UTSA CCDC Red Team

# Documentation Policy

Documentation is an integral part of Red Team engagements. Proper documentation allows both you and your team a better understanding of the steps each individual takes during the lifecycle of a penetration test (Reconnaissance, Exploitation, and Post- exploitation). With your involvement in Red Team at UTSA, you will be expected to take detailed notes during engagements and contribute write-ups as a part of team resources. Write-ups and knowledge sharing are a vital part of a thriving learning environment and result in a stronger team and community.

## Documentable actions include (but are not limited to):

### Executive Summary

* Simple, high-level summary
* Briefly explain any successful actions

### reconnaissance / scanning

* Potentially vulnerable web services
  + Text fields (code injection/non-sanitized input)
  + Note all meaningful findings through web scanning tools like nikto
    - XSS, CSRF, SQL Injection, Etc.
* Potentially exploitable requests (use web request intervention tools like webscarab)
  + Modifiable fields and values that could/have led to exploitation
* Document **how** you **scanned** and **what** you **found** including:
  + Open ports
  + Vulnerable services
  + Operating system types
  + Operating system versions

### Successful Exploitation attempts

* Note **successful exploits** (note what exploit you used, tools, commands/flags, etc)
  + Services
    - Shells, remote logins, etc.
  + Web
    - Dumped databases, RSA keys, defaced websites
  + Social engineering
    - Passwords not given to you
    - Information received from overhearing, spying, etc.
      * Potential passwords/encryption methods, etc.

### Post-Exploitation

* Persistence obtained
  + Metasploit/meterpreter persistence
  + Post exploitation frameworks like Empire
  + Persistence scripts
  + Persistence through services
  + Etc.
* Key-logging
* Remote system modifications
* Passwords/hashes/keys obtained
* Any other meaningful information/actions taken post-exploitation

### Fails / Lessons Learned

* Justify **unsuccessful** **attempts** at exploitation
  + Explain why you thought an attempt would work
  + Use logic
  + Think before just throwing scripts at a target

#### INclude Anything else you may consider important that is not described here or explicitly outlined in documentation templates