# Deceiving Brute Force Attack

[1]Dr. M. Thangavel, [2]Dr. G. Lalli, [3]Dr. J. Vandarkuzhali, [4]Ms. K. S. Saratha,

*[1] Professor, [2]Assistant Professor (Sl.G.-II), [3]Assistant Professor (Sl.G.-I), [4]Assistant Professor,*
*Department of Computer Applications, Erode Sengunthar Engineering College,*
*Thudupathi, Perundurai, Erode-638 057, India.*

**ABSTRACT**

*The "DECEIVING BRUTE FORCE ATTACK" includes the password listening mechanism which listen the hackers intruding to the application. Suppose, if the user enters a password, which nearly match the original password, then the user is allowed to enter into the application but the details displayed are fake. The video taken captured from various areas and displayed in the user administration system. The administrator login the application using authorized username and password. If the hacker is using anagram logic in the application the video information available to the user (intruder) is fake or old data.*

*This will help in deceiving the intruder. The password is given by the user matches if the characters are front and back in position. For example, the character 'a' and 'c' is valid for 'b', 'y' and 'a' for the character 'z'. The administrator is alerted if the intruder user is accessing the site. After the intruder is entering the application, the desktop is taken as snapshot and saved into database so that the administrator views the intruder activity. The administrator can able to know the hacker details in the application which is viewed by the anagram logic.*

***Keywords:***

*Brute Force Attack, Intruder Activity, Anagram Logic.*

## 1. INTRODUCTION

Major security threats to networked computer systems appear to be reaching crisis proportions in recent years. For example, Barracuda Networks, a major supplier of email and Web security appliances, estimates that spam email accounted for between 90 and 95 percent of all email sent during 2007. In addition, new phishing attacks increased by 18% during the first half of 2007, and by the final quarter of last year phishing incidents accounted for nearly 60% of all security incidents reported. Commercial malware kits such as MPack, including maintenance and support agreements for client hackers, are now being offered for sale on the Internet for as little as $500. These trends have continued to grow since Bruce Schneier told the audience at the Hack in the Box Security Conference in Kuala Lumpur, Malaysia that in his estimation the security war was being lost.

Perhaps the single biggest security threat for networked systems going forward is represented by botnets, defined as collections of compromised computer systems used for a variety of criminal activities, including distributed denial-of-service attacks, spamming, traffic sniffing, keylogging, identity theft, and click fraud. The most highly publicized botnet of 2007 was the Storm worm botnet, which is estimated to control as many as 50 million computers.

For most of the recorded history of botnets, dating back to 1999, the robot computers, or zombies, that populate them have been understood to consist primarily of compromised systems running a version of the Microsoft Windows operating system. Propagation of zombie code has been observed to occur through a number of Windows-specific worms, viruses, Trojans, and other forms of malware. More recently, vulnerabilities in Linux machines are being recognized as an important part of the problem. In October 2007 Dave Cullinane, chief information and security officer at eBay, announced at the Trust Online conference that an internal investigation of the security threats faced by the online auction service had been traced to "rootkitted Linux boxes." Alfred Huger, vice president for Symantec Security Response, echoed Cullinane's comments, saying that compromised Linux machines were frequently observed to make up a large portion of the command and control networks for botnets.

While it is true that computers running Linux are not subject to the many worms, viruses, and other malware that target Windows platforms, the Linux platform is known to be vulnerable to other forms of exploitation. A 2004 study conducted by the Londonbased security analysis and consulting firm mi2g found that Linux systems accounted for 65% of "digital breaches" recorded during the twelve-month period ending in October 2004.

Recent studies of vulnerability trends point to two primary attack vectors: brute-force attacks against remote services such as SSH, FTP, and telnet, and Web application vulnerabilities. In its Top-20 2007 Security Risks report, the SANS Institute called brute-force password guessing attacks against SSH, FTP and telnet servers "the

most common form of attack to compromise servers facing the Internet." The report notes that unpatched flaws such as buffer overflow vulnerabilities in the authentication functions of these services can allow arbitrary code execution; however, the report also points up a much more mundane threat. Weak passwords are specifically identified as a potential Achilles heel in these systems, since "brute forcing passwords can be a used as a technique to compromise even a fully patched system."

In this paper, we focus specifically on brute-force SSH attacks. In particular, we analyze data collected from a large number of SSH brute-force attacks against Linux systems connected to different kinds of networks. We discuss patterns in the passwords used in these attacks, as well as the methods employed. We also use the data we collected to evaluate the effectiveness of various countermeasures that have been suggested for protecting systems against SSH brute-force attacks.

## 2. PROJECT OVERVIEW

The beginning process in the application is the admin page which is used to view the monitored video file is the same application. The admin can login the application using authorized username and password. The admin have multiple login process, one is used to view the captured video file another one is viewing intruder details.

In the admin login phase, the administrator is used to see the hacker details such as entry time of the intruder, IP address of the intruder, system name of the intruder, viewed video file details. Those details are fetched from the database and viewed in the grid view control.

The intruder page is which is accessing by unwanted person of hacker. The intruder access the application by wrong password. The password should be in the anagram result. Example if the user name is "admin" anagram password is "benjo", "zcljo".

The login is the main process in the application. The administrator and intruder can login application using authorized password and anagram manner password. The receiver login phase is used to view the monitoring video stream in the media player control.

## 3. ADVANTAGE

- The intruder login means to view the fake video file
- The intruder has possible chance to guess the admin password
- To view multiple video files in same time in the single form
- Administrator can view the hacker file accessed details
- Time and viewed file details are easily taken
- User friendly application
- Well secured process

## 4. CONCLUSIONS

The armies of compromised computer robots, known as botnets, have received a lot of attention over the past few years. To date, most of that attention has been focused on the compromised Windows machines thought to populate the ranks of botnet armies. Until the results of eBay's recent study of internal security threats were publicized last fall, little attention was paid to the role compromised Linux systems might play in supporting botnets.

Compared with systems running the Windows operating system, Linux systems face a unique threat of compromise from brute force attacks against SSH servers that may be running without the knowledge of system owners/operators. Many Linux distributions install the SSH service by default, some without the benefit of an effective firewall. Thus, otherwise conscientious system administrators who keep their systems fully patched may fall prey to a system compromise caused by a carelessly chosen password.

As our study results show, not all vulnerable passwords can be considered weak, based on commonly-held beliefs of password strength. Attackers are using and sharing attack dictionaries of username/password pairs that incorporate a significant percentage of apparently strong passwords. Using a password checking tool, especially one that restricts systematic approaches to password selection, can provide an extra measure of protection against malicious login traffic, especially when combined with other protective measures designed to reduce the visibility of Internet facing servers.

## 5. REFERENCES

1) E. Alata, V. Nicomette, M. Kaaniche, M. Dacier, M. Herrb. "Lessons learned from the deployment of a high-interaction honeypot", in Proc. Dependable Computing Conference (EDCC06), Coimbra, Portugal, October 18-20, 2006, pp. 39 - 46.
2) Barracuda Networks. December 12, 2007. Barracuda Networks Releases Annual Spam Report. Available at: http://www.barracudanetworks.com/ns/news_and_events/ind ex.php?nid=232.
3) Canavan, J. 2005. White Paper: Symantec Security Response; The Evolution of Malicious IRC Bots. Available at: http://www.symantec.com/avcenter/reference/the. evolution.of.malicious.irc.bots.pdf.
4) Christey, S & Martin, R. May 22, 2007. Common Weakness Enumeration. Vulnerability Type Distributions in CVE. Available at: http://cwe.mitre.org/ documents/ vulntrends/index.html.
5) Gaudin, S. September 6, 2007. InformationWeek. Storm Worm Botnet More Powerful Than Top Supercomputers.

Available at: http://www.informationweek.com/news/showArticle.jhtml?articleID=201804528.
6) Hochmuth, P. November 11, 2004. LinuxWorld. Linux is 'most breached' OS on the Net, security research firm says. Available at: http://www.linuxworld.com.au/index.php/id; 188808220;fp;2;fpid;1.
7) The Honeynet Project and Research Alliance. Know Your Enemy, Tracking Botnets. http://honeynet.org/papers/bots, March 2005.
8) http://www.microsoft.com/protect/yourself/password/checker .mspx.