|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incident Report** | | | | |
| **Particulars of incident:** | | | | |
| Date:monday | | Time:7:00 | | Location:addis ababa |
| **Type of incident** | | | | |
| cyber attack | | | | |
| Reported by:amanuel | | | | Phone:+251953884202 |
| Role in the event:attacker | | | | Email:eamanuel283@gmail.com |
| **Attacked server:** | | | | |
| Name:seedlab | | | | Run on: VM |
|  |  | | |  |
| **Witness(s):** | | | | |
| Name:edidia | | | | Phone: |
| Name:nahmya | | | | Phone: |
| Name:esmale | | | | Phone: |
| **Describe the incident:**  *(space overleaf for diagram if needed)* | | | | |
| When the server that run on seedlabs hosts and the client connect it by using username=seed password=dees | | | | |
| So, every thing looks perfect until the attacker uses “netwox 76” this command allow the attacker to SYN\_FLOODING attack and after the attacker did that the client cound not connect to the server. | | | | |
|  | | | | |
| **Describe how it happened:** | | | | |
| It happened when the attacker use “netwox 76 -i server ip -p server port -s raw”. | | | | |
|  | | | | |
| **Describe any property damage:** | | | | |
| In this attack i just use it to find out how the attack was happened so there is now serious damage happened but | | | | |
| If The attacker is describe as a black hat it can use this to much more damage on but server and client. | | | | |
| **Analysis:** *What do you think caused or contributed to the incident?* | | | | |
| I think t was caused because the server we use did not apply system harding that means we can protect it by | | | | |
| Shut down the port that we don’t use . | | | | |
| **Prevention:** *What action has been taken to prevent a reoccurrence?* | | | | |
| 1.using IPS(intrusion prevention system)-used to identify malicious traffic. | | | | |
| 2.using Cloudflare | | | | |
| **3.using IDS(intrusion detection system)-used to monitor and alerts when it discovered a malicious traffic.** | | | | |
| Risk Register updated by: | | | Date: | |

