Faculté des Nouvelles Technologies de l'Information et la Communication

Département de l'informatique et Technologies de l'information

Travail présenté par: Cherbi Borhane ddine & Mezouar Beggari Mh.said.
Encadré par: Khaldi Amine

realization an application to detect and prevent MITM attacks based on linux system

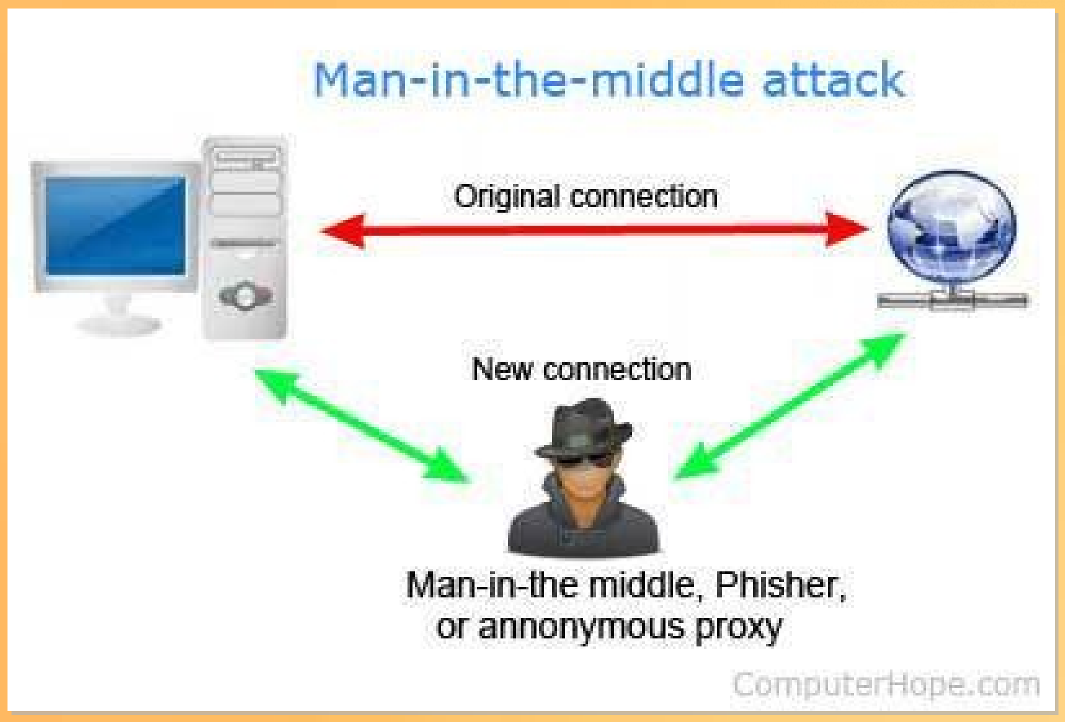
Resume

Security Information has become a very important and indispensable element in people's lives and companies in their work,Providing protection from various threats.

Among these known threats is a type of attack called man in the middle attack of the most dangerous attacks.

used by hackers in inside networks Allows an attacker to spy on traffic, steal sensitive information, and control communications inside the local network.

The goal of our project is to achieve an application that enables us to protect against these attacks so that the source of the attack is detect, block and cancel the attack.



Introduction

local networks are essential in our daily lives where are Used in homes and cafes airports to access the Internet or in companies in the performance of tasks and processes.

In our work we will secure communications between users and the services they use in networks or the Internet.

Our work will consist of three theoretical chapters and a practical chapter.The first chapter presents the basics of information security and the identification of methods and methods of data protection in addition to some offensive techniques and famous vulnerability.

Then we will discuss in the second chapter the concepts of wired and wireless networks and identify the structure of network protocols ARP DNS DHCP HTTP and how to work in the reception and transmission of data.

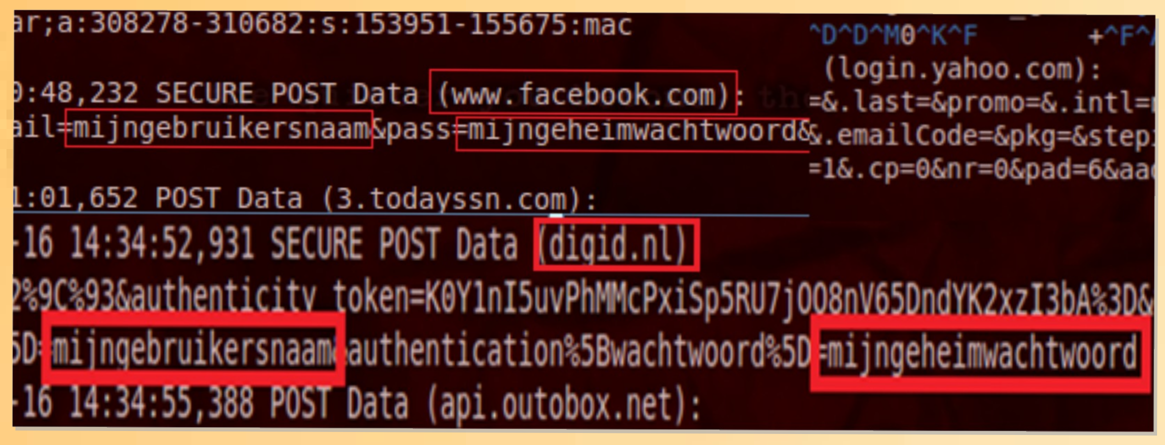
In the third chapter we will talk about the vulnerability of the (ARP,DHCP,DNS) protocols and how they occur, which causes dangerous attacks such ARP Poisoning and DNS Spoofing,DHCP Spoofing. We will simulate attackers by exploiting this vulnerability using some tools such as Ettercap,arpspoof,mitmf

In the last chapter, we will provide our approach in order to enforce the protection of communications in the local network by applying mechanisms to detect and prevent MITM attacks.

Materiel and Method

Programming language and libraries: In our project we will use Python and scapy library on pycharm IDE.

- Create an algorithm that captures up ARP packets and displays our malware packets and blocks them
- Create an algorithm that captures DNS packets and displays our malware packets and blocks them
- Create an algorithm that captures DHCP packets and presents us with malicious packets and prevents them from detecting a malicious DHCP server.
- Capture data packets that are trying to scan devices in the network.



```
ar;a:308278-310682:s:153951-155675:mac                    ^D^D^M0^K^F      +^F^
                                                           (login.yahoo.com):
0:48,232 SECURE POST Data (www.facebook.com):             =&.last=&promo=&.intl=
ail=mijngebruikersnaam&pass=mijngeheimwachtwoord&         &.emailCode=&pkg=&step
                                                          =1&.cp=0&nr=0&pad=6&aa
1:01,652 POST Data (3.todayssn.com):
-16 14:34:52,931 SECURE POST Data (digid.nl)
2%9C%93&authenticity_token=K0Y1nI5uvPhMMcPxiSp5RU7jO08nV65DndYK2xzI3bA%3D&
5D=mijngebruikersnaam&authentication%5Bwachtwoord%5D=mijngeheimwachtwoord
-16 14:34:55,388 POST Data (api.outobox.net):
```

Result

These are the results we will obtain as follows:

- Detection of ARP packets is poisoned by source(attecker IP) and destination(victim IP).
- Block the attacker from ARP tables.
- The detection of DNS packets is also poisoned by source(attecker IP) and destination(victim IP).
- Block these packets.
- The alarm after a DHCP attack is spoofing and then stopped.
- Detection of the scanning the network.

Conclusion

this simple program will be of great benefit to users, especially network administrators, which will increase the protection of confidential information for users(credit cards username,password), privacy and protection against attacks.

users can also use public and private networks freely and securely.

Bibliography

1-https://www.veracode.com/security/man-middle-attack
2-https://www.blackhat.com/presentations/bh.../bh-europe-03-valleri.pdf
3-DETECTION OF MAN-IN-THE-MIDDLE ATTACK IN IEEE 802.11 NETWORKS
Kwame Nkrumah University Of Science And Technology