International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Shellshock Attack on Linux Systems – Bash

A. Caroline Mary

[1] *Assistant Professor, Department of Computer Technology, Sri Krishna Arts and Science College, Tamilnadu, India*

Abstract - ***In this paper, threat to Network Security is discussed. One of the prime attacks on recent days "Shell Shock Attack "is explained in a deeper way. It's important to protect our data in the Network; precautions should be taken to protect our data, so that attackers would not find it easy to steal important data. Possible attacks on Network are denial of service, man in the middle, modification of data etc. Bugs in famous / most used shell causes adverse effects. Here Bash shell is considered, where Shellshock attack causes unauthenticated users to add their malfunctioning codes, which depicts the system behavior in a problematic way. There is a necessary for us to prevent unauthorized access to computer systems. Shell is responsible for executing the user commands. Vulnerabilities in shell, leads to execution of codes which are not appropriate. Bash was found to have remote code execution vulnerability, the Security Research and Emergency Response Center of Antiy Labs (Antiy CERT) determined according to the information at the first time(sep 2014). Shell is a command interpreter, which helps us to find out the respective program and execution of the particular command. Threat to data and malfunctioning of system are deeper issues, which acts as a prime attack on Network Security. Bash is the most common among Linux Shells. This vulnerability in bash will have serious effects.***

Key Words: *Shell , Shellshock, Unauthorized access*

1. INTRODUCTION

Viruses, worms are the most common problems that would affect the security of Network. In recent time's encryption of data have become a most common method to protect our data. But the point is the algorithm should be efficient enough to handle issues. Steganography was a possible technique to protect data by hiding the valuable data under an image. This makes hackers job even more difficult, as he will not be aware of data transfer. Firewalls help us to prohibit attacks. Phishing attacks for example act like a real website and capture private information from the customers. Brute force attacks, try all possible combination of characters to find out the password.

Though Security is concentrated to a greater extent, there exists attack on Network. One such attack is the shell shock attack, which mainly targets UNIX/LINUX machines.

1.1 History of Network Security

The need for Network Security aroused because of the loss based because of the attack on Network . Millions of amount are at risk , and events such as loss of 80 million are the basics for interest on Network Security. Providing safety to the confidential data to safeguard our money is a primitive task. Public networks are being relied upon to deliver financial and personal information. The growth of Internet has forced the growth of Network Security. Due to offense, many companies emphasized security for the intellectual property.

1.2 TYPES OF ATTACKS

CLOSE-IN ATTACK

In these sort of attacks, Person try to come close to network , systems to gather the data. Possible attacks are modifying the data, denial of service. N Number of tricks are followed by the hackers / attackers to gather confidential information. They try to socialize with persons to collect information, through any sort of communication.

HIJACK ATTACK

Here hacker take measures to take over the session. We might believe that we are interacting with the real person. In such a way our data will be acquired by the hackers.

PHISHING ATTACK

Here the hacker creates a fake website. When user uses this site, his information are got. Eg. Bank website, when customers uses this site to login , his username and password in formations are acquired by the hacker. content here.

SPOOF ATTACK

Our data get transferred in the form of Packets. In this form of attacks , the hacker might change the source

address in the packet. So we might come to a conclusion that packet comes from someone else.

BUFFER OVERFLOW

Buffer overflow A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt.

EXPLOIT ATTACK

When a hacker is aware of the security holes in our system. He can easily intrude in to our system.

PASSWORD ATTACK

Password is one of the most confidential data. Hackers try all means to find out the password. So it is advised to change the passwords often and to not write it anywhere. Brute force attacks are possible to find out the password. Brute force in the sense trying out all possible combination to find out the password

2. BASICS

2.1 Shell

Shell is a command Interpreter. When we enter a command on the terminal, it's the responsibility of Shell to execute the command. Shell reads the command line and takes the argument 0 as command.

Example cp a.txt b.txt. Here cp is the command,

which means copy. Shell searches for the file which has to be executed to copy the contents. If the file is not found, it just displays that "File not found". If a file name as "cp" exists, shell helps in executing the command. Thus the Job is done. N number of shells are available. The common ones are Bash , Z , X Shell.. Bash is a *nix shell or in other words, an interpreter that allows you to orchestrate commands on Unix and Linux systems, typically by connecting over SSH or Telnet. It can also operate as a parser for CGI scripts on a web server such as we'd typically see running on Apache. It's been around since the late 80s where it evolved from earlier shell implementations (the name is derived from the Bourne shell) and is enormously popular.

Commands should be followed by $ sign. $ Symbol means that the shell is ready to accept commands. After the processing of command, $ "shell prompt "will be displayed. To find out the shell, ps command can be used. Example,

$ ps -p $$.

Output:

PID TTY TIME CMD

5866 PTS/0 00:00:00 BASH

There are other shells out there for Unix variants, the thing about Bash though is that it's the default shell for Linux and Mac OS X which are obviously extremely prevalent operating systems. Bash is the Shell which is installed on most of the machines. So vulnerability in bash is a major Issue.

2.2 SHELLSHOCK ATTACK

Especially it makes use of the vulnerability in bash shell. Shell is used to execute commands in Unix/Linux. Shell acts as a command language interpreter. Shellshock may even affect the most recent versions of bash shell. It is also known as the bash bug. It allows an attacker to gain control over the computer. One type of variables in bash is the Environmental variables. Vulnerability in bash is gained through this environmental variable. Though certain conditions has to be met for the shellshock to play its role, once its successful attacker can gain control. Generally the code inside the function will have problem in execution. Whereas here code outside the curly braces are executed, resulting in issues. Bash bug CVE-2014-6271, which causes unnecessary code to be executed.

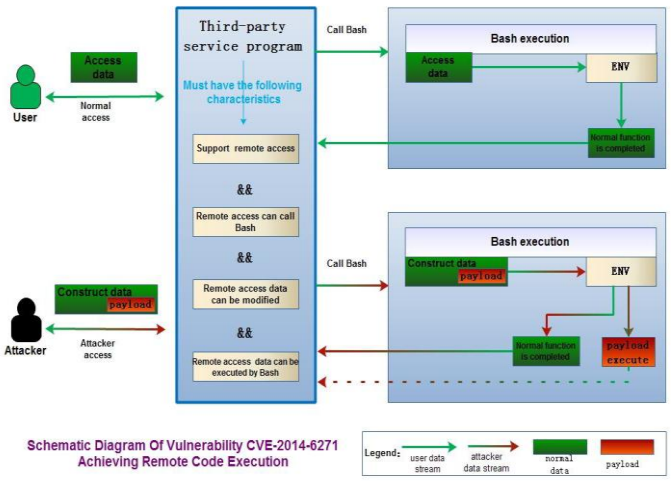

Fig 1 – Vulnerability in Shell

2.3 EFFECTS ON SUCCESSFUL EXPLOITATION

If there is a successful exploitation, the issue might be

quite serious. The attackers might be given a chance to attack other computers on the network. Attacker can also send a malicious command to the router. Bash will run the malicious command first. Successful exploitation could lead to remote code execution.

2.4. VULNERABILITY

Let us consider an example to explain the vulnerability in bash shell.

env ENV_VAR_FN='() { <your function> };'

Bash reads beyond the function definition and executes the command. It should have ignored after the function, but it reads beyond the function which might lead to problems. An attacker can add some Bash commands onto the end of the auto-imported function

Eg. env ENV_VAR_FN='() { <your function> }; <attacker code here>'

As the attackers code is also executed by bash shell , any sort of malfunctioning can be made possible by the hacker. Bash environment can be used in ssh, rlogin etc.. So there is a possibility for it to attack over the network.

Diagnostic Steps:

To find out whether Bash shell has vulnerability this method can be made use of. t to help confirm if a system is patched against to the Shellshock vulnerability.

To manually test, this code can be made use of.

```
$ env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c "echo test"
```

If the output of the above command contains a line containing only the word "vulnerable" , then it depicts that we are using vulnerable bash shell , which has to be replaced or corrected to overcome unnecessary execution of coding.

2.5 PROBLEMS THAT CAN BE EXPECTED

The attacker can literally run any command on his own. Attacker can steal user data from database; he can modify the contents, change access permissions on important documents etc.

Issue is especially dangerous as there are many possible ways Bash can be called by an application. Quite often if an application executes another binary, Bash is invoked to accomplish this. Because of the pervasive use of the Bash shell, this issue is quite serious and should be treated as such.

Linux is used much which holds bash shell to interpret the commands. So this is a serious issue as it can be spread throughout the network.

It's better to upgrade to latest version of bash, to avoid attackers to make use of the vulnerabilities. Malicious requests are sent to Web servers:

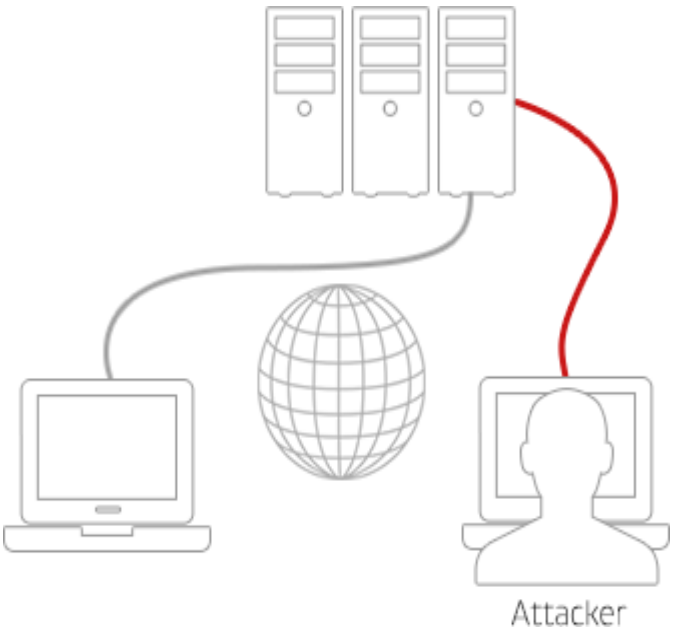

Fig 2 – Attacker access to servers

Certain Antivirus is available to deal with the issue of Shellshock. One among that is Sophos.

3 SOPHOS

Cybercrime is made possible by injecting Shellshock. To overcome this Sophos can be made use of to protect the network. Sophos protect against Shellshock attack in many ways.

Sophos Antivirus helps us to solve the issue.

Shellshock-related malware blocked by Sophos includes:

Mal/PerlBot-A

Linux/Wopbot-A

Troj/PerlShl-A

Linux/Tsunami-A

Troj/PHPFlood-A

Linux/Bdoor-BGG

OSX/Tsunami-Gen

AVG Antivirus are designed to block access to compromised sites that could be affected by Shellshock

4. CONCLUSIONS

It is important to safe guard important data. If hackers find ways to access data over Network, it would lead to serious issues. So there is a necessity for us to provide network security. ShellShock is one such attack which can be handled by antivirus like Sophos. Sophos helps us to prohibit ShellShock, to make use of the vulnerabilities of Bash Shell. Thus various steps are taken to maintain integrity and confidentiality of our data, by providing Network Security. Security never stops because the threat never stops.

REFERENCES

[1] Min-kyu Choi , Rosslin John Robles, Chang-hwa Hong2), Tai-hoon Kim1), “Wireless Network Security: Vulnerabilities, Threats and Countermeasures”, Vol. 3, No. 3, July, 2008

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008