**AIM: To Study DOS,ARP Spoofing and Buffer Overflow attack.**

**THEORY:**

**Software Requirements:**

UBUNTU: For doing the attacks , Hping3: For DOS Attack, Splint: For Buffer Overflow Attack, Cppcheck: For Buffer Overflow Attack, Arpwatch: For ARP Spoofing Attack, Wireshark: To monitor packets

**1.What is DOS attack?**

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means that during the attack period, regular traffic on the website will be either slowed down or completely interrupted. A Distributed Denial of Service (DDoS) attack is a DoS attack that comes from more than one source at the same time. A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets”

hping is a free packet generator and analyzer for the TCP/IP protocol. It is one of the de facto tools for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique (also invented by the hping author), and now implemented in the Nmap Security Scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time.

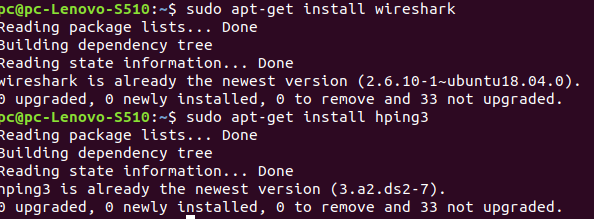
****

Figure 1:Installing tools.

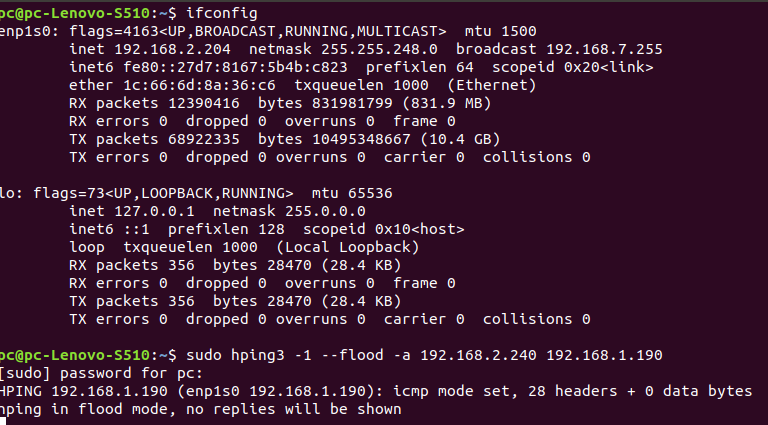
****

Figure 2:Ip configuration

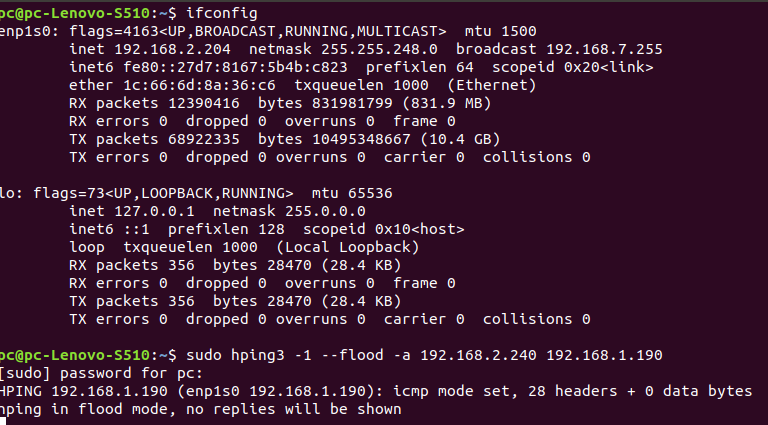
****

Figure 3:Flooding the victim pc

**F:\SEM VI\CSS\exp6\dos2.png**

Figure 4:Flooding the victim pc with different command of hping3

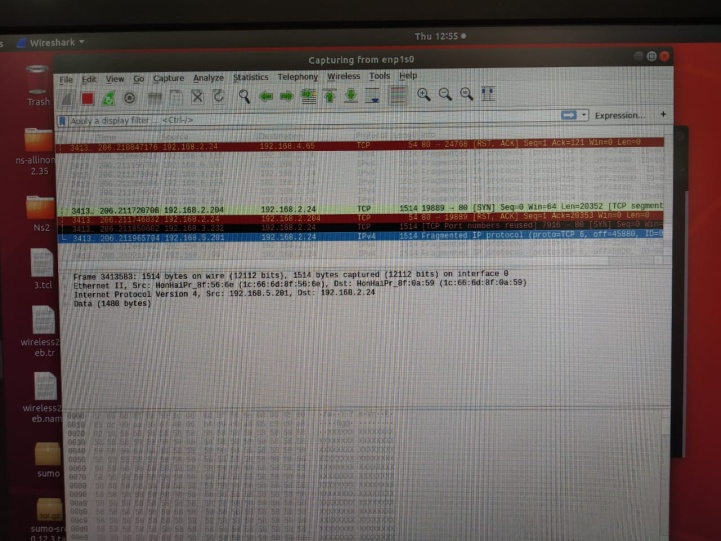
****

Figure 5:Wireshark monitoring in victim pc

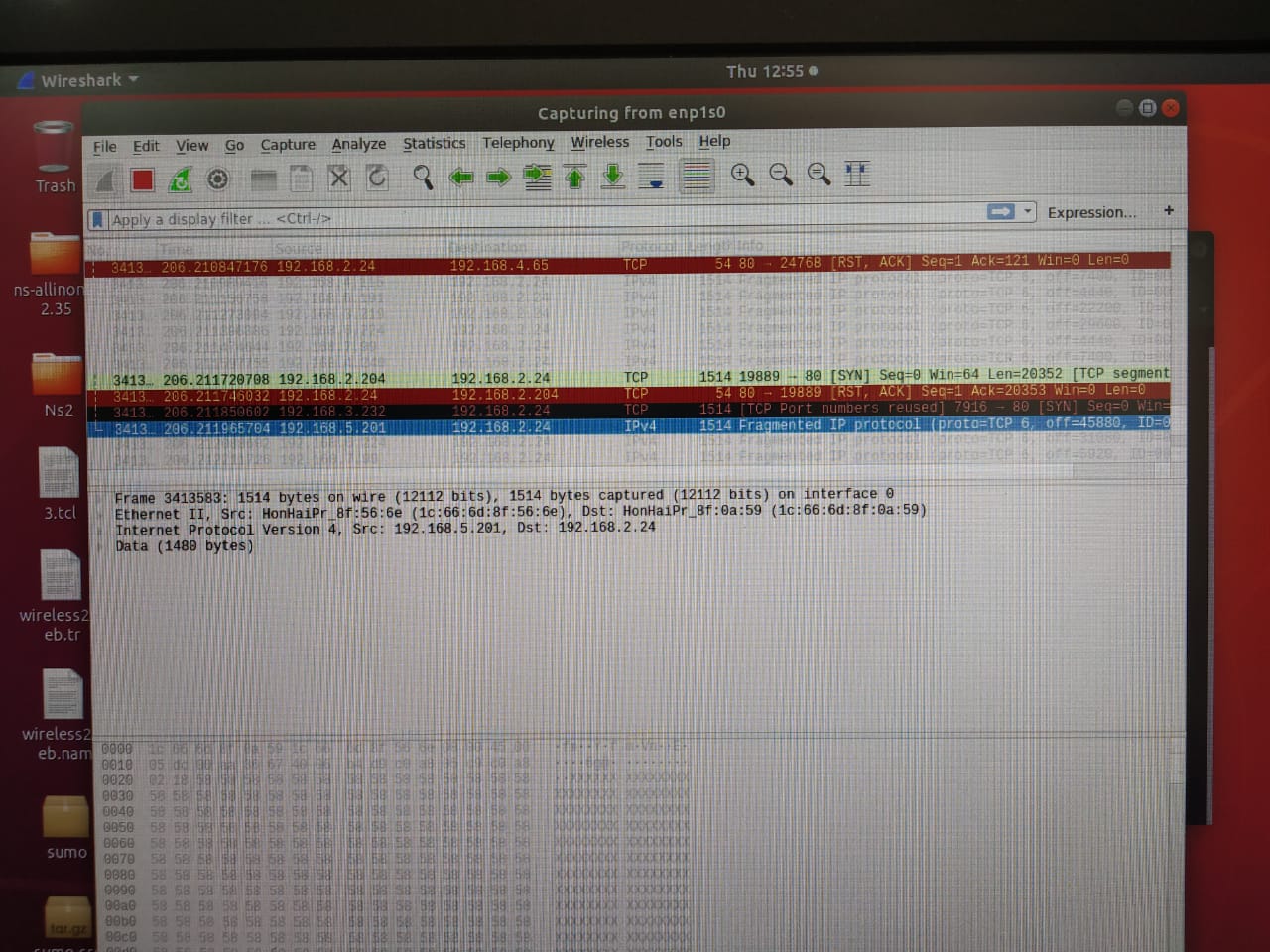
****

Figure 6:Wireshark monitoring in victim pc

****

Figure 7:Wireshark monitoring in sender pc

**2.What is Buffer Overflow Attack?**

In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information.

Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user’s input. There are two types of buffer overflows: stack-based and heap-based. Heap-based, which are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program. Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack: memory space used to store user input.

Cppcheck is a static code analysis tool for the C and C++ programming languages. It is a versatile tool that can check non-standard code

Splint, short for Secure Programming Lint, is a programming tool for statically checking C programs for security vulnerabilities and coding mistakes. Formerly called LCLint, it is a modern version of the Unix lint tool.

Splint has the ability to interpret special annotations to the source code, which gives it stronger checking than is possible just by looking at the source alone. Splint is used by gpsd as part of an effort to design for zero defects.

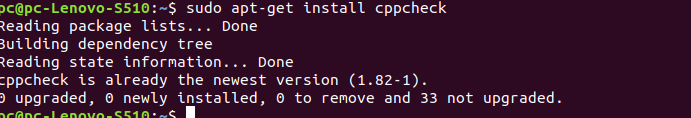
****

Figure 7:Installing Cppcheck

Code:

#include<stdio.h>

void main(){

int a[5];

for(i=0;i<5;i++)

scanf("%d",&a[5]);

scanf("%d",&a[7]);

}

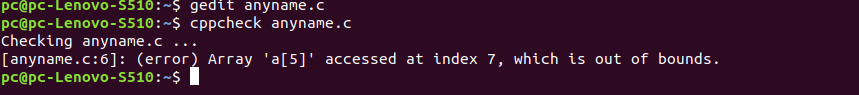
****

Figure 7:Bufferoverflow Error

Code:

#include <stdio.h>

#include <string.h>

int main(void)

{

char buff[15];

int pass = 0;

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

gets(buff);

if(strcmp(buff, "thegeekstuff"))

{

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;

}

Output:

**pc-9@pc9-Lenovo-S510:~$ sudo apt-get install splint**

[sudo] password for pc-9:

Reading package lists... Done

Building dependency tree

Reading state information... Done

splint is already the newest version (1:3.1.2+dfsg-1build1).

0 upgraded, 0 newly installed, 0 to remove and 35 not upgraded.

**pc-9@pc9-Lenovo-S510:~$ gedit exp7.c**

^Z

[1]+ Stopped gedit exp7.c

**pc-9@pc9-Lenovo-S510:~$ splint exp7.c**

Splint 3.1.2 --- 20 Feb 2018

exp7.c: (in function main)

exp7.c:8:1: Use of gets leads to a buffer overflow vulnerability. Use fgets

instead: gets

Use of function that may lead to buffer overflow. (Use -bufferoverflowhigh to

inhibit warning)

exp7.c:8:1: Return value (type char \*) ignored: gets(buff)

Result returned by function call is not used. If this is intended, can cast

result to (void) to eliminate message. (Use -retvalother to inhibit warning)

exp7.c:9:4: Test expression for if not boolean, type int:

strcmp(buff, "thegeekstuff")

Test expression type is not boolean or int. (Use -predboolint to inhibit

warning)

exp7.c:18:4: Test expression for if not boolean, type int: pass

Finished checking --- 4 code warnings

**3.What is ARP Spoofing Attack?**

In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks. The attack can only be used on networks that use ARP, and requires attacker have direct access to the local network segment to be attacked.

arpwatch is a computer software tool for monitoring Address Resolution Protocol traffic on a computer network. It generates a log of observed pairing of IP addresses with MAC addresses along with a timestamp when the pairing appeared on the network. It also has the option of sending an email to an administrator when a pairing changes or is added.

Network administrators monitor ARP activity to detect ARP spoofing, network flip-flops, changed and new stations and address reuse.

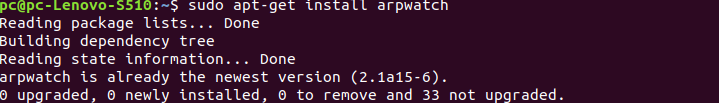
****

Figure 8:Installing ARPwatch

**F:\SEM VI\CSS\exp6\Screenshot from 2020-03-12 11-43-22.png**

Figure 9:Starting ARPwatch Service

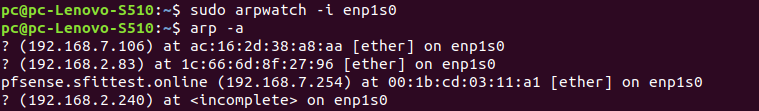
****

Figure 10:Watching Ip and MAC addresses connected to IP of sender

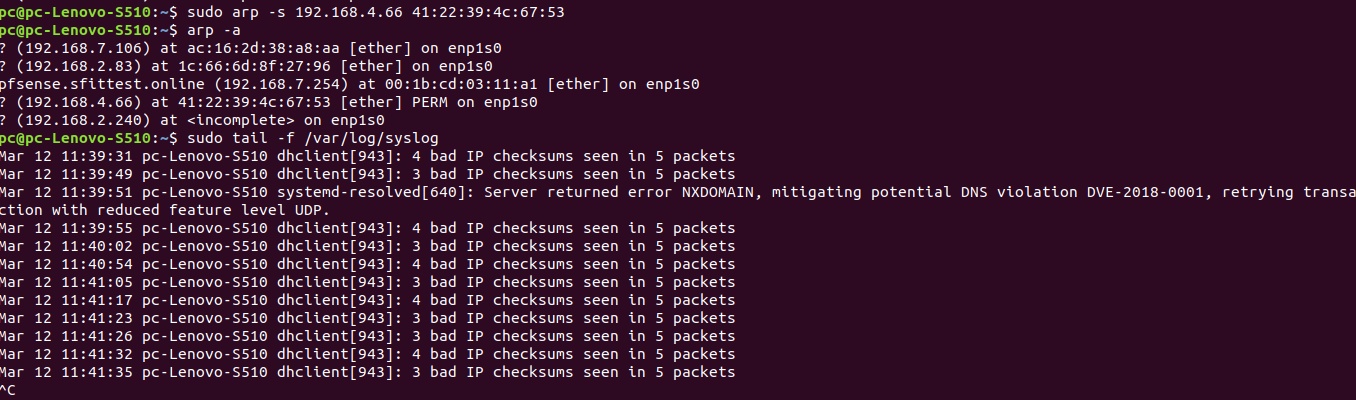
****

Figure 11

**CONCLUSION:**

This experiment taught us three different attacks viz. DOS attack, Buffer Overflow attack and ARP spoofing attack. For each attack we need to install certain tools using sudo apt-get install command of UBUNTU. We used hping3 for DOS attack, cppcheck and splint for buffer overflow attack and arpwatch for ARP Spoofing.Using DOS attack we flooded packets to victim which hanged that pc.Using Buffer overflow tools we saw how tools tell us about overflow error.