Pràctica 1d: Tipus de malware. Detecció eliminació de malware. Eines preventives i paliatives.

Els objectius de la pràctica **m11uf2pr1d** són:

a) Identificar els tipus de malware més importants.

b) Detectar o eliminar malware

c) Implantació d'eines i procediments de treball preventius de l'instal·lació de malware dins d'un sistema.

d) Implantació d'eines i procediments de treball palatius després de la detecció de malware dins d'un sistema.

DOCUMENTACIÓ

1- Definició de malware. Tipus

a) Apunts sobre malware de l'Hèctor López

b) Apunts IOC --> Apartat 1.2

2- Enllaços per l'obtenció de mostres de malware

a) http://www.hackplayers.com/2016/10/recopilatorio-de-recursos-de-analisis-malware.html

b) http://www.tekdefense.com/downloads/malware-samples/

c) http://malwaredb.malekal.com/

d) Revealer Keylogger Simplest Keylogger in C

3- Enllaços per l'obtenció de programari de detecció i eliminació de malware. Eines paliatives

a) Apunts IOC --> Apartat 1.3

b) https://www.malwarebytes.com/

c) http://www.kaspersky.es/ , Security essentials , Trend Micro i https://www.bitdefender.es/

d) Antivirus Linux: ClamAv i Clamtk

4- Eines preventives

a) Apunts IOC --> Apartat 1.2

b) Apunts sobre eines preventives de l'Hèctor Lópezap

EXERCICIS

1- Instal·lació de l'antivirus ClamAv per Debian Linux

a) Sobre la màquina virtual **debian-8.6.0-asix2-m06** que utilitzes pel mòdul M06, instal·la la versió de **ClamAv** (paquets **clamav** i **clamtk** per obtenir la interfície gràfica) per **Debian** des dels dipòsits.

b)- Descàrrega el manual de clamav i llegint l'apart 5 (Usage), troba com escannejar el directori **/home** de forma recursiva des del terminal. Comprova l'us de %cpu i %mem que utilitza el programa. Comprova el número de fitxer infectats que ha donat com a resultat.

c) Escanneja el directori personal de l'usuari de treball des de l'eina gràfica **ClamTk**.

2- Instal·lació de malwarebytes per Windows

a) Instal·la les eines **Anti-Malware** i **Ani-Exploit** de **Malwarebytes** (versió **for Home**).

b) Executa **Anti_Malware**. Fes una actualització i un analisi del sistema (pot trigar uns minuts).

c) Intenta instal·lar el programa **Revealer Keylogger** de **logixoft**. Comprova que passa.

d) Afegeix **Revealer Keylogger** de **logixoft** a la llista de programari exclòs de ser considerat malware. Comprova ara si es pot instal·lar.

3- Política de contrasenyes-I

a) Llegeix la informació sobre la creació de contrasenyes a https://en.wikipedia.org/wiki/Password_policy. Concretament, la informació sobre formació i duració.

b) Instal·la el paqet **pwgen**. Genera **100** contrasenyes que segueixi les 3 principal polítiques indicades a la lectura anterior, amb **pwgen**. El número caracters ha de ser igual o superior al mínim indicat a la lectura.

c) Genera **una** contrasenya amb **pwgen** de **10** caràcters, que tingui minúscules, majúscules i nombres.

d) Crea la versió encriptada del password generat amb el mètode SHA-512 per mitja de l'ordre **mkpasswd**.

e) Calcula quina serà la data d'aquó a **180 dies**. Utilitza date amb l'opció **-d** i **"180 days"**.

d) Crea un usuari amb useradd de nom **jpons**, amb **uid=2000**, grup per defetcte **users**, directori personal **/home/jpons**, shell per defecte **/bin/bash**, i contrasenya la trobada a l'apartat anterior. Fes que la data d'expiració sigui la trobada a l'apartat anterior.

e) Comprova la data d'expiració de l'usuari amb **chage -l jpons**. Comprova el password dins del fitxer **/etc/shadow**.

4- Política de contrasenyes-II

a) Amb la informació que trobaràs a http://fraterneo.blogspot.com.es/2014/01/politicas-de-contrasenas-en-gnulinux.html, crea un politica d'entrada de contrasenyes pels usuari que seguexi les següent directrius:

* No permetre reutilitzar les darreres 5 contrasenyes
* Mida mínima = 10
* Complexitat = Al menys 1 majúscula, 2 minúscules, 1 nombre i un símbol.
* Venciment = 60 dies amb advertències a a partir des de 14 dies abans del venciement.

b) Entra com usuari jpons i intent canviar la contrasenya i comprova que s'apliquen les polítiques de seguretat.

5- Contrasenya de GRUB

a) Amb la informació que trobaràs a http://geekland.eu/proteger-el-grub-con-contrasena/ crea un usuari i contrasenya per accedir a **grub**. L'usuari ha de ser **asix2** i la contrasenya **clotfje**. Ha de mirar-te els passos **2** i **4**.

b) Comprova que funcionen correctament el nom i contrasenya.

6- Encriptació de fitxers i directoris

a) LLegeix la informació que trobaràs a https://saforas.wordpress.com/2011/05/18/encriptacion-de-ficheros-con-gnu-privacy-guard-gpg/.

b) Instal·la els paquets **gnupg i ecryptfs-utils**.

c) Genera una clau RSA de 2048 bytes sense data de caducitat pel programa **gpg**.

d) Descarrega **m11uf2pr1d.pdf** i encripta-ho amb l'eina **gpg**. Utilitza la informació de la lectura.

e) Com a **root**, carrega el mòdul (driver) ecrypts. Executa: **modprobe ecrypts**.

f) Com a **root**, amb l'eina **ecryptfs-migrate-home**, encripta el directori de l'usuari **jpons**. Segueix les instruccions i finalitza les tasques que demana el programa. Si demana **login passphrase [jpons]**, has de posar el password de **jpons**.

7- Comprovació i modificació de permisos

a) Troba tots els fitxers del teu directori personal que no tinguin definits els permisos **644.**

b) Troba tots els fitxers del teu directori personal que no tinguin definits els permisos **755.**

c) Troba tots els fitxers del teu directori personal que tinguin definits els permisos **755.**

d) Troba tots els directoris del teu directori personal que tinguin definits els permisos **777.**

e) Troba tots els fitxers del teu directori personal que tinguin definits els permisos **755** i fes que tinguin els permisos **700**.

8- Treballant amb la màscara per defecte

a) Comprova quina és la màscara per defecte del teu sistema. Crea un directori de nom **mascara00** i comprova que es crea amb els permisos determinats per la màscara per defecte. Crea un fitxer de nom **mascara00txt** i comprova que es crea amb els permisos determinats per la màscara per defecte. Hauràs de llegir https://wiki.archlinux.org/index.php/Umask_(Espa%C3%B1ol).

b) Modifica la màscara per defecte des del terminal. Fes que el seu nou valor sigui **0002**. Comprova que s'ha modificat. Crea un directori de nom **mascara01** i comprova que es crea amb els permisos determinats per la màscara per defecte. Crea un fitxer de nom **mascara01.txt** i comprova que es crea amb els permisos determinats per la màscara per defecte.

c) Tanca el terminal. Torna a obrir el terminal. Torna a comprovar el valor de la màscara per defecte.

d) Canvia el valor de la màscara per defecte de manera permanent per l'usuari root amb la informació que trobaràs a https://wiki.archlinux.org/index.php/Umask_(Espa%C3%B1ol). Fes que sigui la necessària per tenir un sistema completament privat d'acord amb la informació que trobaràs a la següent adreça: https://www.cyberciti.biz/tips/understanding-linux-unix-umask-value-usage.html. Comprova que ara cada cop que obres el terminal, els permisos de creació de fitxers i permisos són sempre els adequats.

f) Fes que el canvi anterior sigui vàlid per tots el usuaris del sistema d'acord amb la informació que trobaràs a https://wiki.archlinux.org/index.php/Umask_(Espa%C3%B1ol)

Forma de lliurament de la pràctica

1- El lliurament de la pràctica es durà a terme el dia **16/12/16** de **15.00 a 16.00 hores**.

2- Es comprovara:

.