Cyber Threat Analysis with Network Packet Analyzers

Tom Cordemans
Belgian IT Academy Support Center BiASC

IT Education Roadshow

6 May 2022

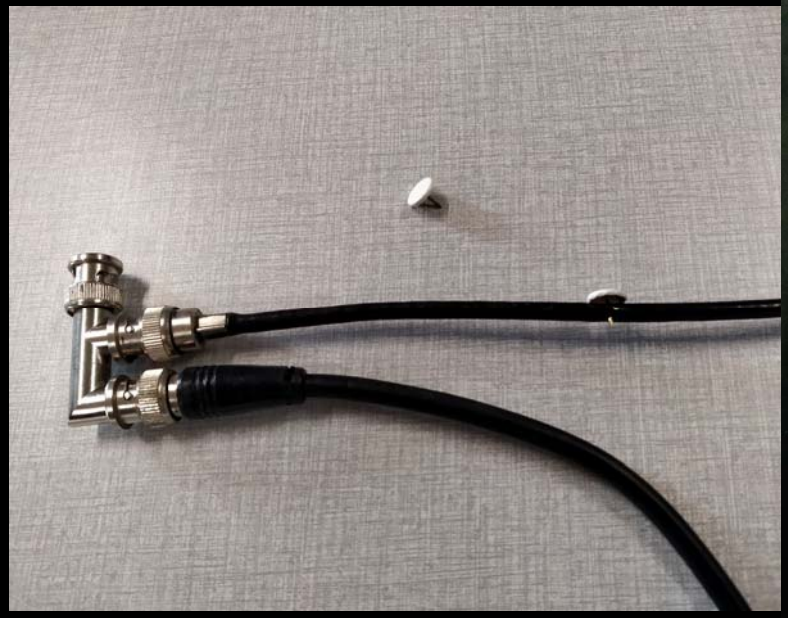
Cisco Networking Academy

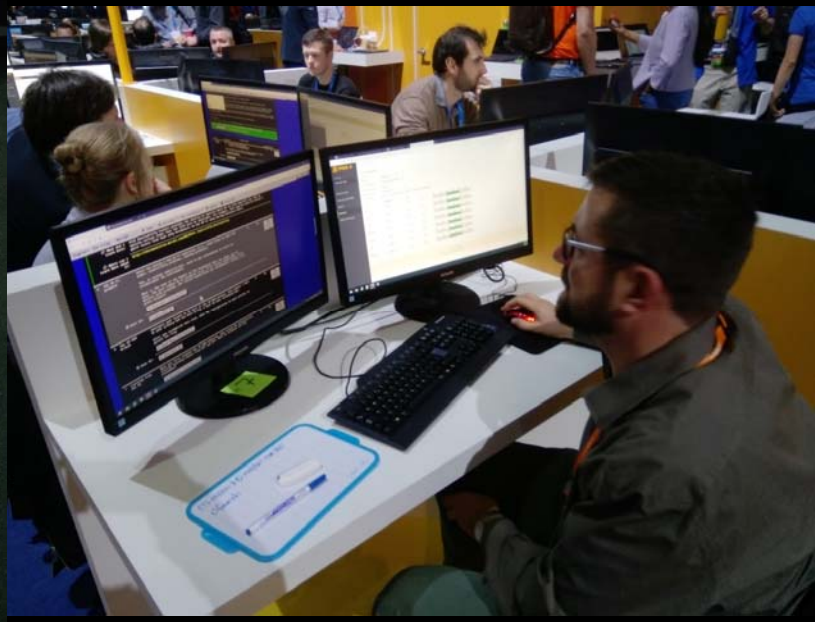
Intro - whoami

- Lecturer at Vives University of Applied Sciences (CCNAv7, IoT Security, …)
- Guest lecturer at Odisee University of Applied Sciences (CyberOps, …)
- Guest lecturer at KU Leuven, Tampere University of Applied Sciences, …
- Researcher:
  - Training the Human Firewall (THUMFI)
  - Secure Industrial Networks (SIN)
- Advisor BiASC

- Contact details: tom.cordemans@biasc.be

Intro – whoami (Cont’d)






Threat analysis

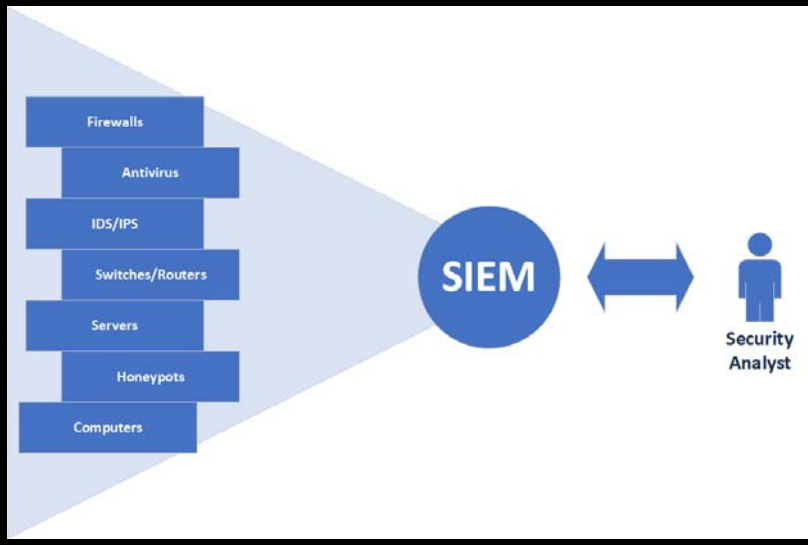
Threat analysis – Introduction

- Objective:
  - A lot of companies use a SIEM (Security Information and Event Management).

    A SIEM provides a holistic view on system data of an organization.

    Once an in-depth investigation is required, people often falls back to “network protocol analyzers”.

    Often there is lack of skills to use those tools efficiently.



Threat analysis - Introduction

- We regularly see a wrong use of “network protocol analyzers”.

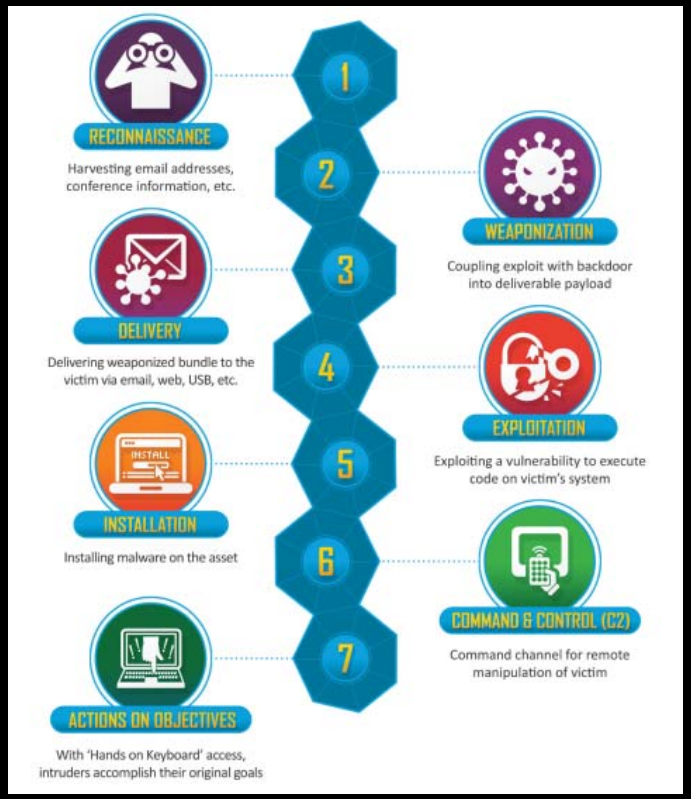
SIEM

Wireshark

- The initial step in investigating cybersecurity threats will therefore never be the use of a “network protocol analyzer”.

Threat analysis - Introduction

- The Cyber Kill Chain Model is often used to represent a cybersecurity related activity.
- Which phases can generate network traffic?



Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Threat analysis – How to tweak Wireshark

- Profiles:
  - Wireshark can be used for various tasks.
    For example: troubleshooting, educational purposes, security threats, ...
  - A profile is a collection of specific settings composed for a particular task.
  - A clean install of Wireshark starts with the "Default Profile".
  - It is a best practice not to make any changes to the "Default Profile“.
  - A better option is to create a profile for each task.
  - Profiles can also be imported and exported.

Threat analysis – How to tweak Wireshark

- Profiles:
  - Exercise: Check-ICMP.pcapng
    - Make a new profile
    - Time Display Format
    - GeoIP
    - Add columns (Socket pairs)
    - Add coloring rules
    - Add filter buttons

Threat analysis – WARNING

- Caution:
  - Since network traffic can contain malware, there is always a risk.
  - A completely separate environment is therefore recommended.
  - In addition, a non-Microsoft operating system is often recommended. In this way we reduce the risk of contamination of the system and spread via the network.
  - One possible method is to use a virtual machine. https://www.kali.org/get-kali/#kali-virtual-machines
  - As an extra security measure, we can disable the virtual machine's network adapter.

Threat analysis – MALWARE!

- Indicators of compromise (IOCs) serve as forensic evidence of potential intrusions on a host system or network.

  Some examples of IoCs:

  - Unusual DNS lookups
  - Suspicious files, applications and processes
  - IP addresses and domains belonging to botnets or malware C&C servers
  - A significant number of accesses to one file
  - Suspicious activity on administrator or privileged user accounts
  - An unexpected software update
  - Data transfer over rarely used ports
  - Behavior on a website that is atypical for a human being
  - An attack signature or a file hash of a known piece of malware
  - Unusual size of HTML responses
  - Unauthorized modification of configuration files, registers or device settings
  - A large number of unsuccessful login attempts
  - …

Threat analysis – MALWARE!

- We take “Remcos RAT” as an example.

  Additional information:

  - A user got an email with an attachment (Payment Remittance Advice.xlsb) on his computer (IP address 10.1.4.101) on January 4th 2022 (21h24)
  - The user opened the Excel file and enabled macros.
  - The macro initialized a connection to OneDrive.

Important note:
This example is retrieved from https://www.malware-traffic-analysis.net/