🛡️ Building an Intrusion Detection System with Snort 🛡️

During my tenure at [**CodeAlpha**](https://www.linkedin.com/feed/?trk=guest_homepage-basic_google-one-tap-submit) Cybersecurity Internship, where the development of an intrusion detection system marked the third and final task, I undertook a project to develop an intrusion detection system using Snort. Given the challenge of resource constraints, Snort emerged as the optimal choice, thanks to its efficient resource utilization, making it ideal for environments with limited hardware resources or low-power devices.

I focused on testing Snort's efficacy in detecting intrusions across various protocols. While my system's limitations prevented exhaustive testing, I've shared some insightful results below.

Despite the hardware limitations hindering extensive testing, the project provided invaluable insights into building robust intrusion detection systems. It underscored the importance of selecting the right tool for the job, especially in resource-constrained environments.

For those venturing into intrusion detection system development, I hope these insights prove helpful.

𝗧𝗼𝗼𝗹𝘀 & 𝗦𝗲𝗿𝘃𝗶𝗰𝗲𝘀 𝗨𝘀𝗲𝗱:

•VirtualBox for running the target server

•Kali Linux OS as the main host

•Ubuntu Server 20.04.4 LTS/Latest

•Snort IDS for intrusion detection

𝐆𝐮𝐢𝐝𝐞:

•Install VirtualBox following official instructions from Kali docs.

•Download Ubuntu Server .iso file from the official source.

•Set up the server using VirtualBox GUI:

  - Open VirtualBox

  - Click on "New" or press Ctrl+N

  - Name the instance, select the .iso file, and follow instructions to complete installation.

•Install SSH on the Ubuntu server (optional):

  𝘴𝘶𝘥𝘰 𝘢𝘱𝘵 𝘪𝘯𝘴𝘵𝘢𝘭𝘭 𝘰𝘱𝘦𝘯-𝘴𝘴𝘩

•Install Snort IDS:

 𝘴𝘶𝘥𝘰 𝘢𝘱𝘵 𝘪𝘯𝘴𝘵𝘢𝘭𝘭 𝘴𝘯𝘰𝘳𝘵

𝐂𝐨𝐧𝐟𝐢𝐠𝐮𝐫𝐞 𝐒𝐧𝐨𝐫𝐭:

 - Run `ifconfig` to get the network adapter device name (e.g., `ens33`) and the server's IP address.

  - Edit Snort configuration file `/etc/snort/snort.conf` with the appropriate network adapter and IP address.

•Connect to the server from the main host (Kali) using SSH (optional):

  𝘴𝘴𝘩 𝘶𝘴𝘦𝘳𝘯𝘢𝘮𝘦@𝘴𝘦𝘳𝘷𝘦𝘳\_𝘐𝘗\_𝘢𝘥𝘥𝘳𝘦𝘴𝘴

•Check Snort configuration file:

  𝘴𝘶𝘥𝘰 𝘴𝘯𝘰𝘳𝘵 -𝘛 -𝘤 /𝘦𝘵𝘤/𝘴𝘯𝘰𝘳𝘵/𝘴𝘯𝘰𝘳𝘵.𝘤𝘰𝘯𝘧 -𝘪 𝘦𝘯𝘴33 (𝘤𝘢𝘯 𝘤𝘩𝘢𝘯𝘨𝘦 𝘢𝘤𝘤𝘰𝘳𝘥𝘪𝘯𝘨 𝘵𝘰 𝘶𝘴𝘦𝘳𝘴)

•Run Snort IDS:

  𝘴𝘶𝘥𝘰 𝘴𝘯𝘰𝘳𝘵 -𝘈 𝘤𝘰𝘯𝘴𝘰𝘭𝘦 -𝘲 -𝘶 𝘴𝘯𝘰𝘳𝘵 -𝘨 𝘴𝘯𝘰𝘳𝘵 -𝘤 /𝘦𝘵𝘤/𝘴𝘯𝘰𝘳𝘵/𝘴𝘯𝘰𝘳𝘵.𝘤𝘰𝘯𝘧 -𝘪 𝘦𝘯𝘴33 (𝘤𝘢𝘯 𝘤𝘩𝘢𝘯𝘨𝘦 𝘢𝘤𝘤𝘰𝘳𝘥𝘪𝘯𝘨 𝘵𝘰 𝘶𝘴𝘦𝘳𝘴)

•Perform attacks to test IDS functionality.

**#Cybersecurity** **#IntrusionDetection** **#Snort** **#CodeAlpha** **#CybersecurityInternship** **#Networking** **#SecuritySolutions**

**#internship** [**CodeAlpha**](https://www.linkedin.com/feed/?trk=guest_homepage-basic_google-one-tap-submit)