Forced Protection Security Wall for Web Server on Network Attacks

Homer Benny Bandela, G Samuel Vara Prasad Raju, T R S Prasad Babu

Dept. of CSE, Sir CRR College of Engineering, Eluru, AP, India
Dept. of CSSE, Andhra University, Visakhapatnam, India
Dept. of EIE, Sir CRR College of Engineering, Eluru, AP, India

Abstract
The term web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver web content that can be accessed through the Internet. Here we deal with software of the server. The most common use of web servers is to host websites, but there are other uses such as gaming, data storage or running enterprise applications. When they are active in network, there is a possibility to attack server by attackers. They can steal valuable information from the server or they can corrupt your system or some may overwrite falls information on existing data. They are also called as hackers. Black hats are meant to damage or do illegal operations on system. Once attacker enters into your server and nobody can stop them. This paper deals with the things that make you aware of such things. Possibly it gives some solutions to the problems which may prevent attackers to attack.

Keywords
Web Server, Websites, Attackers, Black Hats, Attack

I. Introduction
Modern computers based on integrated circuits are millions to billions of times more capable than the early machines, and occupy a fraction of the space. Simple computers are small enough to fit into mobile devices, and mobile computers can be powered by small batteries. Personal computers in their various forms are icons of the Information Age and are what most people think of as “computers.” However, the embedded computers found in many devices from MP3 players to fighter aircraft and from toys to industrial robots are the most numerous. Network devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as servers and personal computers, as well as networking hardware. Two devices are said to be networked when a device is able to exchange information with another device.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. Apart from the physical communications media described above, networks comprise additional basic hardware building blocks, such as network Interface Controller cards (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls.

A server is a piece of computer hardware or software makes available a service that can be accessed by its clients. The server is often (but not always) on another computer system, in which case the communications takes place over network.

Server (computing): a computer system used primarily to provide one or more network services to its clients

• Server (hardware): a computer system that runs one or multiple servers to provide services over network employing some communications protocol to its clients

• Network service: a data storage, manipulation, presentation, communication or other shared function provided by a server and consumed by its clients

Servers operate within a client-server architecture, servers are computer programs running to serve the requests of other programs, the clients. Thus, the server performs some tasks on behalf of clients. The clients typically connect to the server through the network but may run on the same computer. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener.

Servers often provide essential services across a network, either to private users inside a large organization or to public users via the Internet. Typical computing servers are database server, file server, mail server, print server, web server, gaming server, application server, or some other kind of server.

Numerous systems use this client / server networking model including Web sites and email services. An alternative model, peer-to-peer networking enables all computers to act as either a server or client as needed.

Types of Servers

• Application server, a server dedicated to running certain software applications

• Catalog server, a central search point for information across a distributed network

• Communications server, carrier-grade computing platform for communications networks

• Compute server, a server intended for intensive (esp. scientific) computations

• Database server, provides database services to other computer programs or computers

• Fax server, provides fax services for clients

• File server, provides remote access to files

• Game server, a server that video game clients connect to in order to play online together

• Home server, a server for the home

• Mail server, handles transport of and access to email

• Mobile Server, or Server on the Go is an Intel Xeon processor based server class laptop form factor computer.

• Name server or DNS

• Print server, provides printer services

• Proxy server, acts as an intermediary for requests from clients seeking resources from other servers

• Sound server, provides multimedia broadcasting, streaming.

• Stand-alone server, a server on a Windows network that neither belongs to nor governs a Windows domain

• Web server, a server that HTTP clients connect to in order to send commands and receive responses along with data contents
II. Problem

Almost the entire structure of the Internet is based upon a client–server model. High-level root name servers, DNS, and routers direct the traffic on the internet. There are millions of servers connected to the Internet, running continuously throughout the world.

- World Wide Web
- Domain Name System
- E-mail
- FTP file transfer
- Chat and instant messaging
- Voice communication
- Streaming audio and video
- Online gaming
- Database servers

Servers are not safe. They can be attacked by attackers. Some times they are called as Hackers. In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground and is now a known community. While other uses of the word hacker exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks, they are rarely used in mainstream context. They are subject to the long standing hacker definition controversy about the true meaning of the term hacker. In this controversy, the term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a cracker, not making a difference between computer criminals (black hats) and computer security experts (white hats). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.

III. Focus Areas

One generic attack approach is the distributed denial of service (DDoS) attack as shown in Figure. 1 and 2. In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. DoS they say is a tool for registering dissent. Richard Stallman has stated that DoS is a form of ‘Internet Street Protests’. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the Internet Architecture Board’s Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

IV. Analysis

Because of attacks there is lot problems related. Attackers can know everything that is related to server. There are lot of testimonials related to attacks.

A typical approach in an attack on Internet-connected system is:

- Network enumeration: Discovering information about the intended target.
- Vulnerability analysis: Identifying potential ways of attack.
- Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

V. Solution

There are several ways to prevention and detection of DDoS.

- Intrusion detection and prevention systems can help detect a DDoS and take prevention measures
- Start dropping traffic faster
- Take server offline briefly to recover from attackers
- Rotate IP address to deflect attackers
- Many “Smart Borders” (e.g., firewalls, proxy servers) have built-in DDoS detection/ prevention/ mitigation capabilities
A. Techniques

1. Vulnerability Scanner
A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are “open” or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

2. Packet Sniffer
A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

3. Spoofing Attack (Phishing)
A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

4. Social Engineering
When a hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers, who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system. Hackers who use this technique have to be quite savvy and choose the words they use carefully, in order to trick the system administrator into giving them information. In some cases only an employed help desk user will answer the phone and they are generally easy to trick. Another typical hacker approach is for the hacker to act like a very angry supervisor and when his/her authority is questioned they will threaten the help desk user with their job. Social engineering is very effective because users are the most vulnerable part of an organization. All the security devices and programs in the world won’t keep an organization safe if an employee gives away a password. Black hat hackers take advantage of this fact. Social engineering can also be broken down into four sub-groups. These are intimidation, helpfulness, technical, and name-dropping:
   - Intimidation-As stated above, with the angry supervisor, the hacker attacks the person who answers the phone with threats to their job. Many people at this point will accept that the hacker is a supervisor and give them the needed information.
   - Helpfulness-Opposite to intimidation, helpfulness is taking advantage of a person’s natural instinct to help someone with a problem. The hacker will not get angry and instead act very distressed and concerned. The help desk is the most vulnerable to this type of social engineering, because it generally has the authority to change or reset passwords, which is exactly what the hacker needs.
   - Name-dropping-Simply put, the hacker uses the names of advanced users as “key words”, and gets the person who answers the phone to believe that they are part of the company because of this. Some information, like web page ownership, can be obtained easily on the web. Other information such as president and vice president names might have to be obtained via dumpster diving.
   - Technical-Using technology is also a great way to get information. A hacker can send a fax or an email to a legitimate user in hopes to get a response containing vital information. Many times the hacker will act like he/she is involved with law enforcement and needs certain data for record keeping purposes or investigations.

5. Trojan Horses
A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with the conceptually similar function of deceiving defenders into bringing an intruder inside.)

6. Computer Virus
A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes, most computer viruses are considered malicious.

7. Computer Worm
Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not
need to attach itself to an existing program. Many people conflate the terms “virus” and “worm”, using them both to describe any self-propagating program.

8. Key loggers
A key logger is a tool designed to record (“log”) every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user’s password or other private data. Some key loggers use virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a key logger on a computer used at a point of sale and data collected by the key logger could be used for catching employee fraud.

Social Engineering attacks
Stopping social engineering attacks is difficult. Users tend to trust technologies they’re familiar with, and it takes a very strong and deliberate education effort to make them a bit paranoid about those. Maintaining that level of paranoia over the long term can be very difficult for many non-technical users.

Example mobile sms- In USA, some users receive sms as shown in fig. 3.

This message is intended to get user personal information. Based on email they gather information and attack on web server. Sometimes personal websites are not exempted.

When you on your server you cannot even know about the attacker. Behind the screen he/she attempt to steal your information.

One of reasons social engineering can be so effective is that it allows attackers to bypass many of our defenses. Most networks are built with implicit levels of trust for our own users, and we tend to protect primarily against external threats as fig. 4. Social Engineering turns our trusted users into attack vectors.

VI. Key Areas to Protect
Any public facing service such as mail servers, web servers and so forth. Any significant data repository such as database servers, file servers, and so on. Assign a risk level to each major asset, and design specific levels of protection for each risk level.

Protect against Attacks:
DDoS primarily focuses on public facing assets. Any major or complicated software is an attack point, since attackers to exploit known vulnerabilities. Keep your software patched. Running outdated or unsupported software is a major security risk and possibly the most common entry point for attackers.

A. The “Consumerization” of IT
This is a major reason why companies become concerned when users start utilizing external public services in lieu of IT provided equivalents. E.g., using drop box instead of corporate web server to provide the same levels of protection. On the other hand it might provide better, since public services are often engineered on vastly greater scales. It’s always worth looking at, rather than just rejecting out of hand.

VII. Solutions
- High-end firewall
- Leveled Layers
1. High-end Firewall
High-end Firewall means blocking unwanted traffic as shown in fig. 5. Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. The security of HTTPS is therefore the one of the underlying TLS, which uses long term public and secret keys to exchange a short term session key to encrypt the data flow between client and server. An important property in this context is perfect forward secrecy (PFS), so the short term session key cannot be derived from the long term asymmetric secret key, however PFS is not widely adopted.

A site must be completely hosted over HTTPS, without having some of its contents loaded over HTTP, or the user will be vulnerable to some attacks and surveillance. For example, having scripts etc. loaded insecurely on an HTTPS page makes the user vulnerable to attacks. Also having only a certain page that contains sensitive information (such as a log-in page) of a website loaded over HTTPS, while having the rest of the website loaded over plain HTTP will expose the user to attacks. On a site that has sensitive information somewhere on it, every time that site is accessed with HTTP instead of HTTPS, the user and the session will get exposed. Similarly, cookies on a site served through HTTPS have to have the secure attribute enabled.

2. Leveled Layers
More layers you have hard time to attackers. Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term “packet filter” originated in the context of BSD operating systems.

A. Steps to Avoid Attackers to Hack
1. Follow forums. It is always a good idea to follow hacking forums as you will be able to pick up on all the latest methods being used. A good ethical hacking forum can be found at http://zero-security.org
2. Change default password immediately. Some software has built-in password to allow the first log in after installation; it is extremely unwise to leave it unchanged.
3. Identify entry points. Install proper scanning software programs to identify all entry points from the internet into the internal network of the company. Any attack to the network needs to start from these points. Identifying these entry points, however is not at all an easy task. It is better to take the help of skilled ethical hackers who have taken special network security training to perform this task successfully.
4. Perform attack and penetration tests. By running the attack and penetration tests, you can identify those vulnerable points in the network that can be easily accessed from both external and internal users. After identifying these points, you would be able to thwart attacks from external sources and correct the pitfalls that could become the entry points for intruders to hack into your network. The test must be done from both the internal as well as external perspectives to detect all the vulnerable points.
5. Make user-awareness campaigns. All possible steps must be taken to make all the users of the network aware of the pitfalls of security and the necessary security practices to minimize these risks. You can conduct the social-engineering tests to determine the user awareness. Until all the users are aware of certain factors related to the network, protection cannot be carried out in the true sense of the term.
6. Configure firewalls. A firewall if not configured properly can act like an open door for any intruder. Hence it is vitally important to set the rules to allow traffic through the firewall that is important to the business. A firewall must have its own configurations depending upon the security aspect of your organization. From time to time proper analysis of the composition and nature of the traffic itself is also necessary to maintain security.
7. Implement and use password policies. Use strong password policies by having passwords of seven characters which are of secure length and relatively easy to remember. Passwords must be changed in every 60 days. The password should also be made up of both alpha and numeric characters to make it more unique.
8. Use passwordless authentication. Regardless of the policies above, passwords are less secure than SSH or VPN keys so think about using these or similar technologies instead. Where possible, use smart cards and other advanced methods.
9. Delete comments in website source code. Comments used in source code may contain indirect information that can help to crack the site, sometimes even usernames and passwords. All the comments in source code that look inaccessible to external users should also be removed as there are some techniques to view the source code of nearly all web applications.
10. Remove unnecessary services from devices. You will not be dependent on reliability of the modules you actually do not use.
11. Remove default, test and example pages and applications that usually come with web server software. They may be a weak point to attack and as they are the same in many system the cracking experience can be easily reused.
12. Install anti-virus software. Both intrusion detection systems and anti-virus software must be updated regularly and if possible on a daily basis. The updated version of anti-virus software is necessary as it helps in detecting even the latest virus.
13. Ensure physical security. Apart from ensuring the internal security of the network, you need to think about the physical security of your organization. Until and unless your organization has full security, any intruder can simply walk in your office premises to gain whatever information he wants. Hence with technical security, you must also ensure that the physical security mechanisms of your organization are fully functional and effective.

VII. Conclusion
Attackers can attack you organization or personal computer and steal valuable information. Attackers are sometimes called as black hats whose do illegal operations. White hats are opposite to black hats. Attackers watch your network or a system often to attack. If they get any chance to enter your network, you cannot stop them. They can steal your value information and sometimes they can threaten or blackmail you. They inject new virus. It is better to avoid such attackers by taking various measurements as mentioned in above paper. There are lots of things to be done under research.
References


