DEF CON 33: Deep-dive into modern network fingerprinting

Workshop Tasks & Environment

- **Main Tasks Server:** https://workshop.ellio.tech
- **Fingerprinting Server:** https://fingerprints.ellio.tech
- **Credentials:** You'll receive SSH access to two Ubuntu VMs at workshop start:
    - **Server** (for capturing fingerprints)
    - **Client** (to initiate connections)
- **Requirements:**
    - Laptop with terminal emulator & internet access
    - **Backup:** Mobile hotspot in case of connectivity issues
    - Bring your laptop & charger

Key References

- **MuonFP** (Fingerprinting TCP/IP stacks)
  https://github.com/sundruid/muonfp
- **JA4** (TLS 1.3 fingerprinting tool)
  https://github.com/FoxIO-LLC/ja4
  https://github.com/FoxIO-LLC/ja4/blob/main/technical_details/JA4.md
- **Transition from JA3** (TLS extension shuffle)
  https://www.stamus-networks.com/blog/ja3-fingerprints-fade-browsers-embrace-tls-extension-randomization
- **Introduction to JA3**
  https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967/
- **p0f** (Passive OS fingerprinting)
  https://en.wikipedia.org/wiki/P0f

Questions & Feedback

Send questions or suggestions to **vlad.iliushin@ellio.tech** with subject **DC33 Workshop**.

Have fun, and happy fingerprinting!