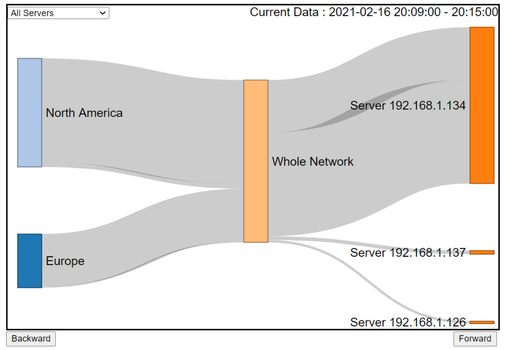
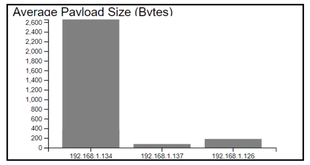
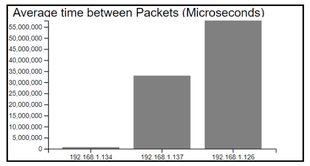
Situational Awareness of Security Incidents for Network Administrators

Introduction

Network intrusion has been a constantly growing problem in the world of computer administration over the last three decades. Each year brings new, more complicated attacks. These can range from advanced, well planned heists to simple annoyances caused by script-kiddies. This has resulted in the need for network administrators to have fast and accurate awareness of the data in their networks and where it has come from. As humans are innately visual beings, this needs to be done through a form of visualisation.

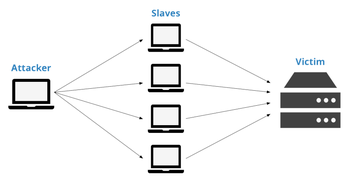






Awareness of the Incident

The security incident chosen is a Distributed Denial of Service (DDoS) attack. This is due to the frequency the attack occurs, with an estimated 12,000 instances over a 3 week period in 2001 [3]. An easy way to visualise this attack is with the image shown below [4]. Too many letters are trying to fit into the letterbox, resulting in a blockage. No letters can make it through. Translating this into the world of computing, the letters represent connection requests and the letterbox represents the server being attacked. The sheer number of connection requests result in the exhaustion of server resources. The server is then unable to process any new requests.



In order to diagnose and stop a DDoS attack, administrators need to be aware one is happening. This is known as situational awareness. To make an administrator aware: the number of packets, how big those packets are and how frequently they are sent would need to be presented. To be able to stop an attack, the administrator would also need to know where said attack is coming from.

Author: Edward Linton

dwl18qgz@bangor.ac.uk

Supervisor: Dr. Cameron Gray

c.gray@bangor.ac.uk

PRIFYSGOL BANGOR UNIVERSITY

[1] J. Bertin, 'Semiology of graphics: Diagrams,' Networks, Maps, vol. 10, no. 00690805.1987, p. 10 438 353, 1983.

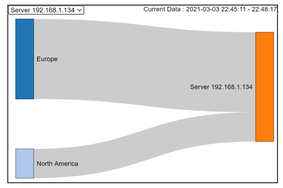
[2] C. K. Morewedge and D. Kahneman, 'Associative processes in intuitive judgment,' Trends in cognitive sciences, vol. 14, no. 10, pp. 435–440, 2010

[3] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker and S. Savage, 'Inferring internet denial-of-service activity,' ACM Transactions on Computer Systems (TOCS), vol. 24, no. 2, pp. 115–139, 2006

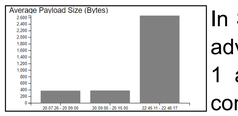
[4] Commissioned work from Christina Linton (@_tinaartwork_)

The Proposed Solution

The Proposed solution uses Wireshark to capture packet data flowing on a network. It then processes this in a Python backend and displays it using the JavaScript framework D3. A data flow diagram called a Sankey Diagram is used to show how many packets are being sent from each continent to each server. This allows the administrator to cut off a continent if the activity is suspicious. The average packet size and average time between packets are shown as bar graphs. The user can decide whether to view data for the whole network, or single servers. Previous data captures can also be displayed. The forward and backward buttons provide this functionality for the Sankey diagram while the bars charts will display previous times when viewing a single server. This gives the user a chance to find any irregularities in that servers data flow.



Backward Forward



In Semiology of Graphics, Jacques Bertin explains the advantages of representing data visually [1]. The type 1 and 2 brain theory from Kahneman solidifies this concept [2] . A Sankey diagram utilises the type 1 brain and allows the administrator to make an instant decision. The bar charts back up that decision by offering more in depth analysis. The information provided by the previous captures then allow for even further analysis should the user wish.

Future Work

Moving forwards, automating of the backend would be beneficial. Running the script every x minutes would allow the administrators to just view the most up to date traffic.

If the project was taken onto a Masters, adding a detection system could be a good way to improve the situational awareness for the administrator. The program could alert the user when unusual data is detected, removing the need for the administrators to go searching for anomalies. This would allow them to solve the problem faster.