11/1 – Round2Day2 **Deep Packet Inspect**

* Deep Packet Inspection (DPI) or packet sniffing is a type of data processing that inspects in detail the data being sent over a computer network, and usually takes action by blocking, re-routing, or logging it accordingly.
  + Ensure that data is in the correct format, to check for malicious code, eavesdropping, and internet censorship, among other purposes.
* Intrusion detection system (IDS)
* Intrusion prevention system (IPS)
* Stateful Firewall
* Denial-of-service attacks (DoS)
* Data Leak Prevention (DLP)
* How DPI works?
  + A form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems interconnection’s application layer
  + DPI evaluates the contents of a packet that is going through a checkpoint
  + DPI is able to check the contents of these packets and then figure out where it came from, such as the service or application that sent it.
  + DPI can work with filters in order to find and redirect network traffic from an online service, such as Twitter or Facebook, or from a particular IP address
* Use cases for DPI:
  + Acts as an intrusion detection system or a combination of intrusion prevention
  + Identify specific attacks that your firewall, intrusion prevention, and intrusion detection systems cannot adequately detect
  + Detect if there are prohibited uses of approved applications
  + Used by network managers to help ease the flow of network traffic
    - E.g., enable high-priority information to passage through
  + Used to enhance the capabilities of ISPs to prevent the exploitation of IoT devices in DDOS attacks by blocking malicious requests from devices
  + Can help you prevent anybody from leaking information, such as when e-mailing a confidential file
* DPI techniques
  + Pattern or signature matching
  + Protocol anomaly
  + IPS solutions
* Challenges of DPI
  + Can also be used to create similar attacks
  + Complicated and harder to manage
  + Slow down your network

Resources referred:

<https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more>