

ESET Smart Security 4

eset



Amenaza detectada
Alerta

Objeto:

E:\SkypeDLLInjector.exe

Amenaza

Win32/Skytap.A Troyano

Comentario:

Suceso ocurrido durante un intento de acceder a un archivo por la aplicación: C:\Windows\explorer.exe.

Desinfectar

Eliminar

Sin acciones

▼ Muestra/oculta parámetros adicionales de configuración

Ciberatacs: recerca i anàlisi sobre DoS i APT



No se puede acceder a este sitio web

www.tribunalconstitucional.es ha tardado demasiado tiempo en responder.

Busca tribunalconstitucional.es Páginas VariaciónRoot en Google

ERR_CONNECTION_TIMEOUT

Mostrar copia guardada



Albert Vilardell Barnosell
2n Batxillerat B
Curs 2016-2018
Tutora: M. José Morena

ÍNDEX

Introducció.....	4
1. Ciberseguretat i <i>pentesting</i>	6
1.1 Introducció a la ciberseguretat i el <i>pentesting</i>	6
1.2 Legislació actual	7
2. Denegació de servei (DoS/DDoS)	7
2.1 Concepte d'un atac de denegació de servei	7
2.2 Tipus d'atacs de denegació de servei	8
2.3 Atacs DDoS més rellevants de l'última dècada.....	11
2.4 Prevenció d'una denegació de servei	13
2.5 Protocol davant d'una caiguda de servei.....	14
3. Amenaça persistent avançada (APT)	15
3.1 Concepte d'una amenaça persistent avançada	15
3.2 <i>Modus operandi</i> d'un atac APT	17
3.2.1 Procés de l'atac	17
3.2.2 Mètodes d'infecció.....	18
3.3 Atacs APT més rellevants de l'última dècada	19
3.4 Prevenció d'un atac APT	21
3.5 Com detectar i actuar davant una amenaça persistent avançada	22
4. Part pràctica.....	23
4.1 Creació d'una web sobre consells de ciberseguretat	23
4.1.1 Llenguatge HTML.....	24

4.1.2 Llenguatge CSS	25
4.1.3 Contingut de la pàgina web	26
4.2 Atac APT a l'administrador de la web creada anteriorment	27
4.3 Atac DoS a la web creada anteriorment i allotjada en un servidor propi	28
4.4 Jornada eBusiness: <i>Ciberseguretat: Amenaces i com protegir-nos de forma eficient</i>	29
Conclusió.....	31
Bibliografia.....	33
Annexes	37
Annex I: Esquema sobre protocols i paquets d'Internet.....	38
Annex II: Glossari.....	39
Annex III: Creació de la pàgina web i del servidor	40
Annex IV: Atac d'amenaça persistent avançada.....	43
Annex V: Atac de denegació de servei	46

INTRODUCCIÓ

Cada dia es detecten 325.000 amenaces a la xarxa¹. Vivim en una època on els ciberatacs són quelcom habitual. Ara és més important que mai saber com evitar ser víctima d'un cibercriminal.

Des de ben petit he sentit molta curiositat per tot el relacionat amb la informàtica; als 12 anys ja vaig ajudar a la direcció de la meua antiga escola a reforçar la seguretat de la seva xarxa informàtica, i amb el temps aquesta passió no ha disminuït. Recentment, a causa de la gran popularitat mediàtica dels *crackers*, he començat a aprofundir en la ciberseguretat. Aquesta és una branca de la informàtica que, en els darrers temps, està agafant molta importància en el món de l'empresa en un entorn creixent de digitalització dels negocis².

El meu treball gira entorn a la *Offensive security* o *pentesting*, terme que fa referència a un estil de protecció d'equips o de xarxes i que es basa en la simulació de ciberatacs tal com els realitzarien els ciberdelinqüents. Dins de l'àmplia gamma de ciberatacs que engloba *offensive security*, n'hi ha dos que destaquen sobre la resta: l'atac de denegació de servei o DoS (atac que persegueix inutilitzar temporalment un servei o recurs informàtic) i l'atac d'amenaça persistent avançada o APT (atac que persegueix apropiat-se d'informació valuosa d'una empresa).

L'objectiu principal d'aquest treball és entendre què hi ha darrere d'aquests dos famosos ciberatacs i proposar pautes per prevenir-los. Els objectius específics se centren a desenvolupar tècniques relacionades en l'adquisició de nous coneixements. Tals coneixements s'han assolit a partir de la recerca i anàlisi de diverses fonts d'informació i tècniques relacionades amb la informàtica. Aquestes tècniques serien: aprendre programació web, crear un servidor i realitzar ciberatacs.

El procés que he seguit per a elaborar aquest treball ha estat un procés jeràrquic; inicialment m'ha requerit una immersió intensa en la teoria relacionada amb la ciberseguretat. Posteriorment he hagut d'estructurar la part pràctica del treball.

¹ Font: *Kaspersky Lab*

² Font: *telefonica.com*

Finalment he arribat a les conclusions de l'estudi a partir dels coneixements adquirits i dels resultats obtinguts en la part pràctica.

Per a la recerca i adquisició dels coneixements teòrics he utilitzat diverses fonts d'informació: bibliografia especialitzada, pàgines webs del sector, accés a fòrums de *hackers* i assistència a una jornada de ciberseguretat. La font d'informació que ha resultat més útil per entendre l'impacte que tenen aquests ciberatacs en les empreses han estat els articles de diferents diaris digitals.

La part pràctica del treball ha consistit en crear una pàgina web (que dóna consells per evitar ser infectats per *malware*³), crear un servidor i realitzar una sèrie d'atacs APT i DoS per comprovar la seva seguretat. Aquest procés m'ha suposat haver d'ampliar el meu coneixement en altres àmbits de la informàtica.

La principal dificultat que m'he trobat durant tot el treball ha estat la comprensió dels tecnicismes associats a la ciberseguretat (*botnet*, *spoofing**, *rootkits**, etc.) i dels fonaments tècnics propis d'Internet (protocols, paquets⁴, DNS, etc.).

Però sense cap mena de dubtes la gran limitació d'aquest treball ha estat no disposar d'un equip amb sistema operatiu GNU/Linux. Aquest sistema operatiu és òptim per realitzar qualsevol tipus de ciberatac (i per entendre'ls millor). Vaig intentar instal·lar aquest sistema en una màquina virtual dins del meu equip, però va resultar tècnicament impossible. En conseqüència ha estat molt difícil i laboriós realitzar les proves dels dos atacs en un equip Windows NT.

³ *Malware*: programa maliciós que pretén causar mal a ordinadors, sistemes o xarxes.

* Mirar Annex 2: Glossari

⁴ Paquet (de xarxa): cada un dels blocs en els que es divideix la informació quan s'envia. Es diferencien segons el protocol que utilitzin.

1. CIBERSEGURETAT I *PENTESTING*

La ciberseguretat és una àrea relacionada amb la protecció de la infraestructura informàtica i, en especial, de la informació.

1.1 Introducció a la ciberseguretat i el *pentesting*

En plena era digital, la seguretat a la xarxa ha esdevingut quelcom necessari. Les organitzacions comencen a invertir enormes quantitats de diners en aquest sector. I no és d'estranyar; a nivell d'exemple, i fixant-nos en el cas de Catalunya, la Generalitat va patir 215 milions de ciberatacs durant l'any 2015⁵. Això ha impulsat la recent creació de l'Agència de Ciberseguretat de Catalunya (12 de juliol de 2017). A més a més, en els darrers cinc anys, les inversions en sistemes de ciberseguretat a tot Catalunya s'han multiplicat per tretze⁶.

Darrere de tots els ciberatacs malintencionats hi ha delinqüents. Popularment se'ls anomena *hackers*, però es tracta d'un ús erroni. Segons el glossari d'Internet, *hacker* és: "Persona que té coneixement profund sobre el funcionament de xarxes de manera que pot advertir els errors i els forats de seguretat del mateix"⁷. Quan parlem d'experts informàtics amb intencions malicioses, hem d'utilitzar l'anglicisme *cracker*.

Un *cracker* sempre intentarà penetrar un sistema sense autorització per realitzar qualsevol tipus d'acció maliciosa. Per aquest motiu, les empreses disposen de grans infraestructures i equips de ciberdefensa. Però, es clar, existeix la necessitat de fer proves d'atacs per veure on flaqueja la defensa.

D'aquí neix el *pentesting* o test de penetració. La finalitat d'aquest test és informar de les vulnerabilitats d'un sistema abans que siguin explotades pels *crackers*, mitjançant una sèrie de ciberatacs controlats i acceptats per l'administrador. Permetrà al propietari prendre mesures preventives i correctores davant d'un atac.

⁵ Font: *elmundo.es*

⁶ Font: *elmundo.es*

⁷ <http://www.internetglosario.com/255/Hacker.html>

1.2 Legislació actual

A Espanya, la legislació castiga severament tota acció maliciosa (o no tan maliciosa) que es produeixi en l'àmbit informàtic sense una autorització prèvia de l'administrador. La Llei Orgànica 1/2015 del 30 de març del Codi Penal ho deixa ben clar.

Pel que fa a un atac de denegació de servei, l'article 264 dicta la prohibició d'obstaculitzar o interrompre el funcionament d'un sistema informàtic. Les conseqüències són penes de presó de sis mesos a tres anys.

Respecte a un atac d'amenaça persistent avançada, l'article 197 dicta la prohibició de l'apoderament de dades confidencials (com per exemple de correus electrònics), d'utilitzar artificis tècnics per "espia" i de vulnerar les mesures de seguretat establertes per obtenir accés a una xarxa. Les conseqüències d'aquests actes poden implicar una pena d'entre sis mesos i set anys de presó. Aquesta llei no diferencia entre les intencions d'un delinqüent i les d'un simple curios que busca comprovar la fortalesa d'una xarxa sense el permís del propietari.

2. DENEGACIÓ DE SERVEI (DoS/DDoS)

"No es pot accedir a aquest lloc web. Twitter.com ha trigat massa temps en respondre". Aquest va ser el missatge que apareixia el dia 21 d'octubre de 2016 quan s'intentava accedir a la famosa xarxa social. Es tractava d'un atac distribuït de denegació de servei.

2.1 Concepte d'un atac de denegació de servei

Un atac de denegació de servei és aquell que té la finalitat de fer que un servei o recurs es trobi inaccessible temporalment. L'objectiu principal d'un atac de denegació de servei no és aconseguir informació, sinó que és alentir o fins i tot fer caure una web o el mateix servidor.

Els motius darrere d'aquest ciberatac poden ser tant econòmics com ideològics. En l'àmbit del *pentesting* es realitza aquest atac amb la finalitat d'estudiar la viabilitat en

la que una empresa pot deixar d'oferir el seu servei i quan pot trigar a recuperar-se després de rebre aquest atac.

Curiosament, la majoria d'empreses o corporacions intenten evitar aquesta prova quan contracten a un grup d'auditoria⁸. Un atac DoS controlat ha d'estar molt ben planificat per evitar que la web del client acabi inhabilitada, fet que ocasionaria importants pèrdues.

Cal diferenciar un atac DoS (*Denial of Service*) d'un DDoS (*Distributed Denial of Service*). L'atac DDoS és una variant del DoS. Mentre que el DoS és realitzat per una única màquina virtual, el DDoS és realitzat per múltiples d'elles. Els atacs DDoS abunden molt més que els DoS, ja que una sola màquina virtual no sol ser suficient per arribar a denegar un servei.

2.2 Tipus d'atacs de denegació de servei

Per poder entendre com són actualment els diferents atacs de denegació de servei cal mirar enrere en el temps. Els primers atacs coneguts daten de finals dels anys '90, i al voltant del 2010 evolucionen tant en nombre com en potència. En el següent gràfic es pot veure l'exponencial increment en la magnitud dels atacs DDoS.

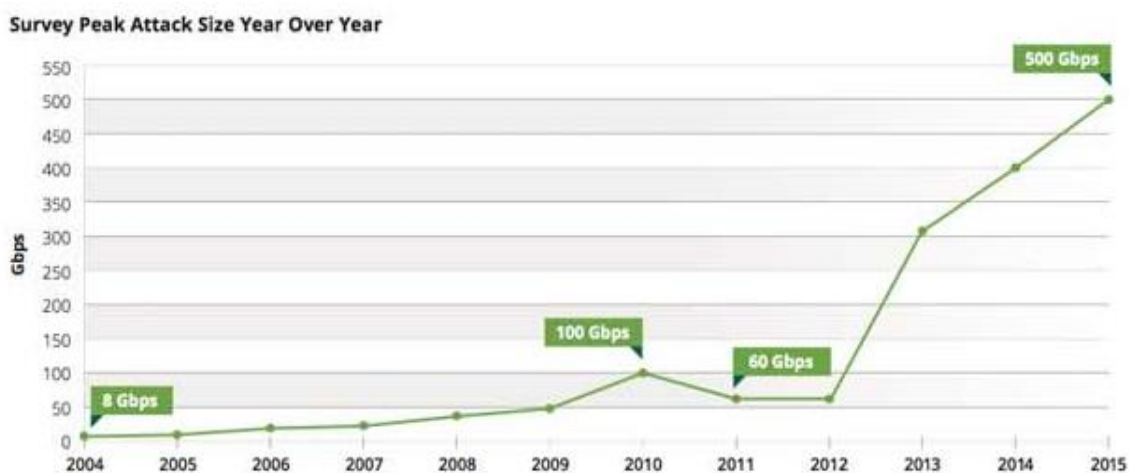


Fig. 1: Augment de la potència dels atacs DDoS en els últims anys

⁸*Ethical Hacking*. Pablo González Pérez. ISBN: 978-84-617-0576-4.

Els primers atacs de denegació de servei estructurats es basaven en un *exploit* (vulnerabilitat del sistema) que permetia l'enviament de múltiples paquets ICMP⁹ (paquets utilitzats per enviar missatges d'error d'Internet) de gran mida, amb l'objectiu de saturar l'equip de la víctima. L'any 1996 es va publicar l'atac *Ping-of-Death* en el que l'atacant enviava directament els paquets a la víctima, i l'any 1997 es va publicar l'atac *smurf*, que a diferència del primer multiplicava el seu efecte sobre la víctima mitjançant una tècnica de reflexió. L'atacant envia paquets ICMP a una sèrie de màquines virtuals utilitzant com a adreça IP¹⁰ d'origen la de la víctima (*IP Spoofing*) i tots els equips de la xarxa contesten el dispositiu de la víctima, amplificant la potència de l'atac. Actualment, el *software* actual ja compta amb una protecció específica per aquests dos atacs.

L'any 2004 es va publicar la primera versió de LOIC, una eina molt útil utilitzada des del seu llançament per a realitzar atacs DDoS. LOIC permet realitzar atacs DoS de tipus *TCP Flood*, *UDP Flood* i *HTTP Flood*.

Un any més tard es va realitzar el primer atac de denegació de servei mitjançant una *DNS Amplification*. Aquesta tècnica va suposar un salt en la potència dels atacs i encara és utilitzada en l'actualitat. Un atacant envia paquets UDP (paquets que segueixen el protocol UDP) mitjançant peticions DNS¹¹ des de l'adreça IP de la víctima. La resposta que envia el servidor DNS a la víctima ocupa entre 40 i 70 vegades més que la pròpia petició DNS¹².

Actualment, els atacs DoS o DDoS deriven de quatre tècniques que s'exposen a continuació.

- *UDP Flood*:

UDP Flood és un tipus d'atac que s'aprofita del protocol UDP. Un exemple és el mètode

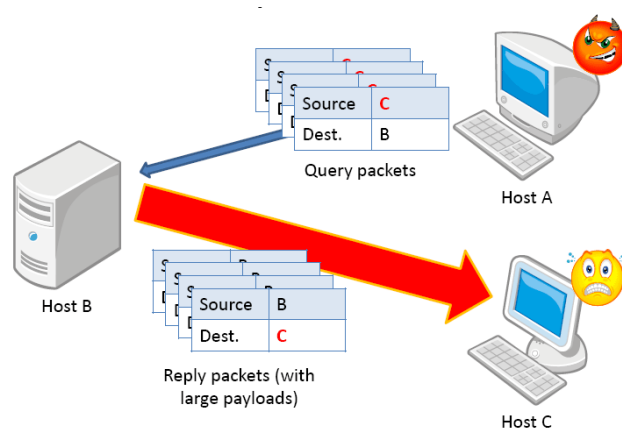


Fig. 2: Esquema d'un atac UDP Flood

⁹ Mirar Annex 1: Esquema sobre protocols i paquets d'Internet

¹⁰ Adreça IP: número que obté un dispositiu a la xarxa i que permet a Internet identificar-lo.

¹¹ Petició DNS: petició a un servidor DNS per canviar un domini a una adreça IP.

¹² *Ethical Hacking*. Pablo González Pérez. ISBN: 978-84-617-0576-4.

DNS Amplification. El protocol UDP permet l'enviament de paquets UDP. Aquests paquets s'envien a gran velocitat (però amb un mecanisme mínim de seguretat). D'aquesta manera, l'atacant realitza un gran nombre de peticions amb la IP de la víctima, perquè així les respostes vagin cap a ella.

- *ICMP Flood:*

ICMP Flood és un atac que deriva de l'atac *smurf*. L'atacant envia un gran nombre de paquets ICMP *echo request* (paquets ICMP de sol·licitud) des d'una adreça IP inexistent. La víctima intenta respondre amb paquets ICMP *echo reply* (paquets ICMP de resposta) a la IP inexistent, però acaba sobrecarregant el seu sistema.

- *TCP Flood:*

TCP Flood engloba una sèrie d'atacs que fan ús del protocol TCP d'Internet. Aquest atac busca saturar una xarxa enviant peticions de connexió TCP. El més comú i del que es parlarà és del *SYN Flood*. Quan es realitza una connexió TCP, es realitza el que s'anomena salutació a tres bandes: el client envia un missatge SYN al servidor, aquest el respon amb un missatge SYN-ACK i finalment el client envia un ACK. L'atac es basa a

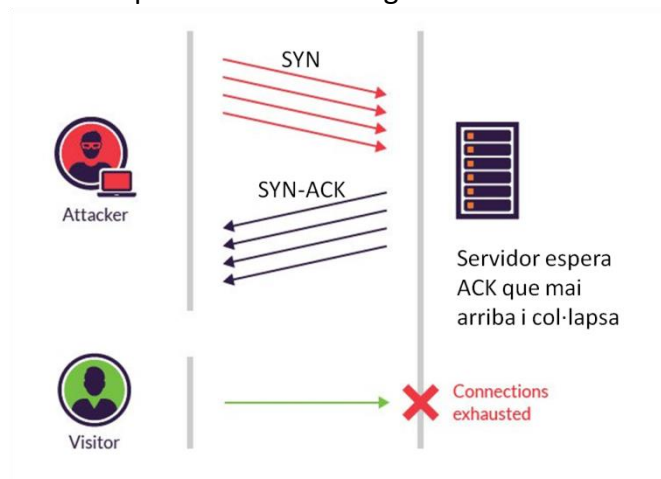


Fig. 3: Esquema d'un atac SYN Flood

enviar una gran quantitat de SYN sense completar la salutació a tres bandes (mai s'envia l'ACK)¹³. D'aquesta manera, el servidor no pot atendre més peticions. LOIC és una eina molt utilitzada per automatitzar un atac DoS o DDoS de *TCP Flood*.

- *HTTP Flood:*

HTTP Flood és un tipus de ciberatac que no s'aprofita de ningun exploit però que es centra en la dificultat que hi ha per distingir entre el tràfic HTTP (accions que realitza

¹³<https://cyberseguridad.net/index.php/197-ataques-de-denegacion-de-servicio-dos-ataques-informaticos-iii>

un usuari en una pàgina web) legítim i el tràfic HTTP maliciós. El que fa que un atac *HTTP Flood* sigui tan complicat de detectar i frenar és que cada un és diferent, ja que els atacs *HTTP Flood* s'adapten a la víctima per treure el màxim profit.

Aquest ciberatac es basa en l'enviament massiu d'*HTTP requests*. Una *HTTP request* és aquella petició que fa un usuari cada cop que interactua amb una web. Aquestes peticions poden ser *GET* o *POST*. Les primeres fan referència a un contingut més senzill, com ara imatges. En canvi, les segones fan referència a un contingut dinàmic que requereix l'atenció del servidor, com buscar informació en la base de dades. L'ús de peticions *POST* acostuma a ser més potent, però les peticions *GET* són més fàcils de programar i dur a terme. La majoria d'atacs *GET Flood* es realitzen amb una *botnet* (xarxa de dispositius infectats sota el control remot d'un individu).

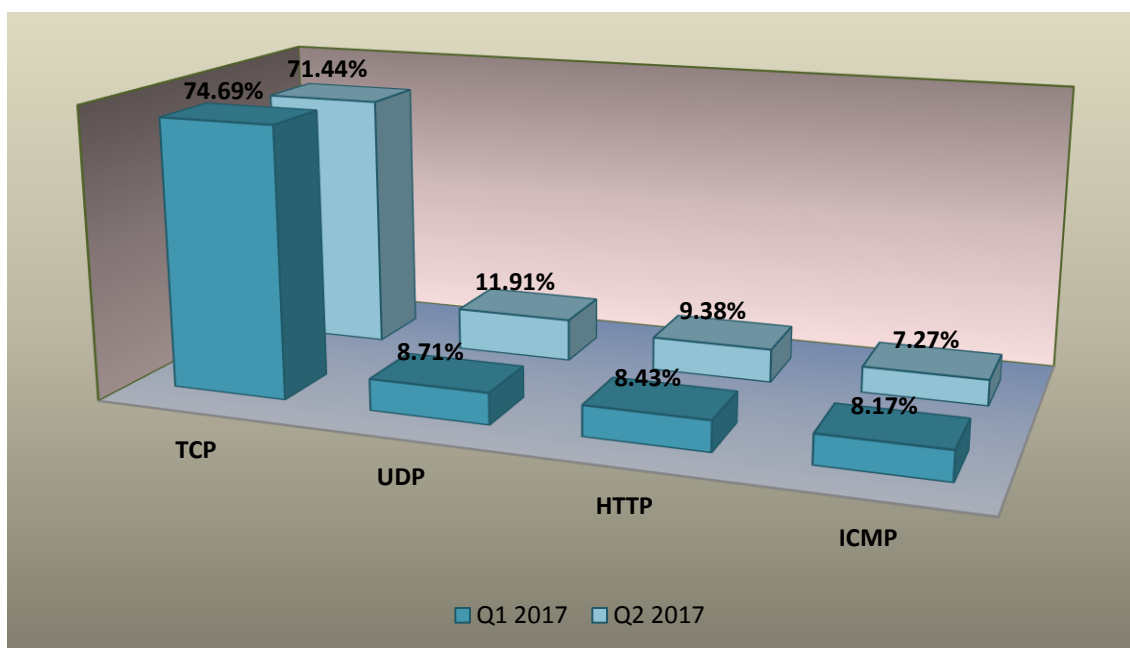


Fig. 4: Atacs DDoS segons el tipus en el primer i segon trimestre del 2017

2.3 Atacs DDoS més rellevants de l'última dècada

Com ja s'ha mencionat anteriorment, els atacs de denegació de servei més potents enregistrats en tota la història se situen en l'última dècada. A continuació, es mencionaran dos dels atacs més rellevants.

1. *Operation Avenge Assange*

Operació realitzada durant el mes de desembre de l'any 2010 pel grup Anonymous* com a forma de defensa de la pàgina web WikiLeaks.

WikiLeaks alberga contingut confidencial (informes i filtracions governamentals). El govern nord-americà va començar a exercir pressió contra certs servidors i certes webs de vital importància per WikiLeaks amb l'objectiu de tancar la pàgina web. El resultat va ser desastrós: WikiLeaks no tenia cap servidor on ser allotjat ni cap servei *online* per a rebre donacions. Com a forma de protesta, el grup Anonymous va realitzar atacs DDoS contra certes pàgines webs que es van oposar a WikiLeaks, com per exemple PostFinance, PayPal o Mastercard.

El famós grup hacktivista va aconseguir, finalment, retornar l'estabilitat que tenia la pàgina.

2. Caiguda del servidor DynDNS

El dia 21 d'octubre de 2016 va ser un dia desastrós per moltes empreses dels Estats Units. La causa va ser la caiguda de servei que va patir el servidor de DynDNS. Aquest servidor s'encarrega de transformar certs dominis en adreces IP dinàmiques (DNS). Per exemple, l'adreça IP de Google és 216.58.204.131, però gràcies als servidors DNS hi podem accedir directament des de <https://www.google.es/>.

Aquest atac va tenir molta rellevància per dos motius: va deixar inaccessible a pàgines webs populars com Twitter, Netflix o Spotify i l'atac va provenir de Mirai Botnet. Aquesta *botnet* es caracteritza per disposar d'accés total a més d'un milió de dispositius d'*Internet of things* (ordinadors o càmeres de vigilància, per exemple).

L'atac en si es va basar en l'enviament massiu de paquets TCP i UDP des de milers de diferents adreces IP.

* Mirar Annex 2: Glossari

2.4 Prevenció d'una denegació de servei

Durant el segon trimestre del 2017, s'han enregistrat una gran quantitat d'atacs DDoS. El dia amb menys atacs va ser el disset d'abril (131), mentre que el dia amb més atacs DDoS va ser el tretze d'abril (904)¹⁴. Davant de tal quantitat d'atacs de denegació de servei és indispensable tenir un sistema de prevenció i protecció d'aquests.

Primerament, és important tenir clar que cap xarxa és segura. El 98% de les empreses diuen haver rebut ciberatacs¹⁵. Aquesta xifra deixa clar que és importantíssim tenir un bon sistema de defensa. En el cas de la denegació de servei, la clau està en tenir un bon sistema de prevenció i un bon protocol específic d'actuació.

Els *crackers* tenen avui en dia una àmplia gamma d'atacs de denegació de servei diferents. No obstant això, hi ha certes peculiaritats que tots ells tenen en comú. Per aquest motiu, és important disposar d'una defensa que tingui en compte totes aquestes característiques comunes, que són les següents:

1. Limitar el tràfic provinent d'un únic *host* (dispositiu connectat a una xarxa que fa ús dels seus serveis)¹⁶.
2. Tenir una autenticació per poder accedir a cert contingut de la pàgina web (*captcha**), com per exemple per descarregar contingut. D'aquesta manera, s'evita l'accés als *bots* (cada integrant d'una *botnet*). Aquest mètode inhabilita en gran mesura els atacs *HTTP Flood* de tipus POST.
3. Limitar el nombre de connexions al servidor per evitar una sobrecarrega.
4. Tenir diferents punts de presència a Internet per poder redirigir el tràfic si hi hagués una caiguda de servei¹⁷.



Fig. 5: Exemple de captcha

¹⁴ <https://securelist.com/ddos-attacks-in-q2-2017/79241/>

¹⁵Font: 2016-2017 Global Application & Network Security Report

¹⁶ <https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/>

* Mirar Annex 2: Glossari

¹⁷<http://interactivadigital.com/como-evitar-los-ataques-de-denegacion-de-servicio/>

5. Tenir un *JavaScript Challenge*. Aquesta eina (característica del servidor *CloudFlare*) permet fer un breu anàlisi del navegador per estudiar la seva legitimitat. Triga uns cinc segons.

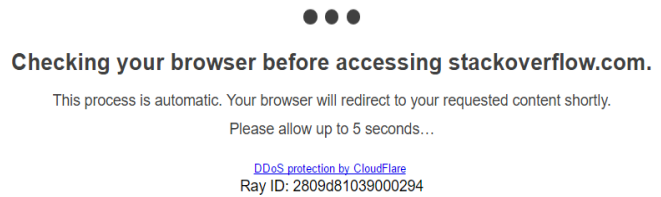


Fig. 6: Exemple de JavaScript Challenge

6. Bloquejar l'accés a la xarxa des del navegador Tor. Aquest navegador es caracteritza per canviar l'adreça IP de l'usuari, per tant és preferible bloquejar l'accés des d'aquest navegador.
7. Disposar d'una llista negra (*BlackList*) amb una sèrie d'adreces IP bloquejades que no tinguin accés al servei.

2.5 Protocol davant d'una caiguda de servei

És indispensable tenir un protocol d'actuació davant d'una caiguda de servei. Com s'ha explicat en els apartats anteriors, rebre aquest tipus de ciberatac pot causar grans pèrdues.

El protocol més eficient a seguir davant d'un atac de denegació de servei sempre tindrà l'objectiu de mitigar l'atac¹⁸.

Primerament, cal analitzar el tràfic de la xarxa en temps real. D'aquesta manera, s'esbrina si realment hi ha tràfic il·legítim. Sempre existeix la possibilitat que la caiguda de servei hagi estat involuntària. Per exemple, la caiguda de Twitter i Google el dia de la mort de Michael Jackson. A causa de l'enorme popularitat de la notícia, els dos serveis van rebre una gran quantitat de visites que van acabar col·lapsant les dues pàgines web.

Un cop analitzat el tràfic, i donat el cas que la denegació sigui intencionada, cal procedir a mitigar l'atac. Aquest procés identifica tots els paquets IP il·legítims i deixa passar els paquets IP legítims.

¹⁸*Ethical Hacking*. Pablo González Pérez. ISBN: 978-84-617-0576-4.

En el cas de patir una caiguda completa de servidor, cal recuperar-se ràpidament i analitzar l'atac per aprendre i millorar el sistema de protecció. També és una bona idea realitzar atacs DDoS rutinàriament per així millorar el sistema de resposta.

Per finalitzar, és important remarcar que la majoria d'empreses contracten assegurances per aquest tipus de ciberatac i també contracten a grans companyies que s'encarreguen de protegir-les davant d'aquest atac. Uns exemples de grans empreses que ofereixen eficients mètodes de protecció serien *CloudFlare*, *OVH*, *Akamai*, etc.

3. AMENANÇA PERSISTENT AVANÇADA (APT)

Una fuga de dades confidencials del govern de Suècia posa en perill l'estabilitat del govern. Un grup de *crackers* ha infectat físicament un ordinador per aconseguir les dades. Es tracta d'un atac d'amenaça persistent avançada.

3.1 Concepte d'una amenaça persistent avançada

Una APT (*Advanced Persistent Threat*) és un conjunt de processos que tenen com a objectiu obtenir informació d'un individu de manera permanent. Habitualment, es busca obtenir accés a la xarxa indefinidament. A diferència d'una denegació de servei, una amenaça persistent avançada no pretén causar mal a la infraestructura, sinó que prefereix obtenir informació valuosa.

APT consta de tres sigles: *Advanced* ja que és un procés on es fa ús de tècniques avançades, dutes a terme en condicions específiques per garantir el seu èxit; *Persistent* degut a l'exhaustiu estudi de la víctima; i *Threat*, ja que tot el procés es basa en les amenaces del món digital.

Com es veurà més endavant, un atac d'APT sol ser dut a terme per un grup de cibercriminals experts. Degut a la dificultat i al cost del mateix procés, una APT sol ser realitzada entre governs o empreses molt importants¹⁹. Habitualment s'associa APT amb espionatge.

¹⁹ <http://www.redseguridad.com/especialidades-tic/amenazas-y-vulnerabilidades/por-que-tienen-exito-los-advanced-persistent-threat-apt>

Quan parlem d'APT sempre ens ve al cap els anomenats *0-day exploit* (vulnerabilitats de sistema que encara no han estat solucionades). Aquest tipus d'*exploit* són, sens dubte, els més perillosos que hi ha en l'actualitat. No obstant això, no estan a l'abast de tothom: o bé inverteixes molt temps per a ser el primer a trobar la vulnerabilitat, o bé pagues una gran quantitat de diners al mercat negre d'Internet (*Dark Web*).

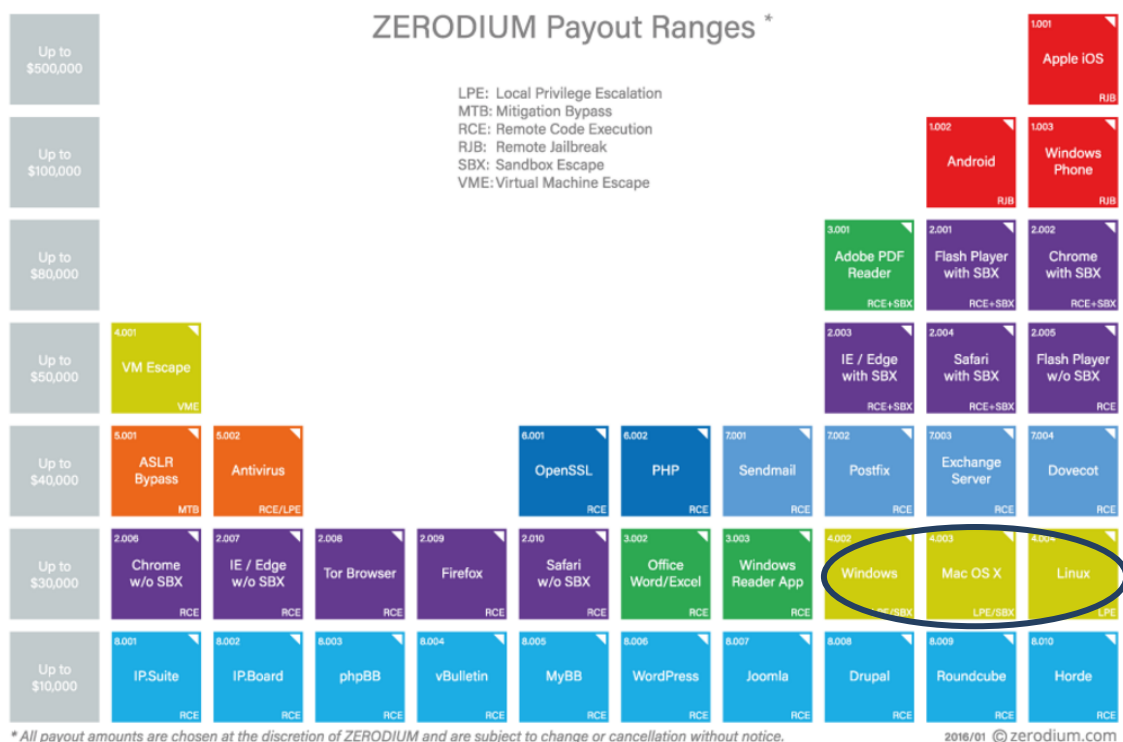


Fig. 7: Preus per la venda d'exploits de dia 0

En l'àmbit del *pentesting*, una APT consisteix a realitzar un conjunt d'atacs sobre una sèrie de treballadors seleccionats d'una empresa, simulant un atac dirigit a persones d'interès²⁰. D'aquesta manera, l'empresa pot veure on flaqueja el seu sistema de seguretat.

Per finalitzar, cal comentar que existeix un tipus d'atac similar al APT, el denominat AVT (*Advanced Volatile Threat*). Aquest es diferencia en l'objectiu de l'atacant: es busca penetrar en el sistema per obtenir informació, però abandonar-lo ràpidament sense deixar cap tipus de rastre. Actualment, els APT són molt més comuns que els AVT (probablement els atacs AVT mai hagin estat detectats).

²⁰ *Ethical Hacking*. Pablo González Pérez. ISBN: 978-84-617-0576-4.

3.2 *Modus operandi* d'un atac APT

Tots els atacs d'amenaça persistent avançada segueixen un patró general durant el procés. En canvi, en el moment d'infectar la víctima amb *malware*, els *crackers* poden fer ús de diferents tècniques.

3.2.1 Procés de l'atac

Els atacs d'amenaça persistent avançada són molt variats. Cada atac és diferent, ja que cada víctima també ho és. Però tots els atacs segueixen un *modus operandi*:

1. Estudi previ de la víctima:

Primerament, l'atacant investiga a la seva víctima. Els seus hobbies, els seus hàbits, les seves persones de confiança, les seves preferències (de sistema operatiu, per exemple), etc. No és una tasca complicada, ja que hi ha molts mètodes per obtenir informació. Des d'un atac *Man In The Middle** fins a les metadades* fins a *google hacking**: la informació és molt accessible per un delinqüent expert.

2. Intrusió a la xarxa:

A partir de la informació obtinguda durant l'estudi de la víctima, l'atacant analitza les diferents maneres per penetrar a la xarxa i "amagar-s'hi".

Un mètode per evitar ser descobert durant la intrusió és el de crear una distracció. Per exemple, realitzar un atac de denegació de servei alhora que s'intenta penetrar a la xarxa per infectar-la. D'aquesta manera, els administradors del sistema se centren en bloquejar l'atac DDoS i no s'adonen de l'APT.

Hi ha ocasions en les quals el delinqüent necessita adquirir més drets per a obtenir informació sensible i més control de la xarxa. Aquest procés s'anomena escalar privilegis.

Una opció és fent una propagació del *malware* a la xarxa interna (intranet). D'aquesta manera, a partir de la infecció d'un treballador d'empresa, pot arribar als alts directius.

* Mirar Annex 2: Glossari

3. Accés als recursos:

Finalment l'atacant s'acomoda a la xarxa i extreu tot allò que vulgui.

4. Moure els recursos a un servidor propi:

Un cop el *cracker* ha obtingut tots els recursos que buscava, els mou a un servidor privat (des del dispositiu de la víctima) per poder accedir a ells des del seu equip.

5. Crear una *backdoor*:

Backdoor, o porta posterior, és una seqüència especial dins del codi de programació que permet accedir a la xarxa en un futur d'una manera molt senzilla. Gràcies a aquesta *backdoor*, l'atacant pot tornar a accedir a la xarxa quan ho desitgi.

3.2.2 Mètodes d'infecció

Actualment hi ha quatre tipus diferents de maneres per infectar un dispositiu amb *malware*. És indispensable saber com actuen els *crackers* per així poder evitar una APT.

1. Enginyeria social:

L'atacant farà ús de diferents tècniques per obtenir la informació o bé infectar a la víctima fent ús de l'enginyeria social.

La tècnica més comuna és el *phishing*. L'objectiu d'aquesta tècnica és el de guanyar-se la confiança de la víctima mitjançant medis electrònics suplantant la identitat d'una persona o entitat de la seva confiança²¹. Així, l'atacant pot tant aconseguir dades sensibles com fer-li descarregar *malware*. Es pot buscar la infecció d'un ordinador o d'un dispositiu mòbil. Segons dades del Centre

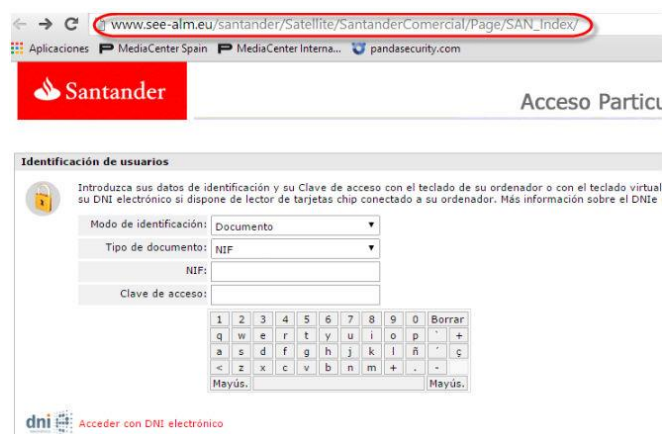


Fig. 8: Exemple d'una pàgina web il·legítima utilitzada durant un atac de phishing

²¹ <https://www.softwaredoit.es/definicion/definicion-phising.html>

Criptològic Nacional, el 75% dels casos d'infecció a companyies es realitzen utilitzant missatges de correus electrònics enganyosos amb un alt nivell de personificació²².

El *malware* descarregat per la víctima habitualment farà ús d'un o més *0-day exploits*, per així evitar ser detectat.

2. Infecció física:

Aquesta segona tècnica és la que més exposa al delinqüent. L'atacant infectarà físicament la xarxa de la víctima. Probablement, la forma més coneguda és la de connectar un dispositiu usb amb *malware* a l'equip. Si el delinqüent treballa a la companyia que vol infectar, no li serà complicat.

3. Infecció del dispositiu personal de la víctima:

Hi ha certes companyies que permeten als seus treballadors portar equips personals (pc) a l'empresa. L'atacant ho sap, ja que ha estudiat minuciosament a l'empresa i a la víctima. És llavors quan té la possibilitat d'infectar un ordinador fora dels límits de l'empresa. És un treball molt més senzill degut a la falta de protecció que implica no estar sota els límits de la companyia. Un cop infectat l'ordinador, només faltaria esperar que es connectés a la xarxa WiFi de l'empresa perquè el *malware* es propagués.

4. Vulnerabilitats:

Tot *software* presenta errors de sistema. Si aquests errors són suficientment greus, permeten a l'atacant executar un codi en el sistema de la víctima sense que se n'adoni²³. Però sens dubte, les vulnerabilitats més perilloses són les de dia 0 (*0-day exploit*).

3.3 Atacs APT més rellevants de l'última dècada

El tret més característic dels atacs APT és la complexitat que tenen. En els dos atacs APT més rellevants que es mencionaran es veu clarament reflectida. Una altra

²² Font: *Europa Press*

²³ http://egov.ufsc.br/portal/sites/default/files/cdn_apt.pdf

característica comuna dels dos atacs és l'elevat cost d'aquests. Disposar de *0-day exploits* surt molt car.

1. *Operation Aurora*

A principis de gener de l'any 2010, Google i 34 empreses multinacionals més van patir una gran fuga d'informació mitjançant un *malware*. El *modus operandi* de l'atac era el següent: els usuaris rebien correus electrònics maliciosos que redirigien a una pàgina web. Aquesta pàgina web contenia un exploit de dia 0 que descarregava automàticament *malware* (un troià*). L'exploit només funcionava en el navegador Internet Explorer. Les víctimes eren alts càrrecs amb importància dins de les companyies.

Avui en dia encara no se sap qui va ser l'autor, encara que les sospites recauen sobre la Xina, ja que en el codi de programació del *malware* hi havia una sèrie d'anotacions en xinès simplificat.

2. Stuxnet

Stuxnet era un cuc* informàtic. Ha estat el primer *malware* que ha aconseguit danyar una infraestructura en tota la història de la humanitat. Va infectar més de mil màquines de producció de materials nuclears d'Iran. Això va ser possible gràcies als quatre exploits de dia 0 que hi havia en el codi de programació. L'autor d'aquest *malware* és els Estats Units.

El *modus operandi* del cuc era el següent: Stuxnet va penetrar a la xarxa del programa nuclear de Natanz (Iran) en una memòria USB infectada. A continuació, es va propagar per tots els ordinadors. Un cop infectats, va modificar el programa de les centrifugadores. Amb el temps, la tensió provocada pels canvis en les centrifugadores va provocar que les mil màquines infectades es desintegressin. Això va suposar una pèrdua del vint per cent de les centrifugadores de la central.

* Mirar Annex 2: Glossari

Symantec (empresa de ciberseguretat) considera que es varen necessitar entre 5 i 10 experts en *software*, treballant fins a sis mesos, per a crear Stuxnet²⁴.

3.4 Prevenció d'un atac APT

Tenir un bon sistema de prevenció d'atac d'amenaça persistent avançada és quelcom complexa però de vital importància a l'hora d'evitar fugues d'informació.

a) Firewall

Un *firewall* (o tallafocs) és un *software* que permet protegir un ordinador de les intrusions que provenen d'una tercera xarxa. El *firewall* és especialment útil per evitar que usuaris externs d'una xarxa privada (intranet) tinguin accés a ella.

b) Antivirus

Un antivirus és un programa que té com a finalitat eliminar el *malware* que detecta. Així i tot, no detecta el *malware* que conté *0-day exploits*.

c) Protecció del correu electrònic

A causa del gran nombre d'infeccions que hi ha mitjançant *phishing*, cal disposar d'una protecció específica del correu electrònic que sigui capaç de comprovar l'autenticitat dels missatges i el contingut d'aquests.

d) Backup

Hi ha ocasions en què l'atacant opta per eliminar contingut important de la base de dades. Per aquest motiu, és essencial disposar de còpies de seguretat que siguin fetes periòdicament (*backup*).

e) Sandbox

Sandbox és una tecnologia que permet aïllar programes per executar-los sense prendre cap risc. D'aquesta manera, davant del dubte sobre la legitimitat d'un programa, es pot executar en una màquina virtual (que emula un sistema operatiu a la perfecció) i observar el seu comportament de forma segura.

²⁴ http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

f) Doble autenticació

Una autenticació és el mecanisme per verificar la identitat d'un usuari o aplicació²⁵. És per això que per evitar l'accés no autoritzat a una xarxa és necessari tenir múltiples capes d'autenticació. Un sistema de *login* amb un usuari i contrasenya és molt poc segur. Per aquest motiu, certes empreses comencen a demanar dues claus diferents per accedir. Per exemple, per accedir a una sessió Apple des d'un dispositiu extern se t'exigeix una clau de sis dígits que es genera a un dispositiu que ja tingui la sessió iniciada.



Fig. 9: Exemple d'inici de sessió amb un mecanisme de doble autenticació

g) Sistema actualitzat

Els sistemes operatius tenen actualitzacions periòdiques de *software* que aporten certes millores. La majoria d'elles són estètiques o funcionals, però sempre hi ha algun error de sistema solucionat. Per exemple, la propagació del *ransomware* WannaCry utilitzava un *exploit* que dos mesos abans Microsoft havia solucionat amb una *update*.

h) Conscienciació del personal

Els éssers humans tenim un paper molt important per evitar la infecció d'una amenaça persistent avançada. És per això que la millor protecció davant d'aquest tipus d'atac és l'educació del personal.

3.5 Com detectar i actuar davant una amenaça persistent avançada

Les empreses triguen una mitja de 98 dies en detectar una intrusió²⁶. Això ocasiona moltes pèrdues (ja siguin econòmiques o fugues d'informació). Per aquest motiu, tenir un bon sistema de detecció és indispensable.

²⁵https://www.ibm.com/support/knowledgecenter/es/SSGU8G_12.1.0/com.ibm.sec.doc/ids_am_044.html

²⁶ Font: *The Ponemon Institute*

La clau d'un sistema de detecció està en el tràfic de la xarxa: cal analitzar el tràfic minuciosament de forma periòdica. Qui es connecta a la xarxa, quines accions realitza, quin usuari té més privilegis dels que hauria de tenir, quines modificacions hi ha hagut en la infraestructura de la xarxa, etc. Tots aquests punts s'han de tenir en compte per adonar-se si algú ha aconseguit accés.

En el cas de detectar un possible fragment de *malware*, caldrà executar-lo en una *sandbox* per comprovar els seus efectes.

Si realment es tracta d'una amenaça persistent avançada, s'ha de realitzar una anàlisi forense. Aquest procés se sol realitzar amb *software* específic. L'objectiu sempre serà el de descobrir qui està darrere de la infecció i quines pèrdues ha pogut ocasionar. L'anàlisi inclou una investigació de les metadades del *malware*, un estudi de les connexions realitzades al servidor, una recerca de *rootkits* desconeguts fins al moment, etc. És un procés complex que serà dut a terme davant de notari per a més tard aportar les proves en un judici (si és possible).

Finalment, caldrà realitzar una neteja completa de la xarxa i dels equips per seguretat. A més a més, serà interessant fer un informe del succés per millorar la seguretat i evitar una infecció futura.

4. PART PRÀCTICA

Per la part pràctica vaig decidir realitzar els dos ciberatacs dels que parlo en aquest treball. Va ser indispensable crear una pàgina web i un servidor on allotjar-la, per així estar dins dels marges de la legalitat.

4.1 Creació d'una web sobre consells de ciberseguretat

Per dur a terme la programació de la web, vaig fer servir de base el codi font d'una web d'exemple que oferia la pàgina w3shcools (W3.CSS, demo 1). Vaig assegurar-me que el codi fos de lliure ús; la mateixa web explica que no es requereix cap llicència per utilitzar el codi. Un cop copiat el codi, vaig modificar-lo utilitzant el programa Sublime Text 3. Com que la web no forma part de cap tipus de comerç, no va ser necessari adaptar-la a la legislació actual.

A l'annex (III) hi ha una explicació més detallada tant del procés de la creació de la pàgina web com del servidor.

Els llenguatges utilitzats per programar la web van ser HTML i CSS. No vaig fer ús d'altres llenguatges, ja que la web és senzilla.

4.1.1 Llenguatge HTML

HTML és el llenguatge de programació web bàsic. S'encarrega de la creació de la pàgina web i de donar-li estructura i contingut. El codi HTML està format per una sèrie d'etiquetes que el navegador interpreta i dona forma a la pantalla.

Un document HTML es programa en una fulla del bloc de notes. Un cop programat, es guarda canviant el format de .txt a .html. Així tot, hi ha una àmplia gamma de programes que faciliten la programació en aquest llenguatge.

Les principals etiquetes que vaig utilitzar són les següents:

Etiqueta	Ús o significat
<code><!DOCTYPE html></code>	Defineix el document per ser html
<code><html> ... </html></code>	Fa referència al principi i fi del codi
<code><title> ... </title></code>	Títol de la pàgina web
<code><body> ... </body></code>	Tot el contingut visible va dins del <i>body</i>
<code><hx> ... </hx></code>	Fa referència a un títol (x és el número de títol)
<code><p> ... </p></code>	Defineix un paràgraf
<code>
</code>	Implica continuar el text a la següent línia
<code></code>	S'utilitza per afegir imatges
<code></code>	S'utilitza per enllaçar altres pàgines web
<code><style> ... </style></code>	Dins d'aquesta etiqueta es defineix l'estètica del document amb CSS
<code><div> ... </div></code>	Serveix per dividir el codi en seccions (solen ser seccions segons el format, CSS)

Taula 1: Etiquetes HTML i el seu ús

4.1.2 Llenguatge CSS

CSS és el llenguatge de programació web que s'encarrega de donar estil al text definit en HTML. Amb HTML s'estructura la pàgina web, mentre que amb CSS s'aporta disseny al contingut prèviament estructurat.

Per definir l'estètica d'un títol, d'un paràgraf, del fons, del marge, etc., cal especificar quina etiqueta es vol modificar, i entre les claus "{" i "}", cal definir quines propietats es modifiquen (color, font, etc.).

```
<style>
h1 {
  font-family: "Times New Roman";
  letter-spacing: 5px;
}
</style>
```

Fig. 10: Fragment d'un document HTML amb llenguatge CSS

Les principals propietats que vaig utilitzar són les següents:

Propietat	Significat
color: ...	Defineix el color de la font
font-family: "..."	Defineix la font
letter-spacing: ... px	Defineix l'espai entre cada lletra en píxels
top: ... px	Defineix l'alçada en la que està situat un element
right: ... px	Defineix la distància respecte el marge esquerra en que es situa un element
left: ... px	Defineix la distància respecte el marge dret en que es situa un element
width= "... px"	Defineix l'amplada d'un element
height= "... px"	Defineix l'alçada d'un element

Taula 2: Propietats CSS i el seu significat

4.1.3 Contingut de la pàgina web

El contingut de la meua pàgina web és sobre consells per evitar formar part d'una *botnet*. La motivació que em va portar a dedicar la pàgina web sobre això va ser l'atac de caiguda de servei que va patir el servidor DynDNS.

Formar part d'una *botnet* implica haver estat infectat per *malware*, així que els consells donats serveixen també per evitar una APT.

La web comença explicant què és una *botnet*, per què tots som possibles víctimes de formar part d'una i el perill que suposa. També explica la notícia que em va motivar a dedicar la web a aquest tema, explicada també en l'apartat (2.3) del treball.



Fig. 11: Explicació, a la web, de la caiguda de servei que va patir DynDNS

Després, dóna cinc consells molt importants per evitar formar part d'una. Aquests consells són alguns dels que s'expliquen al llarg de l'apartat (3) del treball.

Finalment, hi ha un mètode de contacte amb el propietari.

Actualment, aquesta pàgina web està allotjada en un servidor gratuït. Es pot trobar al següent URL: <https://barcelonasecurity.000webhostapp.com/>. Si la web és visitada des d'un *smartphone* o *tablet*, el format canvia.

4.2 Atac APT a l'administrador de la web creada anteriorment

Per poder realitzar els atacs DoS i APT de manera legal vaig haver de crear un servidor propi on allotjar la web.

Vaig necessitar un ordinador més que actués de servidor. Un servidor també pot ser un dispositiu mòbil, però vaig considerar que seria més adequat utilitzar un ordinador, ja que tot el treball està orientat en ordinadors.



Fig. 12: Consells, explicats a la web, per evitar una infecció de malware

Per la creació del servidor vaig instal·lar un programa anomenat Xampp, que permet muntar el servidor web. Per poder disposar d'un domini gratuït, vaig instal·lar un altre programa anomenat DUC. Aquest programa és la versió en *software* de la web no-ip.com.

Vaig haver d'obrir un port pel *router*. Vaig desactivar l'antivirus i el *firewall* per no tenir problemes en el procés.

Finalment, el servidor va ser creat. La meua intenció era que fos un WAN (*Wide Area Network*), però no vaig ser capaç, així que va acabar sent un LAN (*Local Area Network*). La diferència està en el fet que el WAN et permet accedir a la web des de qualsevol part del món, mentre que el LAN només permet accedir a la web estant connectat a la mateixa xarxa WiFi a la que està connectada el servidor.

Un cop finalitzada la creació del servidor, vaig procedir a realitzar l'atac d'amenaça persistent avançada. Vaig realitzar el paper tant d'atacant com de víctima. La meua idea era enviar un correu electrònic maliciós (*phishing*) amb un troià camuflat sota el nom de Facebook (i amb la icona real de Facebook) per així disposar d'accés total al servidor.

Vaig començar descarregant el troià DarkComet. Vaig configurar-lo adequadament i vaig fer certes modificacions al meu *firewall* per poder dur a terme la prova. Finalment, vaig infectar l'ordinador que actuava de servidor.

El meu paper com atacant era el de buscar infectar a un individu prèviament estudiat. El meu paper com a víctima era el d'executar un arxiu que semblava ser una aplicació legítima de la famosa xarxa social.

Un cop infectat, vaig disposar d'un accés total al dispositiu: des de la *webcam*, fins a les contrasenyes guardades a l'ordinador, fins a tots els arxius que tenia l'ordinador. Fins i tot, vaig disposar d'accés al propi escriptori de la víctima.

Un cop la prova va ser acabada, vaig eliminar d'ambdós ordinadors tot rastre de *malware*. No vaig inspeccionar a fons l'ordinador víctima, ja que un cop acabada tota la part pràctica vaig formatejar-lo*.

A l'annex (IV) es mostra més a fons el procés de l'atac APT.

4.3 Atac DoS a la web creada anteriorment i allotjada en un servidor propi

L'última part de la meua part pràctica consistia a realitzar un atac de denegació de servei al servidor per intentar deixar la pàgina web fora de servei. O almenys alentir-la molt.

* Mirar Annex 2: Glossari

Vaig utilitzar el programa LOIC. Vaig tenir problemes amb certes incompatibilitats amb el *software* del meu ordinador (amb *.Net Framework*), però al final vaig solucionar-les.

El programa LOIC permet escollir diferents tipus de *Floods*, ja siguin TCP, UDP o HTTP. Vaig considerar que el més adequat era TCP. També permet escollir el nombre de màquines virtuals des de les quals realitzar les *requests* a la web.

En altres paraules: vaig realitzar un atac de denegació de servei amb LOIC de *TCP Flood*. Consistia en l'enviament massiu de paquets TCP. A l'annex (V) es pot apreciar com és el programa LOIC i el problema d'incompatibilitat amb *.Net Framework* que vaig patir.

Desgraciadament, no vaig aconseguir denegar per complet la pàgina web. Probablement pel fet que dispo de d'un sistema operatiu Windows NT i que el meu ordinador no té suficient potència per arribar a enviar suficients *requests* alhora per arribar a col·lapsar el servidor. Un altre fet que va impedir la denegació total del servidor va ser disposar d'una de les xarxes WiFi amb més velocitat del mercat: 300 Mbps.

No obstant això, vaig aconseguir alentir molt la pàgina web i en certs instants vaig arribar a deixar-la inaccessible. Vaig estar més de dues hores utilitzant LOIC per arribar a aquest punt. Si hagués disposat de més equips sens dubte hauria aconseguit denegar la web completament.

Un fet que va em va sorprendre va ser que l'ordinador que actuava com a servidor anava molt lent (mentre realitzava l'atac) i no permetia accedir a Internet des del navegador. Probablement això fos una conseqüència de dedicar tants recursos al servidor web.

4.4 Jornada eBusiness: *Ciberseguretat: Amenaces i com protegir-nos de forma eficient*

El dimarts 23 de maig vaig assistir a la Jornada eBusiness a la Cambra de Comerç de Barcelona. Més que una conferència, va acabar sent una promoció de diferents serveis informàtics.

Al començament de la jornada es va parlar molt del *ransomware*²⁷ WannaCry, ja que per aquella data tenia molta popularitat mediàtica. Després es va parlar de la companyia SonicWall, de BitDefender i finalment de Veeam Backup. La primera és una companyia de *firewall*, la segona d'antivirus i l'última de còpies de seguretat o *backup*.



Fig. 13: Fotografia de la Jornada eBusiness

Al finalitzar la jornada, em van donar una sèrie de tríptics sobre les tres empreses. Aquests contenen informació que m'ha servit per al treball, com per exemple informació sobre la *Internet of things* i els *rootkits*. Ha estat especialment útil durant tot l'apartat (2) i en l'apartat (3.5).

Aquesta jornada també va servir per adonar-me de la importància de disposar d'un bon *firewall* i de realitzar *backups* de forma periòdica. També em van comentar una sèrie d'anècdotes que han enriquit el meu coneixement d'aquest àmbit.

²⁷ *Ransomware*: tipus de *malware* que restringeix l'accés a certes parts del dispositiu infectat i demana un rescat per treure la restricció.

CONCLUSIÓ

Offensive security és un terme que fa referència a la realització de ciberatacs dirigits a una empresa. Bàsicament, pretén millorar la fortalesa de la infraestructura buscant els seus punts febles. En l'última dècada ha esdevingut quelcom rellevant i crec que en un futur pròxim obtindrà molta més importància.

La meva part pràctica ha consistit, principalment, en l'efectuació d'ambdós atacs. Per mi ha estat una tasca emocionant. Em sento orgullós, en gran mesura, dels resultats obtinguts.

Tant l'estudi com la realització d'aquestes dues proves han esdevingut tot un repte. Per una banda, perquè disposava de molt poc coneixement previ sobre aquest tema. Per l'altra banda, perquè aquest treball ha significat un desafiament personal.

En un principi, volia esbrinar si realment seria capaç d'estudiar allò que crec que m'apassiona superant totes les dificultats que comporta. En especial referint-me a la part pràctica; era conscient que seria una labor molt complicada.

Per aquest motiu, considero que l'objectiu principal del treball ha estat assolit: he acabat dominant per complet els ciberatacs. Els objectius secundaris també han estat assolits: he creat una pàgina web i un servidor i he realitzat els dos ciberatacs amb bastant èxit.

Considero que l'únic punt que no he completat amb triomf ha estat la part pràctica de l'atac de denegació de servei. Si bé m'hagués encantat arribar a deixar la pàgina web fora de servei per un període de temps, m'he hagut de conformar en alentir-la molt i en deixar-la inaccessible eventualment. Espero en un futur acabar completant aquest objectiu personal.

Durant aquest treball he adquirit nous coneixements que prèviament desconeixia. Han servit per decantar-me cap a la branca de la ciberseguretat davant el dubte d'escollir una altra secció d'aquest àmbit (com per exemple, el *Big Data*).

També he après molt a l'hora de buscar informació. Per primer cop en la meva vida m'he vist en la situació d'haver-la de seleccionar minuciosament. He necessitat visitar

centenars de pàgines webs diferents per poder redactar adequadament el treball. En moltes ocasions trobava informació contradictòria. Això m'ha obligat a implementar la recerca d'informació a diferents idiomes. Però, sens dubte, amb aquest treball m'he adonat de l'enorme utilitat que tenen els llibres. Sigui en paper o en format digital, els llibres han estat una gran ajuda per aquest treball. M'han aportat informació molt rellevant.

Com a conclusió final, considero que l'experiència de fer aquest treball ha estat i serà un punt d'inflexió en la meua vida acadèmica. Crec firmament que els coneixements que he obtingut em serviran per a tota la vida.

Vull agrair a la meua tutora del treball, Maria José Morena, per tota la seva ajuda i consells que m'ha donat al llarg de la realització del treball.

Els meus pares es mereixen també un agraïment molt especial, pel seu suport i per les seves múltiples crítiques, sempre constructives, que han fet millorar aquest treball.

BIBLIOGRAFIA

- González, Pablo, *Ethical Hacking*. Ed. OxWORD, Madrid, 2014.
- Tori, Carlos, *Hacking Ético*, Rosario (Argentina), 2008.
https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/Hacking_Etico.pdf
- *Hacker Highschool security awareness for teens*, “Lección 3, Puertos y Protocolos”, Isecom, 2012.
http://www.hackerhighschool.org/lessons/HHS_es3_Puertos_y_Protocolos.v2.pdf
- Nixon, Allison i Camejo, Christopher, *DDoS Protection Bypass Techniques*, Waltham (Massachussetts), 2013. <https://media.blackhat.com/us-13/US-13-Nixon-Denying-Service-to-DDOS-Protection-Services-WP.pdf>
- Redacción Puntoseguridad, *El Parlament aprueba la creación de la Agencia de Ciberseguridad de Cataluña*, a: “Cuadernos de Seguridad” (20.07.2017),
<https://cuadernosdeseguridad.com/2017/07/parlament-aprueba-la-creacion-la-agencia-ciberseguridad-cataluna/>
- *Creada la Agencia de Ciberseguridad Cataluña para prevenir ataques en redes*, a: “La Vanguardia” (12.07.2017),
<http://www.lavanguardia.com/politica/20170712/424077084298/creada-la-agencia-de-ciberseguridad-cataluna-para-prevenir-ataques-en-redes.html>
- Oms, Javier, *Cataluña multiplica por 13 el gasto en ciberseguridad desde el inicio del 'procés'*, a: “El Mundo” (17.04.2017),
<http://www.elmundo.es/cataluna/2017/04/17/58f3b6d7468aeb8f068b458b.html>
- Llei Orgànica 1/2015 del codi penal, «BOE» núm. 77, de 31 de març de 2015
<https://www.boe.es/buscar/doc.php?id=BOE-A-2015-3439>
- García, Alberto, *Tu PC ahora puede ser parte de un ataque DDoS: la botnet Mirai llega a Windows*, a: “ADSLZONE” (22.02.2017),
<https://www.adslzone.net/2017/02/22/pc-ahora-puede-parte-ataque-ddos-la-botnet-mirai-llega-windows/>

- *How To Stop DDoS Attacks & Prevent DDoS Attacks From Happening*, a: “Radware” (14.4.2017), <https://security.radware.com/ddos-experts-insider/ddos-practices-guidelines/how-to-stop-ddos-attacks/>
- *DDoS Attack Definitions – DdoSPedia*, a: “Radware”, <https://security.radware.com/ddos-knowledge-center/ddospedia/>
- Pinuaga, Ramon, *Repaso histórico de ataques DDoS*, a: “Segu-Info” (18.10.2016), <http://blog.segu-info.com.ar/2016/09/repaso-historico-de-ataques-ddos.html>
- FIB, UPC, *Tema 3: TCP/IP, UDP*, <http://personals.ac.upc.edu/jsunyor/STD-T3.pdf>
- el-brujo, *Funcionamiento y configuración protección DDoS de CloudFlare*, a: “elhacker” (13.10.2014), <http://blog.elhacker.net/2014/10/funcionamiento-configuracion-proteccion-ataques-ddos-cloudflare.html>
- *Protocolos de Transporte Tutorial sobre UDP y TCP*, <http://www.it.uc3m.es/lpgonzal/protocolos/transporte.php>
- *¿QUE SON LOS PAQUETES: TCP, ping ICMP, UDP. QUE ES Ping of death, un cable transoceánico y WWW?* a: “Dakert.com” (28.02.2014), <http://dakertcom.blogspot.com.es/2012/02/que-son-los-paquetes-tcp-ping-icmp-udp.html>
- *Cómo manejan las comunicaciones de datos los protocolos TCP/IP*, <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-29/index.html>
- *¿En qué consiste la protección anti-DDoS?*, a: “OVH”, <https://www.ovh.es/anti-ddos/principio-anti-ddos.xml>
- *Qué es un protocolo de red*, a: “Culturacion”, <http://culturacion.com/que-es-un-protocolo-de-red/>
- *DDOS ATTACKS*, a: “incapsula”, <https://www.incapsula.com/ddos/ddos-attacks/>
- el-brujo, *Ataques UDP Reflection Flood DrDoS (Inundación mediante Amplificación)*, a: “elhacker” (12.06.2014) <http://blog.elhacker.net/2014/06/udp-flood-inundacion-reflection-attack-ataque.html>
- Khalimonenko, Alexander, Kupreev, Oleg i Ibragimov, Timur, *DDoS attacks in Q2 2017*, a: “Kaspersky Lab” (1.09.2017), <https://securelist.com/ddos-attacks-in-q2-2017/79241/>

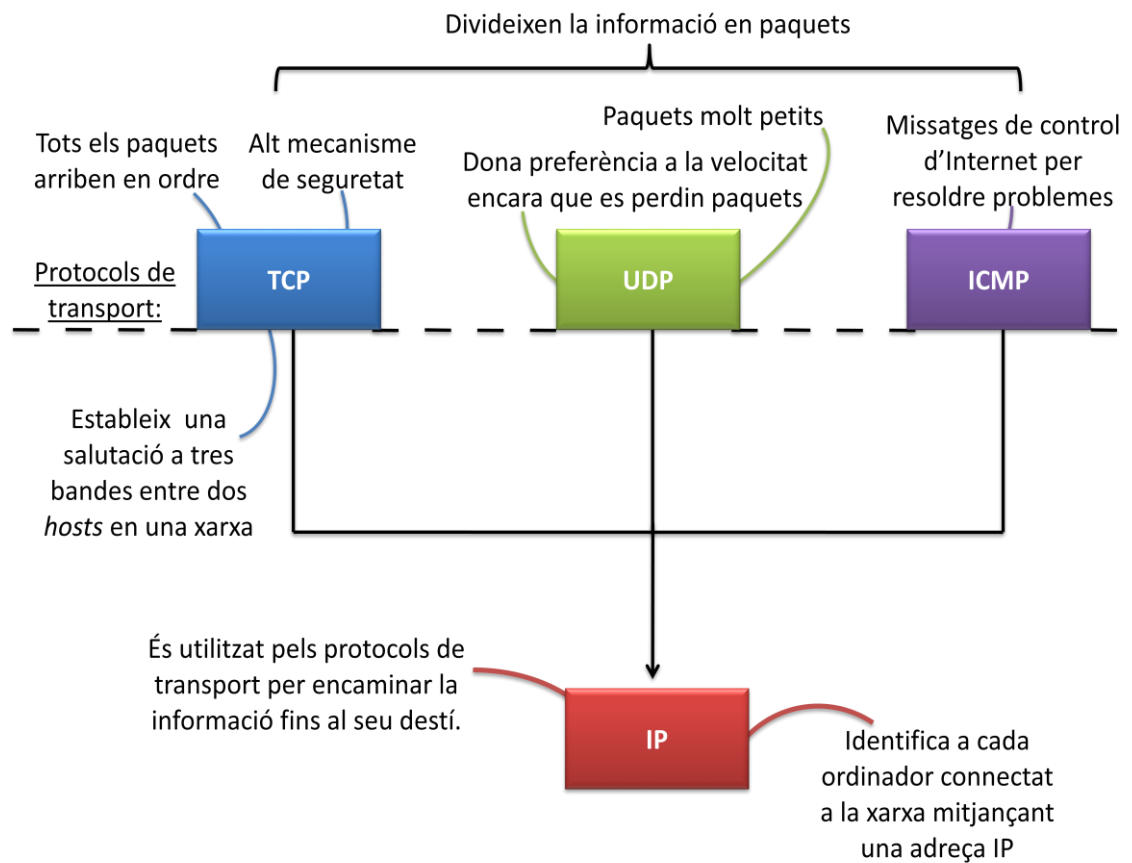
- *Advanced Persistent Threats: How They Work*, a: "Symantec"
<https://www.symantec.com/theme.jsp?themeid=apt-infographic-1>
- K. Daly, Michael, *The Advanced Persistent Threat (or Informationized Force Operations)*, a: "Raytheon" (4.11.2014),
<http://static.usenix.org/event/lisa09/tech/slides/daly.pdf>
- F. Iglesias, Pablo, *#MundoHacker: Tipos de Ataques Dirigidos (Persistentes vs Volátiles)*, <https://www.pabloyglesias.com/mundohacker-apt-frente-avt/>
- *¿Qué es phishing?*, a: "Panda Security",
<http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/>
- Aurnou, Scott, *Advanced Persistent Threats: What Are They & How Do They Work?*, a: "TheSecurityAdvocate" (21.10.2013)
<http://www.thesecurityadvocate.com/2013/10/21/advanced-persistent-threats-what-are-they-how-do-they-work/>
- Inteco, *¿QUÉ SON LAS AMENAZAS PERSISTENTES AVANZADAS (APTs)?*,
http://egov.ufsc.br/portal/sites/default/files/cdn_apt.pdf
- CA technologies, *Defensa frente a amenazas persistentes avanzadas: Estrategias para la nueva era de ataques*,
<http://www3.ca.com/es/~media/files/ebooks/ca-apt-ebook-esn.aspx>
- Koehler, Ed, *APTs Part 2: How the Advanced Persistent Threat Works*, a: "Avaya" (1.02.2017) <https://www.avaya.com/blogs/archives/2017/02/apts-part-2-how-the-advanced-persistent-threat-works.html>
- Craig, Peter, *What is a sandbox? And why do I need one to defend against advanced threats?*, a: "Sophos News" (13.04.2016)
<https://news.sophos.com/en-us/2016/04/13/what-is-a-sandbox-and-why-do-i-need-one-to-defend-against-advanced-threats/>
- *Fortinet ATP (Includes Sandboxing)*,
<https://www.fortinet.com/solutions/enterprise-midsize-business/advanced-threat-protection.html>
- Isaca, *Advanced Persistent Threat Awareness*,
<http://www.trendmicro.de/media/misc/apt-survey-report-en.pdf>

- *Malware and Advanced Persistent Threats - How Long is Too Long to go Undetected?*, a: "Esentire" (24.06.2016),
<https://www.esentire.com/blog/malware-and-advanced-persistent-threats-how-long-is-too-long-to-go-undetected/>
- *DEFINICIÓN TÉRMINOS DE SOFTWARE*, a: "SoftDoit"
<https://www.softwaredoit.es/definicion/index.html>
- *Anexo:Ciberataques*, a: "Wikipedia" (21.06.2017),
<https://es.wikipedia.org/wiki/Anexo:Ciberataques>
- *Online Web Tutorials*, <https://www.w3schools.com/>
- *Glosario de Informática e Internet*, (23.06.2017)
<http://www.internetglosario.com/>
- Gordo, Roberto, *La transmisión de información en Internet*,
<http://www.monografias.com/trabajos32/transmision-informacion-internet/transmision-informacion-internet.shtml>

ANNEXES

Annex I: Esquema sobre protocols i paquets d'Internet.

Per entendre millor l'apartat dels atacs de denegació de servei, he fet un esquema explicant els diferents protocols que es mencionen en aquest treball.



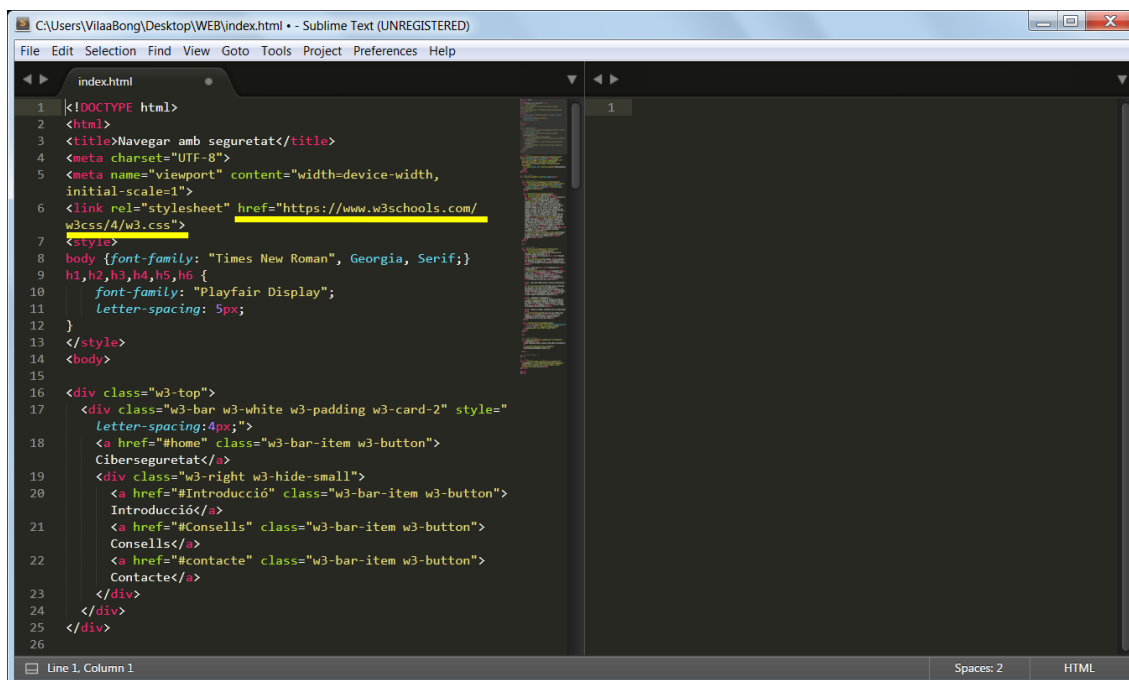
Annex II: Glossari

- **Anonymous:** grup hacktivista que defensa principalment la llibertat d'expressió i la independència d'Internet.
- **Captcha:** prova de desafiament-resposta utilitzada per esbrinar quan un usuari és humà o és un "robot".
- **Cuc:** tipus de *malware* que té la propietat de multiplicar-se a si mateix.
- **Formatejar (informàtica):** eliminar tot el contingut d'una unitat, tornar als valors de fàbrica.
- **Google hacking:** tècnica informàtica utilitzada per filtrar informació a través del buscador Google.
- **Man In The Middle:** ciberatac que consisteix en introduir-se en la comunicació entre dos sistemes per així controlar tot el tràfic i aconseguir dades sensibles.
- **Metadades:** són dades que descriuen a altres dades. Per exemple: les metadades de una fotografia feta des d'un *smartphone* revelen la localització on s'ha fotografiat.
- **Rootkit:** tipus de *malware* que permet accés total a un dispositiu i que es manté completament ocult al sistema.
- **Spoofing:** tècnica mitjançant la qual un criminal pot falsificar les seves dades en una comunicació entre dos dispositius. La més comuna és *IP Spoofing*.
- **Troia:** tipus de *malware* que aparenta ser un programa legítim, però que a l'executar-lo brinda accés total al dispositiu a l'atacant.

Annex III: Creació de la pàgina web i del servidor

El codi de la pàgina web ha estat copiat i modificat del següent URL:
https://www.w3schools.com/w3css/tryw3css_templates_gourmet_catering.htm

El vaig modificar amb el programa Sublime Text 3.

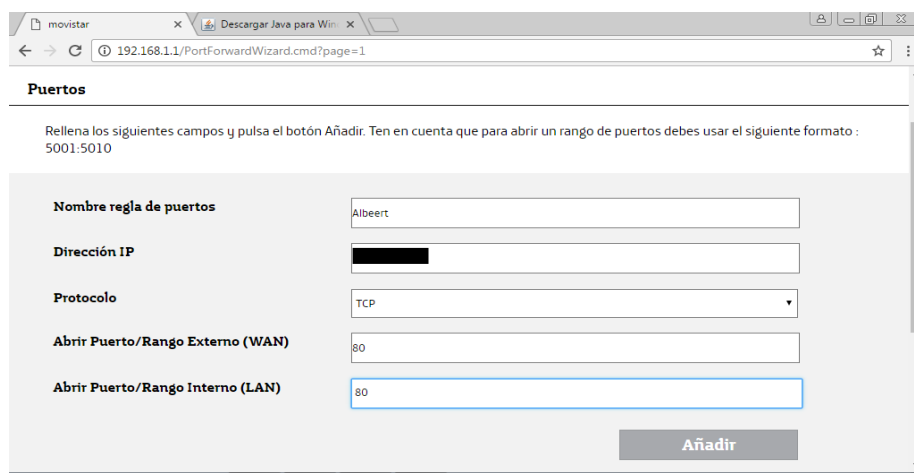


```
1 <!DOCTYPE html>
2 <html>
3 <title>Navegar amb seguretat</title>
4 <meta charset="UTF-8">
5 <meta name="viewport" content="width=device-width,
6   initial-scale=1">
7 <link rel="stylesheet" href="https://www.w3schools.com/
8   w3css/4/w3.css">
9 <style>
10 body {font-family: "Times New Roman", Georgia, Serif;}
11 h1,h2,h3,h4,h5,h6 {
12   font-family: "Playfair Display";
13   letter-spacing: 5px;
14 }
15 </style>
16 <body>
17 <div class="w3-top">
18 <div class="w3-bar w3-white w3-padding w3-card-2" style="
19   letter-spacing:4px;">
20 <a href="#home" class="w3-bar-item w3-button">
21   Ciberseguretat</a>
22 <div class="w3-right w3-hide-small">
23 <a href="#Introducció" class="w3-bar-item w3-button">
24   Introducció</a>
25 <a href="#Consells" class="w3-bar-item w3-button">
26   Consells</a>
27 <a href="#contacte" class="w3-bar-item w3-button">
28   Contacte</a>
29 </div>
30 </div>
31 </div>
```

Fig. 14: Fragment del codi de la pàgina web, amb el programa Sublime Text 3

Es pot veure com el document fa referència a una pàgina web (subratllat amb color groc). Aquesta pàgina web no és més que el codi d'un estil propi creat per la companyia w3schools. És un codi molt complex que fa que el format de la web sigui molt estètic.

La creació del meu servidor web propi va ser una tasca complicada. Primerament vaig obrir un port des de l'adreça IP del router.



Puentes	
Rellena los siguientes campos y pulsa el botón Añadir. Ten en cuenta que para abrir un rango de puertos debes usar el siguiente formato : 5001:5010	
Nombre regla de puertos	Albeert
Dirección IP	[Redacted]
Protocolo	TCP
Abrir Puerto/Rango Externo (WAN)	80
Abrir Puerto/Rango Interno (LAN)	80
<button>Añadir</button>	

Fig. 15: Obertura del port 80 per a poder crear el servidor

Després, vaig instal·lar el programa Xampp, l'encarregat de fer funcionar el servidor. Vaig tenir una sèrie de problemes amb els ports i amb el *firewall*, però finalment tot va sortir bé.

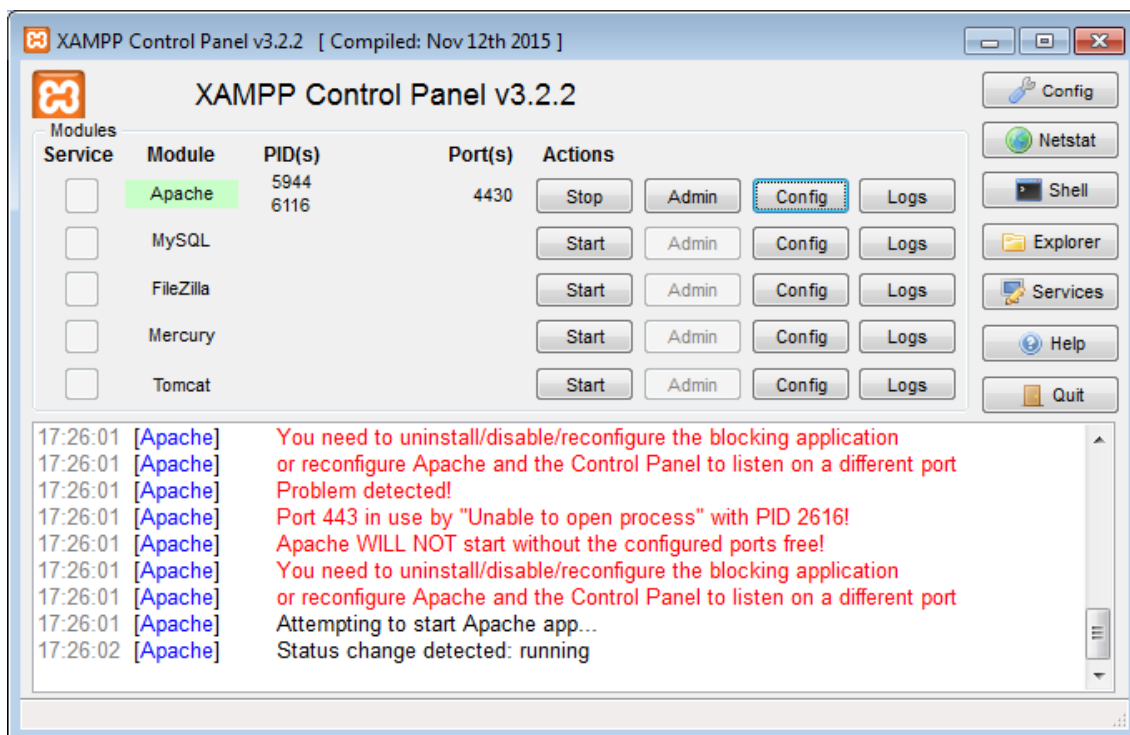


Fig. 16: Programa Xampp

Un cop acabada la instal·lació de Xampp, va tocar escollir domini. Des de la pàgina web noip.com vaig poder quedar-me amb un subdomini de forma gratuïta. Només va faltar instal·lar el programa DUC al servidor i ja tenia la meua pàgina web en un LAN

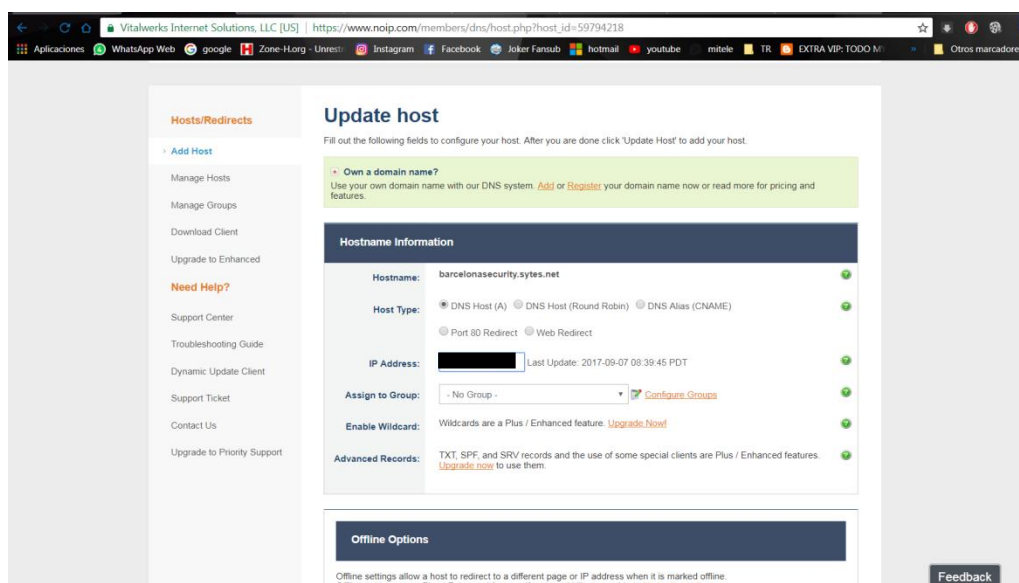


Fig. 17: Escollint el domini des de noip.com

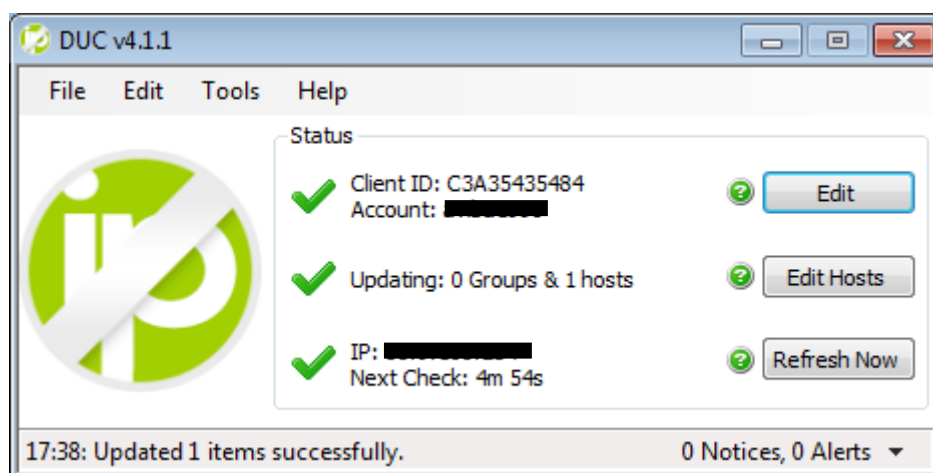


Fig. 18: Executant DUC

Finalment, la web ja estava disponible. Actualment, no disposa de l'URL de <http://barcelonasecurity.sytes.net/>, ja que l'ordinador que actuava com a servidor està apagat. No obstant això, la vaig allotjar en un servidor gratuït, 000webhostapp.



Fig. 19: La meva pàgina web sent accedida des d'un altre dispositiu

Annex IV: Atac d'amenaça persistent avançada

Per realitzar l'atac d'amenaça persistent avançada, vaig fer ús del troià DarkComet.

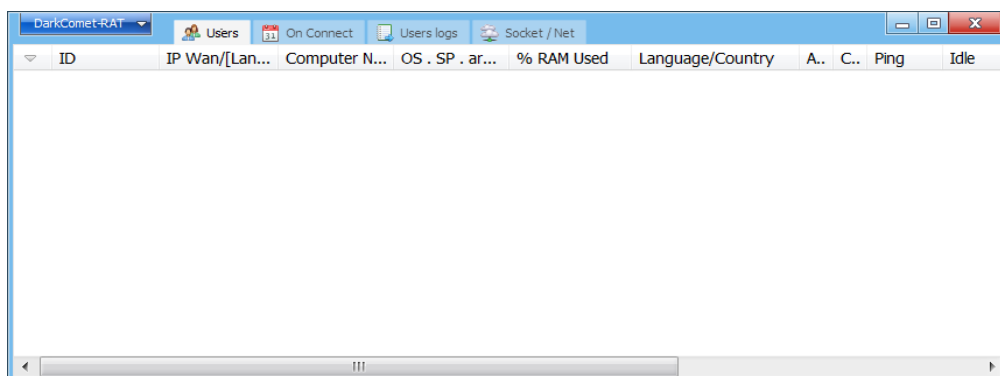


Fig. 20: Menú d'inici del troià DarkComet

Vaig haver de fer una sèrie de canvis en el *firewall* del meu ordinador (ordinador atacant).

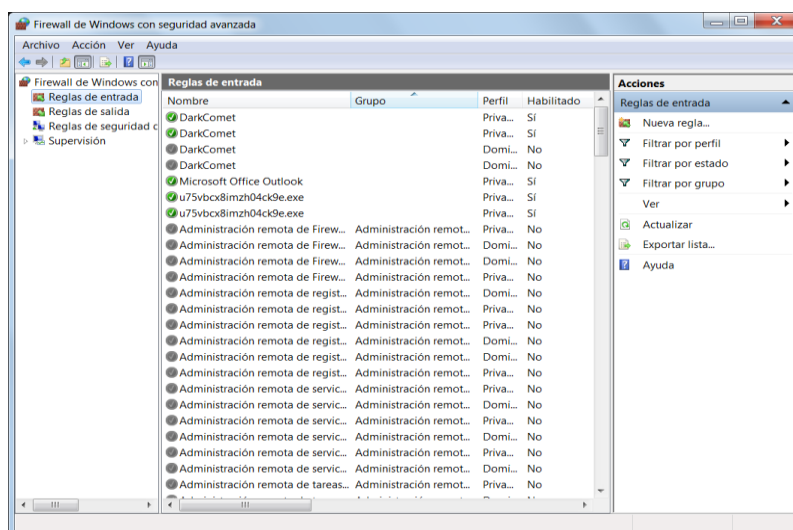


Fig. 21: Canvis del firewall per tal de tenir un bon funcionament del troià

Vaig decidir que la icona del malware fos idèntic al de la famosa xarxa social: Facebook.

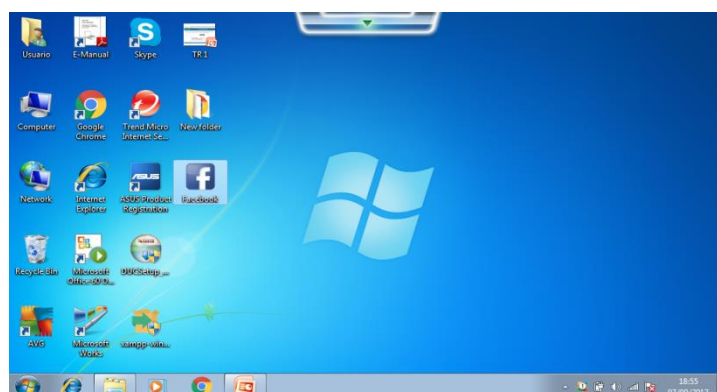


Fig. 22: Escriptori de la víctima (amb l'icona del troià simulant Facebook)

Un cop executat, el programa ja m'indicava la IP de la víctima i alguns detalls.

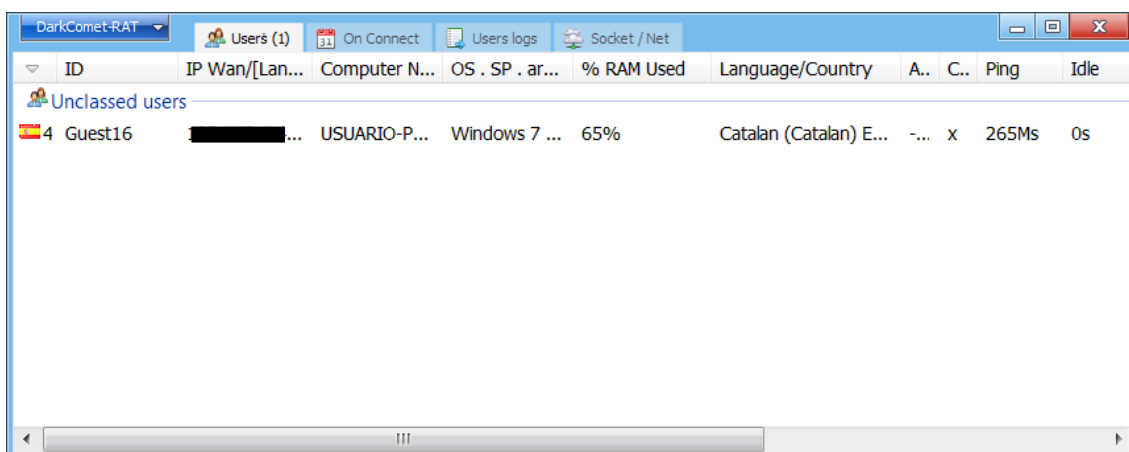


Fig. 23: Menú de DarkComet un cop el troia va ser executat

Entre les diferents opcions que tenia com a atacant, una de les més interessants és l'obtenció de contrasenyes guardades a l'ordinador.

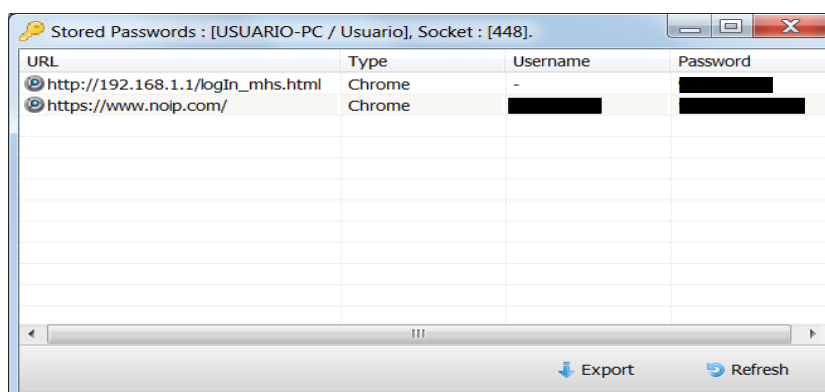


Fig. 24: Contrasenyes guardades al dispositiu de la víctima obtingudes per l'atacant

Una altra opció a destacar és la d'espiar la *webcam* (era un vídeo).



Fig. 25: Captura del vídeo des de la webcam de la víctima

Però sens dubte, l'opció més perillosa que tenia era la d'obtenir accés remot a l'ordinador.

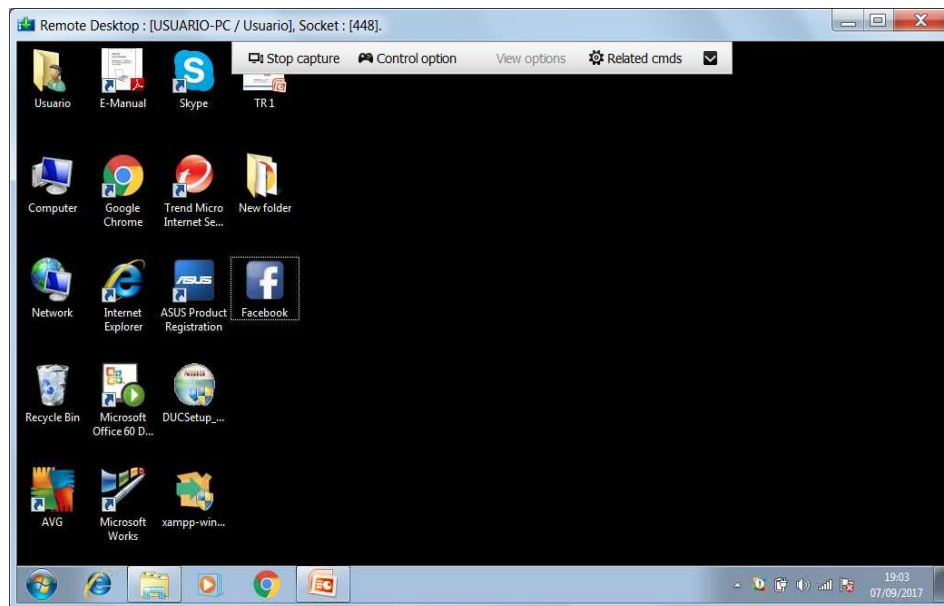


Fig. 26: Accés remot a l'escriptori de la víctima

Vaig tenir accés a qualsevol arxiu.

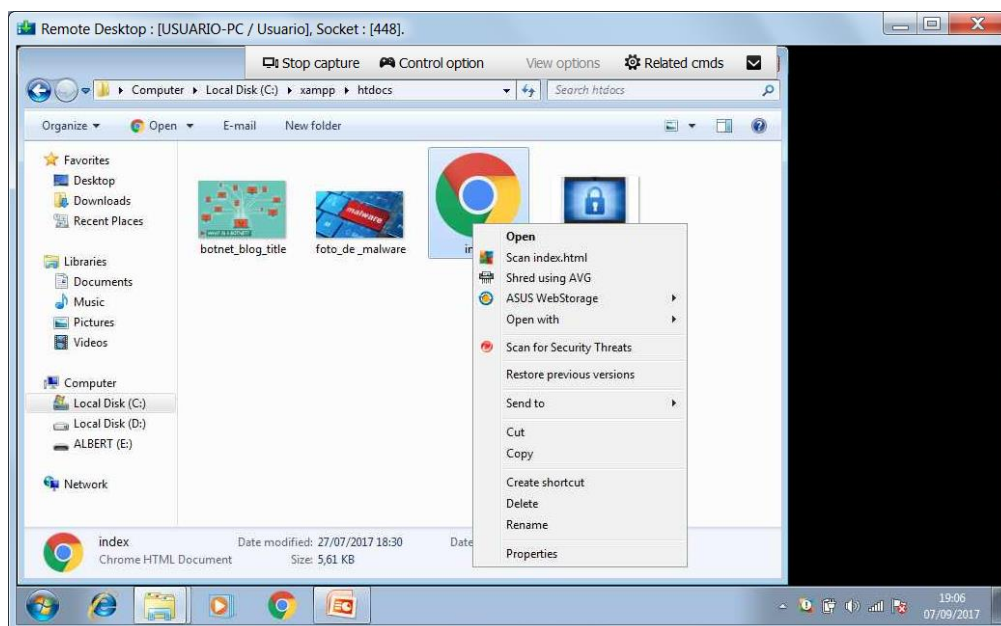


Fig. 27: Accés total als arxius de la víctima

Annex V: Atac de denegació de servei

Per realitzar l'atac de denegació de servei, vaig fer servir l'eina LOIC. En un principi vaig tenir problemes d'incompatibilitat.

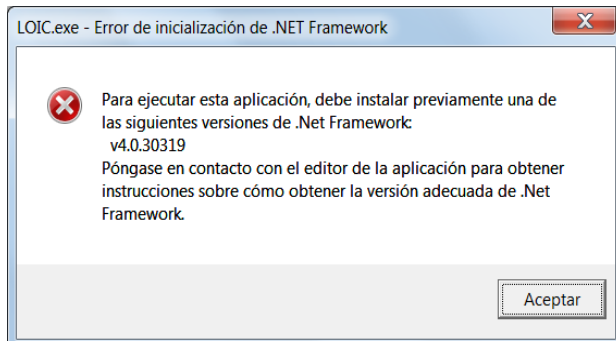


Fig. 28: Problemes amb .NET Framework

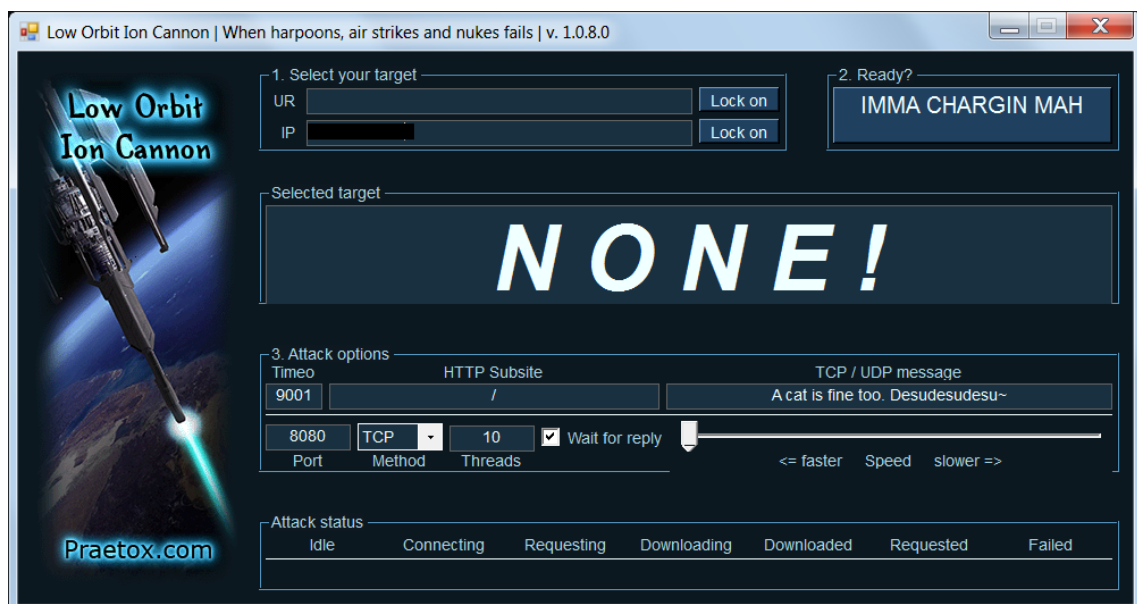


Fig. 29: Menú principal de LOIC