s2 topics for in details reading

Penetration testing

**Intro**

* A penetration test, also known as a pen test , ethical , white hat hacking
* A way to expose potential weakness
* Evaluating the system security
* Penetration tester use same tools techniques, and processes as attackers but the motive is different
* Follow Defensive strategy

**Why it needed?**

* **Test Security Control**: Overall health of applications, networks and physical
* **Ensure Compliance**: Maintain Security standards
* **Real world vulnerabilities**: Exposing weakness of the computer system
* **Handle break-in**: Help organizations to handle any type of break-in from a malicious entity

**Phases of penetration testing**

* Reconnaissance (gathering information without direct interaction e.g using whois software)
* Network scanning (Scanning network to check live hosts and pen ports e.g. using nmap )
* Vulnerability Testing (To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities. e.g. using Nessus)
* Analysis (To organize and document information found during the reconnaissance, network scanning, and vulnerability testing phases of a pentest. E.g using Dradis)

**Types of penetration testing**

* Black Box penetration testing
  + Where the tester provided with the minimum amount of information
  + For example the company name
  + It is best suited for the mature kind of environment
  + Tester spend more time in learning the environment
  + That could be spent on testing for potential weakness
* Grey Box penetration testing
  + The tester is provided with a bit more information,
  + For example, such as specific hosts or networks to target
  + In this types of testing the idea about target attack is provide
  + No need to spent much time on collecting the information about environment
* White Box penetration testing
  + The tester is provided with the detailed information ,
  + For example,  internal documentations, configuration plans, etc.
  + Tester can spent more time focused on exploiting issues rather than performing host enumeration and vulnerability scanning

Tools:

* NMAP.
* Metasploit.
* WireShark.
* Burp Suite.
* Nessus

Honey Pots

**Intro**

Honeypots is a network-attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by hacker

**Working**

A honeypot is a cybersecurity mechanism that uses a manufactured attack target to lure cybercriminals away from legitimate targets. They also gather intelligence about the identity, methods and motivations of adversaries

**Types (Implementation bases)**

Physical Honeypots

* **A physical honeypot is running on a real machine connected to the network using its own assigned IP address**

Virtual Honeypots

* **A virtual honeypot is a fake network designed by computer experts to catch hackers and examine their methods of attack.**

**Types (Interaction level bases)**

High Interaction Honeypots

* A high-interaction honeypot allows attackers to compromise or gain access to the system.

Low interaction Honeypots

* A low-interaction honeypot simply captures connection attempts and alerts the security team an intrusion has been attempted

**Types (Purpose bases)**

Production Purpose

* A production honeypot is a type of honeypot that’s used to collect cybersecurity-related information within a business’s or organization’s production network.

Research Purpose

* A  type of honeypot that’s used to collect information about the specific methods and tactics hackers use.

e.g military, researcher, government organization

**Why should an organization use honeypots?**

* Divert Malicious Traffics from important system
* Get an early warning before critical system are hit
* Gather information about attacker and their method
* Cost Effective