Vidhyayana - ISSN 2454-8596

An International Multidisciplinary Peer-Reviewed E-Journal

www.j.vidhyayanaejournal.org

Indexed in: ROAD & Google Scholar

Trend analysis of Network Attacks: Visualization and Prediction in Complex Multi-Stage Network

Parimalkumar P Patel

Research Scholar, Khyati School of Computer Application, Gujarat University

Dr. Binod Agarwal

Eminent Professor, Calorx Teachers' University

Dr. Dharmeshkumar Bhavsar

Director & Associate Professor, Shri Chimanbhai Patel Institute of Computer Application, Gujarat University

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

ABSTRACT

There are many protocols for network security, however none of them can be considered secure. Additionally, it is difficult and time-consuming to train end users. It is true that developing into a skilled cybersecurity specialist requires a lot of time. Through several incremental penetrations that have the potential to attack crucial systems, many hackers and criminals attempt to exploit the flaws. The standard tools that are available for this purpose are insufficient to handle the situation as needed. With continually changing networks, risks are always there and are very likely to result in serious incidents. A methodology to visualize and forecast cyberattacks in intricate, multilayered networks has been put forth in this scientific effort. The calculation will be in accordance with the networks within the particular domain's cyber software vulnerabilities. There is a summary of all the network security options accessible as well as potential vulnerabilities in the system. The matrix is used to show the attacker's vulnerability-based multi-graph method. Additionally, a proposed attack graph algorithm identifies all the weak points in the network, allowing for the placement of sensors at the required locations to harden the network. Multi-Stage Cyber Attack Vulnerabilities are evaluated using the described attack graph

Keywords: Network vulnerability; attack graph; adjacency matrix; clustering technique; cyber defense.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

1. Introduction

Effective use of the Internet and related technologies has grown in recent years. It may be argued that there are more and more models being identified every day that are in charge of offering services based on the internet and networks. The amount of data being gathered on servers and network computers is significantly growing as more people utilise the internet. The systems' availability of sensitive and vulnerable data makes it relatively simple for an attacker, and a data breach affects businesses' intellectual property (Mishra et al., 2021). The risk of data loss or an assault on network-based devices is rising daily. It is vital to determine how these attacks might be reduced, or better yet, prevented, so programmers everywhere are working to create and design systems that can recognise the entry of unethical attackers from remote sites (Gupta et al., 2020). Every now and then, several cybercrimes are reported, and based on these, vulnerabilities are found (Mishra et al., 2020). (Mishra et al., 2021). There are two ways to detect intrusions: using an intrusion detection system or an intrusion prevention system. The detection system, on the other hand, can sound the alarm and identify a threat to the software-based system or server machines, whereas the prevention system only assigns the risk of getting an exploit. Indeed, the availability of such systems is urgently needed, and more secure techniques must be created and developed to safeguard the confidentiality and integrity of personal data (Sarker et al., 2020). (Mishra, 2020). The intrusion detection system is more effective overall and is divided into different categories based on the following parameters: Analyzed Activities: An activity-based intrusion detection system is one that can analyse network activity while also identifying involvement.

2. Literature Review

It is now possible to design an attack graph or realistic computer networks thanks to a number of developments made in attack graphs in recent years. Researchers have been attempting to process the data related to attack graphs and how they are created, as well as real-time network systems, for a very long time (Husak et al., 2018). We have researched a variety of these methods to incorporate into our strategy in order to maximise its effectiveness (Liu et al., 2020).

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

The techniques discussed in this study were primarily concerned with constructing the adjacency matrix from the attack graphs (Ghadi et al., 2020). A strong report on employing attack graphs to analyse vulnerabilities was also provided by a similar author. The authors of (Liu et al., 2020) provided a highly compelling framework for network security and proactive intrusion prevention at different phases. According to the information provided in (Lallie et al., 2020), one of the most significant causes of cyberattacks was the vulnerability. Finding these vulnerabilities was crucial and was presented in the study as noted by (Pirani et al., 2021). Our project's attack graph visualisation method is another crucial component. For graph visualisation, Cinque et alspecified .'s theory served as the foundation. Another excellent visualisation strategy was offered by the authors in (Stergiopoulos et al., 2021), and it was incorporated into one of the research methodology modules in this study. The deployment of appropriate sensor-based devices at vulnerable locations is the most important aspect of our research. The investigation needs to identify these vulnerable situations, which is another crucial component. It is possible to depict sensors in the attack graphs schematically by positioning them in an alerting and prioritising position.

In order to get the right answers in cyberspace, the author suggested a reliable design for embedding sensors in attack graphs (Pourhabibi et al., 2020). The research's next phase focuses on locating potential attack points and fortifying the network to prevent susceptibility. The work (Ibrahim et al., 2020), (Sansavini & Parigi, 2020), which uses attack graph hardening techniques and topological analysis, adds a new dimension for managing cyber threats at the time of vulnerabilities. Topological examination for vulnerabilities, then, became the study's and the proposal's main foundation. Using attack graphs is a systematic way for identifying relationships between intrusion events and attack scenario. The hierarchical aggregation of these networks was reported in (Singhal & Ou, 2017), yet these graphs are thought to be exceedingly complex.

This strategy changes the game in terms of network security by identifying all exploitation portions from the graph utilising a variety of prediction techniques and the fundamental notion of vulnerability and evaluation.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

The methodology employed in this study creates a method for recognising intricate attack graphs. Unquestionably, there are a lot of strongly connected subgraphs in huge networks. However, this specific paragraph tends to be where the majority of network vulnerabilities exist. The edges that are most susceptible to network attacks are represented by the adjacency matrices for the relevant attack graphs.

To locate the adjacency matrix branches in the graph, an information-theoretic clustering method is used. Linear scaling is necessary because the clustering method is considered to be totally automatic. The adjacency matrix's components often represent the stages taken during an attack. These edges can be used to determine the attacker's reachability. A single matrix can be derived when the different factors have been identified. The research's solution aims to handle all feasible steps as well as the portion of the attacker's graph that is a transitive closure. This research's methodology takes into account the vulnerability-based graph attack. With the aid of this representation, all of the network security conditions that are now in existence and the potential areas where an attacker could exploit the system are compiled.

This allows for the identification of the attacker's attack patterns. With the use of a matrix, the attacker visualises the vulnerability-based multi-graph approach. Although the method is simple, there is a possibility for anomaly or complexity to appear as a general scheme.

3. Research Methods

The research is broken down into four primary sections: establishing network security measurements for cyber-attacks, creating attack graphs, identifying the matrix, and deploying intrusion detection devices in suitable locations.

1. Using the vulnerability assessment in the topologies, attack graphs are then created.

2. This brings us to our fantastic method for applying adjacency matrix criteria to the graph analysis of cyberattacks.

3. Indicates where various network intrusion detection devices should be placed within the specific network for which the cyber-attack graphs were created.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

4.Gives us the most up-to-date, reliable way, in accordance with the research, for locating, positioning, and exploiting network intrusion detection systems.

Cyber-attack graphs can be made to do vulnerability assessments. Identification of network security using the attack graphs, if possible, in the preliminary stage, might be an important step in this particular milestone. The discovery of the attack graph matrix is the second milestone. The many cyber-attack graph approaches that are discussed in the background section can be used to generate it. The adjacency matrix can be found by using the matrix clustering algorithm to discover various edges. The adjacency matrix can also be transformed to reflect various multi-stage assaults that are feasible for the exploit domains. Using a reachability matrix derived from attack graphs, prediction is based on assault and impact. The placement of attack-based sensors responsible for spotting and tracking any form of attack in the network is the third crucial phase in this particular research, according to the adjacency matrix and attack graphs.

Various optimization techniques can be used to determine the best location for sensors.

This strategy proposes a novel and efficient way to find placement spots by analysing assault graphs. Finding security metrics derived from attack graphs will be the final significant research milestone. Using the aforementioned method, the attack graph module will be generated. Based on the attack graphs created in the first and second processes, this matrix will identify and deliver the whole security value.

3.1 Vulnerability Evaluation

This ideology's central tenet is around vulnerability assessment. The topography in which all of the network's components are set up affects the vulnerability assessment we conduct. With the aid of a graph, all of the vulnerabilities and interdependencies are analysed. This type of method has been employed by some researchers to find vulnerabilities based on topology.

The crucial sentence specifies that all network components that are linked are examined for hardware, software, connection, and network configuration vulnerabilities. Network-based vulnerability areas where an intrusion is likely to happen are used for cross-mapping. The targeted custom situations are examined for weaknesses. The topological analyses of the

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

vulnerability, which were used to generate the attack graph, are what are primarily focused on the methods of network penetration. This offers a very proactive strategy where all the areas that are perhaps vulnerable are taken into account. At certain times, it increases the effectiveness of intrusion detection, allowing for excellent attack defence.

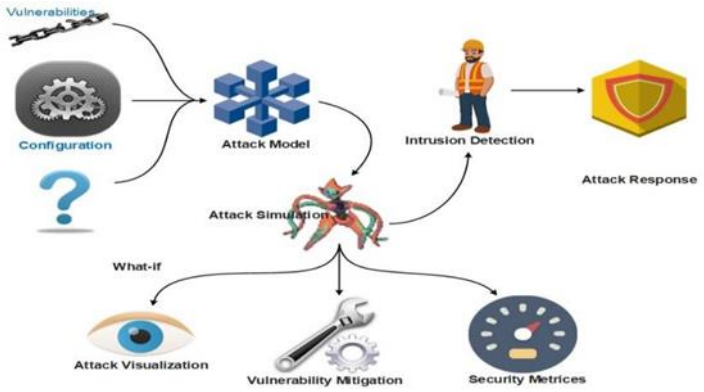


Figure 1: Overview of the Situation

Fig. 1 depicts the hacker's exploitation of the network, along with a general overview and configuration of it.

A multi-stage attack parameter for the network intrusion may be found using the attack graph that is produced. A sample network for creating the attack graph is shown in Figure 2.

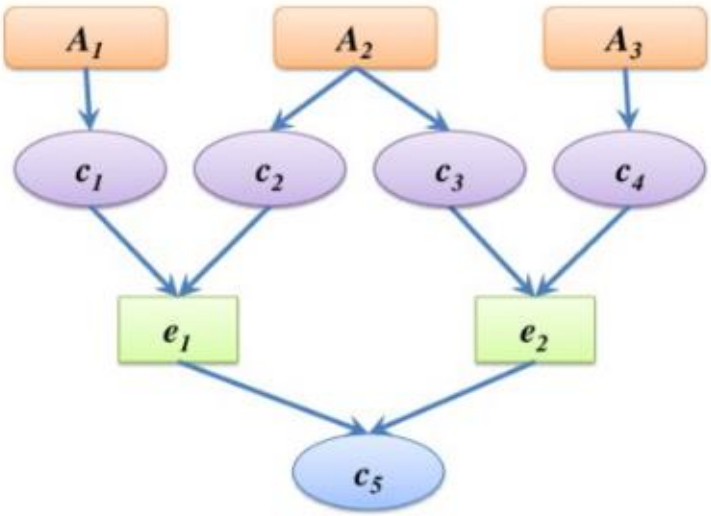


Figure 2: Sample network for generating the attack graph

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

It is assumed that the attack graph generation system may be demonstrated on a small network. The main server and file server are likely only used inside, whereas the web server accepts connections from outside the network. The firewall only enables connections that have a chance of being secure and blocks all other traffic entering the network. It is clear from the scenario whether an attacker from the outside may infiltrate the mail server. The setup elements on the network for the intrusion must be identified in order to mimic this specific scenario with the building of the attack graph. The host computer's systems may contain vulnerable software that can function as a vulnerable device.

When an attacker attempts to enter the internal network, a firewall scans the system to identify any current vulnerabilities. An alternate method to achieve a high level of security is to create the network model using the firewall rules. The first and most crucial action an attacker will do in a certain network is to identify the devices that are weak and have configuration flaws that can be exploited. After breaking into the network, the attacker can run malicious malware and take advantage of the weaknesses in the system. Sometimes, even the firewall can locate such crucial locations and insert the information compromise text. Additionally, it should be mentioned that in the current situation, even the discovery of a single network vulnerability can prevent and stop additional attacks. In most cases, this model is confined to identifying a certain important path that may be a threat source for the entire network, ignoring all other devices, while there are other techniques and packages potentially used for network penetration. The file server has been removed from the above illustration because it is not a crucial component of the exploit. Since it does not form a fundamental aspect of topology-based vulnerability assessments. Fig. 3 displays the attack graph for a compromised mail server. In our network environment, there is no direct route from the attacker to the file server that would link any form of weakness in the graph.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Figure 3 shows the attack graph for the demonstrated network's compromised mail server.

The attack graph's initial step, which has the potential to jeopardise the health of the mail server, is depicted in the above figure. By exposing the firewall's potential weaknesses, the firewall is highly exploited outside of the network. In general, it may be said that this exposure graph indicates that an effort to access and exploit a vulnerability comes from outside the network. With this architecture, the attacker can use the network to execute any acceptable software at will.

The aforementioned illustration depicts a straightforward host that is accessible in the network and can be exploited in a number of ways. In the image above, the main server and web server are both potential targets for exploitation. A specific node cannot be exploited in a direct fashion. A compromise is reached. Perhaps the attacker would follow a set of procedures, or perhaps the attacker would use several steps of exploits to gather all the information.

There are other statistical analysis methods, but one of the best methods that may be used with attack graph analysis is the idea of network hardening. A multi-level graph's information can be used for network hardening. It is possible to map every threat that can be found for each form of network penetration. However, for bigger networks, hardening the network at the outset of an assault minimises network exploitation in the early going. Fig. 4 depicts initial level hardening and its effects.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Figure 4: The effects of Initial Level Hardening

Consequences of not hardening a certain first layer analysis could result in an attacker using internal exploits. When the network is hardened at later tiers, it can be further lowered.

As a result, the last layer's hardening might likewise be unrelated to the attack's origin. In general, any layer can be attacked without warning against the specific possible attacker. Any layer of this type of exploitation will always be attempted to be protected by a solid network vulnerability assessment technique. As shown in Fig. 4, utilising this specific strategy, the network's initial layer of connection can be protected from the outside world to reduce the likelihood of exploitation. It becomes simple for identification and proactive defence to prevent any vulnerability occurring in the network at any time, much like in a broad identification scheme for first-level protection. The goal is to stop the attacker from accessing any level inside the network, not to fully exploit all inputs from outside the network.

The attack graph's edges and patches were used to generate the normalisation of the matrix, which can be an effective way to lessen the uncertainty in the graph. Therefore, we can safeguard the network from any type of compromise scenario with the aid of the security matrix. To increase security and reduce costs, corrective actions can be identified and rated based on risk.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

3.2 The Model's General Scenario

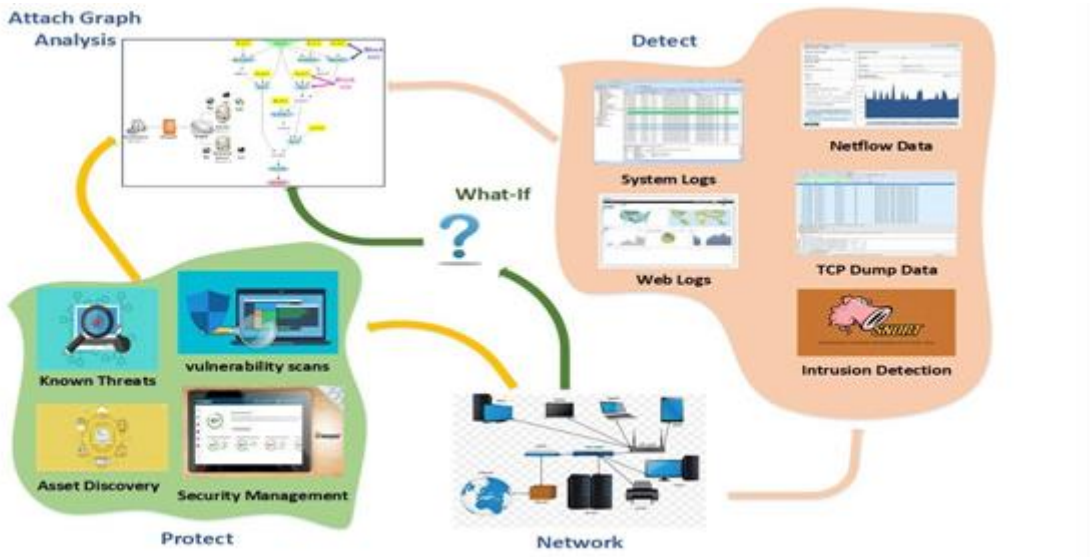


Figure 5: The Model's General Scenario

Attack graphs can locate weaknesses, show their paths, and safeguard the best solutions needed for a certain vital network that is attackable. The best choices for network protection are made with the aid of these attack graphs. However, the remaining patches in the attack graph must be identified in order to find the vulnerabilities and patch the necessary path. This topology-based vulnerability assessment's information enables us to take the necessary proactive steps to protect the forces against potential attacks on a compromised path. Figure 5 depicts the model's overall situation.

3.2.1: Making of the Adjacency Matrix

Depending on the relationship between the Intrusion Alarm: and the assault graph, specific start and endpoints can be used to generate the graph. The network security settings or the attacker exploit may make up the graph's vertices, which can be combined into a single matrix.

The suggested approach is capable of handling all circumstances in which either intrusion alarms or attacker exploits are in charge of handling the problem. The total number of applied vertices for a fully linked graph, as defined by graph theory, is 100 X 100 if we simply take

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

into account a network made up of around 100 machines. However, managing and handling all potential edges when creating this attack graph will not be viable. Therefore, in general, the matrix is 100 square matrixes long.

In general, the adjacency matrix for a network with n machines will contain n X n values. To keep things simple, if we consider that A is a matrix made up of all of the edges that connect our text nodes I and j, then the element aij stands for the matrix element that connects the two nodes. In order to reduce the size of the resulting matrix, we can either represent all of the edges with a value of 1 and all other values with no link or edge with 0. Adjacency lists, a different kind of data structure, are in charge of this and are highly helpful. The only straightforward explanation for this is that, as opposed to controlling an entire matrix with n X n entries, the list contains all edges and vertices that have connections.

3.2.2 Homogenous Groups Clustering Algorithm

The computers that the vertices represent belong to the same subnet or required scheme. For the purpose of creating the attack graphs and matrices, the terminology is dependent on the individual perspective. In general, it is independent of the arrangement of the rows and columns, but when discussing clusters as a whole, it makes sense. As a result, it is necessary to use a clustering algorithm for this square matrix, similar to the one suggested by (C.Ma et al., 2021). The matrix and high and loose density clusters can both be detected by the clustering technique. Information-theoretic optimality can be found where the clusters are concentrated. Data compression is possible for the clusters under consideration in accordance with the minimum description length principle of (Hu et al., 2020). The notion of the collected regularities can also be used to illustrate this fact as the data compression is well established.

In general, the concept centres on the phenomena of clustering in the matrix for a sizable number of network nodes. We can safeguard the cluster density and the intervention probability once the minimal description length has been determined.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

3.2.3 Identification of Multi-Step Attack Paths

We shown in the previous section how the formation of the matrix might be based on the various nodes existing in the network. The assault graph is translated into a square, sorted matrix. All the edges of the connected network attack graphs are represented by the adjacency matrix that can be constructed. Assuming that matrix A is built in square order, all potential edges between network ports will be present. There are n x n possibilities that can be raised for a square matrix with n components, where we can suppose that its value will be A A A.....A (P times). Equation number is one way to numerically describe this (1).

Ap is equal to A. A. A. A. Ap (1)

Let's consider the matrix raised to the power of two, which can be written as (A2)i = k aik akj (2)

All of the matching rows and columns in the matrix multiplication will map to a specific matching step in the attack graph, as shown in the second equation.

This kind of submission can be carried out with the aid of matching steps, and it results in the discovery of the fact that each matrix element, obtained by multiplying the matrix A, will assist us in identifying the elements, responsible for a two-step attack between various bears as well as corresponding row and column of the attack graph matrix. We will find the components of the three-step approach by identifying A3. As a result, the intersection of a I X j) value will consist of all the elements after multiplication. It can be condensed to say that the elements of the n-step attack graph can be found by multiplying the adjacency matrix by the power n. Any arbitrary power will be produced by the same T multiplication for the matrix after spectral decomposition. The eigenvalue equation should be satisfied by an eigenvalue in any square matrix of order n X n: AV = VD

A=VDV^ (-1) (3)

In this equation, D represents the diagonal matrix. The eigenvectors V, corresponding to matrix A, can be calculated with the values of the elements available in the matrix. It is really simple and

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

effective to prove that $Ap = VDpV -1$

As a result, identifying the diagonal matrix for the pth power of matrix A will be very simple.

$A \vee A2 \vee A3 \vee \ldots . An-1$ (5)

3.2.4 Identification of the Detected Intrusions

In the two parts before this one, we discussed the methods used to produce a potential attack graph and established the mathematical basis for the adjacency matrix. We can now pinpoint the areas that are most susceptible to attacks.

This section will attempt to compile all the options and pinpoint the best location for sensors to detect entry using attack graphs.

Regardless of worldwide sharing, it has gotten much harder to define the data and hardware borders since the development of cloud computing technologies. As a result, using sensor placements at all nodes to govern our wide area network becomes difficult or even impossible. The security software for the gadget is in fact incomplete. Even the most advanced software occasionally misses remote threats and weaknesses. Therefore, it becomes difficult to defend the entire network as well as any equipment situated there. Finding malicious behaviour and attacks on important data and data centres drives many enterprises nuts. Sometimes the business finds it challenging to manage the hosted information due to network traffic and intrusion detection at higher rates with false alarm systems.

However, the impact of the attacks can be significantly lessened with the aid of vulnerability assessment. To locate the computer in the network and report its vulnerabilities, numerous conventional tools were previously employed. However, doing this requires a lot of labour and is particularly prone to mistakes. While every computer is connected and every computer is checked for potential vulnerabilities. The key thesis of this study is that rather than securing all assets, they prefer to concentrate on the network's susceptibility. The network's assets that are not evaluated critically can be disregarded.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

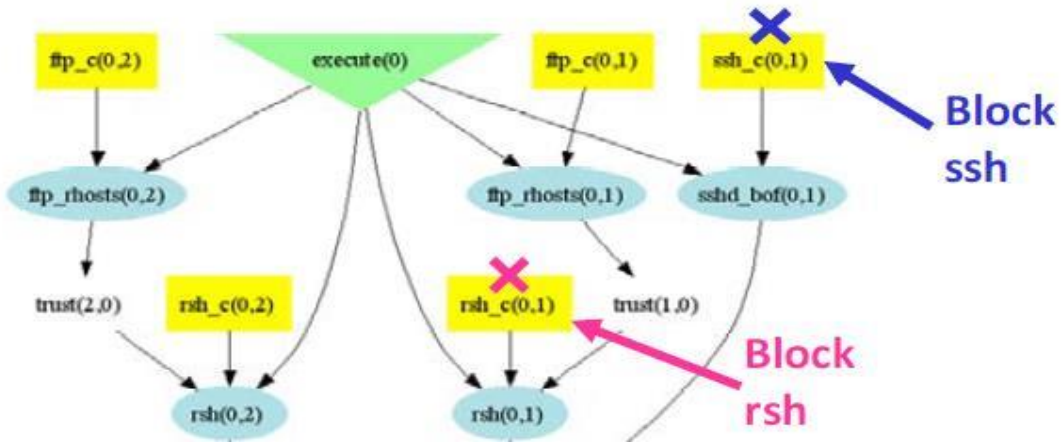
In order to understand the exploitation of the attacker, the study makes an effort to build a model of the complete network, including the topology and connectivity between various devices.

The model suggested in this paper can be used to simulate attacks, and it will be feasible to forecast attack vectors when various assets are compromised, which is highly important at any moment.

The study's main goal is to discover all potential assault vectors that are weak points and strengthen them. The main idea of the study is to automate the outdated and conventionally available solutions for network security. With the use of the analysis suggested in this study, the network can be strengthened. It makes it incredibly simple to find every vulnerability and safeguard the entire network.

Section 3: Attack Graph from the Network

The attack graphs developed for this study enable the identification of all the weak points that can be utilised to harden the network by installing sensors where they are needed. These places could shift and vary from network to network. With the use of several vulnerability scanner tools, vulnerability assessments can be created. However, a variety of computer vulnerability scoring tools must be used in order to generate the adjacency matrix and do the mathematical calculation.



Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Figure 6: Attack Graph from the Network

Figure 6 shows a network attack graph, and the ssh service from computers 0 and terminal1 is represented by ssh c (0, 1).

The number computer is incredibly susceptible to ssh attacks, and the edge symbolises communication between 0 and 1. It's also important to note that rsh c (0,

1) depicts the service that is being spread across the Sample network from the same computer. The rsh services need to be verified because they are also prone to exploitation. The diagram's two variation blocks need to be examined, and the sensor placement can be done at the computer's (0, 1) path. The goal of the study is to identify all such paths that are in charge of protecting the network. The attack graph shown is a single-step vulnerability analysis. The above-discussed m-Step vulnerability assessment, however, can use a similar strategy.

The study, which is centred on this research, contributes to the creation of a very solid mechanism that may help manage any potential network vulnerabilities. It will be extremely beneficial for minimising exploitation and protecting the network from unauthorised access.

4. Results and Discussion

The article proposes a novel methodology for multiple step attack graph visualisation and forecasting in any network. Vulnerability scanners installed on network hosts, along with the firewall and the exploitable software codes of the attacker, can be used to find and deal with software flaws. It is also possible to construct a sophisticated attack graph for M-step prediction. as a means of locating weaknesses in the topology. The demonstrated network's exploited services and vulnerabilities are displayed in Tab. 1.

Table 1 lists the vulnerable services and exploited services in the demonstration network.

Host	Services	Vulnerabilities	OS
Host1	WuFTPD, SSH, RSH	sshd buffer overflow, ftp.rhost overwrite	Linux
Host2	ProFTPD,RSH,XTE	ftp.rhost overwrite, local xterm buffer	Linux

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

The research conducted in this article covers all conceivable ways that online vulnerabilities may be found and that an attacker might attempt to identify every possible route into a network. The demonstration model may not, however, be able to validate all the results. To minimise all potential dangers and attacks, a comprehensive, in-depth analysis is necessary. The cross-mapping between the machines in the illustrative network is displayed in Tab. 2.

Table 2 shows how the machines in the demonstrative network are cross-mapped.

Relation	Host0	Host1	Host2
Host0	Localhost	FTP, SSH	FTP
Host1	Any	Localhost	FTP
Host2	any	FTP	Localhost

With the help of the attack graphs in Fig. 6, it is possible to discover all the weak points in the network and harden it by installing sensors where they are needed. These places could shift and vary from network to networkIt is safe to presume that the problem is NP-Hard. In relation to the set cover problem, we can mimic a similar issue. And instead of calculating all of the vulnerabilities at all of the paths, which could take more time and necessitate the incorporation of extra hardware in the form of sensors, we instead use the greedy technique in this situation to choose the best network path. The study's identified attack paths demonstrate the following issues, and sensor placement can be done depending on the paths seen the examination and identification of several crucial services active on host computers. Services should be prioritised over hosts to prevent the attacks depicted in Figure 7 and Path depth traversal should be increased to address the vulnerability depicted in Figure 8.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

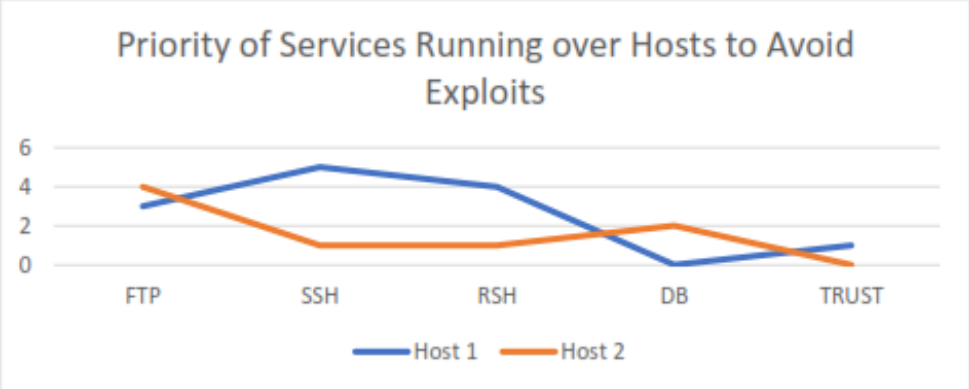


Figure 7: Critical Processes with Priorities

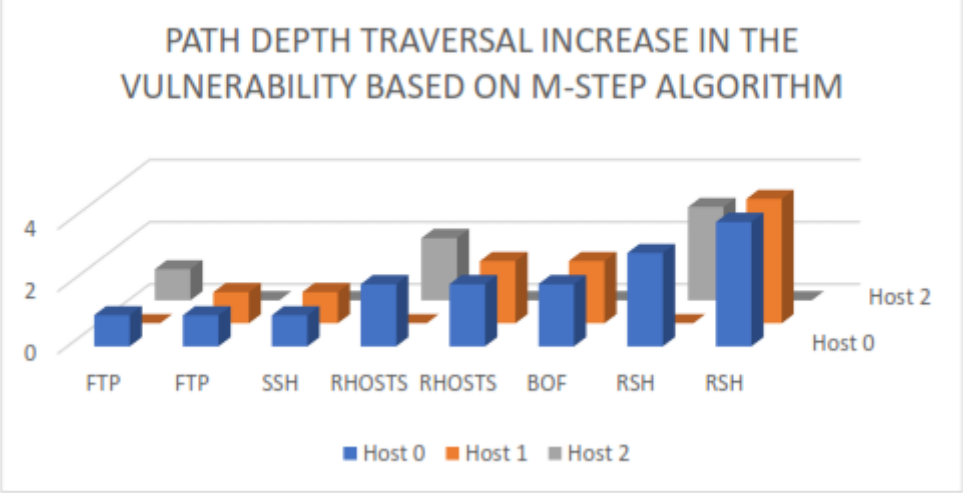


Figure 8 shows the graph's traversal depth.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

5. Conclusion

The approach described in this article is a model that includes the network as a component of the attack graph, which also includes other sorts of services-unrelated vulnerabilities. The computing devices can be guarded with the aid of installing specific sensors after identifying all the services in this respect, and the system can be thought of as having better security against the exploit. The suggested approach visualises and forecasts sophisticated multi-stage cyberattacks. Adjacency matrices and conventional graph-centric modelling are employed. With the use of this methodology, network vulnerabilities can be predicted. The main study combines the crucial idea that an attacker will always target a website with lots of exploitation-ready vulnerabilities. This strategy is maintained with an improved form of network hardening, which identifies the potential targets of exploitation and applies prediction parameters that incorporate some sensor-based research. To best secure the network, it makes correlation and prediction relatively simple. The attack graphs can be made and examined to determine where to install vulnerability assessment tools in the future. However, with the aid of resources and potent computing devices, the geographical assessment can be carried out. In this research, a model was provided that enables a thorough vulnerability analysis depending on the topology of the network. The development of the assault graph makes it simple to recognise the research spots and grey areas. As a result, using M-steps analysis to manage the network and assure cybersecurity is advantageous.

References

1. Mishra. S., Sharma. S.K. and Alowaidi. M.A. (2021). Multilayer self-defense system to protect enterprise cloud," CMC-Computer Materials & Continua, vol. 66, no. 1, pp. 71-85.
2. Gupta. R., Tanwar. S., Tyagi. S., and Kumar. N. (2020). Machine learning models for secure data analytics: a taxonomy and threat model," Computer Communications, vol. 153, pp. 406-440.
3. Mishra. S., Sharma. S.K., and Alowaidi. M.A. (2020). Analysis of security issues of cloud-base. web applications,". Journal of Ambient Intelligence and Humanized Computing, pp.1-12.
4. Mishra. S., and Alowaidi. M.A., Sharma. S.K. (2021). Impact of security standards and policies on the credibility of e-government,". Journal of Ambient Intelligence and Humanized Computing, pp.1-12.
5. Sarker. I.H., Abushark. Y.B., Alsolami. F. and Khan. A.I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model," Symmetry, vol.12, no.5, pp.1-15.
6. Mishra. S. (2020). SDN-based secure architecture for IoT," International Journal of Knowledge and Systems Science (IJKSS), vol.11, no,4, pp. 1-16.
7. Aldweesh. A., Derhab. A., and Emam. A.Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Systems, vol.189, pp.1-19.
8. Husak. M., Komarkova. J., Harb. E. B., and Celeda. P. (2018). Survey of attack projection, prediction, and forecasting in cyber security," IEEE Communications Surveys & Tutorials, vol.21, no.1, pp.640-660.
9. Liu. J., Lu. H., Wang. M. Chen J., and Zhang. Y. (2020). Macro perspective research on transportation safety: an empirical analysis of network characteristics and vulnerability," Sustainability, vol.12,no.15, pp.1-17.
10. Ghadi. M., Sali. A., Szalay. Z., and Torok. A. (2020). A new methodology for analyzing vehicle network topologies for critical hacking," Journal of Ambient Intelligence and Humanized Computing, pp.1-12.

11. Liu. S., Yu. Y., Hu. W., Peng. Y. and Yang. X. (2020). Intelligent vulnerability analysis for connectivity and critical-area integrity in IoV." IEEE Access, vol.8, pp.114239-114248.
12. Lallie. H.S., Debattista. K. and Bal. J., (2020). "A review of attack graph and attack tree visual syntax in cyber security," Computer Science Review, vol.35, pp.1-41.
13. Pirani. M., Taylor. J.A. and Sinopoli. B. (2021). "Strategic sensor placement on graphs," Systems & Control Letters, vol.148, pp.1-8.
14. Cinque. M., Della. C. and Pecchia. A. (2020). "Contextual filtering and prioritization of computer application logs for security situational awareness," Future Generation Computer Systems, vol.111, pp.668-680.
15. Stergiopoulos. G., Dedousi. P. and Gritzalis. D. (2021). "Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0," International Journal of Information Security, pp.1-23.
16. Pourhabibi. T., Ong. K.L., Kam. B.H. and Boo. Y.L. (2020). "Fraud detection: a systematic literature review of graph-based anomaly detection approaches," Decision Support Systems, vol.133, pp.1-15.
17. Ibrahim. M., Qays. A., Elhafiz. R., Alsheikh. A. and Alquq. O. (2020). "Attack graph implementation and visualization for cyber physical systems,"Processes vol.8, no. 1 ,pp.12.
18. Sansavini. F. and Parigi. V. (2020). "Continuous variables graph states shaped as complex networks: optimization and manipulation," Entropy, vol.22, no.1, pp.1-14.
19. Hu. Z., Feiping. N., Chang. W., Shuzheng. H., Wang. R., Xuelong. L. et al.,(2020). "Multi-view spectral clustering via sparse graph learning," Neurocomputing, vol.384, pp.1-10.
20. Liu. L., Luo. S., Guo. F. and Tan. S. (2020). "Multi-point shortest path planning based on an improved discrete bat algorithm," Applied Soft Computing, vol. 95, pp.1-10.
21. Chen. L., Yue. D., Dou. C., Chen. J. and Cheng .Z. (2020). "Study on attack paths of cyber-attack in cyber-physical power systems, IET Generation, Transmission & Distribution, vol.14, no.12, pp.2352-2360.