Intrusion Detection Using Network Monitoring Tools

Gopal Singh
Department of Cyber Law & Information Tech
NLIU, Bhopal (M.P.), India
singh_gopal13@yahoo.co.in

Sachin Goyal
Department of Information Technology
UIT, RGPV Bhopal (M.P.), India
sachingoyal@rgtu.net

Ratish Agarwal
Department of Information Technology
UIT, RGPV Bhopal (M.P.), India
ratish@rgtu.net

ABSTRACT- This paper is mainly concern about how network monitoring, using software tools can be helpful for protection of our communication network, how different kind of network attacks is perform. Now these days network security is main concern for each organization due to this, network monitoring has become an important part of computer security to prevent the attack. There are several other ways to protect communication network such as firewalls, VPN (Virtual Private Network), encryption techniques after all these techniques some time intruder can intrude our communication network. So in this condition network monitoring tools such as Wireshark and Snort play important role in intrusion detection. Wireshark and Snort is capable to monitor network processes or movements in a graphical way to detect intrusion. Network monitoring through IDS and IPS, is increasing the performance and security of the network infrastructure.

KEYWORDS- IDS, IPS, Wireshark, Snort, SQL Injection, Cross Site Scripting, Social Engineering.

I. INTRODUCTION

These days technology changing its way to process new way to perform attack is being come in our knowledge some time existing security parameters is bypass by these novel attacks. So that time, network monitoring plays a significant role in intrusion detection. Tools such as Wireshark and Snort provide graphical view of network processes so that by analyzing these network processes or traffic intrusion can be detected in a easy way.

Today by the use of internet global access is possible, and intruders are making effort to access their malicious intent so Intrusion Detection System is too important to protect our communication network or network system against the outsider attacks as well as insider, to execute their malicious intent in digital environment. Although Wireshark is not a dedicated IDS but its provide feature to detect intruder.

Network monitoring is defined as, "Network monitoring is spying for a good cause. Actually, it's something you want at least one of your systems to be doing. While your other systems are performing their vital functions, you need to set aside at least one computer or set of computers to monitor network activity. Think of this as policing your network traffic".[1]

II. REVIEW OF LITERATURES

A number of papers have been presented by distinguish authors in this area. Some important contributions are given below.

Day by day technology is growing, new kind of tools and techniques are being introduce, in the same way new types of malicious codes are also being invented. D. Stiawan [1], et al. have discussed about that at the

[1] Network monitoring definition available at: <http://www.wisegeek.org/what-is-network-monitoring.htm> Visited on 17/03/2014

very earlier in 1990s when hackers or attackers, started to intrude the network and computer system that time IDS was only capable to detect hostile traffic and sent alert message or signal, but there was no prevention mechanism of attack, also not able to detect all malicious programmes.

Intrusion is a combination of actions aimed at compromising the basic network security pillars confidentiality, integrity, availability of a computing or networking resource. Although IDS is only limited up to intrusion reporting to administrator while IPS is advance version of IDS, which is capable to prevent intrusion as well as detection. A. S. Ashoor [2], et al. have discussed, IDS and IPS are mainly developed for lacking requirements of devices such as firewalls. IDS is mainly used to detecting the intrusion or threat in the network.

What should be parameters to select an IDS?, there are mainly two types of IDS, one is host based and another is network based and available as freeware and commercial also difficult to decide to use whether freeware or commercial. This selection of the IDS also depend on the cost effectiveness and how it is going to secure an organization. D. Mathew [3], have discussed Although by implementing an IDS we cannot say that an organization is fully secure but, yes it will be integral part of the particular section of the organization's security. With the combination of IDS and strong organizational policies and procedures, vulnerability assessments at particular interval of time, secure configuration of routers and firewalls can produce effective results and also can mitigate the risk which an organization facing.

Security is a big issue for all networks in present organization environment. Different methods have been developed to secure the network communications and communication over the Internet, between them the use of firewalls, encryption, and VPN (Virtual Private Networks). Intrusion detection is a comparatively new against the all such techniques. IDS can protect a system from attack, misuse, and compromise, also monitor network activity. R. S. Shirbhate in [4], et al. have discussed, Network process monitoring is increasingly observed as an important function for understanding and improving the processes and security of our cyber infrastructure. The IDS mix the use of pattern matching, stateful pattern matching for rectifying the intruder. The IDS techniques should be economical, practical, cost-efficient, and commercially possible.

Prevention is better than cure, with keeping this in mind combination of both IDS and IPS can provide defense in depth means layered security for the network or system, if in case intrusion is not prevented by the IPS so it's detection will be possible to mitigate the network risks. T. Holland [5], have discussed, Security = visibility + control, IDS technology offers the visibility and provide many other advantages directly related to monitoring the networks. These include the live visibility of what is going on in our networks also as well as the ability to store this information for analysis and reporting at a later point of time. Visibility is prime to decision making. Visibility makes it possible to create a security policy based on quantifiable, real world data.

Conventional intrusion detection systems had some limitations and do not provide a complete solution for the problem. A. Youssef [6], et al. have discussed, Data Mining (DM), Network Behavior Analysis (NBA) for intrusion detection. According to the researcher combination of both DM and NBA potential to detect intrusions in networks more successfully. In this, there are two types of Intrusion Detection Systems (IDS) which is misuse detection systems and anomaly detection systems. Almost commercial IDS utilize the misuse approach in which known intrusions are stored in the systems as signatures. The IDS searches network traffics for intrusive patterns or user behaviors which match the stored signatures, if a pattern matched with a stored signature then an alarm or signal is raised to a security analyst who take decision that what action should be taken based on the type of attack. In anomaly detection, in difference with misuse detection, can identify novel intrusions. It makes models for normal network behavior also called profiles and also detect patterns that much deviate from the stored profiles. These patterns may be suspicious represent as actual intrusions or could basically be a new behavior that need to add in profile for future references.

T. Lappas [7], et al. have discussed, about off line and real time processing in data mining where in off line processing data mining techniques in IDSs, means analysis of the collected data in off line mode by using this way real time detection tasks will be effective. Detection rule analysis, provide good future analysis of intruder and off line mode provide ability to transfer logs from remote sites to centralized system for analysis. In real time analysis of data mining in IDS also develop resourceful approaches that use data on packet header values for network anomaly detection.

Although an IDS is not a fully solution for security but after all, by configuring an IDS in well manner a system administrators can protect their system or network up to the mark. T. Sharma [8], et al. have discussed, some features must have an IDS, discussed by the researcher which is, there should not any human supervisory requirement for regular processing of an IDS, an IDS should be fault tolerant and survivable, it should impose minimal overhead, good observer of deviations from normal behavior network traffic, should be difficult to fool.

Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide . J. Gomez et al. [9] have discussed, H-Snort concept before going further basic of snort working. Snort is an IDPS (Intrusion Detection and Prevention System) which is mainly works on the principle of signature based detection and anomaly based detection and they have their own limitations. In signature based detection, Snort matches the network traffic signature with predefined signature which is present in the library or database of the snort which can continuously updated. Signature based detection gives better performance when it matches the pattern but it is not able to detect new kind of attacks which is not present in the database of snort.

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions . Although wireshark is not either an IDS or IPS but, It can be consider as intrusion detection. S. Gupta et al. [10], the expert info’s is a kind of log of the anomalies found by Wireshark in a capture file. Each expert info will contain the following things, Chat (grey): information about usual workflow e.g. a TCP packet with the SYN flag set, Note (cyan): notable things e.g. an application returned a "usual" error code like HTTP 404, Warn (yellow): warning e.g. application returned an "unusual" error code like a connection problem, Error (red): serious problem e.g. [Malformed Packet]. Intrusion detection can be possible in chat section of the wireshark in which the TCP connection should contain sequence of SYN, SYN+ACK and ACK messages. With the analysis of chat section we can identify the DOS attack and its originating IP. By using firewall ACL Rules which is present in the wireshark firewall can be applied for any of the IP address which we want to deny/allow packet from that particular IP address. Also by using Flow Graph part of the wireshark flow graph shows the communication between two or more different IP’s. If TCP flow graph in which only SYN message is transmitted from client to server using various port number and no any other message mean (SYN+ACK and ACK) is transmitted between the two IP so, on the basis of this we can say connection is not established and DOS attack detected. Another one is by analysis of conversation section intrusion cab be identify. A network conversation is the traffic between two specific endpoints. For example, an IP conversation is all the traffic between two IP addresses.

Network monitoring is the best way to rectify the intruder, there are some software tools which is useful for network monitoring according to research. Sujindar S. et al. [11], have discussed about different monitoring tools which are following: AirWave, Cisco WCS (Wireless control system), 7Signal Sapphire, Big Sister, Cacti, Cricket, MRTG (Multi Router Traffic Grapher), RRDTOOL, Kiwi syslog, Splunk, Nagios, RANCID (Really Awesome New Cisco Config Differ), SNORT, NFDUMP/NFSEN, SmokePing, Munin, NetDisco, WhatsUp Gold, ZABBIX, NAV (Network Administration Visualized), NetXMS, ZENOSS. Apart from these other open source intrusion detection tools are SURICATA, Bro, KISMET, OSSEC, Samhain, Open DLP (Data Loss Prevention).

III. POSSIBLE ATTACKS

SQL Injection Attack, Cross Site Scripting Attack, Brute force and dictionary, Attack, Denial of Service Attack/ Distributed DOS (DOS/DDOS), Social Engineering Attack. Apart from these attacks there are also other attacks such as Zero day attacks, Spoofing, Man in the middle attacks, Spamming, Virus, Worms and Trojans attack, Buffer overflows attack, Spyware, Botnets attack, Advanced Persistent Threats (APT).

SQL Injection Attack: A SQL injection attack consists of insertion or "injection" of a SQL query by means of the input data from the client to the application. In result of successful SQL injection exploit can read sensitive data from the database, change database data (Insert/Update/Delete), can perform administration operations on the database, recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.[2]

Cross Site Scripting Attack: Cross-Site Scripting (XSS) attacks are a type of insertion problem, in which malicious scripts/codes are injected into the otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.[3]

Brute force and dictionary: Brute forcing consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement. In web application testing, the problem we are going to face with the most is very often connected with the need of having a valid user account to access the inner part of the application.[4]

Denial of Service Attack/ Distributed DOS (DOS/DDOS): In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that

[2] SQL (Structured Query Language) Injection attack, threat modeling and example. Available at <https://www.owasp.org/index.php/SQL_Injection> Visited on 19/03/2014

[3] Cross-Site Scripting, Available at <https://www.owasp.org/index.php/XSS> Visited on 19/03/2014

[4] <https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)> Visited on 19/03/2014

rely on the affected computer. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information.[5]

Social Engineering Attack: Social engineering is an 'art' of utilizing human behavior to breach security without the observer (or victim) even understanding that they have been operated. Although social engineering attack is possible through software tool such as Nmap and via internet. [12]
The social engineering is mainly classified in two categories first is computer or technology based deception and second is human based deception. In technological based social engineering it includes impersonation, dumpster diving, shoulder surfing, reverse social engineering. In human based social engineering popup windows, email attachment, online social engineering. In case of successful social engineering attack primary result will be security triad CIA (Confidentiality, Integrity, Availability) breach and the secondary result will be commercial, reputational harm. [13]

IV. INTRUSION DETECTION USING NETWORK MONITORING TOOL

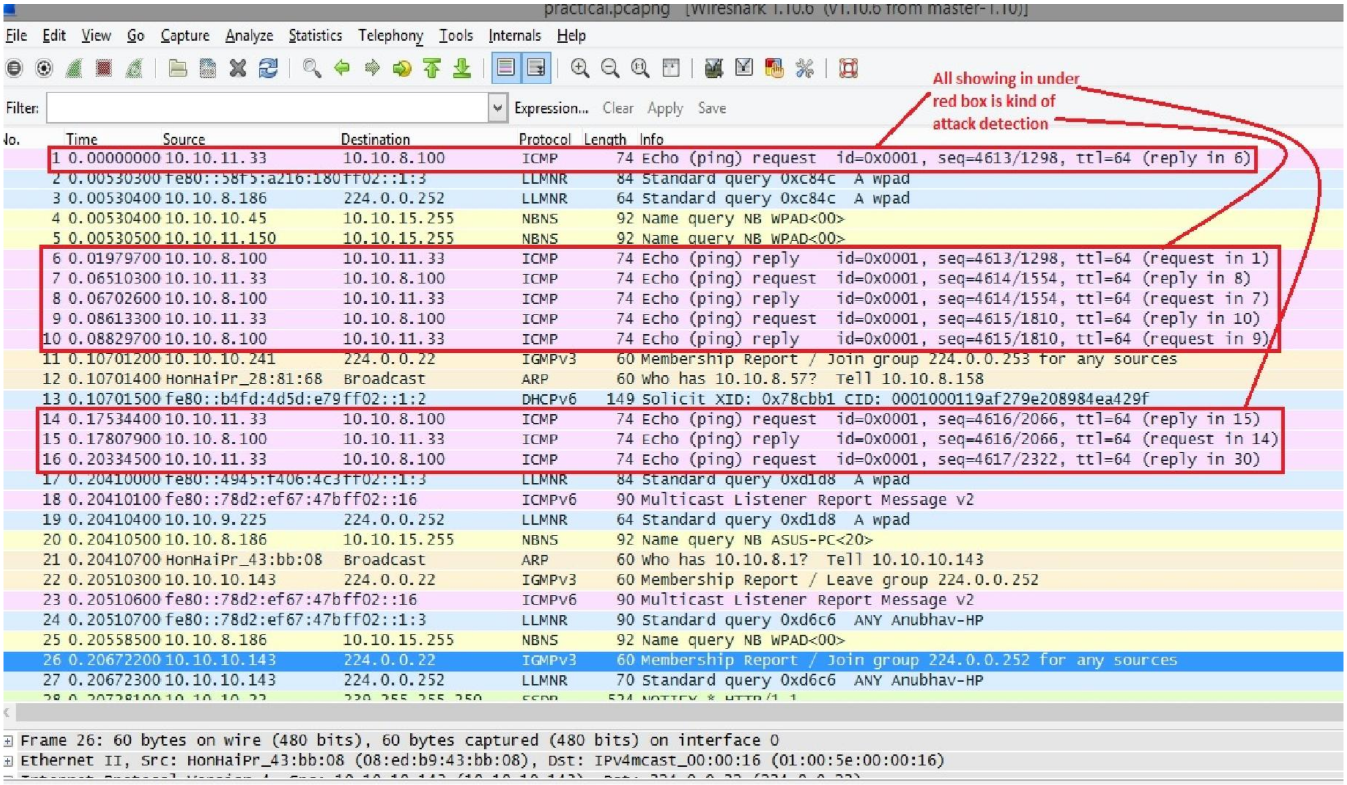
Here in this paper, we are taking Wireshark and Snort for intrusion detection. Below giving brief details of tools respectively.
Wireshark is an open source network packet analyzer tool that captures data packets flowing over the wire (network) and presents them in an understandable form. Wireshark can be considered as a Swiss army knife as it can be used under different circumstances such as network troubleshoot, security operations, and learning protocol internals. This one tool does it all with ease.[14]
Snort is a modern security application with three main functions: it can serve as a packet sniffer, a packet logger, or a Network-based Intrusion Detection System (NIDS).There are also many add-on programs to Snort to provide different ways of recording and managing Snort logfiles, fetching and maintaining current Snort rule sets, and alerting to let your admin know when potentially malicious traffic has been seen. Although not part of the core Snort suite, the add-ons provide a rich variety of features to the security administrator. As you will see, there are many ways to use Snort as part of your company's security design.[15]

Intrusion Detection Practical Approach Through Wireshark: Although Wireshark is not either an IDS or IPS but due to its functionality and features, up to certain limit it can be consider as an IDS. Wireshark has a coloring rule which can be configure or edit according to users instruction. Default coloring rule tells about bad packet, checksum error, and other common packet errors that may occur in a network on the basis of color categorization. Wireshark has some feature which can be helpful for intrusion detection. Using wireshark firewall can be applied for any of the IP address to deny/allow packet from that particular IP. Apart from this, there is a expert info in wireshark, which tells about malformed packet and severity of the packets (error) with packet number. Detection can be done through other means such as graph analysis where we can find which (IP) is communicating with which (IP). This can also be detected by conversation where we can see numbers of packets and bytes which being transferred between two system.

[5] DOS/DDOS, Available at <http://www.us-cert.gov/ncas/tips/ST04-015> Visited on 20/03/2014

In this whole scenario some where a IP is sending flood of ping request which can be a form of DOS or DDOS attact.

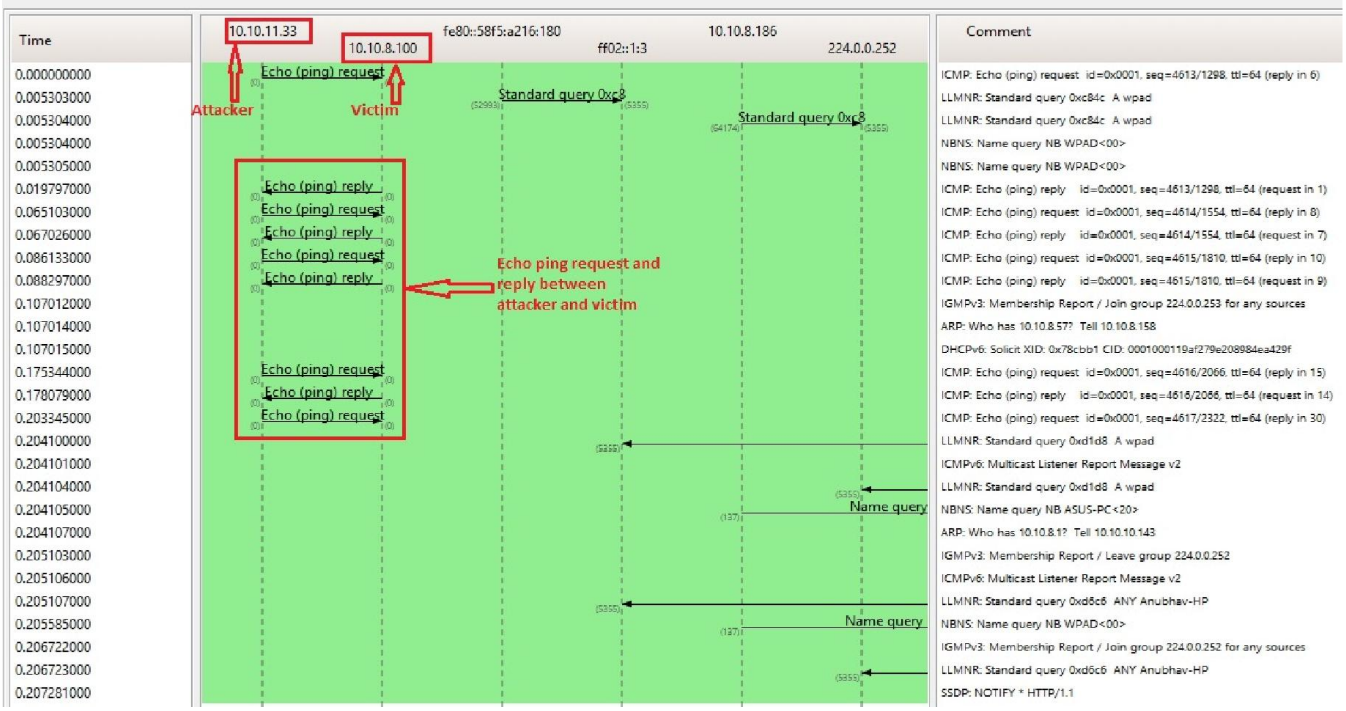
In the below screen short we can see a IP address 10.10.11.33 (attacker) is regularly sending ping request to IP address 10.10.8.100 (victim) which can affect the performance of the victim machine. Below showing



All showing in under red box is kind of attack detection

```
No.  Time        Source                   Destination      Protocol Length Info
  1 0.00000000 10.10.11.33              10.10.8.100      ICMP       74 Echo (ping) request  id=0x0001, seq=4613/1298, ttl=64 (reply in 6)
  2 0.00530300 fe80::58f5:a216:180      ff02::1:3        LLMNR      84 Standard query 0xc84c  A wpad
  3 0.00530400 10.10.8.186              224.0.0.252      LLMNR      64 Standard query 0xc84c  A wpad
  4 0.00530400 10.10.10.45              10.10.15.255     NBNS       92 Name query NB WPAD<00>
  5 0.00530500 10.10.11.150             10.10.15.255     NBNS       92 Name query NB WPAD<00>
  6 0.01979700 10.10.8.100              10.10.11.33      ICMP       74 Echo (ping) reply    id=0x0001, seq=4613/1298, ttl=64 (request in 1)
  7 0.06510300 10.10.11.33              10.10.8.100      ICMP       74 Echo (ping) request  id=0x0001, seq=4614/1554, ttl=64 (reply in 8)
  8 0.06702600 10.10.8.100              10.10.11.33      ICMP       74 Echo (ping) reply    id=0x0001, seq=4614/1554, ttl=64 (request in 7)
  9 0.08613300 10.10.11.33              10.10.8.100      ICMP       74 Echo (ping) request  id=0x0001, seq=4615/1810, ttl=64 (reply in 10)
 10 0.08829700 10.10.8.100              10.10.11.33      ICMP       74 Echo (ping) reply    id=0x0001, seq=4615/1810, ttl=64 (request in 9)
 11 0.10701200 10.10.10.241             224.0.0.22       IGMPv3     60 Membership Report / Join group 224.0.0.253 for any sources
 12 0.10701400 HonHaiPr_28:81:68        Broadcast        ARP        60 Who has 10.10.8.57?  Tell 10.10.8.158
 13 0.10701500 fe80::b4fd:4d5d:e79      ff02::1:2        DHCPv6    149 Solicit XID: 0x78cbb1 CID: 0001000119af279e208984ea429f
 14 0.17534400 10.10.11.33              10.10.8.100      ICMP       74 Echo (ping) request  id=0x0001, seq=4616/2066, ttl=64 (reply in 15)
 15 0.17807900 10.10.8.100              10.10.11.33      ICMP       74 Echo (ping) reply    id=0x0001, seq=4616/2066, ttl=64 (request in 14)
 16 0.20334500 10.10.11.33              10.10.8.100      ICMP       74 Echo (ping) request  id=0x0001, seq=4617/2322, ttl=64 (reply in 30)
 17 0.20410000 fe80::4945:f406:4c3     ff02::1:3        LLMNR      84 Standard query 0xd1d8  A wpad
 18 0.20410100 fe80::78d2:ef67:47b      ff02::16         ICMPv6     90 Multicast Listener Report Message v2
 19 0.20410400 10.10.9.225              224.0.0.252      LLMNR      64 Standard query 0xd1d8  A wpad
 20 0.20410500 10.10.8.186              10.10.15.255     NBNS       92 Name query NB ASUS-PC<20>
 21 0.20410700 HonHaiPr_43:bb:08        Broadcast        ARP        60 Who has 10.10.8.1?  Tell 10.10.10.143
 22 0.20510300 10.10.10.143             224.0.0.22       IGMPv3     60 Membership Report / Leave group 224.0.0.252
 23 0.20510600 fe80::78d2:ef67:47b      ff02::16         ICMPv6     90 Multicast Listener Report Message v2
 24 0.20510700 fe80::78d2:ef67:47b      ff02::1:3        LLMNR      90 Standard query 0xd6c6  ANY Anubhav-HP
 25 0.20558500 10.10.8.186              10.10.15.255     NBNS       92 Name query NB WPAD<00>
 26 0.20672200 10.10.10.143             224.0.0.22       IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
 27 0.20672300 10.10.10.143             224.0.0.252      LLMNR      70 Standard query 0xd6c6  ANY Anubhav-HP
 28 0.20728100 10.10.10.22              239.255.255.250  SSDP      524 NOTIFY * HTTP/1.1

⊞ Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_43:bb:08 (08:ed:b9:43:bb:08), Dst: IPv4mcast_00:00:16 (01:00:5e:00:00:16)
⊟ Internet Protocol Version 4, Src: 10.10.10.143 (10.10.10.143), Dst: 224.0.0.22 (224.0.0.22)
```

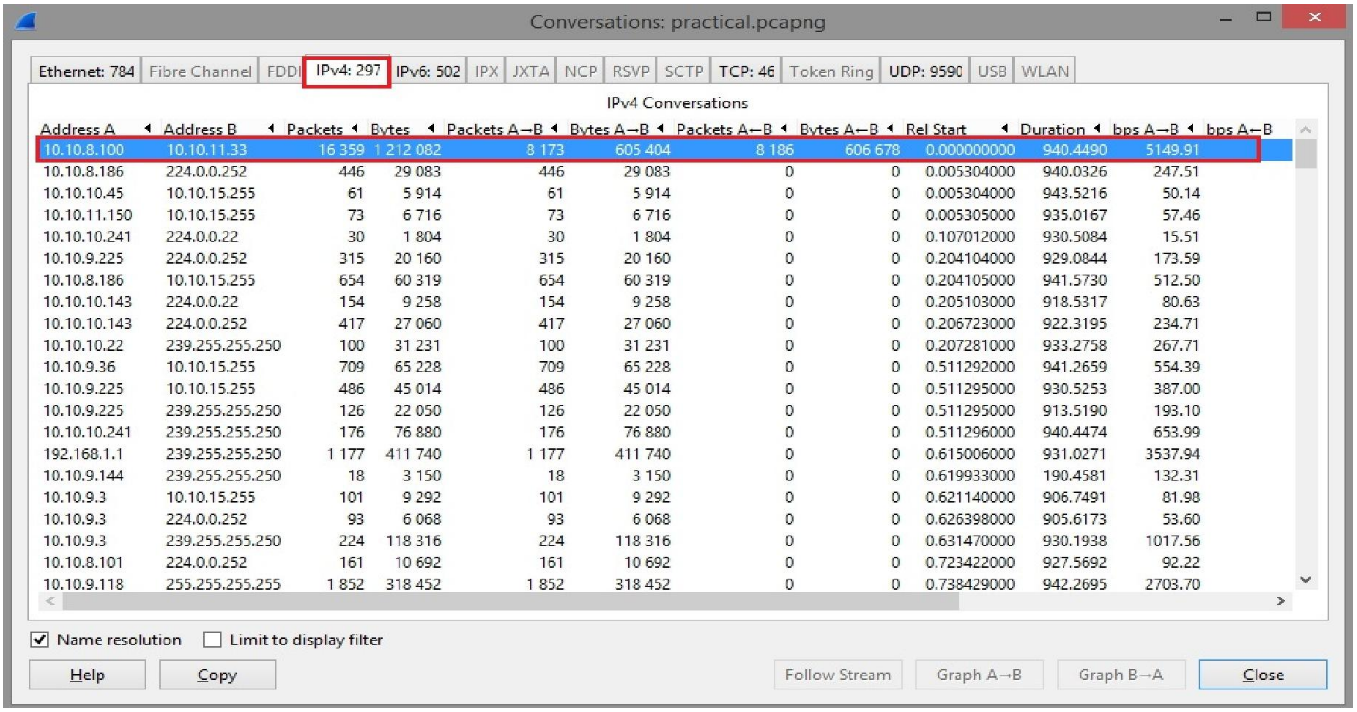
The same thing we can see in the graph analysis which is showing below in screen short.



Echo ping request and reply between attacker and victim

Time	Comment
0.000000000	ICMP: Echo (ping) request id=0x0001, seq=4613/1298, ttl=64 (reply in 6)
0.005303000	LLMNR: Standard query 0xc84c A wpad
0.005304000	LLMNR: Standard query 0xc84c A wpad
0.005304000	NBNS: Name query NB WPAD<00>
0.005305000	NBNS: Name query NB WPAD<00>
0.019797000	ICMP: Echo (ping) reply id=0x0001, seq=4613/1298, ttl=64 (request in 1)
0.065103000	ICMP: Echo (ping) request id=0x0001, seq=4614/1554, ttl=64 (reply in 8)
0.067026000	ICMP: Echo (ping) reply id=0x0001, seq=4614/1554, ttl=64 (request in 7)
0.086133000	ICMP: Echo (ping) request id=0x0001, seq=4615/1810, ttl=64 (reply in 10)
0.088297000	ICMP: Echo (ping) reply id=0x0001, seq=4615/1810, ttl=64 (request in 9)
0.107012000	IGMPv3: Membership Report / Join group 224.0.0.253 for any sources
0.107014000	ARP: Who has 10.10.8.57? Tell 10.10.8.158
0.107015000	DHCPv6: Solicit XID: 0x78cbb1 CID: 0001000119af279e208984ea429f
0.175344000	ICMP: Echo (ping) request id=0x0001, seq=4616/2066, ttl=64 (reply in 15)
0.178079000	ICMP: Echo (ping) reply id=0x0001, seq=4616/2066, ttl=64 (request in 14)
0.203345000	ICMP: Echo (ping) request id=0x0001, seq=4617/2322, ttl=64 (reply in 30)
0.204100000	LLMNR: Standard query 0xd1d8 A wpad
0.204101000	ICMPv6: Multicast Listener Report Message v2
0.204104000	LLMNR: Standard query 0xd1d8 A wpad
0.204105000	NBNS: Name query NB ASUS-PC<20>
0.204107000	ARP: Who has 10.10.8.1? Tell 10.10.10.143
0.205103000	IGMPv3: Membership Report / Leave group 224.0.0.252
0.205106000	ICMPv6: Multicast Listener Report Message v2
0.205107000	LLMNR: Standard query 0xd6c6 ANY Anubhav-HP
0.205585000	NBNS: Name query NB WPAD<00>
0.206722000	IGMPv3: Membership Report / Join group 224.0.0.252 for any sources
0.206723000	LLMNR: Standard query 0xd6c6 ANY Anubhav-HP
0.207281000	SSDP: NOTIFY * HTTP/1.1

Again in conversation part we can see who is communicating with whom and it will also show that how many packets and bytes is transferred between the communication parties.

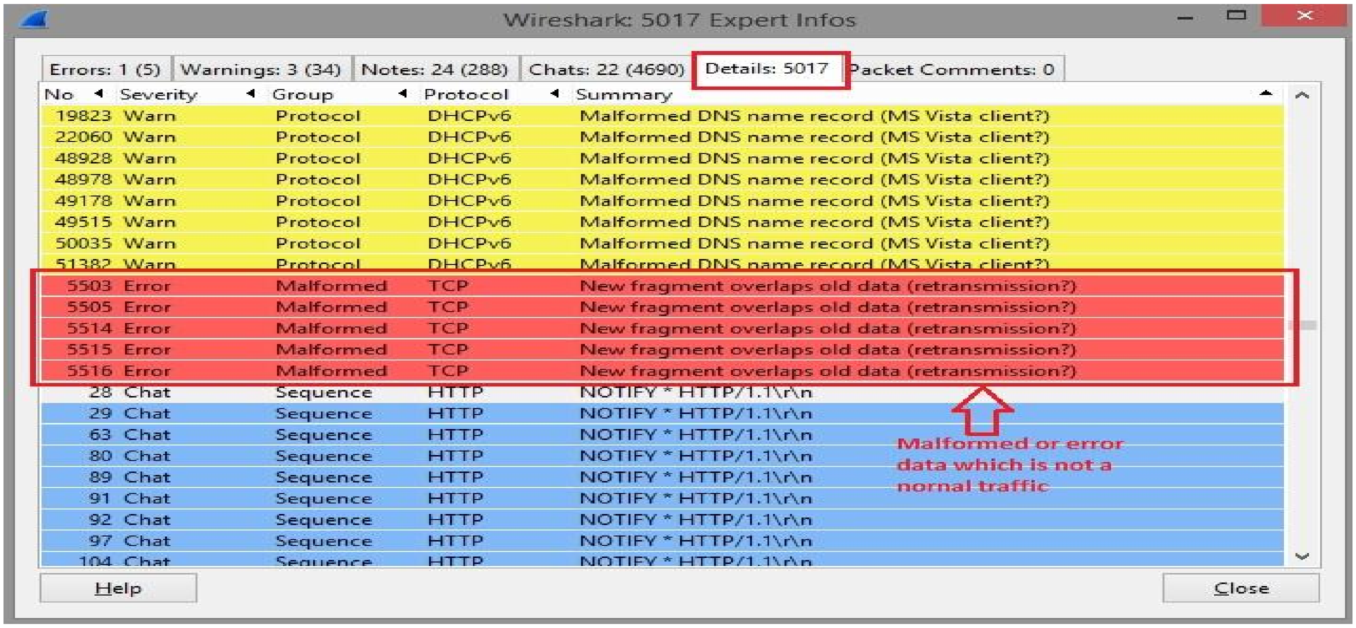


IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
10.10.8.100	10.10.11.33	16 359	1 212 082	8 173	605 404	8 186	606 678	0.000000000	940.4490	5149.91	
10.10.8.186	224.0.0.252	446	29 083	446	29 083	0	0	0.005304000	940.0326	247.51	
10.10.10.45	10.10.15.255	61	5 914	61	5 914	0	0	0.005304000	943.5216	50.14	
10.10.11.150	10.10.15.255	73	6 716	73	6 716	0	0	0.005305000	935.0167	57.46	
10.10.10.241	224.0.0.22	30	1 804	30	1 804	0	0	0.107012000	930.5084	15.51	
10.10.9.225	224.0.0.252	315	20 160	315	20 160	0	0	0.204104000	929.0844	173.59	
10.10.8.186	10.10.15.255	654	60 319	654	60 319	0	0	0.204105000	941.5730	512.50	
10.10.10.143	224.0.0.22	154	9 258	154	9 258	0	0	0.205103000	918.5317	80.63	
10.10.10.143	224.0.0.252	417	27 060	417	27 060	0	0	0.206723000	922.3195	234.71	
10.10.10.22	239.255.255.250	100	31 231	100	31 231	0	0	0.207281000	933.2758	267.71	
10.10.9.36	10.10.15.255	709	65 228	709	65 228	0	0	0.511292000	941.2659	554.39	
10.10.9.225	10.10.15.255	486	45 014	486	45 014	0	0	0.511295000	930.5253	387.00	
10.10.9.225	239.255.255.250	126	22 050	126	22 050	0	0	0.511295000	913.5190	193.10	
10.10.10.241	239.255.255.250	176	76 880	176	76 880	0	0	0.511296000	940.4474	653.99	
192.168.1.1	239.255.255.250	1 177	411 740	1 177	411 740	0	0	0.615006000	931.0271	3537.94	
10.10.9.144	239.255.255.250	18	3 150	18	3 150	0	0	0.619933000	190.4581	132.31	
10.10.9.3	10.10.15.255	101	9 292	101	9 292	0	0	0.621140000	906.7491	81.98	
10.10.9.3	224.0.0.252	93	6 068	93	6 068	0	0	0.626398000	905.6173	53.60	
10.10.9.3	239.255.255.250	224	118 316	224	118 316	0	0	0.631470000	930.1938	1017.56	
10.10.8.101	224.0.0.252	161	10 692	161	10 692	0	0	0.723422000	927.5692	92.22	
10.10.9.118	255.255.255.255	1 852	318 452	1 852	318 452	0	0	0.738429000	942.2695	2703.70	

☑ Name resolution □ Limit to display filter

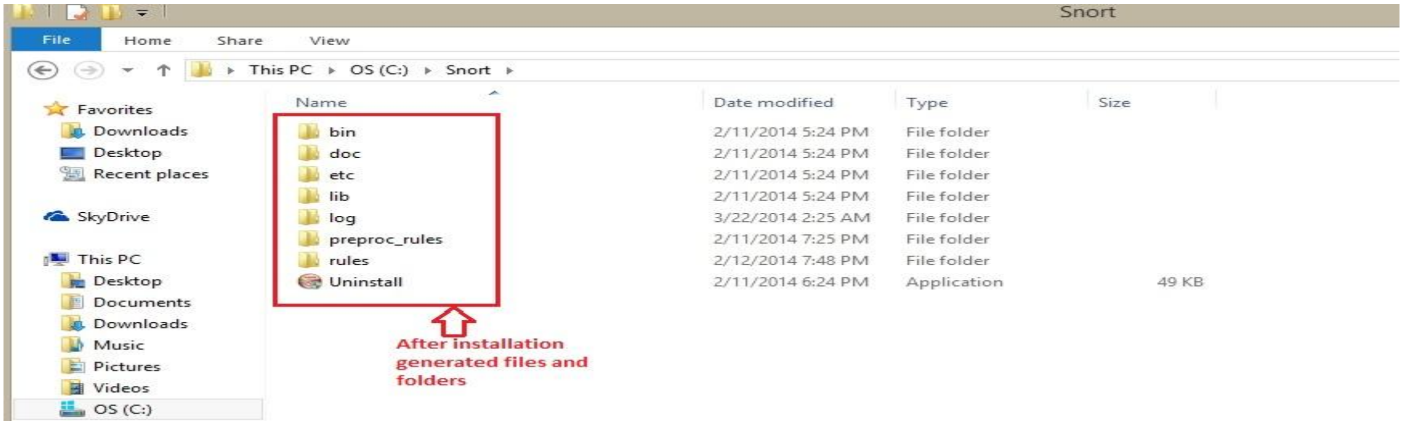
Now in expert info we can see or analyze malformed packets with red color which can be a reason of suspect. When go through the expert info then there is an error details. Talk about coloring rule in which it differentiate the packets on the basis of string in packets with respective color for example bad TCP uses black color as default color in Wireshark.



No	Severity	Group	Protocol	Summary
19823	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
22060	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
48928	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
48978	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
49178	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
49515	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
50035	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
51382	Warn	Protocol	DHCPv6	Malformed DNS name record (MS Vista client?)
5503	Error	Malformed	TCP	New fragment overlaps old data (retransmission?)
5505	Error	Malformed	TCP	New fragment overlaps old data (retransmission?)
5514	Error	Malformed	TCP	New fragment overlaps old data (retransmission?)
5515	Error	Malformed	TCP	New fragment overlaps old data (retransmission?)
5516	Error	Malformed	TCP	New fragment overlaps old data (retransmission?)
28	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
29	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
63	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
80	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
89	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
91	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
92	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
97	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n
104	Chat	Sequence	HTTP	NOTIFY * HTTP/1.1\r\n

Malformed or error data which is not a nornal traffic

Intrusion Detection Practical Approach Through Snort: For configuring the Snort first of all we need to download Snort by going through <http://www.snort.org/> there we will get download Snort and get rules we download it. When we are going to install snort in windows machine then we will have need of Winpcap software to understand the capture packets. When we install and configure all these things then we get the folders showing below.



Name	Date modified	Type	Size
bin	2/11/2014 5:24 PM	File folder	
doc	2/11/2014 5:24 PM	File folder	
etc	2/11/2014 5:24 PM	File folder	
lib	2/11/2014 5:24 PM	File folder	
log	3/22/2014 2:25 AM	File folder	
preproc_rules	2/11/2014 7:25 PM	File folder	
rules	2/12/2014 7:48 PM	File folder	
Uninstall	2/11/2014 6:24 PM	Application	49 KB

After installation generated files and folders

There is no such mandatory guideline for Snort configuration but here giving a way to configure Snort Then for performing configuration we go through the C:\Snort\etc ,where we get the "snort.conf" file we open this file with wordPad where we find the nine sections which is given below: You should take the following steps to create your own custom configuration.

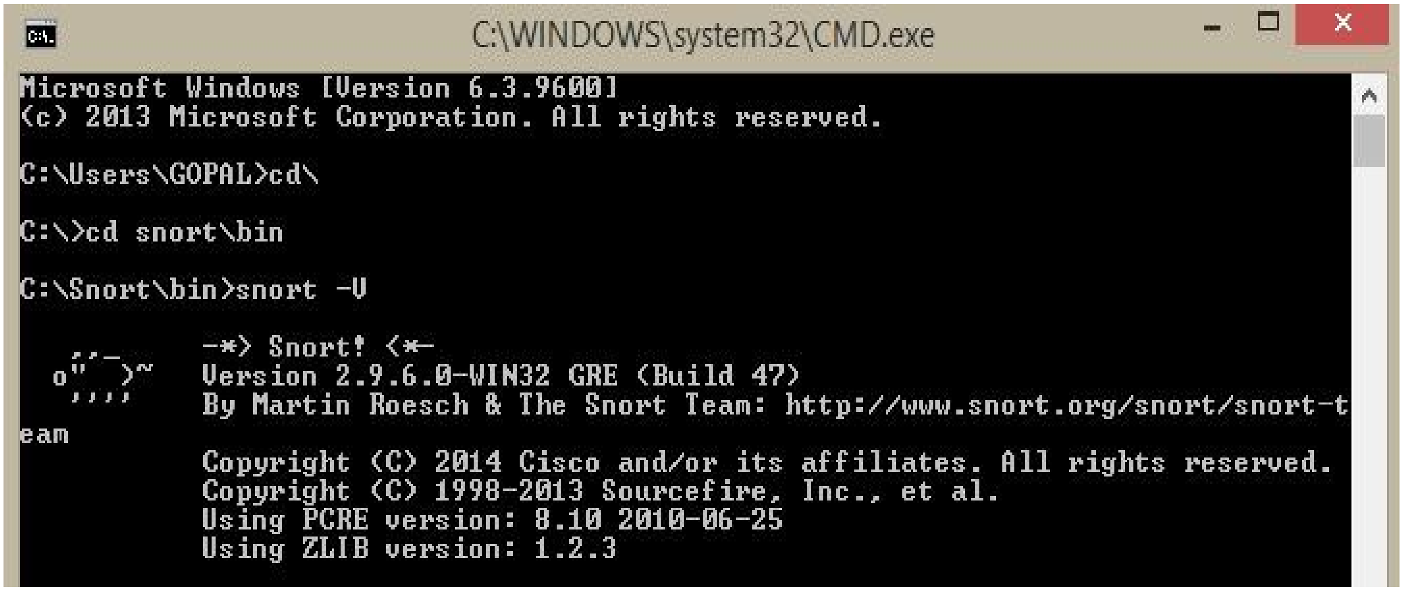
1) Set the network variables.
2) Configure the decoder.
3) Configure the base detection engine.
4) Configure dynamic loaded libraries.
5) Configure preprocessors.
6) Configure output plugins.
7) Customize your rule set.
8) Customize preprocessor and decoder rule set.
9) Customize shared object rule set.

In first section we configure in such a way that we can protect our network Setup the network addresses you are protecting var HOME_NET 10.10.11.33 this is the IP address which we want to protect we can put another IP as per requirement to protect. Set up the external network addresses. Leave as "any" in most situations var EXTERNAL_NET 10.10.12.1/24. List of DNS servers on your network var DNS_SERVERS 10.10.8.1. Here, researcher configuring as per requirement. If there is any SMTP server, HTTP server, SQL server, TELNET server and FTP server then its address we will have to specify. If there is no requirement of other rule set then we will leave as it is. We have to change the rule file "c:\Snort\rules"

In section four we have to make some changes such as: path to dynamic preprocessor libraries

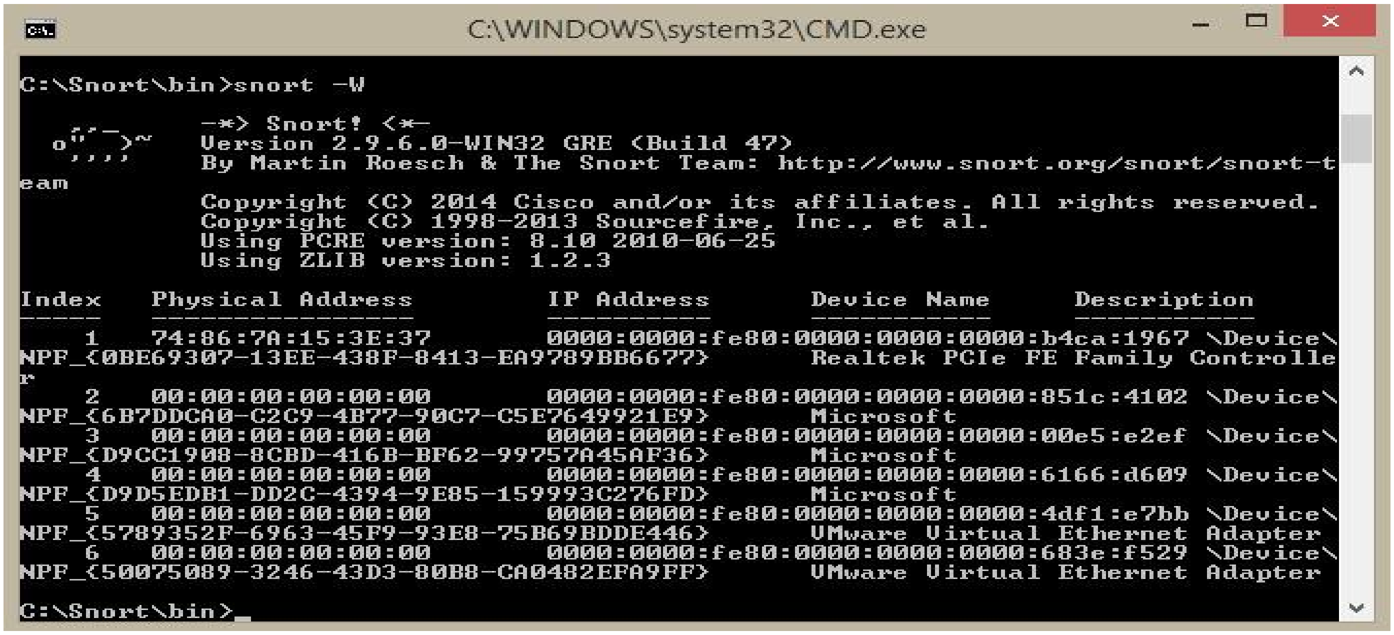
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor, path to base preprocessor engine dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll, path to dynamic rules libraries dynamicdetection directory /usr/local/lib/snort_dynamicrules.

Apart from this we have to create a "alert.ids" with note pad file in log folder. Now we have rule file which we had downloaded earlier that we have to extract in the C:\Snort\rules . In C:\Snort\rules, we can create white.list and black.list file where we can specify the IP addresses according to requirement to which IP we want to allow or to which IP we don't want to allow. In the rule folder there is a file "local" where we create the test rules by opening and specify: alert icmp any any -> any any (msg:"ICMP testing rule"; sid:1000001;), alert udp any any -> any any (msg:"UDP testing rule"; sid:1000002;), alert tcp any any -> any 80 (msg:"TCP testing rule"; sid:1000003;). After configuring all rules we check the snort whether it is working or not. To check, first of all we check the version which is showing below in screen short by using command C:\Snort\bin>snort -V.



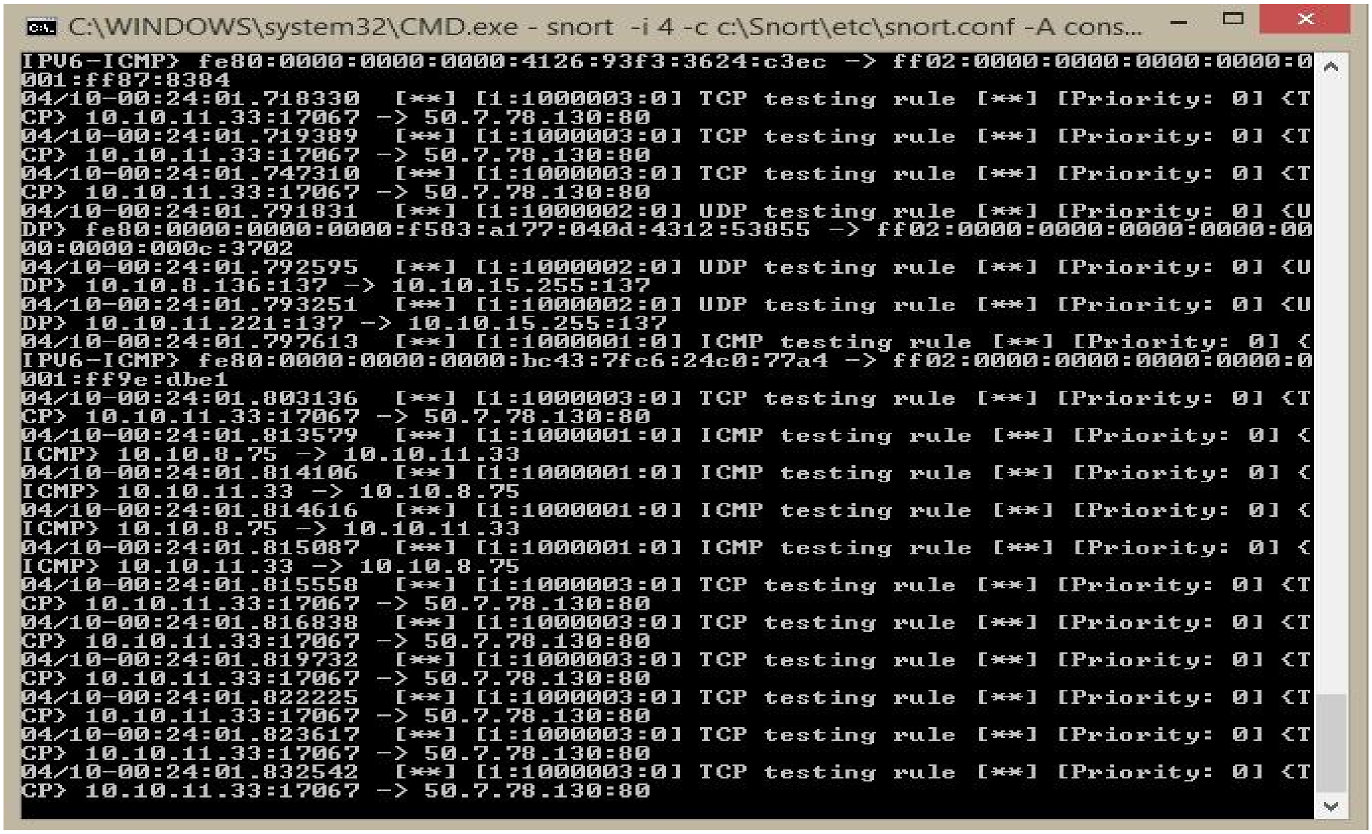
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\GOPAL>cd\

C:\>cd snort\bin

C:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0-WIN32 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3
```

Then we check the interface at which packet capturing will be done which is showing below by using command C:\Snort\bin>snort -W.



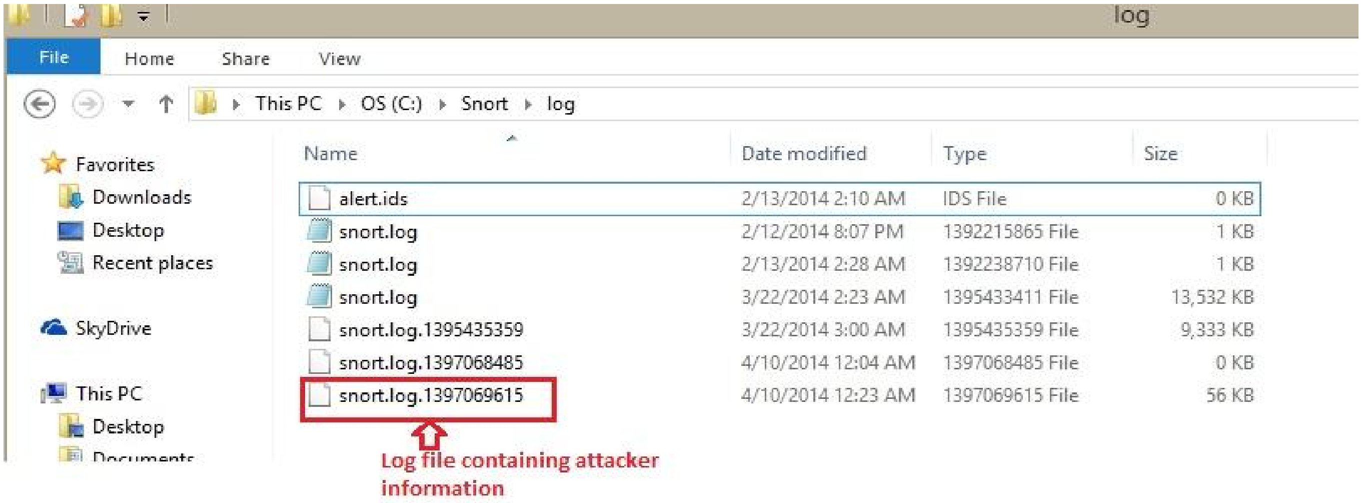
```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0-WIN32 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   74:86:7A:15:3E:37       0000:0000:fe80:0000:0000:0000:b4ca:1967 \Device\
NPF_{0BE69307-13EE-438F-8413-EA9789BB6677}      Realtek PCIe FE Family Controlle
r
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:851c:4102 \Device\
NPF_{6B7DDCA0-C2C9-4B77-90C7-C5E7649921E9}      Microsoft
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:00e5:e2ef \Device\
NPF_{D9CC1908-8CBD-416B-BF62-99757A45AF36}      Microsoft
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:6166:d609 \Device\
NPF_{D9D5EDB1-DD2C-4394-9E85-159993C276FD}      Microsoft
    5   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:4df1:e7bb \Device\
NPF_{5789352F-6963-45F9-93E8-75B69BDDE446}      VMware Virtual Ethernet Adapter
    6   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:683e:f529 \Device\
NPF_{50075089-3246-43D3-80B8-CA0482EFA9FF}      VMware Virtual Ethernet Adapter

C:\Snort\bin>_
```

Here we are using interface 4 for packet capturing. Now we will start the snort by simply typing a command which is "C:\Snort\bin>snort -i 4 -c c:\Snort\etc\snort.conf -A console" . As we execute this command snort starts working and generate the logs in C:\Snort\log. Below showing screen shorts of packet capturing.


C:\WINDOWS\system32\CMD.exe - snort -i 4 -c c:\Snort\etc\snort.conf -A cons...

```
IPV6-ICMP> fe80:0000:0000:0000:4126:93f3:3624:c3ec -> ff02:0000:0000:0000:0000:0
001:ff87:8384
04/10-00:24:01.718330  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.719389  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.747310  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.791831  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] <U
DP> fe80:0000:0000:0000:f583:a177:040d:4312:53855 -> ff02:0000:0000:0000:0000:00
00:0000:000c:3702
04/10-00:24:01.792595  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] <U
DP> 10.10.8.136:137 -> 10.10.15.255:137
04/10-00:24:01.793251  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] <U
DP> 10.10.11.221:137 -> 10.10.15.255:137
04/10-00:24:01.797613  [**] [1:1000001:0] ICMP testing rule [**] [Priority: 0] <
IPV6-ICMP> fe80:0000:0000:0000:bc43:7fc6:24c0:77a4 -> ff02:0000:0000:0000:0000:0
001:ff9e:dbe1
04/10-00:24:01.803136  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.813579  [**] [1:1000001:0] ICMP testing rule [**] [Priority: 0] <
ICMP> 10.10.8.75 -> 10.10.11.33
04/10-00:24:01.814106  [**] [1:1000001:0] ICMP testing rule [**] [Priority: 0] <
ICMP> 10.10.11.33 -> 10.10.8.75
04/10-00:24:01.814616  [**] [1:1000001:0] ICMP testing rule [**] [Priority: 0] <
ICMP> 10.10.8.75 -> 10.10.11.33
04/10-00:24:01.815087  [**] [1:1000001:0] ICMP testing rule [**] [Priority: 0] <
ICMP> 10.10.11.33 -> 10.10.8.75
04/10-00:24:01.815558  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.816838  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.819732  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.822225  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.823617  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
04/10-00:24:01.832542  [**] [1:1000003:0] TCP testing rule [**] [Priority: 0] <T
CP> 10.10.11.33:17067 -> 50.7.78.130:80
```

When we analyzed the log file using the wireshark then we get some results between IP 10.10.11.33 and IP 10.10.8.75 below showing in screen short .



Name	Date modified	Type	Size
alert.ids	2/13/2014 2:10 AM	IDS File	0 KB
snort.log	2/12/2014 8:07 PM	1392215865 File	1 KB
snort.log	2/13/2014 2:28 AM	1392238710 File	1 KB
snort.log	3/22/2014 2:23 AM	1395433411 File	13,532 KB
snort.log.1395435359	3/22/2014 3:00 AM	1395435359 File	9,333 KB
snort.log.1397068485	4/10/2014 12:04 AM	1397068485 File	0 KB
snort.log.1397069615	4/10/2014 12:23 AM	1397069615 File	56 KB

Log file containing attacker information

In above screen short last log file is being analyze through wireshark and get the results.

V. CONCLUSION

It's an era of technology where technology is playing a main role in human life and the dependency on technology is being increase every day. Technology is double edge sword where in one side peoples are enjoying technology as service such as remote communication, home shop, internet banking, e-education, e-ticketing etc and another side some of them is using technology for wrong full gain or unauthorized access. So it is very important to protect technology as well as network communication system or technology.

Wireshark and Snort are the efficient tools for intrusion detection. Network monitoring through wireshark can be very useful for intrusion detection and firewall ACL rule can be used for intrusion prevention, coloring rules and expert info can play important role in intrusion detection. Where Snort tool is also a powerful intrusion detection and prevention system in which by defining security (Snort.conf file) policy we can modulate our security policy according to requirement.

The main role of an IDS and IPS is to protect CIA and other security parameters. It is not possible to make fully secured system but, by deploying an IDS and IPS we can protect our system or network up to certain or maximum limit. By the use of hybrid, IDS and IPS, network and system security can be increase. In the same way integration of IDS and IPS with other network devices such as, routers, firewall, honeypots, SIEM can also increase the efficiency. IDS and IPS is very useful to protect SCADA (Supervisory Control And Data Acquisition) systems. There are some major issues which is false alarm in behavior-based detection and difficult to detect zero day attacks, although by deploying an IDS and IPS at the perimeter of the network this attacks can be mitigate. Social engineering attacks is also the one of the major issue which can also mitigate by providing proper training and awareness.

REFERENCES

[1] D. Stiawan, A. Y. I. Shakhatreh, Md. Y. Idris, K. A. Bakar and A. H. Abdullah, "*Intrusion Prevention System: A Survey*" , Journal of Theoretical and Applied Information Technology, Vol. 40 No. 1, June- 2012, Page No. 44-54.

[2] A. S. Ashoor and S. Gore "*Intrusion Detection System (IDS) & Intrusion Prevention System (IPS): Case Study*", International Journal of Scientific & Engineering Research, Volume 2, Issue 7, July-2011, ISSN 2229-5518.

[3] D. Mathew, "*Choosing an Intrusion Detection System that Best Suits your Organization*" by GSEC Practical v1.4b Option A, SANS Institute 2002.

[4] R. S. Shirbhate and P. A. Patil "*Network Traffic Monitoring Using Intrusion Detection System*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012, ISSN: 2277 128X.

[5] T. Holland, "*Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth*" by GSEC Practical v1.4b, Option 1, SANS Institute February 23, 2004.

[6] A. Youssef and A. Emam, "*Network Intrusion Detection Using Data Mining And Network Behaviour Analysis*" , International Journal of Computer Science & Information Technology (IJCSIT) Vol. 3, No 6, Dec 2011, Page No. 87-98.

[7] T. Lappas, and K. Pelechrinis "*Data Mining Techniques for (Network) Intrusion Detection Systems*", Department of Computer Science and Engineering, UC Riverside, Riverside CA 92521.

[9] J. Gomez, C. Gil, N. Padilla, R. Banos and C. Jimenez , "*Design of a Snort-Based Hybrid Intrusion Detection System*". Omatu et al. (Eds.): IWANN (The International Work Conference on Artificial Neural Networks) 2009, Part II, LNCS 5518, 2009, pp. 515–522.

[10] S. Gupta and R. Mamtora, "*Intrusion Detection System Using Wireshark*", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 11, November 2012, Page No. 358-363

[11] Sujindar S and Malini.K, " *Monitoring Tools for Network Services and System*", International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682, Vol.18, No.18, October 2013, Page No. 114-121.

[12] R. Gulati, "*The Threat of Social Engineering and Your Defense Against It*" Version 1.4b – Option 1, SANS Institue 2003.

[13] J. Janczewski and Lingyan (Rene) Fu, "*Social Engineering Based Attacks: Model and New Zealand Perspective*" Proceeding of the International Multiconference on Computer Science and Information Technology, ISBN 978-83-608-10-27-9, ISSN 1896-7094, Page no. 847-853.

[14] Abhinav Singh, "Instant Wireshark Starter" Packt Publishing Ltd., So, what is Wireshark? Page no 3, eBook

[15] What is Snort?, Andrew R. Baker, Brian Caswell and Mike Poor "Snort 2.1, Intrusion Detection", Syngress Publishing, Inc, eBook page no. 55-56