Abstract—This paper shows a new DNS attack that hijacks DNS requests by frequently injecting fake DNS server, and then network systems communicate with wrong destinations. This type of attack is detectable by neither the IDS nor any anti spoofing software.

Keywords-ARP spoofing; DNS attack; network traffic redirecting; fake DNS server; DNS request

I. INTRODUCTION

The number of people using the internet is increasing for various reasons such as using web based mail servers, internet banking, e-commerce and online social network activities. Users apply LANs to share the internet among themselves using ICS or NAT rather than provide each computer a specific internet connection such as broadband or ADSL. Using LANs to share the internet, there is one default gateway that allows clients to communicate outside of the LAN.

Generally in a LAN, a packet that has different network destination addresses is sent to the default gateway through a switch or an access-point. One type of security weaknesses arises when an attacker knows the host’s network configurations to perform several attacks such as TCP hijacking, ARP spoofing, and eavesdropping.

The other security weaknesses are related to misinterpreting of LAN interconnecting devices such as switches, hubs, and wireless access-points when they are encountering IP and MAC address duplication. Therefore, these devices send the networks packets to both duplicated IP and MAC addresses that one of them might be an attacker. Attackers can either stop the network traffic or redirecting it to perform further attacks such as responding to DNS requests using fake DNS server or redirecting HTTP requests to malicious web servers in order to gain usernames and passwords. So, attackers cannot be detected or prevented by any security mechanisms such as Static ARP [1], AntiSniff programs, ARP spoofing Detection using IDS, and VLAN.

II. IP VISIBILITY

Since computers in a network need to know the destination’s IP address for data transferring, some attacks and threats use the IPs in the network to distribute themselves such as Worms, viruses, and Trojans. Actually, there is no prevention method to stop these attacks because the source of this problem is the way computers in LAN communicate. If a computer does not know the destination IP address, it cannot attack on it and meanwhile it cannot send the real data toward it. The problem is more fatal when the computers are working in a same subnet. In this case an attacker can easily find the victims by IP scanners software and after that they can also find the open ports on victim’s computer by Port Scanners Software to plan an attack [2]. There are more attacks and threats due to following problems in the networks that are because of IP visibility:

TCP Hijacking happens when an attacker simply duplicates the IP and MAC address of the victims by his computer in order to hijack the packets. After that the attacker can communicate to the server like a trusted host in the network. When an IP and MAC address is duplicated in an interconnected device such as switch or Hub, the switch sends the packets to both of its ports and hence the real host and the attacker will receive the packets [3].

Spoofing occurs when attackers exploits to put themselves as a trusted-host in the network in order to gain access to all the resources that a real host has. In this attack, the assailant makes and sends a packet with the trusted host IP source address to the victim and the victim receives the packet and may act upon it [4].

Eavesdropping is done by packet sniffing software in order to obtain the confidential information such as username/passwords and credit card numbers. Although packets that are protected by data transferring methods such as SSL, HTTPS, IP security, and VPN are not understandable by the attackers, the unencrypted packets can be recognized. Some services use the plain text data in order
to communicate with the host like TELNET, FTP, and HTTP [5].

Worms are the viruses that spread themselves using network. A worm usually runs on victim computer as a program or service in order to send the confidential information to a specified destination computer or weaken the victim’s protection system to prepare it for the further attacks. They also can perform the IP/Port scanning attacks to spread themselves through active hosts in a network [6].

MIMT is a form of eavesdropping that an attacker makes private connections with the victims and transmits messages between them, making them think that they are talking directly to each, when in fact the entire conversation is controlled by the attacker [7].

DNS cache poisoning attack is performed when a hacker exploits a bug in the DNS server. If the server does not correctly authenticate DNS responses to guarantee that they are from a reliable source, the server ends up caching the incorrect entries locally and serves them to other users that make the same request [8].

III. SESSION HIJACKING

In order to distinguish logged-in users by the web servers, they send cookies and session IDs through HTTP headers toward user’s browser. Then the browser stores these cookies and whenever users click links on the website, browsers send HTTP requests that contain Cookies and Session ID [9] to the web server in order to recognize the user. Due to this process, if hackers sniff these HTTP requests, they can simply access to the website as an authenticated member rights [10].

The following process leads to session hijacking for accessing the websites by the right of genuine users.

- Hackers capture the Session IDs by sniffing HTTP requests that are being sent by the victim’s browser toward the web server.
- Hackers put the hijacked session IDs in their browser and simply send an HTTP request to web server.

IV. NETWORK TRAFFIC REDIRECTING

ARP spoofing attack causes network traffic to be sent toward both real host and attacker simultaneously. Now, an attacker is able to plan how to treat with the received network traffic. One of these plans might be injecting a fake DNS server, which is used to resolve hostname to IP address, to redirect network traffic. Thus, network host may communicate with wrong destinations. Therefore, the attacker can take advantage of that in order to capture username/password or private information, or direct hosts to a malicious file server in order to update the software or download infected files to plan further attacks.

A. DNS functionality

Network systems usually apply “host name” for communication because names are easier to use rather than IP addresses. Also, host names are usually permanent but the IP address may change periodically. Mapping host names to IP addresses is done by Domain Name Systems. DNS function typically includes the following steps:

1) An application on a host, requests an IP address for a website or another host name to communicate.
2) A process in host computer prepares a DNS query and sends it to a specific DNS server.
3) DNS server checks to see if the requested website name is in its cache. And, if so, returns the IP address to the requestor. Otherwise, it sends an error message [11].

DNS servers, due to their important roles, are one of the unsafe points in networks because the computers use them to translate their name to IP requests and consequently to communicate.

B. ARP Spoofing

Ethernet networks use Address Resolution Protocol for determining a network host. All the Network devices such as computers, switches and routers use this protocol to identify hosts in the network. Through this protocol, these devices are able to send the data to the correct recipients.

There is security vulnerability in networks that make use of ARP and no other methods of address resolution because of the existence of ARP Spoofing attack that cause the network traffic to be modified or to be stopped.

The ARP Spoofing function typically include following steps:

- A hacker finds the Router on any specific server’s IP and MAC address
- The IP and MAC address of hacker’s computer is changed based on above step
- The hacker keeps sending echo requests to any host in the network to deceiving the switch or access-point. Consequently, they send the packets to both hosts mistakenly (hacker’s computer and real host).
- Now that the hacker’s computer receives the packets, they can plan the attack either by redirecting or modifying them.
- This vulnerability arises from two reasons:
  - The lack of security mechanism to check the identity of the hosts in the network
  - Host’s ARP table is changing instantly based on the received ARP reply [10].

C. DNS Requests Redirecting

Duplicating the attacker’s computer MAC and IP address by a default gateway in a LAN and keep sending packets to the any clients connected to the network leads the switch or wireless access-point sends some of the packets to the attacker’s computer mistakenly as illustrated in Figure 1. Through this process, an attacker can inject their DNS server and response to DNS requests in the network. As a result, incorrect IP address might be given to the host. Moreover, assailants might want to gain critical information like username and password for the specific web site by copying and changing a real login page and putting it inside a fake web server.

Getting access to the websites, the browser sends a DNS request to DNS server DNS server responses the request by sending an appropriate IP address to the client. Again, the browser makes a HTTP request and sends it to the IP address.
DNS server is located either inside the LAN or outside the LAN using Public IP address.

If DNS server is located outside the LAN using Public IP address, an attacker needs ‘iptables’ services running on Linux operating system for performing DNS request redirecting. So, attacker should find the IP and MAC address of the network’s gateway, and then duplicate their computer IP and MAC address with the gateway. Due to keep sending echo request to any hosts in the LAN based on regular time, attacker deceives the switch and consequently, it sends whole the network packets directed to the real gateway toward both attacker and gateway. Finally, Attacker may use DNAT to redirect the packets especially ones are DNS requests.

If DNS server is located inside the LAN either combined with the default gateway or is on an isolated computer, as illustrated in Figure 2, the attacker should duplicate the IP and MAC address of the DNS server with its computer and then sends echo requests to one of the hosts in the network. This causes that switch sends the network packets toward both attacker and gateway. Now attacker is able to inject a fake DNS server to reply the wrong IPs to the DNS requests.

DNS redirecting in former state is easier than latter because there is no need to use ‘iptables’ service in order to redirect the DNS request to a fake DNS server. Unfortunately most of the small LANs use this position to reply to DNS requests.

As a result, clients will receive incorrect IP and consequently they will communicate with wrong destinations. These destinations might be fake web servers to gain username/password or private information of theirs members; websites contain malicious content such as worms and viruses; fake update server for the software and operating system, and sometime it threatens the network availability.

D. Result & Experiment

Practically, we redirected the DNS requests toward a specific website to a fake DNS server by following procedure:

1) Finding the IP and MAC addresses of the default gateway of the LAN
2) Changing the IP and MAC addresses of attacker’s computer to the found IP and MAC address
3) Executing following ping loop to deceive the switch (in Linux):

```python
while true do;
ping 127.0.0.1 –c 4;
ping 192.168.1.1 –c 1;
done;
```

The first line, makes a loop to perform an active attack because it needs to be done whole the process of redirecting packets. In second line, ‘c 4’ means sending 4 echo requests to 127.0.0.1 IP address. This leads a few seconds interruption. Upon this command, user would encouter traffic problem, thus this command lets the LAN go back to the normal condition [10]. Actually, the length of interruption time depends on the brand of the switch. Third line sends one echo request to the Default Gateway of the network. By doing this command, switch will be deceived and it sends the network traffic toward both attacker and original gateway. And the last line is for ending the loop.

4) Redirecting the DNS requests toward a specific website to a fake DNS server. In Linux the command might as follow:

```bash
```

In this command line, ‘X.X.X.X’ is a fake DNS server IP address that in the following figure is 192.168.1.X.

5) Preparing a fake DNS server contains “websitename.com” domain with “www” as an ‘A’ record.

The ‘A’ record should resolve fake web server IP address (192.168.1.X).

6) Making a copy of the web site and publishing it on the fake web server.

7) Editing the content of the webpage in order to get the personal information inserted by the victims. This editing contains changing the submit process by putting Ajax code to send a copy of personal information to the attacker as well as the real website.

V. CONCLUSION

Attackers can inject a fake DNS server to redirect the network traffic to wrong destinations. By duplicating the IP and MAC address and keep sending ping request to the switch by the attacker, switch will be confused and consequently, it sends the data to both ports that are connected to the attacker’s system and real host. This kind of attack is not detectable by the IDS or any anti spoofing software. Moreover, the succession percentage of this method depends on the interruption time and the switch functionality.

ACKNOWLEDGMENT

This research is supported by the Ministry of Science & Technology and Innovation (MOSTI), Malaysia and Universiti Teknologi Malaysia (UTM).

REFERENCES


Figure 1. Capturing Network Packets by the Hacker.
Figure 2. Redirecting and Responding to DNS requests by the Attacker.