Botnet Detection and Perimeter Defence

Coursework Submission for CSN08703

Edinburgh Napier University 2018-2021 Trimester 2

Jenny S / 40417718 / April 2018

Table of Contents

Coursework Submission for CSN08703 1
Edinburgh Napier University 2018-2021 Trimester 2 1
Table of Contents 2
Research & Literature Review 2
Botnets 2
Intrusion Detection Systems 3
Bibliography 10

Research & Literature Review

Botnets

According to Norton, a botnet is a series of compromised computers infected with the same Malware. They can perform many repetitive tasks in response to a controller that they are connected to. The controller usually gives commands to the bot using the Internet Relay Chat protocol. Some botnets used in this way can be acting in accordance with the law and help keep the user content. *(Norton, 2016)* Infections are usually passed around the internet using Malware. Botnet software can be written to look for vulnerabilities on systems to exploit. Many botnets use a command and control (C&C) server that can send commands to all bots (infected devices) that are connected to it. *(Rouse, 2017)* The most common use of a botnet are Distributed Denial of Service (DDoS) attacks, where the C&C server sends a command to its bot to send many packets to the same IP address. This can cause the target device to exhaust its resources, overloading it and bringing the system down. DDoS attacks have been used to bring down large organisation's servers to cause a loss of service to its users. *(The Honeynet Project, 2008)*

Botnets have many strengths in that they are very difficult to identify bot traffic from normal user traffic. This means that when configuring Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), it is quite challenging to write rules that will prevent the botnet from infecting a device and acting maliciously. (Zaine, 2012) Many botnets also have a 'worm-like' infection feature, where as soon as they have infected a system, it then looks for any other IP to infect. This makes it very effective in spreading out across a network. *(Aussems, Noë and Rivera, 2018)*

However, from a strength, also comes a major weakness of using botnets. This comes from the fact that they usually rely on a C&C server to command the bots to direct attacks. If these C&C servers can be taken down, or IDS rules can be written to block traffic, the botnet can be unable to operate. *(Aussems, Noë and Rivera, 2018)*

Most recently, there has been a rise of botnets using Internet of Things (IoT) devices, such as the Mirai botnet. The Mirai botnet looks for many devices with open and insecure Telnet ports. Once a port is found, the bots try to login using a list of username and password combinations that are often used as defaults and not changed by the owner of the device. The botnet, after invading a device, looks for malware and removes it, claiming the device. The botnet can launch HTTP flood attacks against an IP address and was used to bring down large Minecraft Servers to direct activity to other servers. *(Fruhlinger, 2018)*

Following the success of the Mirai botnet, the future of botnets could be heading towards using IoT devices to direct attacks more than PCs, servers or other devices on the internet. When developing IoT devices, companies very rarely invest in security, instead opting to prioritise lowering consumer cost and ease of use. (Mcdermott, et al., 2018) It is therefore very important that IoT devices are kept in check and if another incident like the Mirai botnet occurs, we need to be able to defend against infected devices that threaten users on the Internet.

Intrusion Detection Systems

Intrusion Detection Systems (IDS) is software hosted on a device that looks for suspicious activity and threats in network traffic. It issues out alerts when it finds malicious traffic. Some IDS can identify patterns of traffic that are unusual to prevent DoS attacks. (Pratt, 2018) The two main types of IDS are Network-based IDS (NIDS) and Host-based IDS (HIDS). A NIDS may be deployed to inspect all incoming and outgoing packets on the network. Everything on the network is monitored, despite the operating system the communication originates from. A HIDS is deployed on a particular device and inspects all traffic incoming and outgoing on the machine. (Rouse, 2008) A HIDS will not detect as much as a NIDS, because they will not see all network traffic and do not inspect traffic in real time, therefore they can be seen as more effective than HIDS. However, HIDS are advantageous when detecting authorised used accessing or making changes to system files. (Rapid7, 2017)

Recently, extended versions of IDS, Intrusion Prevention Systems (IPS) have been used to both detect and act against malicious activity on a network. IDS often use Tap and Span ports to make a copy of network traffic, meaning that the performance of a network is not affected as it would be if all traffic was filtered as it passed through the IDS. Often, as a result of the speed that an attacker can exploit, IDS are rendered insufficient to defend a system on its own. (Cyberpedia, 2012) However, IDS are still good tools that are able to log intrusions on a network.

IDS have many strengths, for example, they can log the specific content of suspicious packets when they enter a network. This is useful for forensics after an intrusion is detected. They can also generate statistics about the types and volume of attacks, so that security can be adapted to defend against the most frequent types of attacks. However, IDS also have weaknesses, including the fact that IDS will not prevent attacks by themselves and only with the help of IPS. This means that it is often too late when an alert is raised, because malicious activity has already gained access to the network. IDS cannot view the contents of encrypted packets. This means that if an intruder is using a secure protocol, the IDS will not be able to detect an intrusion. False positive alerts (An alert has been raised when there was no intrusion) occur often and can cause network administrators to spend a lot of time dealing with false alerts instead of real threats to the network. (Rapid7, 2017), (Techotopia, 2016)

Some of the most used IDS products that are used industry include: SolarWinds, Snort, OSSEC, Suricata and Bro. All these systems offer a range of tools and some, like Snort are open source and free. Snort also has a large community that regularly updates databases of rules to defend against the most recent threats. (Cooper, 2019) This makes it very easy for anyone to defend their network against the most recent cyber threats.

Botnet Analysis

Static Analysis:

Possibly the most simple and obvious method of analysis is looking at the source code to reverse engineer the function of malware. The first step taken to discover the function of the botnet was to deobfuscate the source

code. Using the tool de4dot, the source code with the names of the commands that can be sent to the bot to run specific functionality (see figure x).

Dynamic Analysis:

To test the function of the botnet as it functioned, it is necessary to construct an isolated environment from which the bot can operate. A diagram of the network used is shown in figure 1.

Basic configuration and connectivity testing:

Each machine has been configured with an IP address, a default gateway, NAT and a DNS server it can access. All logins for VMs have been changed to secure the testbed of the botnet.

All VMs have connectivity with each other, tested with sending ICMP packets from each machine to every other machine. The firewall has been configured with an open stance. All traffic is allowed throughout the network. This is shown in figures 2, 3 and 4.

Botnet connections and traffic:

To observe the behaviour of the bot, the bot is run on the Windows machine on the private network (see figure 1). From the Kali Linux machine, netcat is used to connect to the Windows machine. From that, commands can be sent from Kali Linux to Windows to observe output from the botnet. This is illustrated in figures 5 and 6. As shown in the dynamic analysis, the commands that can be sent to the botnet are shown in figure x. Below is a summary of the functions of the commands investigated during the dynamic analysis of the botnet:

Hello:

Prints the message 'Welcome to the gang' to the console. This is illustrated in figure 6.

Test:

Outputs a series of hashes to the console, as shown in figure x:

Figure x: The output of the 'test' command.

These are encoded using MD5, SHA1 and SHA256 randomly. To decrypt each hash, the tool CrackStation was used.

Below are the hashes and their corresponding strings:

Hash	Plaintext	Hash type
bbccdf2efb33b52e6c9d0a14dd70b2d415fbea6e	the	SHA1
749ab2c0d06c42ae3b841b79e79875f02b3a042e43c92378cd28bd444c04d284	what	SHA256
557f255516719ea16f8f4a0aae1166054e2c9b43	not	SHA1
2bb3d86d95234affa7c5bd68c4bab606	they	MD5
4015e9ce43edfb0668ddaa973ebc7e87	are	MD5
beda14763de0969a064921bfd97d425e109d47e21dd6085bd86f2e89f91cfae6	owls	SHA256
bbccdf2efb33b52e6c9d0a14dd70b2d415fbea6e	the	SHA1
72f15b250fdd58ccfae958dace1213f71d6d41ad	seem	SHA1

Figure x: A table showing the output hashes from the test command. The hash, plaintext and hash type are all shown.

It is can be guessed with reasonable confidence that the message generated from the test command reads: 'the owls are not what they seem'. This is a tagline from a 1990s American television series, Twin Peaks. (Roquelaire, 2016), (O'Connor, 1990)

Failover:

Outputs 'that took a while' to the console, as shown below: ALSO USED BY THE BOT

Connect:

Returns a random URL to the console from a list of six possible outputs. These are: bbc.co.uk, apple.com, twitter.com, microsoft.com, ibm.com and hpe.com

Figure x: Some of the possible outputs by the connect command.

Takedown:

Outputs a random string of ciphertext from a pool of 3 possible outputs. This is shown below:

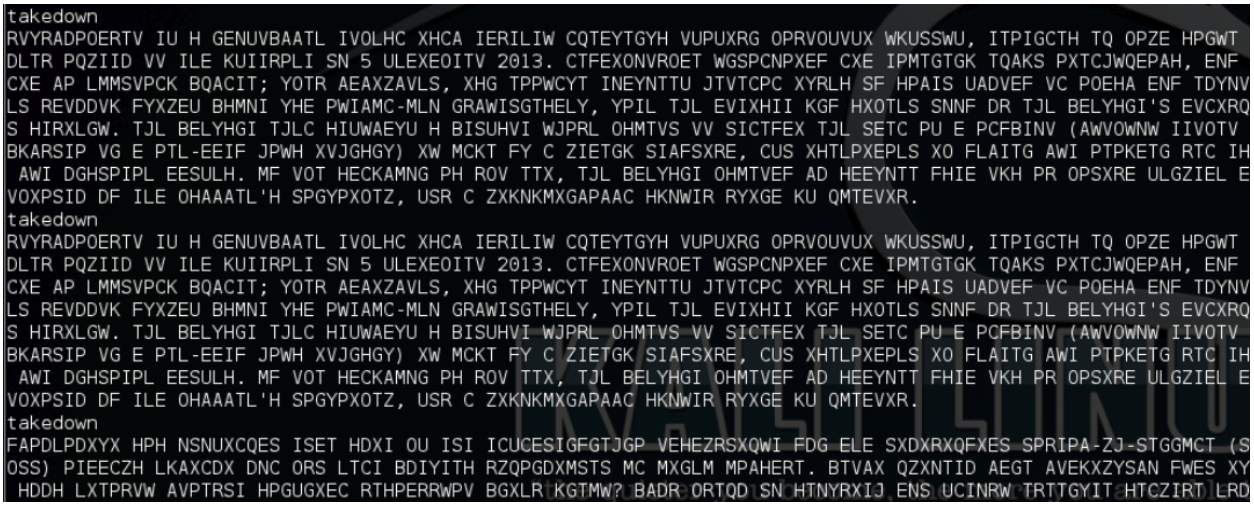


Figure x: The output of the 'takedown' command.

The outputs are shown in the table below:

Ciphertext:	Plaintext:	Key
HYEEK EFV TJU XMGEF UJ FRNFUQKRRR ? RSQBSPXISE RNTWCDWNXI OED RTGFPPGOSB IAAYSANAEK. PCTKFIVSVN EGRGFMJGVS JHBCW O WUYR-WQIERT QSJSNMI HYAG VVSMEAZW MFU SXSA RCPKWGZNT ESII PP UV TZLRY. MH JALY CCL HNBI HF PNE QCEEL (G VOESBS) XC XEG GGQVSF ZS MFUE VG OXAVT. IBTRLVXWFN EGRGFMJGVS THNTKSJ YBAV TZLRY WC POH IEB?K OCKR HYEZ. OX RFEF ZLWJ BL KRQIYCZMBX TUK JWCEF ? YIS KHR JIHRIYY JCI EAZIFGRVYIG JEPZMCE IS ESI?IE VTXSIEFZIR ZN GNI HVCUTSZFGVKW OED GKGVEIDAIG NE?IK WSVN. BRHSI VRXWWFNF UJ FRNFUQ IJUNRPM TLNOQ MFU UGZS UOAK WCDEGNMBX IYRIURL JOXV POHX TQ, RNQ ZLOK YBA EFV BRORU WIAKH PP A CUPWTE SUVQV OE MSJVRASIBK ATKRQP. TUKWS TLNOQG RRR LEZJE. VZ MG R SPGVS KAPZMQ UEFOKBVD GU QOBE LUY DRY GNI AFNRE AWKHBAX HVLYORU RNLURS NHB SMUYT OK EPCE GU VSJTBXI MFUE VG. BVWRX ZSISVURG VNPXCDK TUK JWCEF UR MFUE VG GF YBA GOE?T NIGSJS GNIA, RNQ ZLSE SVSTZP DRSEBU MBTIM KO EKWHFRR ESII FVRIG.	THERE ARE TWO TYPES OF RANSOMWARE ? LOCKSCREEN RANSOMWARE AND ENCRYPTION RANSOMWARE. LOCKSCREEN RANSOMWARE SHOWS A FULL-SCREEN MESSAGE THAT PREVENTS YOU FROM ACCESSING YOUR PC OR FILES. IT SAYS YOU HAVE TO PAY MONEY (A RANSOM) TO GET ACCESS TO YOUR PC AGAIN. ENCRYPTION RANSOMWARE CHANGES YOUR FILES SO YOU CAN?T OPEN THEM. IT DOES THIS BY ENCRYPTING THE FILES ? SEE THE DETAILS FOR ENTERPRISES SECTION IF YOU?RE INTERESTED IN THE TECHNOLOGIES AND TECHNIQUES WE?VE SEEN. OLDER VERSIONS OF RANSOM USUALLY CLAIM YOU HAVE DONE SOMETHING ILLEGAL WITH YOUR PC, AND THAT YOU ARE BEING FINED BY A POLICE FORCE OR GOVERNMENT AGENCY. THESE CLAIMS ARE FALSE. IT IS A SCARE TACTIC DESIGNED TO MAKE YOU PAY THE MONEY WITHOUT TELLING ANYONE WHO MIGHT BE ABLE TO RESTORE YOUR PC. NEWER VERSIONS ENCRYPT THE FILES ON YOUR PC SO YOU CAN?T ACCESS THEM, AND THEN SIMPLY DEMAND MONEY TO RESTORE YOUR FILES.	orange
FAPDLPDXYX HPH NSNUXCQES ISET HDXI OU ISI ICUCESIGFGTJGP VEHEZRSXQWI FDG ELE SXDXRXQFXES SPRIPA-ZJ-STGGMCT (SOSS) PIEECZH LKAXCDX DNC ORS LTCI BDIYITH RZQPGDXMSTS MC MXGLM MPAHERT. BTVAX QZXNTID AEGT AVEKXZYSAN FWES XY HDDH LXTPRVW AVPTRSI HPGUGXEC RTHPERRWPV BGXLR KGTMW? BADR ORTQD SN HTNYRXIJ ENS UCINRW TRTTGYIT HTCZIRT LRD WDDXICV AVOKXOIR DKS. QIGPT QAALLVE IPCKEIH TRTTGYIT DU ELICVD (MOI) SPZIRTD PIZT CSUITCW, DXVTXAA KTHED GPGOGSD (HVGH), LRD LTMGABH/DICJGTXY RPXIRPH, PRSAPGMNV KLWT CJXFEGH ZJ TWTDI DTKTGEH XYXO P QZXNTI, HLIRW TW TWTY YSTS ES CDCOYCI SOSS PIEECZH. QPAHWASICI SES RDYJIGBPH TWPE ET ATLWT HDXI OU ISI DTKTGEH JDID XC ELE SNY HNH PEXARZD ERT SGVS, UJCXHTG XETRWTRG IWP XERWYMCPA TRDXRLXOGH LRD IPNXIRH, EICWCTUUTH, LRD EGZGESJCIS PHDSCXPEID LXEL PGTGMOJH VROLC XMRPX MSTCTE ETIPNOS.	FLASHPOINT HAS CONFIRMED THAT SOME OF THE INFRASTRUCTURE RESPONSIBLE FOR THE DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS AGAINST DYN DNS WERE BOTNETS COMPROMISED BY MIRAI MALWARE. MIRAI BOTNETS WERE PREVIOUSLY USED IN DDOS ATTACKS AGAINST SECURITY RESEARCHER BRIAN KREBS? BLOG KREBS ON SECURITY AND FRENCH INTERNET SERVICE AND HOSTING PROVIDER OVH. MIRAI MALWARE TARGETS INTERNET OF THINGS (IOT) DEVICES LIKE ROUTERS, DIGITAL VIDEO RECORDS (DVRS), AND WEBCAMS/SECURITY CAMERAS, ENSLAVING VAST NUMBERS OF THESE DEVICES INTO A BOTNET, WHICH IS THEN USED TO CONDUCT DDOS ATTACKS. FLASHPOINT HAS CONFIRMED THAT AT LEAST SOME OF THE DEVICES USED IN THE DYN DNS ATTACKS ARE DVRS, FURTHER MATCHING THE TECHNICAL INDICATORS AND TACTICS, TECHNIQUES, AND PROCEDURES ASSOCIATED WITH PREVIOUS KNOWN MIRAI BOTNET ATTACKS.	apple
RVYRADPOERTV IU H GENUVBAATL IVOLHC XHCA IERILIW CQTEYTGYH VUPUXRG OPRVOUVUX WKUSSWU, ITPIGCTH TQ OPZE HPGWT DLTR PQZIID VV ILE KUIIRPLI SN 5 ULEXEOITV 2013. CTFEXONVROET WGSPCNPXEF CXE IPMTGTGK TQAKS PXTCJWQEPAH, ENF CXE AP LMMSVPCK BQACIT; YOTR AEAXZAVLS, XHG TPPWCYT INEYNTTU JTVTCPC XYRLH SF HPAIS UADVEF VC POEHA ENF TDYNVLS REVDDVK FYXZEU BHMNI YHE PWIAMC-MLN GRAWISGTHELY, YPIL TJL EVIXHII KGF HXOTLS SNNF DR TJL BELYHGI'S EVCXRQS HIRXLGW. TJL BELYHGI TJLC HIUWAEYU H BISUHVI WJPRL OHMTVS VV SICTFEX TJL SETC PU E PCFBINV (AWVOWNW IIVOTV BKARSIP VG E PTL-EEIF JPWH XVJGHGY) XW MCKT FY C ZIETGK SIAFSXRE, CUS XHTLPXEPLS XO FLAITG AWI PTPKETG RTC IH AWI DGHSPIPL EESULH. MF VOT HECKAMNG PH ROV TTX, TJL BELYHGI OHMTVEF AD HEEYNTT FHIE VKH PR OPSXRE ULGZIEL EVOXPSID DF ILE OHAAATL'H SPGYPXOTZ, USR C ZXKNKMXGAPAAC HKNWIR RYXGE KU QMTEVXR.	CRYPTOLOCKER IS A RANSOMWARE TROJAN THAT TARGETS COMPUTERS RUNNING MICROSOFT WINDOWS, BELIEVED TO HAVE FIRST BEEN POSTED TO THE INTERNET ON 5 SEPTEMBER 2013. CRYPTOLOCKER PROPAGATED VIA INFECTED EMAIL ATTACHMENTS, AND VIA AN EXISTING BOTNET; WHEN ACTIVATED, THE MALWARE ENCRYPTS CERTAIN TYPES OF FILES STORED ON LOCAL AND MOUNTED NETWORK DRIVES USING RSA PUBLIC-KEY CRYPTOGRAPHY, WITH THE PRIVATE KEY STORED ONLY ON THE MALWARE'S CONTROL SERVERS. THE MALWARE THEN DISPLAYS A MESSAGE WHICH OFFERS TO DECRYPT THE DATA IF A PAYMENT (THROUGH EITHER BITCOIN OR A PRE-PAID CASH VOUCHER) IS MADE BY A STATED DEADLINE, AND THREATENED TO DELETE THE PRIVATE KEY IF THE DEADLINE PASSES. IF THE DEADLINE IS NOT MET, THE MALWARE OFFERED TO DECRYPT DATA VIA AN ONLINE SERVICE PROVIDED BY THE MALWARE'S OPERATORS, FOR A SIGNIFICANTLY HIGHER PRICE IN BITCOIN.	peach

Figure x: The output and decrypted output of the 'takedown' command. The key used to decrypt the text is also shown.

These are encrypted using a Vigenère cipher with different keys every time. Some special characters are replaced with '?' in the first ciphertext. The plaintext are excerpts describing different malware and cyber-attacks: plaintext one is a short description about ransomware, plaintext two is an overview of the Mirai botnet and plaintext three shows information about the trojan Cryptolocker

Command	function
Hello	Prints "Welcome to the gang…" to the console
Test:	Prints a number of random strings
Failover:	
Connect:	
Takedown:	

Capture:	
Keepalive:	
Look:	
Code:	
Generate:	
Get:	
Snoop:	
Loop:	
Goodbye:	

A closed security stance has been used to lock down the network. The firewall rules used for this are shown below:

Bibliography

Aussems, E., Noë, B. & Rivera, N. R., 2014. *Botnets – A tenacious Web Technology.* [Online] Available at: http://mediatechnology.leiden.edu/images/uploads/docs/wt2014_botnets.pdf [Accessed 14 March 2019].

Cooper, S., 2019. *11 Top Intrusion Detection Systems & Tools for 2019.* [Online] Available at: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/ [Accessed 15 March 2019].

Cyberpedia, 2012. *What is an intrusion detection system?.* [Online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids [Accessed 14 March 2019].

Fruhlinger, J., 2018. *The Mirai botnet explained.* [Online] Available at: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [Accessed 13 March 2019].

Kaspersky, 2019. *What is a Botnet?.* [Online] Available at: https://www.kaspersky.co.uk

Mcdermott, C., Majdani, F. & Petrovski, A., 2018. *Botnet Detection in the Internet of Things using Deep Learning Approaches.* s.l., s.n.

Norton, 2016. *What is a Botnet?.* [Online] Available at: https://uk.norton.com/internetsecurity-malware-what-is-a-botnet.html [Accessed 3 March 2019].

Pratt, M. K., 2018. *What is an intrusion detection system?.* [Online] Available at: https://www.csoonline.com/article/3255632/what-is-an-intrusion-detection-system-how-an-ids-spots-threats.html [Accessed 14 March 2019].

Rapid7, 2017. *The Pros & Cons of Intrusion Detection Systems.* [Online] Available at: https://blog.rapid7.com/2017/01/11/the-pros-cons-of-intrusion-detection-systems/ [Accessed 15 March 2019].

Rouse, M., 2008. *HIDS/NIDS.* [Online] Available at: https://searchsecurity.techtarget.com/definition/HIDS-NIDS [Accessed 15 March 2019].

Rouse, M., 2017. *Botnet definition.* [Online] Available at: https://searchsecurity.techtarget.com/definition/botnet [Accessed 13 March 2019].

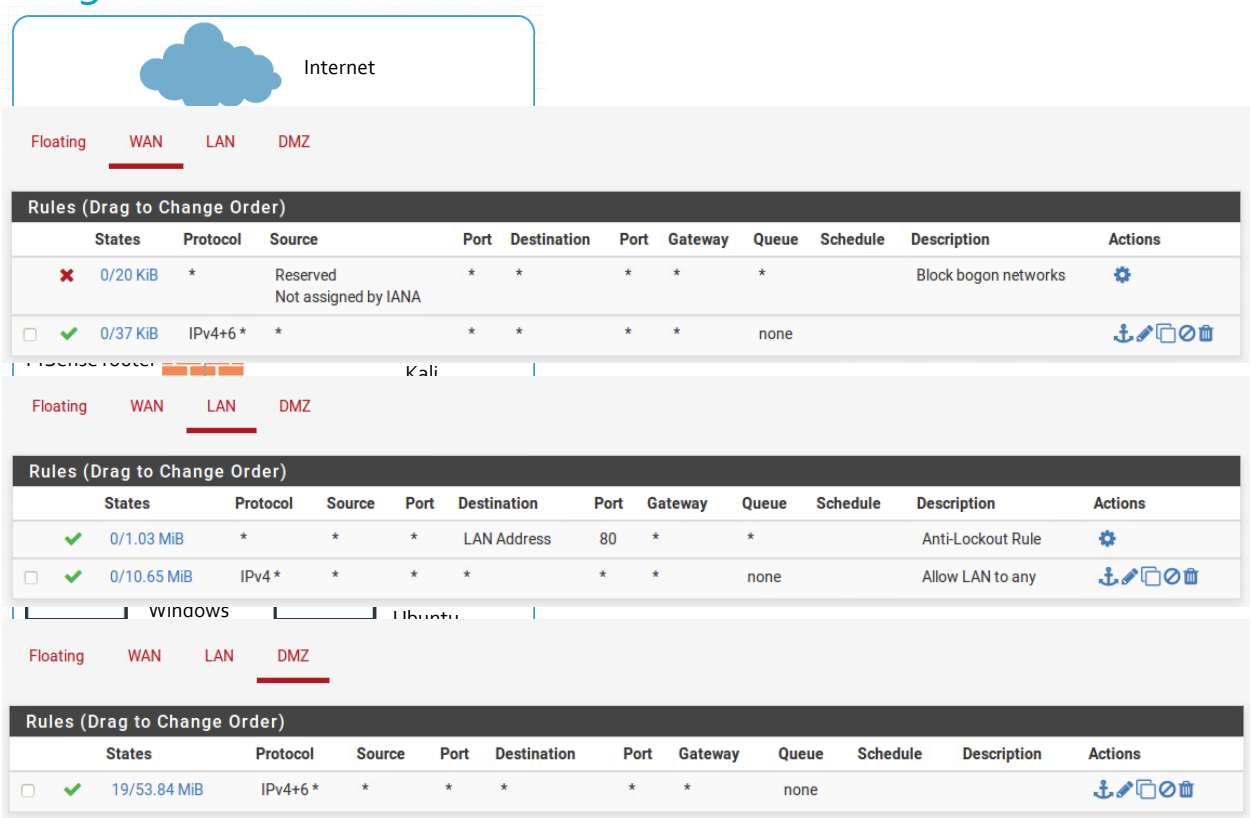
Techotopia, 2016. *Intrusion Detection Systems.* [Online] Available at: https://www.techotopia.com/index.php/Intrusion_Detection_Systems [Accessed 15 March 2019].

The Honeynet Project, 2008. *Uses of Botnets.* [Online] Available at: https://www.honeynet.org/node/52 [Accessed 13 March 2019].

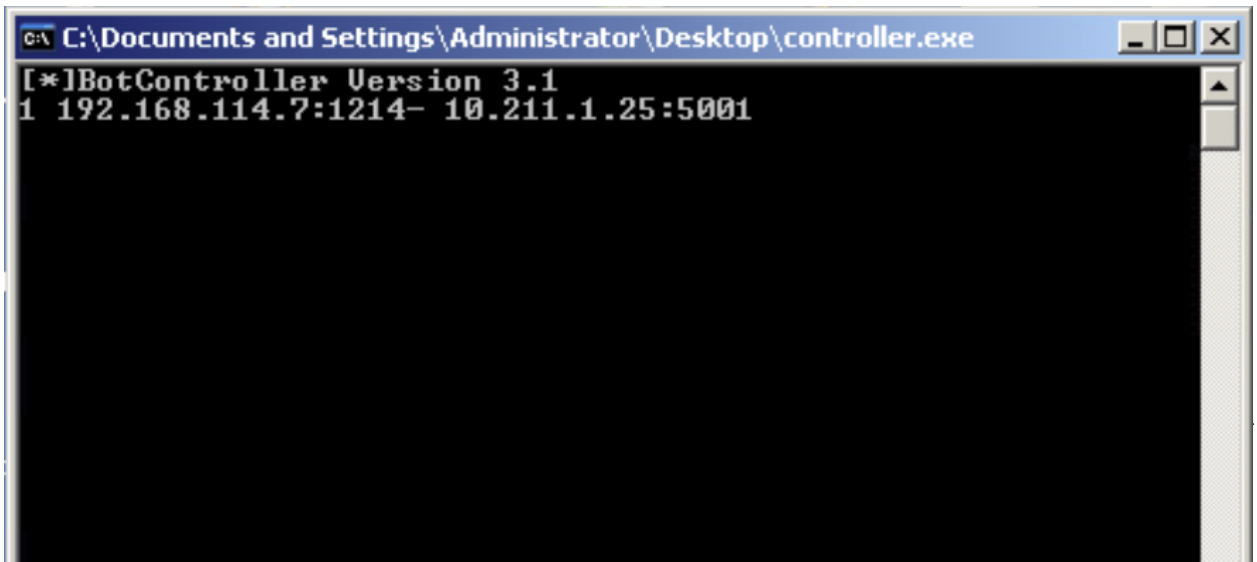
Zaine, B., 2012. *Intro to Botnets.* [Online] Available at: https://www.slideshare.net/ZIANEBilal/intro-to-botnets-bilal-ziane [Accessed 14 March 2019].

Appendix

Images and screenshots:



Figures 2, 3 & 4: pfSense firewall rules allowing all traffic through the network on all three interfaces.



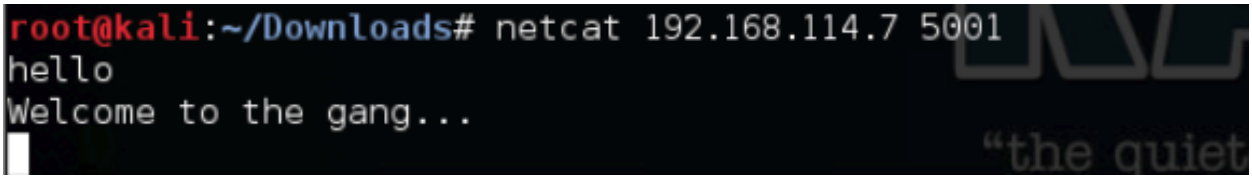


Figure 6: Using netcat, the Kali machine can connect to the Windows machine to send commands to the botnet.

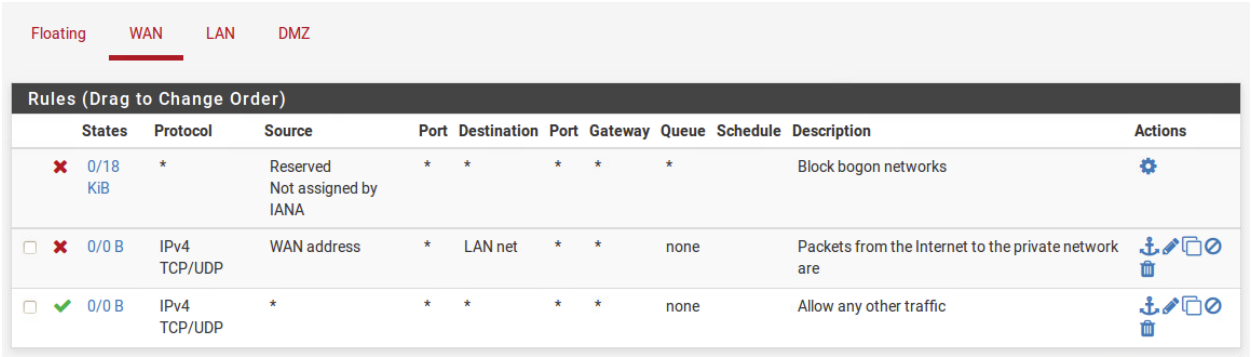


Figure x: Firewall rules for the WAN. All connections originating from the Internet to the LAN network are blocked.

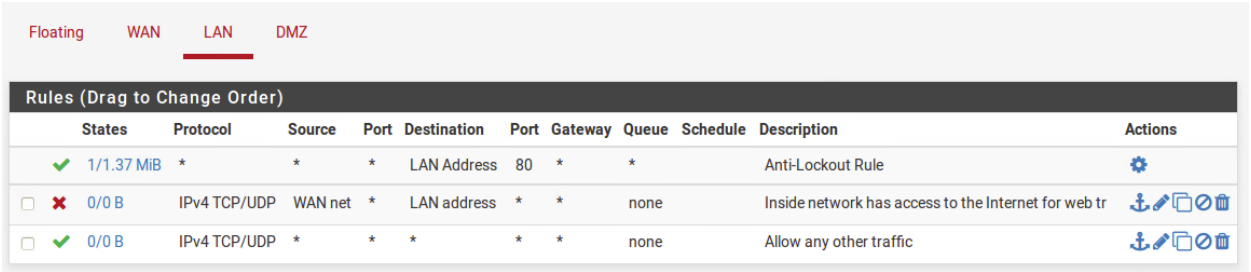


Figure x: Firewall rules for the LAN.