University of Windsor

Project Report - 03

Knowledge Engineering and Cybersecurity

COMP 8920-01 Summer 2019

Project Supervisor: Dr. Sherif Saad

Authors: Mayank Semwal, Vipul Malhotra

1. Knowledge Engineering

- To create a knowledge base, we have selected 10 columns from the dataset which we considered as important nodes.

categoryname	ipcategory_name	alert_ids	ip	weekday	ipcategory_scope	grandparent_category	client_code	notified	overallseverity
Attack	INTERNET	Nhq	YT.LB.32.21	Tue	Internet	A	DPM	0	3
Exploit	PRIV-192	XZt	192.SL.UK.94	Thu	Private network	A	FIN	0	5
Attack	INTERNET	bBz	YT.LB.38.21	Tue	Internet	A	CHP	0	4
Attack	INTERNET	ZNr	JX.NY.13.20	Tue	Internet	A	HPS	0	4
Attack	INTERNET	poV	YT.LB.32.21	Sat	Internet	A	OSC	0	4
Exploit	PRIV-10	ZSX	10.FM.RK.37	Sat	Private network	A	QWB	0	4
Exploit	INTERNET	TVd	IJ.PI.86.150	Thu	Internet	A	IUO	0	4
Attack	INTERNET	xAY	YT.LB.32.21	Fri	Internet	A	GNI	0	5
Attack	INTERNET	suH	EU.FS.44.4	Mon	Internet	A	TDM	0	4
Attack	INTERNET	JhL	YT.LB.38.21	Mon	Internet	A	GBU	0	5

Figure 1: Columns selected from dataset

- Why above-mentioned columns are selected?
  i. Category Name: This defines the category name of an attack that corresponds to its severity such as “Attack” and “Exploit”.
  ii. IP Category Name: This defines the category name of an IP corresponding to IP address such as “Internet” and “Broadcast”.
  iii. Alert ids: This defines the identifier of an alert and generates unique alert id.
  iv. IP: This defines the relation between unique IP addresses with each alert.
  v. Weekday: This defines the day of a week when alert was generated on.
  vi. IP Category Scope: This defines the domain of the category of an IP address such as “Internet”, “Private Network” or “Subnet”.
  vii. Grandparent Category: This defines grandparent category name of the IP category name.
  viii. Client Code: This defines the identifier of the client for which alert was generated.
  ix. Notified: This defines if a client is notified about the alert or not, contains binary value 0, 1.
  x. Overall Severity: This defines the estimation of alert severity.

So, from the definition it can be inferred these columns are intertwined with each other.

A. For each attribute identify the attribute-domain using only the available information in the dataset.

Attribute	Attribute Domain
Category Name	- [Attack, Exploit, Suspicious Reputation, Control and Maintain] - [Reconnaissance, Malicious Activity, Suspicious Network] - [Activity, Attack Preparation, Compromise] - [Suspicious Account Activity, To Be Determined] *Note: Most of the alerts are generated for these categories:* ***Attack, Exploit, Reconnaissance, Control and Maintain***
IP Category Name	- [INTERNET, PRIV-192, PRIV-10, PRIV-172, PRIV-CGN]

	- [LOOPBACK, LINK-LOCAL, BROADCAST, MULTICAST] *Note: Most of the alerts are generated for first list of category names above.*
Alert ids	- Unique Alert ID's
IP	- Unique IP addresses
Weekday	- [Tue, Thu, Sat, Fri, Mon, Wed, Sun] *Note: Most of the alerts are generated in weekdays (Sat and Sun combined is 50% less than any other day of a week).*
IP Category Scope	- ['Internet', 'Private network', 'Host', 'Subnet'] *Note: Only 11 alerts generated for **Host** and **Subnet** which is **0.027% of total**.*
Grandparent_Category	- ['A', 'B'] *Note: Only 7 alerts generated for **B** which is **0. 017% of total**.*
Client Code	- Unique client code
Notified	- [0, 1] *Note: Alerts which are notified to client are **5.77% of total.***
Overall Severity	- [1, 2, 3, 4, 5] *Note: Most of the alert are of **3, 4 and 5** severity and **(1, 2)** is **2.78% of total**.*

Table 1: Attribute and attribute-domains

B. Identify the top K essential attributes in your opinion and create a taxonomy to represent the attribute-domain in a hierarchical structure.

1). <u>On the basis of IP Category Scope and Grandparent</u>:

- Rectangles are attributes, blue circles are attribute- domains

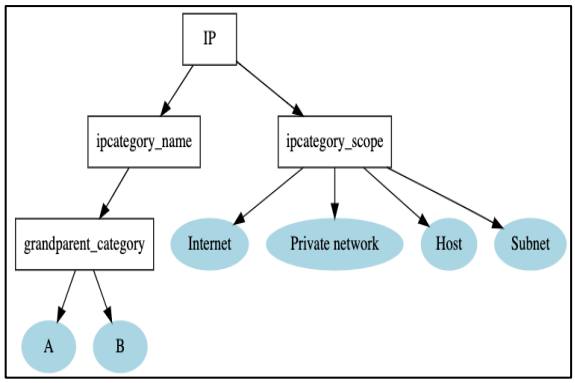


Fig 2: Before best domains

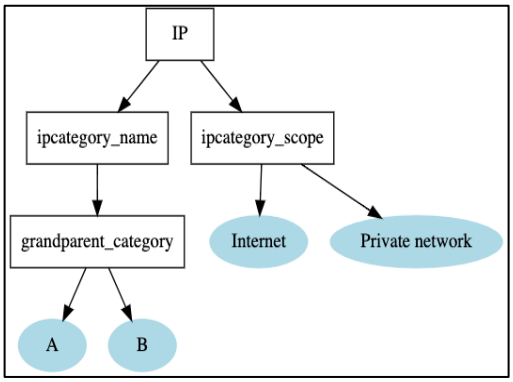


Fig 3: After best domains

As explained in table 1 why few attribute-domains are removed with that explanation we have reached to top k attribute-domains as well.

2). <u>On the basis of Alert, Category Name and Notified</u>

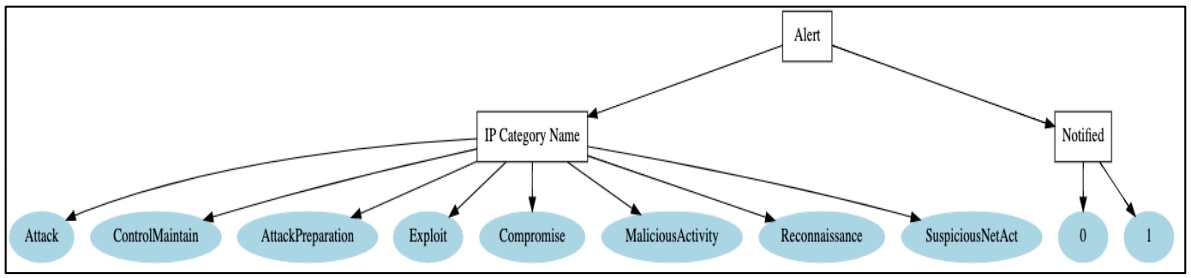


Fig 4: Best Categories

["Suspicious Account Activity" and "To Be Determined"] categories are removed as there is no attack notified for them.

3). Overall Taxonomy of attributes:

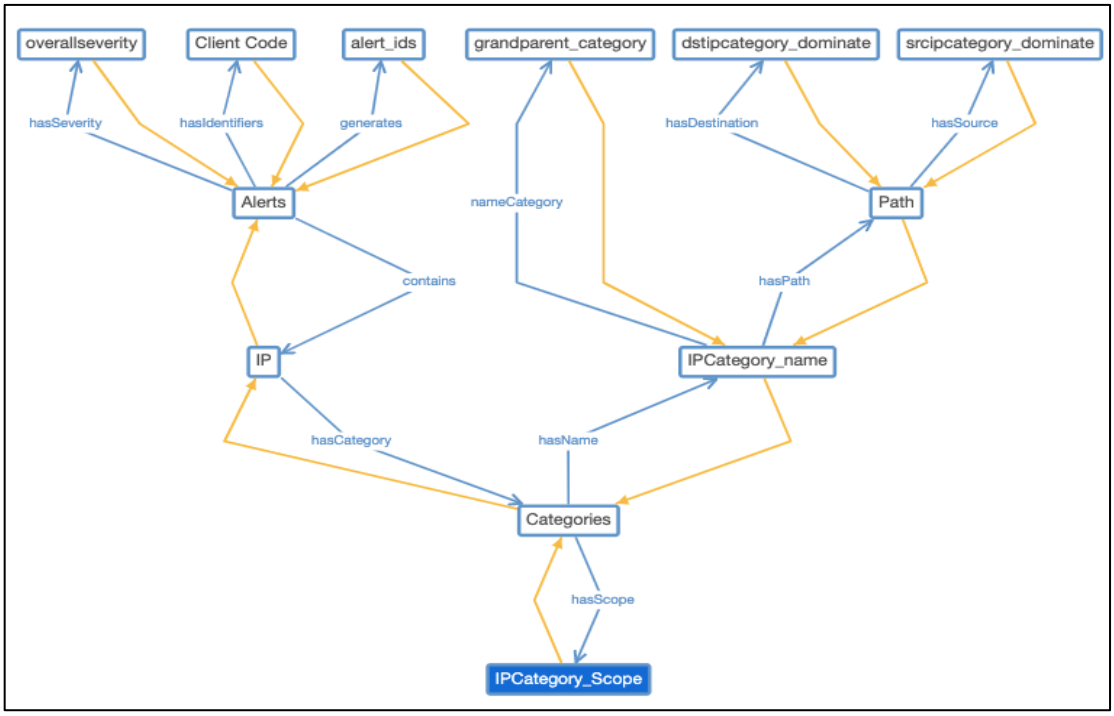


Fig 5: Overall taxonomy of features

Similarly, hierarchical structures can be drawn for Alerts generated on which day of a week of which category name and they are notified or not to client, we can also check the severity of those alerts as well.

Below is the query for categoryname= "Attack" which generates most results which is equal to 556 rows and least number of attacks on weekends (sat and sun).

```
data_cat.loc[(data_cat['weekday'].isin(['Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', 'Sun'])) &
        (data_cat["categoryname"] == 'Attack') & (data_cat['overallseverity'] > 3) &
        (data_cat['notified'] == 1)]
```

C. Identify at least 5 explicit binary relations that could exist between two alert incidents.

1). Given two feature-domains Internet and Private Network (Priv-192, Priv-172, Priv-10) in IPCategory, we consider pair (Private {all used priv networks in dataset}, internet). Where priv belongs to Private networks and Internet belongs to all outside networks.

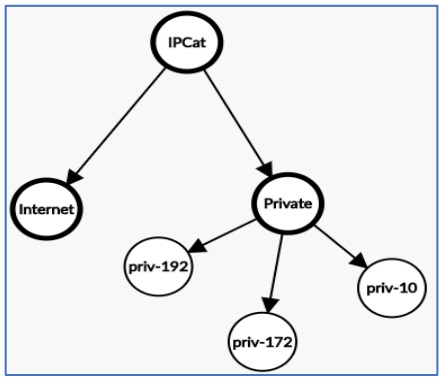


Fig c (1): Binary relation between IPCategory

2). Given two features CategoryName and Weekday, we consider pair (weekdays, Suspicious Network Activity). Where all days of a weeks except Sat there is an attack of type Suspicious Network Activity.

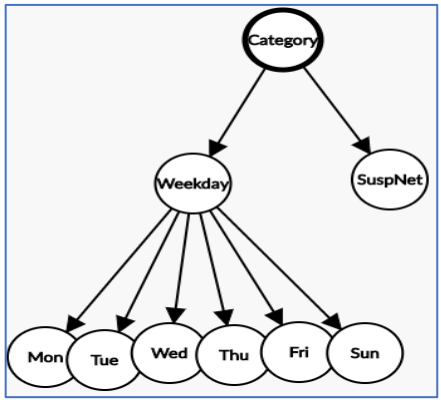


Fig c (2): Binary relation between attack and weeks

3). Given two features Grandparent_categoryIP and Notified, we consider pair (A, 1). Where all notified alerts i.e. 1 are of category= A and no alert notified for category= B.

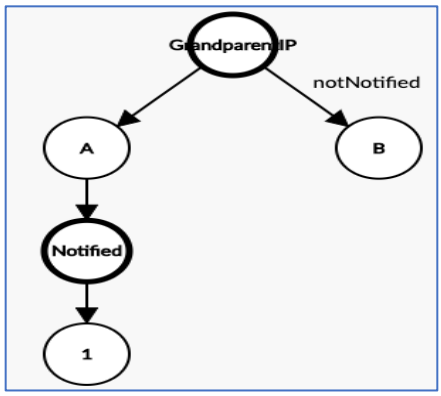


Fig c (3): Binary relation between Grandparent_IP and notified

4). Given two features Category name of an alert and overall severity, we consider pair {(attack, Reconnaissance, Suspicious Reputation, Compromise), 5}. Where category name of an alerts whose severity is 5 and the other categories does not have severity=5.

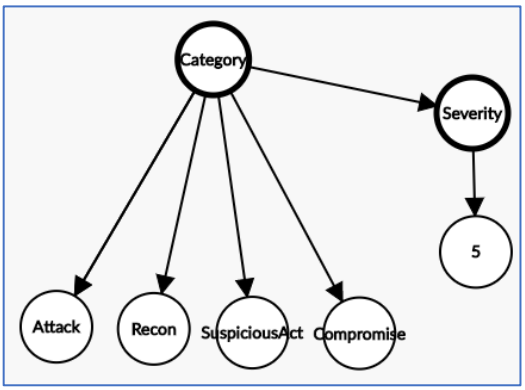


Fig c (4): Binary relation between Alert Category and Overall Severity

5). Given two features IPCategory_Scope and Grandparent_category of an IP, we consider pair {(Internet, Private network), A}. Where category scope of an IP lies in Internet and Private network whose grandparent category is "A" and the other category i.e. "B" does not have any data.

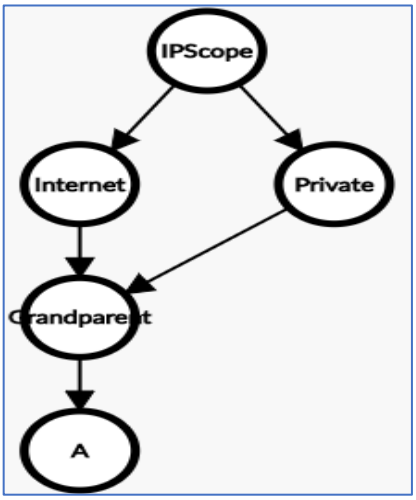


Fig c (5): Binary relation between IP Scope and IP_GrandparentCategory

D. Identify at least 2 N-ary relations that could exist between two or more alert incidents.

1). Based on attributes such as IP, IPCategory Name and Scope generated on Weekdays and their important feature-domains. Importance of feature-domains is measured by finding the greatest number of records generated from total dataset.

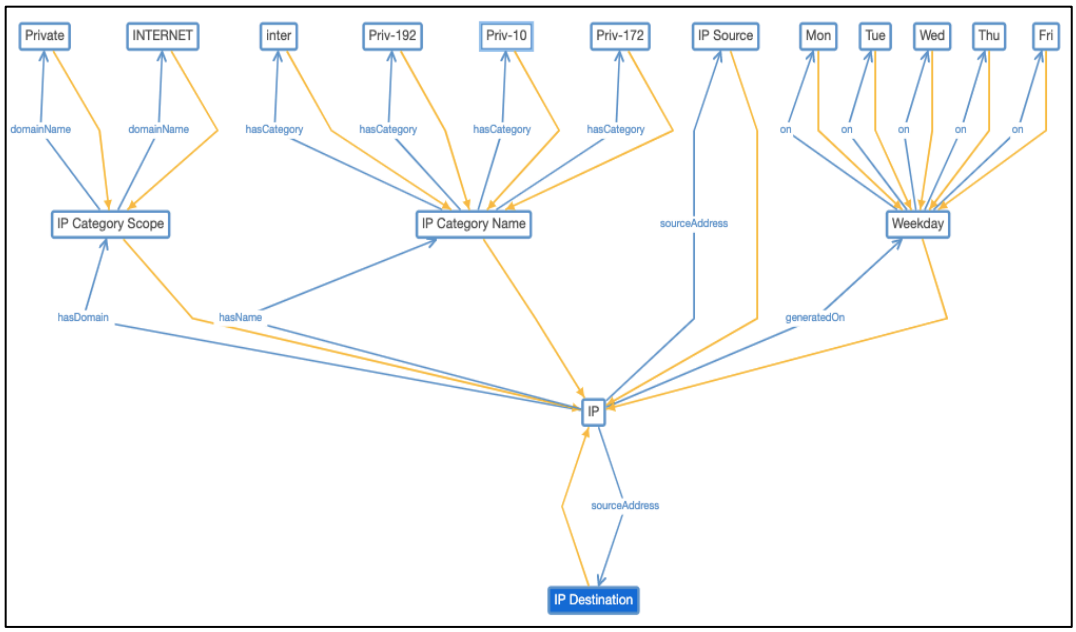


Fig 6: N-ary relations for IP's

2). Based on attributes such as Alert, Severity of an alert, Client Code, Category Name and are alerts notified or not and their important feature-domains. Importance of feature-domains is measured by finding the greatest number of records generated from total dataset.

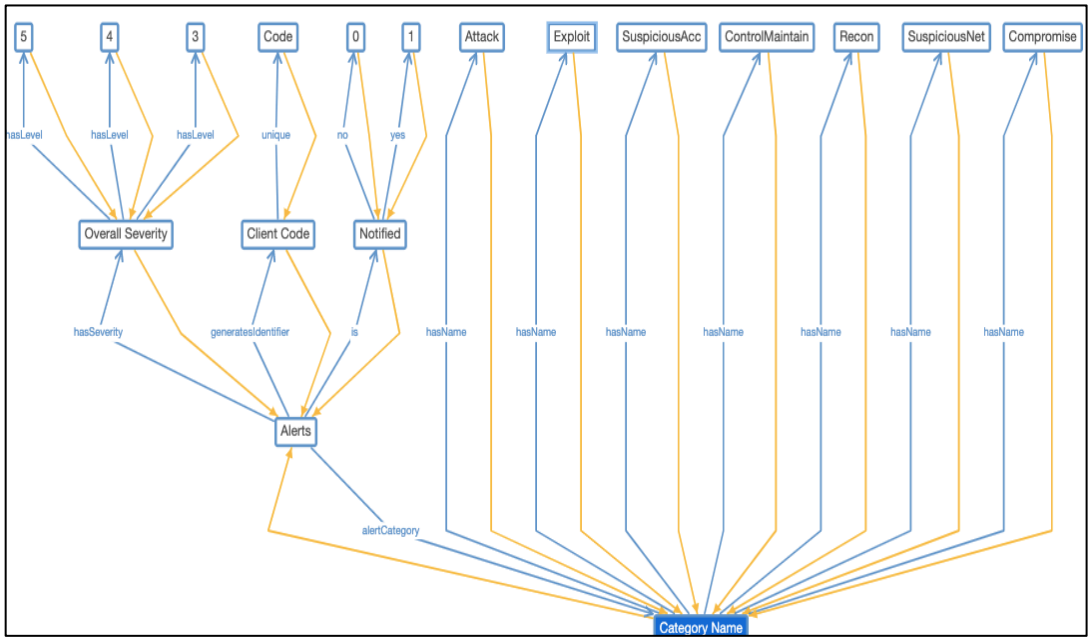


Fig 7: N-ary relations for Alerts

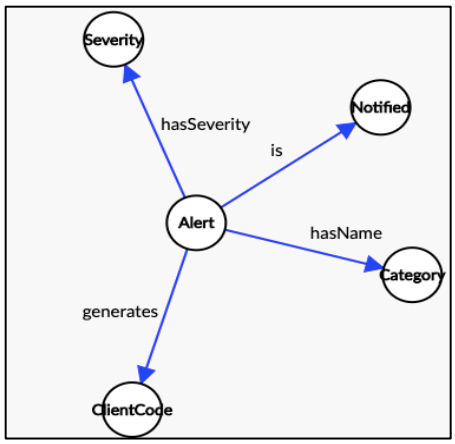


Fig 8: N-ary relations without domains

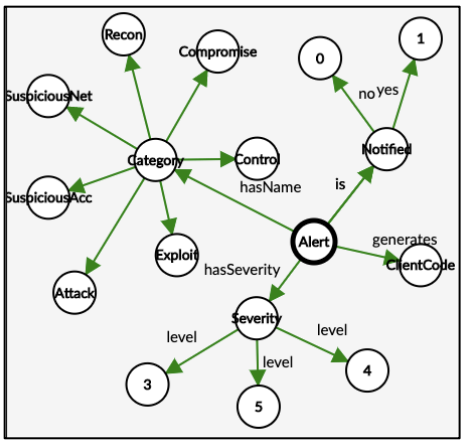


Fig 9: N-ary relations with domains

E. Identify at least 2 implicit relations that could exist between alert incidents.

1) Implicit Relation based on IP, IPCategory Name and their domain-attributes.

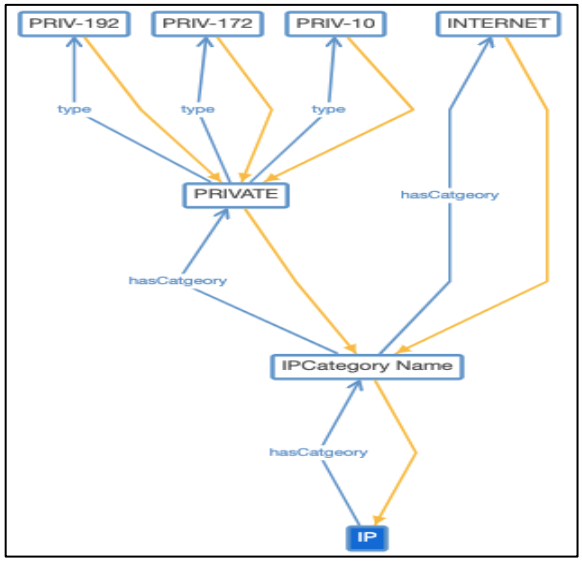


Fig 9: Implicit relation 1

IP address has IP category name has two types of network mainly Internet and Private Network and further private network is divided into three main types. In the dataset we have only used attributes-domains whic h are in majority. So, we have removed [BROADCAST, LINK-LOCAL, LOOPBACK, MULTICAST]

Category Name	Count
BROADCAST	2
INTERNET	26938
LINK-LOCAL	5
LOOPBACK	4
MULTICAST	1
PRIV-10	8410
PRIV-172	1629
PRIV-192	2027

Table 2: attribute-domains with count

2) Implicit Relation based on Alerts, Category Name, Notified and their domain-attributes.

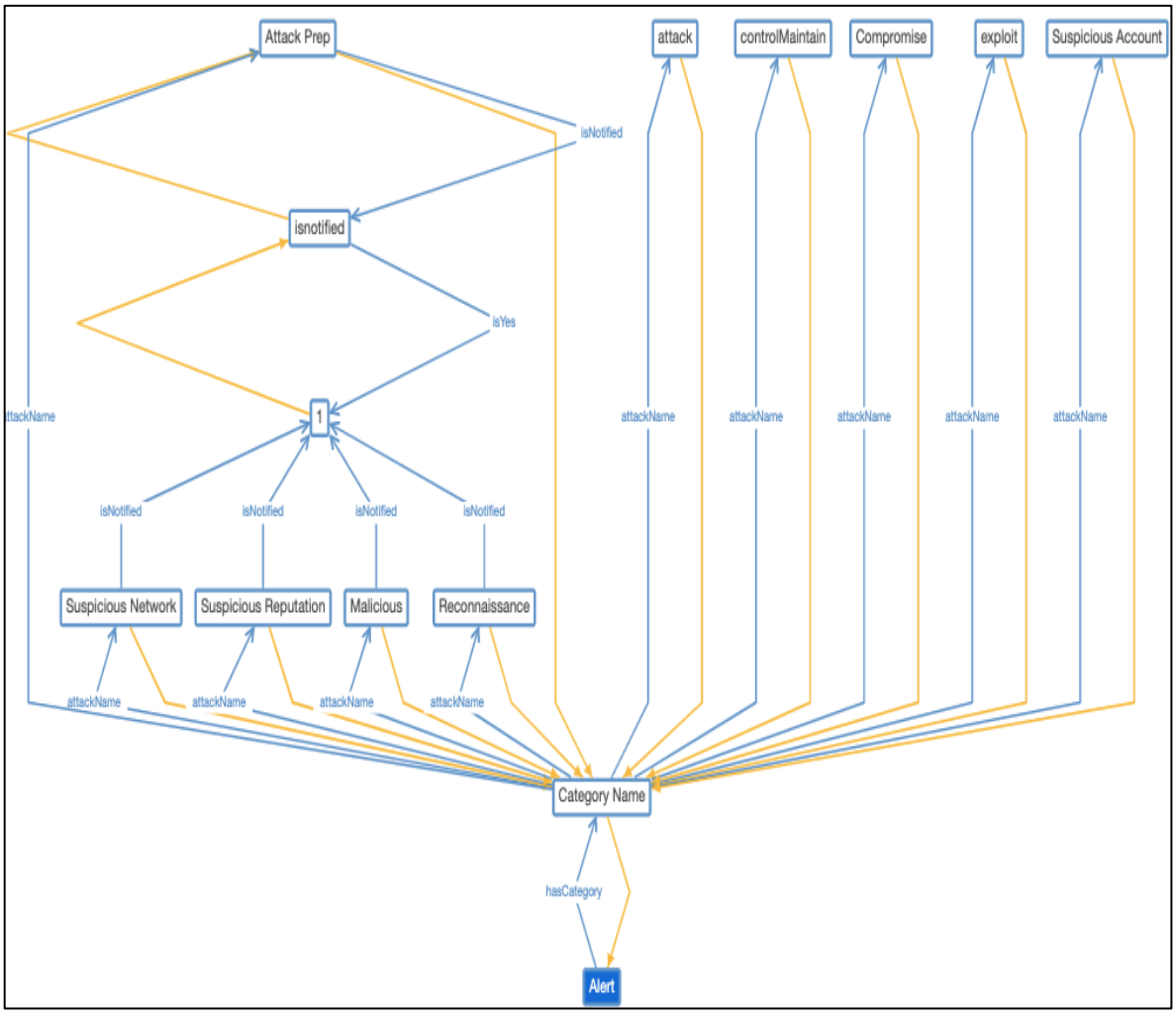


Fig 10: Implicit relation 2

Alert has type of attack, which is Category Name, these are of 11 types (to be determined is not used as it only has 3 tuples) and the relation of these attacks with notified which labels true or false incident. From the graph we can see that in the left side of a graph 5 categories are notified and are true incidents. And the categories in the right are not notified and are false incidents.

2. Graph Representation:

A. Construct a graph to represent the set of all incidents or k subsets of incidents the dataset.

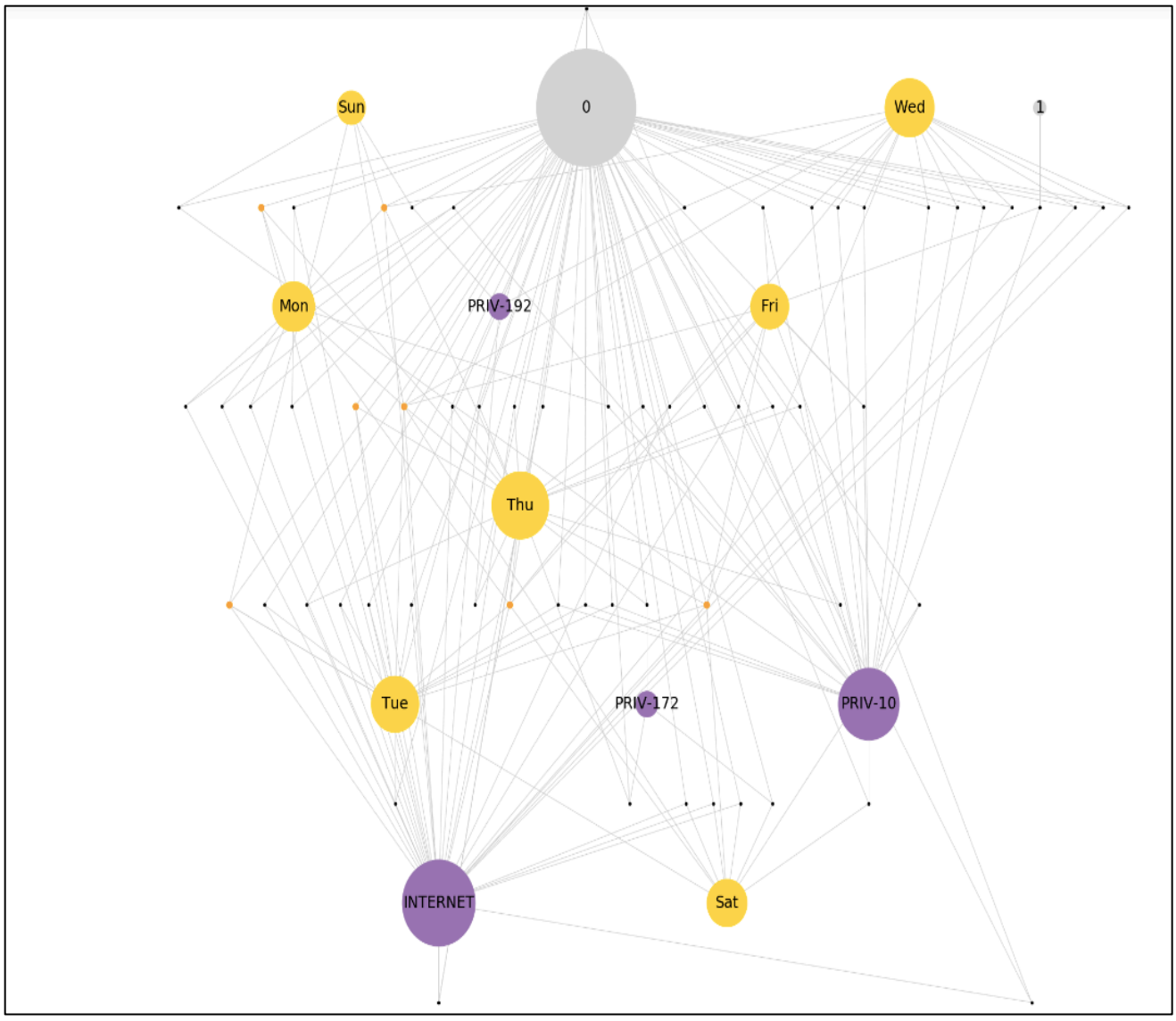


Fig 11: Graph Representing set of incidents

All the ***black nodes*** in the figure 11 indicates the ***Ip addresses*** which has a relationship with type of network and days of the week. However, all the ***orange node*** here indicates ***Ip address*** that are ***most frequently attacked*** and has the degree greater than 4. The above graph is of data size 100 records out of which very few are notified by the expert team. All **purple nodes indicate the type of network** and ***weekdays*** are represented by ***yellow colour***. The major observation from this graph is that the notified attacks are most commonly occurred on private network whereas all the non-notified attacks are on the public network (internet) as well as on weekdays. Very less attacks are reported on weekends.

```
Properties of Graph
radius: 3
diameter: 6
eccentricity: {0: 4, 1: 6, '10.UX.PM.55': 3, 'Wed': 4, 'OW.NT.148.89': 5, 'Sun': 4, '10.FK.AX.24': 3, '10.KW.JR.28':
3, 'KB.FI.252.230': 5, 'XF.CB.202.1': 5, '10.SB.PM.38': 3, 'XI.TB.4.18': 5, 'BG.YX.130.147': 5, '192.SL.GO.61': 5, '1
0.OE.JK.181': 3, '10.YT.EF.102': 3, 'OQ.QJ.38.32': 5, 'EU.FS.44.4': 5, '10.MT.JH.21': 3, 'MD.DO.154.86': 5, '192.SL.U
K.94': 5, 'BI.AL.26.27': 5, 'DJ.TU.110.153': 5, 'XX.AX.31.4': 5, 'JX.NY.13.20': 5, 'OQ.SF.198.19': 5, 'YT.LB.36.21':
5, '10.BW.NO.22': 3, 'MC.ER.197.27': 5, 'Mon': 4, '10.XX.AX.94': 3, 'YA.YT.192.102': 5, '10.CN.CC.70': 3, '172.KM.CM.
79': 5, 'Fri': 4, 'JQ.PJ.190.11': 5, 'YT.LB.38.21': 3, 'VW.OS.0.20': 5, 'JM.OS.196.189': 5, 'SP.OR.134.90': 5, 'Thu':
4, 'IJ.PI.86.150': 5, 'YT.LB.32.21': 3, '10.BK.AX.11': 3, '10.UX.PM.11': 3, 'EE.OS.51.30': 5, '10.XU.ER.118': 3, 'PRI
V-172': 6, '172.BT.EB.7': 5, '192.SL.IV.24': 5, '10.QX.WJ.17': 3, 'PRIV-192': 6, '10.HW.PF.1': 3, '10.ZQ.RC.62': 5,
'10.CD.OO.77': 3, 'UC.ON.242.3': 5, '172.BT.JN.13': 5, '10.YK.ER.10': 3, '10.EI.PJ.221': 3, '10.KW.HM.122': 3, 'EB.Q
D.27.77': 3, 'QP.IJ.202.50': 3, 'YT.LB.34.21': 3, 'Tue': 4, 'UN.BA.28.11': 5, '10.BW.BU.43': 3, 'JM.TR.58.2': 5, 'NZ.
XJ.1.106': 5, 'INTERNET': 4, '10.BH.BV.28': 3, 'DT.DS.64.123': 3, '10.FM.RK.37': 3, 'Sat': 4, 'YT.LB.36.10': 5, 'PRIV
-10': 4}
center: ['10.UX.PM.55', '10.FK.AX.24', '10.KW.JR.28', '10.SB.PM.38', '10.OE.JK.181', '10.YT.EF.102', '10.MT.JH.21',
'10.BW.NO.22', '10.XX.AX.94', '10.CN.CC.70', 'YT.LB.38.21', 'YT.LB.32.21', '10.BK.AX.11', '10.UX.PM.11', '10.XU.ER.11
8', '10.QX.WJ.17', '10.HW.PF.1', '10.CD.OO.77', '10.YK.ER.10', '10.EI.PJ.221', '10.KW.HM.122', 'EB.QD.27.77', 'QP.IJ.
202.50', 'YT.LB.34.21', '10.BW.BU.43', '10.BH.BV.28', 'DT.DS.64.123', '10.FM.RK.37']
periphery: [1, 'PRIV-172', 'PRIV-192']
density: 0.074954954955
```

Properties of Graph:

Eccentricity of a Vertex: It is the maximum of distances between a vertex to all other vertices. To calculate eccentricity of any vertex, we must know the distance between that vertex to all other vertices.
Radius of a connected Graph: Minimum eccentricity of all the vertices of a graph is referred as the radius of that graph.
Diameter of a connected Graph: Radius of a graph is the minimum value of the eccentricity for all the vertices, similarly, Diameter of a graph is the maximum value of the eccentricity for all the vertices.
Central point of a graph: Vertex for which the eccentricity is equal to the radius of the graph is known as central point of the graph.
Periphery of a graph: The periphery is the set of nodes with eccentricity equal to the diameter.
Density of a graph: A measure of how many edges a Graph has. The actual definition will vary depending on type of Graph and the context in which the question is asked. For a complete undirected Graph, the Density is 1, while it is 0 for an empty Graph. Graph Density can be greater than 1 in some situations (involving loops).

B. Apply shared attribute analysis to detect similar sub-graph structures.

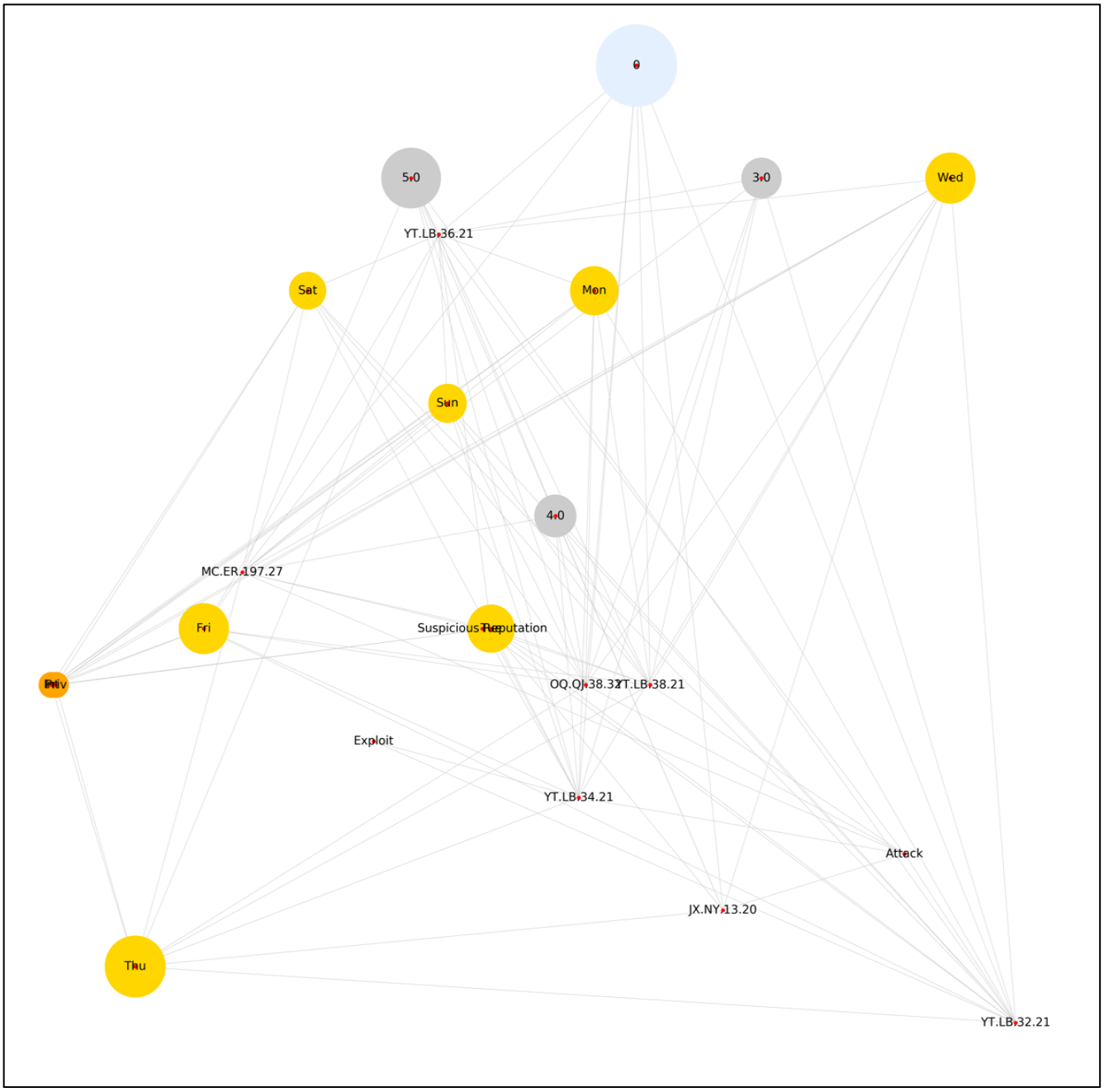


Fig 12: Sub-Graph structure for Non-Notified Attack

The figure 12 and figure 13 are the structural representation of notified vs non-notified attacks. The major difference between two graphs is that the notified attacks has more complex structure and has variance in terms of category of attacks. The common attack categories that are notified includes Exploit, Reconnaissance, Control and Maintain, Suspicious Network Activity etc. On the other hand, for non-notified attacks this variance of attack category is very less (Exploit, Suspicious Network Activity, Attack).

Some observable patterns (Section D) for notified attacks are:

- Most of the attacks occurred on Wednesday.
- The overall severity of most attacks is of level 5, one noticeable fact is level 3 severity attacks are very less.
- Complex bonding between attack categories like Exploit, Reconnaissance, Control and Maintain, Suspicious Network Activity.

Fig 13: Sub-Graph structure for Notified attack

Some observable patterns (Section D) for non-notified attacks are:

- Most of the attacks occurred on Thursday.
- The overall severity of most attacks is of level 5.
- Detached or loose bonding between attack categories like Exploit, Reconnaissance, Control and Maintain, Suspicious Network Activity.

Attributes which are shared between both the structures include:
The overall severity nodes 3,4,5 and all weekdays are included in both the structures. The attack categories like Attack, Exploit and Suspicious Network Activity as well as type of the networks like Internet and Private are also part of both the structures.

C. Apply community's detection algorithm over the confirmed incidents and non-confirmed incidents and comments on the structures of the different communities.

```
([0, 3.0, 4.0, 5.0, 'Attack', 'Fri', 'Int', 'JX.NY.13.20', 'MC.ER.197.27', 'Mon', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Su
n', 'Suspicious Reputation', 'Thu', 'Tue', 'Wed', 'YT.LB.32.21', 'YT.LB.34.21', 'YT.LB.36.21', 'YT.LB.38.21'], ['Expl
oit'])
([0, 3.0, 4.0, 5.0, 'Attack', 'Fri', 'Int', 'JX.NY.13.20', 'MC.ER.197.27', 'Mon', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Su
n', 'Thu', 'Tue', 'Wed', 'YT.LB.32.21', 'YT.LB.34.21', 'YT.LB.36.21', 'YT.LB.38.21'], ['Suspicious Reputation'], ['Ex
ploit'])
([0, 3.0, 4.0, 5.0, 'Attack', 'Fri', 'Int', 'MC.ER.197.27', 'Mon', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Sun', 'Thu', 'Tue',
'Wed', 'YT.LB.32.21', 'YT.LB.34.21', 'YT.LB.36.21', 'YT.LB.38.21'], ['Suspicious Reputation'], ['JX.NY.13.20'], ['Exp
loit'])
([0, 3.0, 5.0, 'Attack', 'Fri', 'Int', 'MC.ER.197.27', 'Mon', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Sun', 'Thu', 'Tue', 'We
d', 'YT.LB.32.21', 'YT.LB.34.21', 'YT.LB.36.21', 'YT.LB.38.21'], [4.0], ['Suspicious Reputation'], ['JX.NY.13.20'],
['Exploit'])
([0, 3.0, 5.0, 'Fri', 'Int', 'MC.ER.197.27', 'Mon', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Sun', 'Thu', 'Tue', 'Wed', 'YT.LB.
32.21', 'YT.LB.34.21', 'YT.LB.36.21', 'YT.LB.38.21'], [4.0], ['Suspicious Reputation'], ['Attack'], ['JX.NY.13.20'],
['Exploit'])
([0, 3.0, 'Fri', 'Int', 'MC.ER.197.27', 'Mon', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Sun', 'Thu', 'Tue', 'Wed', 'YT.LB.32.2
1', 'YT.LB.34.21', 'YT.LB.36.21', 'YT.LB.38.21'], [4.0], [5.0], ['Suspicious Reputation'], ['Attack'], ['JX.NY.13.2
0'], ['Exploit'])
```

Fig 14: Communities detection using Girvan-Newman method for Non- Notified attack.

```
([1, 3.0, 4.0, 5.0, '10.CN.MX.204', '10.WF.ZT.41', 'Attack', 'BI.YA.131.241', 'Exploit', 'Fri', 'Int', 'MC.ER.197.2
7', 'Mon', 'OQ.QJ.38.32', 'Priv', 'QP.LB.207.44', 'Reconnaissance', 'Sat', 'Sun', 'Suspicious Network Activity', 'Th
u', 'Tue', 'Wed', 'YA.HF.189.131', 'YA.JQ.113.123'], ['Control and Maintain'])
([1, 3.0, 4.0, 5.0, '10.CN.MX.204', '10.WF.ZT.41', 'Attack', 'BI.YA.131.241', 'Exploit', 'Fri', 'Int', 'MC.ER.197.2
7', 'Mon', 'OQ.QJ.38.32', 'Priv', 'QP.LB.207.44', 'Reconnaissance', 'Sat', 'Sun', 'Thu', 'Tue', 'Wed', 'YA.HF.189.13
1', 'YA.JQ.113.123'], ['Suspicious Network Activity'], ['Control and Maintain'])
([1, 3.0, 4.0, 5.0, '10.CN.MX.204', '10.WF.ZT.41', 'Attack', 'BI.YA.131.241', 'Exploit', 'Fri', 'Int', 'MC.ER.197.2
7', 'Mon', 'OQ.QJ.38.32', 'Priv', 'QP.LB.207.44', 'Sat', 'Sun', 'Thu', 'Tue', 'Wed', 'YA.HF.189.131', 'YA.JQ.113.12
3'], ['Suspicious Network Activity'], ['Reconnaissance'], ['Control and Maintain'])
([1, 4.0, 5.0, '10.CN.MX.204', '10.WF.ZT.41', 'Attack', 'BI.YA.131.241', 'Exploit', 'Fri', 'Int', 'MC.ER.197.27', 'Mo
n', 'OQ.QJ.38.32', 'Priv', 'QP.LB.207.44', 'Sat', 'Sun', 'Thu', 'Tue', 'Wed', 'YA.HF.189.131', 'YA.JQ.113.123'], [3.
0], ['Suspicious Network Activity'], ['Reconnaissance'], ['Control and Maintain'])
([1, 4.0, 5.0, '10.CN.MX.204', '10.WF.ZT.41', 'Attack', 'BI.YA.131.241', 'Exploit', 'Fri', 'Int', 'MC.ER.197.27', 'Mo
n', 'OQ.QJ.38.32', 'Priv', 'Sat', 'Thu', 'Tue', 'Wed', 'YA.HF.189.131', 'YA.JQ.113.123'], [3.0], ['QP.LB.207.44', 'Su
n'], ['Suspicious Network Activity'], ['Reconnaissance'], ['Control and Maintain'])
([1, 4.0, 5.0, '10.CN.MX.204', '10.WF.ZT.41', 'Attack', 'BI.YA.131.241', 'Exploit', 'Int', 'MC.ER.197.27', 'Mon', 'O
Q.QJ.38.32', 'Priv', 'Sat', 'Thu', 'Tue', 'Wed', 'YA.HF.189.131', 'YA.JQ.113.123'], [3.0], ['QP.LB.207.44', 'Sun'],
['Fri'], ['Suspicious Network Activity'], ['Reconnaissance'], ['Control and Maintain'])
```

Fig 15: Communities detection using Girvan-Newman method for Notified attack

The Girven-Newman Algorithm has four steps and can be given as follows:

a. The betweenness of all existing edges in the network is calculated first.

b. The edge with highest betweenness is removed.

c. The betweenness of all edges affected by the removal is recalculated.

d. Steps b. and c. are repeated until no edges remain.

The Girvan Newman technique for the detection and analysis of community structure depends upon the iterative elimination of edges with the highest number of the shortest paths that pass through them. By getting rid of the edges, the network breaks down into smaller networks, i.e. communities

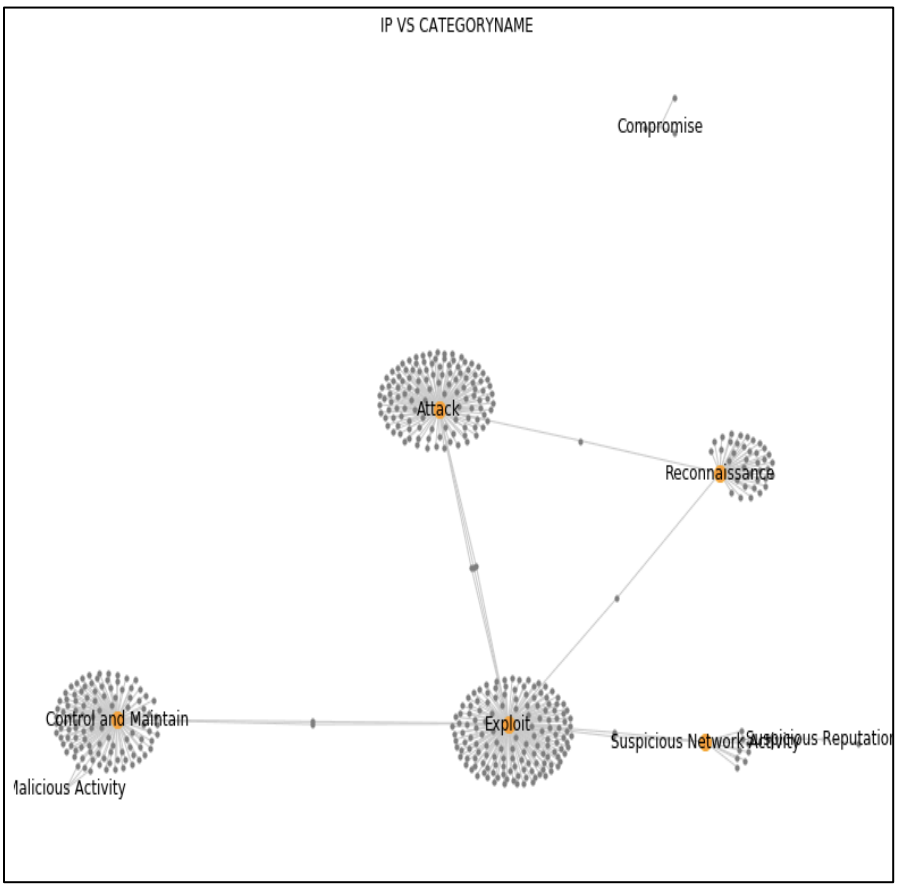
The idea was to find which edges in a network occur most frequently between other pairs of nodes by finding edges betweenness. The edges joining communities are then expected to have high edge betweenness. The underlying community structure of the network will be much fine-grained once we eliminate edges with high edge betweenness.

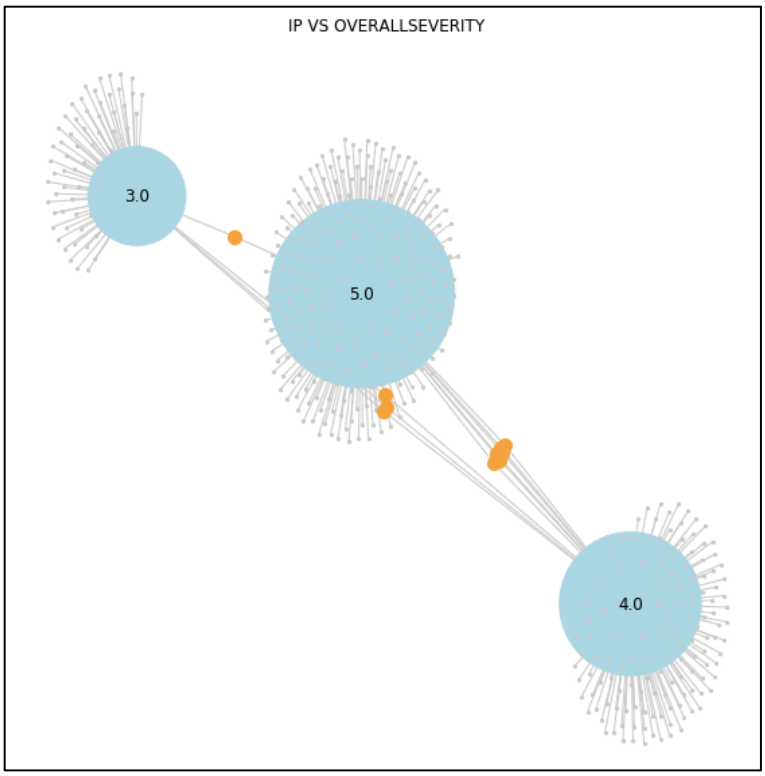
Structure of communities in Notified attack vs Non-notified attack:

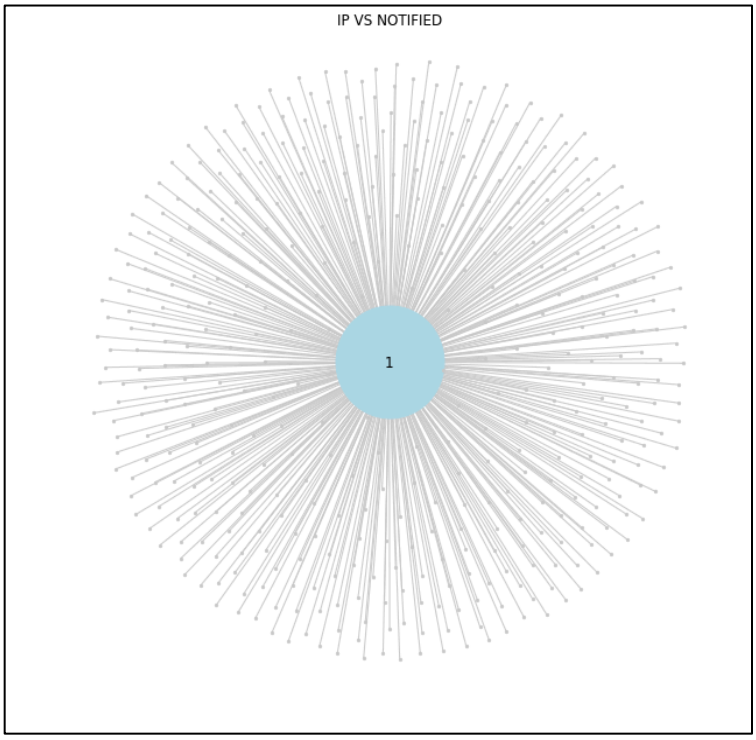
Figure 14 represents ***communities of non-notified attack***, the structural difference which we observe in the community array is ***that all IP's in a single community are generally belong to same sub-network***. Figure 15 represents ***communities of notified attack*** which consist of ***IP's belonging to different sub-networks***. The ***bonding*** between ***the severity node '3' vs '4'or '5***' is less in non-notified community structure compared to notified one. Other difference is the ***number of nodes*** in non-notified community structure are less as compared to notified.

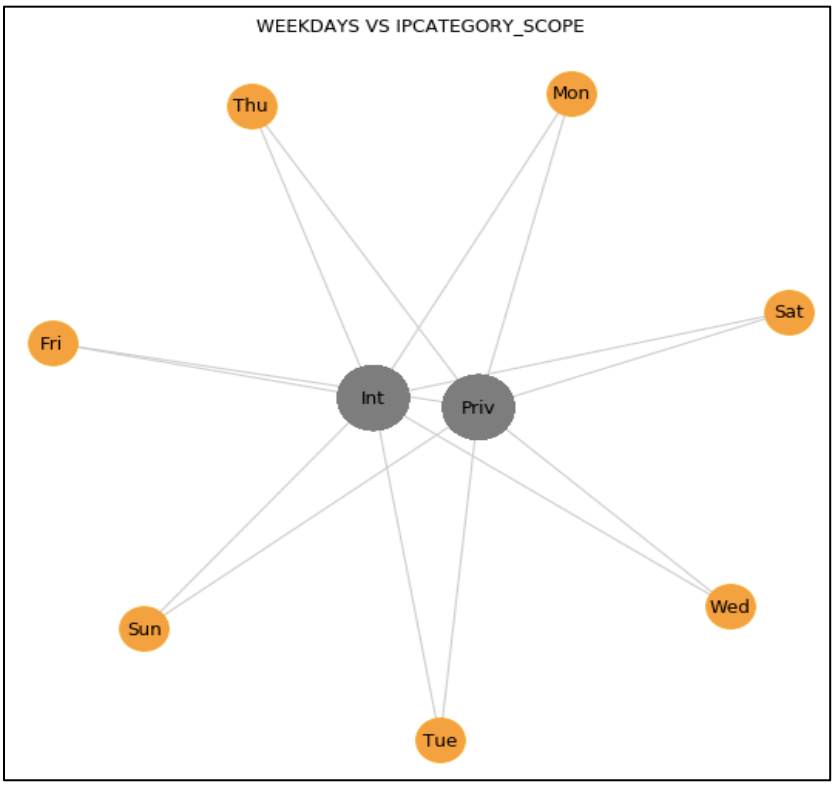
A. Make sure to use proper methods to visualize your graphs

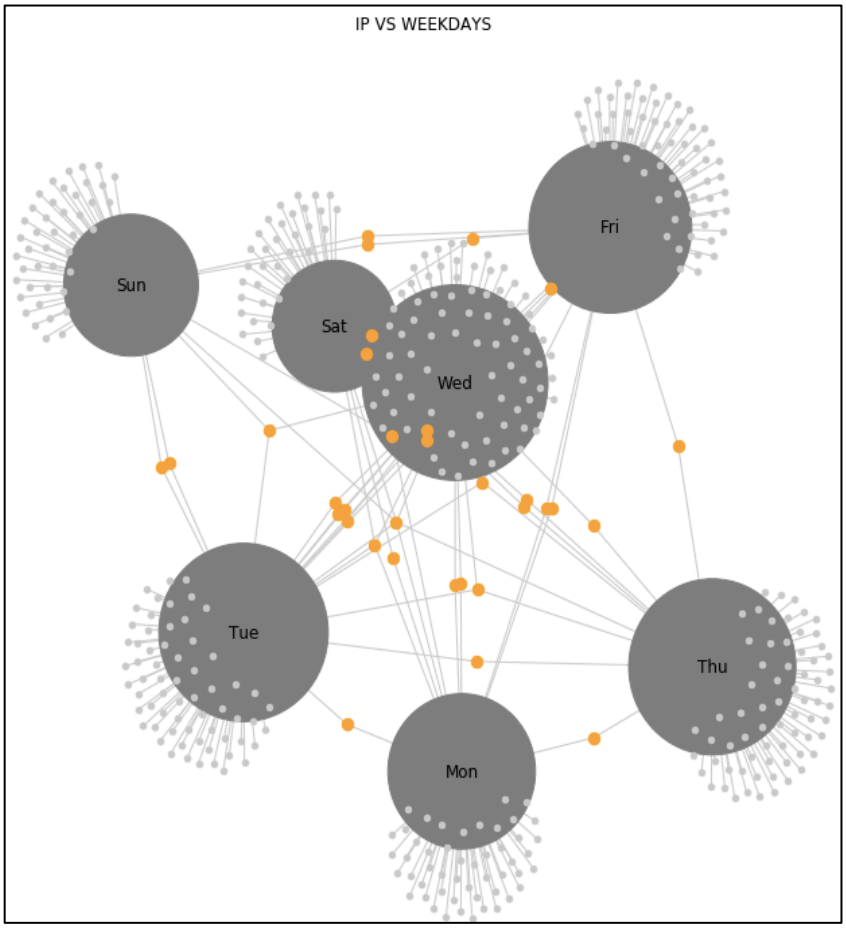
Fig 16: Graphical Structures between individual columns to recognize the pattern for notified attacks.




IP VS OVERALLSEVERITY
3.0
5.0
4.0


IP VS NOTIFIED
1


WEEKDAYS VS IPCATEGORY_SCOPE
Thu
Mon
Fri
Sat
Int
Priv
Sun
Wed
Tue


IP VS WEEKDAYS
Sun
Fri
Sat
Wed
Tue
Thu
Mon

All the above mention in the figure 16 are part of the analysis to figure out the patterns involved in notified attacks by expert team. All the graphs are with respect to one common attribute IP to address questions like:

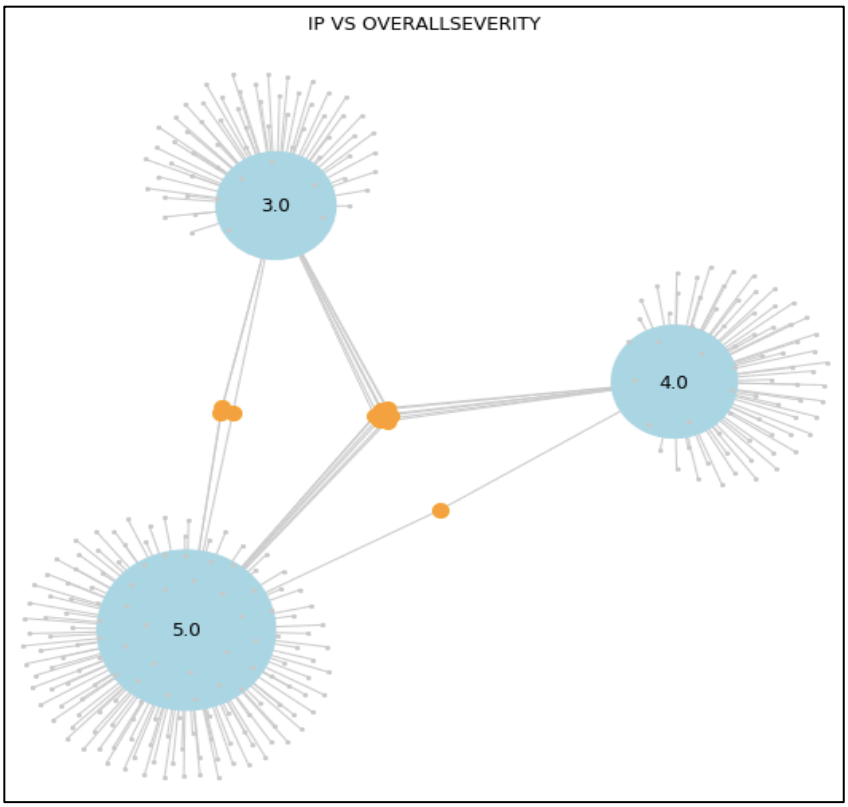
1)Which IP and how many is attacked on weekend vs weekdays?

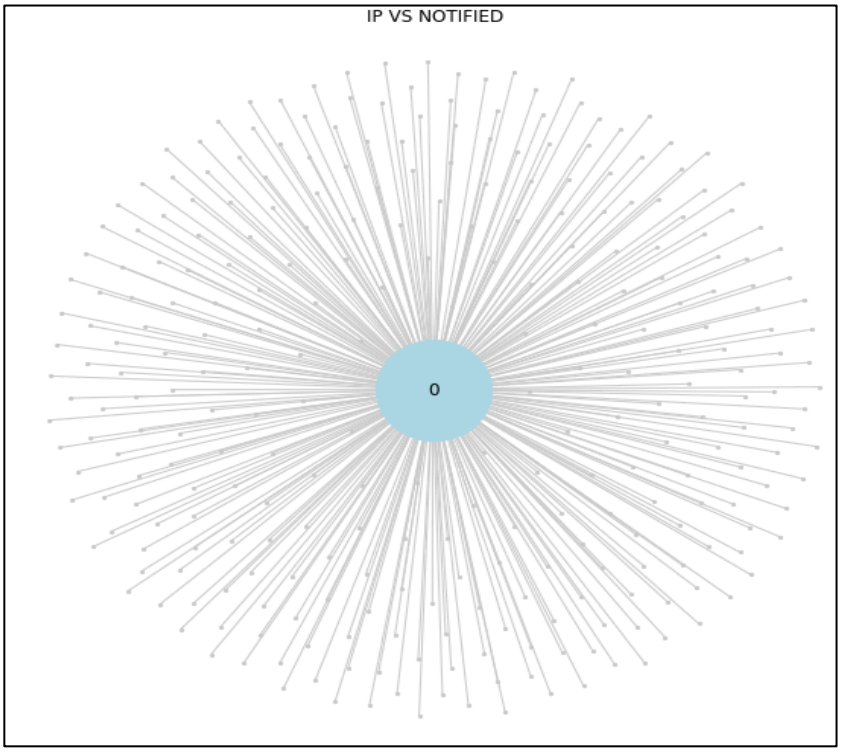
2)To check what is the nature of attack based on the severity and which IP's are involved in all severity categories.

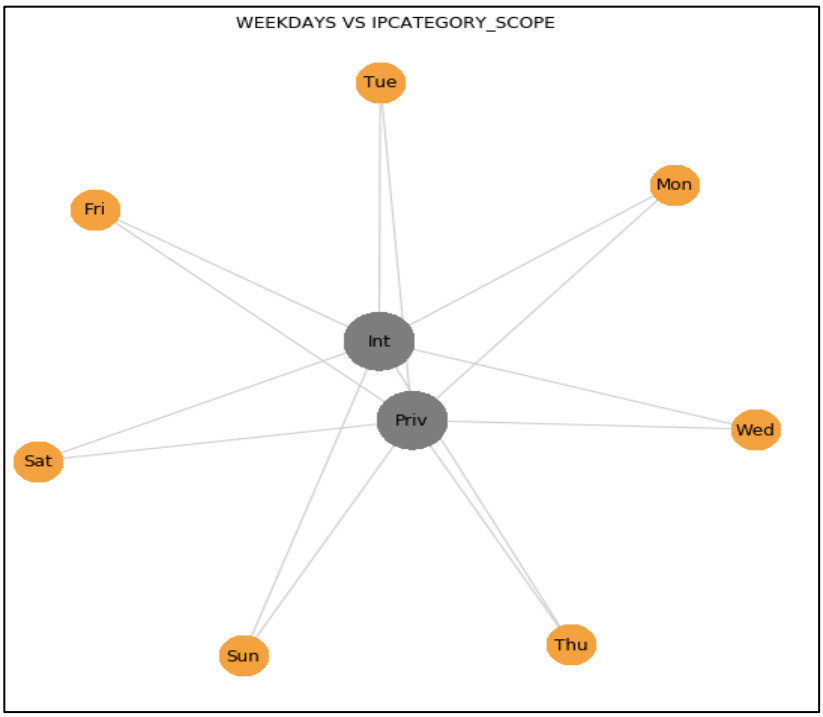
3)Which category of attack is mostly notified by the expert team.

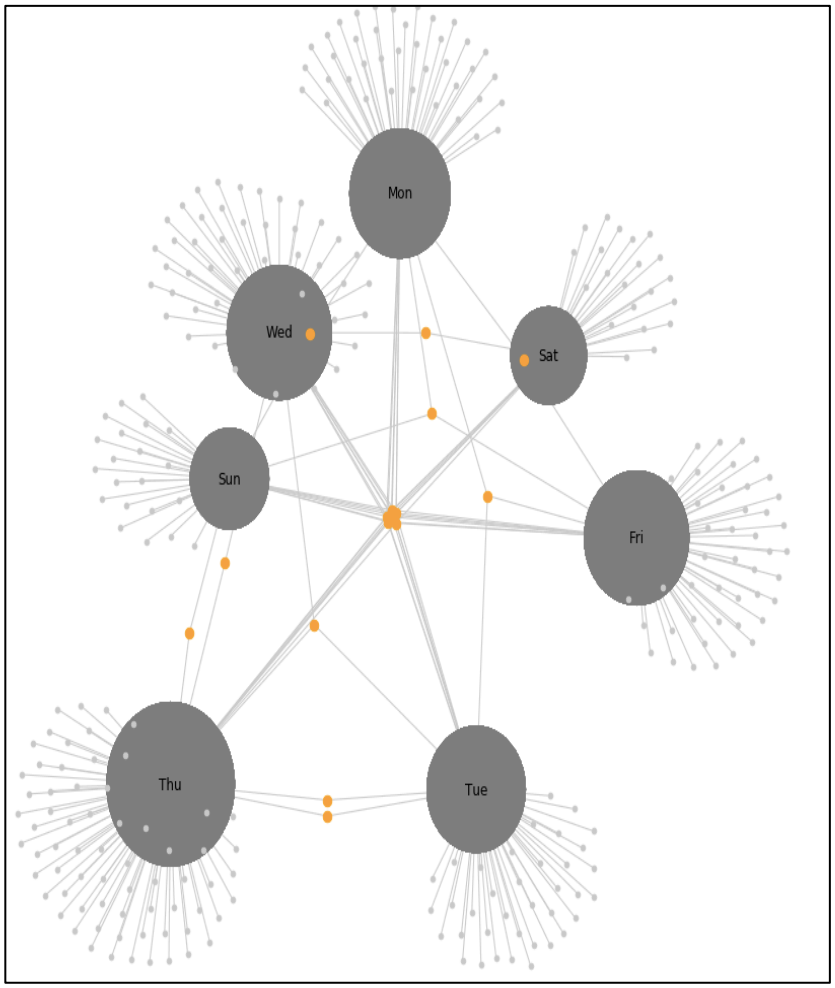
4) Which type of network is repeatedly targeted by the attackers.

Figure 17: Graphical Structures between individual columns to recognize the pattern for non-notified attacks.


IP VS OVERALLSEVERITY
3.0
4.0
5.0


IP VS NOTIFIED
0


WEEKDAYS VS IPCATEGORY_SCOPE
Tue
Mon
Fri
Int
Priv
Wed
Sat
Sun
Thu


Mon
Wed
Sat
Sun
Fri
Thu
Tue

All the above mention in the figure 17 are part of the analysis to figure out the patterns involved in not notified attacks by expert team. All the graphs are with respect to one common attribute IP to address questions like:

1)Which IP and how many is attacked on weekend vs weekdays?

2)To check what is the nature of attack based on the severity and which IP's are involved in all severity categories.

3)Which category of attack is mostly not notified by the expert team.

4) Which type of network is repeatedly targeted by the attackers.