

Open Access

On Compound Attacks Composed of Man-in-the-middle Attacks and Smurf Spoofing

Yao Tong and Shigeo Akashi*

Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan

Abstract

Nowadays there are various kinds of cyber attacks threatening the Internet and there has never been such an age when every cyber incident response team is making effort in developing countermeasures against cyber attacks. Actually, almost all cyber incident response teams develop each countermeasure against each cyber attack on case-by-case basis.

In this paper, if we take smurf attacks and man-in-the-iddle attacks as an example of two cyber attacks which are different from each other, then a simultaneous use of them happens to have a maliciously synergistic effect on the networking system which cannot be prevented by DHCP snooping.

Publication History:

Received: April 27, 2023 Accepted: May 08, 2023 Published: May 10, 2023

Keywords:

Smurf spoofing, Man-in-themiddle attack, DHCP spoofing, DHCP snooping

Introduction

Nowadays there are various kinds of cyber attacks threatening the Internet and there has never been such an age when the Internet plays so important roles as today. Unfortunately, the more skillful and sophisticated the contemporary network skills are, the more vulnerable both the wide and the local area networks are to the cyber attacks. Exactly speaking, as for the vulnerability accompanying the contemporary network skills, they can be classified into the following two cases:

- Inevitable vulnerability: The vulnerability accompanying network skils which cannot be removed from the contemporary network skills, because we have some adverse side effects on the Internet unless the network skills are used.
- Non-inevitable vulnerability: The vulnerability which can be removed from the contemporary network skills without causing any other side-effects on the Internet.

It is a matter of courese that the cyber attacks based on the inevitable vulnerability is more dangerous than the cyber attacks based on the non-inebvitable one. Moreover, as for the distance between the cyber attackers and the victims, they can be clssified into the following two cases:

- Remote attacks: The attack which is made possible by the cyber attackers who are far from the victimes.
- Local attacks: The attack which is made possible by the cyber attackers who are near the victimes.

It is a matter of course that the cyber attacks originating in remote area where the cyber attackers exist is more difficult than the cyber attacks originating in local area where the victims exist [1]. There are some other network theoretic points of view which can be regarded as criteria which can indicate how dangerous and malicious cyber attacks are. If we apply these two classifications to smurf spoofing and man-in-the-middle attack, then we can represent a maliciously synergistic effect as the following:

cyber attacks	remote or local	inevitable or non- inevitable
smurf spoofings only	remote	non-inevitable
man-in-the-middle attacks only	remote	non-inevitable
simultaneous use of smurf spoofings and man-in-the- middle attacks	remote	inevitable

Table 1: Smurf attacks and man-in-the-middle attacks cyber.

In this paper, we discuss smurf spoofings and man-in-the-middle attacks as examples of two cyber attacks which are different from each other, and clarify a malicously synergistic effect on the Internet, which is brought about by a simultaneous use of them.

Network Topology Where Man-in-the-middle Attack Happens

In this section, we show an example illustrating smurf spoofings and man-in-the-middle attacks which can be deployed in the following network:

In the above figure, we can find two network areas encircled in blue and in red, respectively. These two network areas are connected to each other by way of Switch-boundary. A DHCP client which is named as DHCP-client-laptop-192.168.0.1, is located in the right-hand side of the blue-colored network area, while a DHCP server combining a gateway router with a DHCP server simultaneously and being named as DHCP-authenticated-router-192.168.0.254, is alocated in the lefthand side of the blue-colored network area. Moreover, two routers

*Corresponding Author: Prof. Shigeo Akashi, Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan, E-mail: akashi@is.noda.tus.ac.jp

Citation: Tong Y, Akashi S (2023) On Compound Attacks Composed of Manin-the-middle Attacks and Smurf Spoofing. Int J Comput Softw Eng 8: 185. doi: https://doi.org/10.15344/2456-4451/2023/185

Copyright: \mathbb{O} 2023 Tong. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

IJCSE, an open access journal Volume . 2023. 185





following the procedure for the man-in-the-middle attacks and being named as Router-for-man-in-the-middle-attack-192.168.0.253 and Router-for-manin- the-middle-attack-192.168.0.252, respectively, are located in the left-hand side and the right-hand side of the pink-colored network area.

Proposed Solution

In figure 1, we can find two network areas encircled in blue and in red, respectively. These two network areas are connected to each other by way of Switch-boundary. A DHCP client which is named as DHCP-client-laptop-192.168.0.1, is located in the right-hand side of the blue-colored network area, while a DHCP server combining a gateway router with a DHCP server simultaneously and being named as DHCP-authenticated-router-192.168.0.254, is alocated in the lefthand side of the blue-colored network area. Moreover, two routers following the procedure for the man-in-the-middle attacks and being named as Router-for-man-in-the-middle-attack-192.168.0.253, and Router-for-manin-the-middle-attack-192.168.0.252,respectively, are located in the left-hand side and the right-hand side of the pinkcolored network area [2].

Throughout this paper, since the role of attacking on the blue-colored netowrk, which Routerfor-man-in-the-middle-attack-192.168.0.252 plays is almost the same as Router-for-man-in-the-middleattack-192.168.0.253 does, we discuss the cyber attacks played by Router-for-man-in-the-middle-attack-192.168.0.253 only.

Under the above network circumstances, the IP address of the interface of DHCP-client-laptop-192.168.0.1 is assumed to be assigned by DHCP-authenticated-router-192.168.0.254. Since DHCP transactions commuting between DHCP-client-laptop-192.168.0.1 and DHCP-authenticated-router-192.168.0.254 must pass through Switch-boundary, two cyber attackers, namely Router-for-man-in-the-middle-attack-192.168.0.253 and Router-for-man-in-the-

middle-attack-192.168.0.252, is also assumed to connect themselves to Switch-boundary, and the distance bwtween DHCP-authenticatedrouter-192.168.0.254 and DHCP-client-laptop-192.168.0.1 can be characterized by the total number of the switches existing on the shortest route connecting between them and is equal to four. Moreover, the distance between DHCPauthenticated- router-192.168.0.254 and Router-for-man-in-the-middle-attack-192.168.0.253, which is exactly equal to the distance between DHCP-authenticatedrouter-192.168.0.254 and Router-for-maninthe-middleattack-192.168.0.252, can be characterized by the total number of the switches existing on the shortest route connecting between them and is equal to three. Under the above network circumstances, the interface of DHCP-authenticated-router-192.168.0.254 and the interface of Routerfor-man-in-the-middle-attack-192.168.0.253 are configured as figure 2:

The figure 2 shows that both the IP address and the MAC address which are assigned for the interface of DHCP-authenticated-router-192.168.0.254 is 192.168.0.254 and 0005.5ec7.3e01, respectively.

The above figure shows that both the IP address and the MAC address which are assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253 is 192.168.0.253 and 00d0.58a1.0001, respectively.

While the attacker is allowed to share neither IP address nor MAC address which has already assigned for the interfaces of some other authenticated routers, the IP address which is assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253 can be changed intentionally from 192.168.0.253 to 192.168.0.254 for a very short period of time, even though the MAC address which is assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253 can never be changed anytime [3].

Page 3 of 6



Page 3 of 6

Smurf spoofings

Throughout this section, we use the network topology which has been introduced in the previous section and discuss the smurf spoofing which is carried out by Router-for-man-in-the-middle-attack-192.168.0.253 only [4].

Now the smurf spoofing is composed of the following two stages, that is, the first stage is prepared for listeing by Router-for-man-in-the-middle-attack-192.168.0.253 and the second stage is prepared for captureing by this attacker, respectively.

The first stage exists for Router-for-man-in-the-middleattack-192.168.0.253 to listen to broadcast packets commuting betwen DHCP-client-laptop-192.168.0.1 and DHCP-authenticatedrouter-192.168.0.254, and the sequential packet streaming being monitored by Router-for-man-in-the-middle-attack-192.168.0.253, which includes DHCP transactions originating in DHCPauthenticated-router-192.168.0.254 can be illustrated as the following (Figure 4):

- Before the falsified packet is sent, the IP address assigned for DHCP-authenticated-router-192.168.0.254 corresponds to the MAC address assigned for the interface of DHCP-authenticatedrouter-192.168.0.254.
- After the falsified packet has been sent, the IP address assigned for DHCP-authenticated-router-192.168.0.254 corresponds to the MAC address assigned for the interface of Router-for-man-inthe-middle-attack-192.168.0.253.

Here, the difference between the ARP table of DHCP-clientlaptop-192.168.0.1 before the smurf spoofing and the ARP table after the smurf soofing can be illustrated as figure 5 [5]:

In the figure 5, the ARP table DHCP-client-laptop-192.168.0.1 shows that the smurf spoofing which has been carried out by Router-for-manin-the-middle-attack-192.168.0.253 has made the correspondence of the IP address assigned for the interface of DHCP-authenticatedrouter-192.168.0.254 to be changed from 0005.5ec7.3e01 to 00d0.58a1.0001, the former half of which is assigned for the MAC address of the interface of DHCP-authenticated-router-192.168.0.254 and the latter half of which is assigned for the MAC address of the interface of Router-for-man-in-the-middle-attack-192.168.0.253.

<pre>Physical Cong CL Attributes IOS Command Line Interface If you require further assistance please contact us by sending email to export@cisco.com. Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory. Processor board ID FYK152400KS8 2 Gigabit Ethernet interfaces DRAM configuration is 64 bits wide with parity disabled. 25K bytes of non-volatile configuration memory. 249856K bytes of ATA System CompactFlash 0 (Read/Write) Press RETURN to get started! %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2} Router_for_man_in_the_middle_attack_192.168.0.2} Press 0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>				A							
<pre>IdS Command Line Interface If you require further assistance please contact us by sending email to export@cisco.com. Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory. Processor board ID FTX152400KS 2 Gigabit Ethernet interfaces DRAM configuration is 64 bits wide with parity disabled. 255K bytes of non-volatile configuration memory. 249856K bytes of ATA System CompactFlash 0 (Read/Write) Press RETURN to get started! %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2# IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 62, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	Physical	Config	CLI	Attributes							
<pre>If you require further assistance please contact us by sending email to export@cisco.com. Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory. Processor board ID FTX152400K8 2 Gigabit Ethernet interfaces DRAM configuration is 64 bits wide with parity disabled. 25K bytes of non-volatile configuration memory. 249856K bytes of ATA System CompactFlash 0 (Read/Write) Press RETURN to get started! %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2*en Router_for_man_in_the_middle_attack_192.168.0.2*f IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_</pre>					IOS	Command L	ine Interface				
<pre>Clisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory. Processor board ID FTX152400KS 2 Gigabit Ethernet interfaces DRAM configuration is 64 bits wide with parity disabled. 255K bytes of non-volatile configuration memory. 249856K bytes of ATA System CompactFlash 0 (Read/Write) Press RETURN to get started! %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2# Packet debugging is on Router_for_man_in_the_middle_attack_192.168.0.2# IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=256.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=256.255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	If you export@	require cisco.co	further m.	assistance	please	contact us	s by sendir	ng email t	0		^
<pre>Press RETURN to get started! %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2#debug ip packet Packet debugging is on Router_for_man_in_the_middle_attack_192.168.0.2# IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	Cisco C Process 2 Gigab DRAM co 255K by 249856K	ISCO1941 or board it Ether nfigurat tes of n bytes o	/K9 (re ID FTX net int ion is on-vola f ATA S	vision 1.0) 152400KS erfaces 64 bits wid tile config ystem Compa	with 49 e with p uration r ctFlash	1520K/3276 arity disa nemory.) (Read/W1	58K bytes o abled. rite)	of memory.			
<pre>%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2#debug ip packet Packet debugging is on Router_for_man_in_the_middle_attack_192.168.0.2# IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	Press R	ETURN to	get st	arted!							
<pre>Router_for_man_in_the_middle_attack_192.168.0.2>en Router_for_man_in_the_middle_attack_192.168.0.2#debug ip packet Packet debugging is on Router_for_man_in_the_middle_attack_192.168.0.2# IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 62, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	%LINEPR	OTO-5-UP	DOWN: L	ine protoco	l on Inte	erface Gio	gabitEtherr	net0/0, ch	anged st	ate to up	
<pre>IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	Router_ Router_ Packet Router_ IP: s=0	for_man_ for_man_ debuggin for_man_ .0.0.0 (in_the_i in_the_i g is on in_the_i Gigabit	niddle_atta niddle_atta niddle_atta Ethernet0/0	ck_192.1 ck_192.1 ck_192.1), d=255	68.0.2>en 68.0.2#dek 68.0.2# .255.255.2	oug ip pack 255 len 62,	rcvd 2			
<pre>IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	IP: s=0	.0.0.0 (Gigabit	Ethernet0/0), d=255	.255.255.2	255 len 77,	rcvd 2			
<pre>IP: s=0.0.0.0 (GigabitEthernet0/0), d=255.255.255.255 len 77, rcvd 2 IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	IP: s=1	92.168.0	.254 (G	igabitEther	net0/0),	d=255.255	5.255.255 1	en 81, ro	vd 2		
<pre>IP: s=192.168.0.254 (GigabitEthernet0/0), d=255.255.255.255 len 81, rcvd 2 Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#</pre>	IP: s=0	.0.0.0 (Gigabit	Ethernet0/0), d=255	.255.255.2	255 len 77,	rcvd 2			
Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2# Router_for_man_in_the_middle_attack_192.168.0.2#	IP: s=1	92.168.0	.254 (G	igabitEther	net0/0),	d=255.255	5.255.255]	en 81, ro	evd 2		
	Router_ Router_ Router_ Router_ Router_ Router_ Router_	for_man_ for_man_ for_man_ for_man_ for_man_ for_man_ for_man_	in_the_ in_the_ in_the_ in_the_ in_the_ in_the_ in_the_	niddle_atta niddle_atta niddle_atta niddle_atta niddle_atta niddle_atta niddle_atta	ck_192.1 ck_192.1 ck_192.1 ck_192.1 ck_192.1 ck_192.1 ck_192.1 ck_192.1	68.0.2# 68.0.2# 68.0.2# 68.0.2# 68.0.2# 68.0.2# 68.0.2# 68.0.2#					>

Page 4 of 6

Physical Config Desktop Programming	Attributes			
Command Prompt			Х	
C·\>				
C:\>ping 192.168.0.254				
Pinging 192.168.0.254 with 32 bytes of	ata:			
Reply from 192.168.0.254: bytes=32 time Reply from 192.168.0.254: bytes=32 time Reply from 192.168.0.254: bytes=32 time Reply from 192.168.0.254: bytes=32 time	1ms TTL=255 15ms TTL=255 33ms TTL=255 1ms TTL=255			
Ping statistics for 192.168.0.254: Packets: Sent = 4, Received = 4, Lo Approximate round trip times in milli-s Minimum = Oms, Maximum = 33ms, Aver	et = 0 (0% loss), conds: ge = 12ms			
C:\> C:\>arp -a Internet Address Physical Addres 192.168.0.254 0005.5ec7.3e01	Type dynamic			
C:\> C:\>arp -a Internet Address Physical Address 192.168.0.254 00d0.58a1.0001	Type dynamic			d
C:\> ure 5: The difference of the ARP table of the victim	before and after the attack.			
Router_for_man_in_the_middle_attack_192.168.0.253			- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config <u>CLI</u> Attributes	IOS Command Line Interface		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config <u>CLI</u> Attributes #NIS-5-CONFIG_1: Configured from console by console	IOS Command Line Interface		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLL Attributes #SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Time consects as phone.	IOS Command Line Interface		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config <u>CLI</u> Attributes *NYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout	IOS Command Line Interface .168.0.1 s 2 seconds:		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLI Attributes #SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IF: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes *SYS-5-CONFIG_1: ConFigured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending		- 0	Ŷ
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLL Attributes %SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes *SYS-5-CONFIG_1: ConFigured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes *SYS-5-CONFIG_1: ConFigured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending		- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config <u>CLI</u> Attributes *SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via B	RIB	- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes *SYS-5-CONFIG_1: ConFigured From console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via R (GigabitEthernet0/0), len 128, rcvd 3	RIB	- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLL Attributes *SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB (GigabitEthernet0/0), len 128, rcvd 3 igabitEthernet0/0), routed via RIB	RIB	- 0	×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes *8YS-5-CONFIG_1: ConFigured From console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.1	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB igabitEthernet0/0), len 128, rcvd 3 igabitEthernet0/0), routed via RIB net0/0), len 128, sending	RIB		×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes *SYS-5-CONFIG_I: ConFigUred From Console by Console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.1 (GigabitEthe	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via R igabitEthernet0/0), len 128, rcvd 3 igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via R	RIB		×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes **SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 P: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 P: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 P: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 P: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=192.1	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB	RIB		×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLIAttributes **SYS-5-CONFIG_1: ConFigured From Console by Console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IOS Command Line Interface IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB	RIB		×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLI_Attributes **SYS-5-CONFIG_I: ConFigUred From console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.1 (GigabitEtherne	IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via R (GigabitEthernet0/0), len 128, rcvd 3 igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via R (GigabitEthernet0/0), len 128, rcvd 3 igabitEthernet0/0), routed via RIB net0/0), len 128, sending	RIB		×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLI_Attributes **SYS-5-CONFIG_1: Configured from console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe P: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.254 (local)	IOS Command Line Interface IOS Command Line Interface .168.0.1 s 2 seconds: igabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed igabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB	RIB		×
Router_for_man_in_the_middle_attack_192.168.0.253 Physical Config CLI_Attributes **YIS-5-CONFIG_I: ConFigured From console by console Router_for_man_in_the_middle_attack_192.168.0.2#ping 19 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! r tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! r tableid=0, s=192.168.0.1 (GigabitEthernet0/0), d=19 IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! r tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.254 (local), d=192.168.0.1 (GigabitEthe ! IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 IP: tableid=0, s=192.168.0.254 (local), d=192.168.0.1 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.168.0.254 (IP: s=192.168.0.1 (GigabitEthernet0/0), d=192.	IOS Command Line Interface .168.0.1 s 2 seconds: ligabitEthernet0/0), routed via RIB net0/0), len 128, sending net0/0), len 128, encapsulation failed ligabitEthernet0/0), routed via RIB net0/0), len 128, sending .168.0.254 (GigabitEthernet0/0), routed via RIB	RIB		×

Smurf-spoofing-aided man-in-the-middle Attacks

In this section, we show that a simultaneous use of smurf spoofings and man-in-the-middle attacks brings about a maliciously unexpected synergistic effect. Here, if we assume that the smurf spoofings have been intentionally carried out by Router-for-man-in-the-middle-attack-192.168.0.253 and that the MACaddress table of DHCP-client-laptop-192.168.0.1 has come to contain the malicious correspondence between the IP address assigned for the interface of DHCP-authenticated-router-192.168.0.254 and the MAC address assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253, then, by way of Switch-boundary, any packet whose source IP address and destination IP address is 192.168.0.1 and 192.168.0.254 turns to be bound for Router-for-man-in-the-middle-attack-192.168.0.253 as its final destination. Therefore, if Router-for-man-in-the-middle-attack-192.168.0.253 configures the following default route:

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.254

in its routing table, then the packet having stopped by Router-forman-in-the-middle-attack-192.168.0.253 halfway on the optimal route connecting between DHCP-authenticated-router-192.168.0.254 and DHCPclient-laptop-192.168.0.1 results in being forwarded to DHCP-authenticated-router-192.168.0.254. Unfortunately, this round trip route constructed maliciously by the smurf spoofing can be recognized neither DHCP-authenticated-router-192.168.0.254 nor DHCP-client-laptop-192.168.0.1.

Here the sequential progress, which are monitored by Routerfor-man-in-the-middle-attack-192.168.0.253 can be illustrated as Figure 6:

Conclusions

A large part of the comtemporary networking systems provide authenticated network clients with IP addresses and other information which are required for the authenticated clients' connecting to the Internet according to Dynamic Host Configuration Protocol. Therefore, if man-in-the middle-attacks are based on DHCP spoofings, then DHCP snooping can completely prevent the network clients from the cyber attacks being carried out DHCP spoofers. Actually, as we have seen, a simultaneous use of the man-in-the-middle attacks and the smurf spoofings cannot be prevented by DHCP snooping, because the man-in-the-middle attackers who are combined with smurf spoofers do not play a malicious role of the DHCP spoofers.

Such man-in-the-the middle attacks based on smurf spoofings as stated in this paper cannot capture any packets originating in the authenticated gateway routes and being bound for the authenticated metwork clients. Therefore, if the attackers want to the packets originating in the gateway routers and being bound for the network clients, then some other attackers such as Router-for-man-in-themiddleattack-192.168.0.252 in Figure 1 should play this role.

Competing Interests

The author declare that he has no competing interests.

References

 A Cisco Guide to Defending Against Distributed Denial of Service Attacks, September, 2019.

- 2. Santos O, Muniz J (2017) CCNA Cyber Ops Secfnd 210-250, Cisco Press, Indianapolis, 1st edition,
- Santos O, Muniz J (2017) CCNA Cyber Ops Secfnd 210-255, Cisco Press, Indianapolis, 1st edition,
- 4. Knuth DE (1973) The Art of Computer Programming, Addison-Wesley Publishing Company, Massachusetts, 2nd edition, 1973.
- Kumar S (2007) Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet, Proceedings of International Conference on Internet Monitoring and Protection.