International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 4, April-2014, pp: (371-378), Impact Factor: 1.252, Available online at: www.erpublications.com

A Survey: Wisdom of Web Intelligence advanced and Networking knowledge

Vishal Singh
B.Tech. [C.S.E.], M.Tech. [C.S.E] Final Year, Kanpur, India

Abstract: Web Intelligence is a next generation scientific research area that introduces World Wide Wisdom Web (W4). Web and Internet have become great necessity for every organization, industry, human etc., Therefore Wisdom of Web is warmly important against anonymous behavior. This paper focuses on various fields of Web Intelligence by which researchers gain advance knowledge about WI. And brief description about DDoS attack on Web and how to identify it using python code, python is an advance code for networking knowledge and plays an important role in wisdom of Web Intelligence. As well as advance topics of Web Intelligence and how Web server works and query filters of WI are also describe in this paper.

Keywords: Web Intelligence, Python, DDoS, Liso server, W4, Ontologies.

Introduction

Web Intelligence (WI) is a new direction for scientific research and development that exploits Artificial Intelligence (AI) and advanced Information Technology (IT) on the new territories of the Web and Internet. WI may be considered as an enhancement of AI, such as knowledge representation, planning, knowledge discovery, data mining, intelligent agents, social network intelligence and advance IT, such as wireless networks, ubiquitous devices, social networks, data/knowledge grids, next generation of Web-empowered products, systems, services. A practical goal of WI research is the design and implementation of Intelligent Web Information System which involves a large number of machine learning technologies such as natural language processing, information extraction, information retrieval, text mining, web data mining for knowledge discovery, business intelligence and security, classification/clustering of web pages and multimedia content, E-mail spamming and classification, web-based personalized techniques, etc. Via the integration of machine learning and web related technologies, the object of Intelligent Web Information System is to create next generation intelligent web services. The dream of web intelligence is the wisdom web. The new generations of the web will enable us to gain information from data, knowledge, and life from living. In realizing this dream, there may be more questions than answers, more problems than solutions, more unknowns and uncertainty. We can explore the Web one step at a time, and build the Wisdom Web piece by piece. WI has great potential to make useful contributions to e-business (including e-commerce and e-finance), e-science, e-learning, e-government, e-community, and so on.

Python is a high-level, interpreted, and interactive and object- oriented scripting language. Python was designed to be highly readable which uses English keywords frequently where as other languages use punctuation and it has fewer syntactical constructions than other languages. Python is derived from many other languages, including ABC, Module-3, C, C++, Algol-68, SmallTalk and Unix shell and other scripting languages. Python is used by many of the most highly productive professional programmers. A few of the places that use Python extensively are Google, the New York Stock Exchange, Industrial Light and Magic. Python provides an excellent development platform to build your own offensive tools. It is copyrighted. Like Perl, Python source code is now available under the GNU General Public License (GPL).

World Wide Wisdom Web (W4)

The goal of the new generation WI is to enable users to gain new wisdom of living, working, playing, and learning, in addition to information search and knowledge queries. According to the Webster Dictionary, the word Wisdom implies the following meanings:

1. The qualityof being wise; knowledge, and the capacity to make due use of it; knowledge of the best ends and the best means; discernment and judgment; discretion; sagacity; skill; dexterity.
2. The result of wise judgments; scientific or practical truth; acquired knowledge; erudition.

Capabilities of the Wisdom Web

There are ten fundamental capabilities of the Wisdom Web:

1. **Self-organizing servers**– A Wisdom Web server self-nominates automatically to other services its functional roles as well as corresponding spatial or temporal constraints and operational settings.
2. **Specialization** – A Wisdom Web server is an agent by itself, which is specialized in performing some roles in a certain service.
3. **Growth** – The population of Wisdom Agents will change dynamically, as new agents are self-reproduced by their parent agents to become more specialized agents.
4. **Autocatalysis** – Wisdom agents consists various roles that are created through specialization and are activated by the Wisdom Search requests, their associations with some services and among themselves must be aggregated auto catalytically.
5. **Problem Solver Markup Language (PSML)** – PSML is necessary for wisdom agents to specify their foles and settings as well as relationships with any other services.
6. **Semantics** – The Wisdom Web needs to understand what is the right judgment of "best," and what are meant by "Montreal", "Season", "year", and "night life" by understanding the granularities of their corresponding subjects.
7. **Metaknowledge**– Metaknowledge deals with the relationships between concepts and the spatial or temporal constraint knowledge in planning and executing services. It allows agents to self-resolve their conflict of interests.
8. **Planning** – Planning plays in important role in the wisdom web by which already have knowledge about furthermore happening.
9. **Personalization** – The Wisdom Web remembers the recent encounters and related different events.
10. **A sense of humor** – The Wisdom Web does not tell a funny story explicitly, it adds some punch lines to the situation or anxiety.

Levels of Web Intelligence

There are four conceptual levels of Wisdom Web for fast development as well as applications of many WI techniques and technologies:

1. Internet-level communication, infrastructure, and security protocol
2. Interface- level multimedia presentation standards
3. Knowledge-level information processing and management tools
4. Application- level ubiquitous computing and social intelligence environments

DDOS Attack on web and identifying DDOS Attack

DDoS Attack is a powerful version of DoS attack in which many attacking systems are involved and many computers start performing DoS attacks on the same target server. Attackers use a Zombie network, which is a group of infected computers on which the attackers has silently installed the DoS attacking tool. Whenever we want to perform DDoS, we can use all the computers of Zombie network to perform the attack.

In December 2010, Dutch police arrested a teenager for participating in distributed denial-of-service attacks against Visa, MasterCard, and PayPal as part of an operation to target companies opposed to Wikileaks. Less than a month later, the FBI issued forty search warrants and British police made five arrests as well. Attackers used the Low Orbit Ion Cannon (LOIC) distributed denial-of-service toolkit.

LOIC floods a target with large volumes of UDP and TCP traffic. A single instance of LOIC will do very little to exhaust the resources of a target; however, when hundreds of thousands of individuals use LOIC simultaneously, they quickly exhaust the target's resources and ability to provide services.

LOIC offers two modes of operation. In the first mode, a user can enter a target address. In the second mode, dubbed HIVEMIND, the user connects LOIC to an Internet Relay Chat (IRC) server where users can nominate targets that the IRC-connected users will automatically attack.

To start an attack, a member of Anonymous logs onto a specific Internet Relay Chat (IRC) server, and issues an attack command, such as !lazortargetip=66.211.169.66 message=test_test port=80 method=tcp wait=false random=true start. Any member of Anonymous connected to the IRC with LOIC connected in HIVEMIND mode can immediately start an attack against the target. In this case, the IP address 66.211.169.66 refers to the address of paypal.com, targeted during Operation Payback.

When a user starts a LOIC attack, it fires a massive amount of TCP packets towards a target. These packets, combined with the collective packets from the hive, essentially exhaust the resources of the target. We start a tcpdump session and see several small (length 12) TCP packets sent every 0.00005 seconds. This behavior repeats until the attack terminates. Notice that the target has difficulty responding and only acknowledges about one out of every five packets. Let's quickly write a function that finds a DDoS attack in progress. To detect an attack, we will set a threshold of packets. If the number

of packets from a user to a specific address exceeds this threshold, it indicates something we might want to invertigate further as an attack. But this does not definitively prove a user has initiated an attack. Then adding some option parsing in our code, finally our script now detects the download, overhears the HIVE commands, and detects the attack.

```
import dpkt
import optparse
import socket
THRESH =1000
def findDownload(pcap):
    for (ts, buf) in pcap:
        try:
            eth=dpkt.ethernet.Ethernet(buf)
            ip=eth.data
            src=socket.inet_ntoa(ip.src)
            tcp=ip.data
            http=dpkt.http.Request(tcp.data)
            if http.method=='GET':
                uri=http.uri.lower()
                if '.zip' in uri and 'loic' in uri:
                    print '[!] '+src+' Downloaded LOIC.'
        except:
            pass

def findHivemind(pcap):
    for (ts, buf) in pcap:
        try:
            eth=dpkt.ethernet.Ethernet(buf)
            ip=eth.data
            src=socket.inet_ntoa(ip.src)
            dst=socket.inet_ntoa(ip.dst)
            tcp=ip.data
            dport=tcp.dport
            sport=tcp.sport
            if dport==6667:
                if '!lazor' in tcp.data.lower():
                    print '[!] DDoSHivemind issued by: '+src
                    print '[+] Target CMD: '+tcp.data
            if sport ==6667:
                if '!lazor' in tcp.data.lower():
                    print '[!] DDoSHivemind issued to: '+src
                    print '[+] Target CMD: '+tcp.data
        except:
            pass
```

```
deffindAttack(pcap):
    pktCount= {}
    for (ts, buf) inpcap:
        try:
            eth=dpkt.ethernet.Ethernet(buf)
            ip=eth.data
            src=socket.inet_ntoa(ip.src)
            dst=socket.inet_ntoa(ip.dst)
            tcp=ip.data
            dport=tcp.dport
            ifdport==80:
                stream=src+':'+dst
                ifpktCount.has_key(stream):
                    pktCount[stream] =pktCount[stream] +1
                else:
                    pktCount[stream] =1
        except:
            pass

    for stream inpktCount:
        pktsSent=pktCount[stream]
        ifpktsSent> THRESH:
            src=stream.split(':')[0]
            dst=stream.split(':')[1]
            print'[+] '+src+' attacked '+dst+' with ' \
                +str(pktsSent) +' pkts.'

defmain():
    parser=optparse.OptionParser("usage %prog '+\
     '-p <pcap file> -t <thresh>"
                        )
    parser.add_option('-p', dest='pcapFile', type='string',\
      help='specify pcap filename')
    parser.add_option('-t', dest='thresh', type='int',\
      help='specify threshold count ')

    (options, args) =parser.parse_args()
    ifoptions.pcapFile==None:
        printparser.usage
        exit(0)
    ifoptions.thresh!=None:
        THRESH =options.thresh
    pcapFile=options.pcapFile
```

```
    f =open(pcapFile)
    pcap=dpkt.pcap.Reader(f)
    findDownload(pcap)
    findHivemind(pcap)
    findAttack(pcap)
if __name__ =='__main__':
    main()
```

Running the code, we see the results. Four users downloaded the toolkit. Two attackers actually participated in the attack. Thus, the script now identifies an entire DDoS in action.

```
analyst# python findDDoS.py –p traffic.pcap
[!] 192.168.1.3 Downloaded LOIC.
[!] 192.168.1.5 Downloaded LOIC.
[!] 192.168.1.7 Downloaded LOIC.
[!] 192.168.1.9 Downloaded LOIC.
[!] DDoSHivemind issued by: 192.168.1.2
[+] Target CMD: TOPIC #LOIC:!lazortargetip=192.168.95.141
message=test_test port=80 method=tcp wait=false random=true start
[!] DDoSHivemind issued to: 192.168.1.3
[+] Target CMD: TOPIC #LOIC:!lazortargetip=192.168.95.141
message=test_test port=80 method=tcp wait=false random=true start
[!] DDoSHivemind issued to: 192.168.1.5
[+] Target CMD: TOPIC #LOIC:!lazortargetip=192.168.95.141
message=test_test port=80 method=tcp wait=false random=true start
[+] 192.168.1.3 attacked 192.168.95.141 with 1000337 pkts.
[+] 192.168.1.5 attacked 192.168.95.141 with 4133000 pkts.
```

Web Server

Web Server implements using a subset of the Hyper Text Transport Protocol (HTTP), Hyper Text Transport Protocol Secure (HTTPS) via Transport Layer Security (TLS), Common Gateway Interface (CGI). Web applications are becoming increasingly important today. Many startups and businesses are based entirely on web applications. In which Liso web server is fully functional and capable of running interactive web applications via its CGI interface. Liso serverimplements HEAD, GET, and POST.

- **HTTP 1.1**
  - GET – requests a specified resource; it should not have any other significance other than retrieval.
  - HEAD – asks for an identical response as GET, without the actual body.
  - POST - submit data to be processed to an identified resource; the data is in the body of this request.
  - For all other commands, server must return “501 Method Unimplemented”. If you are unable to implement one of the above commands, server must return the error response “501 Method Unimplemented”, rather than failing silently.
- **Command Line Arguments**

  Liso have 6 arguments :

```
usage: ./lisod<HTTP port><HTTPS port><log file><lock file><www folder><CGI
        folder or script name><private key file><certificate file>
```

  - HTTP port – the port for the HTTP (or echo) server to listen on
  - HTTPS port – the port for the HTTPS server to listen on

- Log file – file to send log messages to (debug, info, error)
- Lick file – file to lock on when becoming a daemon process
- www folder – folder containing a tree to serve as the root of a website
- CGI folder or script name – folder containing CGI programs – each file should be executable;
- Private key file – private key file path
- Certificate file – certificate file path

➢ **How Liso server Runing**

./lisod 8080 4443 /tmp/lisod.log /tmp/liso.lock /tmp/www /tmp/cgi/flaskr.py /tmp/priv.key /tmp/cert.crt

The Liso server will be passed the ports to run on, what log file to use, what lock file to use, when daemonizing, folders to serve static data from as well as CGI applications, and TLS private/public key pairs.

Advance Topics for Studying WI

WI can be studied in several ways:

- **Studying the Semantics in the Web –** Issues on the WI is the study of semantics in the Web, called the semantic Web. The modeling of semantics of Web information is to allow more of the Web content to become machine readable and processible as well as to allow for recognition of the semantic context in which Web materials are used. The semantic Web is a step toward intelligence of the Web.
- **Roles of Ontologies –** Ontologies provide a way of capturing a shared understanding of terms that can be used by human and programs to aid in information exchange. Ontologies will play a major role in supporting information exchange processes in various areas. The roles of ontologies for WI include communication between Web communities, agent communication based on semantics, knowledge-based Web retrieval, understanding Web contents in a semantics way, social network and web community discovery.
- **Studying the web as Social Networks –**Better understanding of the sociology of Web content creation. It has improved the search engines on the Web dramatically and has created more effective algorithms for community mining and for knowledge management. Because social networks have massive graph, main questions about the Web graph include How big is the graph, Can we browse from any page to any other, Can we exploit the structure of the Web, How to discover and manage the Web communities.
- **Soft Computing for WI –**The problem in WI is how to deal with uncertainty of information on the wired and wireless Web. Artificial neural networks, probabilistic and statistical reasoning, fuzzy sets, rough sets, granular computing, genetic algorithm, and other methodologies in the soft computing paradigm, to construct a hybrid system for Web Intelligence.

Query Filters in Web Intelligence

Query filters are used to restrict the data obtained from a query with respect to requirement. There are four types of query filters that can be constructed in Web Intelligence:

1. **Predefined query filters:** A predefined query filter in Web Intelligence is a filter defined in Universe. It appears in the list of classes and objects in Web Intelligence Query panel, identified by a yellow funnel icon. A predefined query filter limits the data returned by the query to specified values.

Figure 1: Predefined query filter

2. **Single and multi-value filters:** A single value query filter limits the data that an object returns to the individual value that you specify. A single value query filter always uses the 'Equal to' operator. A multi value query filter limits the data that an object returns to the multiple values that you specified. A multi value query filter can use the operators like 'InList', 'Between', 'Greater than', 'Less than' etc.

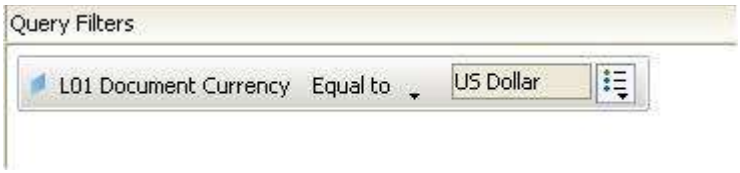

Figure 2: Single value query filter

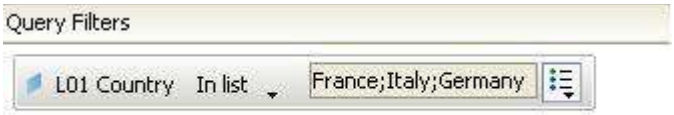

Figure 3: Multi value query filter

3. **Prompted Query Filters:** For creating a prompted query filter, you have to select the Prompt operand in the definition of the query filter in Web Intelligence. A prompt can be defined for all dimensions, measure, or detail objects listed in the Data tab in query panel.

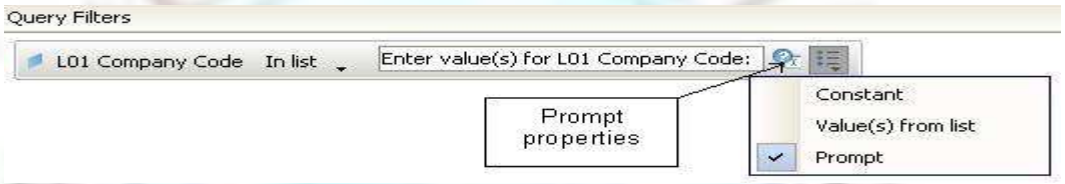

Figure 4: Prompted query filter

4. **Complex Filters:** The need for complex filter arises when you have to define the multiple filters plus specify the relationship between them in the form of logical association. The operators AND and OR are used.

Figure 5: Complex query filter

Conclusion/Future Work

This paper presents brief knowledge of next generation Web Intelligence that is advance IT field with intelligent behavior. W4 provides wisdom of web by which web technology have great potential about advancement wand security. We can secure our web against anonymous attackers with easy and advance python codes. Python is a high-level scripting language that is used for cracking and hacking but it also security scripts that are also used for caution and protection from harmful as well as harmless attacks. Web server is an important network application for advancement of business of today's fastest knowledgeable IT world and introduces how web server works with command line arguments.

Some advance topics of Web Intelligence are also defines that are helpful for researchers as well as query filters of WI participate for more advanced Web Intelligence. Through this paper researcher can have Wisdom of Web Intelligence, We can develop python script for becoming more secure Web that work from backdoor of web applications.

References

[1]. Yiyu (Y.Y.) yao Department of Computer Science, University of regina, Saskatchewan, Canada S4S 0A2 http://www.cs.uregina.ca/-yyao
[2]. Bellinger, G. Castro, D. and Mills, A. Data, Information, Knowledge,and Wisdom, http://www.systems-thinking.org/dikw/dikw.htm (accessedFebruary 25, 2005).
[3]. Berners-Lee, T. (with Fischetti, M.) Weaving the Web: the OriginalDesign and Ultimate Destiny of the World Wide Web by Its Inventor,HarperSanFrancisco, 1999.
[4]. Berners-Lee, T. How It All Started,http://www.w3.org/2004/Talks/w3c10-HowItAllStarted/(accessed February 26, 2005).
[5]. Berners-Lee, T., Hendler, J. and Lassila, O. Semantic Web, a new formof Web content that is meaningful to computers will unleash a revolutionof new possibilities, Scientific American, **248**, 34-43, 2001.
[6]. Bj¨orneborn, L. Small-World Link Structures across an Academic WebSpace: A Library and Information Science Approach, Ph.D. Thesis,Department of Information Studies, Royal School of Library and InformationScience, Denmark, 2004, http://www.db.dk/lb/phd/phd-thesis.pdf(accessed March 1, 2005).
[7]. Web Intelligence Consortium, http://wi-consortium.orgYao, J.T. and Yao, Y.Y. Web-based support systems, Proceedings of 2003WI/IAT Workshop on Applications, Products and Services of Web-basedSupport System (WSS 2003), 63-67, 2003.
[8]. Yao, J.T. and Yao, Y.Y. Web-based information retrieval support systems:building research tools for scientists in the new information age, Proceedingsof the IEEE/WIC International Conference on Web Intelligence,57-573, 2003.
[9]. Yao, Y.Y. A framework for Web-based research support systems, Proceedingsof COMPSAC'2003, 601-606, 2003.
[10]. Yao, Y.Y. Web-based research support systems, Proceedings of theSecond International Workshop on Web-based Support Systems, 1-6,2004.
[11]. Yao, Y.Y., Zhong, N., Liu, J. Web-based support systems, manuscript,2005.
[12]. J. Liu, N. Zhong, Y. Y. Yao, Z. W. Ras, The wisdom web: newchallenges for web intelligence (WI), J. Intell. Inform. Sys.,20(1): 5–9, 2003.
[13]. J. Liu, Web intelligence (WI): what makes wisdom web? Proc.Eighteenth International Joint Conference on Artificial Intelligence(IJCAI-03), 2003, pp. 1596–1601.
[14]. J. Liu, New challenges in the world wide wisdom web (W4)research, in N. Zhong, et al. (eds.), Foundations of IntelligentSystems, LNAI 2871, Springer, 2003, pp. 1–6.
[15]. Y. Y. Yao, N. Zhong, J. Liu, and S. Ohsuga, Web intelligence(WI): research challenges and trends in the new informationage, in N. Zhong, et al. (eds.), Web Intelligence: Research andDevelopment, LNAI 2198, Springer, 2001, pp. 1–17.
[16]. N. Zhong, J. Liu, Y. Y. Yao, and S. Ohsuga, Web intelligence(WI), Proc. 24th IEEE Computer Society International ComputerSoftware and Applications Conference (COMPSAC2000), Piscataway, NJ: IEEE CS Press, 2000, pp. 469–470.
[17]. N. Zhong, Y. Y. Yao, and M. Ohshima, Peculiarity oriented multi-database mining, IEEE Trans. Knowl. Data Engineer.,15(4): 952–960, 2003.
[18]. J. Hu and N. Zhong, Organizing multiple data sources for developing intelligent e-Business Portals, Data MiningKnow. Dis., 12 (2–3): 127–150, 2006.
[19]. M. Cannataro, and D. Talia, The knowledge grid, CACM, 46:89–93, 2003.: N. Zhong, J. Hu, S. Motomura, J. L. Wu, and C.
[20]. Liu, Building a data mining grid for multiplehumanbrain dataanalysis, Computat. Intell., 21(2): 177–196, 2005.
[21]. J. Nabrzyski, J. M. Schopf, J. Weglarz, Grid Resource Management,Dordrecht: Kluwer, 2004.
[22]. Voilent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
[23]. M.Missikoff, R. Navigli, P. Velardi, Integrated approach to web ontology learning and engineering, IEEE Computer, 35(11):60–63, 2002.
[24]. N. Zhong, Representation and construction of ontologies for web intelligence, Internat. J. Foundations Comp. Sci., 13(4):555–570, 2002.
[25]. R. Kumar, P. Raghavan, S. Rajagopalan, A. Tomkins, The weband social networks, IEEE Computer, 35 (11): 32–36, 2002.
[26]. W. Li, N. Zhong, J. Liu, Y. Y. Yao, C. Liu, Perspective of Applying the Global E-mail Network, Proc. 2006 IEEE/ WIC/ACM International Conference on Web Intelligence(WI'06), IEEE Computer Society Press, pp. 117–120, 2006.

.

About Author

Vishal Singh received B.Tech (C.S.E.) degree in 2012 from Dr. A.I.T.H., Kanpur, India and pursuing M.Tech (C.S.E.) final year degree admitted in 2012 from PSIT, Kanpur, India. One International journal paper has been published found at:
http://www.erpublications.com/uploaded_files/download/download_07_03_2014_14_15_24.pdf
E-mail: vishalsingh1807@gmail.com
Contact: +91 9580672832