RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Enhancement of Data Security from IDS by Configuring Router and Virtual Machine in GNS3

[1]Sushila Rani & [2]Dr Mukesh Kumar

[1]Research Scholar, The technological Institute of Textile & Sciences (India)
[2]A.P. The technological Institute of Textile & Sciences (India)

ARTICLE DETAILS

Article History
Published Online: 15 May 2019

Keywords
IDS, IDS Triggers, GNS3, GNS3 Topology, Manet, Md5, Multiplicative Inverse.

ABSTRACT

This paper has simulated the data using GNS3 and node creation. The reserved port numbers are not used for data transmission. The size of packets has been decreased by exchanging contents of data file with some short words during send and original words are restored at receiving end. The numbers of packets are also reduced in queue so that during routing it becomes easy to secure the packets from intrusion detection. This paper provides the Testing of transmission delay in packet transmission due to security for IDS. Here it offers the Developed packet sender and receiver module. The presented work is helpful to secure the information by MD5 using the concept of IDS mechanism. Here Development of algorithms is made to secure packet by integration of MD5 and Multiplicative inverse function when data is sent from sender to receiver. Use of User datagram protocol makes the transmission reliable because there is no confirmation in this case so we have use TCP based data transmission protocol in our research.

1. Introduction

Intrusion detection system

An ID is referred as burglar alarm. For example lock system in house protects house from theft. But if somebody breaks the lock system & tries to enter into house, it is burglar alarm that detects that lock has been broken & alerts owner by raising an alarm.

Moreover, Firewalls do a really excellent job of air filtering incoming visitors from Internet to circumvent firewall. For instance, external people might link to Intranet by dialing by way of a modem set up on private network [one] of organization; this particular type of access can't be recognized by firewall. An Intrusion Prevention System (IPS) is a system security/threat prevention technological innovation which audits network traffic moves to identify & prevent vulnerability exploits. You will find 2 kinds of prevention method they're Network [two] (NIPS) & Host (HIPS). These systems view network traffic & automatically take measures to safeguard networks [three] & systems. IPS issue is false negatives and positives. False positive is determined to become an event that creates an alarm in intrusion detection system where there's absolutely no strike. False negative is determined to become an event and that doesn't yields an alarm when there's an episodes takes place. Inline operation can make one point of failure, mark updates & encrypted traffic. Actions occurring in a method [four] or maybe network are assessed by IDS.

Types of IDSS

There are 3 kinds of IDSs as found in fig 1Host based IDS views sign of intrusion in neighborhood system. For analysis they utilize host system's logging & some other info. Host based handler is known as sensor. Host-based sensor can get information, contain other logs and system[5] generated by operating system processes & contents of items not mirrored in regular os audit & logging mechanisms. Host based system trust clearly on audit trail.

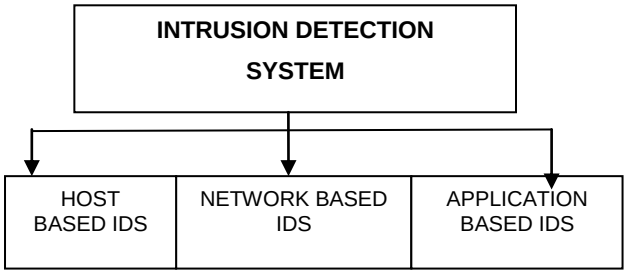

Fig 1 Intrusion Detection Systems

2. Research Objective

The main objective of research is to boost data transmission speed over network without introducing any new hardware.. This paper is focusing on following objectives:

1. Simulation using GNS3 and node creation.
2. Development of Intrusion detection System
3. Testing transmission delay in packet transmission due to security for IDS
4. Testing processing delay during packet transmission
5. Testing queuing delay of network packets
6. Testing propagation delay at time of data transmission
7. Development of algorithm to secure packet by integration of MD5 and Multiplicative inverse function when data is sent from sender to receiver securely.
8. Development of packet sender & receiver module

3. Comparison chart of literature review

SNO.	YEAR	NAME	TOPIC	OBJECTIVE
1	2017	Dharmateja, M., & Vaishnavi, K	Energy Optimization In Wireless Sensor Networks Using Leach Protocol	To discuss the Energy Optimization with the use of Leach Protocol
2	2017	Rani, A., & Bindal, A.	Review of Energy Saving Protocols in WSNs	To study the Energy Saving Protocols in WSNs
3	2017	Malhotra, R.	Review on Wireless Sensor Network Issues Related to Broken Link Problem	To study the Wireless Sensor Network challenges Related to Broken Link issue
4	2016	Rathee, A., Singh, R., & Nandini, A	Wireless Sensor Network-Challenges and Possibilitie	To provide an overview on WSNs and related issue
5	2016	Verma, N., & Sangwan, S.	Secure and Energy Efficient Routing in Wireless Sensor Networks: A Review	To review the Secure and Energy Efficient Routing in Wireless Sensor Networks
6	2015	Tiwari, P., Saxena, V. P., Mishra, R. G., & Bhavsar, D.	A survey of localization methods and techniques in wireless sensor networks	To propose a review on WSNs techniques
7	2015	Dureja, R., & Malik, M.	Routing in Wireless Sensor Networks: A Review	To offer the review on Routing in Wireless Sensor Networks
8	2015	Kaur, A., & Kaur, K.	A Review of Different Energy Efficiency Techniques in Wireless Sensor Networks	To explain the Different Energy Efficiency Techniques in Wireless Sensor Networks
9	2014	Rathna, R., Dhanalakshmi, R., & Sasipraba, T.	Secure Hierarchical Data Aggregation in Wireless Sensor Networks	To present the Secure Hierarchical Data Aggregation in Wireless Sensor Networks
10	2014	Kumar, J., & Sangwan, S.	State of Art Techniques for Wireless Sensor Network Lifetime Maximization	To highlight the State of Art Techniques for WSNs Lifetime Maximization
11	2014	Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M	Wireless sensor networks: a survey on recent developments and potential synergies	To offer a review on WSNs
12	2014	Gupta, S., K., & Sinha, P.	Overview of Wireless Sensor Network: A Survey	To do survey on WSNs
13	2013	Toldan, P., & Kumar, A. A.	Design Issues and Various Routing Protocols for Wireless Sensor Networks (WSNs)	To discuss the Design Issues and Various Routing Protocols for WSNs
14	2013	Sharma, D., Verma, S., & Sharma, K	Network topologies in wireless sensor networks: a review.	To explain the Network topologies in wireless sensor networks
15	2013	Sharma, S., & Mittal, D. P.	Wireless Sensor Networks: Architecture, Protocols	To present the knowledge on WSNs, Architecture and Protocols
16	2012	Kumar, D. M	Healthcare Monitoring System Using Wireless Sensor Network	To offer their view on Healthcare Monitoring System
17	2012	Alkhatib, A. A. A., & Baicher, G. S.	Wireless sensor network architecture	To explain the WSNs and its architecture
18	2012	Othman, M. F., & Shazali, K	Wireless sensor network applications: A study in environment monitoring system.	To provide a study on WSNs applications
19	2006	Gharajeh, M. S., & Khanmohammadi, S	DFRTP: Dynamic 3D Fuzzy Routing Based on Traffic Probability in Wireless Sensor Networks.	To highlight the DFRTP in WSNs
20	2004	Zhao, F., & Guibas, L. J.	*Wireless sensor networks: an information processing approach*	To provide an information processing approach on WSNs

4. Implementation

Node Creation in GNS 3

GNS3 integrates with Virtual Box to management of linked clone VMs. Once it is properly configured, GNS3 will do the work of creating a new VirtualBox linked clone from a base VM every time a node is dragged onto the GNS3 network topology panel. GNS3 will save the clone's file system in the GNS3 project folder.

Create a GNS3 topology:

To create a new GNS3 topology, select a group of devices in the Devices Toolbar by clicking the Browse End Devices button as shown in figure 2

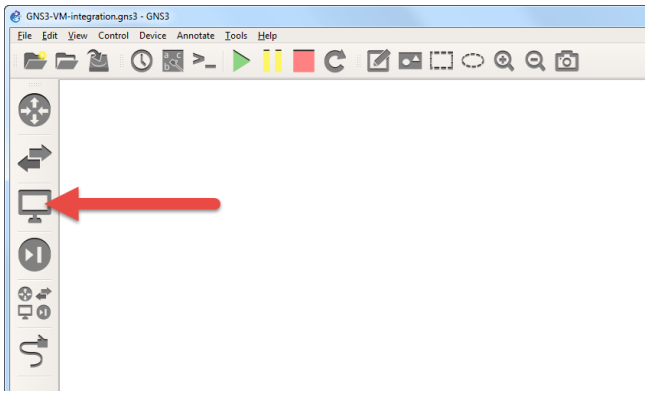

Fig 2 GNS3 interface

The new virtual machine is now available to be added to a GNS3 topology as shown in figure3

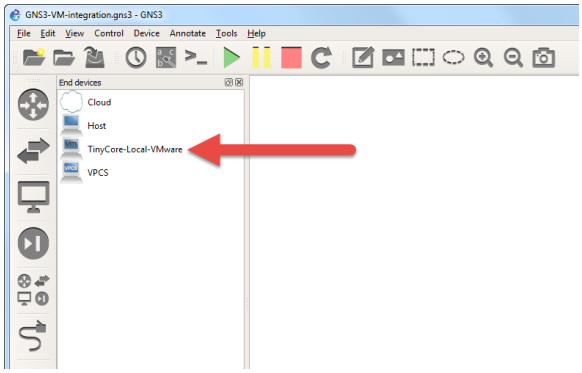

Fig 3 End device management in GNS3

Drag and drop the selected node (device) to the GNS3 **Workspace**. An instance of the node becomes available in the **Workspace** as shown in figure 4:

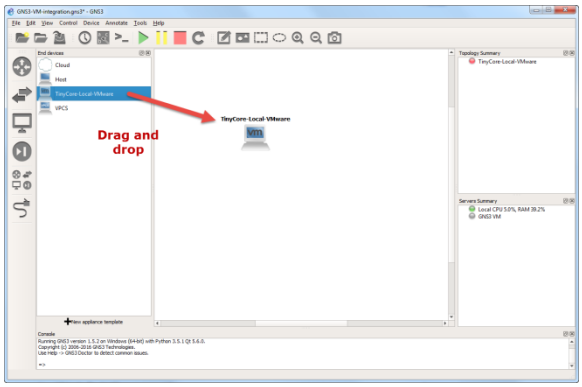

Fig 4 Drag and drop of end device

Select an interface on the second device to complete the connection. In this example, **Fast Ethernet 0/0** on **R2** was selected as shown in figure 5

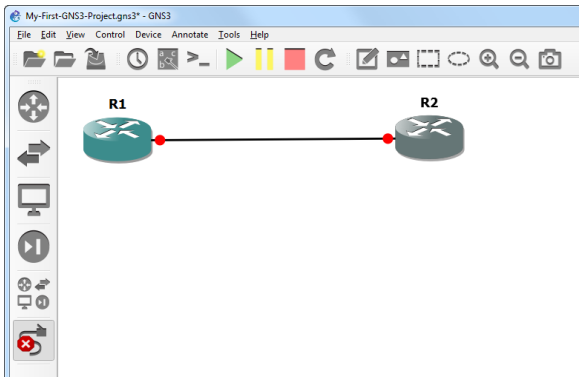

Fig 5 Routers connectivity

Click the **Add a Link** button to stop adding links as shown in figure 6.

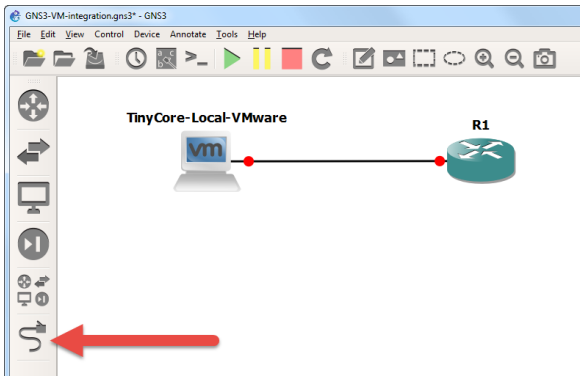

Fig 6 Connecting router to tiny core local VM ware

The **GNS3 Toolbar** to display interface labels in your topology as shown in figure 7

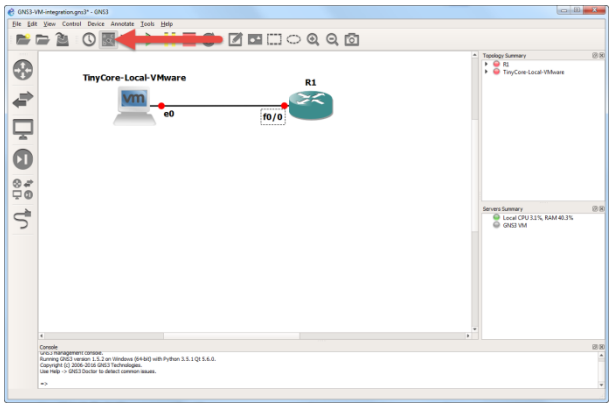

Fig 7 Interface Labels

The **GNS3 Toolbar is** to display interface labels in your topology as shown in figure 8

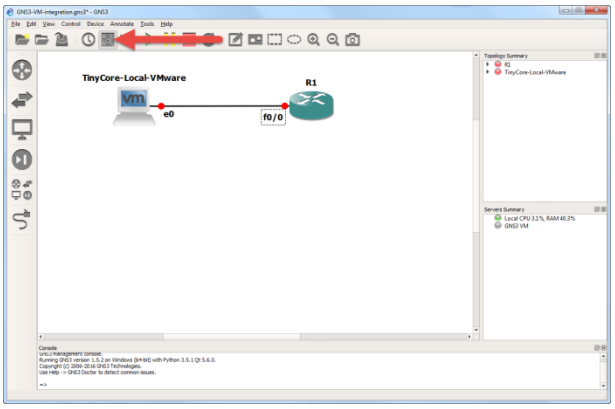

Fig 8 Interface Labels

A console connection is opened to the router in the topology as shown in figure 9

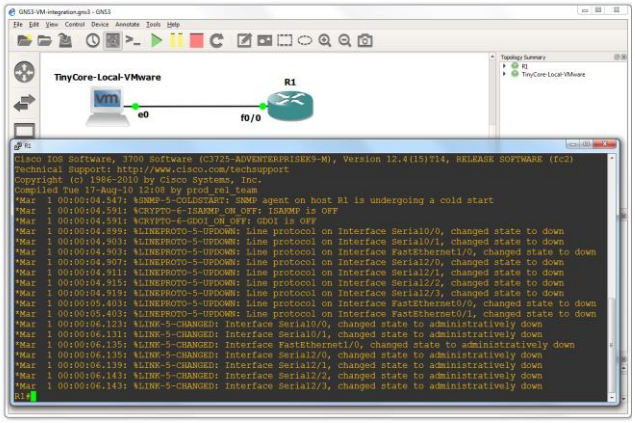

Fig 9 Console connection

CONFIGURING ROUTER AND VIRTUAL MACHINE IN GNS3

Then these groups are inter connected with centralized router as shown in figure 10

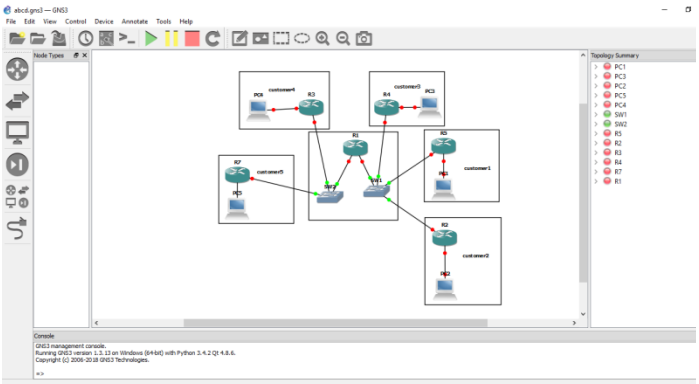

Fig 10 Setting router and virtual machine in GNS3

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis as it is shown by below figure 11:

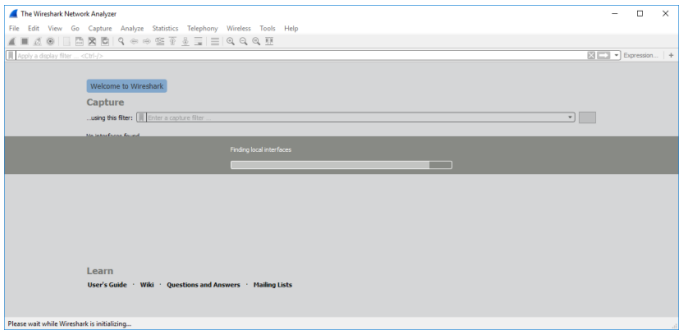

Fig 11 Wireshark interface to simulate packet transmission

Inspecting the time, source, destination protocol in Wireshark has been shown by below given figure:

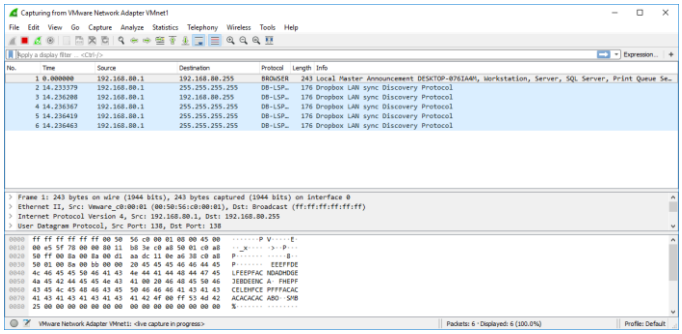

Fig 12 Inspecting the time, source, destination protocol in Wireshark

5. Conclusion

GNS3 integrates with Virtual Box to management of linked clone VMs. Once it is properly configured, GNS3 will do the work of creating a new Virtual Box linked clone from a base VM every time a node is dragged onto the GNS3 network topology panel. GNS3 will save the clone's file system in the GNS3 project folder. This way, we eliminate problem of false negatives that might result from incomplete identification of all untrusted data sources. False positives, although possible in some cases, could typically be easily eliminated during testing. We had studied of existing Testing transmission delay in packet transmission & Testing processing delay during packet transmission. We also make study of testing queuing delay of network packets. There had been need to focus on Establishment of Network Environment to test flow of packets & also need of Development of packet sender & receiver module

6. Future Scope

It would boost data transmission speed over network without introducing any new hardware. To do this we have to understand reasons of delay in data transmission. Simulation and node creation the GNS3 Would be helpful in future time. It also helpful the overall life time of the network by diminishing the power consumption by the node is required. It would provide the Developed algorithm to secure packet by integration of MD5 and Multiplicative inverse function when data is sent from sender to receiver securely. It is capable to offer the Testing of transmission delay in packet transmission due to security for IDS. It would provide the Testing of processing delay at the time of packet transmission with testing of queuing delay of network packets

References

1. Dharmateja, M., & Vaishnavi, K. Energy Optimization In Wireless Sensor Networks Using Leach Protocol. *International Journal of Wireless Communication and Simulation*, 8(1), 21-30.
2. Rani, A., & Bindal, A. (2017). Review of Energy Saving Protocols in WSNs. *International Journal of Advanced Research in Computer Science*, *8*(3), 991-995.
3. Sharma, D., Verma, S., & Sharma, K. (2013). Network topologies in wireless sensor networks: a review. *International Journal of Electronics & Communication Technology,* 4(3), 93-97
4. Rathee, A., Singh, R., & Nandini, A. (2016). Wireless Sensor Network-Challenges and Possibilities. *International Journal of Computer Applications*, *140*(2).
5. Verma, N., & Sangwan, S. (2016). Secure and Energy Efficient Routing in Wireless Sensor Networks: A Review. *International Journal of Computer Science & Engineering Technology (IJCSET)*, 7(2), 33-37.
6. Tiwari, P., Saxena, V. P., Mishra, R. G., & Bhavsar, D. (2015). A survey of localization methods and techniques in wireless sensor networks. *HCTL Open International Journal of Technology Innovations and Research (IJTIR)*, *14*, 2321-1814.
7. P., & Sangwan, S. (2014). Secure Hierarchical Data Aggregation in Wireless Sensor Networks – General framework. *International Journal of Engineering Research & Technology*, 3(6), 1015-1019.
8. Kaur, A., & Kaur, K. (2015). A Review of Different Energy Efficiency Techniques in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(6), 283-288.
9. Rathna, R., Dhanalakshmi, R., & Sasipraba, T. (2015). Centralised against distributed medium access control scheduling for environmental monitoring sensors. *IET Wireless Sensor Systems*, *5*(6), 271-276.
10. Kumar, J., & Sangwan, S. (2014). State of Art Techniques for Wireless Sensor Network Lifetime Maximization. *International Journal of Enhanced Research in Science Technology & Engineering*, 3(5), 275-279.
11. Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of supercomputing*, *68*(1), 1-48.
12. Gupta, S., K., & Sinha, P. (2014). Overview of Wireless Sensor Network: A Survey. *International Journal of Advanced Research in Computer and Communication Engineering*, 3(1), 5201-5207.
13. Toldan, P., & Kumar, A. A. (2013). Design Issues and Various Routing Protocols for Wireless Sensor Networks (WSNs). In *Proceedings of National Conference on New Horizons in IT-NCNHIT* (p. 65).
14. Dureja, R., & Malik, M. (2015). Routing in Wireless Sensor Networks: A Review. *International Journal of Emerging Research in Management & Technology*, 4(10), 124-129.
15. Sharma, S., & Mittal, D. P. (2013). Wireless Sensor Networks: Architecture, Protocols. *International journal of advanced research in computer science and software engineering*, *3*(2).
16. Kumar, D. M. (2012). Healthcare Monitoring System Using Wireless Sensor Network. *International Journal of Advanced Networking and Applications*, *4*(1), 1497.
17. Alkhatib, A. A. A., & Baicher, G. S. (2012). Wireless sensor network architecture. In *2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)*.
18. Othman, M. F., & Shazali, K. (2012). Wireless sensor network applications: A study in environment monitoring system. *Procedia Engineering*, *41*, 1204-1210.
19. Gharajeh, M. S., & Khanmohammadi, S. (2016). DFRTP: Dynamic 3D Fuzzy Routing Based on Traffic Probability in Wireless Sensor Networks. *IET Wireless Sensor Systems*, *6*(6), 211-219.
20. Zhao, F., & Guibas, L. J. (2004). *Wireless sensor networks: an information processing approach*. Morgan Kaufmann.
21. https://www.amrita.edu/center/awna/research/ energy-optimization issues

