|  |
| --- |
| Ročník 2022 |
| Threat modeling |
| Autori: Samuel Sedlačko |

Threat modeling je proces, pri ktorom sa odhaľujú zraniteľnosti (ang. „vulnerabilities“) počítača, servera alebo sietí, aby sa predišlo možným útokom na tieto zariadenia a následným únikom dát alebo získaniu nepovoleného prístupu. Následne ľudia, zhotovujúci tento model, hľadajú efektívne riešenia na opravu týchto problémov alebo zraniteľností.

Študijný program je určený pre úplných začiatočníkov, alebo ľudí, ktorí už majú nejaké znalosti ohľadom tejto problematiky. Pozostáva zo siedmich modulov, ktoré vysvetľujú základy tvorenia týchto modelov. Trvanie tohto kurzu je odhadované na 3 h 12 min. Vysvetľuje, ako fungujú procesy, ako sa dáta premiestňujú, čo sa s nimi počas rôznych procesov deje a ukazuje aj techniku zapisovania do nákresu. Pri zápise do nákresu ukazuje jeho vrstvy (ang. „layers“), čo znamenajú, poprípade aké informácie sa doň uvádzajú.

Vrstvy (Layers):

* Layer 0 – The system layer
* Layer 1 – The process layer
* Layer 2 – The subprocess layer
* Layer 3 – The lower-level layer

Uvádza aj kategórie nebezpečenstiev (ang. „threats“), ktoré hackeri používajú na získanie prístupu alebo dát. Posledné moduly sa venujú stanoveniu priority na opravu a aj odporúčaniu softwaru na tvorbu nákresov. Uvádza sa tam najmä program Microsoft Visio. Kurz je výborne spracovaný nakoľko sa účastník tohto kurzu naučí základy a pochopí časté pojmy používané v tomto odvetví. Každý modul obsahuje aj časť „knowledge check“, pri ktorom sa účastník otestuje, či pochopil správne danú lekciu.