Offensive technologies
Fall 2016

Class 9

Final report

Final report

- ***Write a report in which you provide a thorough description of***
  - **Analyst track →** all the exploits you prepared: 0-day Linux, HT, NSA, etc.
  - **Tech. track →** all the attack scenarios you prepared (you will show them in the final demo as well)
- ***Format***
  - IEEE layout (two columns)
  - Final report < 6 pages
    - This is an upper bound, not an expectation in length.

Analyst track: structure of the report

- ***For each exploit***
  - **Introduction**
    - A very brief “abstract” of an exploit to be described (e.g. 200-300 words)
  - **Technical analysis of the exploit**
    - Analysis of the source code of the exploit
    - Description of target environments
    - Detailed description of possible exploitation scenarios
    - Possible detection/evasion techniques
  - **Analysis of the social and financial impact**
    - Number/types of potential victims (e.g. from the media, prev. reports,..)
    - Potential impact on individual person/society/nation
  - **Compare and rank exploitation techniques and sophistication**
    - Exploit adapts to several scenarios/exploit execution varies etc.
    - Possible detection/mitigation techniques?
- ***Final summary table comparing each exploits in terms of***
  - **Vulnerability type**
  - **Exploit sophistication (description)**
  - **Exploit sophistication (rank)**
  - **Known Victims/targets**

Tech. track: structure of the report

- *For each attack*
  - **Introduction**
    - A very brief "abstract" of an attack to be described (e.g. 200-300 words)
  - **Technical description of each vulnerability used in the attack**
    - Analysis of the vulnerable source code
    - Why the attack is possible?
  - **Description of the target environment(s) that will be affected by the attack**
    - Roles → attackers, victims, intermediaries
    - OS, versions of vulnerable software, other prerequisites
  - **Detailed description of the attack scenario**
    - Attack development
    - Manual steps to reproduce against target environments + how it is automated
    - Improvement over "vanilla" exploits (e.g., found on Exploit DB)
    - Details on replication on "slightly" different target environments (e.g., older/newer versions of vulnerable software)
- *Replication guide*
  - **Schematic description of how to replicate your environment (installed software, specific configurations, exploitation code, automation code, etc.)**