Networking and Server Attacks

Interception Attacks

- Man-in-the-Middle
  - Between two hosts
- Man-in-the-Browser
  - Between the browser and underlying computer, usually by Trojan-installed extension
- Replay Attacks
  - copies credentials or session token

Poisoning Attacks

- ARP Poisoning
  - "Yep, I'm x:x:x:x! I promise!", "you hear that guys, he's x:x:x:x!"
- DNS Poisoning
  - can be performed locally or at a higher echelon
  - "Yep, x.x.x.x is the ip of foo.com!", "you hear that guys, x.x.x.x is foo.com!"
- Privilege escalation
  - exploits vulnerabilities in a trusted process
  - or, hijacks control of a horizontal *other* user

Server Attacks

- Denial of Service
  - overwhelms a server by saturating its resources
  - DDoS - performed by a botnet
  - Smurf attack - spoofed echo request with target as `from`
  - DNS amplification - pretend like the target is asking for DNS lookups
  - SYN flooding - spoofed with bogus IP, asks target to sync with it - forever waiting for ACK
- Hijacking
  - Session hijacking - stolen session token - via XSS, MITM, or guessing
  - URL hijacking - aka "typo squatting" - also "bit squatting"
  - Domain hijacking - attacker somehow changes DNS record
  - Clickjacking - Zero-pixel element in HTML
- Overflow Attacks
  - Buffer overflow - bleed out a buffer, and write an instruction into forbidden memory space
  - Integer overflow - goes negative
- Advertising Attacks
  - Malvertising - poisoned ads; using ads to distribute malware
  - Ad Fraud - forges / spoofs "clicks" to steal revenue
- Exploiting Browser Vulnerabilities

  - Extensions, plugins, add-ons
  - Extensions affect a single site, FIXME check graph
- Zero-Day Attack - nobody saw it coming, because nobody knew the vulnerability existed

Web Server Application Attacks

- Cross-Site Attacks
  - Cross-Site Scripting (XSS) - attacker's facebook bio is a script, and victim looks at their profile
  - Cross-Site Request Forgery (XSRF) - Clicks on threat agent's web page (with CORS enabled) and obtains their previous session tokens
- Injection Attacks
  - SQL Injection - unsanitized input that's used in a SQL query can have its command overridden