**Module 1 Threats, Attacks & Vulnerabilities**

**1.3 Threat Actor Types & Attributes**

**Threat/Threat Actor**

* Potential occurrence that can result in undesirable outcomes
* Person/thing likely to cause damage/danger
* *Threat Actor* is person/entity responsible for event/incident that impacts/has potential to impact, the safety/security of another entity

**Types of Threat Actors**

* Script Kiddies

1. Derogatory term for people who use hacking techniques but have limited skill
2. Such attackers often rely almost entirely on automated tools they download from internet

* Hacktivist

1. Person who uses hacking techniques to accomplish some activist/political goal
2. Usually seeking to deface websites

* Insiders – internal employees seeking to cause damage to their organisation
* Organised Crime – organised groups seeking to steal money, identities or corporate secrets
* Competitors – outside organisations seeking to commit corporate espionage for financial/market gain
* Nation States – countries sponsoring illegal/fraudulent actions
* APT (Advanced Persistent Threat)

1. Attack where unauthorised persons gain access to network using advanced exploitation techniques & stays there undetected for a long period of time
2. Intentions of APT attack is to steal data rather than cause damage to network/organisation

**Deep Web/Dark Web**

* *Deep Web* is anything on internet that search engine can’t find
* *Dark Web* is part of Deep Web internet that Is only accessible by means of special software (TOR), allowing users & website operators to remain anonymous/untraceable
* Dark Web Market – part of Dark Web often illegally selling goods, merchandise, data/information or services

**Open Source Intelligence (OSINT)**

* Open-Source – any information that readily available to anyone (eg. Newspapers/news sites)
* Intelligence – collection of information of military, political, organisational or financial value
* Websites & tools that allow you to gather information on current threats/specific security issues

1. ThreatCrowd, OpenPhish, OSINT Framework, Shodan

**Attributes of Threat Actors**

* Internal/external – access
* Level of sophistication – knowledge
* Intent/motivation
* Resources/funding