Hackathon Iasi, 11- 12 Aprilie 2019

Theme: Recycle an obsolete PC into a Free & Open Source Home Cyber-Security Gateway

Description: Teams are given a previous-generation functional laptop with the following configuration:

Dell Latitude E5430 / E5440

Intel Core i5 3230M, Ivy Bridge
4 GBytes RAM
At least 250 GB Mechanical Storage
Intel Gigabit Ethernet On-Board
Intel Centrino 6205-N Wi-Fi Chip

Using only open source and/or free software, including the operating system(s), the teams will compete into building a cyber-security gateway that has the following minimum functionality:

NAT & Routing + DHCP: The gateway shall be able to route and translate between WAN and LAN interfaces. As the laptops have two network interfaces, Ethernet and Wi-Fi, one could be use as WAN and the other as LAN. We do not mandate the use of one specific interface as either WAN or LAN. It is completely up to the teams' to decide. IF they chose Ethernet as WAN and Wi-Fi as LAN, they could use the Wi-Fi adaptor in AP mode and –practically – build a Home Cyber-Security Wi-Fi Router.

Anti-Virus: The gateway shall be able to scan 'in flight' packets routed through interfaces (or VLANs). This could be accomplished with any available open-source or free scanning engine. This will apply only to unencrypted traffic.

URL Monitoring and URL Blocking: The Gateway shall be able to monitor the HTTP requests and block specific URLs by whitelisting or blacklisting. This functionality should be available on a category-basis (i.e. – Block ALL sites in the "Streaming Video Category").

Firewall: The Gateway shall have a Firewall installed. This shall provide basic-ALG functionality and Source-Destination-Port-type of blocking.

Additional functionality shall be take into consideration by the jury but it is not mandatory for validation.

Implementation:

-The teams can use any x86 / x86-64 open-source or free software.
-The teams shall use only the provided computer as hardware and will not use ANY other hardware computing resource (i.e. – their own laptops, Raspberry PIs etc.).
-The teams can, however, use virtualization platforms (open source / free) to 'split' the available hardware resources of the laptop into virtual machines, if they wish to provide additional functionality (i.e – they could use OPNsense in one VM and something like Pihole for adblocking in another VM)

-It is completely up to the teams on HOW they use the computing power of the laptops to provide as many functionalities as possible.

Validation:

-The validation of the build will be made exclusively on the 4 functionalities required (NAT/Routing, Anti-Virus, URL Mon, Firewall). ANY and all additional functionality, regardless of how it has been implemented will count as differentiators for the jury.

-The method for validation is inspection and (if possible) testing.

Hints:

IPFire, OPNSense, pfSense, untangle, pihole

Notes:

If required at boot-time, the setup password for all the laptops is ‘bright’