SNA Lab - Network Sniffing

This is not only about security and evesdropping. Sniffing can also be useful for troubleshooting network and application level protocols. Knowing how to use tcpdump or Wireshark will be helpful in your career. Explore their respective filtering (and searching) features. Show how you managed to take advantage of those in your report. Copy/pasting text is also fine instead of screenshots.

Choice 1 - Sniff & Scan

- Sniff your network and explain what you can see there. Gain as much information about it while remaining passive.
- Scan your network without attempting any attack. Just proceed with a gentle network discovery and report your analysis. This should *not* be illegal esp. on an internal network.
- Bonus: if you're on the SNE LAN, you can go rogue and experiment anything within it, but do something elegant and try to remain unnoticed, and so people who live there can continue to work.

Choice 2 - SSL/TLS dissection

& presentation

Sniff a SSL/TLS handshake like a fanatic[1] and show how it goes. Bonus: eventually get into the SSL stream with a session key (if there is an easy way to obtain it) – or if you really like math, you can try to do the calculations yourself…

Choice 3 - IPSEC

team of two & presentation

Setup any flavor of Open Source IPSEC (SSL-based VPN) software. Design a decent network architecture for that purpose, describe it in a diagram, integrate and validate it accordingly.

You get NetBSD and Slackware guests at will on the SNE LAN.

Choice 4 - Strip out STARTTLS

team of two & presentation

Do something similar to sslstrip, but against STARTTLS. E.g. try https://github.com/tintinweb/striptls.

Bonus: what would it take to proceed with STARTTLS MITM instead? No PoC required, just think about it.

Choice 5 - IPv6

& presentation

Attempt to reach an IPv6 host www.kame.net from Innopolis. Evaluate if https://ipv6.ip4market.ru/ fits the purpose (untested, but that should do it). If you need a public IPv4 address, you can ask @pbraun which one you can take from the SNE students IP Range (188.130.155.32/27).

[1] OpenSSL tips and tricks https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art030
The TLS Handshake at a High Level https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art057
A walk-through of an SSL handshake https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art059
SSL Key Exchange example https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art060
SSL Certificate Exchange https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art061
A walkthrough of a TLS 1.3 handshake https://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art080