The continued and growing trend of the frequency and severity of network attacks[1] against corporations, private individuals in addition to countries has prompted the development of network attack detection tools. In order to defend against threats – security is not only required in a pre-emptive scenario, but also ex post facto; whereby the criminal/ civil act has been detected and the acquisition of evidence has begun in order to provide a conviction. This project and its scripted application have been created in response to these escalating movements towards network vulnerability enumeration and distributed denial of service attacks (DDoS).

There is a clear lack of network attack tool detection products for the Linux/ UNIX operating system, and therefore this project should also address this imbalance. Within society, the UNIX / Linux operating system makes up an extremely minute fraction of operating systems that are in use within the world of today. With the increasing amounts of attacks, there is also a lack of skilled experts within this area, and as such the frequency of which we detect and convict criminals will decrease. Another additional aspect of the project is that within the Linux community, development and maintenance of projects will cease, eventually resulting in deprecation months or years later after creation. This project has been designed to be highly backward compatible, thus time-proof.

---

[1] Freed, A. (2012) DDoS Attacks are Increasing in Frequency and Severity – Study. *SecurityBistro*, [blog] November 16th, 2012, Available at: http://www.securitybistro.com/blog/?p=3683 [Accessed: February 22nd, 2013].

All results retrieved by the scripted application are based around the semantics of language or symbolic notation[2]; rather than attempting to find related but not symbolically or semantically linked strings/ artefacts which have recently been created. This is a more inaccurate methodology when concerning in-vivo or recently in-vitro systems due to the processes within Linux which create and edit files. Therefore the scripted application instead directly relies on symbolically/ semantically related files which contain information related to the operation of the network attack tools specified by the user or by default.

Recently edited/ created files are still examined, except without the main premise that their identification be based around file time stamps, which are easily modifiable. The author has personally seen examples of system administrators who were able to edit files time stamps to make the files appear unchanged; even though MD5 hash comparisons of the files showed that their contents had inextricably changed [often done to whitewash omissions in coding]. Therefore, rather than identifying files/ artefacts which have been marked as created or modified, the basis of the local search is founded instead on the semantic/ symbolic link between the file or its content's and the network tool(s) specified as the search query.

---

[2] Programming - Variables
Cs.utah.edu (2008) *Programming - Variables*. [online] Available at: http://www.cs.utah.edu/~germain/PPS/Topics/variables.html [Accessed: 1 Mar 2013].

The scripted application is only as good as the investigator using it. Its use requires a competent capable individual, and its operation can be further customised through editing the symbolic word lists. These word lists are shipped with the program, and offer an internal way to customize the results seen. By using UNIX based text editors, these word lists can be customized and thus changed.

Present Linux digital attack tools: partially supported

Wireshark[i] is an example of a current investigative and possibly an offensive criminal security/ hacking tool[ii]. Wireshark is an example of a program that can be used to investigate network traffic and change their values on the fly, this allows an attacker to manipulate and change packets whilst they are being captured; thus, this can be used to perform man-in-the-middle, or spoofing attacks.

Nmap[iii] is another security auditing tool. Although it's main usage and intent for creation is investigative, the legal ramifications of its usage are often not so plausible – especially if written consent and authorization has not been secured from the required parties to be scanned[iv].

Metasploit[v] is a penetration testing and network auditing tool. It incorporates the use of network exploits, and allows the user to include custom made payloads into attacks. This is truly an offensive security tool, and as such it offers a vast array of aggressive methods in order for an attacker to gain access, or cause disruption to a local or remotely networked

system. The program comes in three different editions; respectively separated by an ascending pricing system.

tcpdump is a terminal based network port scanner/ analyser to be used with UNIX and Linux. This tool is best used to see the raw data that comes through the interface. (Certified Ethical Hacker, 2010) This program often comes bundled with many Linux operating systems, and therefore will often be a weapon of opportunity rather than by choice for the average potential attacker.

LOIC (Low Orbit Ion Cannon) is based on a fictional energy weapon concept whereby multiple units provide a high target diversions factor.[vi] Like the fictional weapon, many users are encouraged to use this product together in digital meetings termed 'operations'; their high attacker to target ratio's also allow the users to take down larger targets through working together as a collective. It has been the main tool used by hacktivist groups such as "Anonymous".

Other tools also supported include some of the following: Nessus, OpenVAS, AutoScan, UnicornScan, implementation6, netifera, scapy, zenmap, aircrack-ng, snort, John the Ripper, netcat, rkhunter, Argus2, portscan, pof, Nikto, DSniff, and KISMET.

Although not all tools are currently supported, strides are being made to include each tool into the focus. This scripted application works on symbolic notation, and thus keywords.

"On a UNIX system, everything is a file; if something is not a file, it is a process." (M. Garrels, 2006)[vii] As a Linux system is entirely based around text, whether stored as a string or an integer all values are held within files. If it is not a file, then as stated – it is a process (which often cannot be interrupted). Therefore from this small piece of information, the assumption is made, that the contents of a Linux/ UNIX hard drive may be enumerated very easily. Strings held within files are able to identify compromised systems or those which had been used for attack purposes, by dynamically searching through every file (ignoring all processes currently running), using specific search criteria, we are able to - similar to a search engine - return results based on a ratings value system using keywords. Search engines[viii] enumerate the results, looking for keywords and returning hits; the scripted application uses data mining[ix] to examine the hard drive, returning results based on keywords and provides them with a relevancy rating. This method of analysis also tests for false positives, allowing for incorrect results to be ignored; all keywords used by the scripted application can easily be edited by competent users.

The tool also dynamically generates visual statistical reports based on the results, and helps an investigator sift through the data whilst separating the important from the irrelevant. Its operation is simple, in some cases questionably so – but this is what it is, a tool to assist investigators in aggregating and elucidating key information from a big data set…

[i] Wireshark.org (2011) *Wireshark · Go deep.*. [online] Available at: http://www.wireshark.org/ [Accessed: 25 Oct 2012].

[ii] Wired.com (2012) *Watch Out, White Hats! European Union Moves to Criminalize 'Hacking Tools' | Threat Level | Wired.com*. [online] Available at: http://www.wired.com/threatlevel/2012/04/hacking-tools/ [Accessed: 25 Oct 2012].

[iii] Nmap.org (2009) *Nmap - Free Security Scanner For Network Exploration & Security Audits.*. [online] Available at: http://nmap.org/ [Accessed: 25 Oct 2012].

[iv] Nmap.org (1999) *Legal Issues*. [online] Available at: http://nmap.org/book/legal-issues.html [Accessed: 25 Oct 2012].

[v] Metasploit.com (2012) *Penetration Testing Software | Metasploit*. [online] Available at: http://www.metasploit.com/ [Accessed: 25 Oct 2012]

[vi] Command and Conquer Wiki (2013) *Ion cannon*. [online] Available at: http://cnc.wikia.com/wiki/Ion_cannon [Accessed: 10 Apr 2013].

[vii] Redhat.com (2006) *Introduction to Linux*. [online] Available at: http://www.redhat.com/mirrors/LDP/LDP/intro-linux/html/intro-linux.html [Accessed: 12 Feb 2013].

[viii] TheFreeDictionary.com (2000) *search engine*. [online] Available at: http://encyclopedia.thefreedictionary.com/search+engine [Accessed: 12 Feb 2013].

[ix] TheFreeDictionary.com (1999) *Data mining*. [online] Available at: http://encyclopedia.thefreedictionary.com/Data+mining [Accessed: 12 Feb 2013].