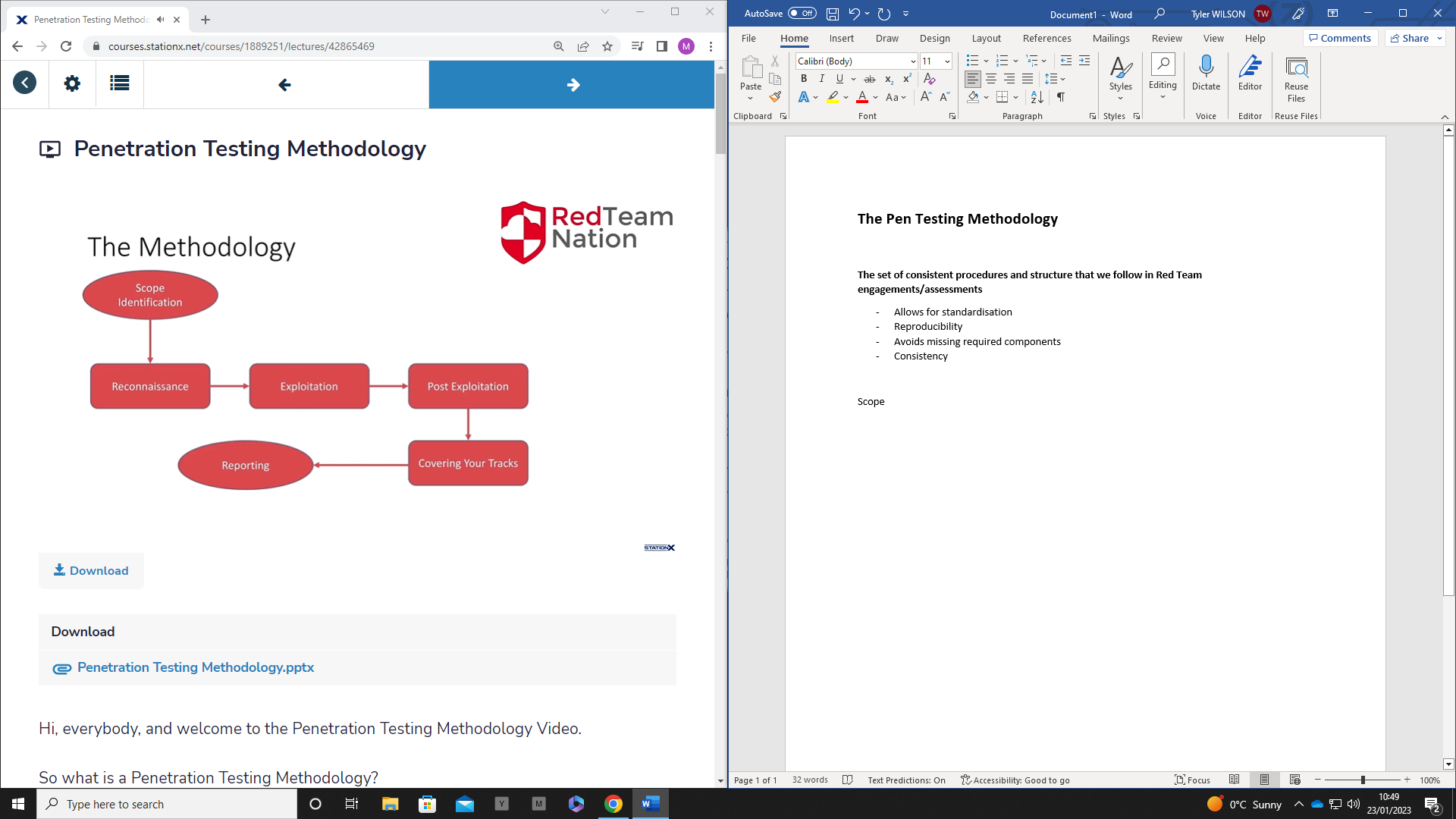
**The Pen Testing Methodology**

**The set of consistent procedures and structure that we follow in Red Team engagements/assessments**

* Allows for standardisation
* Reproducibility
* Avoids missing required components
* Consistency



Scope Identification 🡪 Reconnaissance 🡪 Exploitation 🡪 Post-Exploitation 🡪 Covering Steps 🡪 Reporting

**Scope Identification**

Understanding what could happen during an engagement

* Goal identification
* Stability and service consideration
  + Maybe the java service that is temperamental when receiving a lot of traffic
* Route of engagement

**Reconnaissance**

* Enumeration
* Active or Passive
  + Running scans
  + Vs using google
* Scanning
* Identifying all the information that you need for the exploitation

**Exploitation**

* Validating findings found in the reconnaissance
* Exploiting the target, gaining control
* Ensuring stability and persistence

**Post-Exploitation**

* Based on getting full access to machine (root or admin)
  + Privilege escalation
* Persistence
* Moving laterally
  + Being able to move from one device to another
* Looking for good stuff

**Covering Your Tracks**

* Wiping logs
* Hiding persistence
* Cleaning up
  + If you change a password/configuration, it must be cleaned up
* Log files and their location
* Is it required?
  + Sometimes clearing files will indicate your presence more

**The CIA Triangle**

**Confidentiality**

* Controls the access of information
* Commonly called authorisation
  + No unauthorised access

**Integrity**

* Ensuring the data itself is trusted and accurate at all times
  + If you can’t trust the data you’re accessing, what use is it

**Availability**

* If the data is unavailable, it’s useless
* DDOS attack
* Disaster Recovery Plan (DRP) is crucial for this step so everything can be mitigated and brought up quickly