Web Authentication based on Trusted Connection

Lawrence Amer

Abstract- Demonstrating the ability to develop a new type of defense technique to your administration panel , sensitive folder using a simple user friendly interface to authenticate administration , client authorized permission depending on trusted IP address using a simple front end application which is running in external host ,responsible for managing , organizing sessions ip while on the other hand , a server side scripting file running on background to retrieve these sessions and store them for further authentication process

I. Introduction

Now days , Web Applications are the most used and targeted on Cyber space , i am coming with a Cyber Space definition instead of Internet ,because many of users are not just normal users .

There are a new type of users who are considered as threat on the Cyber space called themself as hackers .

Hackers could get into your system in many different ways using Un patched or private vulnerabilities , or by using Social Engineering .

So the defense strategy for these attacks in most cases expensive , and needs a lot of rules to follow , if we are talking about small firm or medium one , it will be hard ,expensive for them to hire security experts to protect them.

Regarding this topic , i have made a research paper to discuss the best way to secure your protected one with simple,easy,cheap project to start with

Research Guide Index
1) Protocols
2) introduction into Apache Web Server
3) T.Auth project from idea into building .

II. Protocols

Is a set of rules that governs the commnications between computers on a network . many different types of network protocols and standards are required to ensure the computers can communicate with each other regarding the type of cards or operation systems .

Reference model defines seven layers of networking protocols as shown below in a box

OSI Layer	Name	Common Protocols
7	Application	HTTP | FTP | SMTP | DNS | Telnet
6	Presentation	
5	Session	
4	Transport	TCP | SPX
3	Network	IP | IPX
2	Data Link	
1	Physical	Ethernet

So as picture above , we can see the OSI Layers , but at this time we are going to explain

Application OSI Layer which is related to research paper .

DNS - Domain Name System - translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa

DHCP - Dynamic Host Configuration Protocol - can automatically assign Internet addresses to computers and users

FTP - File Transfer Protocol - a protocol that is used to transfer and manipulate files on the Internet

HTTP - HyperText Transfer Protocol - An Internet-based protocol for sending and receiving webpages

IMAP - Internet Message Access Protocol - A protocol for e-mail messages on the Internet IRC - Internet Relay Chat - a protocol used for Internet chat and other communications POP3 - Post Office protocol Version 3 - a protocol used by e-mail clients to retrieve messages from remote servers

SMTP - Simple Mail Transfer Protocol - A protocol for e-mail messages on the Internet

III. Apache HTTP Server . (wikipedia Reference)

Apache Server is free and open-source cross-platform web server software, released under the terms of Apache License 2.0. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation.

The Apache HTTP Server is cross-platform; as of 1 June 2017 92% of Apache HTTPS Server copies run on Linux distributions. Version 2.0 improved support for non-Unix operating systems such as Windows and OS/2. Old versions of Apache were ported to run on OpenVMS and NetWare.

Originally based on the NCSA HTTPd server, development of Apache began in early 1995 after work on the NCSA code stalled. Apache played a key role in the initial growth of the World Wide Web,quickly overtaking NCSA HTTPd as the dominant HTTP server, and has remained most popular since April 1996. In 2009, it became the first web server software to serve more than 100 million websites.As of July 2016 was estimated to serve 46% of all active websites and 43% of the top million websites.

IV. Feature overview

Apache supports a variety of features, many implemented as compiled modules which extend the core functionality. These can range from server-side programming language support to authentication schemes. Some common language interfaces support Perl, Python, Tcl and PHP. Popular authentication modules include mod_access, mod_auth, mod_digest, and mod_auth_digest, the successor to mod_digest. A sample of other features include Secure Sockets Layer and Transport Layer Security support (mod_ssl), a proxy module (mod_proxy), a URL rewriting module (mod_rewrite), custom log files (mod_log_config), and filtering support (mod_include and mod_ext_filter).

Popular compression methods on Apache include the external extension module, mod_gzip, implemented to help with reduction of the size (weight) of Web pages served over HTTP. ModSecurity is an open source intrusion detection and prevention engine for Web applications. Apache logs can be analyzed through a Web browser using free scripts, such as AWStats/ W3Perl or Visitors.

Virtual hosting allows one Apache installation to serve many different Web sites. For example, one machine with one Apache installation could simultaneously serve www.example.com, www.example.org, test47.test-server.example.edu, etc.

Apache features configurable error messages, DBMS-based authentication databases, and content negotiation. It is also supported by several graphical user interfaces (GUIs).

It supports password authentication and digital certificate authentication. Because the source code is freely available, anyone can adapt the server for specific needs, and there is a large public library of Apache add-ons

V. The idea of T.Auth Application

Publishing your site ,blog..etc into the Internet is some thing very popular these days specially web application developers made it easy to you to setup it correctly .
but many of these websites got hacked or being hacked every day The reason behind this , is the weakness of security knowledge on sites administrators . or even published vulnerabilities that allow hackers to get access into your zone .

Most of usage techniques used these days to protect your site is to install and configure security tools that makes it hard into hackers to get in . but this actually doesn't put an end for hackers there is always a way to break in .

So after deep thinking of a way to know how to secure it in a kind of easy to use the idea of developing a project to do it was screaming in my mind .

My thought was toward developing a way to secure administration folders depending on IP Address Whitelist , but how to do that if there are many administrators and each one of them connecting from dynamic ip address not a static one .

VI. Preparation of the idea

Using Dynamic Dns is the only way that can we use to make sure that host is resolved into IP address .

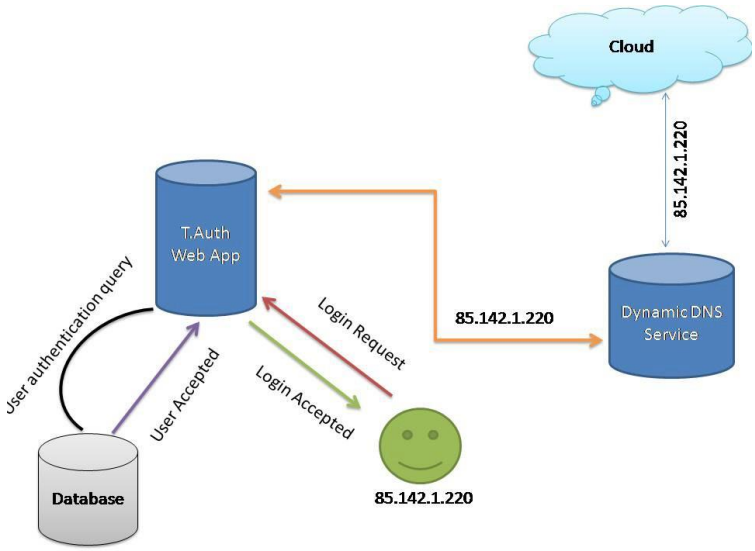
There are many Dynamic Dns Free Providers like no-ip company , but as you know these applications are standalone and every user must download the client and enter the information then establish the connection , i think it is also hard for simple users and for sure they will not accept it as solution besides every administrator should has his own DNS entries . in this case it is waste of time and energy .

So the only way was is to start building web application which will do all these things to gather with out so much interactions of users .

Features of T-Auth Web application

- unlimited users accounts with isolated panels
- simple and user friendly
- Dynamic DNS Login information are stored in database
- Customized external host & domain .
- monitoring users activity with super administration panel .

easy to ban unwanted sessions .



Project Requirement

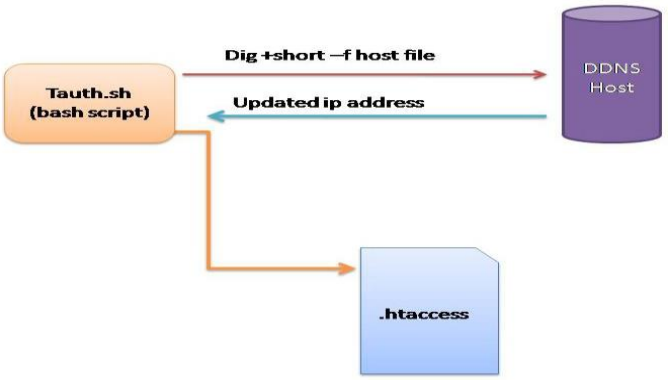
- Apache Web Server
- Apache Rewrite mode enabled (Allow Override All)
- Php 5.6 or above
- Mysql Database
- an Account on Dynamic Dns Prodvider (no-ip is supported)
- Linux Sever

Working Strategy

Developing a bash script to get the current Ip address from the selected Dynamic Dns provider the idea of bash script is to add it as cron job into targeted Linux server , and will be running every 5 min to get user updated ip address then add it into .htaccess file on administrator folder . with custom rule to deny all IP Address and only allow the authorized ones .

Below is digram to explain how bash script will connect into specific ddns host to get the new IP Address which is updated from T.Auth CMS php Application .

Digram 1. 2 - bash script



uth Frontend CMS

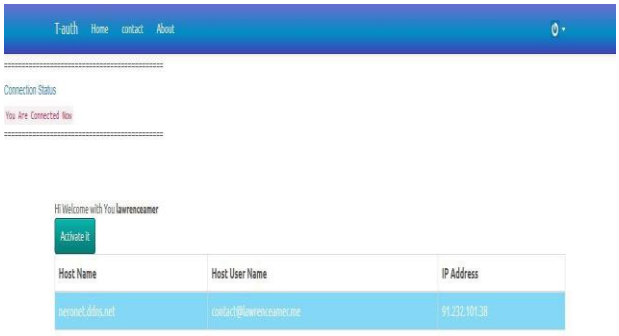
Developing this application wasn't easy as expected , since we have to add many feature including permissions ,groups . and connection libraries to start with on establishing DDNS updating through their public Api

CMS contains of :

- Login user interface
- table for current ddns host with username , so every user has his own host ddns details stored in database .

Update user current ip after clicking on Activate button

So after clicking on activate it button , the application will connect using details saved and response with connection status .



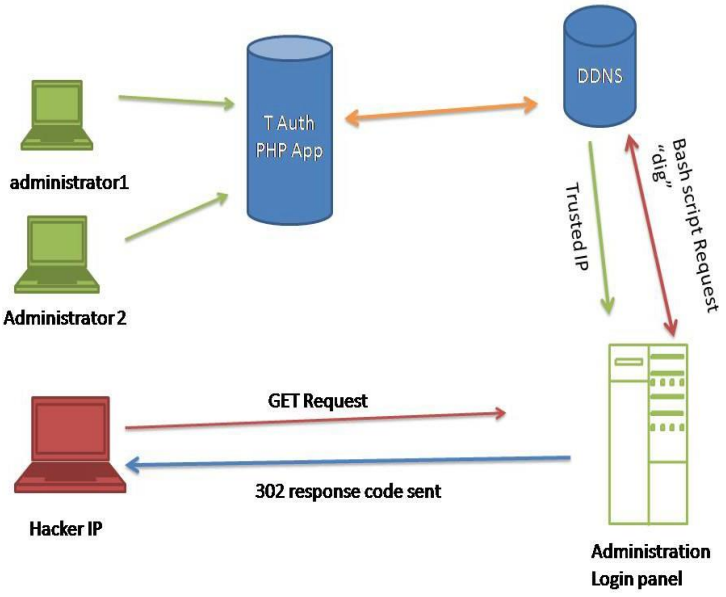


Image above shows expect work of how server will know that administrators are already have their trusted IP Address since they have login into different external host to send their ip address into verification process , which finally will be allowed to get into administrators folders .

AUTHORS

First Author – Lawrence Amer