**ST. THOMAS’ COLLEGE OF ENGINEERING AND TECHNOLOGY**



CYBER LAW AND SECURITY POLICY

CS802B (8009)

Term Paper on:

PROXY SERVERS, PASSWORD CHECKING AND RANDOM CHECKING

Prepared by Group 2

Members:

Sulagna Bhattacharyya(Roll No. 10)

Ayan Bhunia(Roll No. 12)

Shreeja Biswas(Roll No. 13)

Deepanjan Bose(Roll No. 14)

Ishika Chakraborti(Roll No. 15)

Agniva Chakraborty(Roll No. 16)

Saptarshi Chakraborty(Roll No. 19)

Swarnava Chakraborty(Roll No. 20)

**ABSTRACT**

Cyber crime is a serious offence and it is not rare when people fall victims to such cases. As much as the cyber space is meant to make things easier for us, it also makes us vulnerable to notorious attacks. As a result, it is imperative to adopt tools that help prevent cyber crimes. A proxy server is a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network. Password checking on the other hand refers to programs that help in verifying any password integrity and prevent password cracking.

**CONTENTS**

**INTRODUCTION**

Cyber crimes are nothing new. They can get vicious and people have a lot to lose under such attacks. The Internet is filled with users always looking out to resort to these crimes. Network attack incidents reveal that attackers are often very systematic in launching their attacks. The basic stages of how an attacker can compromise a network are as follows-

Initial Uncovering- Two steps are involved here. In the first step called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means – searching the information about the target on the Internet by searching for social networking websites and people finder websites.

Network probe- At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a “ping sweep” of the network IP addresses is performed to seek out potential targets, and then a “port scanning” tool.

Crossing the line toward electronic crime (E-crime)- Now the attacker is toward committing what is technically a “computer crime.” He/she does this by exploiting possible holes on the target system.

Capturing the network- At this stage, the attacker attempts to “own” the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack.

Grab the data- Now that the attacker has “captured the network” he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface web pages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.

Covering tracks- This is the last step in any cyber-attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

Thus it is necessary that we resort to tools that help us protect ourselves from such attacks. Some common tools include proxy servers, password checking, random checking etc.

**PROXY SERVERS**

**What is a proxy server?**

A proxy server is a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall. The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the user. All requests to the Internet go to the proxy server first, which evaluates the request and forwards it to the Internet. Likewise, responses come back to the proxy server and then to the user.

**Proxy servers and their role in Network Security**

Proxies provide a valuable layer of security for your computer. They can be set up as web filters or firewalls, protecting your computer from internet threats like malware. This extra security is also valuable when coupled with a [secure web gateway](https://www.fortinet.com/products/secure-web-gateway) or other [email security](https://www.fortinet.com/products/email-security) products. This way, you can filter traffic according to its level of safety or how much traffic, your network—or individual computers—can handle.

Some people use proxies for personal purposes, such as hiding their location while watching movies online. For a company, however, they can be used to accomplish several key tasks such as:

* Improve security
* Secure employees’ internet activity from people trying to snoop on them
* Balance internet traffic to prevent crashes
* Control the websites employees access
* Save bandwidth by caching files or compressing incoming traffic

**How do proxy servers work?**

A proxy server performs the function of a firewall and filter. The end-user or a network administrator can choose a proxy designed to protect data and privacy. This examines the data going in and out of your computer or network. It then applies rules to prevent you from having to expose your digital address to the world. Only the proxy’s IP address is seen by hackers or other bad actors. Without your personal IP address, people on the internet do not have direct access to your personal data, schedules, apps, or files.

With it in place, web requests go to the proxy, which then reaches out and gets what you want from the internet. If the server has encryption capabilities, passwords and other personal data get an extra tier of protection.

**Benefits of using a proxy server**

* **Enhanced security**: Can act like a firewall between your system and the internet. Without them, hackers have easy access to your IP address, which they can use to infiltrate your computer or network.
* **Private browsing, watching, listening, and shopping**: Use different proxies to help you avoid getting inundated with unwanted ads or the collection of IP-specific data.
* **Access to location-specific content**: You can designate a proxy server with an address associated with another country. You can, in effect, make it look like you are in that country and gain full access to all the content computers in that country are allowed to interact with

.

* **Prevent employees from browsing inappropriate or distracting sites**: You can use it to block access to websites that run contrary to your organization’s principles. Also, you can block sites that typically end up distracting employees from important tasks. Some organizations block social media sites like Facebook and others to remove time-wasting temptations.

**Types of proxy servers**

**Forward Proxy**- A forward proxy sits in front of clients and is used to get data to groups of users within an internal network. When a request is sent, the proxy server examines it to decide whether it should proceed with making a connection.

**Transparent Proxy**- A transparent proxy can give users an experience identical to what they would have if they were using their home computer. In that way, it is “transparent.” They can also be “forced” on users, meaning they are connected without knowing it.

**Anonymous Proxy**- An anonymous proxy focuses on making internet activity untraceable. It works by accessing the internet on behalf of the user while hiding their identity and computer information.

**High Anonymity Proxy**- A high anonymity proxy is an anonymous proxy that takes anonymity one step further. It works by erasing your information before the proxy attempts to connect to the target site.

**Distorting Proxy**- A distorting proxy identifies itself as a proxy to a website but hides its own identity. It does this by changing its IP address to an incorrect one.

**Data Center Proxy**- Data center proxies are not affiliated with an internet service provider (ISP) but are provided by another corporation through a data center. The proxy server exists in a physical data center, and the user’s requests are routed through that server.

**Residential Proxy**- A residential proxy gives you an IP address that belongs to a specific, physical device. All requests are then channeled through that device.

**Public Proxy**- A public proxy is accessible by anyone free of charge. It works by giving users access to its IP address, hiding their identity as they visit sites.

**Shared Proxy**- Shared proxies are used by more than one user at once. They give you access to an IP address that may be shared by other people, and then you can surf the internet while appearing to browse from a location of your choice.

**SSL Proxy**- A secure sockets layer (SSL) proxy provides decryption between the client and the server. As the data is encrypted in both directions, the proxy hides its existence from both the client and the server.

**Rotating Proxy**- A rotating proxy assigns a different IP address to each user that connects to it. As users connect, they are given an address that is unique from the device that connected before it.

**Reverse Proxy**- Unlike a forward proxy, which sits in front of clients, a reverse proxy is positioned in front of web servers and forwards requests from a browser to the web servers. It works by intercepting requests from the user at the network edge of the web server. It then sends the requests to and receives replies from the origin server.

**How to obtain a proxy server?**

There are hardware and software versions. Hardware solutions sit between your network and the internet, where they get, send, and forward data from the web. Software proxies are typically hosted by a provider or reside in the cloud. You install an app on your computer that facilitates interaction with the proxy. Often, a software proxy can be obtained for a monthly fee. Sometimes, they are free. The free versions tend to offer users fewer addresses and may only cover a few devices, while the paid proxies can meet the demands of a business with many devices.

**PASSWORD CHECKING**

**What is password checking?**

Passwords are surprisingly easy to crack, particularly if the person attempting to crack the password has physical access to the system. One might think that matching a password to a dictionary of words might take a long time, but it doesn't. This is why it is imperative to have programs that can help users verify the integrity of their passwords and set so accordingly. This process is known as password checking.

**How are passwords easily cracked?**

Tools exist that take dictionaries and apply a set of rules to the words to create a match table that dramatically reduces the time required to break the password by simple brute force matching. Dictionary programs like Crack 5 or Jack the Ripper look for passwords that do things like reverse a word, change cases, replace or insert characters, and so on. L0phtCrack is the most widely used Windows cracking tool.

Given the enormous processing power even individual computers have, the speed with which a password can be broken depends on how strong the password is. If one has a PC that can perform 100,000 encryption operations per second (reasonable for a fast PC) a password composed of only the 26 lower case letters would take the following amount of time on average to crack: 3 letters; 0.18 seconds; 6 letters, 51.5 minutes; 7, 22.3 hours; 8, 24.2 days; 9 characters, 1.72 years, 10, 44.8 years; 11, 11.6 centuries, and 12 letters, 30.3 millennia. It's faster still when you can put a DVD disk with millions of string combinations to use.

**What can general users do to set strong passwords?**

When we add digits, casing, and symbols from the ASCII character set these times go up dramatically. A good goal is to find a password that takes 4 years to crack, and you can achieve this by making sure that a password of 8 characters or more has one of each of these types as in the password "S0s1nsky?" That's why many security conscious programs insist on eight letter passwords, and will often show you how secure a password is in a bar graph. Those ratings are based on the rules measuring the average cracking time (approximately).

**Using password cracking tools to our advantage**

As a network administrator one can use password cracking tools to your advantage. When considering a new password, or just to test existing ones he/she can use something like L0phtCrack to test the password to see how long it takes to crack it. There are several places we can download the program which sells an administrator's version of this program that will allow you to test and recover both Windows and UNIX account passwords from a precompiled table of trillions of passwords. We can use this tool to recover lost passwords, as well as run risk assessment reports to find and eliminate risky passwords.

**REFERENCES**

* Nina Godbole & Sunit Belapure “Cyber Security”, Wiley India, 2012
* https://www.pcmag.com/encyclopedia/term/proxy-server
* https://www.fortinet.com/resources/cyberglossary/proxy-server
* https://searchnetworking.techtarget.com/tip/Password-checking