Journal scientific and applied research, vol. 3, 2013
Association Scientific and Applied Research
International Journal

Original Contribution ISSN 1314-6289

A TAXONOMY OF THE CYBER ATTACKS

Petar K. Boyanov

DEPARTMENT OF COMMUNICATION AND COMPUTER TECHNIQUES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN
E-MAIL: PESHOAIKIDO@ABV.BG

ABSTRACT: *In this paper is made a sophisticated taxonomy of the malicious cyber attacks. The cyber attacks are summarized into several mainly types with additional subtypes for everyone attack. Thanks to the achieved comparative results in this paper many users can find and analyze different flaws and vulnerabilities in their computer and network systems and thereby they could detect and prevent future malicious cyber attacks.*

KEY WORDS: *Cyber attacks, Vulnerabilities, Unauthorized access, Computer and network security, Taxonomy.*

1. Introduction

Most of the accomplished cyber crimes are based on the flaws and vulnerabilities in computer and network systems. Thereby the smart knowledge of the cyber criminals find a way to implement and exploit dangerous malicious computer and network attacks, which cause irreparable damages to the important and confidential computer and network resources [1] - [30].

Previous technical papers presented different methodologies and taxonomies in order to explain and describe the different cyber attack types and the purpose of this paper was to analyze and summarize the different cyber attack classifications in order to achieve comparative results, which could cause an useful influence for the network administrators, software programmers and users in the process of detecting and preventing future cyber attacks [1] - [30].

This paper is structured as follows. First, in section 2, the relative analyzes and performances of the malicious cyber attack taxonomies are compared. After that, in section 3, a sophisticated cyber attack taxonomy is composed. The advantages and limitations of the achieved final cyber attack classification as well as the upcoming future work are concluded in section 4.

2. A relative analysis and performances of the malicious cyber attack taxonomies

Retaining computer and network security against cyber attacks is a serious problem, that constantly

causes huge damages such as stealing login credentials of the users, unauthorized electronic money drawing from the credit cards, malicious intrusions into the computer systems in order to interception the user conversation or to delete critical important electronic documents and resources, etc. [4], [5], [7], [8], [9], [10], [11], [12], [14], [25]. Hence, the main aim in this paper is to summarize and classify the highly varied computer and network attacks.

First, this study will analyze and compare the related studies to the cyber attacks. After this, a sophisticated classification of the most dangerous and malicious computer and network attacks will be made.

In [7] Hansman explained the relationship between network and computer attacks and in addition to him research he separated the cyber attacks into four dimensions such as type of the attack, target of the attack, mischievous vulnerabilities techniques and types of payload attacks. Ye at el. [30] made a framework for attack classification with placing the emphasis on the risk evaluation and assessment. Friedman and Hoffman [5] both gave a taxonomy of security vulnerabilities and threats to mobile computing. Igure and Williams [11] also gave a classification of the cyber attacks and made a comprehensive analysis of the flaws and vulnerabilities in the computer systems. Their mainly aim was to describe the types of attacks, future goals, measurement of the classification and descriptions.

In [16] Meyers, Powers, and Faissol analyzed and investigated the types of cyber adversaries and malicious attacks. Their taxonomy was different oriented and was separated into three groups such as class of the attack, subtypes of the attack and additional information for the given attack. Another type of cyber attack classification was given in [26], that described the type of the attack, influence on the operating system device, specific defense techniques and applied damages. Stiawan [29] summarized a lot of different types of attack and additional depicted varied viruses according to cisco systems.

There are also other previous studies, that presented and suggested detailed types of different cyber attacks, including viruses, malwares, keyloggers, rootkits, spywares, worms, trojans, denial of service (DoS), distributed denial of service (DDoS) intrusion detection system attacks, networks exploits, web applications attacks, wireless attacks, social engineering, buffer overflow and sniffers [1], [2], [3], [6], [13], [15], [18], [19], [20], [21], [22], [23], [24], [26].

3. A sophisticated cyber attack taxonomy

After analyzing and comparing the achieved results of all papers of investigations, in this study was systematized a sophisticated classification of varied malicious cyber attacks. This classification is consisted of [1] - [30]:

- Information Footprinting and Reconnaissance attacks [5], [30];
- Information Scanning attacks;
- Enumeration attacks [21], [30];
- Information System attacks;
- Trojan and Backdoor attacks;
- Virus attacks;
- Worm attacks;
- Sniffer attacks;
- Social Engineering attacks;
- Denial of Service attacks;
- Session Hijacking attacks;
- Webserver vulnerabilities attacks;
- Web-based applications attacks;
- Wireless network attacks [20], [21];
- Intrusion Detection System (IDS), Firewalls and Honeypots attacks;
- Buffer overflow attacks;
- Physical attacks.

The Footprinting and Reconnaissance attacks

The Footprinting and Reconnaissance attack [5], [30] is characterized as gathering and collecting a lot of information about the selected victim. This attack thoroughly includes a set of blended mechanisms for assessment the version and the modification of the used operating system, version of the used webserver, the range of IP addresses in the selected network, etc. This attack includes the following attacking subtypes [5], [30]:

- Internet footprinting and reconnaissance attacks;
- Website footprinting and reconnaissance attacks;
- DNS footprinting and reconnaissance attacks;
- Google footprinting and reconnaissance attacks and etc.

The Information Scanning attacks

The Information Scanning attack scans only determinate targets in order to obtain information about the used IP addresses, the opened TCP or UDP ports, the version and platform of the used operating systems and the started services and processes in the target host. This attack includes the following attacking subtypes [1], [6], [7] - [16], [28], [29]:
TCP handshake scanning attack, Stealth scan attack, Xmas scanning attack, FIN scanning attack, Null scanning attack, Idle scanning attack, UDP scanning attacks, etc..

Enumeration attacks

Enumeration attacks pull up varied information about the computer names, users, passwords, shared host and network resources. The criminals use this attack only in Local Area Networks (LANs) environments [15], [21], [30]. The Enumeration attack uses different attacking subtypes:

- Lightweight Directory Access Protocol (LDAP) attacks;
- Network Basic Input/Output System (NetBios) attacks;
- Simple Mail Transfer Protocol (SMTP) attacks;
- Simple Network Management Protocol (SNMP) attacks;

- Network Time Protocol (NTP) attacks;
- Domain Name System (DNS) attacks, etc [15], [21], [30].

Information system attacks

Information system attacks are set of several blended malicious attack techniques. These attacks cause huge damages to the selected device targets. Information system attacks consist of:

- **Password attacks** such as Dictionary attacks, Brute force attacks, Hybrid attacks, Syllable attacks, Default password attacks, Manual guessing password attacks, atc [1], [7], [11], [12], [25], [16].
- **Keylogger attacks** are divided into two groups - Hardware keystroke attacks and Software keystroke attacks [5], [6], [7], [8], [10]. [16].
- **Spyware attacks** are a lot of types of spyware attacks such as Multimedia spyware attacks (audio and video), Desktop attacks, GPS attacks, Print attacks, Fax attacks, USB attacks, Print Screen Capturing attacks and Cell phone attacks [6], [7], [16], [23], [29].
- **Rootkit attacks** as separated into several levels Rootkits attacks like Kernel, Hardware and Application level Rootkit attacks, etc [1] - [30].

Trojans and Backdoors attacks

Trojans and Backdoors attacks are the most malicious and maleficent attacking programs, that can cause incorrigible damages to all electronic devices. Actually trojans are programs, that contain a maleficent code wrapped into an executable file with extensions ending at .exe, bat, com and also with a hidden file extension [6], [7] - [30]. There are lots of Trojan attacking subtypes [15], [24] - [30]:

- Credit Card attacks;
- E-banking attacks;
- Hypertext Transfer Protocol (Http);
- Hypertext Transfer Protocol Secure (Https) attacks;
- Botnet attacks;
- Internet Control Message Protocol (ICMP) attacks;
- Mobile Computing attacks;
- Remote login and access attacks, etc [1], [3], [4], [6], [7],[16], [29].

Virus attacks

The virus is a self-replicating program that copies and replicates the own code into other executable files. The attacking subtypes of viruses are [16] - [30]: system and boot record, polymorphic, cluster, file, macro, shell, metamorphic, sparse infector, file, intrusive, extension, tunneling, encryption viruses, etc. [7].

Worm attacks

The worm [3], [5], [6], [7] is a self-replicating program that copies and replicates over public and private computer networks. The types of worms are - **Mass-mailing worms and Network-aware worms**.

The most dangerous worms are [6] - [30]:

- W32/Bangle.GE;
- W32/Netsky;
- W32/ Mydoom.B;
- W32/hllp.zori.c@M;
- W32/Feebs.gen@MM;
- W32/Detnat;
- W32/Virut; W32/MyWife, etc [6], [7], [15], [16], [29], [30].

Sniffer attacks

The sniffer is a new technique, that can eavesdrops the user information. In practice sniffer is an executable program or specific network device that intercepts and obtain some confidential information. The subtypes of sniffer attacks are [1], [7], [15] - [30]:

- Mac flooding attacks;
- Mac address spoofing and replicating attacks;
- Address Resolution Protocol (ARP) poisoning attacks;
- ARP spoofing attacks;
- Internet Protocol (IP) spoofing attacks;
- Domain Name System (DNS) Spoofing attacks;
- DNS Cache Poisoning attacks;
- Fraudulent Dynamic Host Configuration Protocol (DHCP) attacks;
- DHCP starvation attacks, etc. [29].

Social Engineering attacks

Social Engineering [7] is the most malicious and dangerous technique to break into computer and network systems regardless of installed Firewalls, Intrusion Detection Systems, Intrusion Prevent Systems, Virtual Local Area Networks, Virtual Private Networks, etc. [6], [16] - [29]. This attack is accomplished only by people, who have varied reasons to exposure top secret and confidential corporate information. There are two subtypes of this attack - **human-based attack and cyber-based attack** [15], [16].

Denial of Service attacks

This attack is based on the restricting and limiting the possibility the authorized and legitimate users to explore and use their computer and network resources [28]. There are mainly two types of denial of service attacks. The first attack type is **Denial of Service (DoS)** and it is consists of several subtypes such as [1], [6], [7], [14] - [30]:

- Bandwidth attacks;
- SYN Flooding attacks;
- ICMP Flooding attacks;
- Peer-to-Peer attacks and Botnet attacks;
- Ping of death attacks;
- Teardrop attacks;
- Smurf attacks, etc.

The second attack type is **Distributed Denial of Service (DDoS)** and it is consists of the following attack subtypes [5], [6], [9], [16] - [30]:

- TCP flooding attacks [6], [7], [16];
- UDP flooding attacks [29], [30];
- ICMP flooding attacks;
- Amplification attacks;

- Protocol oriented exploit attacks;
- Smurf attacks [15], [30];
- Fraggle attacks, etc [26], [28].

Session Hijacking attacks

Cyber criminals use Session Hijacking attack to steal the legitimate user ID session in order to intercept and snoop the transfer of information between several hosts [7]. This attack uses the following attacking subtypes [6], [15] - [30]:

- Man-in-the-browser attack;
- Session fixation attack;
- Sequence number prediction;
- IP spoofing attacks;
- Reset (RST) packet attacks;
- UDP spoofing attack;
- Blind attacks, etc.

Webserver vulnerabilities attacks

Webserver attacks are consisted of the following attack subtypes [15] - [30]:

- Web cache poisoning attack;
- Http response splitting attack;
- Directory Traversal attacks;
- Http response hijacking attacks;
- SSH brute-force attacks;
- Man-in-the-Middle attacks;
- Webserver password cracking attacks;
- Set of web application attacks, etc.

Web-based applications attacks

These attacks are thoroughly network-based attacks pointed against web application destruction. The subtypes of this attack are [1], [6], [7], [13] - [30]:

- Cross Site Scripting (XSS) attacks;
- SQL Injection attacks;
- Cookie Poisoning attacks;
- Misconfiguration attacks;
- Platform exploits attacks;
- Parameter tampering attacks;
- Injection flaw attacks;
- Command injection attacks;
- LDAP Injection attacks;
- Hidden File Manipulation attacks;
- Cross-Site Request Forgery (CSRF) attacks;
- Denial of Service (DoS) attacks;
- Buffer overflow attacks;
- Web services attacks;
- XML Poisoning attacks, etc.

Wireless network attacks

These attacks include the following attacking subtypes [7], [16], [21], [22]:

- Media Access Control (MAC) Address Spoofing attacks;
- Rogue Access Point attacks;
- WEP Injection attacks;
- Data Frame Injection attacks;
- Cracking WEP key attacks;
- Eavesdropping attacks [21], [22];
- Masquerading attacks [15], [16];
- Beacon Flooding attacks;
- ARP Cache Poisoning attacks;

- Routing attacks;
- VPN Login cracking attacks [30] ;
- Shared Key Guessing attacks, etc.

Intrusion Detection System (IDS), Firewalls and Honeypots attacks

Intrusion Detection systems, Firewalls and Honeypots [2], [5] are software programs or hardware devices, that aimed to detect, analyze, stop and prevent malicious attacks from cyber criminals (hackers and crackers). The attacking subtypes include [1] - [30]: IDS insertion attacks, Denial of Service attacks (DoS) attacks, False-Positive Generating attacks, Session Splicing attacks, IDS Fragmentation attacks, Polymorphic shellcode attack, IP Address spoofing, Additional Evading Firewall attack techniques, etc. [2], [5], [7], [11], [15] - [30].

Buffer overflow attacks

a full control to determined process of the computer system in order to block and destroy the significant executing processes in the system [1] - [30]. There are only two attacking subtypes - **Stack-based buffer overflow attacks** and **Heap-based buffer overflow attacks** [7], [15], [16], [29], [30].

Physical attacks

These attacks are mainly aimed to damage and crash the physical devices and elements of a computer system and network. The subtypes of this attack are: Physical shearing of power supply cable or network cable, Putting explosives to subvert the whole computing system, High energy radio frequency (HERF) attacks, Low energy radio frequency (LERF) attacks, Electro-magnetic pulse (EMP) attacks, Van Eck Attacks, etc. [1] - [30]. The sophisticated taxonomy of cyber attacks is shown in table 1.

Table 1. *A sophisticated taxonomy of cyber attacks*.

Attack type	*Attack subtype*
Information Footprinting and Reconnaissance attacks	*Internet footprinting and reconnaissance attacks, Website footprinting and reconnaissance attacks,* *DNS footprinting and reconnaissance attacks, Google footprinting and reconnaissance attacks.*
Information Scanning attacks	*TCP handshake scanning attack, Stealth scan attack, Xmas scanning attack, FIN scanning attack, Null scanning attack, Idle scanning attack, UDP scanning attack.*
Enumeration attacks	*Lightweight Directory Access Protocol (LDAP) attack, Network Basic Input/Output System (NetBios) attack, Simple Mail Transfer Protocol (SMTP) attack, Simple Network Management Protocol (SNMP) attack, Network Time Protocol (NTP) attack, Domain Name System (DNS) attack.*
Information System attacks	***Password attacks*** *- Dictionary attacks, Brute force attacks, Hybrid attacks, Syllable attacks, Default password attacks, Manual guessing password attacks* ***Keylogger attacks*** *- Hardware keystroke attacks and Software keystroke attacks* ***Spyware attacks*** *- Multimedia spyware attacks (audio and video), Desktop attacks, GPS attacks, Print attacks, Fax attacks, USB attacks, Print Screen Capturing attacks and Cell phone attacks.* ***Rootkit attacks*** *- Kernel, Hardware and Application level Rootkit attacks.*
Trojan and Backdoor attacks	*Credit Card attacks, E-banking attacks, Hypertext Transfer Protocol (Http) and Hypertext Transfer Protocol Secure (Https) attacks, Botnet attacks, Internet Control Message Protocol (ICMP) attacks, Mobile Computing attacks, Remote login, access attacks.*
Virus attacks	*System and boot record, polymorphic, cluster, file, macro, shell, metamorphic, sparse infector, file, intrusive, extension, tunneling and encryption viruses.*
Worm attacks	*Mass-mailing worms and Network-aware worms.* *The most dangerous worms are W32/Bangle.GE, W32/Netsky, W32/ Mydoom.B, w32/hllp.zori.c@M, W32/Feebs.gen@MM, W32/Detnat, W32/Virut, W32/MyWife.*
Sniffer attacks	*Mac flooding attacks, Mac address spoofing and replicating attacks, Address Resolution Protocol (ARP) poisoning attacks, ARP spoofing attacks, Internet Protocol (IP) spoofing attacks, Domain Name System (DNS) Spoofing attacks, DNS Cache Poisoning attacks, Fraudulent Dynamic Host Configuration Protocol (DHCP) attacks, DHCP starvation attacks.*
Social Engineering attacks	*Human-based attacks and cyber-based attacks*
Denial of Service attacks	***Denial of Service (DoS) attacks*** *- Bandwidth attacks, SYN Flooding attacks, ICMP Flooding attacks, Peer-to-Peer attacks, Botnet attacks, Ping of death attacks, Teardrop attacks, Smurf attacks.* ***Distributed Denial of Service (DDoS) attacks*** *- TCP flooding attacks, UDP flooding attacks, ICMP flooding attacks, Amplification attacks, Protocol oriented exploit attacks, Smurf attacks and Fraggle attacks.*
Session Hijacking attacks	*Man-in-the-browser attack, Session fixation attack, Sequence number prediction, IP spoofing attacks, Reset (RST) packet attacks, UDP spoofing attack and Blind attacks.*
Webserver vulnerabilities attacks	*Web cache poisoning attack, Http response splitting attack, Directory Traversal attacks, Http response hijacking attacks, SSH brutefore attacks, Man-in-the-Middle attacks, Webserver password cracking attacks and set of web application attacks*
Web-based applications attacks	*Cross Site Scripting (XSS) attacks, SQL Injection attacks, Cookie Poisoning attacks, Misconfiguration attacks, Platform exploits attacks, Parameter tampering attacks, Injection flaw attacks, Command injection attacks, LDAP Injection attacks, Hidden File Manipulation attacks, Cross-Site Request Forgery (CSRF) attacks, DoS attacks, Buffer overflow attacks, Web services attacks, XML Poisoning attacks*
Wireless network attacks;	*Media Access Control (MAC) Address Spoofing attacks, Rogue Access Point attacks, WEP Injection attacks, Data Frame Injection attacks, Cracking WEP key attacks, Eavesdropping attacks, Masquerading attacks, Beacon Flooding attacks, ARP Cache Poisoning attacks, Routing attacks, VPN Login cracking attacks, Shared Key Guessing attacks.*
Intrusion Detection System (IDS), Firewalls and Honeypots attacks	*IDS insertion attacks, Denial of Service attacks (DoS) attacks, False-Positive Generating attacks, Session Splicing attacks, IDS Fragmentation attacks, Polymorphic shellcode attack, IP Address spoofing, Additional Evading Firewall attack techniques.*
Buffer overflow attacks	*Stack-based buffer overflow attacks and Heap-based buffer overflow attacks.*
Physical attacks	*Physical shearing of power supply cable or network cable, Putting explosives to subvert the whole computing system, High energy radio frequency (HERF) attacks, Low energy radio frequency (LERF) attacks, Electro-magnetic pulse (EMP) attacks, Van Eck Attacks.*

3. Conclusion and future work

In this paper a sophisticated classification of varied malicious cyber attacks is achieved and summarized. Thanks to this classification of cyber attacks, many IT experts, software programmers, Web developers and users can understand and find the crucial flaws and vulnerabilities in their information and computing systems and thereby they can prevent future unauthorized penetration using difference defense techniques and methods.

However, there is no explanation for applied and developed countermeasures and penetration tests against the cyber attacks in this paper. Some practical issues like analyzing and building countermeasures against the varied malicious cyber attacks in computer and network systems need to be done in my further researches and investigations.

References:

[1] Avizienis, Algirdas,. Laprie J-C., Randell Brian., and Landwehr Carl., "Basic concepts and taxonomy of dependable and secure computing." Dependable and Secure Computing, IEEE Transactions on 1, no. 1 (2004): 11-33.

[2] Bråthen A., "Correlating IDS alerts with system logs by means of a network-centric SIEM solution." (2011).

[3] Collins M., Gates C., and Kataria G., "A model for opportunistic network exploits: The case of P2P worms." In Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK. 2006.

[4] De Vries J. A., Warnier M. E., and Hoogstraaten H., "Towards a roadmap for development of intelligent data analysis based cyber attack detection systems." (2012).

[5] Friedman J., and Hoffman D. V., "Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses." Information, Knowledge, Systems Management 7, no. 1 (2008): 159-180.

[6] Hajian S., And Hendessi Faramarz B M., "A Taxonomy for network vulnerabilities." International Journal Of Information And Communication Technology (Ijict) (2010).

[7] Hansman S., and Hunt R., "A taxonomy of network and computer attack methodologies." Retrieved March 22 (2003): 2007.

[8] Hansman S., and Hunt R., "A taxonomy of network and computer attacks." *Computers & Security* 24, no. 1 (2005): 31-43.

[9] Howard J. D., An analysis of security incidents on the Internet 1989-1995. CARNEGIE-MELLON UNIV PITTSBURGH PA, 1997.

[10] Howard J. D., and Longstaff T. A., "A common language for computer security incidents." Sandia Report: SAND98-8667, Sandia National Laboratories, http://www. cert. org/research/taxonomy_988667. pdf (1998).

[11] Igure V., and Williams R., "Taxonomies of attacks and vulnerabilities in computer systems." Communications Surveys & Tutorials, IEEE 10, no. 1 (2008): 6-19.
[12] Климовский А. А., "Таксономия кибератак и ее применение к задаче формирования сценариев их проведения." Труды Института системного анализа Российской академии наук 27 (2006): 74-107.
[13] Kjaerland M., "A taxonomy and comparison of computer security incidents from the commercial and government sectors." Computers & Security 25.7 (2006): 522-538.
[14] Lipson H. F., "Tracking and tracing cyber-attacks: Technical challenges and global policy issues." (2002).
[15] Lough D. L., (2001). A taxonomy of computer attacks with applications to wireless networks (Doctoral dissertation).
[16] Myers C., Powers S., and Faissol D., "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches." Lawrence Livermore National Laboratory (April 2009) 7 (2009).
[17] Meyers C., Powers S., and Faissol D., Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2009.
[18] Mishra B. K., and Saini H., "Cyber Attack Classification using Game Theoretic Weighted Metrics Approach." (2009).
[19] Monahan-Pendergast, MaryTheresa. "Attack Evolution: Identifying Attack Evolution Characteristics to Predict Future Attacks." PhD diss., 2006.
[20] Nasr K., El Kalam A. A., and Fraboul., "Generating Representative Attack Test Cases for Evaluating and Testing Wireless Intrusion Detection Systems." International Journal of Network Security & Its Applications (IJNSA) 4, no. 3 (2012): 1-19.
[21] Nunes S. R., "Web attack risk awareness with lessons learned from high interaction honeypots." PhD diss., CARNEGIE MELLON UNIVERSITY, 2009.
[22] Rutkowska J., "Introducing stealth malware taxonomy." COSEINC Advanced Malware Labs (2006).
[23] Saber M., Bouchentouf T., Benazzi A., and Azizi M., "Amelioration of attack classifications for evaluating and testing intrusion detection system." Journal of Computer Science 6, no. 7 (2010): 716-722.
[24] Sharma A., Kalbarczyk Z., Iyer R., and Barlow J., "Analysis of credential stealing attacks in an open networked environment." In Proc. of the Fourth International Conference on Network and System Security. Washington, DC, USA: IEEE Computer Society, pp. 144-151. 2010.
[25] Simmons C., Shiva S., Dasgupta D., and Wu Q., "AVOIDIT: A cyber attack taxonomy." University of Memphis, Technical Report CS-09-003 (2009).
[26] Singh P. K., Vatsa A. K., Sharma R., & Tyagi P., “Taxonomy

based intrusion attacks and Detection management scheme in peer-to-peer network", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012
[27] Specht S M., and R. B. Lee., "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures." In Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, pp. 543-550. 2004.
[28] Stiawan D., "Network Security Violation: a review."
[29] Ye N., Newman C., and Farley T., "A system-fault-risk framework for cyber attack classification." Information, Knowledge, Systems Management 5, no. 2 (2006): 135-151.
[30] Van Heerden R. P., Irwin B., and Burke I. D., "Classifying network attack scenarios using an Ontology." Academic Conferences Limited, 2012