**Ethical Hacking Assignment 4**

**Man-in-the-Middle**

Perform a MitM attack by using ARP poising and capture images, Urls and web content using Driftnet and SSLStrip to remove security from an https site. **Tools:** Etttercap, arpspoof, driftnet and SSLStrip

1. Using Ettercap and driftnet perform a man-in-the-middle attack where the hacker can see all of the images assessed by the victim.

To perform the Mitm attack, using ettercap to view all of the images going between the XP machine and the proxy server that takes you out of the virtual environment to the internet.

Start ettercap (in Kali)

* Select the self-sniff and enter the interface eth0
* Then select Host and the “scan for host”
* Select Host and “host list”
* Set Target 1 to the gateway (10.106.130.5)
* Set Target 2 to your XP machine
* Select Targets and the “current targets” to verify attack
* Select Mitm and then “ARP poisoning”
* Select Start and “Start Sniff”

Open a new terminal and enter driftnet –i eth0 and group the new window

Once this is setup, access the internet and open a page that has images.

What do you see at the driftnet window?

I am using the XP machine provided and the kali machine provided. They did not have any internet access. I did open internet explorer to see what I could get. Due to this all I see in the driftnet window are the images of internet explorer and little images on the window.

Explain what is happening?

I am sniffing my XP machine to see all the web activity that I’m currently doing while driftnet sees the images.

Would this be picked up using an intrusion detection system? and Why?

This can be picked up by intrusion detection because we are using ARP poising.

Can driftnet capture and show other forms of data? Hint: use the help capability.

Driftnet can obtain images and TCP streams being sent.

Explain the difference between ARP and DNS poisoning, what are iptables?

ARP poisoning is when an attacker sends out fake ARP messages over a network to link the attacker’s mac address to an IP of an actual computer or server.

DNS poisoning is when an attacker exploits system vulnerability to divert traffic away from real servers onto fake ones.

IP tables are lists of IPs for the computers and devices connected to a network, assigned by the DNS.

Explain the different between ettercap and driftnet as it relates on how it manages the information it captures?

Driftnet watches network traffic and displays images on screen by getting TCP packets from the network.

Ettercap does man in the middle attacks and filters the information obtained on IP source and destination. It can intercept traffic on a network and uses ARP poisoning.

**Given the program below:**

#include <stdio.h>

#include <string.h>

void foo(int a, int b, int c)

{

int tmp;

a=2;

tmp = b+c\*a;

}

int main(int argc, char \* argv[])

{

int pass = 0;

char buff[15];

foo(3,4,5);

    printf("\n Enter the password : \n");

    gets(buff);

    if(strcmp(buff, "testpilot"))

    {

        printf ("\n Wrong Password \n");

    }

    else

    {

        printf ("\n Correct Password \n");

        pass = 1;

    }

    if(pass)

    {

       /\* Now Give root or admin rights to user\*/

        printf ("\n Root privileges given to the user \n");

    }

    return 0;

}

Assume the program is in a file called: test.c

It is compiled and linked using gcc test.c –a test

and is executed as ./test

Show the activation records up to where the arrow indicates:

Parameter 🡪 right-to-left local variables 🡪 top-to-bottom word size is 32 bits

|  |
| --- |
| Tmp=27 |
| C=5 |
| B=4 |
| A=3 |
| A=2 |
| tmp |
| Return tmp to main |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| buff |
| Pass = 0 |
| Return address to OS |
| 1 |
| ./test |

Show what input, other than **testpilot** will give root privileges.

Anything larger than 17 characters to cause a buffer overflow.

So XXXXXXXXXXXXXXXXX.

What are DEP and ASLR?

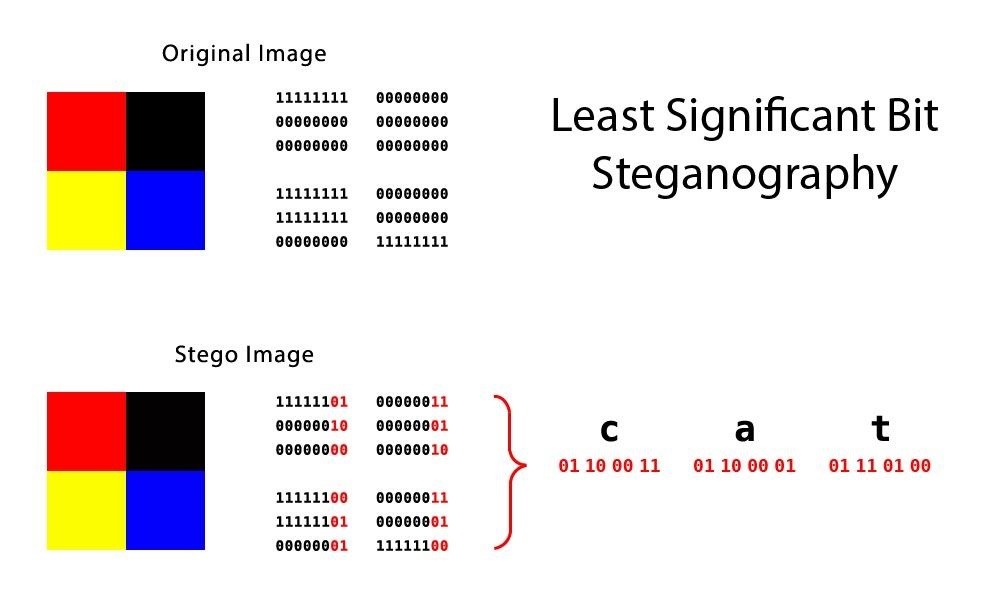
DEP stands for Data execution Prevention and ASLR stands for Address Space layout Randomization. ASLR is used to prevent shellcode from being successful and DEP prevents memory sectors from being executed.

How do these techniques prevent attacks on the system?

ASLR randomly offsets the location of modules and in memory structures which prevents the shellcode from running successfully and prevents buffer overflow attack.

DEP can prevent the attacker from being able to leverage code that is already executable or make the attacker's data become executable. It prevents the execution of a code in the heap or stack in the case of buffer overflow.

Given the following original and stego images



Determine

The maximum percentage of changed bits: 15.625%

The actual number of changed bits: 15

Using the original image, but now using single bit (lsb) and only hiding the letter c,

The maximum percentage of changed bits: 4.6875%

The actual number of changed bits: 3