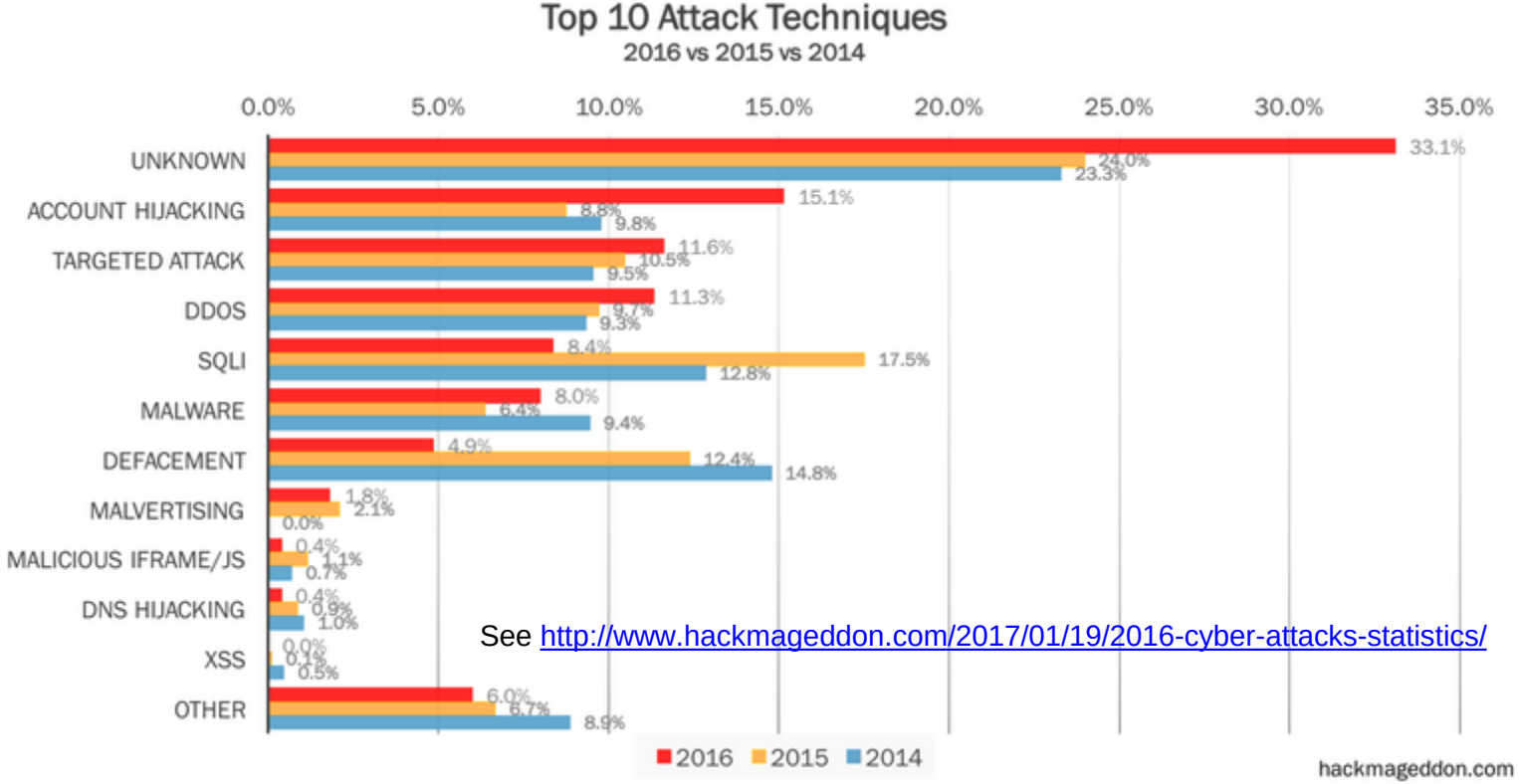
T54B417 Advanced Information Security

Introduction to PART 2: ATTACKING/DEFENDING

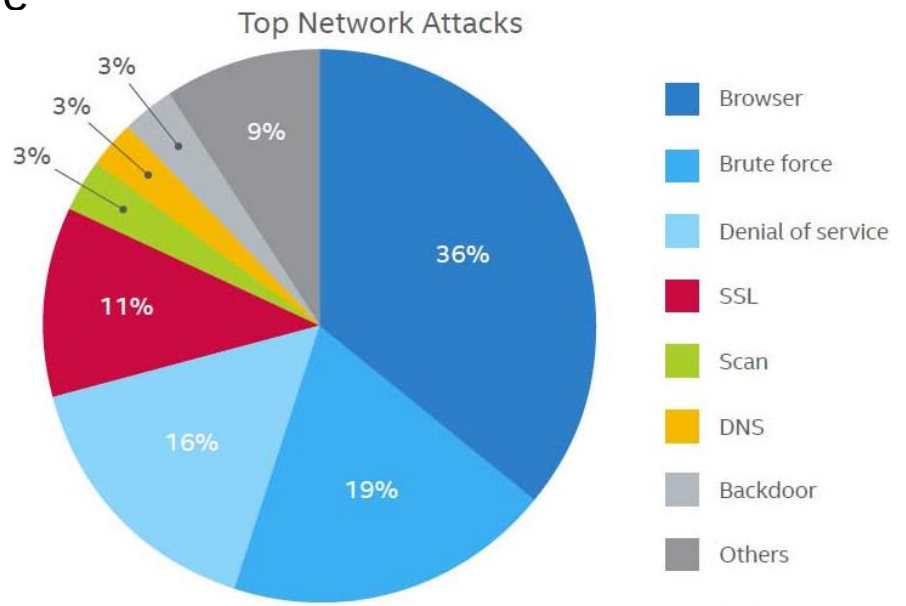
Matti Juutilainen
Mikpoli, MB311
Matti.Juutilainen@xamk.fi

The purpose of part 2

- The idea of the part 2 is to **build deeper understanding** of a specific attack type
  - How exactly it works?
  - What prerequisites are needed to get it work?
  - What kind of tools there are available to actually attack a target?
  - How do you use the tools?
  - How can you defend against the attack?
- A practical case: actually **test the attack in action** and see **how to defend**
- This is a good chance to **develop your practical skills** on security, networking and using the attack (audit) tools!



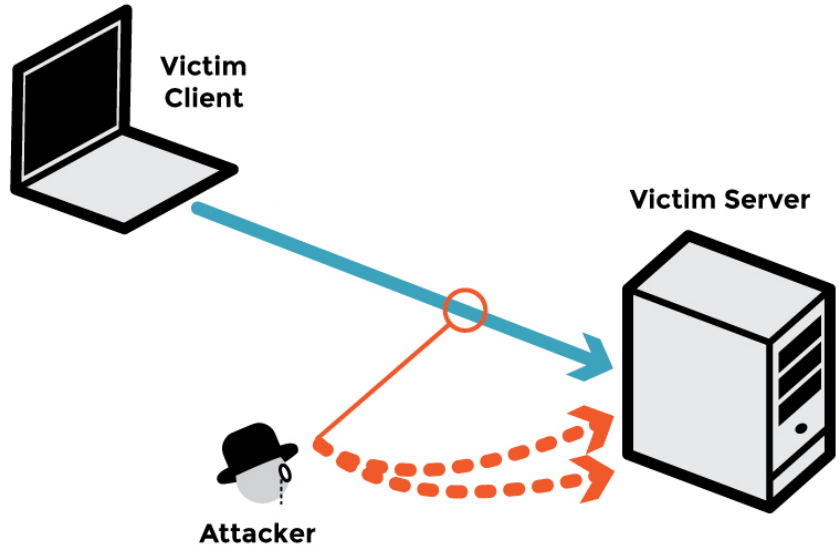
See http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/



See for example,
http://www.digitalattackmap.com/
https://cybermap.kaspersky.com/
http://map.norsecorp.com/
https://www.fireeye.com/cyber-map/threat-map.html
https://threatmap.fortiguard.com/
…

Task 1. Background work

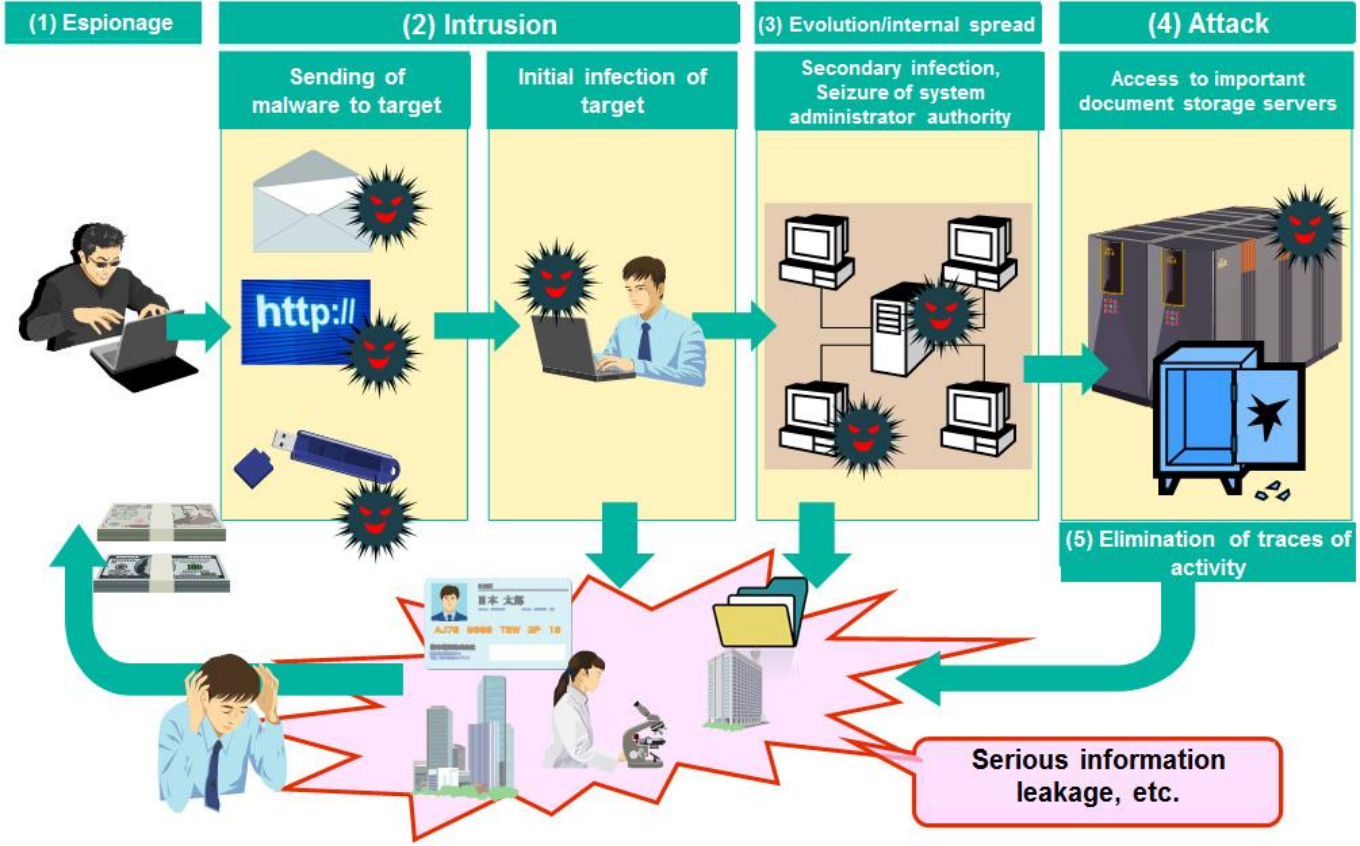
- Investigate the CCNA security materials, Google around etc. and get yourself familiar to different attack types
- **Select some attack(s) that you think can be implemented in practice** with our resources
  - Based on your interests, you can concentrate on wireless/cable networks, our Cisco device(s), Windows/Linux desktops/servers
  - You can use the Best Education Inc. network as a target, or you can implement a new network based on the needs
- Describe the **goal** of the attack: What does the attacker gain with this attack?
- Investigate and describe the **attack process** deeper
  - How exactly the attack works? What steps need to be carried out?
  - What kind of devices/protocols/software/configurations/vulnerabilities are required for the attack to work?
  - What kind of knowledge is required from the attacker?
  - **Go all the way to the details!**



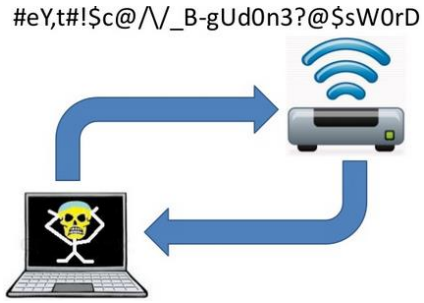
- **Outcome**: a report describing the **attack type**, **requirements for success**, **goals** and the theoretical **attack process** in detailed steps

Task 2. Attack plan

- How do you **actually** implement the attack?
- What **resources** you need?
  - What kind of a network environment?
  - What kind of hosts?
  - What kind of operating systems and software?
- What **tool(s)** you need?
  - Download the tools and learn how to actually use them (don't practice in public networks!)
- How do you **configure** the tools/environment?



- Also consider **how you can defend** against the attack?
  - What are the security configurations/solutions that help protecting against the attack?



- **Outcome**: continue the report from the previous part and include a **practical plan for the attack and defence**

Task 3. Attack!

- With your plan, **deploy the attack in practice IN A CONTROLLED ENVIRONMENT** (**=MB316**)
  - In any case, **DON'T DO THIS IN A PUBLIC NETWORK!**
  - You can (and in some attack types, should) use (earlier prepared) virtual machines
  - Document the attack process, your experiences and results

- Also **test the defensive configurations in practice**
  - Harden the target with the planned protective measures
  - Repeat the attack and see how the added protections affect the attack process

- **Outcome**: continue the report from the previous part and add description of your **attack process**, **experiences** and **results** (including **screenshots**). Also document the applied **defensive mechanisms** and how they affected the attack process.

What?!? Where do I start?

- Form a **group of 2-4 people** (or do it **yourself**)
- Check some **materials**
  - CCNAS: https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html
  - Network security threats and solutions: http://www.computernetworkingnotes.com/ccna-study-guide/network-security-threat-and-solutions.html
  - Common Vulnerabilities and Exposures: http://www.cvedetails.com/, http://cve.mitre.org/
  - CERT: http://www.cert.org/
  - Hacker tools top ten: https://www.concise-courses.com/hacking-tools/top-ten/
- Go learn and test it: https://www.hackthissite.org/

- In practice?!?
  - IP, ICMP, TCP, UDP, SNMP, SMTP, HTTP, CDP, DTP, 802.1Q, ARP, RIP, EIGRP, OSPF, WEP, WPA, WPA2, KRACK, EAP, DHCP, DNS, DB, RADIUS, AD, DoS, DDoS, FTP, Telnet, SSH, SSL, IPsec, VPN, NTP, IDS, IPS, firewall, ACL, IOS, Windows, Linux, virus, trojan, worm, backdoor, malware, sniffing, spoofing, poisoning, scanning, accounting, authentication, authorization, certificates, hash, permissions, Kerberos, PKI, handshaking, flooding, congestion, performance, convergence, competition, eavesdropping, smurfing, modification, compromise, password strength, brute force, dictionary attack, hub, switch, router, wireless ap, …

Tunne huominen - All for the future.