**Goals**

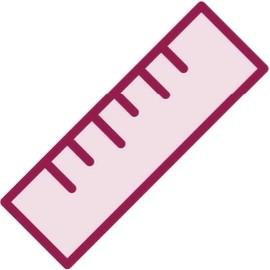
* An achievable outcome
* Should be SMART
  + Specific
  + Measurable
  + Ac hieva ble
  + Realistic - Win – Win( buyer)
  + Time-bound ( 12- 15 days)

(

**Objectives**

* How we achieve our goal
* Actionable steps
* Determine the types of attacks that mitigate the risk identified by the goal

**Scope of Work**

* Identify resources and end-points that will be targeted
* \*.cleanaway.com.au ( in scope)
* Dev.cleanaway.com.au ( out scope)
* What is out of scope?
* Destructive attacks
* DDOS -attack
* Weekend
* Working on the scope directly impacts your statement of work

**Budget**

#### Based on the scope

#### 4 server , 50 ws = 1 lac

#### 8 server – 200 ws = 3lac

#### 20 k + 1 lac + 2 lac

* + Based on your rates
  + Scope may change as a resuIt

**Schedule**

* Availabi lity of environment / end-points
* Availability of company resources
* Agreed upon timeframes for attack -
* Your availa bility – 9 – 5 pm : Contact point:
* Budget and scope play are considered as well

**Communications Plan**

* + Point of contact for support
  + Escalation path for reporting critical issues
  + Where to report illegal activity
  + Who gets the fina l report? –
  + Two-way street

**Project Note Taking**

* + - Clear and concise phrases
    - Write the notes based on your understanding of what was said
    - IT head – manager C level man
    - Use heading, bullets,or numbered lists to create sections
    - Underline or "star" items of importance
    - \*\* immediate ac
    - \* 30 days

\*\*

**Pen Test Note Taking**

* + - * Evidence
      * Steps to recreate the attac k
      * Organize by tools used
        + Capture commands/scripts used
        + Any significant results
        + Screenshots
        + Video

**Confidentiality**

* Notes you take demonstrate vulnerabilities
* Must be encrypted,if kept online
* Can only be shared within the scope of the signed Non-disclosure agreement
* ( NDA) :

**Note Requirements**

* + Digital (preferred)
  + Hierarchical
  + Searchable
  + Support for multiple media types
  + Access from anywhere
  + Secure

( -pass )

**Notes Applications**

* Cherry Tree
* Trilium Notes
* Microsoft OneNote
* Many, many others,including Typora, Trilium, Joplin,and KeepNote
  + Documents
    - Non-disclosure Agreement (NDA)
    - Master Service Agreement (MSA)
    - Statement of Work (SoW)
    - Rules of Engagement (RoE)
    - Communications Plan

**Legal Requirements**

* Protects pen tester and client
* Allows client to share privileged details

**Project Requirements**

* Determines what 's in scope
* Establishes work standards

**Pre-engagement**

### Non-disclosure

* Master Service Agreement

**Engagement**

## Statement of Work

* + Rules of Engagement

**Details of an NOA**

* + Defines what information is covered

###### Obligations for both parties

* + Scope of information
  + Lengt h of time
  + Exclusions

- Remedies - Mitigation

**Statement of Work**

* Defines the pen testing activities
* Can include time and pricing information

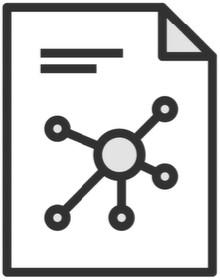
# ---

------

---

**RoE Details**

* In-scope attack surface
* Out-of-scope items
* Disclaimer
* May incorporate a communications plan
* Client acceptance of terms

**Communications Plan**

* Defines a clear path for communication
* Includes different levels of communication
* Should be agreed upon with the client

**Points of Contact**

* + General support and assistance
  + Critical issues
  + Reporting illegal activity
  + Who gets the report
  + Cloud Provider