|  |  |  |  |
| --- | --- | --- | --- |
| **Component** | **Plan** | **Resources** | **Time** |
| Bridge-in: | Why network security matters in the real-world | Examples of real-world network security attacks | 2 |
| Learning objectives | Present learning objectives for microlectures (pre-requisites) + game. | Netsim instructor notes for games’ LOs + Miti’s slides for LOs for pre-requisites | 2 |

|  |  |  |  |
| --- | --- | --- | --- |
| **What I will do as a facilitator** | **What my learners will do** | **Resources** | **Time (minutes)** |
| Present networking pre-requisites (packets, protocols, IP). Run Q&A | Listen to my microlecture. Participate in Q&A. | Slides with analogies / examples | 4 |
| Present security pre-requisites (attacker, threats, threat types). Run Q&A | Slides with definitions & examples | 5 |
| Address learners’ questions on the game | Play Netsim games in the ‘*Basics’* level | Web browser to play Netsim. Register & login | 7-10 |
| Walk through *Stealing Packets* game, asking & soliciting questions | Listen & participate in Q&A. Draw a switch table. Write to and read from it as simulation progresses. | Pause *Stealing Packets* game at various stages of simulation. | 12-15 |
| Post-assessment: Run TPS activity on threat types. Segue into next class for interruption threats. | TPS: Classify *Spoofing* & *Stealing Packets* games into threat types. Listen to wrap up. | Slide on threat types as a reminder. Pen & paper / Poll. | 3-5 |

Extending Netsim:

* Improve abstractions (e.g. IP addresses instead of names).
* Tweak RHS panel to include networking / security prerequisites.
* Tweak success message to include takeaways.
* Use Netsim to teach other protocols (e.g. DNS) and demonstrate attacks against them (e.g. DNS poisoning)
* Extend Netsim to other types of attacks (e.g. side channels)
* Motivate defenses (e.g. IP spoofing and IPSec)
* Motivate networking commands (e.g. traceroute activity).
* Play Netsim before preparing for CTFs.