MITRE | Engage™

MISSION ESSENTIAL TASK LIST (METL)

The following is intended to serve as an exemplary METL for a generic adversary engagement team. The METL is made up of a series of Mission Essential Tasks (METs). These tasks are the core activities that must be completed during the planning, execution, or analysis phases of an engagement operation. These METs should drive progress towards the operational outcome.

- Establish Gating Criteria
  - Identify exit criteria and appropriate escalation procedures
  - Define operational success
  - Establish acceptable level of risk
  - Define acceptable response time
- Create Engagement Narrative
  - Create persona(s)
  - Determine storyboarding
  - Select pocket litter
  - Define pattern of life for persona(s)
- Establish Monitoring System
  - Build out the collection system
  - Include/establish dashboards for default searches/queries
  - Establish additional systems needed for monitoring
- Build Out Victim Windows System
  - Build computer/system(s) to meet the mission objective/requirements
  - Use Microsoft Deployment Toolkit for operating system deployment
  - Use tools for software provisioning, configuration management, and application-deployment (e.g. Ansible)
- Build Out Victim Linux System
  - Same as Windows but Linux specific
- Deploy Monitoring System to Engagement Environment
  - Deploy collection system
  - Establish security controls
- Deploy Persona(s) and Deceptive Assets to Engagement Environment
  - Build active directory, file/app server
  - Connect client to environment
  - Litter both server and client(s)
  - Establish connectivity that aligns with storyboard and persona(s) (i.e. teleworker with a VPN)
- Monitor Operational Activity
  - Conduct overwatch and observation
  - Identify basic persistence
  - Identify network activity of interest
  - Identify probable lateral movement
- Forensically Investigate Victim Post Operation
  - Collect disk and memory image
  - Process disk/memory image in to establish timeline of artifacts (e.g. log2timeline/plaso)
- Analyze Data from Live Operation and Forensic Investigation
  - Identify artifacts from live operational data in the post-op at rest data
  - Document findings
  - Inform existing threat model and CTI data
- Conduct Open-Source Intelligence (OSINT) Searches Pre/Post Operation
  - Search for related network activity (ip/domain)
  - Search for related on-system activity (e.g. persistence mechanism)

✉ **engage@mitre.org**

engage.mitre.org

in **@ MITRE Engage**

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2022 MITRE PR_21-01759-11 2-28-2022 VERSION 1.0