Botnet Detection and Perimeter Defence

Coursework Submission for CSN08703

Edinburgh Napier University 2018-2021 Trimester 2

Jenny S / 40417718 / April 2018

Table of Contents

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 infecting a device, looks for other malware on the device and removes it, to claim the device for itself. 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 monitors network traffic, looking for malicious activity and threats. It issues out alerts when it finds suspicious traffic. Some IDS can identify patterns of traffic that are unusual to prevent DoS attacks. (Pratt, 2018) There are two main types of IDS: 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 are often use Tap or Span ports to scan a copy of the incoming traffic to a network. This means that the performance of a network is not affected. 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 below:

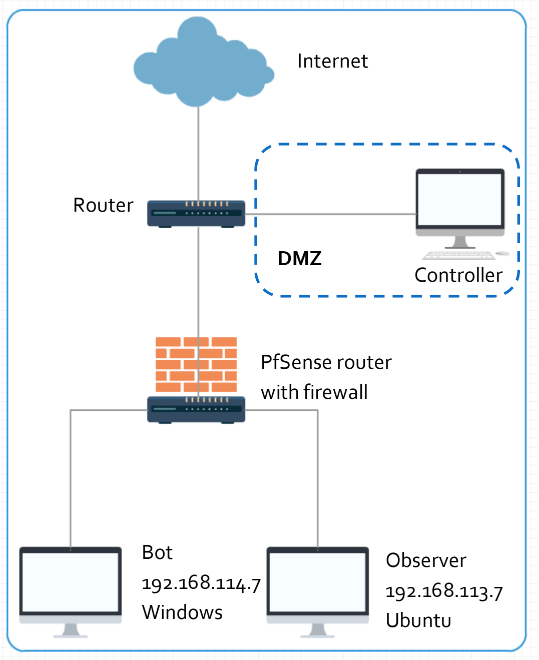
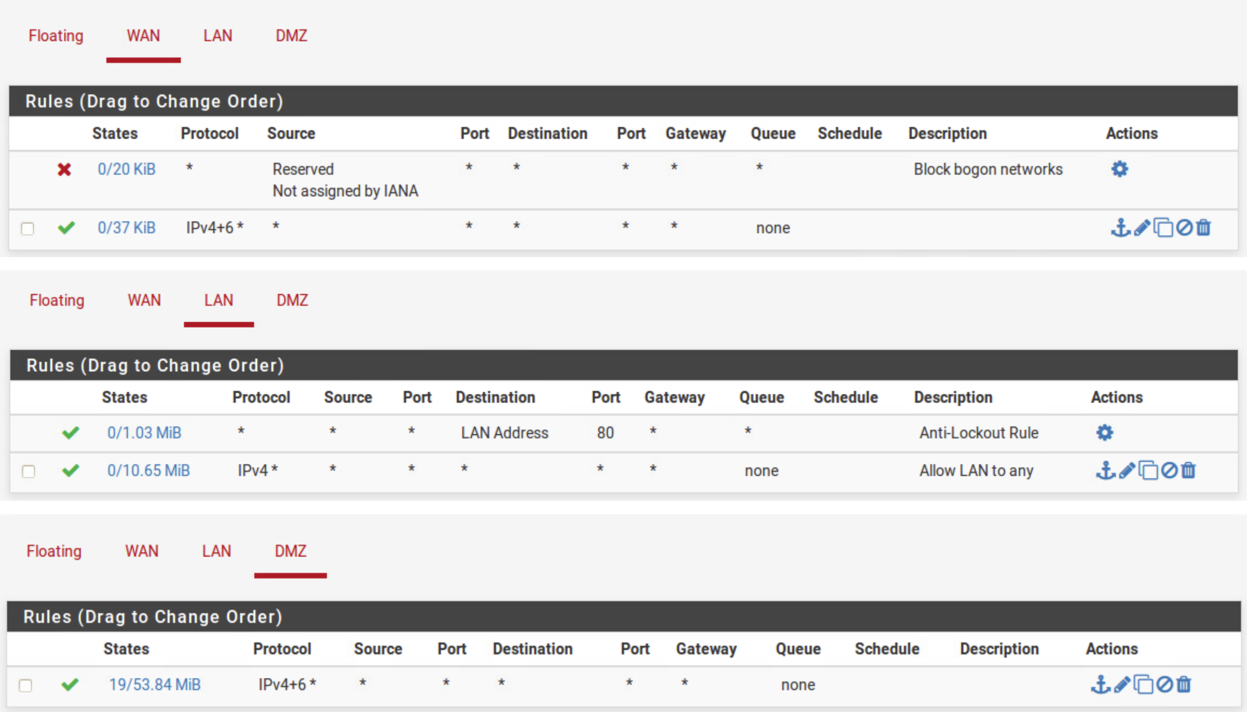


Figure 1: A diagram showing the design of the network used to test the botnet. The observer is used to pick up network traffic generated by the bot and controller communicating.

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 the following firewall rules:



Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/20 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	0/37 KiB	IPv4+6 *	*	*	*	*	*	none			⚓✎⧉⊘🗑

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0/1.03 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✓	0/10.65 MiB	IPv4 *	*	*	*	*	*	none		Allow LAN to any	⚓✎⧉⊘🗑

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	19/53.84 MiB	IPv4+6 *	*	*	*	*	*	none			⚓✎⧉⊘🗑

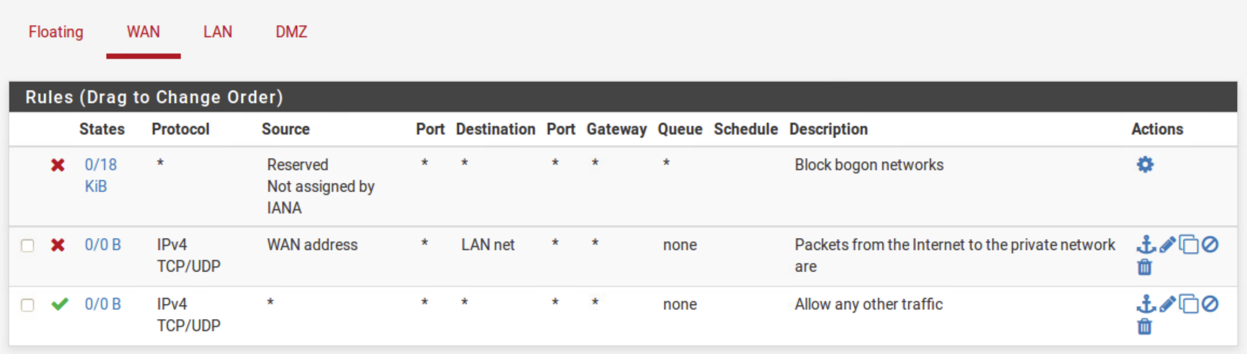
Figures 2, 3 & 4: pfSense firewall rules allowing all traffic through the network on all three interfaces.

Botnet connections and traffic:

The commands and their functions are as follows:

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:	

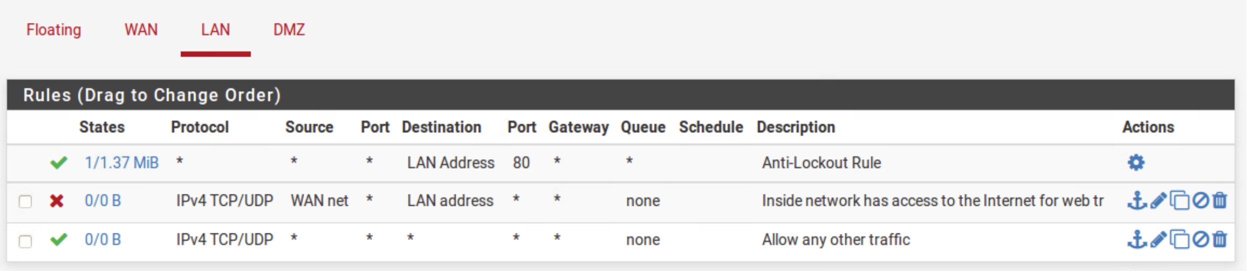
A closed security stance has been used to lock down the network. The firewall rules used for this are shown below:



Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/18 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✗	0/0 B	IPv4 TCP/UDP	WAN address	*	LAN net	*	*	none		Packets from the Internet to the private network are	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0/0 B	IPv4 TCP/UDP	*	*	*	*	*	none		Allow any other traffic	⚓ ✎ ⧉ ⊘ 🗑

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



Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/1.37 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✗	0/0 B	IPv4 TCP/UDP	WAN net	*	LAN address	*	*	none		Inside network has access to the Internet for web tr	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0/0 B	IPv4 TCP/UDP	*	*	*	*	*	none		Allow any other traffic	⚓ ✎ ⧉ ⊘ 🗑

Figure x: Firewall rules for the LAN.

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].