

ClubHACKMag

1st Indian "HACKING" Magazine

Issue 26 | Mar 2012

www.clubhack.com



**If a Computer Network was a game of chess,
isn't this how your server would look like?**

TechGyan Network Security | LegalGyan Sending offensive or false messages |

ToolGyan Who wants to be a Millionaire | Mom's Guide Protect your privacy online with 'TOR' |

Hello Readers. Hope you enjoyed the colorful festival of holi. It is our pleasure to tell you that we are adding a strong member to CHmag Team - K.V.Prashant. Prashant, working with Infosys, has spoken at various security conferences like ClubHack, nullcon, SecurityByte, c0c0n and a recipient of Mentor of the Year award at c0c0n.



Pankit Thakkar

Coming to this issue we have Network Security in Tool Gyan which will put light on how to set up a secured network, Who wants to be aMillionaire in Tool Gyan, check out yourself of what exactly its all about ;)TOR in Mom's guide for all those who thought 'It sounds very complicated to use, I'm not a hacker! I can't use it!' by our Author- Federico from Italy. I promised last time, a coverage on a game, here is an interesting coverage. Thanks to photographer Madhav Goel for an amazing click.

And as always I would end by saying keep your articles, suggestions , criticism if any :P flowing to info@chmag.in

Issue 26, March 2012.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

K.V.Prashant
good.best.guy@gmail.com

Sagar Nangare
sagar@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Pg **TechGyan**
03 Network Security

Pg **ToolGyan**
08 Who wants to be a Millionaire

Pg **Mom'sGuide**
11 Protect your privacy online with 'TOR'

Pg **LegalGyan**
16 Section 66A - Sending offensive or false messages

Pg **MatriuxVibhag**
19 EtherApe – Graphical Network Monitoring



Network Security

Introduction

Computer Networks are the back bone of all organizations which rely on Information Technology (IT) and are the primary entry point for users to access the Information resources of an organization. Networks today are no longer limited within the physical location of an organization, but are required to be accessible from anywhere in the world which makes it vulnerable to several threats.

In a recent survey conducted by the Computer Security Institute (CSI), 70 percent of the organizations polled stated that their network security defenses had been breached and that 60 percent of the incidents came from within the organizations themselves. Organizations have realized that having a secure network infrastructure is critical to safeguard their IT assets.

Network design can vary from one organization to the other but, it is recommended to use the layered design approach – core layer, aggregation modules and the access layer. These layers comprise of hardware necessary to control access between internal and external resources.

Though we will not deal with the layers in depth, the basic building blocks of a network are the router which is part of the core layer, firewall and switch which are part of the access layer. Along with these we have supporting aggregation modules such as IDS/IPS, antivirus, etc. Before we begin on network design and security, let's understand the basic network components:

Router

In simple words, router is a network device which connects two different networks. Perimeter router or the Edge router is placed in the outermost layer of the network and forms a part of the core layer of the network architecture and serves as the very first line of defense. It is responsible for forwarding IP packets to the networks to which it is connected. These packets can be inbound requests from Internet clients to Web server, request responses, or outgoing requests from internal network. The router can also be configured to block unauthorized or undesired traffic between networks. The router itself must also be secured against reconfiguration by using secure administration interfaces and ensuring that it has the latest software patches and updates applied.

Firewall

A firewall is often imagined as a wall of defense in a building which prevents spreading of fire from one part of the building to another. In a network world a firewall is a device primarily used to protect the boundary of an organization's internal network while it is connected to other networks. The role of the firewall is to block all unnecessary ports and to allow traffic only from known ports such as port 80 for all HTTP traffic, port 25 for SMTP traffic and in some cases known network segments.

Unfortunately the hackers have become so smart these days that they manage to get through the firewall through the permitted ports and try to compromise the IT assets of an organization. Thus firewall cannot evaluate the contents of "legitimate" packets and can unknowingly pass through some attacks to the inside network.

Hence these days most organizations deploy Intrusion Detection System (IDS) which have the capability to monitor network traffic and logs any unauthorized access attempts and suspicious network patterns and report them to network administrators at the earliest. But again, there is a problem if the administrators are not able to take immediate action, though the attack is detected it is not stopped.

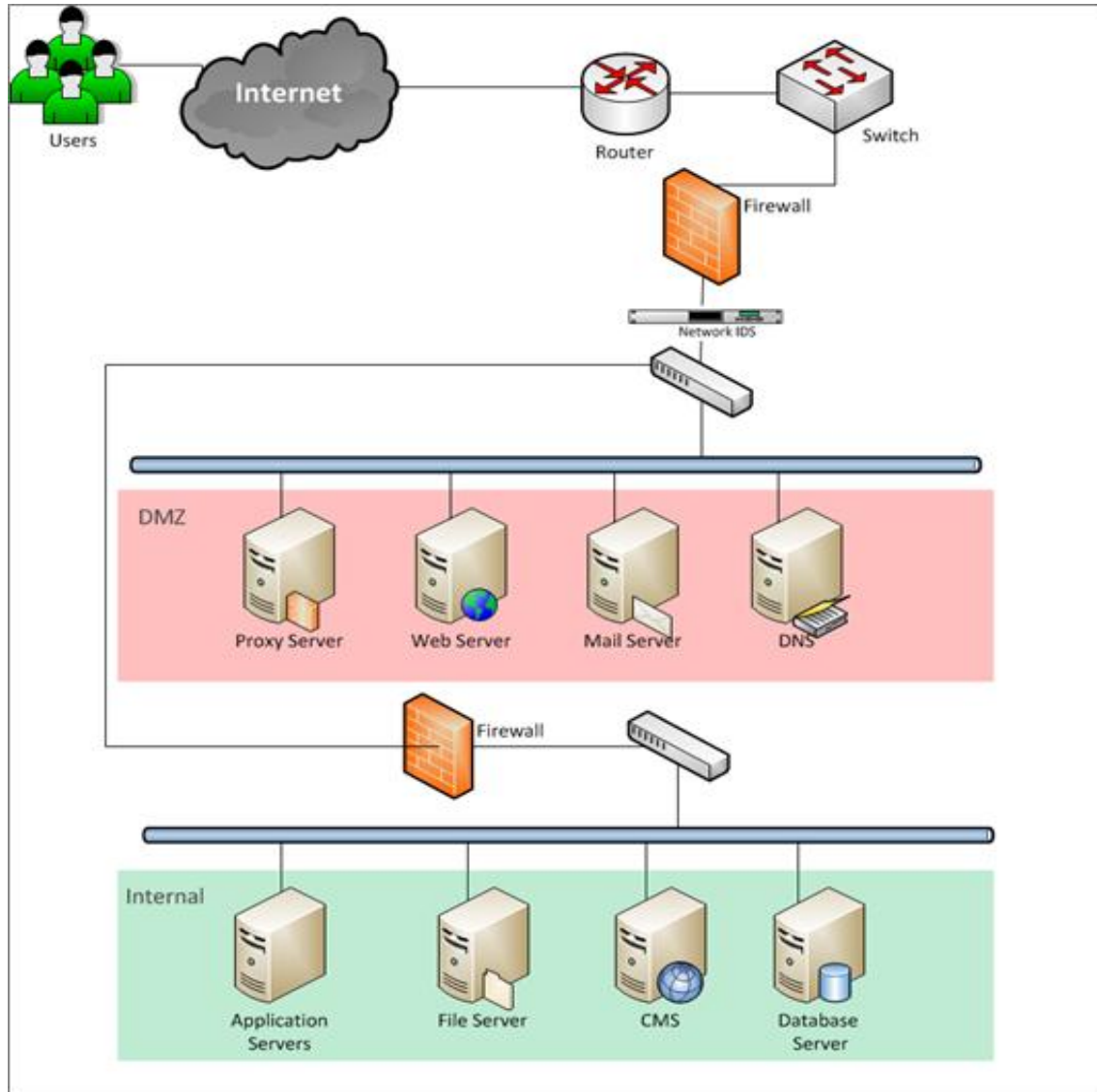
To prevent such malicious activities, Intrusion Prevention Systems (IPS) were introduced in the network architecture. When any such malicious activity is detected an IPS can block such traffic and notify the administrators. Coupled with IPS/IDS, the firewall is a useful tool for preventing attacks and detecting intrusion

attempts, or in worst-case scenarios, the source of an attack.

Switch

A network switch is a device which enables networked devices to talk to each other efficiently. The main purpose of using a switch in a network is to segment the network into logical pieces. The network devices which are part of the network segment are connected to the switch and any communication to these devices happens through the network switch. Some amount of security is built into the switch to prevent packet sniffing by intruders between networks. A switch can forward packets to a specific host or a network segment, rather than sharing the data with the entire network

The second most important factor in the network design is the network segmentation. Having a flat network allows an intruder to gain easy access to organizations critical assets. Network is segmented logically with the help of network devices such as routers and switch and access between these zones is controlled by a firewall.



Let's understand the network design aspects with the help of the above diagram. Though this is not a full-fledged network diagram of a typical organization network, it does provide the basic understanding of network architecture with more focus on the perimeter security. As depicted above perimeter router is the outermost network device exposed to the external world with a public interface, followed by an optional network switch or directly connected to a firewall interface which allows traffic only on specific ports. An IDS/IPS device is connected in line with the network firewall

for detecting and preventing network intrusions. Further a switch is used to segment the network into different logical segments.

In most organizations we see their data center network segmented into the DMZ and Internal zone. DMZs are used to separate Internet facing devices such as Web servers, Mail Gateway, Domain Name Servers Proxy server. DMZ allows inbound or outbound traffic to be initiated to or from the internal network without revealing the actual details of the internal network. This

adds an additional layer of security and provides a certain extent this assumption holds good, if network paths are configured properly. There should not be a direct path to internal network should one of the devices in the DMZ be compromised.

Internal zone mainly comprises of infrastructure required to support business applications. There can be more logical separations in the internal network based on customer needs such as a separate DB segment which is also a mandate by few regulations.

Having understood the network components and the basic layout of a network let's focus on the need for security.

An intruder usually looks for poorly configured network devices to exploit. Some of the most common network vulnerabilities which intruders exploit are default installation settings, open access controls, unpatched devices and easy access to network devices. Some of the most common Network threats are:

- Information gathering – information about network design, system configuration, and network devices is gathered and an attack is planned later.
- Packet Sniffing – Intruder monitors data packets using network sniffers to read all clear text information and may steal some confidential information in clear text.
- Spoofing – where the original source of attack is spoofed to appear as a trusted source and can cause a denial of service attacks.
- Session hijacking - also known as man in the middle attacks in which an intruder uses an application that

appears the genuine client or the server. This results in either the server or the client being tricked into thinking that the upstream host is the legitimate and share confidential information.

- Denial of service – is the act of denying legitimate users access to required resources. Attackers deny service by flooding the network with traffic and throttle the available bandwidth and resources.

As attacks are evolving and becoming more mature, the security solutions to prevent them are also evolving. As you might have seen so far, organizations use collection of layered security devices such as firewalls, intrusion detection systems, antivirus, etc. But managing all these devices individually is a complex process. This led to the evolution of Unified Threat Management Solutions (UTM). UTM systems are bundled with many security features and capabilities such as intrusion detection and prevention, Anti-Virus solution, e-mail spam filtering and Web content filtering, functions of a firewall, integrated into a single appliance.

Though UTM is still in its evolution stage, it has managed to be of much use to smaller organizations and still a long way to be of much use to larger organizations. UTM device face the challenge of performance with a significant consumption of bandwidth as they analyze more and more data. But security experts believe that UTM is here to stay and hope to see a more mature UTM in future.

Network design is an evolving process, organizations must never sit back and relax once the initial network setup is complete. Networks must be monitored continuously and improve security from time to time. Security can mean different to different organizations and must take appropriate measures to secure themselves. Just remember we are never alone in this world, we always have company.



Pradeep A. R.

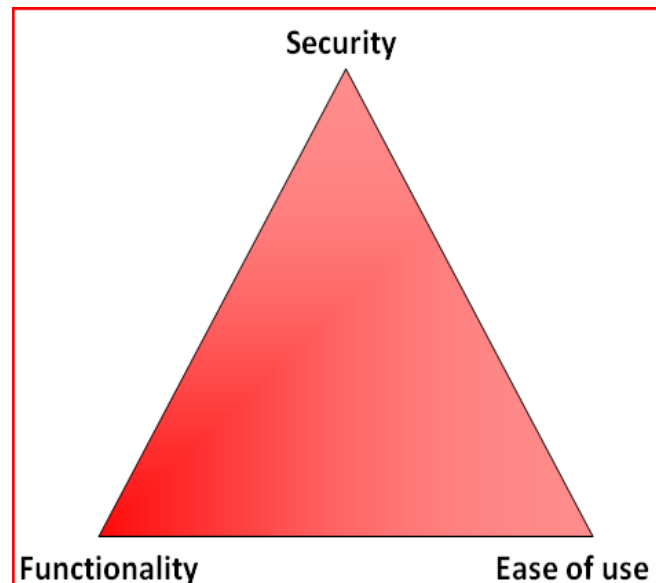
Pradeep_ar@infosys.com

Pradeep works as an Infrastructure Security consultant with Enterprise Security and Risk management –Cloud practice, Infosys Ltd. Pradeep is currently working on Security Information and Event Management & Data loss prevention solutions. As a security enthusiast, Pradeep intends to become a cyber-forensic professional.



Who wants to be a Millionaire

Everyone wants to be Millionaire and this article is just going to tell you how you can become one. The Web 2.0 has opened lots of opportunities and possibilities along with lots of security issues. One of the popular technology is “Flash” along with its never ending security issues. People laugh when they hear the terms “Flash” and “Security” together. Industry experts say that Flash is actually moving the ball towards ease of use and functionality and thus compromises on security.



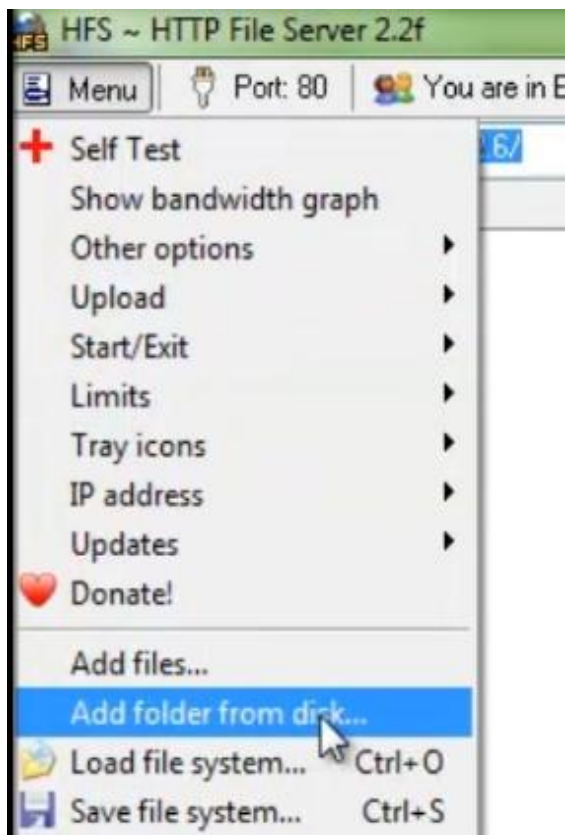
Here we are actually trying to show you the security issues related with Flash applications and how you can test or exploit them for fun and profit.

Let's get our lab ready, all that you needed are:

1. OWASP Mantra Security Framework
- <http://www.getmantra.com/>
2. Who wants to be a Millionaire flash game -
<http://sourceforge.net/projects/vulfa>
3. HTTP File Server -
<http://www.rejetto.com/hfs/>

Now call up your bank and make all the arrangements in advance to transfer this huge amount, don't blame us at the end for not informing you ;)

Step 1:



Extract the contents from the archives. We want a HTTP server to properly run the game. HFS will serve this purpose, just run

it and point it to the folder where we have extracted Who Wants to Be a Millionaire.zip.

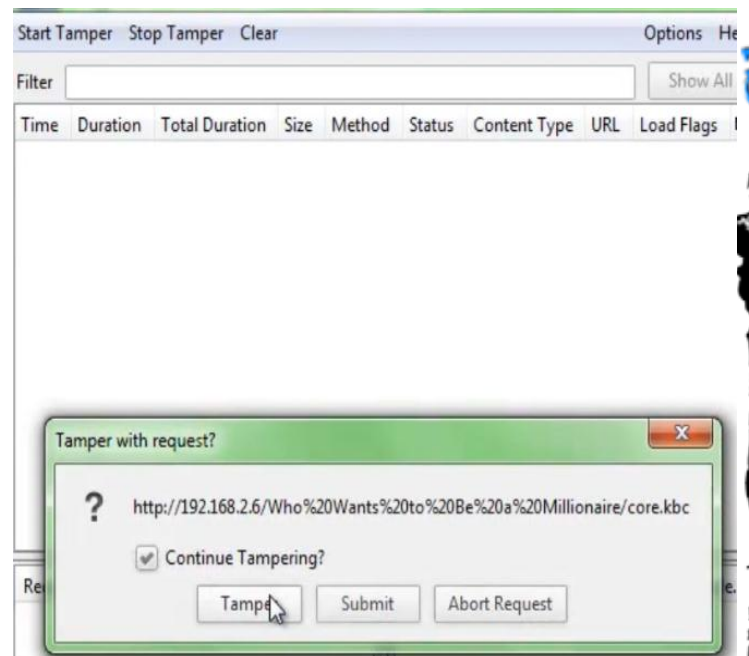
Just below the menu button you can see your HTTP server IP address and URL. Paste it onto Mantra address bar.

Step 2:

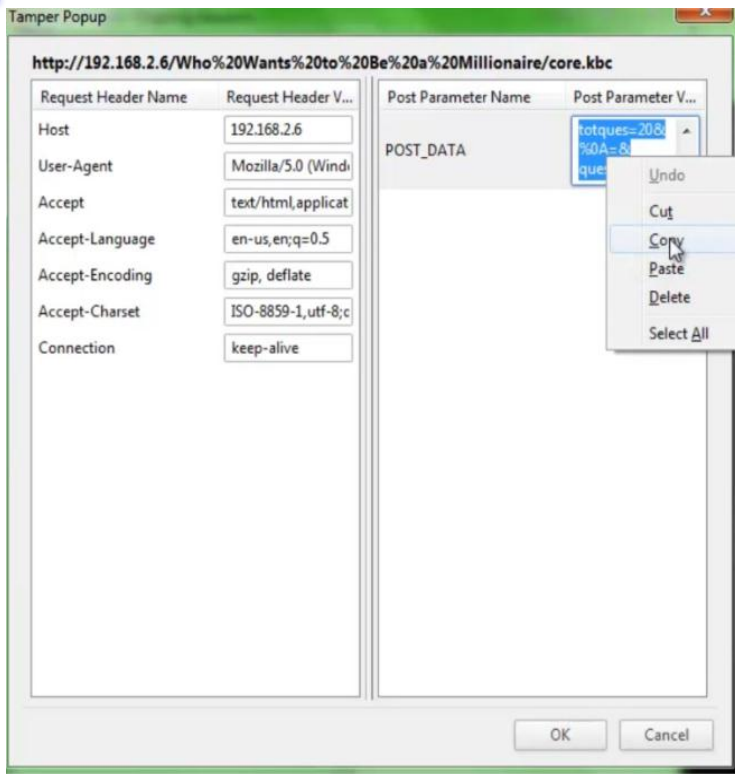
Get failed in the game somehow. We know it's hard for you, but do it. Once you fail game will ask you whether you would like to replay the game or not. Before clicking on "Replay" go to OWASP Logo → Tools → Application Auditing → Tamper Data

Step 3:

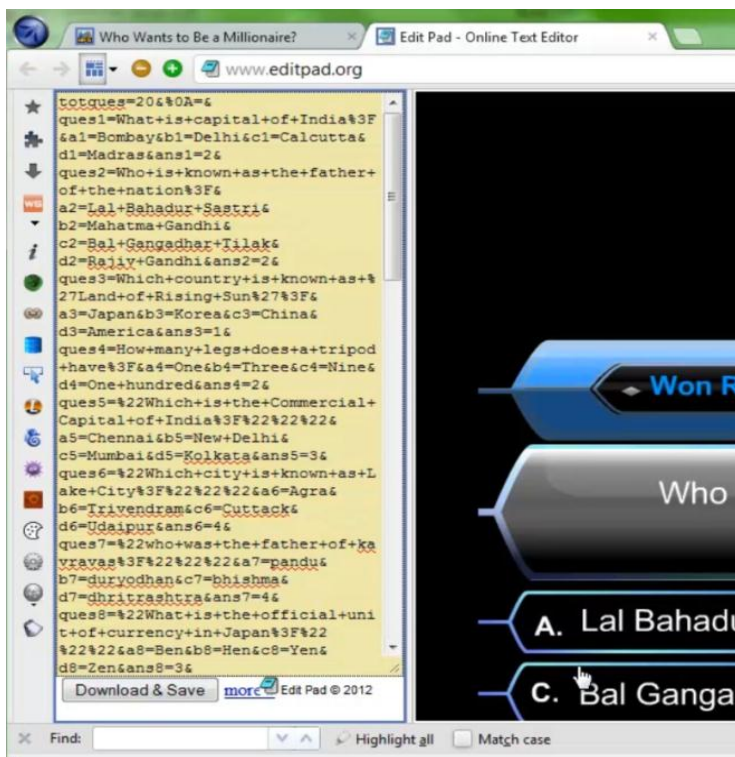
Now go back to the game and press on "Replay" button.



Tamper Data will come up with a pop up asking you to tamper the request or not. Click on "Tamper" button.

Step 4:

Copy the POST_DATA and paste it into any note taking application like Notepad.

Step 5:

Now all you have to do is to go ahead with playing the game. All the answer keys are there in the POST_DATA. You can use the search feature of your note taking application to find the correct answer easily.

In the above screenshot, EditPad is used for taking the notes in Mantra itself and "Find" feature of Mantra helps to easily find out the answer.

You can also watch it at -

<http://youtube.com/watch?v=aPk5vCqh-2k>

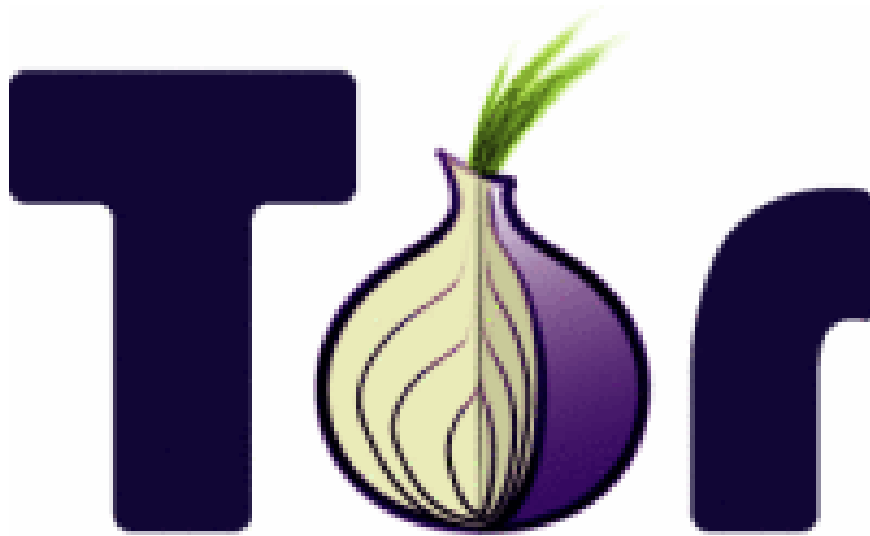
Happy Hacking!!!



Abhi M Balakrishnan

abhimbalakrishnan@gmail.com

An electronics hobbyist turned security evangelist who is working as an information security consultant to put food on table and roof over head. Abhi M has performed several security consulting assignments in the area of penetration testing, code reviews, web application assessments, security architecture reviews etc.



Protect your privacy online with 'TOR'

What is Tor?

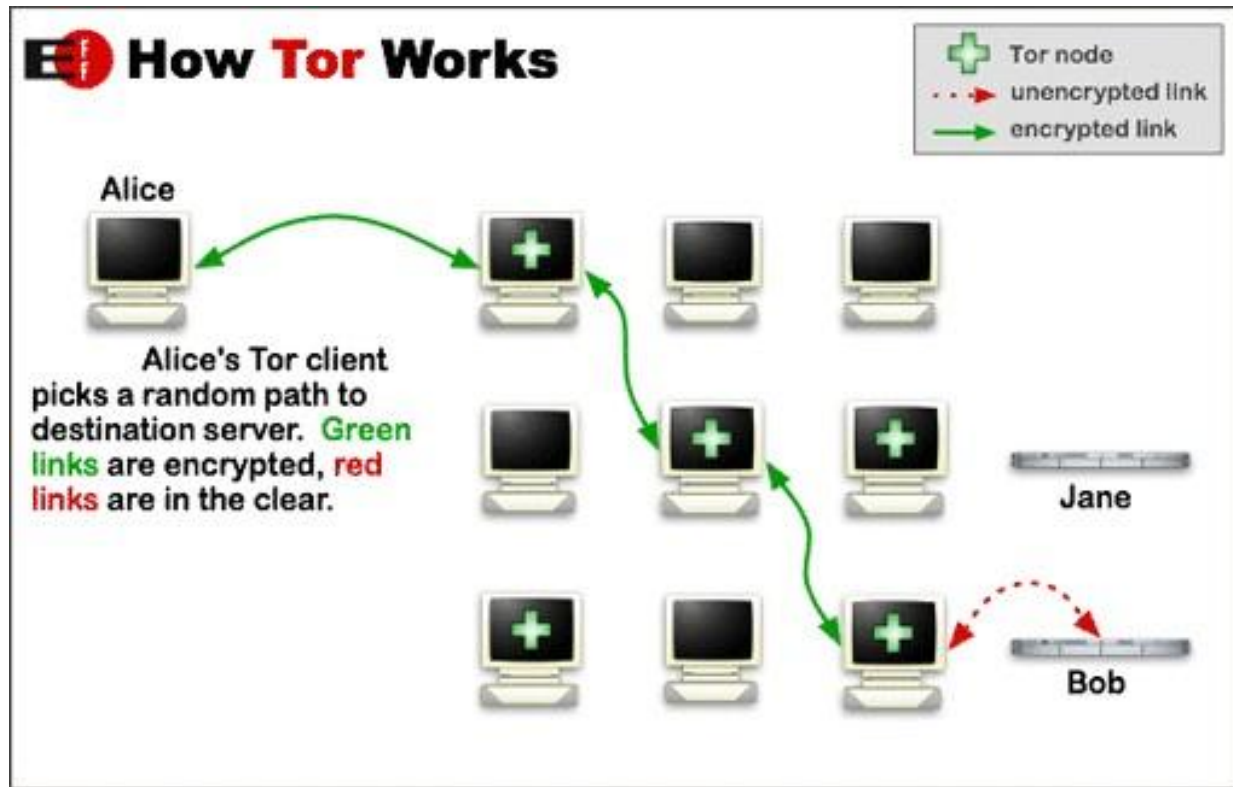
Let's begin with what Tor means: The Onion Router. A router is a device that handles your request to go from your home, office, mobile connection to a website or a web service. If you write in your browser URL bar <http://chmag.in/> and hit return, you'll send your request to your ISP router, which will send the request to another router and so on, until you reach the CHMag ISP router, and finally get your page back. Every one of these steps is called a "hop".

TOR works exactly like this router system, but then there's the onion. Well an onion is... an onion! But the reason TOR developers used the onion metaphor is because when you pass inside the TOR router system to get to you requested website, you send your data inside multiple levels of encryption, exactly like sending them inside the layers of an onion!

So you "launch" this onion inside the Tor network and it's decrypted at every hop it makes, until it reaches the final destination you've requested.

The Tor Wikipedia page has a great image showing how Tor works:

that he can read and then it passes the onion to the next hop.



Electronic Frontier Foundation “How Tor Works” – licensed CC Attribution 3.0

But there are a lot of people inside there! Shouldn't it be defending my privacy?

It may sound strange, but it **does** defend your privacy.

First of all, when using the traditional router network, you **still** pass on a lot of routers, but every request you make can be **intercepted, read, and modified**. That's because everyone who controls that “hop” can see what you've requested, where you're going and what you're doing.

Inside the Tor network this can't happen. Because the path is chosen randomly, every “hop” can just decrypt the small onion layer

As you can see in the “How Tor Works” image only the last step, from the so called **exit node** to the webserver is actually sent in clear text. This has to happen since the last node must know what to ask and to who. But your privacy is still safe because even “sniffing” (means intercepting packages sent over the net), the exit node cannot know who has requested the page, and **nobody can identify you**. The server owner will see the IP address, the number that identifies you as unique on the Internet, from the exit node only. We'll see how simple it works later on.

Since the Tor network usage is **absolutely free of charge**, every peer that connects, including you, became a member of the

network and starts passing “onions” over and over. But don’t worry, you won’t be enabled to be an exit node, if you want to serve as the last hop you can, but this is an optional setting that must be explicitly enabled.

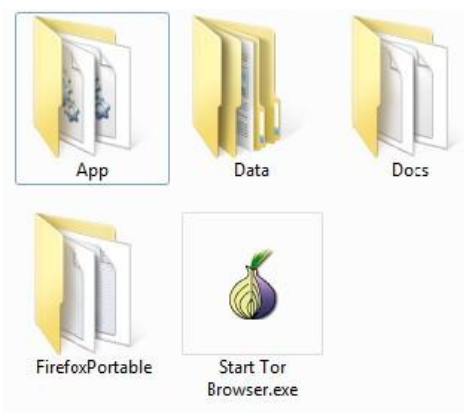
It sounds very complicated to use, I’m not a hacker! I can’t use it!

Well, you’re right, Tor is a very complicated project. But the developers are doing an incredibly amazing work to make it accessible to everyone, so you can use it! And it’s extremely easy!

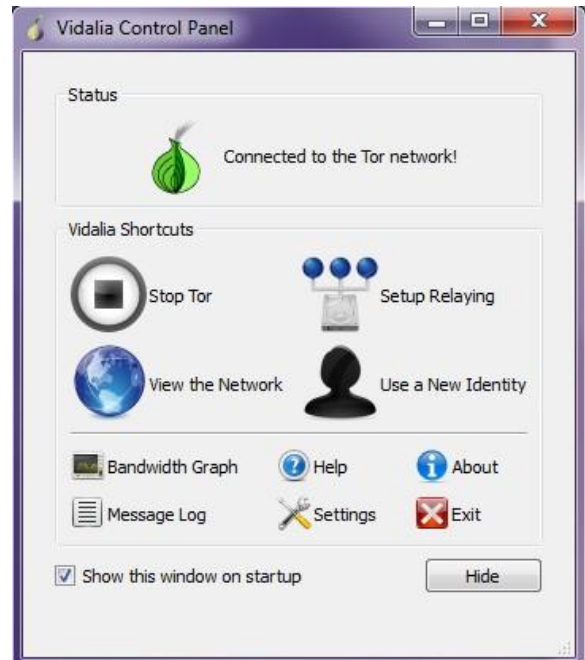
Tor has a side project named “Tor Browser Bundle”, which is a no-installation tool that allows you to surf safely and defend your privacy online with just one click! As said this is an installation free program, and that means you can copy it on a USB key, bring it with you and use it on every system you want, even in hotel or internet cafés workstations.

Just download it from the project page: <https://www.torproject.org/projects/torbrowser.html.en>, where you’ll find versions for Windows, Mac OS X or Linux.

Once downloaded, extract the .exe archive wherever you want and you’ll find this set of icons:



And now you’re just on click away from your safe browsing. Double click “Start Tor Browser.exe”, and Tor will start connecting. Within a few second you’ll see this window:



You really don’t need to worry about all the buttons and the functions inside the Vidalia Control Panel, you just need to see those words “Connected to the Tor network!”. And that means that you’re now protected.

But the magic doesn’t end here, because after the Tor connection has been established, a special version of Firefox, included in the bundle, will automatically open up, with this page:



And you're done! If you keep using this Firefox window you'll be channeled inside the Tor network and surf anonymously and safe. Want to give it a shot? Go to <http://whatsmyip.net/> from both the Tor browser and the browser you used before and you'll see that the IP addresses are different. You are actually using the IP from the exit node, as explained before. If you want to stop using it, all you have to do is close the browser window, the Vidalia panel will also close and the connection with the Tor network will end.

So it is that easy. From now on if you want to defend yourself, don't forget to use Tor browser, and bring it everywhere you go. You have learned that is not as complicated as you thought, in fact it's not complicated at all! This is just the beginning of a lot of services that are available within the Tor project, but this first step is all you have to do to be safe and sound.

Happy privacy and safe browsing everyone!



Federico

glamis@glamisonsecurity.com

Federico "glamis" Filacchione, born and living in Rome - Italy, he is a security professional with more than 10 years of experience. He tries constantly to spread security awareness, explaining that security is not a simple tool, but thinking to the same old stuff in a totally different way (and it's not that hard!). You can read his thought (in Italian) on <http://glamisonsecurity.com>, follow him @glamis on Twitter



"India's Cyber Security Kumbh..."

OWASP InfoSec India Conference 2012

Open Web Application Security Project

August 24th & 25th 2012, Hotel Crowne Plaza, Gurgaon

<http://owasp.in>

India's Cyber Security Kumbh is back

Dates - 24-25th August, 2012.

Venue - Hotel Crown Plaza Gurgaon

Special Discounts for ClubHack Members,
stay connected for the next issue!

CFP Opening on 9th March.

<http://www.owasp.in/category/cfp/>



Section 66A - Sending offensive or false messages

As we have discussed in the earlier articles, under the amended Information Technology Act, Section 66 has been completely amended to remove the definition of hacking. Amendments also introduced a series of new provisions under Section 66 covering almost all major cyber-crime incidents. From this article onwards we will look at those sections.

With internet and telecommunication virtually controlling communication amongst people, amendments in the Information Technology Act, 2000 (IT Act) have made it clear that transmission of any text, audio or video that is offensive or has a menacing character can land a sender in jail. The punishment will also be attracted if the content is false and has been transmitted for the purpose of causing annoyance, inconvenience, danger or insult.

Incidents

5-6 per cent of spam e-mails originate from India - The share of spam e-mails originating from India is about 5-6 per cent of the total worldwide spam email traffic. **FB effect, Bangalore: IIMB girl kills self for boyfriend.** Girl's friend charged with abetment to suicide as well as under the provisions of the Information Technology Act. Malini Murmu, 22, a first year MBA student from the prestigious Indian Institute of Management (IIM), Bangalore allegedly committed suicide after her boyfriend dumped her and made the announcement on Facebook. Police sources say Malini left behind a suicide note saying she was killing herself since her boyfriend left her. Investigations revealed that on the day she killed herself, Malini and her boyfriend had an argument which led to the breakup. Later her boyfriend left a post on Facebook saying, "Feeling super cool today, dumped my new ex-girlfriend, Happy Independence Day".

The Law

Section 66A of the IT Act is a relevant section which penalizes ‘sending false and offensive messages through communication services’. The section reads as under –

Any person who sends, by means of a computer resource or a communication device,—

- a) Any information that is grossly offensive or has menacing character; or
- b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
- c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

Punishment

Imprisonment for a term which may extend to three years and with fine.

Explanation

For the purpose of this section, terms “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

The section covers two different acts –

1. Sending offensive or menacing messages sent by using electronic communication means.
2. Sending false messages to cheat, mislead or deceive people or to cause annoyance to them.

While proving false message is relatively easy, but the real question is ‘What constitutes an electronic message to be offensive or of menacing character?’ Indian law has not defined anywhere the meaning of ‘offensive’ or ‘menacing’. As per the laws of general English, a person receiving message should find that to be offensive to apply this provision, so its interpretation becomes relative and differs from person to person.

Cyber-crimes like, intentionally sending SPAM messages, phishing emails, threatening messages, etc. can also be punished under this section. This section is also applied along with Section 67 or 67B which is related to cyber and child pornography respectively.



SagarRahurkar

contact@sagarrahurkar.com

He is a Law graduate, a Certified Fraud Examiner (CFE) and a certified Digital Evidence Analyst. He specializes in Cyber Laws, Fraud examination, and Intellectual Property Law related issues.



Get the best real-world Android education anywhere!

Attend

AnDevCon III

The Android Developer Conference

May 14-17, 2012
San Francisco Bay Area

AnDevCon is the biggest, most info-packed, most practical Android conference in the world!

"AnDevCon was an informative and comprehensive presentation of Android development concepts, tools and techniques."

—Patrick Burrell, Sr. Research Scientist, Amway

"The conference is worth the time and expense. It's a great place to meet talented people in the Android industry."

—Keith Collins, CTO, Neusoft

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."

—Joshua Turner, Software Engineer, Primary Solutions

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!

Register Early and SAVE!



A BZ Media Event

Follow us: twitter.com/AnDevCon

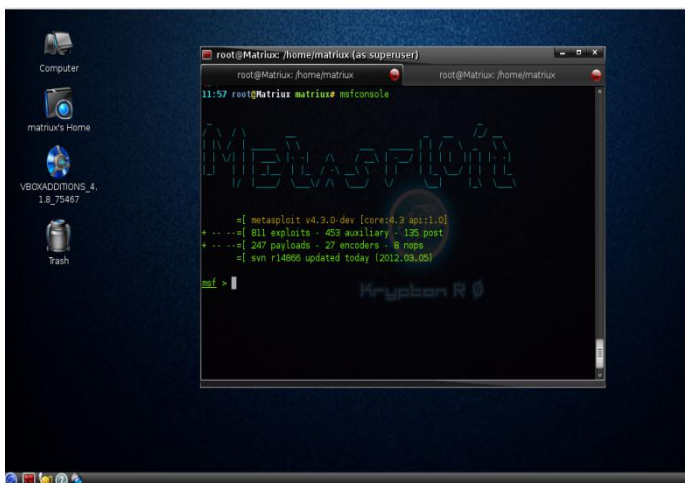
AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

Register NOW at www.AnDevCon.com



EtherApe - Graphical Network Monitoring

Hello readers, we are back again with a new release, Matriux Krypton v1.2 at nullcontritiya,Goa 2012. Thank you for your support throughout these years that we are able to bring in the bigger and better security solutions. This version includes some great features with 300 powerful penetration testing and forensic tools. The UI is made more elegant and faster. Based on Debian Squeeze with a custom compiled kernel 2.3.39-krypton Matriux is the fastest distribution of its kind and runs easily on a p-IV with as low as 256MB RAM and just 6GB HDD. Included new tools like reaver-wps, androguard, apkinspector, ssh server and many more. Installer (MID) is made more easy this time.

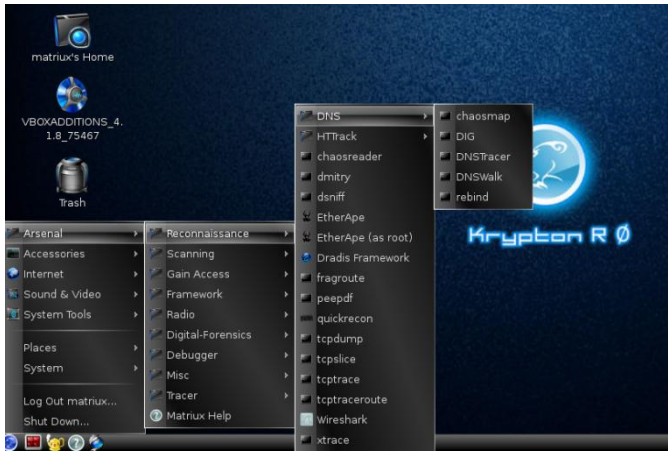


Doesn't it look cool? Go, ahead give a try and let us know what you think of the new version.

Now coming to this months' article on EtherApe, which is an open source graphical network monitor for Unix systems. It displays the network activity graphically with host and link sizes shrink and grow accordance with the traffic activity. Protocols are color coded. Some features of EtherApe include:-

- Network view can be modified by applying filters
- Can read traffic from file along with the network
- A variety of protocols, packet types and frames are supported.
- Clicking on any link or node will provide additional information regarding the protocols and traffic information
- Handles traffic on Ethernet, WLAN, VLAN plus several other media and encapsulation types
- Output can be exported into a XML file supported from version 0.9.11

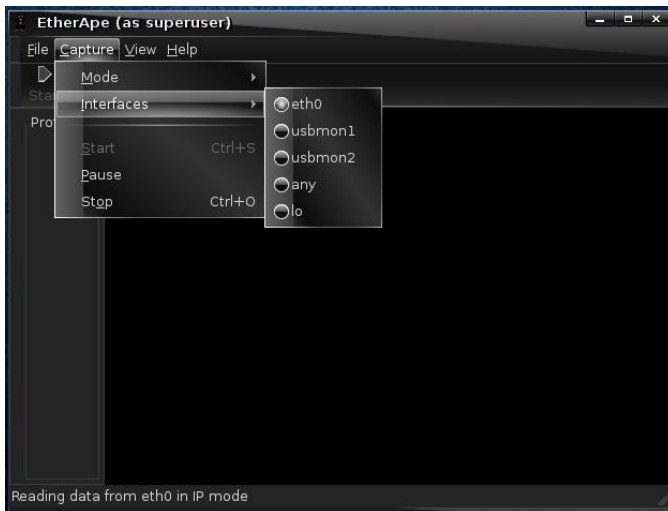
EtherApe can be found in Matriux Arsenal under Arsenal → Reconnaissance → EtherApe (root)



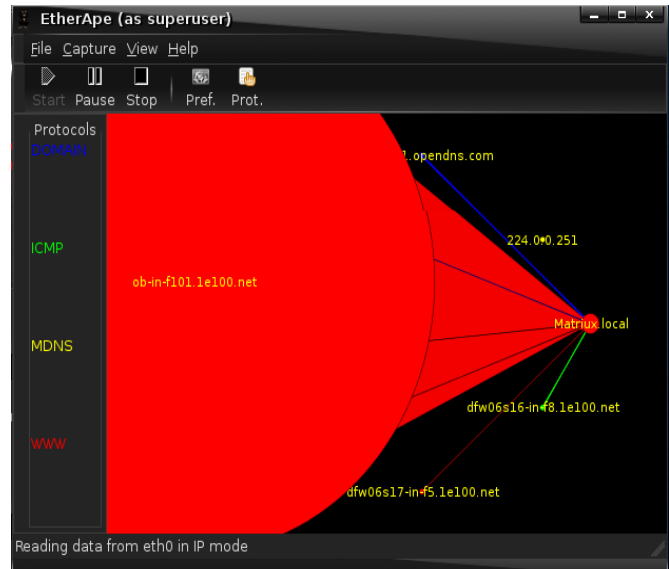
Or simply fire up EtherApe by typing EtherApe in terminal.

Note: Remember that EtherApe requires root permission to run, else you will get an error “No suitable Device found”.

To start monitoring the network select the network interface from the Menu Capture → Interfaces.

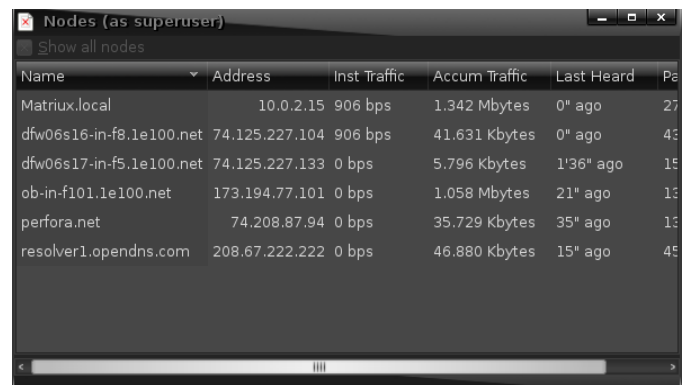


This will start reading the network data from the interface selected and displays the network in graphical representation.

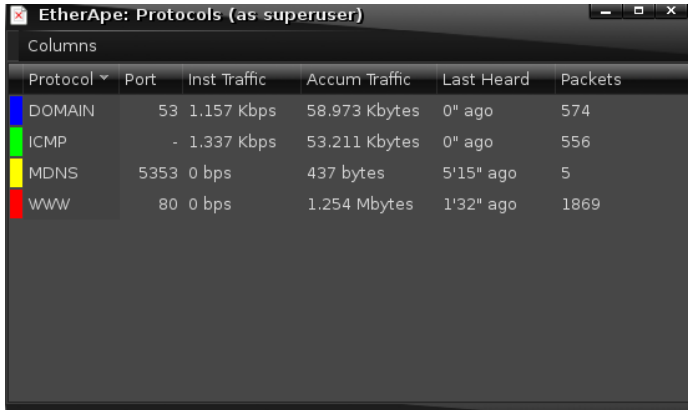


When you start EtherApe, you may or may not see traffic depending on whether there is traffic actively passing through your network. (Here I pinged Google and opened Matriux Forums in a browser to generate some network activity).

Also the data regarding this network activity can be viewed from Menu → View → Nodes/Protocol.



Showing the activity at the nodes.



Protocol	Port	Inst Traffic	Accum Traffic	Last Heard	Packets
DOMAIN	53	1.157 Kbps	58.973 Kbytes	0" ago	574
ICMP	-	1.337 Kbps	53.211 Kbytes	0" ago	556
MDNS	5353	0 bps	437 bytes	5'15" ago	5
WWW	80	0 bps	1.254 Mbytes	1'32" ago	1869

Showing the activity with respect to protocols, this data is useful in many ways to trouble shoot network or check for unwanted traffic etc.

Also clicking on any link/node in the network map will display the activity at that node/link.



Protocol	Port	Inst Traffic	Accum Traffic	Last Heard	Packets
DOMAIN	53	960 bps	32.770 Kbytes	0" ago	388

You can also configure EtherApe from the preferences in the menu.

Conclusion

EtherApe can also read a tcpdump file that will allow us to capture network traffic to a file and analyze that traffic later or in offline mode. Reason being, using EtherApe as root is not recommended to remotely monitor the network as you run a risk of transmitting the root information over the network. EtherApe is a great tool that can

monitor the network and can be used for monitoring the network activity and their protocols. Go ahead and run EtherApe to see the visual beauty of the network ;)

Happy Hacking ☺

Reach us at:-

report@matriux.com

[@matriuxtig3r](https://twitter.com/matriuxtig3r)

www.facebook.com/matriuxtig3r

Also if you are interested in supporting Matriux project as a Developer/Contributor or any other forms such as feedback you are welcome to write to us!



Team Matriux

<http://matriux.com/>



**If a Computer Network was a game of chess,
isn't this how your server would look like?**

Photography: Madhav Goel

<https://www.facebook.com/madhavgoyalphotography>

Concept & Design: pankit@chmag.in