Project: Phishing Prevention and Detection

Members:

* Aminia
* Nicolai
* Benoit

Planning:

* Deadline 30/8

Tasks:

* Setting up PC1:
  + Setting up phishing tools
  + Create and send phishing mail
  + Test malware
* Setting up PC2:
  + Installation Splunk Universal Forwarder
  + Config Splunk
* Setting up PC3
  + Installation Splunk Enterprise
  + Config Splunk
* Link Splunk PC2 to Splunk PC3
* Setting up rules
* Setting up alerts
* Setting up incident response
* Documentation:
  + Setup up PC’s
  + Phishing campaign
  + Detection methods
  + Incident response
  + Findings
  + Recommendations

Setup machines:

* PC1: Attacker:
* PC2: Victim:
  + Ubuntu
  + Splunk Universal Forwarder
* PC3: Detection/SIEM:
  + Kali LInux
  + Splunk Enterprise or ~~Splunk OVA(only for vmware)~~
  + 4GB RAM
  + 2 processors
  + 20GB hard disk

Installation/configuration PC1 :

Installation/configuration PC2 :

*Installation Splunk Universal Forwarder*

*wget -O splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb "*[*https://download.splunk.com/products/universalforwarder/releases/9.3.0/linux/splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb*](https://download.splunk.com/products/universalforwarder/releases/9.3.0/linux/splunkforwarder-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb)*"*

*Sudo tar xvzf splunkforwarder-linux-x86\_64.tgz -C /opt*

*Cd /opt/splunkforwarder/bin*

*./splunk start —accept-license*

*#follow instructions to create account*

*#change “splunker” to the name you used to make an account*

*Sudo su*

*./splunk enable boot-start -user splunker*

*Configuration Splunk Universal Forwarder*

Installation/configuration PC3 :

In this section we will explain how to install and configure PC3. PC3 will function as the SIEM on which we will install Splunk Enterprise. Splunk Enterprise will act as a server, which collects, analyzes and visualizes all collect data from the connected devices.

*Installation Splunk Enterprise:*

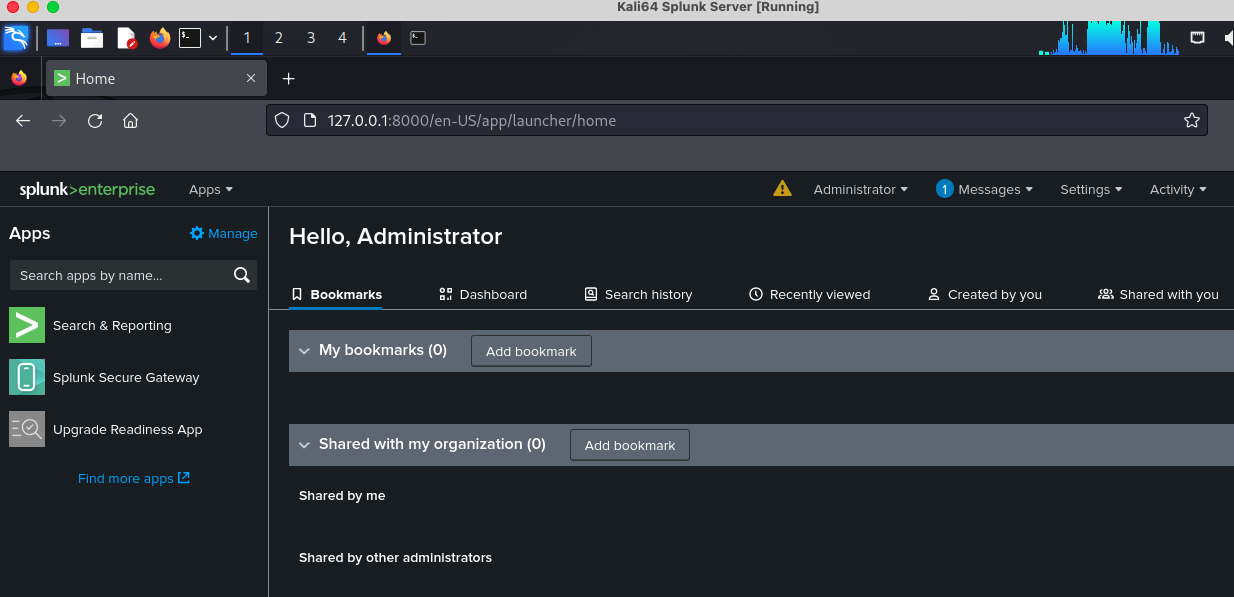
* Create account on [www.splunk.com](http://www.splunk.com)
* In terminal:
  + wget -O splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb <https://download.splunk.com/products/splunk/releases/9.3.0/linux/splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb>
  + sudo dpkg -i splunk-9.3.0-51ccf43db5bd-linux-2.6-amd64.deb
  + sudo /opt/splunk/bin/splunk start --accept-license
  + follow prompts on screen
    - admin: becode
    - passw: becodeisfun

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

After installation and configuration, you can access Splunk using your browser:

* http://<IP\_Splunk\_server>:8000
* Now you can log in with your credentials



*Configuration Splunk Enterprise:*

issues:

* Splunk Enterprise is taking much CPU