Introduzione

In cybersecurity, ci sono almeno 5 aree esterne differenti che si mischiano fra loro, e poi 3 aree interne relative all'hardware ed al software.
"L'attore principale" sono applicazioni Internet-based:

- vulnerabilità del sistema, della rete etc
- come difendersi o evitare tali vulnerabilità, o almeno mitigarle

Molta configurazione pratica: laboratori da 0, ma è utile rifare tutto a casa (**CAZZI**).
Per via del fatto che è davvero difficile oggi separare cosa è la rete da cosa è il software, è utile parlare di tutti i diversi campi che riguardano sia la rete che il software.
Punti chiave:

- Access networks and perimetral security: Ethernet, VLAN, IPv6, 802.11x, firewall, packet classification algorithms
- Core networks: BGP, MPLS, DDos e Botnets, VPNs con BGP
- End to End security: PKIs, DNS security, HTTPS, Overlay VPNs
- Sw and Operating System
- Virtualization & Cloud

Piattaforme da utilizzare per la parte da 6 CFU (Hardware):

- GNS3
- Tinycore Linux
- VMware o Virtual Box: Virtual Box sembra lavorare meglio con GNS3
- Cumulus Linux: serve per emulare le funzionalità di livello 2 di uno switch. Net OS, **scaricare la versione 4.1** e non le ultime. C'è un insieme di VM pronte per essere installate su un virtualizzatore
- Immagini CISCO (da cercare online, if you know what I mean)
- Lubuntu
- Ubuntu server

Capitolo 1

Introduzione alla cybersecurity

Ci sono 3 fattori principali quando si parla di cyberscurity:

- Cosa bisogna proteggere?
- Da quali minacce? Ci sono diverse fonti di attacco da cui proteggersi
- Come fare per contrastare queste minacce? Integrità, encryption, etc...

Definizione di computer security: le misure ed i controlli che garantiscono confidenzialità, integrità e disponibilità degli assets dei sistemi informativi, incluso hardware, software etc...

- confidenzialità: i dati sono privati, le informazioni confidenziali non sono note ad entità non autorizzate. Esempi: usare SSH o HTTPS per scambiare credenziali con un server.
- Privacy: assicurarsi che gli individui controllino o influenzino quale informazione è legata a loro potrebbe essere raccolta e a chi potrebbe essere rivelata;
- Integrità: se dei dati, indica che essi sono cambiati solo in maniera autorizzata. Se voglio traferire un messaggio con cui trasferisco del denaro, non voglio che il contenuto sia compromesso. Se si parla di integrità dei sistemi, si intende che il sistema performi, che sia libero da una manipolazione dello stesso;
- disponibilità: si assicura che il sistema lavori in maniera corretta e che i servizi non siano negati ad utenti autorizzati. In infrastrutture critiche, la disponibilità può diventare di gran lunga l'obiettivo di sicurezza più importante

Altri aspetti importanti:

- Authenticity: dell'utente, indica che sia possibile verificare che l'utente è chi dice di essere. Della sorgente: capacità di verificare che un messaggio arriva da una sorgente effettivamente affidabile.
- Controllo d'accesso (autorizzazione), ovvero l'abilità di verificare che l'utente ha il permesso di effettuare alcune attività;
- accountability, ovvero poter tenere traccia delle azioni di qualche entità, incluso la possibilità di salvare tali attività in un file di log per analisi forensi successive;
- adversary: individuo, gruppo governo... che vuole condurre attività dannose

- contromisure: un dispositivo o tecnica che ha come obiettivo la prevenzione di spionaggio etc...
- rischio, ovvero una misura di quanto una entità sia minacciata da potenziali eventi
- policy di sicurezza, quindi un insieme di criteri per fornire servizi di sicurezza
- risorsa di sistema: un'applicazione major, un supporto generale al sistema, un programma ad alto impatto ...
- minaccia (threat): una qualunque circostanza o evento col potenziale di impattare in maniera avversa delle organizzazioni
- vulnerabilità: debolezza di un sistema informativo, procedura di sicurezza ...

Quali sono le diverse superfici di attacco:

1. la rete stessa: i sistemi sono Internet-based, quindi è sempre possibile attaccare la rete. Attaccare la rete implica sfruttare vulnerabilità della rete Internet: ARP, WEP, link fisici, intrusioni nella rete etc...
2. attacchi al software: vulnerabilità nell OS, server web, code injection etc...
3. attacchi all'umano: molte vulnerabilità create da noi stessi, social engineering, errori umani, mancanza di competenze etc...

È importante non pensare che la sicurezza sia data solo dalla tecnologia, ma anche dalle persone.

CIS critical security controls: 20 applicazioni pratiche che la SANS suggerisce di applicare per verificare la sicurezza di una corporation (anche piccola Enterprise). Ogni controllo ha dei sotto-controlli più "concreti"
Quindi, non avendo il tempo di fare tutto, ci concentrare su alcuni aspetti fondamentali di tutto l'insieme visto.