Having a Blue Team Blast

Because there’s more than red team…

root@mcti ~$ **whoami**

- Lead SOC Engineer at Netizen Corporation

- MCTI alumni

- Avid security enthusiast

root@mcti ~$ **cat blue-team.txt**

- Architectural and defensive personnel

- SOC analysts, network engineers, etc.

- We keep businesses running and out of the news!

root@mcti ~$ **man blue-team**

- Security doesn’t end at the computer in front of you.
  - Cloud
  - AI
  - Vendors (HVAC units?)

- Security stacks
  - SIEM (Wazuh)
  - NSM (Bro/ Suricata)
  - EDR/XDR (Symantec, SentinelOne)
  - IPS/IDS (Suricata, Snort)
  - Vulnerability scanners (Greenbone)

root@mcti ~$ **cat extra-resources.txt**

- DEFCON 28 - OpenSOC YouTube videos
- TryHackMe SOC career path
- HackTheBox “Sherlocks”
- Kali Purple

OpenSOC Resources

mcti@root ~$ **python3 setup.py**

- Recommended tools for Hands-on challenges
  - Kali Linux virtual machine
  - Suricata
    - *sudo apt install suricata*
    - Configure your /etc/suricata/suricata.yaml
      - HOME_NET = “any”
      - EXT_NET = “any”
  - WireShark
  - CyberChef (website)

- To download all necessary .pcaps

  https://github.com/JordanMcGrathhhh/MCTI-Presentation (4 ‘h’s)

root@mcti ~$ **./challenge-1**

- Pretext: Robert was administering a custom website on the open MCTI WiFi network. Silly him, he was using HTTP. Can you recover Robert's correct password to show him how dangerous unencrypted protocols are?

Hint: Ensure you cover all of your **bases**

Tools: WireShark, CyberChef

root@mcti ~$ **./challenge-2**

- Pretext: Welcome to the beautiful, dreadfully hot desert- Las Vegas! You're a SOC analyst ensuring that nothing suspicious happens on the DEFCON 2017 open WiFi network. It looks like you just got an alert from Suricata…

07/29/2017-15:31:25.120363 [**] [1:2002677:15] ET SCAN Nikto Web App Scan in Progress [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 10.151.31.252:40394 -> 54.245.134.126:80

Can you confirm the validity of this alert? Anything we should be worried about, captain?

Tools: Wireshark, Suricata

root@mcti ~$ **./challenge-3**

Pretext: As a SOC analyst, you'll have to dig through quite a bit of false positives. It's up to you to find the exploit inside of this network capture…

Hint: Consider disabling a certain rule within Suricata

Tools: WireShark, Suricata