outsourcing implies that they need to review and improve them for ICT outsourcing implementation which encourages the development of more comprehensible and effective approach managing information security risk for ICT outsourcing project.

One of topical tasks of policy-based security management is checking that the security policy stated in organization corresponds to its implementation in the computer network. The paper considers an approach to proactive monitoring of security policy performance and security mechanisms functioning. This approach is based on different strategies of automatic imitation of possible users' actions in the computer network, including exhaustive search, express-analysis and generating the optimized

test sequences. It is applicable to different security policies. The paper describes stages, generalized algorithms and main peculiarities of the suggested approach and formal methods used to fulfill the test sequence optimization. We consider the generalized architecture of the proactive monitoring system Â proactive security scanner Â (PSC) developed and its implementation.

A **penetration test**, occasionally **pen test**, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Security issues uncovered through the penetration test are presented to the system's owner. Effective penetration tests will couple this information with an accurate assessment of the potential impacts to the organization and outline a range of technical and procedural countermeasures to reduce risks.

We knew that penetration tests are valuable but several reasons to support this statement are:

1. The feasibility in determining a particular set of attack vectors.
2. Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
3. A particular sequence in which the identification of higher-risk vulnerabilities that are resulted from a combination of lower-risk vulnerabilities is exploited
4. The assessment of the range of potential business and their operational impacts of successful attacks.
5. Testing the ability of network defenders to successfully detect and respond to the attacks
6. Providing evidence to support increased investments in security personnel and technology.

## 4. CONCLUSION

Penetration testing framework for preventive measures along with the existing penetration system procedures solves the problem of security for some extend in addition to patch management. The existing systems take protocol specification as manual and through GUI. The testers are unaware of the protocol specifications causing usability issues. The proposed system solves the problem with pcaps.

## 5. REFERENCES

[1] Khidzir, N.Z., Mohamed, A. and Arshad, N.H.H., "Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing", NETAPPS 2010.

[2] Kshetri, N., "The simple economics of cybercrimes", IEEE Security and Privacy (2006), Volume: 4, Issue: 1.

[3] Kotenko, I. and Bogdanov, V., "Proactive monitoring of security policy accomplishment in computer networks", IDAACS 2009.

[4] Hamisi, N.Y., Mvungi, N.H., Mfinanga, D.A. and Mwinyiwiwa, B.M.M., "Intrusion detection by penetration test in an organization network", ICAST 2009.

[5] Bishop, M., "About Penetration Testing", IEEE Security and Privacy (2007), Volume: 5, Issue: 6.

[6] CERT Coordination Center Statistics, "http://www.cert.org/stats".

[7] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks", Computers Security (2005), Volume: 24, Issue: 1, Publisher: Elsevier, Pages: 31-43.

[8] Long, M., Chwan-Hwa Wu, Hung and J.Y., "Denial of service attacks on network-based control systems: impact and mitigation", IEEE

Transactions on Industrial Informatics (2005), Volume: 1, Issue: 2.

[9] Meadows, C, "A formal framework and evaluation method for network denial of service", Computer Security Foundations Workshop, 1999.

[10] Ansari, S., Rajeev, S.G. and Chandrashekar, H.S., "Packet sniffing: a brief introduction", IEEE Potentials (2003), Volume: 21, Issue: 5.

## Authors

***KUDIKAL SATYANARAYANA*** received his B.Tech Degree in Computer Science and Engineering under JNTUH. He is currently M.Tech student in the Computer Science Engineering from MRCET affiliated to Jawaharlal Nehru Technological University (JNTU), Hyderabad. And he is interested in the field of Data Mining.

***Mr. MADDURU SAMBASIVUDU***, Assistant Professor, Department of CSE, Malla Reddy College of Engineering & Technology, affiliated by JNTU Hyderabad, Andhra Pradesh, India. He received M.Tech in CSE from JNTUH. His research interests include Mobile Computing, Data Mining, and Machine Learning.