Individual assignment

Having a strong web presence is not only important in today's world, it is vital for survival in today's super connected world. Companies, banks, agencies and private industries must be able to create an environment to interact with customers, government officials and other companies in order to thrive. Opening yourself up to anyone through the Internet often means opening your system up to the world.

Today we are more connected than ever, and cyberspace is littered with a multitude of individuals, some with the intent to compromise network infallibility, integrity and availability. Anyone with a computer and Internet access can become a victim or criminal over the web. As a result, networks and servers are under constant attack these days. Attackers are changing their techniques daily and are on a never ended endeavor to disrupt companies for their selfish reasons. Two such forms of disruption are Denial of Service (DOS) and Distributed Denial of Service (Dos) attacks.

These forms of disruption have cost companies millions of dollars and are showing no signs of stopping. That is why it is up to security professionals to create the best safeguards and impose efficient and proper techniques to prevent, mitigate and discover these attacks before they inflict terrible harm. In the following assignment, these important topics of prevention, mitigation and discovery will be discussed as they relate to DOS and DOS attacks on today's systems. Specifically, three academic journals have been selected that relate to this topic.

This essay will first briefly summarize each article that was selected and state the methods of prevention, mitigation or discovery as they relate to

denial of service attacks. The second part of this essay ill explore in detail the specific methods discussed in the summaries as they relate to a proposed technique and practical approach, which can be implemented, into a platform. The strengths and weaknesses of each method that is selected will also be discussed within the summary. Brief Overview In order to better understand the reasons for discovering, mitigating and preventing these attacks, it is necessary to first review what exactly Denial of Service and Distributed Denial of Service attacks are and why these specific journal articles were selected for this assignment. DOS and Dos attacks re extremely popular cyber attacks launched by attackers because of their effectiveness and ease. The goal of a DOS attack is for the attacker to render certain specific resources of the victims' computer or server unusable or make them unavailable.

The attacker does this by sending large amounts of traffic that appear to be legitimate request to the victim. As a result, the victim's computer or server is tangled up and that particular resource cannot be used. These attacks expose a significant loophole not just in certain applications, but loopholes in the TCP/IP suite (Josh & Miser, 2010). A DOS attack only occurs when a resource on a computer or network is slowed down or stopped completely by an individual maliciously. A Dos attack is very similar to a DOS attack.

However, this form of attack is launched on multiple computers or devices in an organized manner. The goal, once again, is to attack a specific target or multiple computers and servers and make them unavailable for use. The first ever reported DOS attack occurred at a University in 1999. From then on, these attacks have become increasingly more complex and sophisticated.

Their widespread effect as ranged from simply slower speeds on websites, to financial institutions losing millions for not being accessible to customers.

The journal article “ Dos Prevention Techniques” was chosen because it does a fantastic job of explaining the differences between the two attacks, multiple Dos tools that attackers use, and lastly ways to prevent and defend against the attacks. The second article selected is titled “ Prevention of Attacks under Dos Using Target Customer Behavior. ” I selected this article because it not only gives an overview of this form of attack but also a specific method of protecting a potential server by locking DOS attacks with behavior based actions.

The last article chose “ A Novel Technique for Detection and Prevention of Dos” also gives a brief overview of the attack as well as a specific method to help filter Dos attacks on online banking websites. 3 Article One The article “ Dos Prevention Techniques” mainly centered around Dos attack and the methods of preventing them as well as the tools that criminals use to execute these attacks. One example of a tool that these individuals use is Triton, which can be used to, “ launch a coordinated UDP flooding attack against target yester” (Josh & Miser, 2010).

Another tool that Josh & Miser discussed was Trinity. This Dos attack tool is IIRC based and uses flooding methods of the TCP SYNC, TCP REST, TCP SACK request. This tool not only can flood the TCP/IP but also flood the UDP and IP Fragment. This article offers various forms of preventative methods against Dos attacks. They separated them into two groups: General Techniques and Filtering Techniques. Since the article gave a plethora of examples of general

techniques I will discuss two of them as well as the advantages and disadvantages to these practical approaches.

One method of preventing against Dos attacks is “ disabling unused services. ” Attackers can’t take advantage of something if it is not available to them. So, the fewer applications and open ports that are on a given host, the less likely an attacker can manipulate any vulnerability on that host. Therefore, if a network application is unnecessary it should be disabled or closed immediately (Josh & Miser, 2010). The advantage of this approach is that it minimizes the attack surface, thus protecting the host from receiving certain request from ports that can be used to flood the system.

The disadvantage to this approach is that you limit the amount of applications you may need to help run your organization more efficiently. Another method of preventing these attacks is by using a firewall. A firewall can help mitigate against simple Dos attacks by using simple rules such as implicit deny, or deny any for certain ports and IP addresses. However, the disadvantage of using a firewall to mitigate attacks occurs when sophisticated attacks are launched on ports such as Port 80 used for web traffic.

A firewall, cannot tell the difference between legitimate traffic and malicious traffic that comes through he port (Josh & Miser, 2010). This can lead to an attack still being carried out if the firewall cannot decide what is good and bad traffic. One filtering technique that was discussed in the journal article was the technique of “ History Based IP Filtering. ” During normal function, traffic seems to stay balanced and stable. Yet, during most DOS attacks they

are carried out with IP addresses that have never been seen before on the network to flood the system.

This form of filtration relies on an IP Address Database (DAD) to store the IP addresses that are used frequently. If an attack is launched and the source address does not match any in the DAD the request is dropped. The advantage to this form of protection against DOS attacks is that it will keep unknown IP address from ever reaching the host. However, the draw back is that it will not keep out legitimate or real IP address that are already in the database. Also, " Cost of storage and information sharing is very high" Shoos & Miser, 2010).

So if cost is an issue for an organization, this method may not be best. These methods can be implemented fairly easy for any organization. Most security professionals should already have these measures n place such as firewalls and minimizing the attack surface with an emphasis on disabling unnecessary services. History based IP filtering is a costly alternative to those methods but can be an additional form of security. 4 Article Two The second article that will be discussed is titled, " Prevention of Attacks under Dos Using Target Customer Behavior. This article discusses a method using an algorithm to determine if request to a specific server should be blocked or allowed in real time to mitigate the attack. The algorithm is used to maintain a list of users and to stop attacks from unknown users. The purpose of this tool is to prevent only authorized clients onto the server. This method accomplishes this by first determining which category the requesting client should be registered or non-registered. The tool uses an anomaly-based

system during peak times to help determine if certain requests are deemed malicious or not.

A client will deemed malicious if the client sends repeated request during peak hours and deemed an anomaly client, or possible attacking client (Suppurates & Militia, 2012). This tool can track which request made on the server are authorized or unauthorized. Once the request is deemed unauthorized, the client is then placed in a group of non-registered users and blocked temporarily until the peak time is finished. This proposed method also features a count system for the amount of request a client may attempt, which are “ Access Count” and ‘ Warning Counts. The article explains this in depth by stating, ‘ The access count is the count that can be incremented every time the client sends the request. The Warning Count is the count that can be incremented once the unregistered client sends anomalous request” (Suppurates & Militia, 2012). This mount system helps to determine if the request are legitimate and if so are only temporally blocked during peak times in order to keep systems running and not flooded with request. This feature also presents a permanent block alternative as well. This occurs once the warning count reaches it’s threshold (Suppurates & Militia, 2012).

This can be extremely useful when defending against Dos attacks because it works in real time. The chart below illustrates how this method is carried out for all users trying to request information from the server. This tool could easily be implemented for any organization looking to defend heir systems as well as monitor customer and client user data. The only disadvantage that may occur while implementing this will be the temporarily lockout

mechanism that legitimate users may encounter if they enter too many incorrect requests.

Inconvenience for some users is the only drawback. However, this approach is extremely promising because it does not completely block IP addresses like some filtration systems. They are placed in a certain unauthorized category away from authorized clients and systems. And once they meet certain requirements their request may be authorized if they do not go over the warning mount. Also as an added security feature if the client goes over the warning number of request and is also unauthorized they are blocked completely. Article Three The final article that will be discussed is titled “ A Novel Technique for Detection and Prevention of Dos. ” This article was dedicated around a specific method for detecting and preventing DOS attacks. This method focused on using the Hidden Markova Model. Very similar to the previous method in being an anomaly based system that uses request behavior to block or authorize users. This method also uses an algorithm to track user behavior and determine whether he requests are legitimate or an attack. However uses a different form of authorizing request before allowing access into the system.