Host Website from Home Anonymously

Prerna Mahajan[1] and Kashish Gupta[2]
[1]Professor, Department of Computer Science, IITM Janakpuri, New Delhi, India
[2]Research Scholar, Department of Computer Science, IITM Janakpuri, New Delhi,India
prerna.mahajan00@gmail.com, kashishgupta1990@yahoo.com

Abstract

Hosting a website anonymously is possible by the infrastructure provided by the Onion Router which provides anonymous connections that are strongly resistant to track web server which host the website. It hides not only the server, but also traffic by using inbuilt feature of encrypting data stream. Onion Routing's anonymous connections are bidirectional and near real-time, and can be used anywhere even from home. Socket connections used here to establish or terminate connection. It uses series of proxies to host website and other services like e-mail etc. Website hosted with Onion Router can only be visit by using Tor Hidden Services. In order to access or visit these websites on Tor, the client should be available on Tor network via Tor Browser. Tor includes its own DNS resolver which will dispatch queries over the mix network. Each website hosted on Tor network has unique Base 16 encoding with .onion extension. Access to onion routing network can be configured through various ways as per the needs, policies, and facilities of the connecting router. In this paper we discuss the anonymous web services used to host website from home using Tor Network. The method proposed here provides reliable, secure and cost effective alternative for hosting website. The discussion also includes the comparison of the proposed facility with the standard web hosting features.

Keywords: Tor, Onion, Anonymous, Host, Web Server

1 Introduction

The purpose of hosting a website anonymously is to make a web server secure and untraceable. With the growth of the communication over the Internet leads to lack of security to web server and there hosted website. Attacks like Cross-site request forgery and XSS on websites leads to compromise the website users as well [1]. Anonymous communication is a fundamental building block to protect privacy by obscuring relationship between communicating parties (Client and Server). Without this protection attackers are able to deduce information about the web server location, operating system and others private services. This is often enough to hack the web server by finding vulnerability on it. Web Scanner, Traffic Analyzer, and Network packet sniffer can be used by attacker to infer further information about server as well as client also [2][3][4].

There are many approaches proposed to provide anonymity at the network layer, e.g., Tor [5], I2P [6], and JAP [7] with Tor being the most widespread and popular system today The Tor network is a circuit switched, low-latency anonymizing network. It is an implementation of the onion routing technology, which is based on routing TCP streams through randomly chosen paths in a network of onion routers (OR), while using layered encryption and decryption of the content. Tor is very dynamic network anybody can join it by running a router and thus offer available resources for the other user, that's why hosting website on the Tor network make the web server secure and anonymous [5].It differs from the public network which connects node which that are connected to each other creates their networks which are often configured with "public" Internet Protocol (IP) addresses that is, and are "visible" to devices outside the network (from the Internet or another network).However Networks can also be configured as "private" where devices outside the network cannot "see" or communicate directly to them [8].

2 Standard Way of Hosting Website

Usually we need Web server for hosting website, domain name for ease of access and database to store data. Security issues on web become a big issue now days, to achieve security on network layer we use HTTPS or we can say Secure Socket Layer (SSL) or Transport Layer Security (TLS). There are lots of issues in Authentication and Authorization of users, SQL Injection, Blind SQL Injection, SQL Backdoors attack breach the security and gain access to website database. Website physical location is easily available on Internet, and other useful information like phone number, Domain registration number which may leads to social engineering. The process starts with providing static ip address with some qualified (registered) host name are required to host website, the hosting server should support language required by website like Apache Tomcat support java[13], WAMP support php[14] etc. After the above mentioned things have been done these deployment phase starts, where web application get installed on server and ready to use via appropriate URL of website.

3 Experiments' and Results

This section includes several test cases using Backtrack Linux, Kali Linux penetration testing operating system, wireshark tool for traffic analysis etc. The following parameters have been discussed

3.1 Information Gathering

There are many tools which are used to help in gathering information, information retrieved by the tools are like Operating System running on server, OS Version, Number of ports open etc. We have nmap tool used to gather information [3].It lists the numbers of ports open as shown in Fig.1 which help in identifying the services provided by the server. The nmap tool has also been used to identify the operating system installed on server as shown in Fig.2

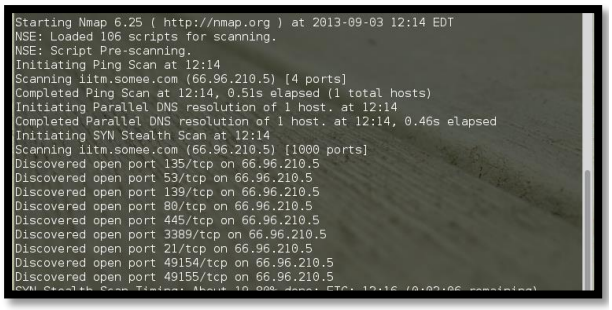


Figure 1: Number of Ports open on Server

Figure 2: Operating System Information on Server

3.2 Network Traffic Analysis

Wireshark network traffic monitor can quickly identify network bottleneck and detect network abnormities [4].The Fig.3 shows the details of the network traffic and communication between client and server. It leaks the password. It grabs the packets communicated which can leads the sensitive information of the user ,if further investigated .

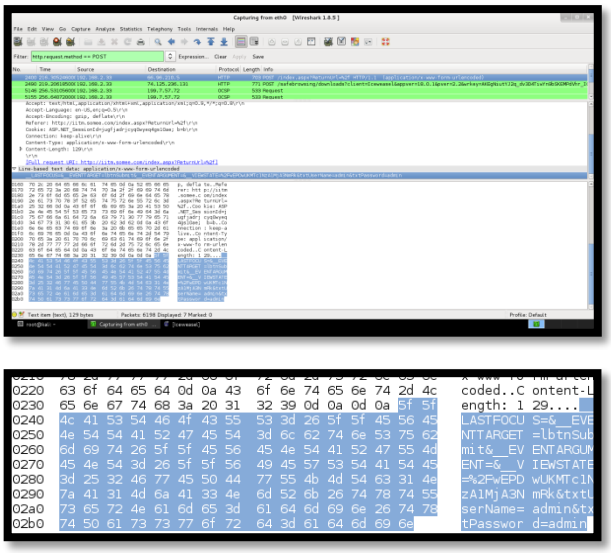


Figure 3 Password Retrieval via Network Analysis

3.3 Web Page Vulnerability Scanner

Are the automated tools that scan web applications to look for known security vulnerabilities such as cross-site scripting, SQL injection, command execution, directory traversal and insecure server configuration. A large number of both commercial and open source tools are available and all these tools have their own strengths and weaknesses [16]. These tools can highlight the vulnerability like Cross Site Request Forgery as shown in Figure5

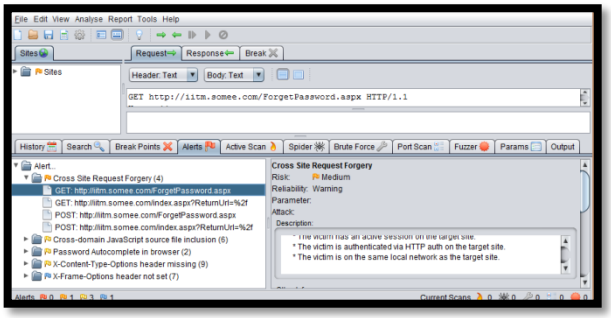


Figure 5: Webpage Vulnerability Information

3.4 Geographical Location

In standard webhosting physical location of the web server can easily located which leads to social engineering as shown in Fig.6 which further makes web server more vulnerable to attack or hijack [17]

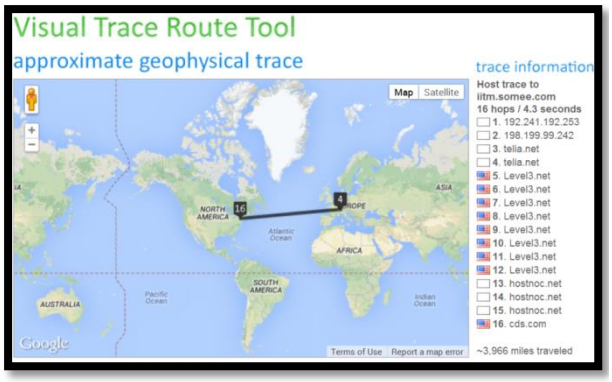


Figure 6: Web Server Location

4 Limitations of Standard Server

Web applications are not completely secured, and can easily compromise due to vulnerabilities in websites. The important information about server can easily be gather by web tools like nmap, website crawler, which can reveal information like number of ports open on server and such information leaks server important information about server and makes it vulnerable like type of operating system on server, so that attacker can find vulnerability on that flavor of operating system as discussed previous. Packet spoofing on network result leads to discloser of session variables and session cookies which can be used for session Hijacking or Man In Middle Attack (MIMA) [11].

Such Vulnerability Analysis tool highlights all the vital information about server or website. Hence Deny of service (DOS) and Distributed Deny of service (DDOS) have been common and are difficult to avoid, so generally load balancer and filters are used to prevent from these types of attack but Input Validation attack, Impersonation attack, Buffer Overflow attack are still security issues [12].

5 Anonymous Web Hosting

As discussed in previous section, It is possible to infer who is talking to whom over a public network using traffic analysis . This section discuss a flexible communication infrastructure, onion routing, which hides seen to traffic analysis over network, gather information related to web server, host location, host operating system etc. Onion routing works behind the application layer, and provides interface with a wide variety of unmodified Internet services by means of proxies. Onion routing has been implemented on Sun Solaris 2.4; in addition, proxies for World Wide Web browsing (HTTP), remote logins (RLOGIN), e-mail (SMTP), and file transfers (FTP) [5]. This research we manly focus on HTTP protocol. It provides application independent, real-time, and bi-directional anonymous connections that are resistant to both eavesdropping and traffic analysis. Applications making use of onion routing's anonymous connections may (and usually should) identify their users over the anonymous connection. User anonymity may be layered on top of the anonymous connections by removing identifying information from the data stream. The main aim here is to provide web server anonymous connections, not anonymous communication. The use of a packet switched public network should not automatically reveal who is talking to whom. The onion routing complicates the traffic analysis by applying encryption on network layer which does not reveal identifies (Who is talking to whom)

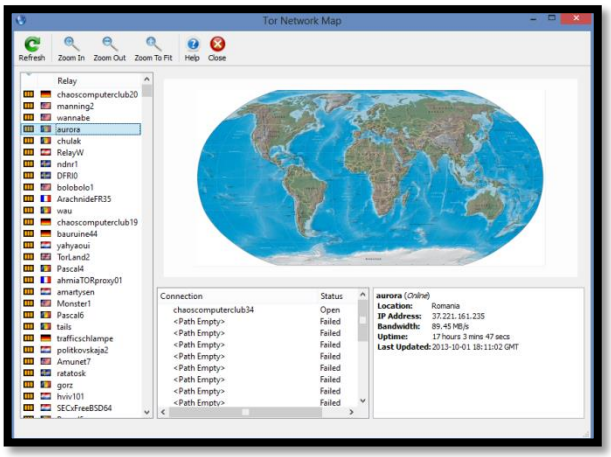
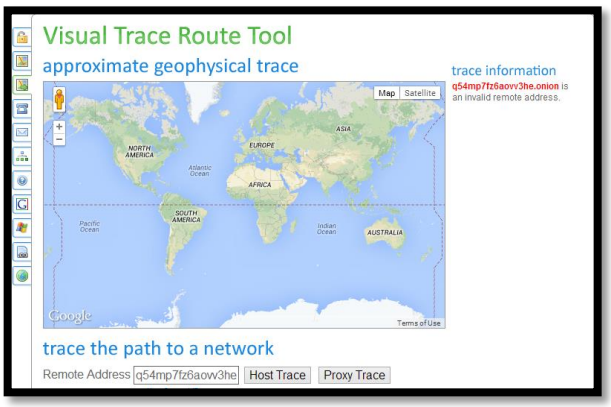


Figure 7: Tor Network Map

5.1 Geographical Location

In standard webhosting physical location of the web server can easily located which leads to social engineering which further makes web server more vulnerable to attack or hijack. But Anonymous Website hosted in Tor network can make it possible to hide the physical location where the website is actually hosted as shown in Fig.8.[17]



Figue 8: Web Server Location NOT FOUND

5.2 5.2 Network Traffic Analysis

Wireshark network traffic monitor can quickly identify network bottleneck and detect network abnormities [4].The Fig.9 shows the details of the network traffic and communication between client and server. All the data between client and server are encrypted using RSA algorithm (Public and Private Key Scheme). Because of encryption network traffic analysis failed to see credential on network.

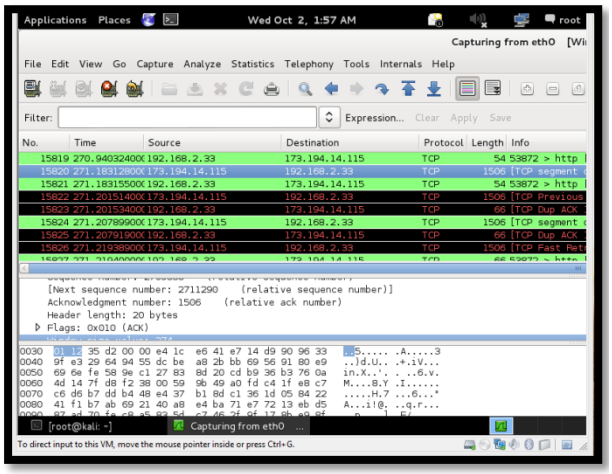


Figure 9: Encrypted Traffic in Network

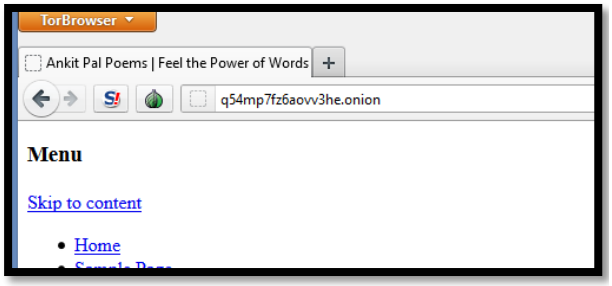


Figure 10: Hosting Website from Home Anonymously

6 Benefits of Research

Both the parties' client and server are hidden behind the Tor network, Tor provides many hidden service on their network using Tor routers and allow any of the peer to be a part of its router family and can able to share resources via protocol allowed in Tor like HTTP, FTP, RLOGIN, SMTP etc. Out of these hidden services we use Tor HTTP service to Host Website Anonymous on Onion Network. This will provide security on Network Layer itself client which are present on onion network can access the website. However the large number of proxy's and multilayer encryption between circuits of onion router degrades the response time.

Any peer can become a part of Onion network ,it gives the privilege to Host Website even from home in Onion network. Some of the research benefits are:-

- It's FREE, ZERO investment required, we can run website from home itself.
- It is secure, and can use for military and defense purpose.
- No Footprint, Who is talking Whom
- Support all web server like Apache Tomcat, Internet Information Services etc
- Uses RSA encryption mechanism for security.
- Free auto generated 16 character alphanumeric domain name is provided by onion.

7 Conclusion

Onion routing provides real-time, bi-directional communication through anonymous connections that are resistant to both eavesdropping and traffic analysis. These anonymous connections can substitute for socket connections in a wide variety of unmodified Internet applications using proxies. The proposed prototype of onion routing includes proxies for Web Server, hosting website on these server we are achieving anonymous web hosting on internet by using tor network, using this technique it is possible to host website from home in Tor network and achieve anonymous web hosting from home. Anonymity of web server increase security of website agenised in both physical location discloser of server and tool based attack as discussed above. However similar to every other network, it also has some tradeoffs associated with it. The Latency time is increased in Onion network and it requires high bandwidth to surf on Tor network. If we use FTP protocol for downloading any file over this network it may reduce security.

References

[1] Open Web Application Security Project, https://www.owasp.org/index.php/Category: Attack, visited on 1/11/ 2017.

[2] Acunetix Web Vulnerability Scanner, http://www.acunetix.com/, visited on 4/12/2017.

[3] NMAP Network Scanning, http://nmap.org/, visited on 15/12/2017.

[4] Gerald Combs – Wireshark, http://www.wireshark.org/, visited on 18/12/2017.

[5] Tor Project, https://www.torproject.org/, visited on 20/12/2017.

[6] J. P. Timpanaro, Monitoring the I2P Network, http://www.i2p2.de/papers.html, visited on 22/12/2017.

[7] JonDonym Anonymous Proxy Servers, http://anon.inf.tu- dresden.de/index_en.html, visited on 25/12/ 2017.

[8] University of Miami, http://it.med.miami.edu/x198.xml, visited on 28/12/2017.

[9] A. Pfitzmann, B. Pfitzmann and M. Waidner, “ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead”, *GI/ITG Conference:Communication in Distributed Systems, Mannheim,* Heildelberg, pp 451- 463 (1991).
[10] A. Iyengar, M. S. Squillante and L. Zhang, Analysis and characterization of large-scale web server access patterns and performance, *World Wide Web, 2(1-2),* pp.85-100 (1999).
[11] Network Forensic Analysis of SSL MITM Attacks, http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks, visited on 2/1/2018.
[12] E. Wimberley and N. Harrison, ”Morden Overflow Targets”, http://packetstormsecurity.com/files/download/121751/ModernOverflowTargets.pdf, visited on 2/2/2018 .
[13] T. Khare, “Apache Tomcat 7 Essentials”,ePackt Publishing (2012).
[14] WAMP, http://www.wampserver.com/en/, visited on 5/2/2018.
[15] J. D. Ford and B.Smit, "A Framework for Assessing the Vulnerability of Communities in the Canadian Arctic to Risks Associated with Climate Change". *ARCTIC* ,57 (4),pp.389–400 (2004).
[16] Open Web Application Security Project Vulnerability Scanning Tool, https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools, visited on 10/2/2018.
[17] You Get Signal, http://www.yougetsignal.com/tools/visual-tracert/, visited on 20/3/2018.