**Module 1 Threats, Attacks & Vulnerabilities**

**1.4 Penetration Testing Concepts**

**Penetration Testing**

* *Penetration Test/Pen Test* is authorised, simulated attack on computer system, performed to evaluate security of system by actively exploiting found vulnerabilities
* AKA Ethical Hacking

**Penetration Test Requirements**

* Scope document of what will be tested
* Permission to test (get-out-of-jail-free-card)
* Skills to attack resources limiting harm/collateral damage
* Plan of attack/steps
* Resources & access to conduct test

**Information Gathering/Discovery/Reconnaissance**

* Passive Reconnaissance

1. Attempt to gain information about targeted computers & networks w/o actively engaging with systems
2. Eg. Collecting information from public databases, talking to employees/partners, dumpster diving etc.)

* Active Reconnaissance

1. Gathering information about targeted systems by actively engaging with targeted system
2. Directly focuses on system (port scans, traceroute information, network mapping, vulnerability scanning) to identify weaknesses that could be used to launch attack

**Types of Testing**

* Black Box – tester has absolutely no knowledge of system & functioning in same manner as outside attacker
* White Box – tester has significant knowledge of system. Simulates attack from insider (rogue employee)
* Grey Box

1. Middle ground between first 2 types of testing
2. Tester has some limited knowledge of targeted system

* *Nonintrusive Tests* involve passively testing of security controls – performing vulnerability scans & probing for weaknesses but not exploiting them
* *Intrusive Tests* involve actually trying to exploit vulnerabilities to break into network

**Penetration Test Activities**

* Initial Exploitation – gain foothold on system/network often with lesser privileges/access
* Pivot – attacking system using another, compromised system that’s trusted to one you attacking, often done on same network through *Island Hopping*
* Persistence – maintaining access for period of time/hiding
* Escalation of Privileges – gaining elevated privileged access to resources that are normally protected from app/user

**Penetration Testing vs. Vulnerability Scanning vs. Risk Assessment**

* Penetration Test – see above definition
* Vulnerability Scanning

1. Allows tester to identify specific vulnerabilities in network/system/app
2. Most pen testers will start with this procedure so they can identify likely targets to attack

* Risk Assessment – allows organisation to understand the cybersecurity risk to organisational operations (including missions, functions, image or reputation), organisational assets, systems or individuals