Attacks and Defense Mechanisms on Routers and Switches Using Packet Tracer

Priyanka Sharma, Manoj Awana

***Abstract*— In computer networking, attacking has become very common to unauthorized groups. In order to fight against attacking, we have designed a defense mechanism through which information can be prevented from being attacked. We can not only safe user information but can increase network efficiency too. Here defense mechanism does not allow switches to get attacked by unauthorized groups and hence sharing of information with hacker minimizes. In this paper, we demonstrate Layer 2 and Layer 3 attacks on Packet Tracer and also provide their defense mechanism.**

***Index Terms*— Attack, Configuration, Dynamic Trunking Protocol, Dynamic Host Configuration Protocol, DHCP starvation, DHCP spoofing, VLAN, Network Security**

I. INTRODUCTION

The data link layer is that layer in the OSI reference model on which hacking is easily possible. There are various types of network attacks are created by the attacker. In these attacks, sensitive information of the user is acquired and normal behavior of network is maniputated. In order to fight against attacking, different types of defense mechanisms are provided to restrict the attack. These defense mechanism controls the network access from unauthorized groups.

II. ATTACKS ON ROUTERS AND SWITCHES

Most of the time hacking is performed on data link layer because it is easily possible on this layer. There are various types of attack which are performed on this layer, some of them are listed here

- Root Attack
- DTP Attack
- Routing Protocol Attack
- DHCP Starvation
- DHCP Spoofing

2.1 Root Attack and DTP Attack

There is more than one root for the destination in the given topology so in this situation STP (Spanning tree protocol) is used. STP disables other path and enable only single path to form the loop free structure. This path must have root node or root switch which is made either by election among the switches on basis of priority or network administrator assign it. To attack the given network, the hacker connects its switch to the network switches and configures its switch as the root switch.

In the root attack we attack the network assuming the network top be in VLAN 1 but suppose the network which is to be hacked is not in the VLAN 1. First attacker has to search the VLAN group used by looking whether bridge id and root id are same. After searching the VLAN makes its switch as root switch and block the path using the following command and change the VTP domain name.

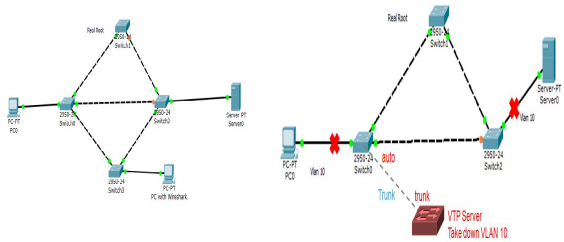

Figure: Root Attack and DTP Attack

2.2 Routing Protocol Attack

In routing attack instead of original route a fake root is provided to router whose distance is shorter than the original root. Hence user is connected to the fake server.

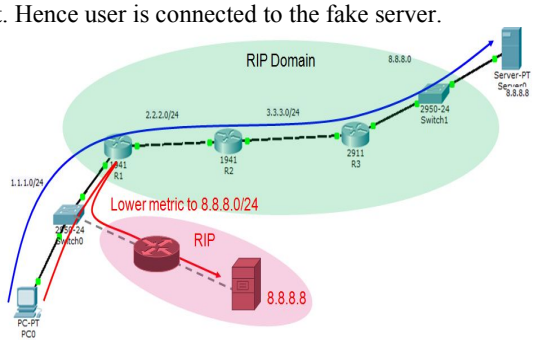

Figure: Routing Protocol Attack

2.3 DHCP Starvation and DHCP Spoofing

In this attack, an attacker consumes all the available IP addresses with change of its MAC address. After these IP addresses are issued, the server cannot issue any more addresses, now new clients cannot obtain network access. [2] In DHCP spoofing fake DHCP server is configured in the network to assign the DHCP address to the clients. Now user machine is under the control of the attacker.

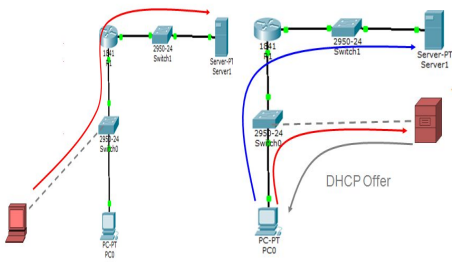

Figure: DHCP Starvation and Spoofing Attack

Manuscript received June 11, 2016
Priyanka Sharma, M.Tech scholar, NGFCET Palwal
Manoj Awana, Assistant Prof., NGFCET Palwal

III. DEFENSE MECHANISM

The attacks which are created on packet tracer affect the layer 2 and 3 are overcome by using the following defense mechanism.

3.1 Defense for Root Attack and DTP Attack

To overcome this attack we can enable the root guard, in this situation another switch will not be Root Bridge and information will not check out. Secondly by changing the VLAN group of the client machine.

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 disabling dynamic trunking protocol, dot1x authentication, VTP Transparent and VTP Authentication.

3.2 Defense for Routing Protocol Attack

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

3.3 DHCP Starvation and Spoofing attack

By using the port security feature and making the unused port shut down the DHCP starvation and spoofing problem can be overcome. A time limit is configured to the DHCP server to assign the IP address to prevent DHCP starvation attack. DHCP spoofing problem can be overcome by using Dot1x authentication and making snooping trust port which means valid MAC address machine can use the port.

IV. RESULT AFTER ATTACK

After these different attacks, the normal behavior of the network is changed and it is manipulated by the attacker. In root attack path of the packet is changed and in DTP attack path is blocked. The following figures show working of the network after attack.

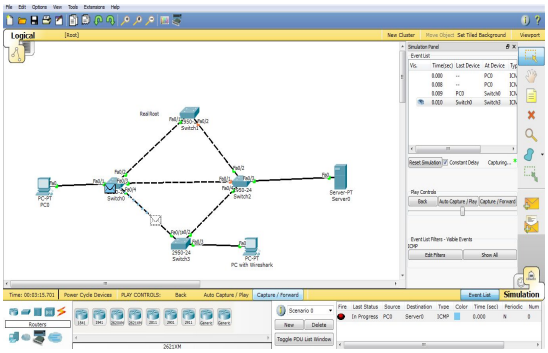

Figure: Packet Forwarding after Root Attack

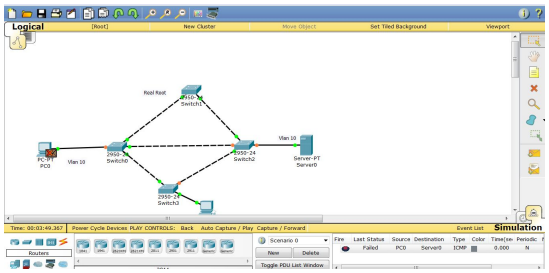

Figure: Packet does not forward after DTP Attack

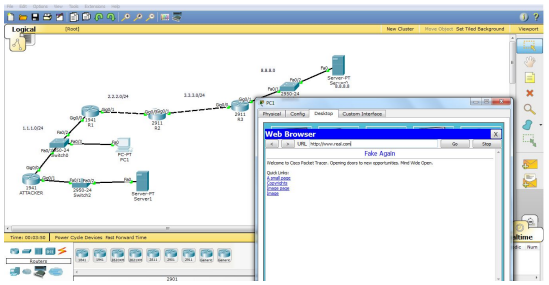

Figure: Routing Protocol Attack

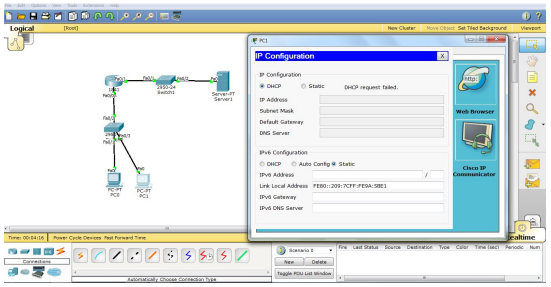

Figure: DHCP Starvation Attack after consuming all the IP Addresses

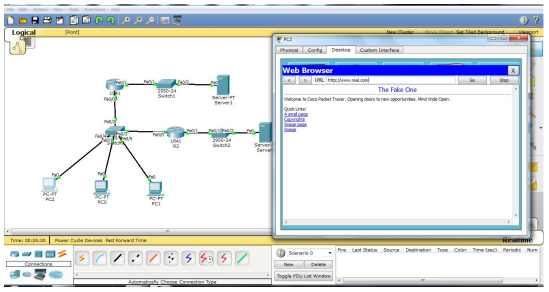

Figure: Web Browser of PC2 connected with Fake Server in DHCP Spoofing

CONCLUSIONS

Data link layer and Network layer devices are vulnerable to attacks like Root attack, DTP attack, Routing Protocol attack, DHCP starvation and spoofing attack. These attacks can be prevented by using defense mechanism. DHCP attack can be prevented by configuring port security and snooping security feature. Root attack can be overcome by enabling root guard and BPDU guard. To prevent DTP attack access mode is configured.

This paper has provided solutions to the attacks on router and switches. 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] "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.

[3] "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.

[4] "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.

[5] "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.

[6] www.cisco.com