International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Improving Defense Mechanism Using Packet Tracer for Switches and Router

Kusum Bhardwaj[1], **Poonam Singh**[2]
[1]M.Tech ECE, [2]Associate Professor
Department of ECE, Shri Ram College of Engineering & Management,
Palwal, Haryana, India

ABSTRACT
We live in that era of time where security is the prime concern everywhere. Nowadays several unauthorized groups are now available in the domain of computer networking. Designing a secure system against attacking is always a challenging task for network developers. Here you can see Layer 2 and 3 attacks on Packet Tracer and also provide their defense mechanism.

Keywords: router, security, packet tracer, router, hubs, networking, network admistrator, hacking

I. INTRODUCTION

As we know that data link layer is completely responsible for encoding as well as decoding where hacking is easily possible. The data link layer is the second layer which is mentioned into the OSI reference model. In addition to this this layer is also responsible for transmission error as well as regulate the flow of data. This paper explains different defense mechanism for restricting against the hacking. Here we can see many mechanism including DHCP spoofing, DHCP spoofing and many more. These defense mechanisms actually control the various network access from unauthorized groups.

II. ROOT ATTACK

As we know that we may have more than one root for any destination s we may consider STP protocol. STP stands for spanning tree protocol which is IEEE 802.1D. Spanning tree protocol builds a loop-free logical topology for any Ethernet networks. This algorithm is specially designed for avoiding any bridge loops. In any case if the best path fails, the algorithm recalculates the network and finds the next best route. As we can see that this path may have root switch or root node which is made either by election among the switches on basis of priority or network administrator assign it.

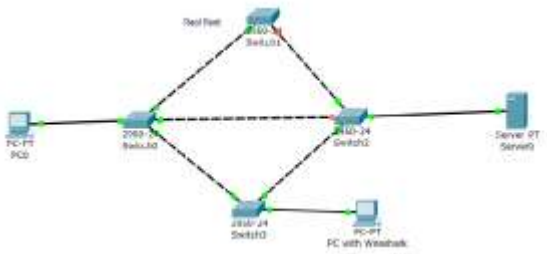

Fig. Root Attack

III. DTP Attack

DTP stands for dynamic trunking protocol which is used to negotiate a trunk between two cisco devices. As we know that dynamic trucking protocol is Cisco proprietary trunking protocol which is used for negotiating the encapsulation type of either IEEE 802.1Q or Cisco ISL (Inter-Switch Link).

Here we design the system for VLAN1 (Virtual local area nework1) but suppose the network which is to be hacked is not in the VLAN 2. Then we analyze the root id as well as bridge id having VLAN group.

Configuration to Block the Path

Switch>enable

Switch#show vtp status

Switch#conf t

Switch(config)#vtp domain screm

Changing VTP 2 domain name from NULL to srcem

Switch(config)#no vlan 10

IV. DHCP SPOOFING

As we know that DHCP stands for dynamic host configuration protocol which is used to dynamically assign IP (Internet Protocol) to any device. Additionally, in DHCP spoofing we can easily have configured fake DHCP server to assign the DHCP address to the clients.

V. DHCP Starvation

This is DHCP starvation in which any of the attacker consumes all the available IP addresses with change of its MAC (Media Access Control) address. Here we have a new concept of IP address which are issued. Now the server can't issue any new more address for accessing any network.

VI. Defense Mechanism

Now we can easily observe that here are some attacks which are created on packet tracer affect the layer 2 and 3 are overcome by using the following defense mechanism.

7.1 Root Attack

This is a defense mechanism which affects the layer 2 and layer 3 using packet tracer. Now we can easily enable root guard. In addition to this we can also the VLAN group.

7.2 DTP Attack

For preventing DTP attack port security feature is used. If another MAC address device use the port then port of the switch automatically becomes off. We can also prevent the DTP attack by configuring access mode and disable dynamic trunking protocol.

7.3 Routing Protocol Attack

If inner port of the router is configured as passive port then no updates will exchanged with the attacker.

7.4 DHCP Starvation and Spoofing attack

Nowadays we have an additional feature of port security. In addition to this we can also shut down the unused ports. Now we can say that by using the above two methods we can easily get from the problem. This is called DHCP starvation and spoofing attack. Also time limit is also configured to the DHCP server for assigning the IP address.

VIII. results

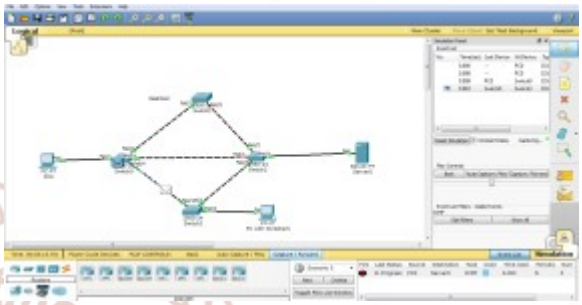

Fig.1

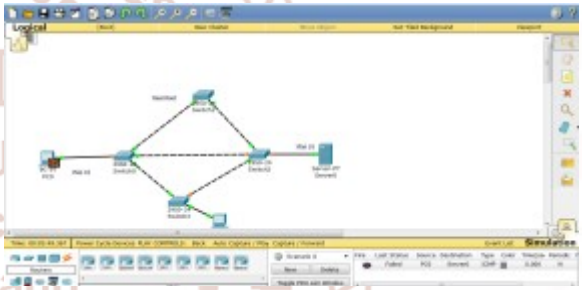

Fig.2

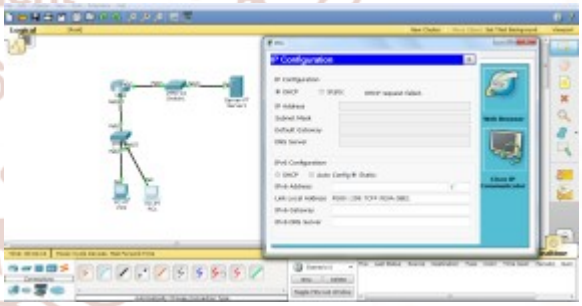

Fig.3

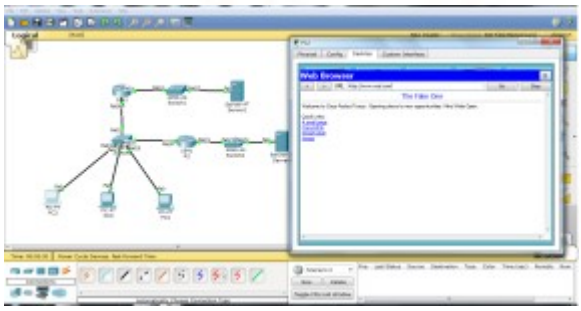

Fig.4

Conclusions

After reading this technical paper we can easily predict that the two layers including data link layer as well as network layer both are vulnerable to attacks including spoofing attack, DHCP starvation and DTP attack also. Now we can say that port security can be considered as one of the trustworthy method. In addition to this we can also say that root attack can also be overcome by enabling root guard and BPDU guard. Additionally we can also consider the concept of AD (Administrative Distance) for selecting the optimum path.

In this thesis, attacks are shown and demonstrated using a simulator called "PACKET TRACER".

References

1) "Exploiting DHCP Server-side IP Address Conflict Detection: A DHCP Starvation Attack'',Nikhil Tripathi, Neminath Hubballi Conference Paper · December 2015.
2) "Tracking Low Grade Attack Using Cisco Packet Tracer Netflow" Manish khule1, Megha Singh2, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 5, Issue 1, January 2015.
3) "Increasing Network Efficiency By Preventing Attacks At Access Layer", G.Narasimha, M. Jithender Reddy, International Journal of Research in Engineering and Technology Volume: 03 Special Issue: 05 | May-2014 , eISSN: 2319-1163 | pISSN: 2321-7308.
4) "A Review of types of Security Attacks and Malicious Software in Network Security" Inam Mohammad and Rashi Pandey, International Journal of Advanced Research in Computer Science and Software EngineeringVol.4, Issue 5,May-2014 ISSN: 2277 128X.
5) "Investigation of DHCP Packets using Wireshark", Mohsin khan, Saleh Alshomrani, Shahzad Qamar, International Journal of Computer Applications (0975 – 8887) Volume 63– No.4, February 2013.
6) "Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks", Biju Issac International Journal of Network Security, Vol.8, No.2, PP.107-118, Mar. 2009.
7) "Tools for Attacking Layer 2 Network Infrastructure" Kai-Hau Yeung, Dereck Fung, and Kin-Yeung Wong, International Multi Conference of Engineers and Computer Scientists 2008 Vol II IMECS 2008, 19-21 March, 2008, Hong Kong.
8) www.cisco.com