Periodicals of Engineering and Natural Sciences ISSN: 2303-4521
Vol. 6, No. 2, December 2018, pp. 148 – 158
Available online at: *http://pen.ius.edu.ba*

Implementation of DoS and DDoS Attacks on Cloud Servers

Sefat Mahjabin
Daffodil International University, Dhaka, Bangladesh

Article Info

Article history:
Received June 18, 2018
Revised November 29, 2018
Accepted December 13, 2018

Keyword:
Cloud Computing
DoS attack
DDoS attack
Phyton Scripts

ABSTRACT

Cloud environments face many threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target. Thus the security level of data on the cloud servers is always a key issue from preventing potential attacks. This paper intends to show a relatively easy way to implement a Denial of Service (DoS) attack and/or a Distributed Denial of Service (DDoS) attack. The used Phyton scripts like HULK or XML-RPC are able to make several hundred requests to the server in short period of time. The HULK is better for DoS attack, while XML-RPC is for pure DDoS attack. It is concluded that with proper tools and applications, the access to the VM and DDoS can be implemented relatively easy way.

Corresponding Author:
Name Sefat Mahjabin
Affiliation Daffodil International University
Address Dhaka, Bangladesh
Email mahjabin248@gmail.com

1. Introduction

Cloud computing is a revolutionary concept that offers a new way to access personal data and applications, which are no longer located on the computer but in the cloud - which means that the program records and documentation can be accessed from multiple devices, anytime and from different locations. As a result, user services in the cloud can be better, faster and easier to use and modify. Unfortunately, nowadays the cloud environments face many threats as traditional corporate networks. Nevertheless, due to the vast amount of data stored on cloud servers, the providers become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. The Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are well-known. The DoS attack typically uses one computer and one internet connection to flood a targeted system or resource. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. The DDoS attacks in cloud computing are also termed as Economic Denial of Sustainability (EDoS) attacks, due to the substantial economic losses both from resource usage and business disruption. These losses are directly proportional to the downtime incurred by the attack. In recent times, cloud computing has been adopted across the globe to support the major information technology requirements of organizations from all industry sectors. As highlighted in, majority of the organizations ($>$ 87%) across the globe are using cloud infrastructure to run their mission critical applications. This adoption trend is due to the profound resources and availability of on-demand resources in the cloud. However, the emergence of cloud computing has also led to the shift of DDoS attackers more towards the cloud driven services. More than 33% of the overall reported attacks in year of 2015 were targeted towards cloud services [1]. In addition, cloud features are becoming attractive to the attackers. Most of the reported DDoS attacks usually last between few minutes to few hours and some major attacks may last few days to even weeks. A recent report on global DDoS attack reveals that close to a quarter of current DDoS attacks target the application layer, and one-fifth of the HTTP DDoS attacks are HTTP GET floods [2]. There are many recent DDoS attacks on cloud services among which the attacks on Amazon EC2 services, RackSpace and Linode are major incidents resulting into considerable service outages [3].

There are numerous interesting survey as well as research papers (e.g., [2,4–38]) available which include works

DOI: 10.21533/pen.v6i2.170

related to DDoS attacks in various networks both from the perspective of attacks and solutions. Major motivation behind DDoS attacks includes business rivalry, political ideology, and cyber war among countries. The most common outcome of DDoS attacks is unavailability of target service. The unavailability causes many short term and long term business and reputation losses, which are actually a set of consequences of the service downtime [39]. There are various ways of implementing DoS and DDoS attacks. There are also various ways of protecting servers from DoS and DDoS attacks. For examples, Lonea et al. [40] suggested a model to detect and analyze DDoS attacks in cloud computing environments using Dempster-Shafer Theory (DST) [41]. But the computational complexity [42] of DST increases exponentially with the number of elements in the frame of discernment (e.g., a mass function goes $2^n - 1$ for n elements in the state). Hiziroglu et al. [43] proposed a conceptual model of a cloud-based customer analytics tool for retail small and medium enterprises. Sabanovic et al. [44] presented a comparative analysis of data formatting technology in AMF, JSON and XML, during data transfer between client and server. Sharif et al. [45] implemented an exemplary parallelization of artificial neural network training by dint of Java and its native socket libraries. Simpson et al. [46] proposed a solution of DDoS attacks in computer networks considering an inter-domain collaboration scheme. Kolandaisamy et al. [47] suggested a multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular Ad Hoc networks. Chadd [48] described the kinds of DDoS attacks for past, present, and future. Bhardwaj et al. [49] compared single tier and three tier infrastructure designs against DDoS attacks. Swain et al. [50] presented an approach for DDoS attacks to discriminate the attack level and provided security for DDoS nodes in MANET.

This paper addresses an easy implementation of a DoS attack on servers and it shows that the cloud servers have some protection against basic attacks. When it comes to larger DDoS attacks, the virtual machine (VM) on those clouds can misbehave and fail. VM is based on computer architecture and provides functionality (e.g., [51]) of a physical computer. The protection of VM on the cloud can be provided by some software or simple blocking of the certain server connections. The blocking of those servers is very dangerous, since the block can affect some the users trying to fetch their data or trying to get response from service without intention of DoS attack. It is worth mentioning that implementations of both DoS and DDoS attacks are not so difficult but due to lack of approval from appropriate authorities, we could not implement the XML-RPC script wholly to any clouds and its VM. Thus this paper is limited to the implementation a DoS attack on servers using HTTP Unbearable Load King (HULK) script[1]. Durakovic [52] explored historical aspects of Design of Experiments (DOE) and provided state-of-the-art of DOE's applications for guiding researchers how to conceptualize, plan, conduct experiments, analyze, and interpret data. It is said that DOE was most popular tool in scientific areas of medicine, engineering, biochemistry, physics, computer science and counts about 50% of its applications compared to all other scientific areas [52]. Although recently DOE mathematical methodology is using for planning and conducting experiments as well as analyzing and interpreting data obtained from the experiments, in this paper DOE has not been considered because of widely lack of huge experimental data and proper experimental permission from appropriate authorities. Consequently, the consideration of DOE has been left for future study.

The rest of this paper is organized as follows: Section 2. delineates the implementation of DoS and DDoS attacks; Section 3. reports the empirical results and our observations; and Section 4. concludes the work with few clues for further investigation.

2. Implementation

This section briefly explains architecture of DDoS attacks and security measures against them. As a part of this paper, an experiment will briefly explain how a DDoS attacked is performed in order to fully understand what kind of process is it. After understanding DDoS, conclusions and logical solution to the problem and potential breakout will potentially arise.

2.1. DoS attack using HULK script

To implement a DDoS attack from one machine, a script can be made in various programming languages. This experiment uses Phyton as a language in which script is calling a request-response service multiple times in

[1] All experiments shown in this paper are performed legally and with proper permissions from appropriate authorities. Author of this paper is not responsible for any loss or damage made whatsoever if the experiment is repeated.

certain amount of time. The HULK script was originally developed as a proof-of-concept to illustrate how easy it is to take down a web server. The HULK script works by opening a flood of HTTP GET requests to overwhelm its target. The HULK script is unique in that every request has a random header and URL parameter value to bypass a server's caching engine. The Listing 1 demonstrates a part of HULK script which calls other methods. It executes the final attack to the servers and keeps making request-response until master machine stops it.

Listing 1. Execution process of HULK script in Python (hulk.py).

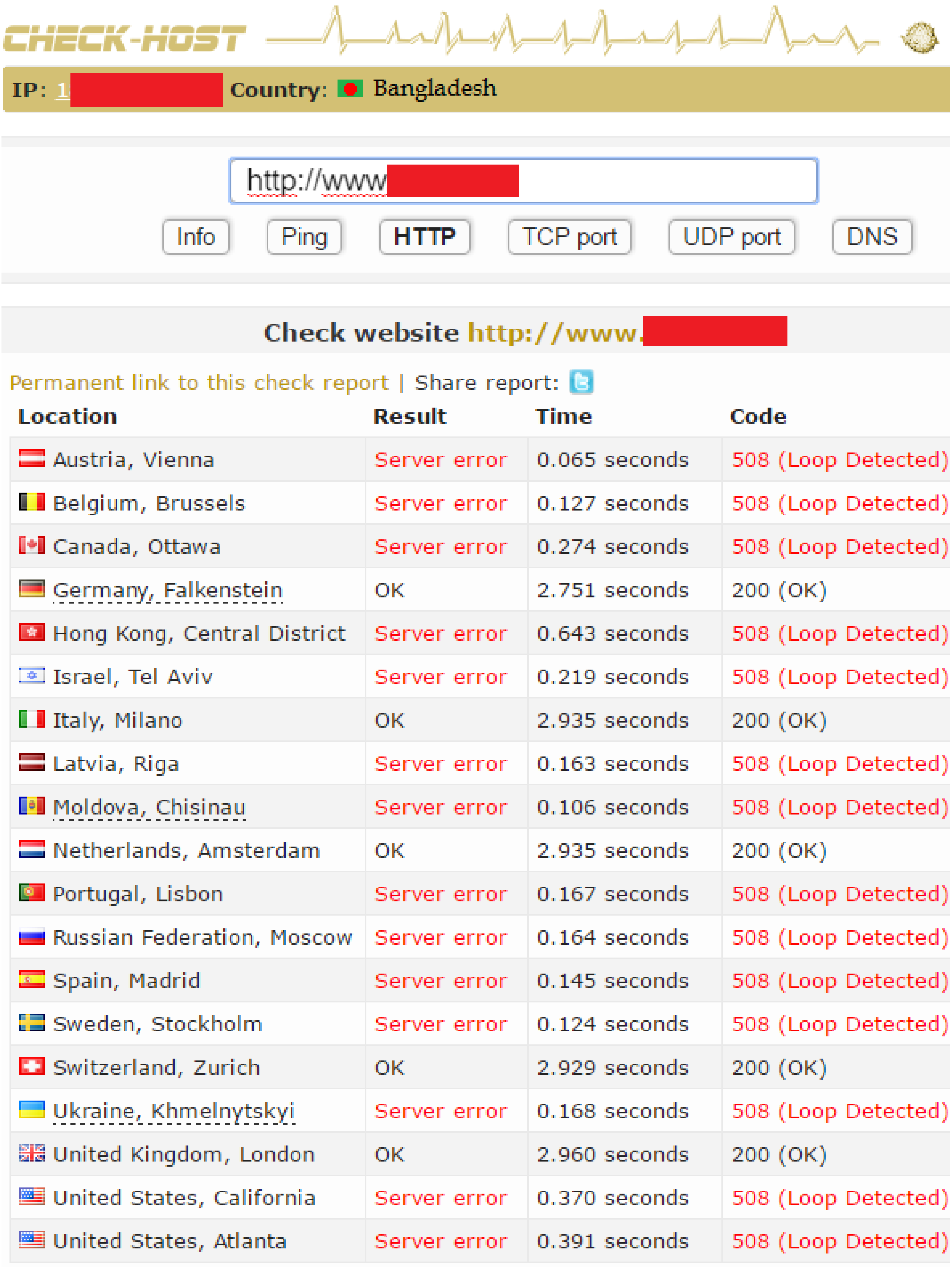
```
#execute
if len(sys.argv)<2:
          usage()
          sys.exit()
else:
    if sys.argv[1] == ”help”:
          usage()
          sys.exit()
    else:
        print(”−− HULK Attack Started −−”)
        if len(sys.argv) == 3:
            if sys.argv[2] == ”safe”:
                set_safe()
        url = sys.arg[1]
        if url.count(”/”) == 2:
               url = url + ”/”
        m = re.search(”http\://([^/]*)/?.*”,url)
        host = m.group(1)
        for i in range(500):
              t = HTTPThread()
              t.start()
        t = MonitorThread()
        t.start()
```

The targeted site was firstly checked is it responsible and does it works without any DoS attacks. The site was available for several servers. Consequently, it was ready for testing. Figure 1 represents the response from target website to host servers. All sensitive links in the images are blocked with red color for security reason. After finishing the checkup, the target has been attacked with HULK script. The HULK script that is making requests is doing *while() do* loop, which means it is attacking all the time. Figure 2 demonstrates HULK script performing in the command prompt commands. After the attack it is notable that the website is not responding. This indicates that the HULK script made out target server go down. To make sure that nobody can access the server, the check was made once more from host server list. The conclusion is that nobody can access the site anymore. Figure 3 depicts the host server list after a DoS attack.

2.2. Cloud servers with DoS attack

A cloud server is a logical (rather than a physical) server that is built, hosted, and delivered through a cloud computing platform over the internet. Billions of Internet of Things (IoT) devices are connected via internet. The IoT cloud service creates excessive communication between inexpensive sensors (e.g., [53]) in the IoT. However, the cloud servers possess and exhibit similar capabilities and functionality to a typical server. But the cloud servers are accessed remotely from a cloud service provider. The cloud server hosting services are provided by multiple connected servers that comprise a cloud. The advantages of cloud server include: (i) Onsite hardware and capital expenses are not needed; (ii) Best fit for smaller companies which would outgrow storage too quickly; (iii) The costs of the data recovery would outweigh the benefits for companies which are not as dependent on uptime and instant recovery.

It is interesting to know what happens in cloud servers with DoS attacks. The HULK script attack will be applied to several cloud servers. To understand the way how the script is attacking, an example is given hereby. As targeted site was attacked from Master PC, and then from remote server it has to go down as request from larger servers were to trying multiple times to access relatively small server. Similarly, for attacking the cloud servers, we would need a bigger amount of machines performing attack on cloud so that they will go down. Figure 4 shows how this script is unable to perform any damage to cloud servers in general. It is clear that script was not able to do anything to the clouds themselves, as the google.bd and google.com and facebook.com and



IP: 1[redacted] Country: Bangladesh

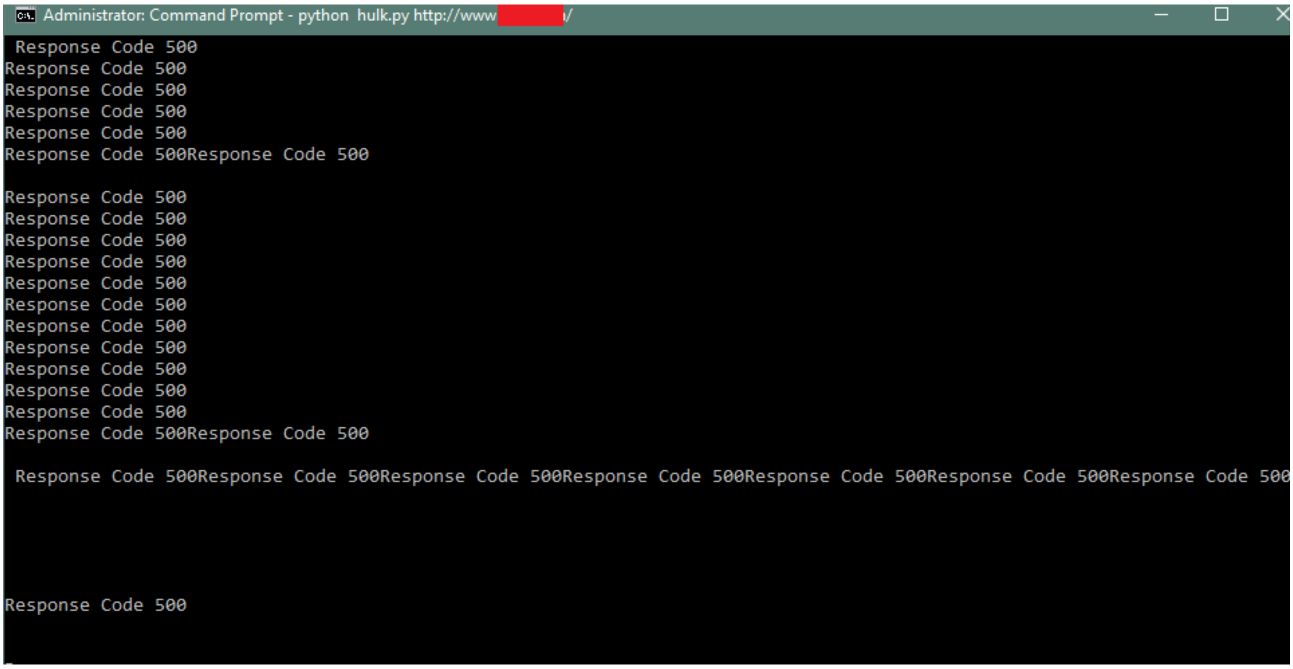
http://www[redacted]

Check website http://www.[redacted]

Permanent link to this check report | Share report:

Location	Result	Time	Code
Austria, Vienna	Server error	0.065 seconds	508 (Loop Detected)
Belgium, Brussels	Server error	0.127 seconds	508 (Loop Detected)
Canada, Ottawa	Server error	0.274 seconds	508 (Loop Detected)
Germany, Falkenstein	OK	2.751 seconds	200 (OK)
Hong Kong, Central District	Server error	0.643 seconds	508 (Loop Detected)
Israel, Tel Aviv	Server error	0.219 seconds	508 (Loop Detected)
Italy, Milano	OK	2.935 seconds	200 (OK)
Latvia, Riga	Server error	0.163 seconds	508 (Loop Detected)
Moldova, Chisinau	Server error	0.106 seconds	508 (Loop Detected)
Netherlands, Amsterdam	OK	2.935 seconds	200 (OK)
Portugal, Lisbon	Server error	0.167 seconds	508 (Loop Detected)
Russian Federation, Moscow	Server error	0.164 seconds	508 (Loop Detected)
Spain, Madrid	Server error	0.145 seconds	508 (Loop Detected)
Sweden, Stockholm	Server error	0.124 seconds	508 (Loop Detected)
Switzerland, Zurich	OK	2.929 seconds	200 (OK)
Ukraine, Khmelnytskyi	Server error	0.168 seconds	508 (Loop Detected)
United Kingdom, London	OK	2.960 seconds	200 (OK)
United States, California	Server error	0.370 seconds	508 (Loop Detected)
United States, Atlanta	Server error	0.391 seconds	508 (Loop Detected)

Figure 1. Testing target responses before a DoS attack.



```
Administrator: Command Prompt - python hulk.py http://www[redacted]/
 Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500Response Code 500

Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500
Response Code 500Response Code 500

 Response Code 500Response Code 500Response Code 500Response Code 500Response Code 500Response Code 500Response Code 50




Response Code 500
```

Figure 2. Applying HULK script for a DoS attack.

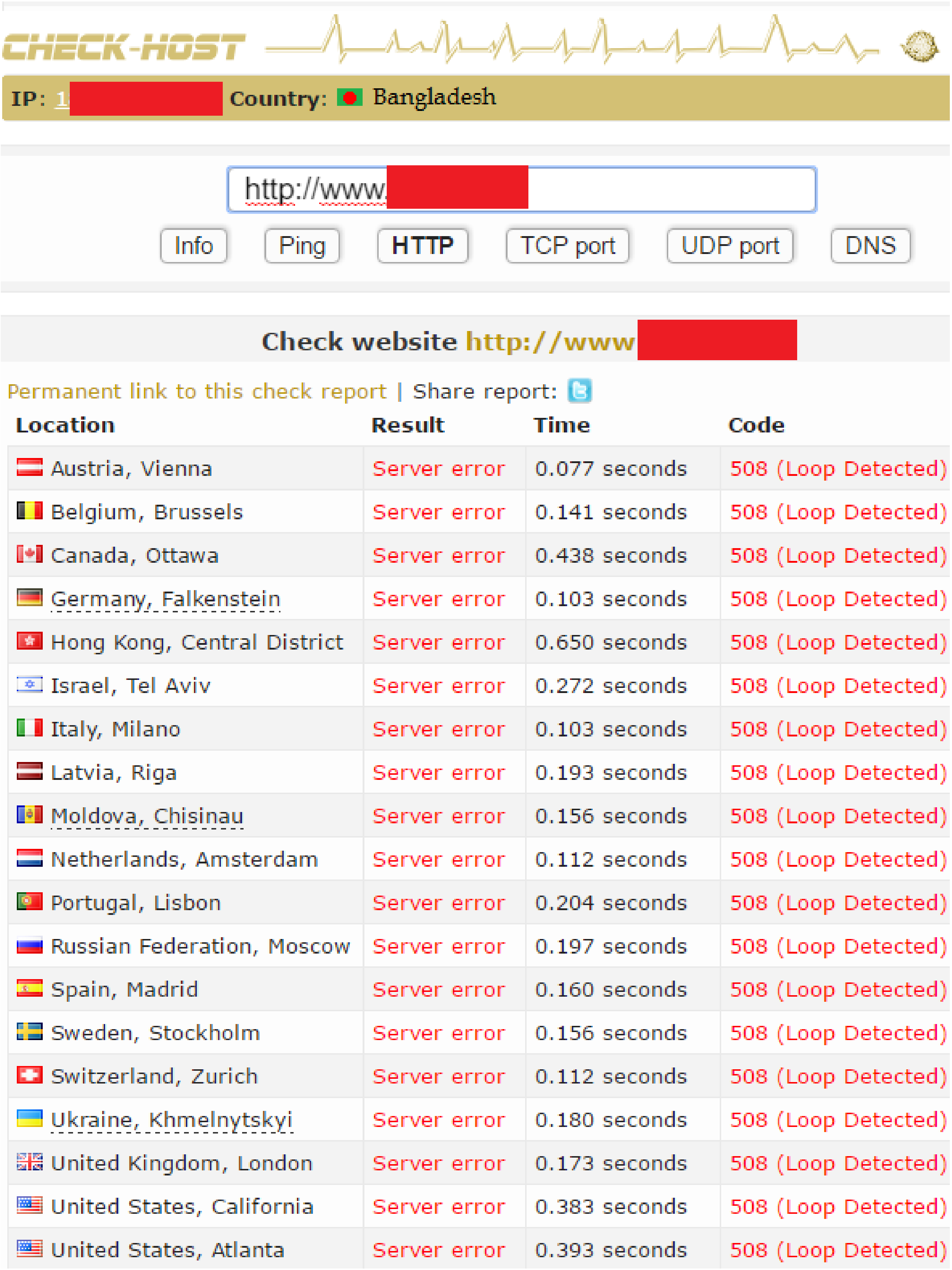
amazon.com did not reply to attack. This protection is actually not a real protection as this server is just prepared for this amount of requests. As the data clouds are having hundreds of requests each second, this little peak does nothing to the cloud server. Nevertheless, this is not the case if we would have access to certain VM and penetrate directly to it. The VM has limitations and has a maximum workflow. Consequently, it would not stand DoS attacks. The HULK script was not applied to any cloud VM as there was no direct access to cloud VM.

2.3. XML-RPC DDoS attack

Unlike XML-RPC DDoS attack, HULK script is not using multiple servers (server list) as a zombie army for attack. The Hulk is rather attack from few or few dozen machines. XML-RPC DDoS attack is more complicated and more dangerous for web servers and clouds. Most of the people are unfamiliar with the concept of the XML-RPC DDoS attack. The main misunderstanding is that one of the most famous web-site makers is the holder of the script that is attacking servers. Unlike the opinion of some people that it is some list of pirated servers that is holding those scripts. Namely WordPress websites are holding XML-RPC script which can be a part of a larger network of DDoS attack. XML-RPC is a simple, portable way to make remote procedure calls over HTTP. It can be used with Perl, Java, Python, C, C++, PHP, and many other programming languages. The WordPress, Drupal and most content management systems support XML-RPC. This HTTP call can be repeated multiple times thus make a DDoS attack. Taking into consideration that there are dozen millions of WordPress impact of the of the attack of so many machines cannot be fully understood. As a security measure, there is a way to prevent this misuse. Raising awareness of WordPress users that their services can misused. This will just prevent other machines to misuse that server/website for further DDoS attacks as some of the users can choose another platform for their website. Secondly, WordPress (WP) using XML-RPC should manually prevent the misuse. The simple script provided in Figure 5 will prevent misuse with XML-RPC API.

3. Empirical Results and Observations

In this section, the experimental results along with our observations of this study have been presented. Cloud environments always face unlimited mumbler of the threats. But due to the vast amount of data stored on cloud servers the providers become an attractive target. The main reasons behind the DDoS attacks include business rivalry, political ideology, and cyber war among countries. The most common outcome of DDoS attacks is unavailability of target service. The unavailability causes many short term and long term business and reputation losses. The DDoS attacks often cause a data breach. Thus companies may incur fines or they may face lawsuits



IP: 1[redacted] Country: Bangladesh

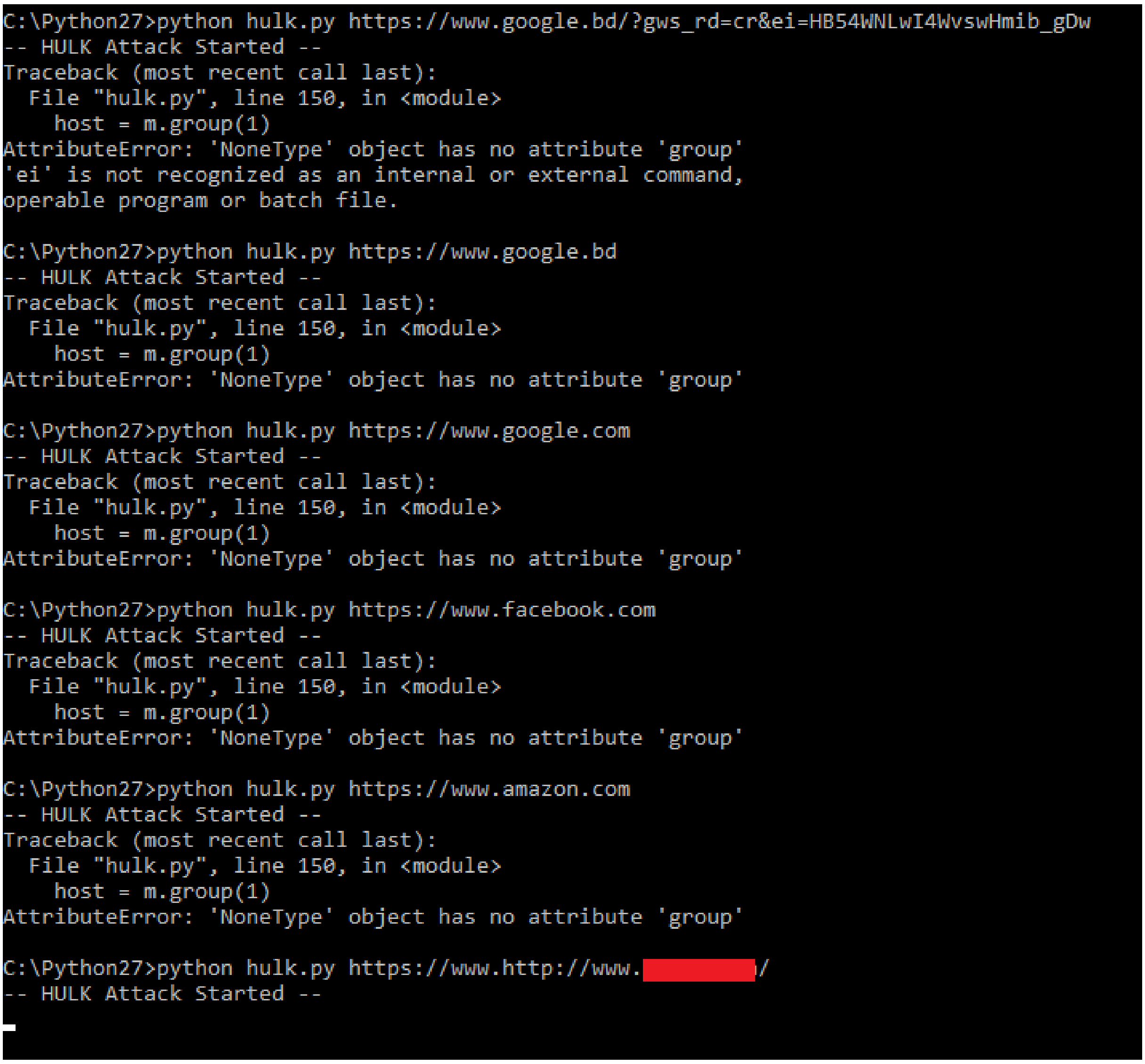
http://www.[redacted]

Check website http://www[redacted]

Permanent link to this check report | Share report:

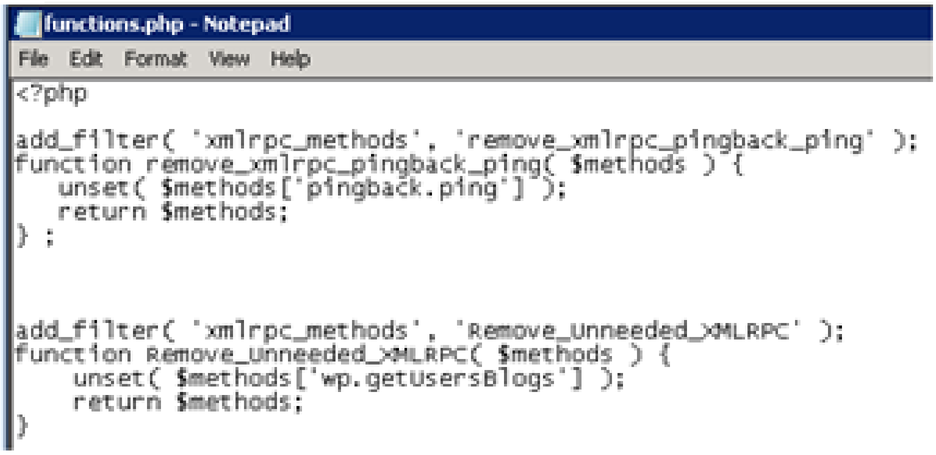
Location	Result	Time	Code
Austria, Vienna	Server error	0.077 seconds	508 (Loop Detected)
Belgium, Brussels	Server error	0.141 seconds	508 (Loop Detected)
Canada, Ottawa	Server error	0.438 seconds	508 (Loop Detected)
Germany, Falkenstein	Server error	0.103 seconds	508 (Loop Detected)
Hong Kong, Central District	Server error	0.650 seconds	508 (Loop Detected)
Israel, Tel Aviv	Server error	0.272 seconds	508 (Loop Detected)
Italy, Milano	Server error	0.103 seconds	508 (Loop Detected)
Latvia, Riga	Server error	0.193 seconds	508 (Loop Detected)
Moldova, Chisinau	Server error	0.156 seconds	508 (Loop Detected)
Netherlands, Amsterdam	Server error	0.112 seconds	508 (Loop Detected)
Portugal, Lisbon	Server error	0.204 seconds	508 (Loop Detected)
Russian Federation, Moscow	Server error	0.197 seconds	508 (Loop Detected)
Spain, Madrid	Server error	0.160 seconds	508 (Loop Detected)
Sweden, Stockholm	Server error	0.156 seconds	508 (Loop Detected)
Switzerland, Zurich	Server error	0.112 seconds	508 (Loop Detected)
Ukraine, Khmelnytskyi	Server error	0.180 seconds	508 (Loop Detected)
United Kingdom, London	Server error	0.173 seconds	508 (Loop Detected)
United States, California	Server error	0.383 seconds	508 (Loop Detected)
United States, Atlanta	Server error	0.393 seconds	508 (Loop Detected)

Figure 3. Testing target responses after a DoS attack.



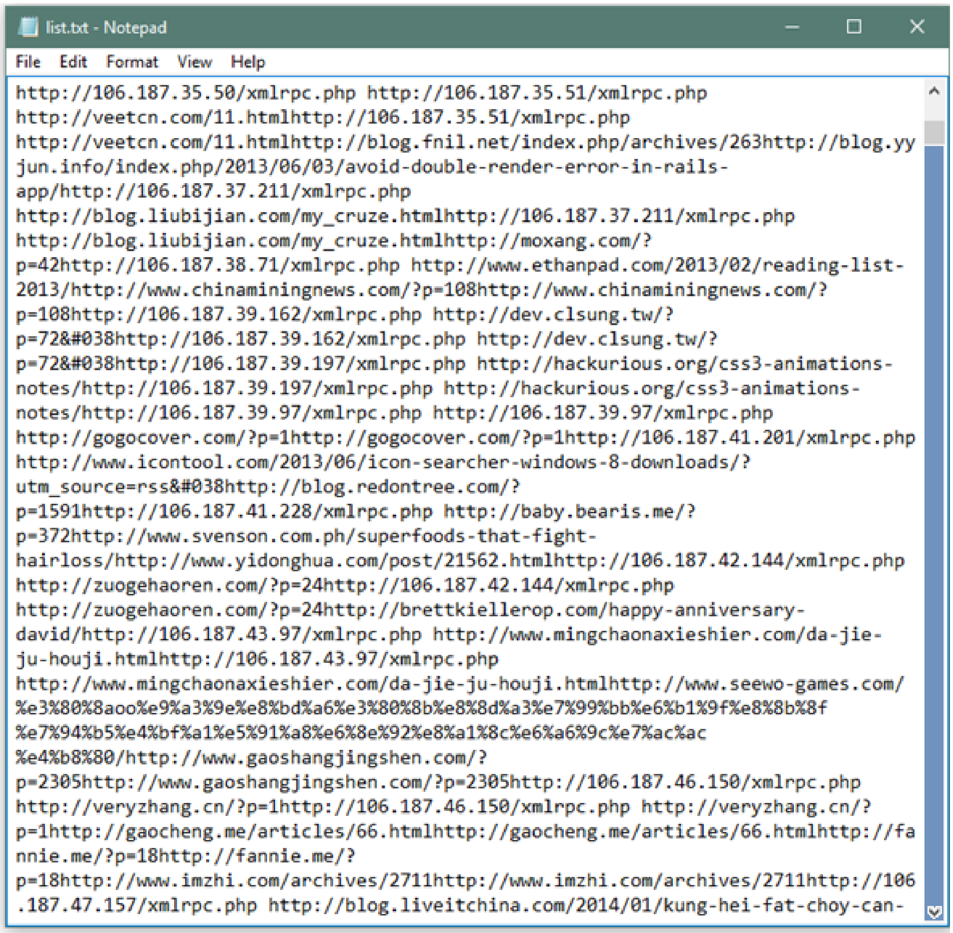
```
C:\Python27>python hulk.py https://www.google.bd/?gws_rd=cr&ei=HB54WNLwI4WvswHmib_gDw
-- HULK Attack Started --
Traceback (most recent call last):
  File "hulk.py", line 150, in <module>
    host = m.group(1)
AttributeError: 'NoneType' object has no attribute 'group'
'ei' is not recognized as an internal or external command,
operable program or batch file.

C:\Python27>python hulk.py https://www.google.bd
-- HULK Attack Started --
Traceback (most recent call last):
  File "hulk.py", line 150, in <module>
    host = m.group(1)
AttributeError: 'NoneType' object has no attribute 'group'

C:\Python27>python hulk.py https://www.google.com
-- HULK Attack Started --
Traceback (most recent call last):
  File "hulk.py", line 150, in <module>
    host = m.group(1)
AttributeError: 'NoneType' object has no attribute 'group'

C:\Python27>python hulk.py https://www.facebook.com
-- HULK Attack Started --
Traceback (most recent call last):
  File "hulk.py", line 150, in <module>
    host = m.group(1)
AttributeError: 'NoneType' object has no attribute 'group'

C:\Python27>python hulk.py https://www.amazon.com
-- HULK Attack Started --
Traceback (most recent call last):
  File "hulk.py", line 150, in <module>
    host = m.group(1)
AttributeError: 'NoneType' object has no attribute 'group'

C:\Python27>python hulk.py https://www.http://www.[redacted]/
-- HULK Attack Started --
```

Figure 4. Testing cloud servers with DoS attack.



```
<?php

add_filter( 'xmlrpc_methods', 'remove_xmlrpc_pingback_ping' );
function remove_xmlrpc_pingback_ping( $methods ) {
   unset( $methods['pingback.ping'] );
   return $methods;
} ;


add_filter( 'xmlrpc_methods', 'Remove_Unneeded_XMLRPC' );
function Remove_Unneeded_XMLRPC( $methods ) {
    unset( $methods['wp.getUsersBlogs'] );
    return $methods;
}
```

Figure 5. DDoS defense in cloud.



```
http://106.187.35.50/xmlrpc.php http://106.187.35.51/xmlrpc.php
http://veetcn.com/11.htmlhttp://106.187.35.51/xmlrpc.php
http://veetcn.com/11.htmlhttp://blog.fnil.net/index.php/archives/263http://blog.yy
jun.info/index.php/2013/06/03/avoid-double-render-error-in-rails-
app/http://106.187.37.211/xmlrpc.php
http://blog.liubijian.com/my_cruze.htmlhttp://106.187.37.211/xmlrpc.php
http://blog.liubijian.com/my_cruze.htmlhttp://moxang.com/?
p=42http://106.187.38.71/xmlrpc.php http://www.ethanpad.com/2013/02/reading-list-
2013/http://www.chinaminingnews.com/?p=108http://www.chinaminingnews.com/?
p=108http://106.187.39.162/xmlrpc.php http://dev.clsung.tw/?
p=72&#038http://106.187.39.162/xmlrpc.php http://dev.clsung.tw/?
p=72&#038http://106.187.39.197/xmlrpc.php http://hackurious.org/css3-animations-
notes/http://106.187.39.197/xmlrpc.php http://hackurious.org/css3-animations-
notes/http://106.187.39.97/xmlrpc.php http://106.187.39.97/xmlrpc.php
http://gogocover.com/?p=1http://gogocover.com/?p=1http://106.187.41.201/xmlrpc.php
http://www.icontool.com/2013/06/icon-searcher-windows-8-downloads/?
utm_source=rss&#038http://blog.redontree.com/?
p=1591http://106.187.41.228/xmlrpc.php http://baby.bearis.me/?
p=372http://www.svenson.com.ph/superfoods-that-fight-
hairloss/http://www.yidonghua.com/post/21562.htmlhttp://106.187.42.144/xmlrpc.php
http://zuogehaoren.com/?p=24http://106.187.42.144/xmlrpc.php
http://zuogehaoren.com/?p=24http://brettkiellerop.com/happy-anniversary-
david/http://106.187.43.97/xmlrpc.php http://www.mingchaonaxieshier.com/da-jie-
ju-houji.htmlhttp://106.187.43.97/xmlrpc.php
http://www.mingchaonaxieshier.com/da-jie-ju-houji.htmlhttp://www.seewo-games.com/
%e3%80%8aoo%e9%a3%9e%e8%bd%a6%e3%80%8b%e8%8d%a3%e7%99%bb%e6%b1%9f%e8%8b%8f
%e7%94%b5%e4%bf%a1%e5%91%a8%e6%8e%92%e8%a1%8c%e6%a6%9c%e7%ac%ac
%e4%b8%80/http://www.gaoshangjingshen.com/?
p=2305http://www.gaoshangjingshen.com/?p=2305http://106.187.46.150/xmlrpc.php
http://veryzhang.cn/?p=1http://106.187.46.150/xmlrpc.php http://veryzhang.cn/?
p=1http://gaocheng.me/articles/66.htmlhttp://gaocheng.me/articles/66.htmlhttp://fa
nnie.me/?p=18http://fannie.me/?
p=18http://www.imzhi.com/archives/2711http://www.imzhi.com/archives/2711http://106
.187.47.157/xmlrpc.php http://blog.liveitchina.com/2014/01/kung-hei-fat-choy-can-
```

Figure 6. IP addresses and web pages hosting XML-RPC API and behaving as a zombie in DDoS attacks.

or criminal charges. Breach investigations and customer notifications can rack up significant costs. Indirect effects, such as brand damage and loss of business, can impact organizations for years. Thus security level of the data on the cloud servers will always be the cardinal concern.

Our study intended to show the security level of the cloud servers. The experiments in our study are relatively easy to implement a DoS or DDoS attack. Phyton scripts like HULK or XML-RPC are able to make several hundred requests to the server in short period of time. HULK script made HTTP requests for the server which was immediately unresponsive for all other requests. The amount of the requests made the server block and hold all incoming request as it was unable to respond due to request flood. This resulted in failure of the certain domain that is tested and the server was down. Tested domain was located on private server with small or no protection level. The machine that was holding this web page can be seen as VM on the cloud, if there is access to a VM in the cloud. It would be relatively easy to apply the script to it and the result with the same outcome could be expected. Unlike HULK script, XML-RPC is using a server list of available machines that are making multiple requests to the server. HULK is rather DoS than DDoS attack, while XML-RPC is pure DDoS attack as it sends *request* for its hosts to attack the certain domain. This is the main difference between the HULK and XML-RPC. XML-RPC can be much more efficient when it comes to flooding, making server to be unavailable and breaking the server down. Figure 6 depicts the IP addresses and web pages hosting XML-RPC API and behaves as a zombie in DDoS attacks. As those lists are available on the internet, the easiest protection of VM could be limitation of those servers and IP addresses. Putting those servers could easily block penetration to the VM and hence block the DDoS attacks. Based on our observations, the accessing of VM on the cloud can be as easy as the first experiment in this study - attacking the standalone server with Hulk script. Thus it can be concluded that with proper tools and applications, access to the VM and DDoS can be implemented relatively easy. As there are records of those attacks, it can be seen that XML-RPC script is doing its job very effectively.

The target VM goes down just like the standalone server. Consequently, the protection of the VM of the clouds can be improved. The target VM cannot protect itself from the pingback attack of the XML-RPC API's. This should be done by the cloud which should regulate the high slope of the unexpected requests.
It is noteworthy that we did not implement the XML-RPC script to any clouds and its VM since we had no approval to implement the experiment to any cloud and VM. It is an excellent idea to take into account the DOE mathematical methodology. Nowadays, DOE is using for planning and conducting experiments, analyzing, and interpreting data. But due to lack of huge experimental data and proper experimental permission from appropriate authorities, the consideration of DOE has been left for future investigation.

4. Conclusion

An easy implementation of DoS attack was performed using HULK script in Python. The used script is able to make several hundred requests to the server in short period of time. The HULK script is good for DoS attack, while XML-RPC goes pure for DDoS attack. With proper tools and applications, the access to the VM and DDoS can be implemented in a relatively easy way. The implementation of the XML-RPC script was not performed entirely due to lack of permission, and henceforth the future work would implement the XML-RPC script to any clouds and corresponding VM.

5. Acknowledgement

Author would like to give thanks to the unknown reviewers of this paper for their remarks.

REFERENCES

[1] G. Somani, M. S. Gaur, D. Sanghi, and M. Conti, “Ddos attacks in cloud computing: Collateral damage to non-targets,” *Computer Networks*, vol. 109, pp. 157–171, 2016.

[2] F. F. Wong and C. X. Tan, “A survey of trends in massive ddos attacks and cloud-based mitigations,” *International Journal of Network Security and Its Applications*, vol. 6, pp. 57–71, 2014.

[3] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, “Ddos victim service containment to minimize the internal collateral damages in cloud computing,” *Computers & Electrical Engineering*, vol. 59, pp. 165–179, 2017.

[4] M. S. Fallah and N. Kahani, “TDPF: a traceback-based distributed packet filter to mitigate spoofed ddos attacks,” *Security and Communication Networks*, vol. 7, no. 2, pp. 245–264, 2014.

[5] H. Chen, T. Gaska, Y. Chen, and D. H. Summerville, “An optimized reconfigurable power spectral density converter for real-time shrew ddos attacks detection,” *Computers and Electrical Engineering*, vol. 39, no. 2, pp. 295–308, 2013.

[6] H. Luo, Y. Lin, H. Zhang, and M. Zukerman, “Preventing ddos attacks by identifier/locator separation,” *IEEE Network*, vol. 27, no. 6, pp. 60–65, 2013.

[7] U. B. Porat, A. Bremler-Barr, and H. Levy, “Vulnerability of network mechanisms to sophisticated ddos attacks,” *IEEE Trans. Computers*, vol. 62, no. 5, pp. 1031–1043, 2013.

[8] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks,” *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[9] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, “A game theoretic defence framework against dos/ddos cyber attacks,” *Computers and Security*, vol. 38, pp. 39–50, 2013.

[10] H. Beitollahi and G. Deconinck, “Connectionscore: a statistical technique to resist application-layer ddos attacks,” *J. Ambient Intelligence and Humanized Computing*, vol. 5, no. 3, pp. 425–442, 2014.

[11] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, “Botnet in ddos attacks: Trends and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.

[12] M. M. Alam, M. Y. Arafat, and F. Ahmed, “Study on auto detecting defence mechanisms against application layer ddos attacks in SIP server,” *JNW*, vol. 10, no. 6, pp. 344–352, 2015.

[13] S. Hong, “Efficient and secure DNS cyber shelter on ddos attacks,” *J. Computer Virology and Hacking Techniques*, vol. 11, no. 3, pp. 129–136, 2015.

[14] M. Simsek, “A new metric for flow-level filtering of low-rate ddos attacks,” *Security and Communication Networks*, vol. 8, no. 18, pp. 3815–3825, 2015.

[15] Q. Yan, F. R. Yu, Q. Gong, and J. Li, “Software-defined networking (SDN) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[16] S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, “A novel dos and ddos attacks detection algorithm using ARIMA time series model and chaotic system in computer networks,” *IEEE Communications Letters*, vol. 20, no. 4, pp. 700–703, 2016.

[17] A. Saidi, E. Bendriss, A. Kartit, and M. E. Marraki, “Techniques to detect dos and ddos attacks and an introduction of a mobile agent system to enhance it in cloud computing,” *IJIMAI*, vol. 4, no. 3, pp. 75–78, 2017.

[18] N. Agrawal and S. Tapaswi, “Defense schemes for variants of distributed denial-of-service (ddos) attacks in cloud computing: A survey,” *Information Security Journal: A Global Perspective*, vol. 26, no. 2, pp. 61–73, 2017.

[19] K. Kalkan, G. Gur, and F. Alagoz, “Filtering-based defense mechanisms against ddos attacks: A survey,” *IEEE Systems Journal*, vol. 11, no. 4, pp. 2761–2773, 2017.

[20] M. Merouane, “An approach for detecting and preventing ddos attacks in campus,” *Automatic Control and Computer Sciences*, vol. 51, no. 1, pp. 13–23, 2017.

[21] S. Behal and K. Kumar, “Detection of ddos attacks and flash events using information theory metrics-an empirical investigation,” *Computer Communications*, vol. 103, pp. 18–28, 2017.

[22] M. Semerci, A. T. Cemgil, and B. Sankur, “An intelligent cyber security system against ddos attacks in SIP networks,” *Computer Networks*, vol. 136, pp. 137–154, 2018.

[23] M. Petkovic, I. Basicevic, D. Kukolj, and M. Popovic, “Evaluation of takagi-sugeno-kang fuzzy method in entropy-based detection of ddos attacks,” *Comput. Sci. Inf. Syst.*, vol. 15, no. 1, pp. 139–162, 2018.

[24] K. D. Thilak and A. Amuthan, “Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets,” *Future Generation Comp. Syst.*, vol. 82, pp. 304–314, 2018.

[25] S. Hameed and H. A. Khan, “SDN based collaborative scheme for mitigation of ddos attacks,” *Future Internet*, vol. 10, no. 3, p. 23, 2018.

[26] K. Sharma and B. B. Gupta, “Taxonomy of distributed denial of service (ddos) attacks and defense mechanisms in present era of smartphone devices,” *IJESMA*, vol. 10, no. 2, pp. 58–74, 2018.

[27] S. M. Mousavi and M. St-Hilaire, “Early detection of ddos attacks against software defined network controllers,” *J. Network Syst. Manage.*, vol. 26, no. 3, pp. 573–591, 2018.

[28] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, “Intrusion detection systems of icmpv6-based ddos attacks,” *Neural Computing and Applications*, vol. 30, no. 1, pp. 45–56, 2018.

[29] M. Saad, M. T. Thai, and A. Mohaisen, “POSTER: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization,” in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security (AsiaCCS), Incheon, Republic of Korea, June 04-08*, 2018, pp. 809–811.

[30] B. Kurt, C. Yildiz, T. Y. Ceritli, B. Sankur, and A. T. Cemgil, “A bayesian change point model for detecting sip-based ddos attacks,” *Digital Signal Processing*, vol. 77, pp. 48–62, 2018.

[31] A. P. Abidoye and I. C. Obagbuwa, “Ddos attacks in wsns: detection and countermeasures,” *IET Wireless Sensor Systems*, vol. 8, no. 2, pp. 52–59, 2018.

[32] Y. J. Lee, N. Baik, C. Kim, and C. N. Yang, “Study of detection method for spoofed IP against ddos attacks,” *Personal and Ubiquitous Computing*, vol. 22, no. 1, pp. 35–44, 2018.

[33] M. Idhammad, K. Afdel, and M. Belouch, “Detection system of HTTP ddos attacks in a cloud environment based on information theoretic entropy and random forest,” *Security and Communication Networks*, vol. 2018, pp. 1 263 123:1–1 263 123:13, 2018.

[34] C. Wang, T. Miu, X. Luo, and J. Wang, “Skyshield: A sketch-based defense system against application layer ddos attacks,” *IEEE Trans. Information Forensics and Security*, vol. 13, no. 3, pp. 559–573, 2018.

[35] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, “Ensemble classifiers with drift detection (ECDD) in traffic flow streams to detect DDOS attacks,” *Wireless Personal Communications*, vol. 99, no. 4, pp. 1639–1659, 2018.

[36] N. Dayal and S. Srivastava, "An RBF-PSO based approach for early detection of ddos attacks in SDN," in *International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, January 3-7*, 2018, pp. 17–24.

[37] H. Li and L. Wang, "Online orchestration of cooperative defense against ddos attacks for 5g MEC," in *2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, April 15-18*, 2018, pp. 1–6.

[38] T. Lukaseder, L. Maile, B. Erb, and F. Kargl, "Sdn-assisted network-based mitigation of slow ddos attacks," *CoRR*, vol. abs/1804.06750, 2018. [Online]. Available: http://arxiv.org/abs/1804.06750

[39] O. A. Osanaiye, K. R. Choo, and M. E. Dlodlo, "Distributed denial of service (ddos) resilience in cloud: Review and conceptual cloud ddos mitigation framework," *J. Network and Computer Applications*, vol. 67, pp. 147–165, 2016.

[40] A. Lonea, D. Popescu, and H. Tianfield, "Detecting ddos attacks in cloud computing environment," *International Journal of Computers Communications & Control*, vol. 8, pp. 70–78, 2013.

[41] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[42] M. H. Sharif, "A numerical approach for tracking unknown number of individual targets in videos," *Digital Signal Processing*, vol. 57, pp. 106–127, 2016.

[43] A. Hiziroglu and H. I. Cebeci, "A conceptual framework of a cloud-based customer analytics tool for retail smes," *Periodicals of Engineering and Natural Sciences*, vol. 1, no. 2, 2013.

[44] M. Sabanovic, M. Saracevic, and E. Azizovic, "Comparative analysis of amf, json and xml technologies for data transfer between the server and the client," *Periodicals of Engineering and Natural Sciences*, vol. 4, no. 2, 2016.

[45] M. H. Sharif and O. Gursoy, "Parallel computing for artificial neural network training using java native socket programming," *Periodicals of Engineering and Natural Sciences*, vol. 6, no. 1, 2018.

[46] S. Simpson, S. N. Shirazi, A. K. Marnerides, S. Jouet, D. Pezaros, and D. Hutchison, "An inter-domain collaboration scheme to remedy ddos attacks in computer networks," *IEEE Trans. Network and Service Management*, vol. 15, no. 3, pp. 879–893, 2018.

[47] R. Kolandaisamy, R. M. Noor, I. Ahmedy, I. Ahmad, M. R. Zaba, M. Imran, and M. Alnuem, "A multivariant stream analysis approach to detect and mitigate ddos attacks in vehicular ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 2 874 509:1–2 874 509:13, 2018.

[48] A. Chadd, "Ddos attacks: past, present and future," *Network Security*, vol. 2018, no. 7, pp. 13–15, 2018.

[49] A. Bhardwaj and S. Goundar, "Comparing single tier and three tier infrastructure designs against ddos attacks," *IJCAC*, vol. 7, no. 3, pp. 59–75, 2017.

[50] J. Swain, B. K. Pattanayak, and B. Pati, "A new approach for ddos attacks to discriminate the attack level and provide security for ddos nodes in MANET," *IJCNIS*, vol. 9, no. 3, 2017.

[51] M. H. Sharif, "High-performance mathematical functions for single-core architectures," *Journal of Circuits, Systems, and Computers*, vol. 23, no. 4, 2014.

[52] B. Durakovic, "Design of experiments application, concepts, examples: State of the art," *Periodicals of Engineering and Natural Sciences*, vol. 5, no. 3, pp. 421–439, 2017.

[53] M. H. Sharif, I. Despot, and S. Uyaver, "A proof of concept for home automation system with implementation of the internet of things standards," *Periodicals of Engineering and Natural Sciences*, vol. 6, no. 1, 2018.

BIOGRAPHY OF AUTHOR

Sefat Mahjabin obtained her BSc in Computer Science and Engineering from the Faculty of Science and Information Technology, Daffodil International University, Dhaka, Bangladesh in 2018. She has very good knowledge in the field of Digital Security. Currently, she is looking for starting her MSc in Computer Engineering study in abroad. Her research interests include Cloud Computing, Parallel & Distributed Computing, Web Application & Development, Artificial Intelligence & Neural Networks, Data Mining, Medical Image Analysis & Pattern Understanding, and Brain-Driven Computer Vision.