International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2659-2662

Implementing of IP address Recovery for DHCP Service

Mayoon Yaibuates[1] and Roungsan Chaisricharoen[2]

School of Information Technology, Mae Fah Luang University, Chiang Rai, Thailand.
E-mail: [1]mayoon@outlook.com, [2]roungsan.cha@mfu.ac.th

Abstract

DHCP server is always threatened by several types of attack. DHCP starvation is one of the method widely been used as a method aim to ruin the availability of the server by consumed all available IP addresses. To recover the DHCP service from starvation attack, the using of ICMP has been proposed as a method for recovering IP address hold by attacker. The objective of this paper is to implement the ICMP based IP address recovering method on *chilli* daemon DHCP service. The experimental result from this implementation revealed that DHCP service with ICMP based IP address recovering method had 100 % of true positive and 0 % of false positive.
Keywords: Dynamic Host Configuration Protocol, DHCP, DHCP Discover, DHCP security, IP address recovery

INTRODUCTION

In the last decade, communication over computer network especially internet has become an essential part of our daily life. To make life easier, computer is just not only device used for accessing the internet. Mobile phone and others smart devices are also able to access the internet conveniently. Wireless network communication, commonly known as Wi-Fi is a new popular trend using for accessing to the internet.

Captive portal is being used as a convenient tool for authenticated Wi-Fi user before accessing to the internet via webpage. C*oovaChill* is open source software widely used for provides function of captive portal.

Dynamic host configuration protocol (DHCP) is a protocol used for providing Internet Protocol (IP) address and other necessary host configuration parameters such as network address, subnet mask, and default router dynamically to network devices correctly. IP address and other network parameters are needed for communicating with other devices and network services located in the network. Without the use of DHCP in the network for providing the following network parameter the situation can become time consuming and inconvenient for completing a task. It's imperative that network users must configure the IP address and other network parameters to their device manually. Moreover, incorrect configuration will deny the device from accessing to the network and services. That's the reason why DHCP server is one of the most important network infrastructures [1].

Although DHCP server has played an important role in the network, there is a lack of security concern during the development of DHCP protocol [2]. The following protocols have been used by attackers to attack the network [3]. DHCP starvation attack is an attack that exhausts all available IP address in the server pool. After the attack has been launch, attackers might attach their own DHCP server, Rouge DHCP [4], acting as DHCP server to provide network configuration parameters to the other legitimate user devices. Furthermore, attackers could assign an IP address of their own computer as a default router parameter. Thus, attackers can capture, modify, and analyze every packet sent from the attacked device [5].

Our recent work in [6] introduces an ICMP based IP address recover method for DHCP. The mentioned method applies the use of ICMP echo and echo reply message for differentiate between the IP address had taken by legitimate client from malicious client. If the client be able to respond back with ICMP echo reply message, it can be implying that this IP address had taken by legitimate client. Otherwise, the IP address had taken by malicious client.

This present paper provides implementation results of an ICMP based IP address recover method on DHCP service.

BACKGROUND THEORY

DHCP protocol

DHCP has mostly been used as an implemented mechanism for automating assigned network configuration parameters of TCP/IP implementation system [7]. In order to communicate with other hosts in the network, network configuration parameters have to be required in each device. Examples of general parameters are IP Address, Subnet Mask, IP Address of default gateway, IP Address of DNS Server and etc. Without using DHCP, a network administrator is required to assign those parameters to client devices manually which becomes more time consuming and causing inconvenience. Moreover, an incorrect configuration may cause some network problems to each device and other technical aspects.

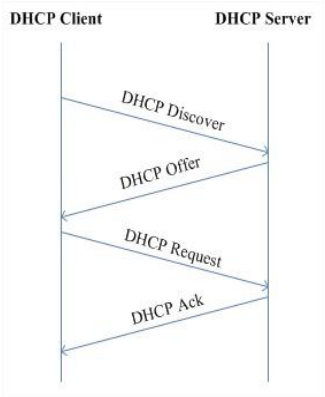

Figure 1: Exchanging messages in DHCP Protocol

Figure 1 demonstrates the process of DHCP operation as the following:

1) DHCP client broadcasts DHCP Discover message to the network in order to find DHCP server located in the connected network.
2) A DHCP server, that receives the broadcast message, will check its available IP address. An unused address will be selected and responded to the DHCP Offer message for requesting client.
3) The client receives the DHCP Offer message. After that, the client uses it to set an IP address before sending DHCP Request message to be confirmed by accepting the setting parameters.
4) The DHCP server, that receives the DHCP Request message, will return the DHCP Ack message as an acknowledgement to the client.

CoovaChilli

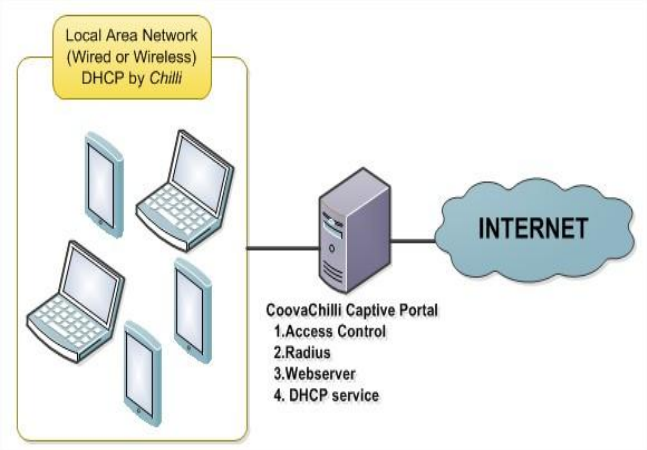

Figure 2: Components of *CoovaChilli* captive portal [8]

CoovaChilli is open source captive portal based on *chillispot*. Figure 2 shows the components of *CoovaChilli* captive portal. The *chilli* daemon will be used as DHCP service for providing an IP address and other network configuration parameters to the client. Before accessing to the internet, the client needs to authenticate itself via webpage using credentials stored in radius server.

DHCP starvation attack

A DHCP starvation attack is considered as a kind of Denial of Services (DOS) attack. *Scapy*, *Gobbler*, and *Yersinia* are well-known tools for attackers to launch DHCP starvation attack. Attackers will send a number of DHCP Discover with a spoofed MAC addresses to a DHCP server in order to decrease the number of address in the pool. Finally, legitimate clients will not be able to obtain the IP address from DHCP service.

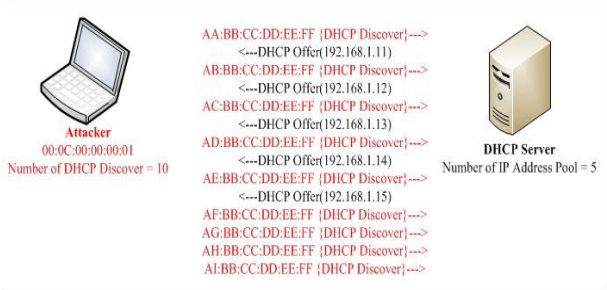

Figure 3: Demonstration of DHCP Starvation attack

Figure 3 demonstrates DHCP starvation attack. The attacker is sending a lot of DHCP Discover messages with a spoofed MAC address to the DHCP server. The server responds to each incoming message with a DHCP Offer until it run out of IP address. As a consequence, the server will not be able to assign IP address to any legitimate incoming request.

ICMP based IP address recovery method for DHCP [6]

ICMP echo service was introduced to identify the IP address which had taken by malicious clients [9]. All of the IP address offered by the DHCP server will be collected. After that, ICMP echo message will be sent to the network host using all offered IP addresses as destination. As ICMP echo service has been implemented in every internet devices [10]. Therefore, the legitimate network host should be able to respond back with ICMP echo reply message while the IP address that had taken by an attacker will never respond.

EXPERIMENTAL SETUP

In this experiment, ICMP based IP address recovery is implementing on the server running *chilli* daemon as DHCP service. The DHCP IP address pool is configuring to accommodate 10 clients. Pool start from 192.168.1.11 – 192.168.1.20. There are 5 legitimate clients (A, B, C, D, and E) and 1 malicious client (F) to perform IP address request. The network tool, *Scapy*, is used by malicious client to launches DHCP starvation attack.

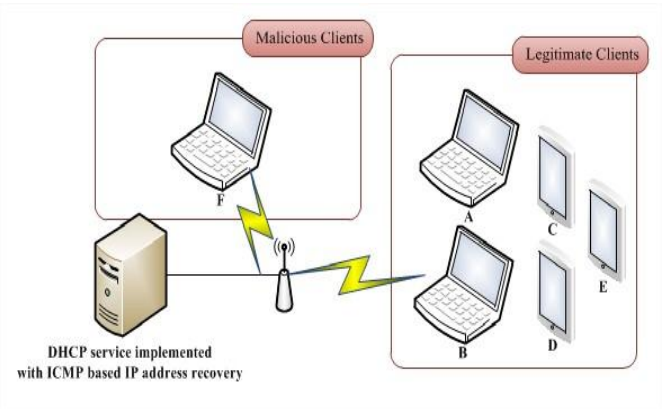

Figure 4: Network diagrams of experimental.

First, all of the legitimate clients request for IP address from the DHCP service. The server then assigns the IP address to these clients. After that, malicious client launch DHCP starvation attack. The information on IP address assign to client is shows in Table 1 as below.

Table 1: The list of IP address assign to clients

IP address	Client	Type of client
192.168.1.11	A	Legitimate
192.168.1.12	B	Legitimate
192.168.1.13	C	Legitimate
192.168.1.14	D	Legitimate
192.168.1.15	E	Legitimate
192.168.1.16	F	Malicious
192.168.1.17	F	Malicious
192.168.1.18	F	Malicious
192.168.1.19	F	Malicious
192.168.1.20	F	Malicious

The performance analysis of the implementation result is will be using four parameters as following:

True positive (TP) represents number of IP address hold by malicious and got recovered

True negative (TN) represents number of IP address hold by legitimate and got recovered

False positive (FP) represents numbers of IP address hold by legitimate client and got assigned

False negative (FN) represents numbers of IP address hold by malicious client and got assigned.

EXPERIMENTAL RESULTS

Table2 shows the result of the IP address recovery on the server running *Chilli* daemon as DHCP service. There were 5 IP addresses (192.168.1.11-192.168.1.15) mark as assigned and 5 IP addresses (192.168.1.16-192.168.1.20) mark as recovered.

Table 2: The IP address status after running ICMP based IP address recovery

IP address	IP address status
192.168.1.11	assigned
192.168.1.12	assigned
192.168.1.13	assigned
192.168.1.14	assigned
192.168.1.15	assigned
192.168.1.16	recovered
192.168.1.17	recovered
192.168.1.18	recovered
192.168.1.19	recovered
192.168.1.20	recovered

After the IP address recovers was launch, there were 5 IP addresses (192.168.1.11-192.168.1.15) still assigned to legitimate client. So the values of TP and FP can be compute as:

$$TP = \frac{5}{5} \times 100 = 100\ \%$$

$$FP = 0$$

There were 5 IP addresses (192.168.1.16-192.168.1.20) recovered. The values of TN and FN can be compute as:

$$TN = \frac{5}{5} \times 100 = 100\ \%$$

$$TP = 0$$

Table3 shows the time spent for recovering IP address from malicious client. The recovery usage time is approximately 1 second.

Table 3: The IP address recovery usage times

IP address	Recovered time
192.168.1.16	1.014s
192.168.1.17	1.010s
192.168.1.18	1.009s
192.168.1.19	1.052s
192.168.1.20	1.060s

CONCLUSION

This paper showed the implementation of ICMP based IP address recover method on *Chilli* daemon DHCP service. The experimental results of an implementation revealed that the DHCP service implemented with ICMP based IP address recover method is able to work with existing DHCP services. Moreover, the DHCP service implemented with ICMP based IP address recover method achieves 100% of True Positive and 0 % of False Positive.

REFERENCES

[1] Lin, C. Su, T. and Wang, Z., 2011, "Summary of high-availability DHCP service solutions," in 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT) , Shenzhen, pp. 1-5.

[2] Senecal, L., 2006, "Understanding and Preventing Attacks at Layer 2 of the OSI Reference Model," in 4th Annual Communication Networks and Services Research Conference, pp.6-8.

[3] 2002, "DHCP servers subject to remote takeover," Network Security, vol. 2002, no. 5, p. 3.

[4] Wilson, P., 2003, "Rogue Servers," Network Security, vol. 2003, no. 8, pp. 16-18.

[5] Duangphasuk, S., Kungpisdan S., and Hankla, S., 2011 "Design and implementation of improved security protocols for DHCP using digital certificates," in 17th IEEE International Conference on Networks (ICON), pp. 287-292.

[6] Yaibuates, M., Upra, R., and Chaisricharoen, R., 2016, "ICMP Based IP Address Recovery Method for DHCP," in Global Wireless Summit 2016 (GWS2016), Aarhus, pp. 267-271.

[7] Droms, R., 1999, "Automated configuration of TCP/IP with DHCP," IEEE Internet Computing, vol. 3, no. 4, pp. 45-53.

[8] "CoovaChilli", http://coova.github.io/CoovaChilli.

[9] Yaibuates, M. and Chaisricharoen, R., 2014, "ICMP Based Malicious Attack Identification Method for DHCP," in 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE) , Chiang Rai, pp. 1-5.

[10] Braden, R., 1989, "Requirements for Internet Hosts -- Communication Layers", RFC 1122, pp. 42.