ATTACKERS INTENTION RECOGNITION BASED ON REAL—TIME NETWORK DATA

T. DHARSHINI, G. MANISHA, A.R. ANITHA
Bachelors of Engineering, Bachelors of Engineering, Bachelors of Engineering
Computer Science and Engineering,
Thiagarajar College of Engineering, Madurai, India.

ABSTRACT: A system could be misused in various ways. Data in the system could be accessed in different forms. Proper measures are to be taken to secure our system data from illegitimate users. The main objective is to detect an attack and take necessary steps to stop the hacker from hacking the data. Prediction is made in the early stage so that a quick action can be taken. There are legitimate users and hackers who try to access data, only the hacker is found and he is stopped. Any kind of unusual activity is detected in the system and immediately the user is notified. The java code in the system is used to detect unusual activities and with the help of packet capturing tool, captured data is manipulated. All these activities happen automatically in the system when a system boots, so the user need not be aware of the procedures of how the system is periodically checked

***Index Terms* – Intention prediction, threshold, hackers, intimate, unusual activities.**

1. INTRODUCTION:

The paper is about identifying the intention of the hackers and prevents them from doing such activities. We have different types of attacks like spoofing, data modification, man-in-the-middle, etc., which helps the hackers to steal the data. As the technology develops day by day, the techniques of stealing the data also develops. Every person who steals the data must have a reason for doing such activities. So we thought it is very important to find the intention of the hackers, so that when someone else who try to do the same thing, it would be easy for us to identify it earlier and stop such activities. Only when we know the intention of the hacker, we can divert them by providing certain data that are similar but not the exact one which they are searching for.

So, to find the intention of the hacker, we capture all the packets that request for the service of the server in a constant time interval using packet capturing tool. The captured packets are stored as file and we process this. From the file we collect all the sources, destinations and the protocol types along with the unique count of each. And then we find the sources which have requested the same destination for the same type of request. With this data we find the intention of the hackers. When we keep track of the path in which the hacker attacks the data and the types of files that they access, gives us the intention of them.

Packet capturing tool will be started at every boot process and it keeps capturing the packets continuously in a constant time interval. When there is any suspicious activity like a single source repeatedly requests the same destination for a same type of files, then we will try to divert the particular person by providing a similar data that they request and check if the person is a hacker or a genuine user. If the person is a genuine user we will allow the user to continue with the work that they do. If we predict the person as a hacker, then we will keep providing them only the similar data, but not the exact one that they are requesting for.

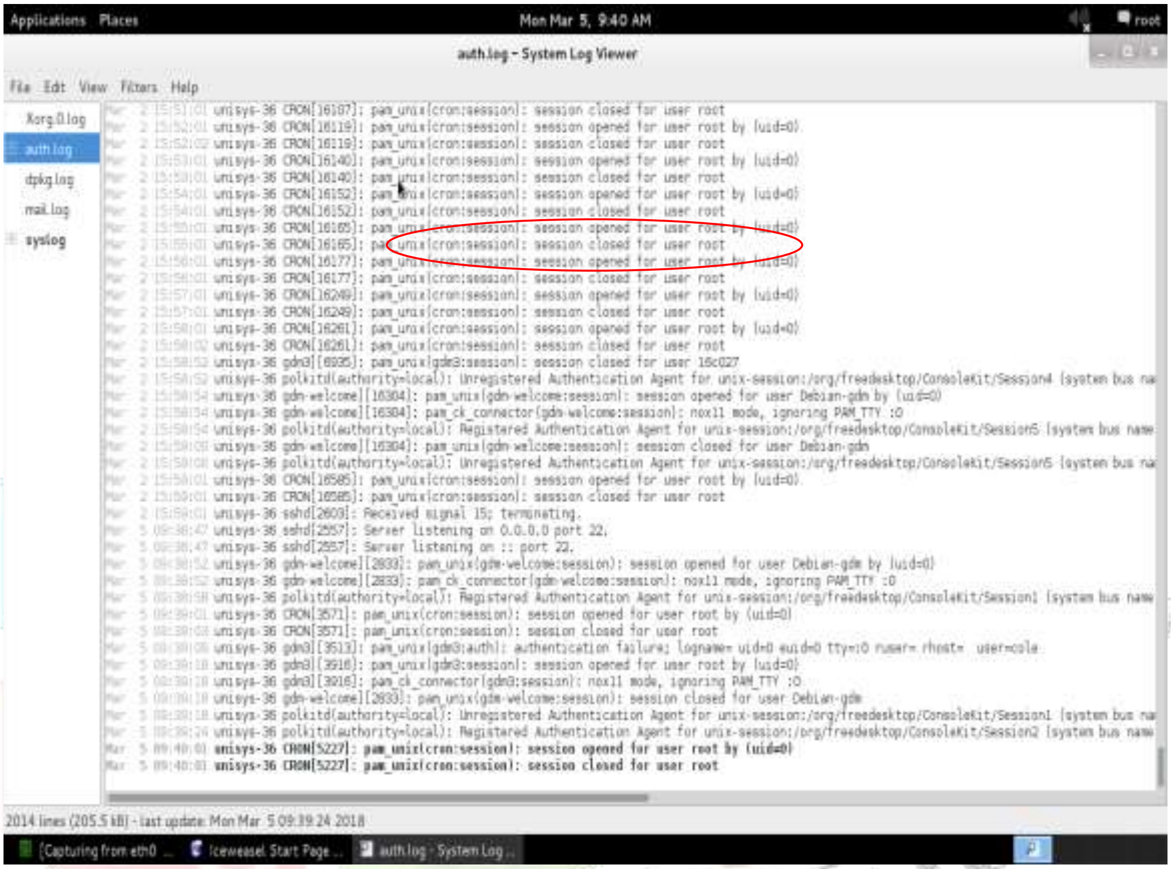
2. DIFFERENT TYPE OF ATTACKS:-

2.1. Remote Accessing:-

Remote access is a method that is being used to access a personal system from another system. By using this method we can see all the data that is allowed for access. All these activities will be stored in the system logs that keep track of all the activities that happen in a particular system. There are different types of logs located in a system.

2.1.1. Auth logs:-

In this log all the authentication activities will be stored. Whenever the system asks for authentication the access permission will be allowed only if the correct password is being provided. This log stores how many times the user has provided a password, whether the password was right or wrong, at what time the person has tried to log in. If we try to access a system from other system, then this log will be stored in the auth logs along with the system details like source address, system name, etc.



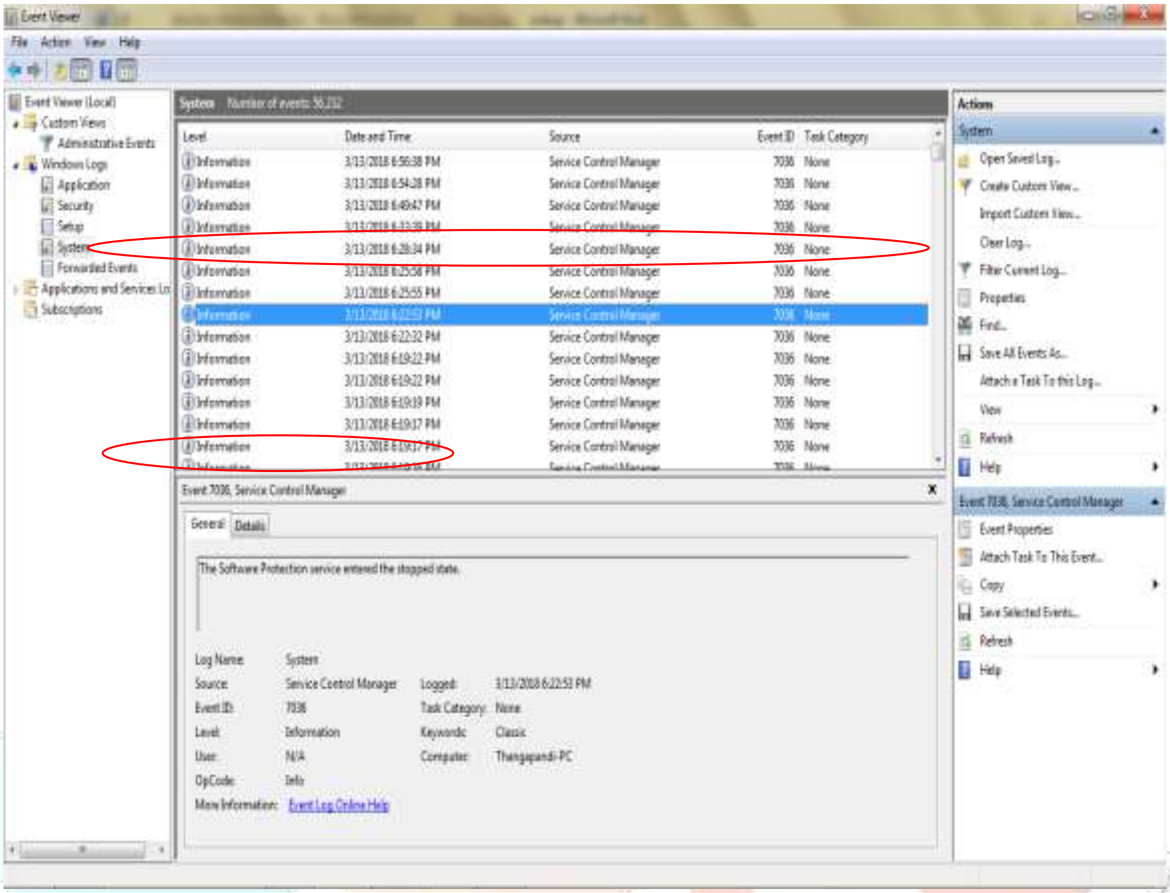
```
Mar  2 15:51:01 unisys-36 CRON[16107]: pam_unix(cron:session): session closed for user root
Mar  2 15:52:01 unisys-36 CRON[16119]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:52:02 unisys-36 CRON[16119]: pam_unix(cron:session): session closed for user root
Mar  2 15:53:01 unisys-36 CRON[16140]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:53:01 unisys-36 CRON[16140]: pam_unix(cron:session): session closed for user root
Mar  2 15:54:01 unisys-36 CRON[16152]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:54:01 unisys-36 CRON[16152]: pam_unix(cron:session): session closed for user root
Mar  2 15:55:01 unisys-36 CRON[16165]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:55:01 unisys-36 CRON[16165]: pam_unix(cron:session): session closed for user root
Mar  2 15:56:01 unisys-36 CRON[16177]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:56:01 unisys-36 CRON[16177]: pam_unix(cron:session): session closed for user root
Mar  2 15:57:01 unisys-36 CRON[16249]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:57:01 unisys-36 CRON[16249]: pam_unix(cron:session): session closed for user root
Mar  2 15:58:01 unisys-36 CRON[16261]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:58:02 unisys-36 CRON[16261]: pam_unix(cron:session): session closed for user root
Mar  2 15:58:52 unisys-36 gdm3][6935]: pam_unix(gdm3:session): session closed for user 16c027
Mar  2 15:58:52 unisys-36 polkitd(authority=local): Unregistered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session4 (system bus na
Mar  2 15:58:54 unisys-36 gdm-welcome][16304]: pam_unix(gdm-welcome:session): session opened for user Debian-gdm by (uid=0)
Mar  2 15:58:54 unisys-36 gdm-welcome][16304]: pam_ck_connector(gdm-welcome:session): nox11 mode, ignoring PAM_TTY :0
Mar  2 15:58:54 unisys-36 polkitd(authority=local): Registered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session5 (system bus name
Mar  2 15:59:00 unisys-36 gdm-welcome][16304]: pam_unix(gdm-welcome:session): session closed for user Debian-gdm
Mar  2 15:59:00 unisys-36 polkitd(authority=local): Unregistered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session5 (system bus na
Mar  2 15:59:01 unisys-36 CRON[16585]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  2 15:59:01 unisys-36 CRON[16585]: pam_unix(cron:session): session closed for user root
Mar  2 15:59:01 unisys-36 sshd[2603]: Received signal 15; terminating.
Mar  5 09:38:47 unisys-36 sshd[2557]: Server listening on 0.0.0.0 port 22.
Mar  5 09:38:47 unisys-36 sshd[2557]: Server listening on :: port 22.
Mar  5 09:38:52 unisys-36 gdm-welcome][2833]: pam_unix(gdm-welcome:session): session opened for user Debian-gdm by (uid=0)
Mar  5 09:38:52 unisys-36 gdm-welcome][2833]: pam_ck_connector(gdm-welcome:session): nox11 mode, ignoring PAM_TTY :0
Mar  5 09:38:58 unisys-36 polkitd(authority=local): Registered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session1 (system bus name
Mar  5 09:39:01 unisys-36 CRON[3571]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  5 09:39:03 unisys-36 CRON[3571]: pam_unix(cron:session): session closed for user root
Mar  5 09:39:06 unisys-36 gdm3][3513]: pam_unix(gdm3:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=  user=cole
Mar  5 09:39:18 unisys-36 gdm3][3916]: pam_unix(gdm3:session): session opened for user root by (uid=0)
Mar  5 09:39:18 unisys-36 gdm3][3916]: pam_ck_connector(gdm3:session): nox11 mode, ignoring PAM_TTY :0
Mar  5 09:39:18 unisys-36 gdm-welcome][2833]: pam_unix(gdm-welcome:session): session closed for user Debian-gdm
Mar  5 09:39:18 unisys-36 polkitd(authority=local): Unregistered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session1 (system bus na
Mar  5 09:39:24 unisys-36 polkitd(authority=local): Registered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session2 (system bus name
Mar  5 09:40:01 unisys-36 CRON[5227]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  5 09:40:01 unisys-36 CRON[5227]: pam_unix(cron:session): session closed for user root
```

2014 lines (205.5 kB) - last update: Mon Mar 5 09:39:24 2018

figure 1. auth logs

2.1.2. Sys Logs:-

The actions that are performed in the system will be stored in the system log. If an application is opened or if any action is performed in the system, it will be stored in the system logs. If anyone access our system and do some suspicious activities, it will be stored in the sys logs. By analyzing this logs we can know the source address of the hacker.



System Number of events: 56,232

Level	Date and Time	Source	Event ID	Task Category
Information	3/13/2018 6:56:38 PM	Service Control Manager	7036	None
Information	3/13/2018 6:54:28 PM	Service Control Manager	7036	None
Information	3/13/2018 6:49:47 PM	Service Control Manager	7036	None
Information	3/13/2018 6:33:38 PM	Service Control Manager	7036	None
Information	3/13/2018 6:28:34 PM	Service Control Manager	7036	None
Information	3/13/2018 6:25:58 PM	Service Control Manager	7036	None
Information	3/13/2018 6:25:55 PM	Service Control Manager	7036	None
Information	3/13/2018 6:22:53 PM	Service Control Manager	7036	None
Information	3/13/2018 6:22:32 PM	Service Control Manager	7036	None
Information	3/13/2018 6:19:22 PM	Service Control Manager	7036	None
Information	3/13/2018 6:19:22 PM	Service Control Manager	7036	None
Information	3/13/2018 6:19:19 PM	Service Control Manager	7036	None
Information	3/13/2018 6:19:17 PM	Service Control Manager	7036	None
Information	3/13/2018 6:19:17 PM	Service Control Manager	7036	None

Event 7036, Service Control Manager

General Details

The Software Protection service entered the stopped state.

Log Name: System
Source: Service Control Manager Logged: 3/13/2018 6:22:53 PM
Event ID: 7036 Task Category: None
Level: Information Keywords: Classic
User: N/A Computer: Thangapandi-PC
OpCode: Info
More Information: Event Log Online Help

figure 2. system logs

2.2. Flooding:-

Flooding is one of the important attacking techniques that are followed by the hackers. This technique can be implemented in two different ways which is being followed by most of the attackers.

2.2.1. DOS Attack:

In DOS attack, the hacker attacks the server by giving a continuous request to that server. That is, the hacker connects to a specific network as an external user and sends continuous request to that server. By doing this, the hacker can make the server stop its service to the other users. As the servers follow "First come, first served" technique, the server will keep on serving the requests of the hacker as he will be continuous requesting for the service of the server.

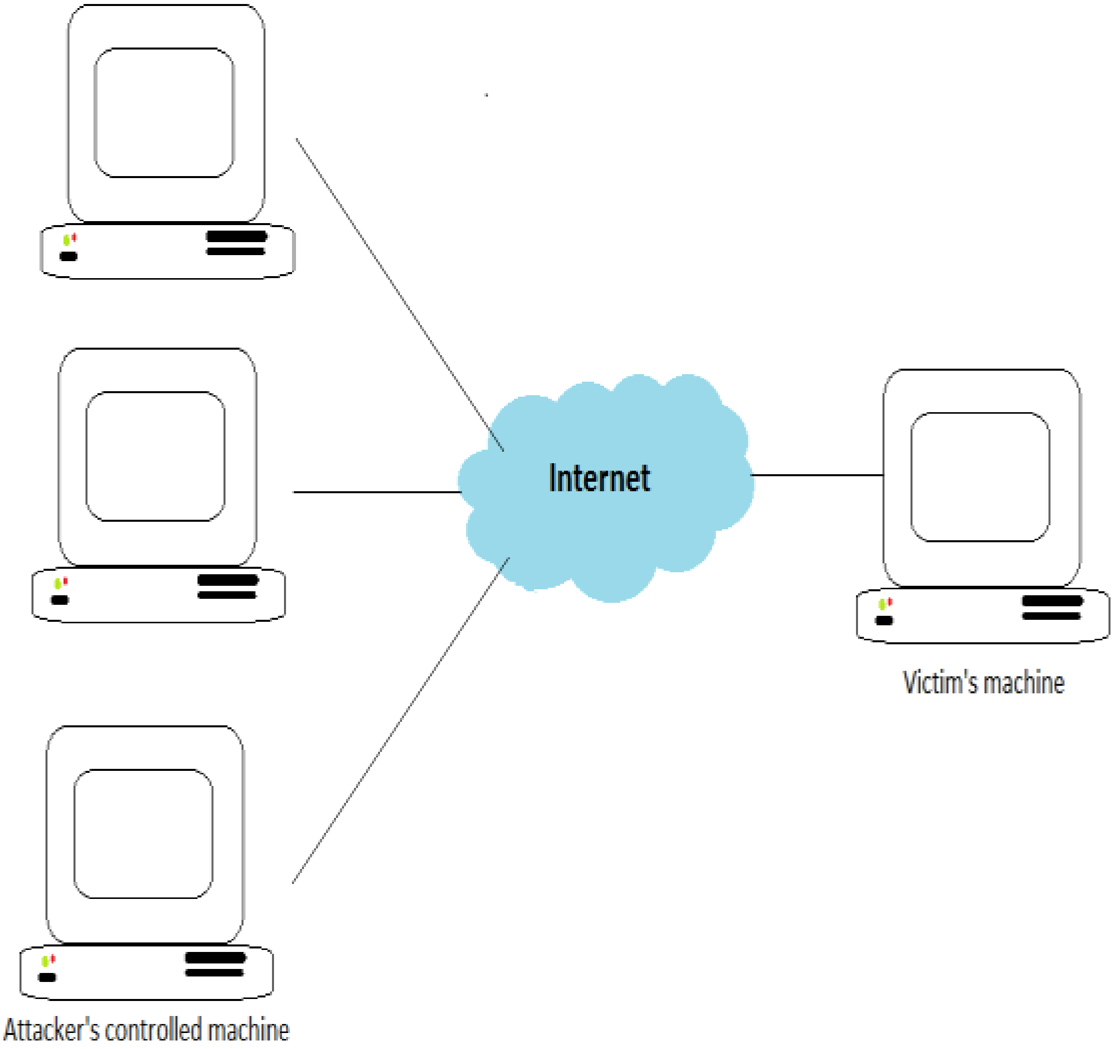


figure 3. dos attack

2.2.2. DDOS Attack:

In DDOS attack, the hacker attacks the server in the same way as DOS attack. But, the main difference is that, in DOS attack the hacker request the service of the server from the same system. But in DDOS attack the hacker uses multiple systems to attack the server. That is, the hacker uses multiple systems to send request to the server. As the hacker keeps on requesting for service from different systems, other users cannot get the service of the server. This happens because, the hacker will send request continuously without leaving any gap in such a way that other users request does not interrupts their attack.

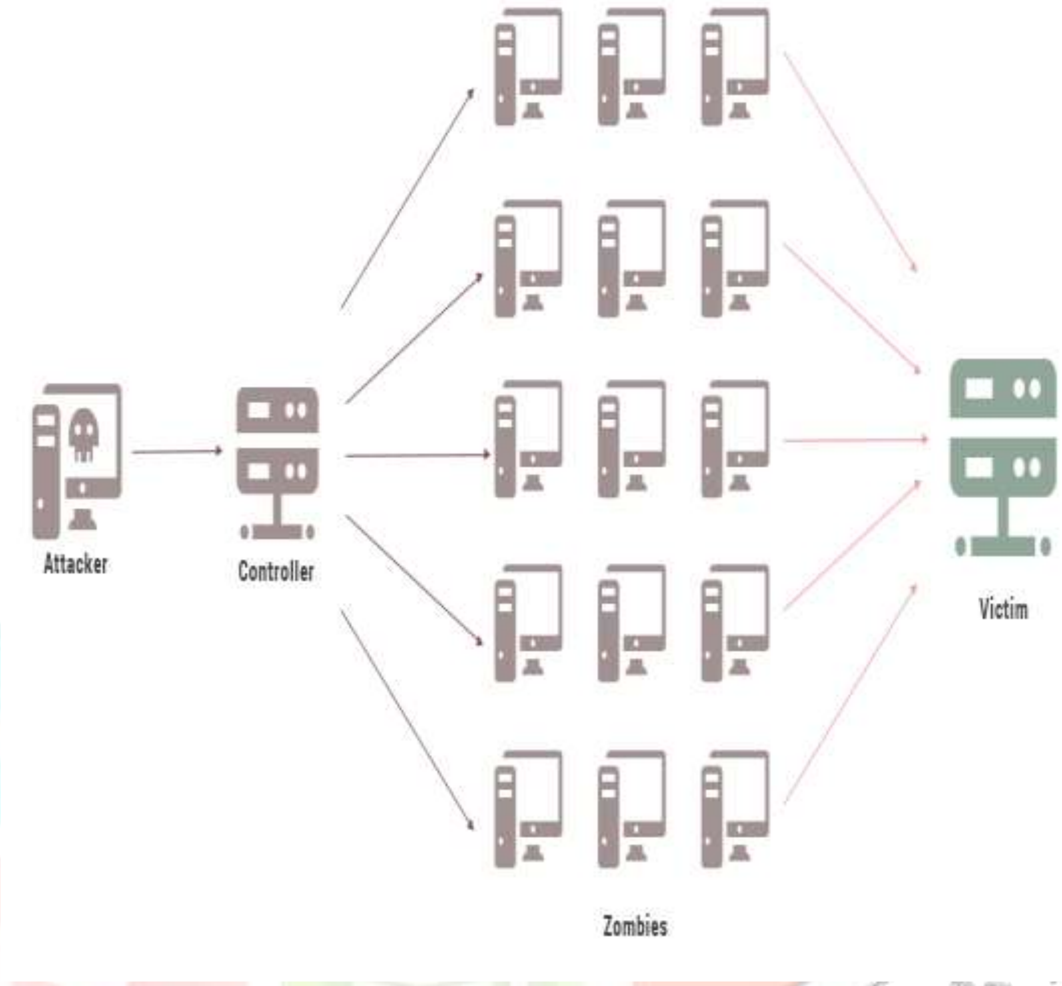


figure 4. ddos attack

3. INTENTION RECOGNITION AND ATTACKER PREVENTION MODEL:

Intention recognition is the most important work in attack prevention. This will help us to protect the data from other hackers who try to attack the similar kind of data. Only when the intention of one hacker is known, it can be stopped or prevented from other hackers who try to do the same kind of activity. Only when it is known that some unwanted work is being held in the system, one can predict and prevent the hacker from accessing the data. So it is important to analyze the activities that are being held in the system.

Since this takes a lot of time when it is performed manually, it is better if it is performed automatically. It is also important that, one should identify the attack as early as possible. Since, it could be of no use, if we do that after the hacker does all the works. So, here is an idea proposed to find the intention of the hacker and also prevent them in an early stage.

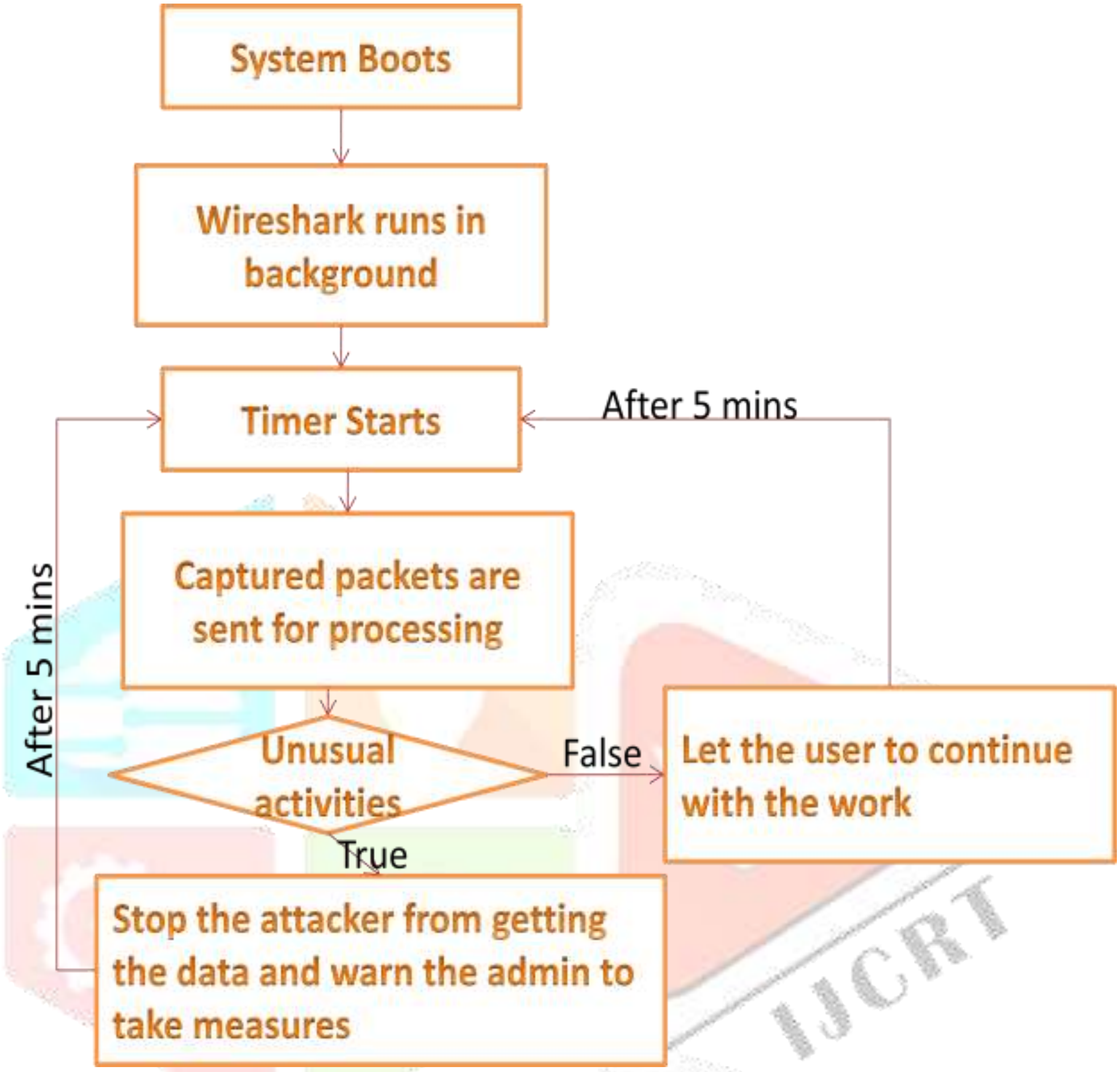
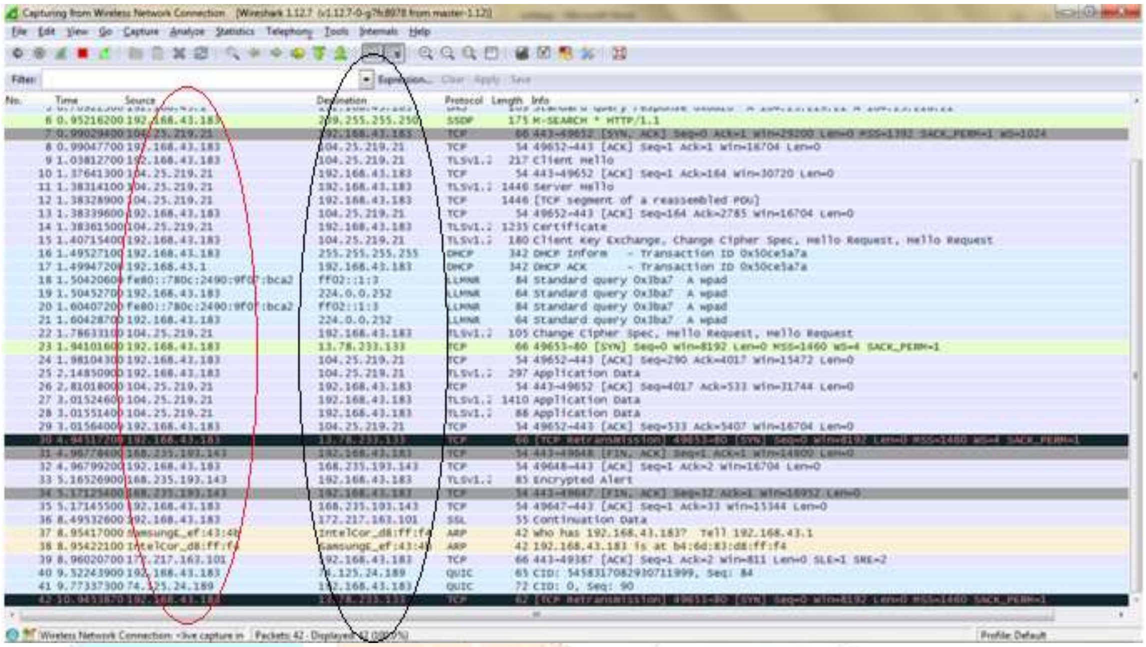

System Boots
Wireshark runs in background
Timer Starts
After 5 mins
Captured packets are sent for processing
After 5 mins
Unusual activities
False
Let the user to continue with the work
True
Stop the attacker from getting the data and warn the admin to take measures

Figure 5. the proposed idea of intention recognition and attack prevention

This idea could help the server or the user whose system contains some confidential data, to find the attacker and also prevent them from attacking the data. Start the packet capturing application automatically by making the application as a start up application. This will help to capture all the requesting packets which can be stored for analyzing.

The saved data can be analyzed for checking the requesting source address and the destination address. If the same source request for the same data to the same destination continuously, it can be predicted us an attack. Make the packet capturing application store the capturing data once for every 5 minutes. And then fix a threshold level for the number of request that can be made by a source. If the user's number of request crosses the threshold limit, then declare it as an attack.

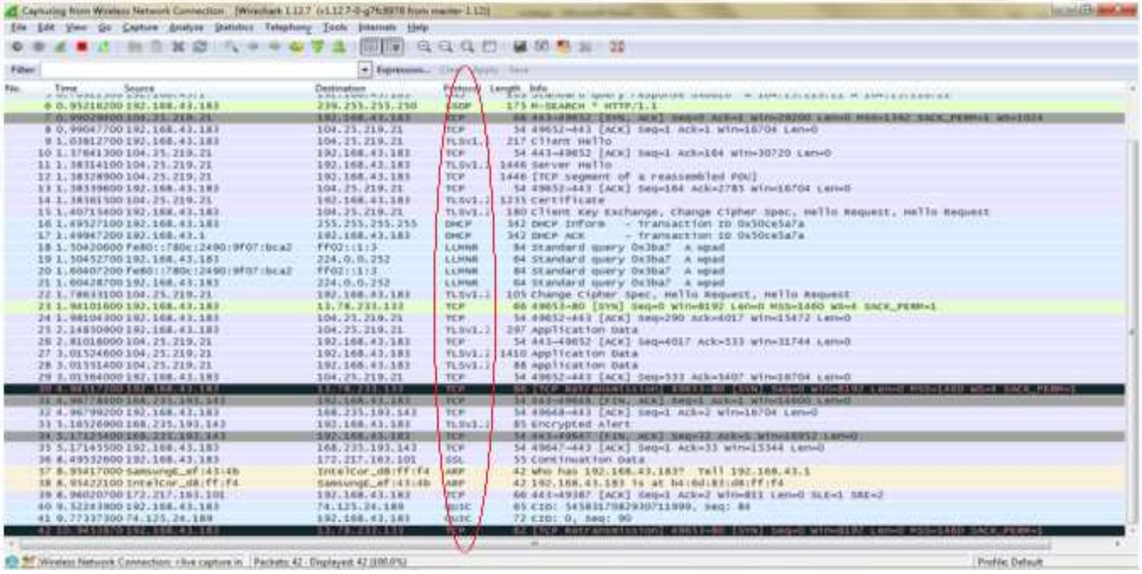

Capturing from Wireless Network Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source                      Destination        Protocol Length Info
 6 0.95216200 192.168.43.183              239.255.255.250    SSDP     175 M-SEARCH * HTTP/1.1
 7 0.99029400 104.25.219.21               192.168.43.183     TCP       66 443-49652 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1392 SACK_PERM=1 WS=1024
 8 0.99047700 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=1 Ack=1 Win=16704 Len=0
 9 1.03812700 192.168.43.183              104.25.219.21      TLSv1.2  217 Client Hello
10 1.37641300 104.25.219.21               192.168.43.183     TCP       54 443-49652 [ACK] Seq=1 Ack=164 Win=30720 Len=0
11 1.38314100 104.25.219.21               192.168.43.183     TLSv1.2 1446 Server Hello
12 1.38328900 104.25.219.21               192.168.43.183     TCP     1446 [TCP segment of a reassembled PDU]
13 1.38339600 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=164 Ack=2785 Win=16704 Len=0
14 1.38361500 104.25.219.21               192.168.43.183     TLSv1.2 1235 Certificate
15 1.40715400 192.168.43.183              104.25.219.21      TLSv1.2  180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
16 1.49527100 192.168.43.183              255.255.255.255    DHCP     342 DHCP Inform   - Transaction ID 0x50ce5a7a
17 1.49947200 192.168.43.1                192.168.43.183     DHCP     342 DHCP ACK      - Transaction ID 0x50ce5a7a
18 1.50420600 fe80::780c:2490:9f07:bca2   ff02::1:3          LLMNR     84 Standard query 0x1ba7  A wpad
19 1.50452700 192.168.43.183              224.0.0.252        LLMNR     64 Standard query 0x1ba7  A wpad
20 1.60407200 fe80::780c:2490:9f07:bca2   ff02::1:3          LLMNR     84 Standard query 0x1ba7  A wpad
21 1.60428700 192.168.43.183              224.0.0.252        LLMNR     64 Standard query 0x1ba7  A wpad
22 1.78633100 104.25.219.21               192.168.43.183     TLSv1.2  105 Change Cipher Spec, Hello Request, Hello Request
23 1.94101600 192.168.43.183              13.78.233.133      TCP       66 49653-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
24 1.98104300 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=290 Ack=4017 Win=15472 Len=0
25 2.14850900 192.168.43.183              104.25.219.21      TLSv1.2  297 Application Data
26 2.81018000 104.25.219.21               192.168.43.183     TCP       54 443-49652 [ACK] Seq=4017 Ack=533 Win=31744 Len=0
27 3.01524600 104.25.219.21               192.168.43.183     TLSv1.2 1410 Application Data
28 3.01551400 104.25.219.21               192.168.43.183     TLSv1.2   88 Application Data
29 3.01564000 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=533 Ack=5407 Win=16704 Len=0
30 4.94517200 192.168.43.183              13.78.233.133      TCP       66 [TCP Retransmission] 49653-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
31 4.96778400 168.235.193.143             192.168.43.183     TCP       54 443-49648 [FIN, ACK] Seq=1 Ack=1 Win=14800 Len=0
32 4.96799200 192.168.43.183              168.235.193.143    TCP       54 49648-443 [ACK] Seq=1 Ack=2 Win=16704 Len=0
33 5.16526900 168.235.193.143             192.168.43.183     TLSv1.2   85 Encrypted Alert
34 5.17125400 168.235.193.143             192.168.43.183     TCP       54 443-49647 [FIN, ACK] Seq=32 Ack=1 Win=16952 Len=0
35 5.17145500 192.168.43.183              168.235.193.143    TCP       54 49647-443 [ACK] Seq=1 Ack=33 Win=15344 Len=0
36 8.49532600 192.168.43.183              172.217.163.101    SSL       55 Continuation Data
37 8.95417000 SamsungE_ef:43:4b           IntelCor_d8:ff:f4  ARP       42 Who has 192.168.43.183?  Tell 192.168.43.1
38 8.95422100 IntelCor_d8:ff:f4           SamsungE_ef:43:4b  ARP       42 192.168.43.183 is at b4:6d:83:d8:ff:f4
39 8.96020700 172.217.163.101             192.168.43.183     TCP       66 443-49387 [ACK] Seq=1 Ack=2 Win=811 Len=0 SLE=1 SRE=2
40 9.52243900 192.168.43.183              74.125.24.189      QUIC      65 CID: 5458317082930711999, Seq: 84
41 9.77337300 74.125.24.189               192.168.43.183     QUIC      72 CID: 0, Seq: 90
42 10.9453870 192.168.43.183              13.78.233.133      TCP       62 [TCP Retransmission] 49653-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
```

Wireless Network Connection: <live capture in
Packets: 42 · Displayed: 42 (100.0%)
Profile: Default

figure 6. this picture shows the different source (red) requesting different destinations (black).

By analyzing the type of data that they try to access, the intention of the hacker can be predicted. With the type of protocol that they have requested, one can predict the type of file that they have tried to access. By analyzing the logs that are stored in the system, the data that was accessed by the hacker can be found.

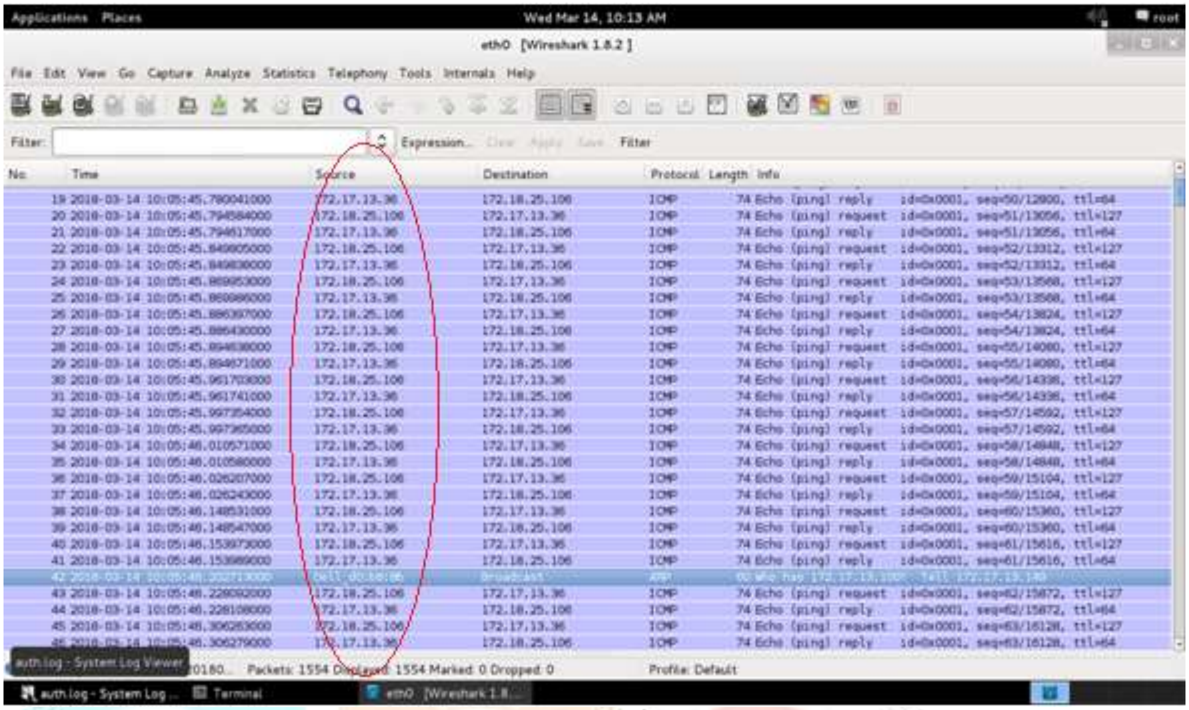

Capturing from Wireless Network Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source                      Destination        Protocol Length Info
 6 0.95216200 192.168.43.183              239.255.255.250    SSDP     175 M-SEARCH * HTTP/1.1
 7 0.99029400 104.25.219.21               192.168.43.183     TCP       66 443-49652 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1392 SACK_PERM=1 WS=1024
 8 0.99047700 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=1 Ack=1 Win=16704 Len=0
 9 1.03812700 192.168.43.183              104.25.219.21      TLSv1.2  217 Client Hello
10 1.37641300 104.25.219.21               192.168.43.183     TCP       54 443-49652 [ACK] Seq=1 Ack=164 Win=30720 Len=0
11 1.38314100 104.25.219.21               192.168.43.183     TLSv1.2 1446 Server Hello
12 1.38328900 104.25.219.21               192.168.43.183     TCP     1446 [TCP segment of a reassembled PDU]
13 1.38339600 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=164 Ack=2785 Win=16704 Len=0
14 1.38361500 104.25.219.21               192.168.43.183     TLSv1.2 1235 Certificate
15 1.40715400 192.168.43.183              104.25.219.21      TLSv1.2  180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
16 1.49527100 192.168.43.183              255.255.255.255    DHCP     342 DHCP Inform   - Transaction ID 0x50ce5a7a
17 1.49947200 192.168.43.1                192.168.43.183     DHCP     342 DHCP ACK      - Transaction ID 0x50ce5a7a
18 1.50420600 fe80::780c:2490:9f07:bca2   ff02::1:3          LLMNR     84 Standard query 0x1ba7  A wpad
19 1.50452700 192.168.43.183              224.0.0.252        LLMNR     64 Standard query 0x1ba7  A wpad
20 1.60407200 fe80::780c:2490:9f07:bca2   ff02::1:3          LLMNR     84 Standard query 0x1ba7  A wpad
21 1.60428700 192.168.43.183              224.0.0.252        LLMNR     64 Standard query 0x1ba7  A wpad
22 1.78633100 104.25.219.21               192.168.43.183     TLSv1.2  105 Change Cipher Spec, Hello Request, Hello Request
23 1.94101600 192.168.43.183              13.78.233.133      TCP       66 49653-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
24 1.98104300 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=290 Ack=4017 Win=15472 Len=0
25 2.14850900 192.168.43.183              104.25.219.21      TLSv1.2  297 Application Data
26 2.81018000 104.25.219.21               192.168.43.183     TCP       54 443-49652 [ACK] Seq=4017 Ack=533 Win=31744 Len=0
27 3.01524600 104.25.219.21               192.168.43.183     TLSv1.2 1410 Application Data
28 3.01551400 104.25.219.21               192.168.43.183     TLSv1.2   88 Application Data
29 3.01564000 192.168.43.183              104.25.219.21      TCP       54 49652-443 [ACK] Seq=533 Ack=5407 Win=16704 Len=0
30 4.94517200 192.168.43.183              13.78.233.133      TCP       66 [TCP Retransmission] 49653-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
31 4.96778400 168.235.193.143             192.168.43.183     TCP       54 443-49648 [FIN, ACK] Seq=1 Ack=1 Win=14800 Len=0
32 4.96799200 192.168.43.183              168.235.193.143    TCP       54 49648-443 [ACK] Seq=1 Ack=2 Win=16704 Len=0
33 5.16526900 168.235.193.143             192.168.43.183     TLSv1.2   85 Encrypted Alert
34 5.17125400 168.235.193.143             192.168.43.183     TCP       54 443-49647 [FIN, ACK] Seq=32 Ack=1 Win=16952 Len=0
35 5.17145500 192.168.43.183              168.235.193.143    TCP       54 49647-443 [ACK] Seq=1 Ack=33 Win=15344 Len=0
36 8.49532600 192.168.43.183              172.217.163.101    SSL       55 Continuation Data
37 8.95417000 SamsungE_ef:43:4b           IntelCor_d8:ff:f4  ARP       42 Who has 192.168.43.183?  Tell 192.168.43.1
38 8.95422100 IntelCor_d8:ff:f4           SamsungE_ef:43:4b  ARP       42 192.168.43.183 is at b4:6d:83:d8:ff:f4
39 8.96020700 172.217.163.101             192.168.43.183     TCP       66 443-49387 [ACK] Seq=1 Ack=2 Win=811 Len=0 SLE=1 SRE=2
40 9.52243900 192.168.43.183              74.125.24.189      QUIC      65 CID: 5458317082930711999, Seq: 84
41 9.77337300 74.125.24.189               192.168.43.183     QUIC      72 CID: 0, Seq: 90
42 10.9453870 192.168.43.183              13.78.233.133      TCP       62 [TCP Retransmission] 49653-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
```

Wireless Network Connection: <live capture in
Packets: 42 · Displayed: 42 (100.0%)
Profile: Default

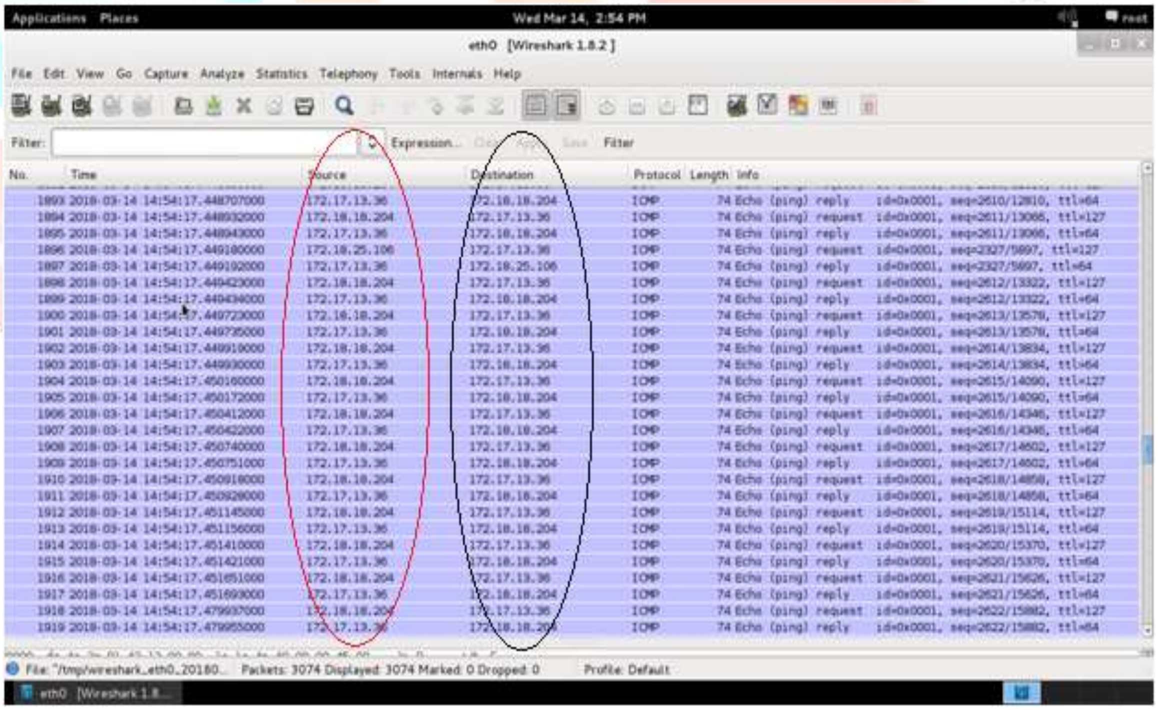
figure 7. different types of protocols

When an attack happens, the packet capturing application captures it and gives us certain information. The captured packets will be saved and sent for processing. During processing the packets will check the count of the request sent by the hacker. This will help the admin to differentiate a user and a hacker.


Applications Places
Wed Mar 14, 10:13 AM
root
eth0 [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save Filter
auth.log - System Log Viewer
auth.log - System Log ...
Terminal
eth0 [Wireshark 1.8...

```
No.  Time                           Source          Destination     Protocol Length Info
19 2018-03-14 10:05:45.780041000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=50/12800, ttl=64
20 2018-03-14 10:05:45.794584000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=51/13056, ttl=127
21 2018-03-14 10:05:45.794617000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=51/13056, ttl=64
22 2018-03-14 10:05:45.849805000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=52/13312, ttl=127
23 2018-03-14 10:05:45.849838000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=52/13312, ttl=64
24 2018-03-14 10:05:45.869953000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=53/13568, ttl=127
25 2018-03-14 10:05:45.869986000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=53/13568, ttl=64
26 2018-03-14 10:05:45.886397000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=54/13824, ttl=127
27 2018-03-14 10:05:45.886430000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=54/13824, ttl=64
28 2018-03-14 10:05:45.894638000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=55/14080, ttl=127
29 2018-03-14 10:05:45.894671000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=55/14080, ttl=64
30 2018-03-14 10:05:45.961703000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=56/14336, ttl=127
31 2018-03-14 10:05:45.961741000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=56/14336, ttl=64
32 2018-03-14 10:05:45.997354000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=57/14592, ttl=127
33 2018-03-14 10:05:45.997365000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=57/14592, ttl=64
34 2018-03-14 10:05:46.010571000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=58/14848, ttl=127
35 2018-03-14 10:05:46.010580000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=58/14848, ttl=64
36 2018-03-14 10:05:46.026207000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=59/15104, ttl=127
37 2018-03-14 10:05:46.026243000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=59/15104, ttl=64
38 2018-03-14 10:05:46.148531000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=60/15360, ttl=127
39 2018-03-14 10:05:46.148547000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=60/15360, ttl=64
40 2018-03-14 10:05:46.153973000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=61/15616, ttl=127
41 2018-03-14 10:05:46.153989000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=61/15616, ttl=64
42 2018-03-14 10:05:46.202713000   Dell_00:b8:06   Broadcast       ARP      60 Who has 172.17.13.100?  Tell 172.17.13.140
43 2018-03-14 10:05:46.228092000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=62/15872, ttl=127
44 2018-03-14 10:05:46.228108000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=62/15872, ttl=64
45 2018-03-14 10:05:46.306263000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=63/16128, ttl=127
46 2018-03-14 10:05:46.306279000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=63/16128, ttl=64
0180...  Packets: 1554 Displayed: 1554 Marked: 0 Dropped: 0     Profile: Default
```

Figure 8. example of an attack performed from a single system


Applications Places
Wed Mar 14, 2:54 PM
root
eth0 [Wireshark 1.8.2]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save Filter
eth0 [Wireshark 1.8...

```
No.   Time                             Source          Destination     Protocol Length Info
1893 2018-03-14 14:54:17.448707000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2610/12810, ttl=64
1894 2018-03-14 14:54:17.448932000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2611/13066, ttl=127
1895 2018-03-14 14:54:17.448943000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2611/13066, ttl=64
1896 2018-03-14 14:54:17.449180000   172.18.25.106   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2327/5897, ttl=127
1897 2018-03-14 14:54:17.449192000   172.17.13.36    172.18.25.106   ICMP     74 Echo (ping) reply    id=0x0001, seq=2327/5897, ttl=64
1898 2018-03-14 14:54:17.449423000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2612/13322, ttl=127
1899 2018-03-14 14:54:17.449434000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2612/13322, ttl=64
1900 2018-03-14 14:54:17.449723000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2613/13578, ttl=127
1901 2018-03-14 14:54:17.449735000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2613/13578, ttl=64
1902 2018-03-14 14:54:17.449919000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2614/13834, ttl=127
1903 2018-03-14 14:54:17.449930000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2614/13834, ttl=64
1904 2018-03-14 14:54:17.450160000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2615/14090, ttl=127
1905 2018-03-14 14:54:17.450172000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2615/14090, ttl=64
1906 2018-03-14 14:54:17.450412000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2616/14346, ttl=127
1907 2018-03-14 14:54:17.450422000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2616/14346, ttl=64
1908 2018-03-14 14:54:17.450740000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2617/14602, ttl=127
1909 2018-03-14 14:54:17.450751000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2617/14602, ttl=64
1910 2018-03-14 14:54:17.450918000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2618/14858, ttl=127
1911 2018-03-14 14:54:17.450928000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2618/14858, ttl=64
1912 2018-03-14 14:54:17.451145000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2619/15114, ttl=127
1913 2018-03-14 14:54:17.451156000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2619/15114, ttl=64
1914 2018-03-14 14:54:17.451410000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2620/15370, ttl=127
1915 2018-03-14 14:54:17.451421000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2620/15370, ttl=64
1916 2018-03-14 14:54:17.451651000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2621/15626, ttl=127
1917 2018-03-14 14:54:17.451693000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2621/15626, ttl=64
1918 2018-03-14 14:54:17.479937000   172.18.18.204   172.17.13.36    ICMP     74 Echo (ping) request  id=0x0001, seq=2622/15882, ttl=127
1919 2018-03-14 14:54:17.479955000   172.17.13.36    172.18.18.204   ICMP     74 Echo (ping) reply    id=0x0001, seq=2622/15882, ttl=64
File: "/tmp/wireshark_eth0_20180...  Packets: 3074 Displayed: 3074 Marked: 0 Dropped: 0     Profile: Default
```

Figure 9. example of an attack performed from multiple systems

4. CONCLUSION:

The system will be monitored continuously and any kind of unusual activity is detected in the early stage itself. Necessary steps will be taken to protect the data in the system. All these activities are automated in the system and the user need not be aware of it. DOS attack, Dictionary attacks can be identified with this work. By analyzing the different types of protocols which was requested by the attacker, the intention of the attacker can be found. Once the intention is identified it would be easy to stop the attacker from hacking the data. Since the attack is being detected in the early stage, the hackers cannot get a large amount of data that they need which can help them take any unauthorized data.

5. REFERENCES:

1. Qiu Hui, Wang Kun 2016. “Real-time Network Attack Intention Recognition Algorithm”. http://www.sersc.org/journals/IJSIA/vol10_no4_2016/6.pdf
2. Carlos Garcia Cordero, Emmanouil Vasilomanolakisa, Nikolay Milanov, Christian Koch, David Hausheer, Max Muhlh .2015. “ID2T: a DIY Dataset Creation Toolkit for Intrusion Detection Systems”. http://ieeexplore.ieee.org/document/7346912/
3. Kou Guang,Tang Guangming,Ding Xia,Wang Kun.2016. “A Network Security Situation Assessment Method Based On Attack Intention Perception”. http://ieeexplore.ieee.org/document/7924882/
4. Yanjie Zhao.2016. “Network Intrusion Detection System Model Based On Data Mining”. http://ieeexplore.ieee.org/abstract/document/7515894/
5. Prashant, Ramesh Krishnan.2016. “A Novel for Network Intrusion Detection with Anomaly Detection”. https://www.ijecs.in/index.php/ijecs/article/view/412
6. Harvindar Pal Singh Sasan.2016. “Intrusion Detection Using Feature Selection and Machine Learning Algorithm With Misuse Detection”. http://aircconline.com/ijcsit/V8N1/8116ijcsit02.pdf
7. Ed Wilson Tavares Ferreira, Ailton Akira Shinoda, Ruy De Oliveira, Valtrmir Emerencio Nascimento, Nelcileno Virgilio De Souza Araujo.2015. “A Methodology for building a Dataset to Assess Intrusion Detection Systems in Wireless Networks”. http://www.wseas.org/multimedia/journals/communications/2015/a305704-607.pdf
8. Sahil Sanjay Tanpure, Jayraj Jagtap, Gunjan Patel, Zishan Raja, Apashabipathan.2016. “Intrusion Detection System in Data Mining using Hybrid approach”. http://www.rroij.com/open-access/intrusion-detection-technique-using-datamining-approach-survey.php?aid=47104
9. Monowar H. Bhuyan, Dhruba K. Bhattacharyya, Jugal K. Kalita.2015. “Towards Generating Real-life Datasets for Network Intrusion Detection”. https://pdfs.semanticscholar.org/4fb2/b57f1aa0a83d5978b6980748f22d160f18f0.pdf
10. Xinzhou Qin, Wenke Lee. 2004. “Attack Plan Recognition and Prediction Using Causal Networks”. http://wenke.gtisc.gatech.edu/papers/acsac_Qin_04.pdf
11. Wathiq Laftah Al-Yaseen, Zulaiha Ali Othman, Mohd Zakree Ahmad Nazri. 2016. “Real-Time Intrusion Detection System Using Multi-agent System”. https://pdfs.semanticscholar.org/90eb/b093952b1c62235380376c344edd08a4a4a1.pdf
12. Jeong Kyu Lee, Seo Yeon Moon, Jong Hyuk Park. 2016. “HB-DIPM: Human Behavior Analysis-Based Malware Detection and Intrusion Prevention Model in the Future Internet”. https://www.researchgate.net/publication/309530548_HB-DIPM_Human_Behavior_Analysis-Based_Malware_Detection_and_Intrusion_Prevention_Model_in_the_Future_Internet
13. Purushottam R, Yogesh Sharma, Manali Kshirasagar. 2016. “Performance Analysis of Intrusion Detection Systems Implemented using Hybrid Machine Learning Techniques”. https://www.researchgate.net/publication/290787776_Performance_Analysis_of_Intrusion_Detection_Systems_Implemented_using_Hybrid_Machine_Learning_Techniques
14. O. Al-Jarrah and A. Arafat, 2014 “Network Intrusion Detection System using attack behavior classification”. http://ieeexplore.ieee.org/document/6841978/
15. Z. Wanlei, Keynote, 2012. “Detection of and Defense Against Distributed Denial-of-Service (DDoS) Attacks”. http://ieeexplore.ieee.org/document/6295948/
16. Zhi Peng, Chao Feng, Cao jing.2016. “Malware Classification based on Behavior Analysis and Back Propogation neural network”. https://www.itm-conferences.org/articles/itmconf/pdf/2016/02/itmconf_ita2016_02001.pdf
17. Johannes Landstorfer, Ivo Herrmann, Jan Erik Stange, Marian Dork, Relo Wettach. 2014. “A Network Security Visualization built With Co-Creation”. http://mariandoerk.de/papers/vast2014.pdf
18. Neha G. Relan and Dharmaraj R. Patil. 2015. “Implementation of network intrusion detection system using variant of decision tree algorithm”. http://ieeexplore.ieee.org/document/7029925/
19. Xinming Ou, Sudhakar Govindavajhala, Andrew W. Appel. 2005. “MulVAL: A logic-based network security analyzer”. https://www.usenix.org/legacy/event/sec05/tech/full_papers/ou/ou.pdf
20. Lv Huiying, P. Wu, W. Ruimei, W. Jie. 2014. “A Real-time Network Threat Recognition and Assessment Method Based on Association Analysis of Time and Space”. http://crad.ict.ac.cn/EN/Y2014/V51/I5/1039#
21. M. Schiffman, 2011. “Common Vulnerability Scoring System (CVSS)”. https://www.first.org/cvss/
22. F. Cuppens, F. Autrel, A. Miege, S. Benferhat. 2002. “Recognizing malicious intention in an intrusion detection process”. https://pdfs.semanticscholar.org/dcff/311940942dcf81db5073e551a87e1710e52a.pdf
23. Peng Ning, Dingbang Xu, 2003, “Learning attack strategies from intrusion alerts”. http://discovery.csc.ncsu.edu/pubs/ccs03-ids-full.pdf

24. H. Debar and A.Wespi.2001. “Aggregation and Correlation of Intrusion-Detection Alerts”. http://wenke.gtisc.gatech.edu/ids-readings/Herve_Debar_IDS_Correlation_Raid01.pdf
25. X. Chai, Q. Yang, 2005. “Multiple-goal recognition form low-level signals” https://pdfs.semanticscholar.org/f98f/db037b21c27829c8eb295ef3d8f439764224.pdf