**Distributed DoS**



rectangle

INCIDENT

RESPONSE

**RUNBOOK**

**Contents**

[**SANS Framework 3**](#_jjgwduoidzh0)

[**Detection 3**](#_uvgbvb8lobwf)

[**Analysis 4**](#_vjojt4ws7zsl)

[**Containment 5**](#_nqxphh4ipp8o)

[**Eradication 6**](#_6t3uitywa737)

[**Recovery 7**](#_lbpcmiina1)

[**Post incident activity 8**](#_a190devfa18v)

[**Incident Response Checklist 9**](#_xaj7r79oe8dx)

[**Appendix A - Incident Response Report Form 10**](#_qcddp6nib639)

[INCIDENT RESPONSE REPORT FORM 10](#_h8wiqr3ynmdy)

[**Appendix B - Evidence Log and Strategy 12**](#_fzdekbq8cp70)

[**Appendix C – Exercise evaluation 16**](#_rezb1xwv9wit)

[RED Team Evaluation 16](#_sfaqbjzhn3ls)

[BLUE Team Evaluation 17](#_wxo9rkuhf8kv)

[**Appendix D - Team minutes - Runbook Pre-Development Discussion 18**](#_2i4w80n2vnil)

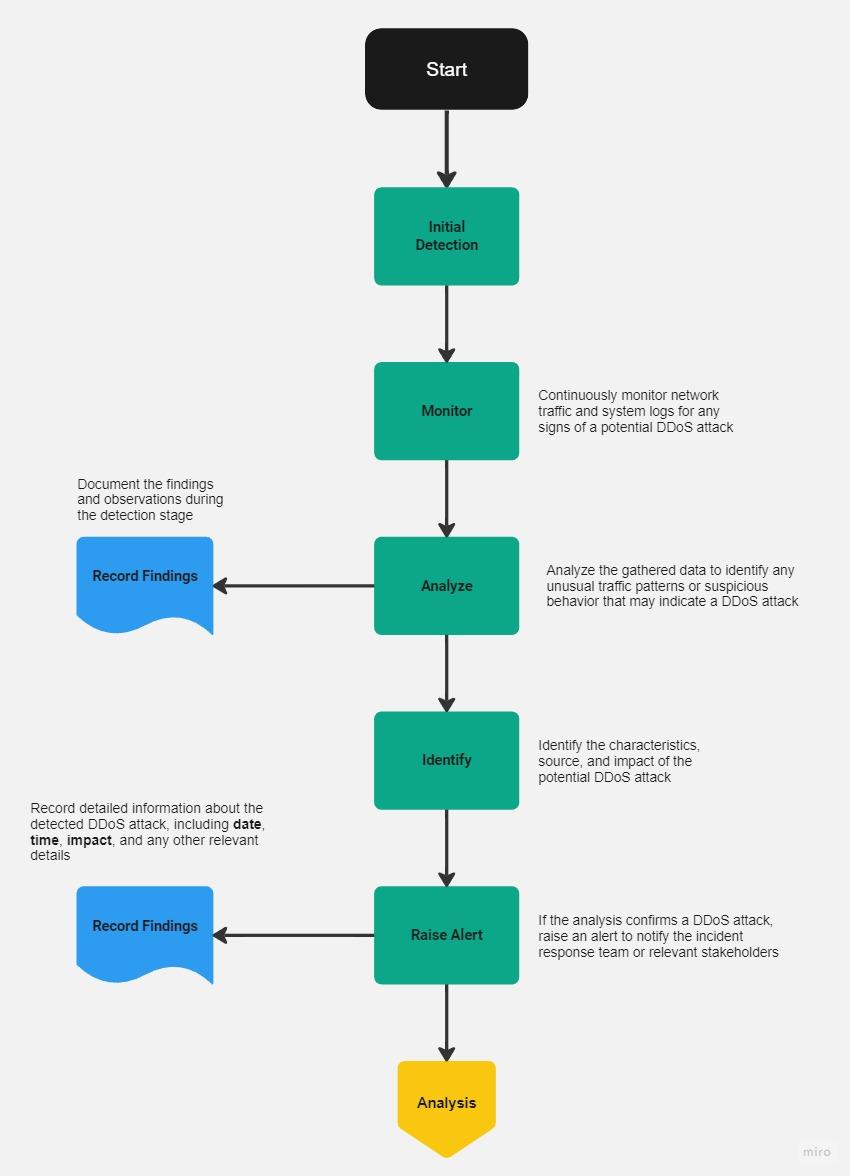
## 

|  |
| --- |
| SANS Framework |

## 

|  |
| --- |
| Detection |

## 



## 

|  |
| --- |
| Analysis |

## 

## 

|  |
| --- |
| Containment |

## 

## 

|  |
| --- |
| Eradication |

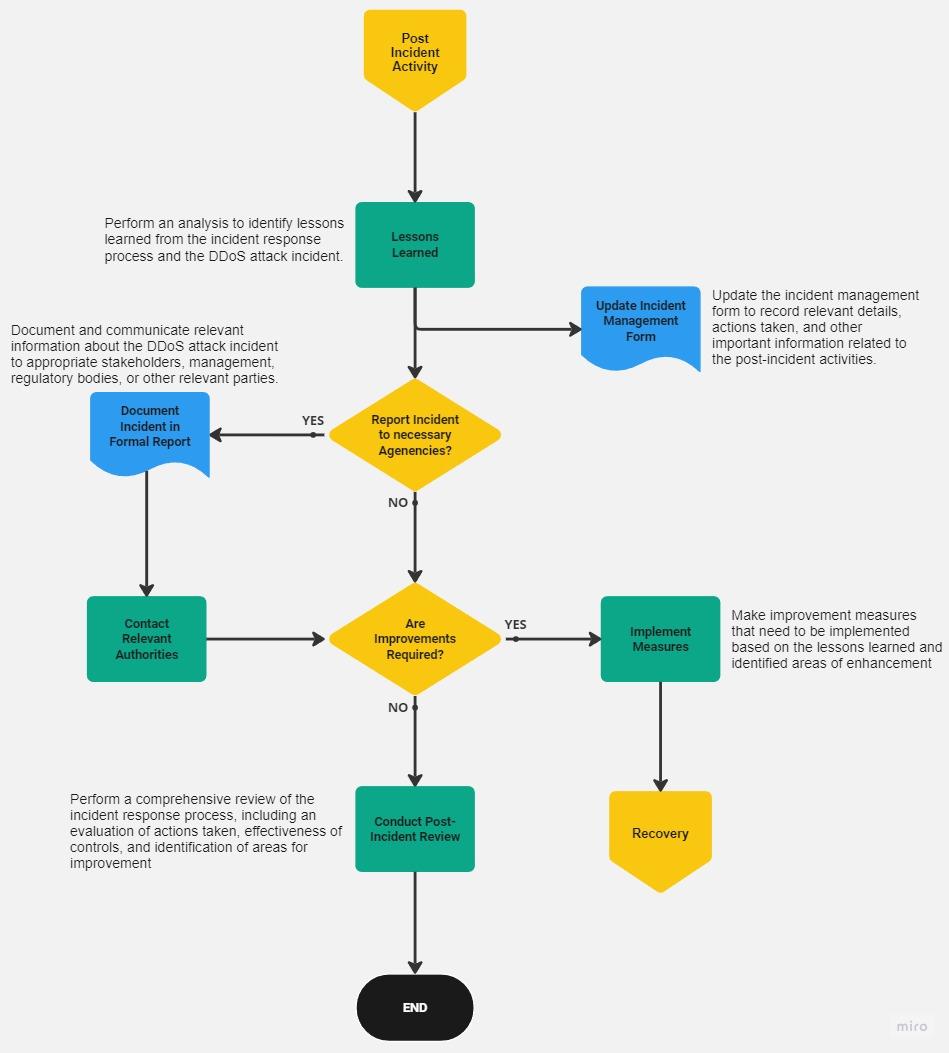
## 

|  |
| --- |
| Recovery |

## 

## 

|  |
| --- |
| Post incident activity |



|  |
| --- |
| Incident Response Checklist |

## 

|  |  |  |
| --- | --- | --- |
| **Detect** | | |
| **#** | **Action** | **Completed** |
| 1 | Monitor network traffic for abnormal patterns or sudden increases in traffic volume. | Done |
| 2 | Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to identify and mitigate potential DOS attacks. | Done |
| 3 | Implement network traffic analysis tools to detect and analyze suspicious traffic patterns. | Done |
| 4 | Set up real-time alerts and notifications to promptly identify and respond to DOS attacks. | Done |
| 5 | Utilize network monitoring tools to track and analyze network performance metrics for signs of a DOS attack. | Done |

## 

|  |  |  |
| --- | --- | --- |
| **Analysis** | | |
| **#** | **Action** | **Completed** |
| 1 | Collect and analyze network logs, including firewall logs, to identify the source and nature of the DOS attack. | Done |
| 2 | Conduct packet-level analysis to determine the characteristics and patterns of the attack traffic. | Done |
| 3 | Perform traffic flow analysis to identify any anomalies or deviations from normal traffic patterns. | Done |
| 4 | Use network forensics tools to capture and analyze network packets for evidence of the attack. | Done |

## 

|  |  |  |
| --- | --- | --- |
| **Containment** | | |
| **#** | **Action** | **Completed** |
| 1 | Isolate affected systems or networks from the rest of the infrastructure to minimize the impact of the DOS attack. | Done |
| 2 | Implement access control lists (ACLs) or firewall rules to block traffic from suspicious or malicious sources. | Done |
| 3 | Deploy rate-limiting mechanisms or traffic filtering to mitigate the impact of the attack. | Done |
| 4 | Utilize load balancers or content delivery networks (CDNs) to distribute traffic and alleviate the effects of the attack. | Done |
| 5 | Implement traffic shaping techniques to prioritize critical network traffic and ensure essential services remain accessible. | Done |

## 

|  |  |  |
| --- | --- | --- |
| **Eradicate** | | |
| **#** | **Action** | **Completed** |
| 1 | Identify and remove any malicious software or compromised systems contributing to the DOS attack. | Done |
| 2 | Patch vulnerabilities or misconfigurations that were exploited during the attack. | Done |
| 3 | Conduct a comprehensive security audit to identify and address any weaknesses in the infrastructure. | Done |
| 4 | Enhance network security measures, such as implementing stricter access controls and updating firewall rules. | Done |
| 5 | Review and revise incident response plans and procedures to better prepare for future DOS attacks. | Done |

## 

|  |  |  |
| --- | --- | --- |
| **Recovery** | | |
| **#** | **Action** | **Completed** |
| 1 | Restore affected systems and services to their normal state after ensuring the attack has been contained. | Done |
| 2 | Validate the integrity of data and perform backups to ensure no critical information was lost or compromised. | Done |
| 3 | Test and verify the functionality of restored systems and applications to ensure proper recovery. | Done |
| 4 | Communicate with stakeholders and users to provide updates on the status of the recovery process. | Done |
| 5 | Conduct post-recovery monitoring to identify any residual effects or vulnerabilities and address them promptly. | Done |

## 

|  |  |  |
| --- | --- | --- |
| **Post Incident Review** | | |
| **#** | **Action** | **Completed** |
| 1 | Conduct a thorough review and analysis of the incident, including the response actions taken. | Done |
| 2 | Document lessons learned and identify areas for improvement in incident response procedures. | Done |
| 3 | Update security policies and procedures based on the insights gained from the DOS attack. | Done |
| 4 | Provide training and awareness programs for staff to enhance their understanding of DOS attacks and response measures. | Done |
| 5 | Collaborate with external parties, such as law enforcement or industry peers, to share information and prevent future attacks. | Done |

|  |
| --- |
| Appendix A - Incident Response Report Form |

|  |
| --- |
| INCIDENT RESPONSE REPORT FORM |

|  |  |  |
| --- | --- | --- |
| **INCIDENT IDENTIFICATION INFORMATION** | | |
| **Date and Time of Notification:** Sunday 9 July 2023 | | |
| **Incident Detector’s Information: Mauricio G. Guerra** | | |
| **Name:** Mauricio | **Date and Time Detected:** 09 July 2023. 12:30 PM | |
| **Title:** Technology Watch | **Location:** Melbourne, AUS | |
| **Phone/Contact Info:** | **System or Application:** Linux Web Server Ubuntu 23.04 | |
| **INCIDENT SUMMARY** | | |
| **Type of Incident Detected:**  ✓ Denial of Service ☐ Malware ☐ Ransomware  ☐ Unauthorized Access ☐ Phishing Attack ☐ Malicious Code  ☐ Other: (Specify) | | ☐ Unauthorized Use  ☐ Other |
| **Description of Incident:** Employee identified with the ID number8965247 in this company noticed an unusual increase of requests in the Linux Server while he was monitoring the network with the software Splunk Enterprise. After notice the increase of requests he filtered the the events in the Sophos Firewall, after that he could determine that the LInux WEb SErver was under attack, however the Sophos Firewall could handle the requests due to it was configured for floods detection and IP Spoofing. There wasn't any real threat for the network. | | |
| **Names and Contact Information of Others Involved:** Mauricio G. Guerra | | |
| **INCIDENT NOTIFICATION – OTHERS** | | |
| ☐ IS Leadership ☐ System or Application Owner  ✓ Security Incident Response Team ☐ Public Relations Dept  ☐ Administration ☐ Human Resources  ☐ Other: | | ☐ System or Application Vendor  ☐ Legal Counsel |
| **ACTIONS** | | |
| **Identification Measures (Incident Verified, Assessed, Options Evaluated):** | | |
| * The incident was verified with Splunk and Snort software. | | |
| **Containment Measures:** | | |
| * Isolate affected Linux Web Server | | |
| **Evidence Collected (Systems Logs, etc.):** | | |
| * System logs | | |
| **Eradication Measures:** | | |
| * Enhance network security measures, such as implementing stricter access controls and updating firewall rules. | | |
| **Recovery Measures:** | | |
| * Restore the affected Linux Server after the eradication measures has been done | | |
| **Other Mitigation Actions:** | | |
| * Review and revise incident response plans and procedures to better prepare for future DOS attacks. | | |
| **How Well Did Work Force Members Respond?** | | |
| * The response was immediate. The employee was monitoring the network. | | |
| **Were the Documented Procedures Followed? Were They Adequate?** | | |
| * They were adequate and ready to follow the procedures indicated for OZ Casual. The IT Team followed and applied the procedures there were in the document. | | |
| **What Information Was Needed Sooner?** | | |
| * There is no data compromised | | |
| **Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?** | | |
| * N/A | | |
| **What Could Work Force Members Do Differently the Next Time an Incident Occurs?** | | |
| * Be more aware that DOS attacks can reach the level of a DDOS attack and affect the entiver system. | | |
| **What Corrective Actions Can Prevent Similar Incidents in the Future?** | | |
| * Keep monitoring Snort and Splunk on an hourly basis, always aware of any incident. | | |
| **What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?** | | |
| * Obtain the most “premium” service from Sophos XG Firewall. | | |
| **Other Conclusions or Recommendations:** | | |
| * A cloud base server with IDS and IPS services integrated could enforce the security of the network. | | |
| **FOLLOW-UP** | | |
| **Reviewed By:**  ✓ IT Management ☐ Security Officer ☐ IS Department/Team  ☐ Privacy Officer ☐ Other | | |
| **Recommended Actions Carried Out:** | | |
|  | | |
| **Initial Report Completed By:** Mauricio G. Guerra | | |
| **Follow-Up Completed By:** Giuseppe Raciti | | |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appendix B - Evidence Log and Strategy | | | | |
| **Date, Time and Location** | **COLLECTED BY** | **ITEM DETAILS** (serial #, model #, hostname, (MAC) address, and IP addresses) | **Evidence Log** | **ACCESS  (**date, time, person and rationale for access after collection**)** |
| **9/7/2023** | Name:  Mauricio G. Guerra  Title:  Technology watch  Contact:  0400 855 855  email:  mauriciogguerra@live.vu.edu.au | Target:  IP Address: 124.187.235.214 | **A NMAP scan was performed in order to detect what ports are open.**  **nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script default or discovery and safe 124.187.235.214** | **Mauricio G Guerra**  **12:20 PM** |
| **9/7/2023** | Name:  Mauricio G. Guerra  Title:  Technology watch  Contact:  0400 855 855  email:  mauriciogguerra@live.vu.edu.au | Target:  IP Address: 124.187.235.214 | **The open ports are 67, 68, 80, 1900, 3389. The port 80 was selected to perform the Dos attack.** | **Mauricio G Guerra**  **12:25 PM** |
| **9/7/2023** | Name:  Mauricio G. Guerra  Title:  Technology watch  Contact:  0400 855 855  email:  mauriciogguerra@live.vu.edu.au | Target:  IP Address: 124.187.235.214 | **In this step we performed the DOS attack dropping 50 packets with the following commands: sudo hping3 -S -p 80 -c 50 124.187.235.214 –rand-source** | **Mauricio G Guerra**  **12:30 PM** |
| **9/7/2023** | Name:  Mauricio G. Guerra  Title:  Technology watch  Contact:  0400 855 855  email:  mauriciogguerra@live.vu.edu.au | Target:  IP Address: 124.187.235.214 | **Splunk was able to detect the pings blocked for Sophos firewall and at the same time displayed a graphic where the main ping event was reached. This probe that Sophos was able to mitigate the DOS attack.** | **Mauricio G Guerra**  **12:30 PM** |
| **9/7/2023** | Name:  Mauricio G. Guerra  Title:  Technology watch  Contact:  0400 855 855  email:  mauriciogguerra@live.vu.edu.au | Target:  IP Address: 124.187.235.214 | At the same time when the attack was running Snort (IDS-IPS) was enabled and analyzing real time network traffic. We was able to capture the incoming pings from the DOS track. | **Mauricio G Guerra**  **12:30 PM** |

|  |
| --- |
| Appendix C – Exercise evaluation |

|  |
| --- |
| RED Team Evaluation |

|  |
| --- |
| **Activity name and description:** DOS attack |
| The Red Team will create a NMAP scan of the target  After identified the vulnerabilities and open ports the Red Team will attack with a DOS attack |
| **Did you have available to you all of the information and resources needed to fulfill your responsibilities?  If so, comment on its suitability. If not, provide details of what was missing.** |
| Kali contains all the tools needed to create the DOS track including NMAP and HPING3. |
| **Did you feel that there was an adequate level of training to support the attack? If, not provide details** |
| Yes |
| **Was the structure of the exercise realistic? If not, provide details** |
| Yes |
| **Please provide comments regarding what you believe worked and did not work during the exercise?** |
| The Red Team did a NMAP scan and a DOS track, both works. However the Sophos Firewall was able to stop the attack due to all the rules, IP Spoofing and detection for floods were enabled. |
| **How can the red team’s actions be improved?** |
| If we want to go ahead with a denial of service we should implement a DDOS attack with hundreds of thousands or millions of bots that could overpass the Sophos Firewall rules. |
| **How can the red team’s training be improved?** |
| Training ourselves on the use of other pen-testing tools to create different types of attacks, would allow us to deploy more sophisticated techniques, such as DDOS attacks. |
| **How appropriate was the pre-training to the exercise?** |
| It was very realistic due to the fact that we were able to implement the different tools for a DOS attack. |
| **How could the pre-training be improved?** |
| A training in Sophos Firewall XG in order to understand how this software works and how we can overpass or exploit vulnerabilities. |

|  |
| --- |
| BLUE Team Evaluation |

|  |
| --- |
| **Activity name and description : Distributed Denial of Server (DDoS) attack** |
| Red Team will start a DOS attack in order to flood the Linux Web Server  Blue Team will monitor, contain and eradicate the attack |
| **Did you have available to you all of the information and resources needed to fulfill your responsibilities? If so, what information and resources were used? If not, provide details of what was included and what should have been included.** |
| Yes. We did have available virtual machines with Splunk Software and Snort installed.Also VM with Sophos FIrewall XG active and intercepting all the incoming requests. |
| **Was the structure of the exercise realistic? If not, provide details** |
| Yes, it was realistic. As a DOS attack response, the Blue team did have training how to respond to this attack. |
| **Please provide comments regarding what you believe worked and did not work during the exercise?** |
| The Blue Team operations did intercept the DOS attack using the Firewall Sophos XG and at the same time did monitor Splunk and Snort to analyze the logs and make better decisions. |
| **How can the blue team’s response be improved?** |
| Getting to know the tools that attackers can use to perform DOS attacks and at the same time how this attacks work. Also be aware of the standard procedures for DOS and DDOS mitigation. |
| **How can the blue team’s training be improved?** |
| A training in [Splunk Enterprise Security Certificate Admin](https://www.splunk.com/en_us/training/certification-track/splunk-es-certified-admin.html) will be a good training to practice real cyber attack scenarios. |

|  |
| --- |
| Appendix D - Team minutes - Runbook Pre-Development Discussion |

**09/07/2023 : Minutes of the Meeting**

**Giuseppe Raciti** - Project Manager / Team Lead

* The style of the framework was initially a step by step detailed guide, but eventually, it was decided that the SANS Incident Response format was preferred in a flowchart format.
* Using a runbook for the DOS Incident response, each group member was able to allocate a task they wanted to perform during the functional exercise.
* The red team was originally going to flood the Windows Server, however we decided to change it for the Linux Web Server.

**Mauricio Guerra** - Server Administrator

* **The detection step** could be improved if a Cloud Detection System is incorporated at the same time with Sophos XG and Snort. For example Google IDS Cloud service could predict some events and this level of predictivity could raise the security level.
* **Eradication step:**  As a result of the DOS attack and the possibility that there is no other Linux Web Server it is critical to create a backup Web Server that can be replaced if this type of attacks achieves their purpose.
* **Pos incident step:** It is imperative to update policies, procedures, controls and technologies in place to build capacities for backups, physicals and in the cloud.

**Shaun Heywood** - Cyber Security Specialist

* Configure network devices to limit the rate of incoming traffic and filter out suspicious or malicious requests, helping to mitigate the impact of a DOS attack.
* Install an IPS to monitor network traffic in real-time, other than Snort due to sometimes the software was unresponsive.
* Create a comprehensive plan outlining steps to be taken during a DOS attack, including communication protocols, personnel responsibilities, and predefined mitigation strategies.

**Mark Byrne** - Cloud Architect / Engineer

* Design the cloud infrastructure to dynamically scale resources based on demand, allowing for efficient handling of increased traffic during a DOS attack.
* Use the infrastructure of a dedicated DDoS protection service provided by the cloud provider or a third-party vendor to identify and mitigate DOS attacks in real-time.
* Use load balancers in order to distribute incoming traffic across multiple servers, preventing any single server from becoming overwhelmed during a DOS attack.