Pràctica 1c:

Els objectius de la pràctica **m11uf2pr1c** són:
a) Aprendre quines són les fases típiques d'un atac informàtic (Anatomi d'un atac informàtic)
b) Trobar les mesures preventives i paliatives contra aquests atac.
c) Reconeixer i utlitzar algunes de les eines utilitzades per realitzar un atac informàtic
d) Reconeixer i utlitzar algunes de les eines utilitzades per prevenir i paliar un atac informàtic

Exercici 1: Questionari

1- Troba quines són les fases d'un atac informàtic
2- Quins són els objectius de la fase de reconeixement? Quines tèniques habituals s'utilitzen?
3- Quins són els objectius de la fase d'escanneig (o exploració)?. Quines tèniques habituals s'utilitzen?
4- Quins són els objectius de la fase d'intrusió? Quin altre nom pot tenir?. Quines tèniques habituals s'utilitzen?
5- Quin és l'objectiu de la inserció de malware o codi maliciós, un cop s'ha passat la fase d'intrusió?
6- Quins tipus de malware existeiexen?
7- Quin és el propòsit de la darrera fase d'un atac informàtic?, Com es pot dur a terme aquesta fase?
8- Indica quins són els aspecte de seguretat que poden quedar compromesos per un atac informàtic?
9- Quines són les contramesures bàsques per fer front a la Ingenieria social?
10- Quines són les contramesures bàsiques per fer front a les violacions de seguretat provocdes per Factor Insider (personal propi de l'organització)?
11- Quines són les contramesures bàsques per fer front al malware o codi maliciós?
12- Quin és el principal problema de les contrasenyes? Què es pot fer per millorar-les?
13- Quin és el principal problema d'una configuració predeterminada?. Quines contramesures es poden utilitzar?
14- Quina és la problemàtica de l'Open Source Intelligence? Quines contramesures es poden utilitzar?
15- De quina manera es pot detectar el codi maliciós?
16- Què és una eina preventiva?. Indica quines són les principals mesures preventives.
17- Què és una eina paliativa?. roodpkg-trndica les principals mesures paliatives.
18- Com definiries el programa Dell SonicWall Next-Generation Firewall? És una eina paliativa o preventiva?
19- Com utlitzaries les eines d'atac informàtic per fer prevenció?

Exercici 2: Treballant amb l'eina GnuPG i Kali Linux

1- Instal·la la màquina virtual **Metasplotable2-Linux**.
NOTA 1: L'usuari definit és **msfadmin** i la seva contrasenya és **msfadmin**.
NOTA 2: Accés com a root executant **sudo su -** i escribint la contrasenya de **msfadmin**.
NOTA 3: Per canviar la llengua del mapa de teclat executa l'ordre **dpkg-reconfigure console-setup** com usuari **root**.
2- Fes les següent accions:

a) Configura **Metasplotable2-Linux** de manera que treballi amb **xarxa interna**, amb una adreça IP estàtica **192.168.1.3**, màscara **255.255.255.0**, IP de la xarxa **192.168.1.0**, IP de broadcast **192.168.1.255**, IP del gateway **192.168.1.1** i adreces IP dels DNS **80.58.0.33** i **80.58.32.97**.

b) Configura **Kali-Linux** de manera que treballi amb amb **xarxa interna**, amb una adreça IP estàtica **192.168.1.2**, màscara **255.255.255.0**, IP de la xarxa **192.168.1.0**, IP de broadcast **192.168.1.255**, IP del gateway **192.168.1.1** i adreces IP dels DNS **80.58.0.33** i **80.58.32.97**.

c) Comprova la connectivitat entre màquines.

3- Descobreix des de **Kali Linux** i **nmap** tots els servidors de la xarxa a la qual es troba.
4- Descobreix des de **Kali Linux** i **nmap** tots els serveis disponibles del servidor **Metasplotable2-Linux** i el sistema operatiu que utilitza.
5- Descobreix des de **Kali Linux** i **nmap** la versió dels servidors **SSH**, **FTP**, **Apache** i **SAMBA** de **Metasplotable2-Linux**.

6- Des de **Kali-Linux** inicia la **Consola de Metasploit Framenetwork**.
7- Determina els noms d'usuaris existents de **Metasplotable2-Linux** des de **Kali-Linux** per mitjà d'un exploit del servei **SAM RPC** necessari per treballar amb **SAMBA**.
8- Des de **Kali-Linux** i amb el programa **hydra** aconsegueix la contrasenya d'alguns usuaris de **Metasploitable2-Linux**.
9- Des de **Kali-Linux** accedeix a **Metasploitable2-Linux** via **SSH**.

Recursos sobre integritat i autenticació:

a) https://www.sonicwall.com/documents/anatomy-of-a-cyber-attack-ebook-24640.pdf
b) Enllaç apunts IOC (apartat 1.1.2, 1.1.3, 1.2 i 1.3)
c) https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf
d) http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf
e) http://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/

Forma de lliurament del questionari (50%)
1- Examen de **15 minuts** el dia **4-11-2016**

Forma de lliurament de la part pràctica (50%)
1- El lliurament de la pràctica es durà a terme el dia **15/11/16** de **15.00 a 16.00 hores**. Es comprovara:
a) Fer un llistat de tots els serveis i sistema operatiu de la màquina **metasploitable2**.
b) Utilitzar un **exploit** per visualitzar els usuaris de SAMBA de la màquina **metasploitable2**.

.