ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

"OSINT pratico con tool gratuiti o quasi… ossia come si fanno le investigazioni da fonti non convenzionali"

Massimiliano Graziani CFE CIFI CFIP CDFP OPSA ACE TCNU

Roma 14/05/2021

Presentazione relatore

Massimiliano Graziani *attualmente CEO Cybera Srl e CISO Adora ICT srl*

Fondatore, insieme ad altri nel 2005 del capitolo italiano dell'OWASP.

Socio fondatore del capitolo italiano dell' International Information Systems Forensics Association (IISFA), e dell'Osservatorio Nazionale Informatica Forense (ONIF), è in possesso delle seguenti certificazioni internazionali:

- CIFI (Certified Information Forensics Investigator rilasciata da IISFA)
- CFE (Certified Fraud Examiner rilasciata da ACFE)
- ACE (AccessData Certified Examiner rilasciata da AccessData)
- OPSA (OSSTMM Professional Security Analyst rilasciata da ISECOM)
- CIFIP (Certified Forensic Investigation Professional rilasciata da IICFIP)
- CDFP (Certified Digital Forensics Professional rilasciata da IICFIP).

Docente in materia di Digital Forensics Pratica presso Scuola di Polizia Tributaria della Guardia di Finanza (Corso Operativo di Computer Forensics con Logicube Dossier e Falcon), Università La Sapienza Roma (Corso Informatica Giuridica con Aterno), Università LUMSA Roma (Corso Diritto Penale dell'Informatica con Zanotti), Università di Salerno (Convegno La Tecnologia al servizio dell'Indagine Scientifica con De Santis, Cattaneo, Palmieri), Università del Molise (Master Information Security Management – Modulo Computer Forensics con Perrone), Università degli studi Link Campus University di Roma (modulo forensics di vari master, ultimo con Saccone). Docente volontario presso IISFA, OLAF, FF.OO., Consiglio Superiore Magistratura Milano, Ministero Economia e Finanze UCAMP, ISACA Roma e ACFE Italia e Centro Interforze di Formazione Intelligence/GE, Board of Directors ACFE Central.

Maggiori info sul mio background: www.cobrasoft.it

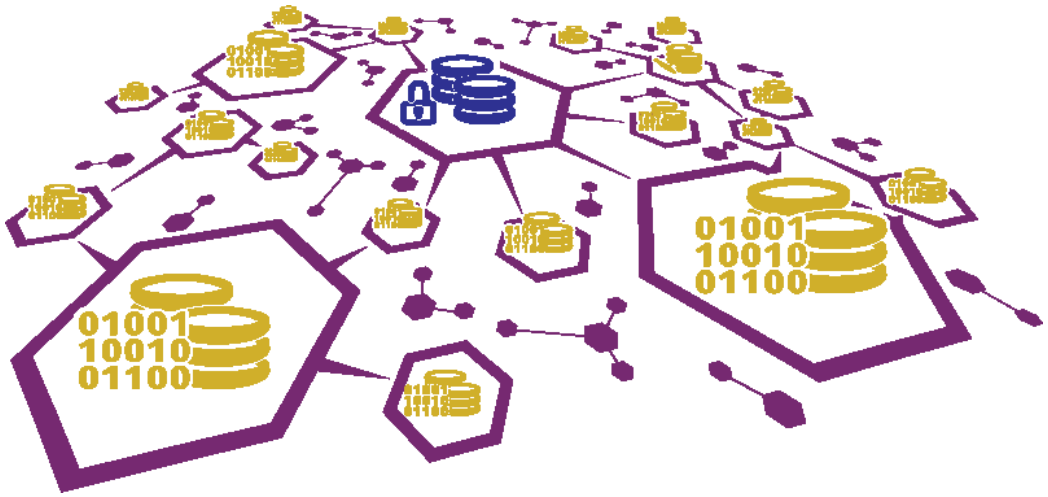
Agenda

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

ATTENZIONE:

QUELLO CHE VEDRETE IN QUESTO SEMINARIO,
E' MATERIALE A SCOPO EDUCATIVO.
VI RICORDO CHE EFFETTUARE PORT SCANNING E VULNERABILITY ASSESSMENT SENZA ESSERE AUTORIZZATI COSTITUISCE UN REATO.

Open Source INTelligence, acronimo OSINT
(in italiano: "Intelligence su fonti aperte"), è quella disciplina dell'intelligence
che si occupa della ricerca, raccolta ed analisi di dati e di notizie
tratte da fonti aperte.



OSINT è un processo di raccolta ed elaborazione di informazioni altamente degradabili…

…“Un sistema ‘puro’ che non ha bisogno di compromessi oscuri con le fonti, non viola la legge con attività investigative illegali, ma si basa solo sulla capacità tecnica e operativa di trovare le informazioni, la mentalità investigativa, la conoscenza delle tecniche di analisi e correlazione dei dati e infine il lavoro metodico e organizzato di consultazione delle fonti aperte che sono per definizione accessibili a tutti”…

(tratto da: Leonida Reitano - "Esplorare Internet”)

Classificazione attività di intelligence:

HUMINT (Human Intelligence - informatori)

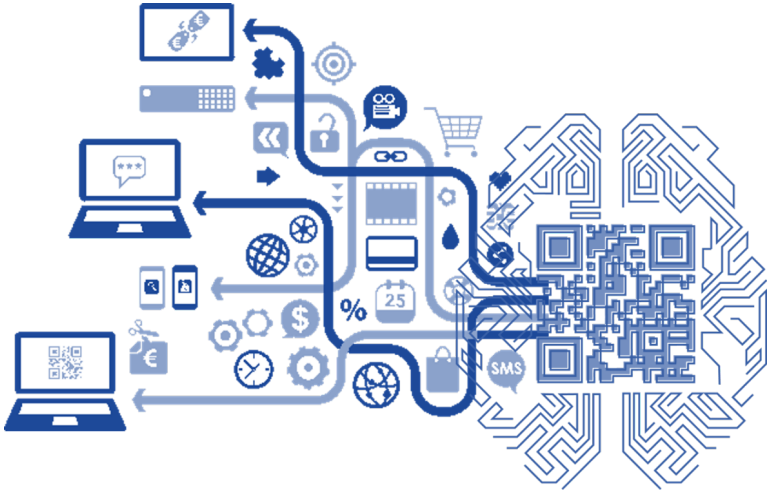
SIGINT (Signals Intelligence - intercettazioni) vediamo subito un esempio!

GEOINT o IMINT (Image intelligence - immagini satellitari, aerei spia e altri vettori)

OSINT (Open Source intelligence)

TECHINT (Technical Intelligence)

FININT (Financial Intelligence)



SIGINT (Signals Intelligence - intercettazioni) vediamo subito un esempio!

Wide-band WebSDR in Enschede

Non sicuro | websdr.ewi.utwente.nl:8901

Amateur radio club ETGD
PI4THT

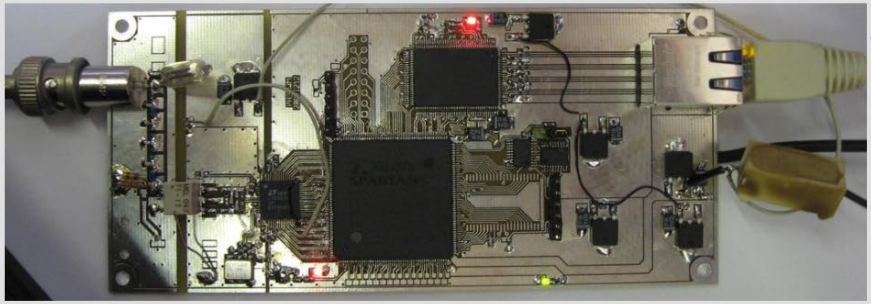
Faculty for Electrical Engineering,
Mathematics and Computer Science

University of Twente
Enschede - The Netherlands

Wide-band WebSDR

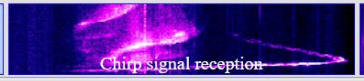
On this page you can listen to and control a short-wave receiver located at the amateur radio club ETGD at the University of Twente. In contrast to other web-controlled receivers, this receiver can be tuned by multiple users simultaneously, thanks to the use of Software-Defined Radio.

This site, which in 2008 was the very first WebSDR site ever, was finally reactivated in July 2012 after an interruption of more than 1.5 years; read also the old news since then.



The system is currently composed of a "Mini-Whip" antenna, a homebuilt SDR board (as pictured; see here for background) which samples the entire shortwave spectrum and sends all of this via a gigabit ethernet link to a PC, where a special version of the WebSDR server software processes it. The Mini-Whip is based on a design from PA0RDT (google finds it); see some pictures. The active receiving element is about 5 by 10 cm large. Such an antenna only works well with a good grounding; ours is on top of a 20m high building, the upper part of which is all metal.

Other services available on this system:



Questions and remarks about this WebSDR can be sent to the developer and maintainer: pa3fwm@websdr.org (but please check the FAQ first).

Please log in by typing your name or callsign here (it will be saved for later visits in a cookie):

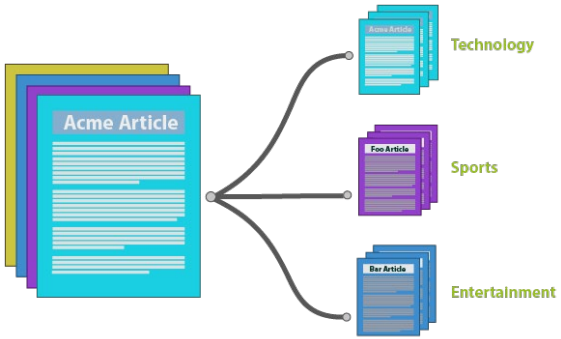
DATI PUBBLICI (rendiconti governativi, piani finanziari, dati demografici, notizie stampa, ecc.)
MEZZI DI COMUNICAZIONE DI MASSA
DATABASE EDITORIALI
FILE MULTIMEDIALI
DATABASE ISTITUZIONALI

trattati con la conscenza di:

STRUMENTI DI HACKING (ottenere informazioni sulle identità digitali)
AVANZATO USO DEI MOTORI DI RICERCA (usando ad esempio GHDB)
UTILIZZO DI PORTALI DI INVESTIGAZIONI ON LINE (informazioni istituzionali su persone fisiche o giuridiche, partecipazioni azionarie/societarie, proprietà immobiliari, ecc.)
TECNICHE DI ANALISI INVESTIGATIVA (analizzare e poi rappresentare anche graficamente le informazioni estrapolate)

e capacità di analisi:

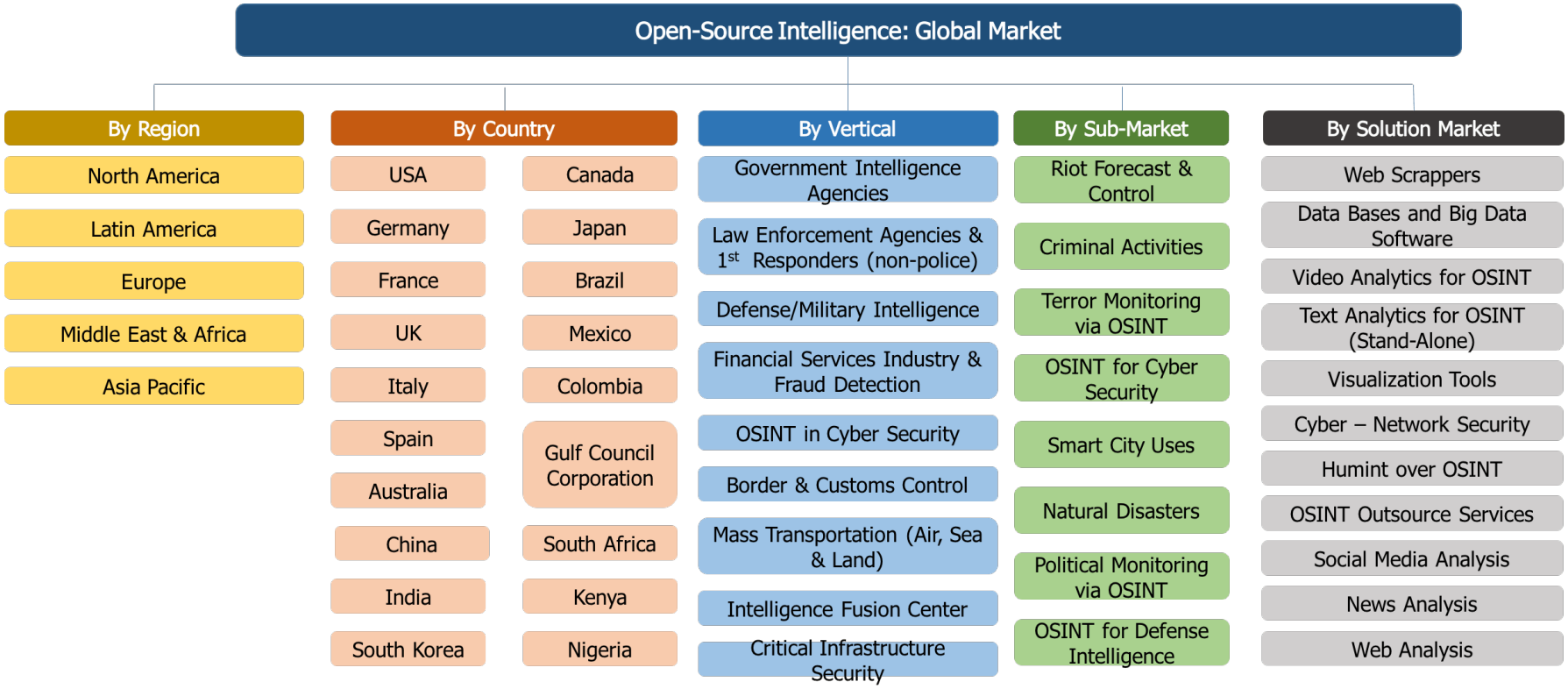
INDIVIDUAZIONE, VALUTAZIONE, SELEZIONE ED ELABORAZIONE DEI DATI MIRATA AD OTTENERE INFORMAZIONI DI VALORE
Circa l'80% delle informazioni di pertinenza investigativa viene raccolta tramite OSINT
Circa il 90% delle attività di information gathering si basa su fonti aperte



Classificazione delle FONTI:

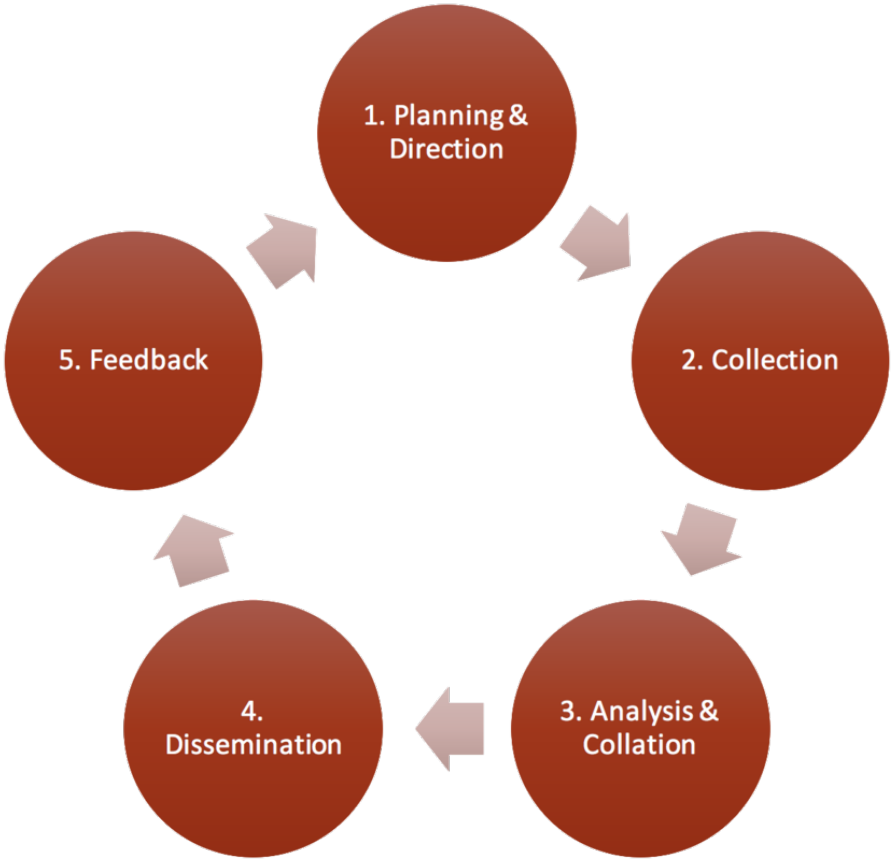
INFORMAZIONI GENERALI (info provenienti dal web o dai media)
INFORMAZIONI A PAGAMENTO (database commerciali o siti a pagamento)
ESPERTI (interviste e opinioni di esperti, tecnici, specialisti, ecc)
DOCUMENTI "GRAY" (brevetti, report, pubblicazioni ad uso interno, atti di convegni, ecc.)
O.D.S. (Open Source Data): Dati grezzi, generici, generati da registrazioni, fotografie, immagini satellitari, in generale tutta la documentazione pubblicata su canali pubblici da fonti non attendibili
O.S.I.F. (Open Source Information): Informazione pubblica che ha subito un processo di filtraggio e convalida, come giornali, libri, comunicazioni e divulgazioni da fonti attendibili
L'O.S.I.N.T. è l'unione di ODS e OSIF, consiste in informazioni filtrate, cercate, selezionate e destinate a soddisfare una specifica richiesta informativa

A chi interessa?



Le 5 fasi dell'OSINT:

1) Planning e Direction (definisco obiettivo e fonti)
2) Collection (raccolgo i dati)
3) Analysis e Collation (analizzo e confronto)
4) Dissemination (diffusione dei report)
5) Feedback (misuro il gradimento del cliente)



Operazioni manuali o automatiche?

Manuali:
Raccolta e confronto oneroso, difficilmente “scalabile” ed elevato rischio di “perdere” informazioni

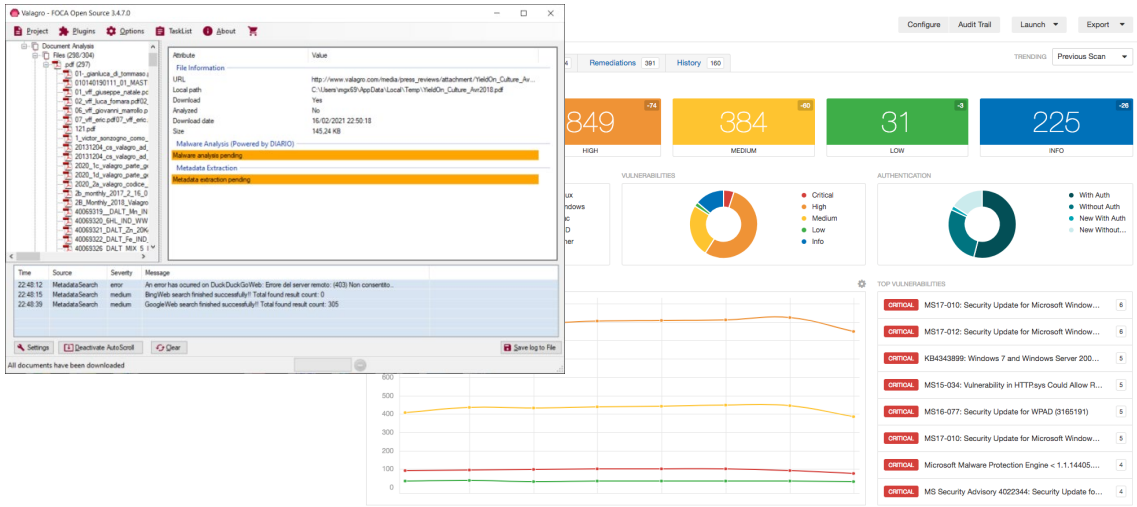
Automatiche:
Potenzialmente molto efficace, facilmente “scalabile” ed integrabile, richiede enormi investimenti, le tecnologie sono in rapida convergenza

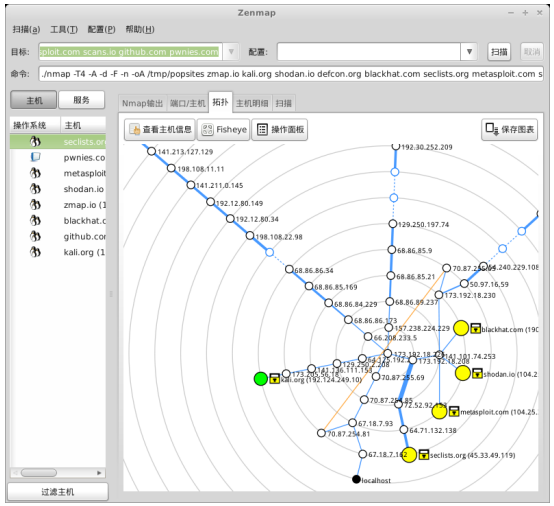
Agenda

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

INFORMATION GATHERING ATTIVA

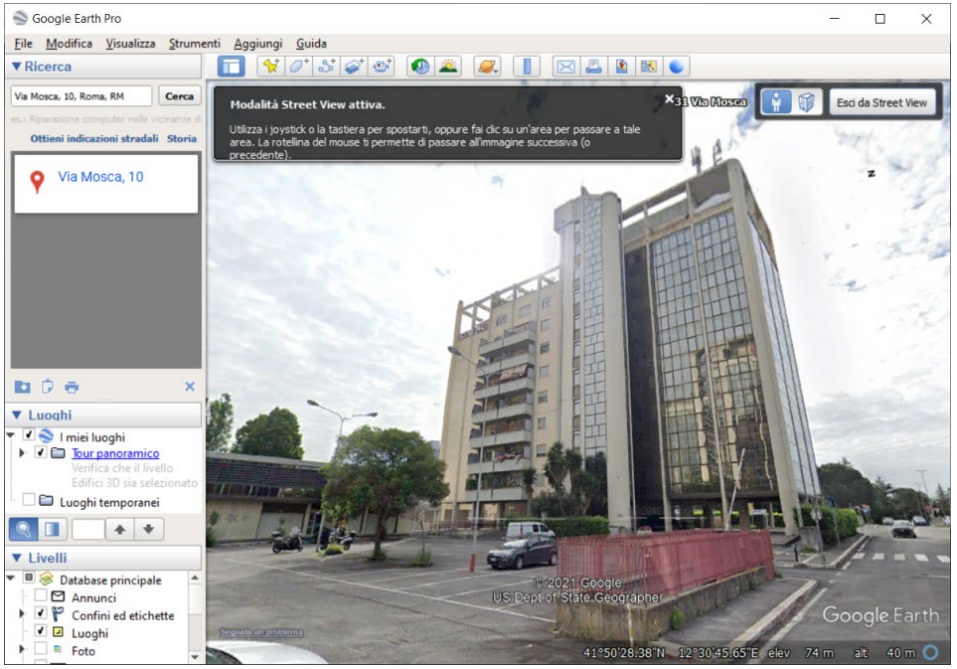
- Tracing
- Port Scanning (NMAP)
- Scansione dei siti web (esempi: analisi dei robots.txt, ecc.)
- Scansione delle risorse (esempi: ricerche dentro repository FTP, ricerche tramite FOCA, ecc.)
- Rilevamento di configurazioni errate o predefinite (esempi: GHDB, directory listing, ecc.)
- Mappatura delle vulnerabilità (esempi: vulnerability assessment, scansioni con Nessus, scansioni con OpenVAS, ecc.)
- Ricerca Exploit utilizzabili





INFORMATION GATHERING PASSIVA

- Analisi dei dati della rete (esempio: sniffing con Wireshark, uso di TCPdump, ecc.)
- Motori di ricerca (google, bing, ecc.)
- Social Network (analisi Facebook, LinkedIn, ecc.)
- Analisi header email (manuale oppure on line)
- Crawling (download e analisi contenuto dei siti web)
- Analisi tra entità (esempio: Maltego)
- Analisi di mappe (Google Hearth)



CYBER INTELLIGENCE

PASSIVA

OSINT
Open Source Intelligence, Intercettazioni non invasive, interviste, opinioni, ecc.
Non genera nessun traffico di rete.

SEMI PASSIVA

Stealth Intelligence
Modalità attiva che si svolge sotto la soglia di rilevamento, più costosa, genera un traffico di rete normale.

ATTIVA

Intelligence Proattiva
Social engeenering, attività sotto copertura, sfruttamento di vulnerabilità, utilizzo di malware, ecc. Genera un traffico di rete anomalo e rilevabile.

NETWORK INFORMATION GATHERING

- IP
- DNS
- Domini e Whois
- Siti web e web server
- Posta elettronica
- Data Base

ANALISI DI UN SITO WEB

- Chi ha registrato un dominio
- Chi sta gestendo il sito
- Dove si trova l'hosting
- Domini collegati
- Email e numeri di telefono
- Il passato di un sito web
- ecc.

Agenda

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

NMAP HANDS ON

nmap — Strumento di network exploration e security / port scanner
znmap è la versione GUI (con interfaccia grafica) per windows.

nmap [<Tipo di Scansione> ...] [<Opzioni>] { <Obiettivo> }

Nmap ("Network Mapper") è uno strumento open-source per l'esplorazione della rete e l'auditing. È stato progettato per scansionare rapidamente reti di grandi dimensioni, ma è indicato anche per l'utilizzo verso singoli host. Nmap usa pacchetti IP "raw" (grezzi, non formattati) in varie modalità per determinare:

- quali host sono disponibili su una rete
- che servizi (nome dell'applicazione e versione) vengono offerti da questi host
- che sistema operativo (e che versione del sistema operativo) è in esecuzione
- che tipo di firewall e packet filters sono usati

Nonostante Nmap sia comunemente usato per audits di sicurezza, molti sistemisti e amministratori di rete lo trovano utile per tutte le attività giornaliere come ad esempio l'inventario delle macchine presenti in rete, per gestire gli aggiornamenti programmati dei servizi e per monitorare gli host o il loro uptime.

NMAP HANDS ON

L'output di Nmap è un elenco di obiettivi scansionati, con informazioni supplementari per ognuno a seconda delle opzioni usate. Tra queste informazioni è vitale la "tabella delle porte interessanti". Questa tabella elenca il numero della porta e il protocollo, il nome del servizio e lo stato attuale.
Lo stato può essere

- open (aperto)
- filtered (filtrato)
- closed (chiuso)
- unfiltered (non filtrato)

Aperto significa che vi è sulla macchina obiettivo un'applicazione in ascolto su quella porta per connessioni o pacchetti in entrata. Filtrato significa che un firewall, un filtro o qualche altro ostacolo di rete sta bloccando la porta al punto che Nmap non riesce a distinguere tra aperta o chiusa. Le porte chiuse non hanno alcuna applicazione in ascolto, anche se potrebbero aprirsi in ogni momento. Le porte vengono classificate come non filtrate quando rispondono ad una scansione di Nmap, ma non è stato possibile determinare se sono aperte o chiuse. Nmap mostra le combinazioni aperta|filtrata e chiusa|filtrata quando non può determinare quale dei due stati descrive una porta.
La tabella delle porte può anche includere dettagli quali le versioni dei software disponibili se è stata usata l'opzione appropriata.

NMAP HANDS ON

Prima di scansionare un target, Nmap proverà ad inviare un ICMP echo request per verificare che l'host sia “alive”.
Questo serve a salvare del tempo quando si scansionano più host, se gli host non sono online non si perderà del tempo inutilmente. Dato che le ICMP request sono spesso bloccate dal firewall, Nmap tenterà di connettersi anche alle porte 80 e 443, visto che spesso queste porte sono aperte. Le opzioni “discovery” di default non sono utili quando si scansionano sistemi messi in sicurezza. Nmap dispone di molti plugin già pronti e la maggior parte delle volte, non ha bisogno di utilizzare parametri particolari, quando è necessario, dispone comunque di moltissime opzioni.
I profili disponibili su ZNMAP sono:

Intense scan - Una scansione completa.
Contiene il controllo sul Sistema Operativo utilizzato, sulla versione, sugli script, effettua il traceroute ed è piuttosto aggressiva. Viene considerata una scansione intrusiva.
Ping scan - Questa scansione controlla semplicemente se il bersaglio è online, non controlla nessuna porta.
Quick scan - È più veloce della scansione regolare grazie a tempistiche aggressive e al fatto che effettua lo scan solo di alcune porte.
Regular scan - È la scansione che viene effettuata di base da Nmap, se non modificate alcun parametro. Pingherà il bersaglio e vi restituirà le eventuali porte aperte.
Slow comprehensive scan - È la scansione più verbose che include la maggior parte delle opzioni.

NMAP HANDS ON

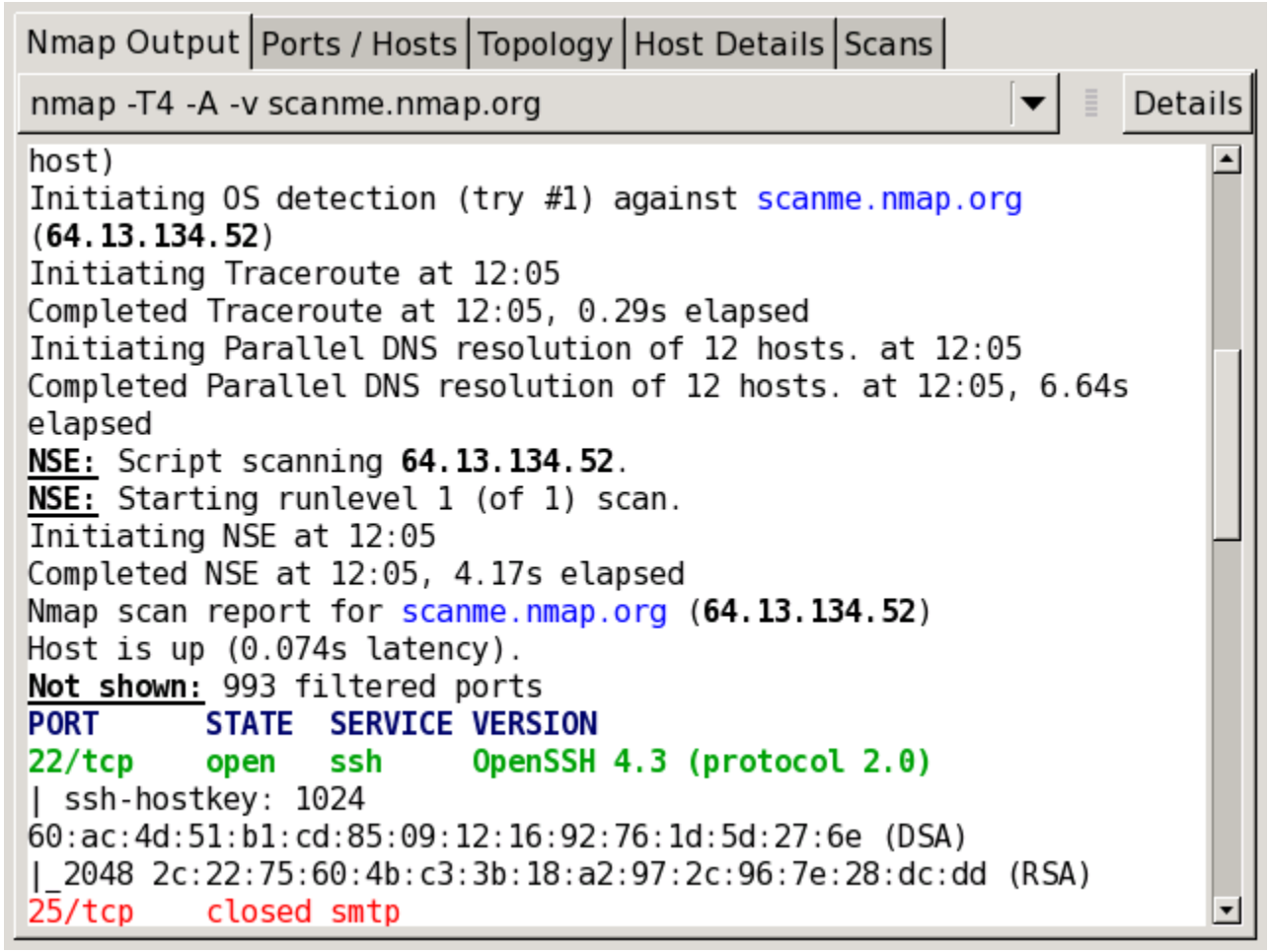
Puoi aggiungere dei parametri per modificare il tipo di scansione e aggiungere o rimuovere specifici particolari dai risultati. Cambiare i parametri della scansione, ne varierà l'intrusività.
Puoi utilizzare più parametri separati da uno spazio. I parametri vanno inseriti prima del target:

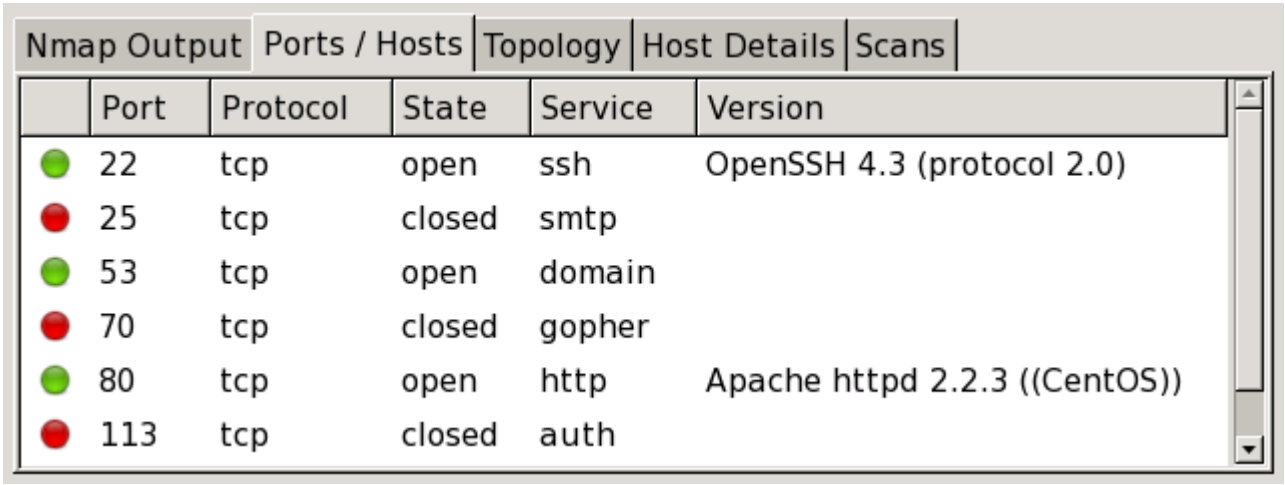
nmap <parametro> <parametro> <target>

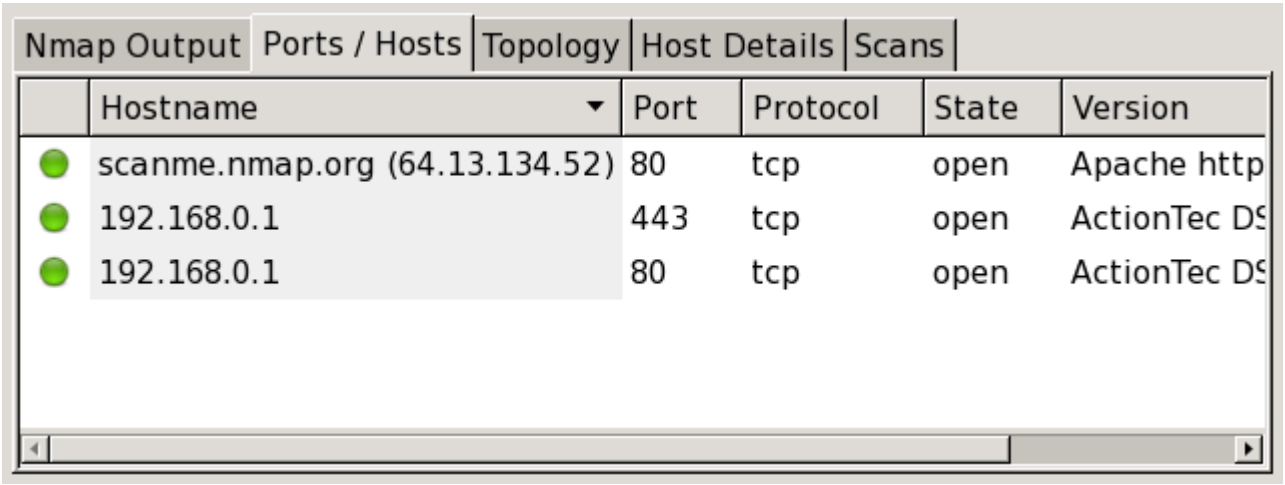
Quando la scansione sarà terminata, vedrete il messaggio: "Nmap done" in cima alla scheda con l'output.
Potrai ora controllare i risultati, a seconda del tipo di scansione selezionata. Tutti i risultati saranno elencati nella scheda Nmap Output, ma puoi usare le altre schede per controllare nel dettaglio i risultati specifici.

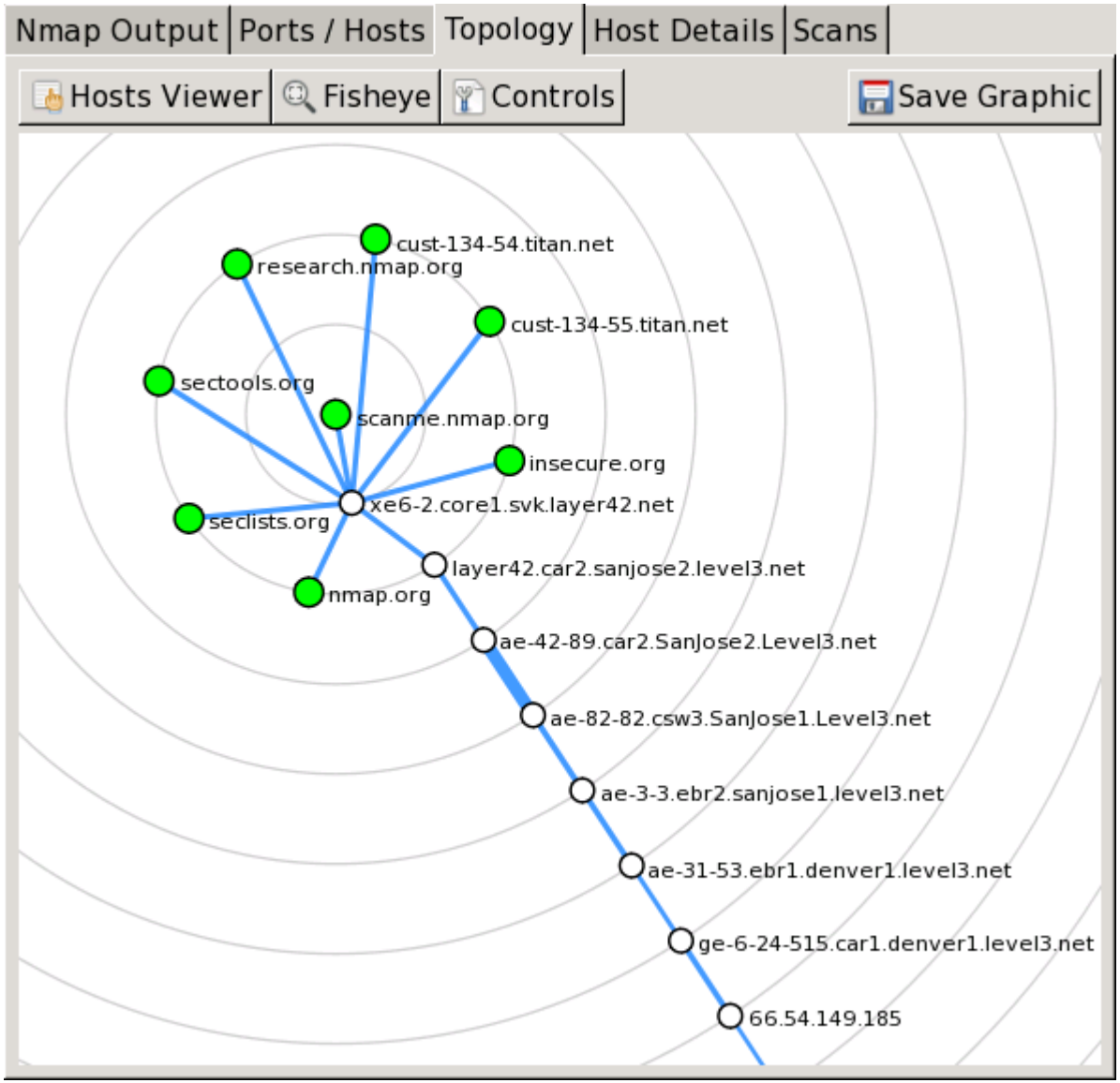
- Ports/Hosts: mostra i risultati elencando le porte e i servizi corrispondenti.
- Topology: mostra il traceroute per la scansione appena effettuata.
- Host Details: Questa scheda mostra tutto ciò che la scansione ha collezionato sul bersaglio durante la scansione.
- Scans: Questa scheda memorizza i comandi usati per lanciare le tue scansioni precedenti per riutilizzarle.

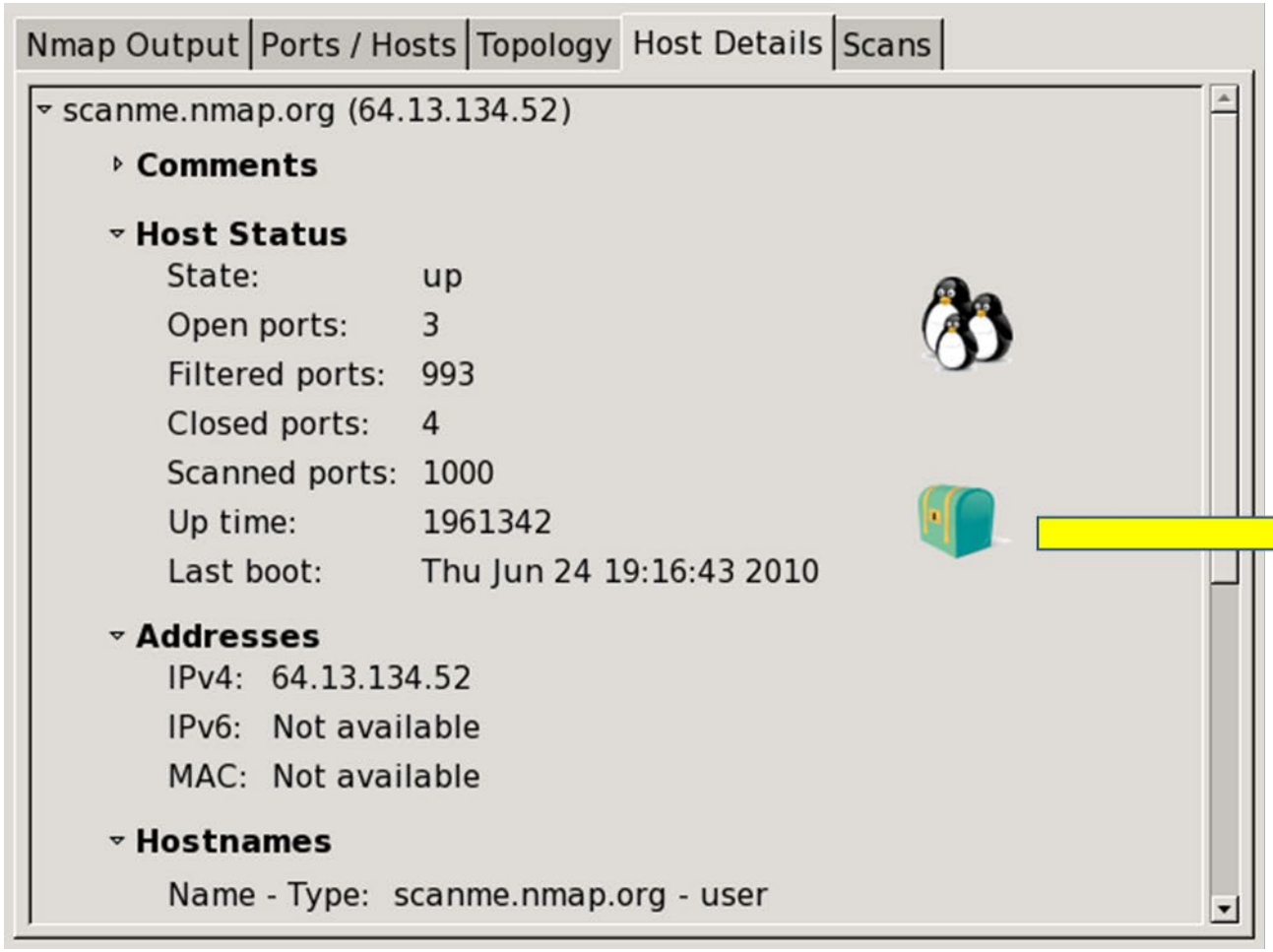
Nella sezione Nmap Output vedrete tutto il dettaglio delle informazioni raccolte dal comando nmap.

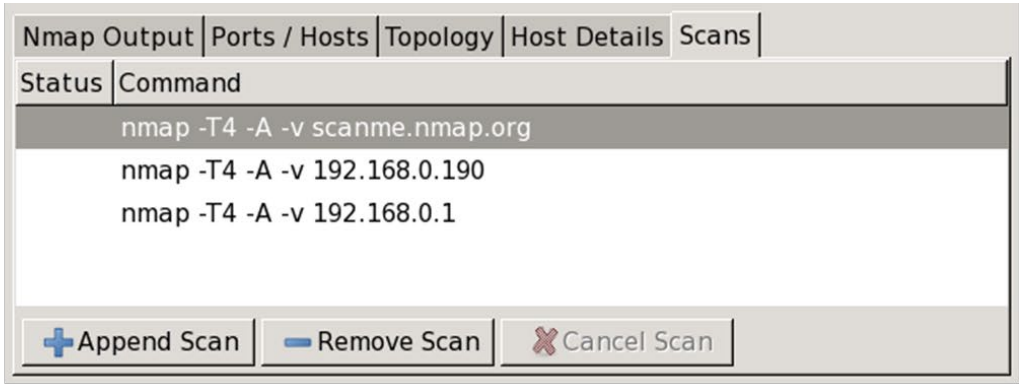


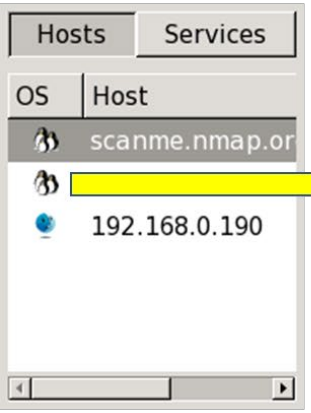


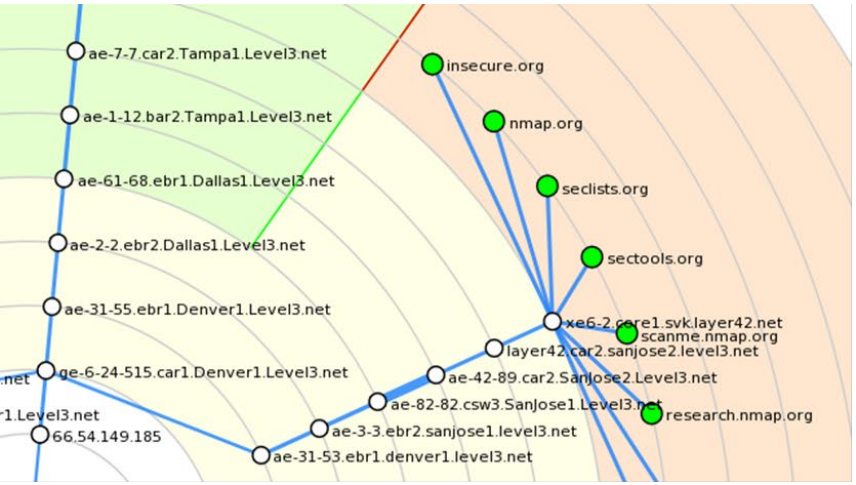












The topology view uses many symbols and color conventions. This section explains what they mean.

Each regular host in the network is represented by a little circle. The color and size of the circle is determined by the number of open ports on the host. The more open ports, the larger the circle. A white circle represents an intermediate host in a network path that was not port scanned. If a host has fewer than three open ports, it will be green; between three and six open ports, yellow; more than six open ports, red.

If a host is a router, switch, or wireless access point, it is drawn with a square rather than a circle.

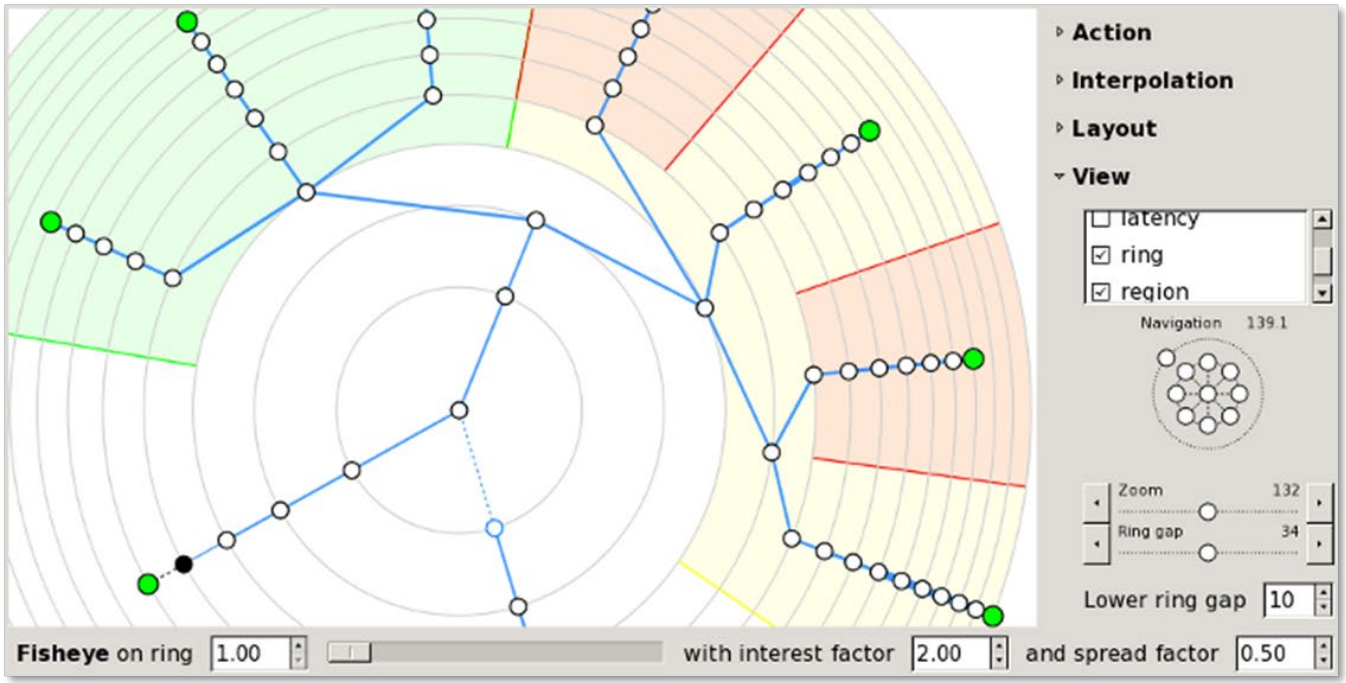
Network distance is shown as concentric gray rings. Each additional ring signifies one more network hop from the center host.

Connections between hosts are shown with colored lines. Primary traceroute connections are shown with blue lines. Alternate paths (paths between two hosts where a different path already exists) are drawn in orange. Which path is primary and which paths are alternates is arbitrary and controlled by the order in which paths were recorded. The thickness of a line is proportional to its round-trip time; hosts with a higher RTT have a thicker line. Hosts with no traceroute information are clustered around localhost, connected with a dashed black line.

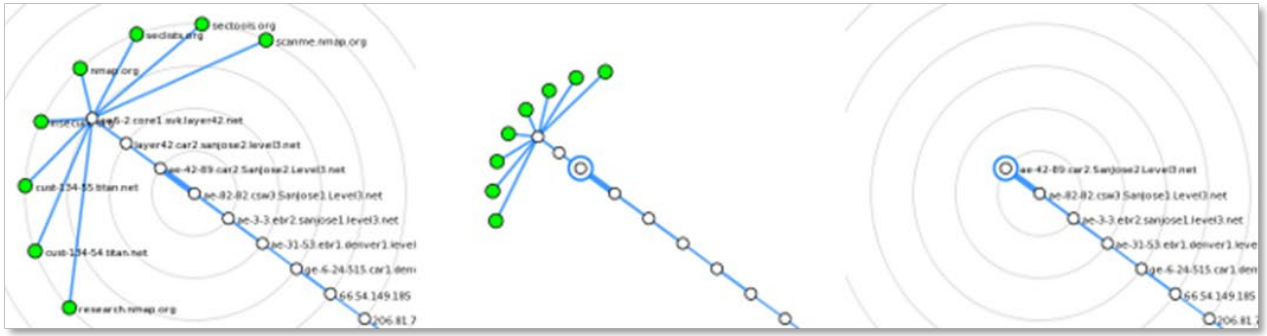
If there is no RTT for a hop (a missing traceroute entry), the connection is shown with a blue dashed line and the unknown host that makes the connection is shown with a blue outline.

Some special-purpose hosts may carry one or more icons describing what type of host they are:

- A router.
- A switch.
- A wireless access point.
- A firewall.
- A host with some ports filtered.


Action
Interpolation
Layout
View
latency
ring
region
Navigation
139.1
Zoom
132
Ring gap
34
Lower ring gap
10
Fisheye on ring
1.00
with interest factor
2.00
and spread factor
0.50


Action



NMAP HANDS ON

Overview di alcuni parametri importanti:

-sS esegue una scansione SYN stealth, meno rintracciabile di una scansione normale, ma più lenta. Molti firewall aggiornati possono comunque rilevarla.
-sn effettua una scansione di tipo ping. La scansione delle porte verrà disabilitata e vedrete solo se il target è online.
-O pratica una scansione sul sistema operativo. La scansione proverà a determinare il sistema operativo utilizzato.
-A questo parametro esegue le scansioni più comuni: scansione del sistema operativo, della versione, scan tramite script e traceroute.
-F è il parametro abilita la modalità veloce, ma riduce il numero di porte scansionate.
-v mostrerà più informazioni nei risultati, rendendoli più semplici da leggere e interpretare.
-vv oppure -v -v come sopra ma con maggiori dettagli.
-P0 diciamo a Nmap di non pingare l'host bersaglio, utile se sappiamo che l'host è up.
-PT pinga sulla porta 80 con un TCP Ack invece che con ICMP.
-T0 oppure -T Paranoid è la modalità più prudente, in grado di eludere anche gli IDS, esegue lo scan in modo seriale ed aspetta almeno 5 minuti tra uno scan e l'altro, da T1 a T4 impiega sempre meno tempo con T5 viaggia alla massima velocità, rischia di perdere pacchetti e di far crashare il TARGET

NMAP HANDS ON

Il range di sistemi da scansionare possono essere scritti con wildcard:

nmap 192.168.1.1,2,3 scansiona i primi 3 IP della stessa subnet

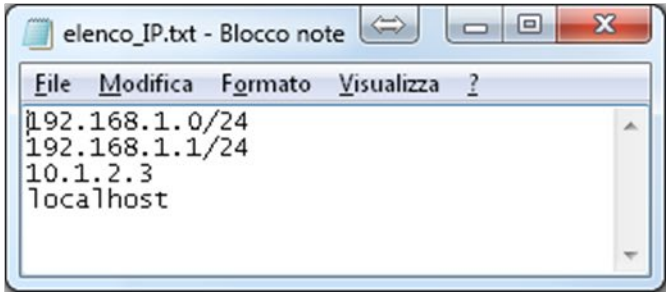
nmap 192.168.1.1-20 scansiona i primi 20 IP della stessa subnet

nmap 192.168.1.* scansiona tutta la subnet

nmap 192.168.1.0/24 scansiona tutta la subnet

nmap 192.168.1.0/24 --exclude 192.168.1.5 esclude un indirizzo

nmap -iL /mgx/desktop/elenco_IP.txt



NMAP HANDS ON

nmap -A 192.168.1.254 --
nmap -v -A 192.168.1.1 |-> Rilevazione del Sistema Operativo
nmap -A -iL /mgx/desktop/elenco_IP.txt --

nmap -sA 192.168.1.254 Rilevazione di un sistema filtrato da un firewall

nmap -PN 192.168.1.1 Rilevazione di un sistema protetto da un firewall

nmap --packet-trace 192.168.1.1 Visualizza tutti i pacchetti inviati e ricevuti

nmap -sV 192.168.1.1 Rileva e visualizza la versione del servizio rilevato

nmap -PS 192.168.1.1 Se un firewall blocca ICMP potete usare TCP Syn

nmap -PA 192.168.1.1 Se un firewall blocca ICMP potete usare TCP Ack

nmap -f 192.168.1.1 Frammenta i pacchetti per eludere il firewall

NMAP HANDS ON

Firewall evasion con IP spoofing

Sintassi “nmap -n -Ddecoy-ip1,decoy-ip2,il_tuo_ip,decoy-ip3,decoy-ip4 TARGET”

nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5

Firewall evasion con MAC address spoofing

Sintassi “nmap --spoof-mac MAC-ADDRESS-HERE TARGET”

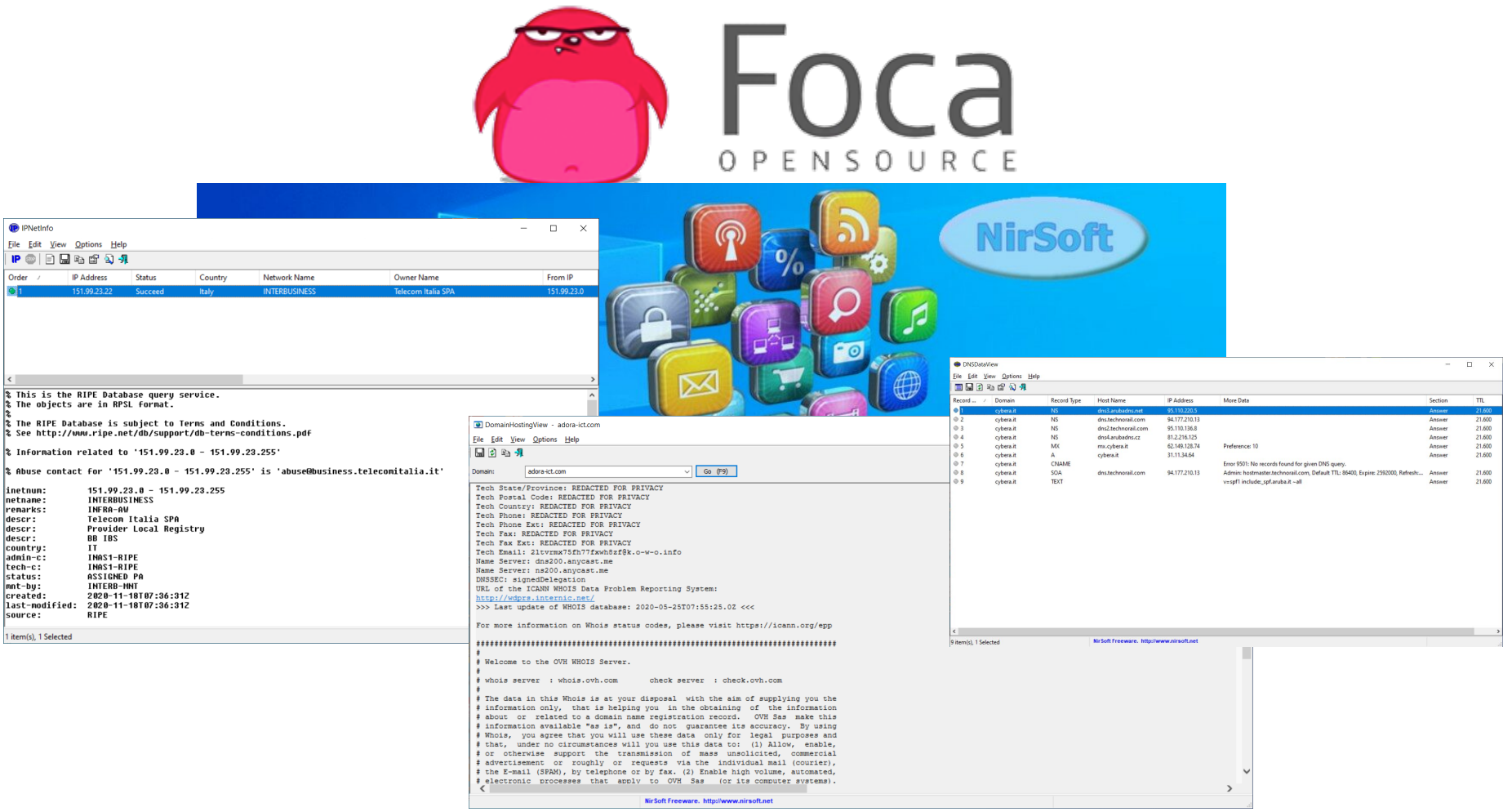
nmap -v -sT -PN --spoof-mac 0 192.168.1.1 Con 0 il MAC viene generato in modo causale

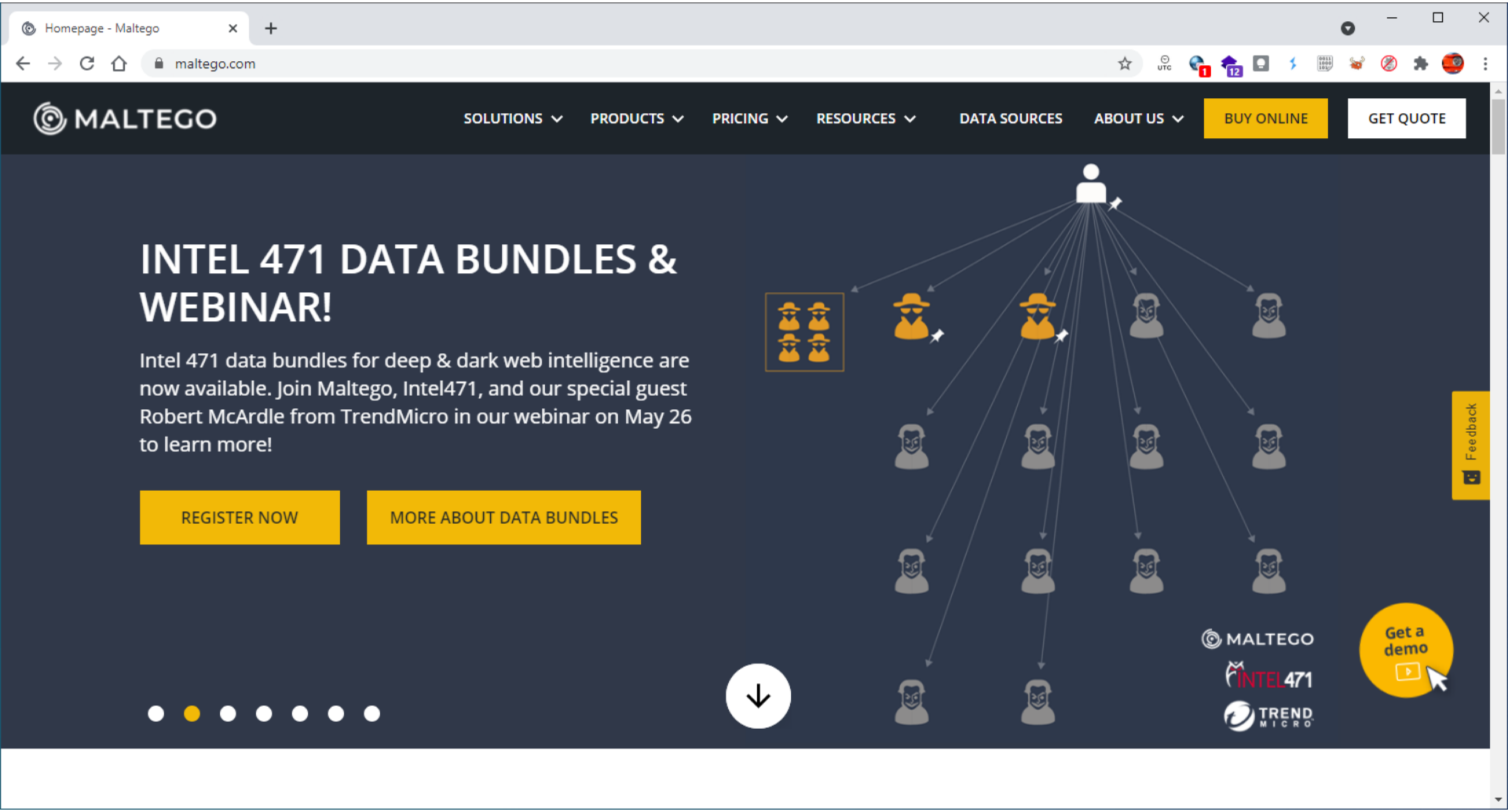
NESSUS

Nessus possiede un archivio di oltre 100.000 plugin. Ognuno con particolari compiti di

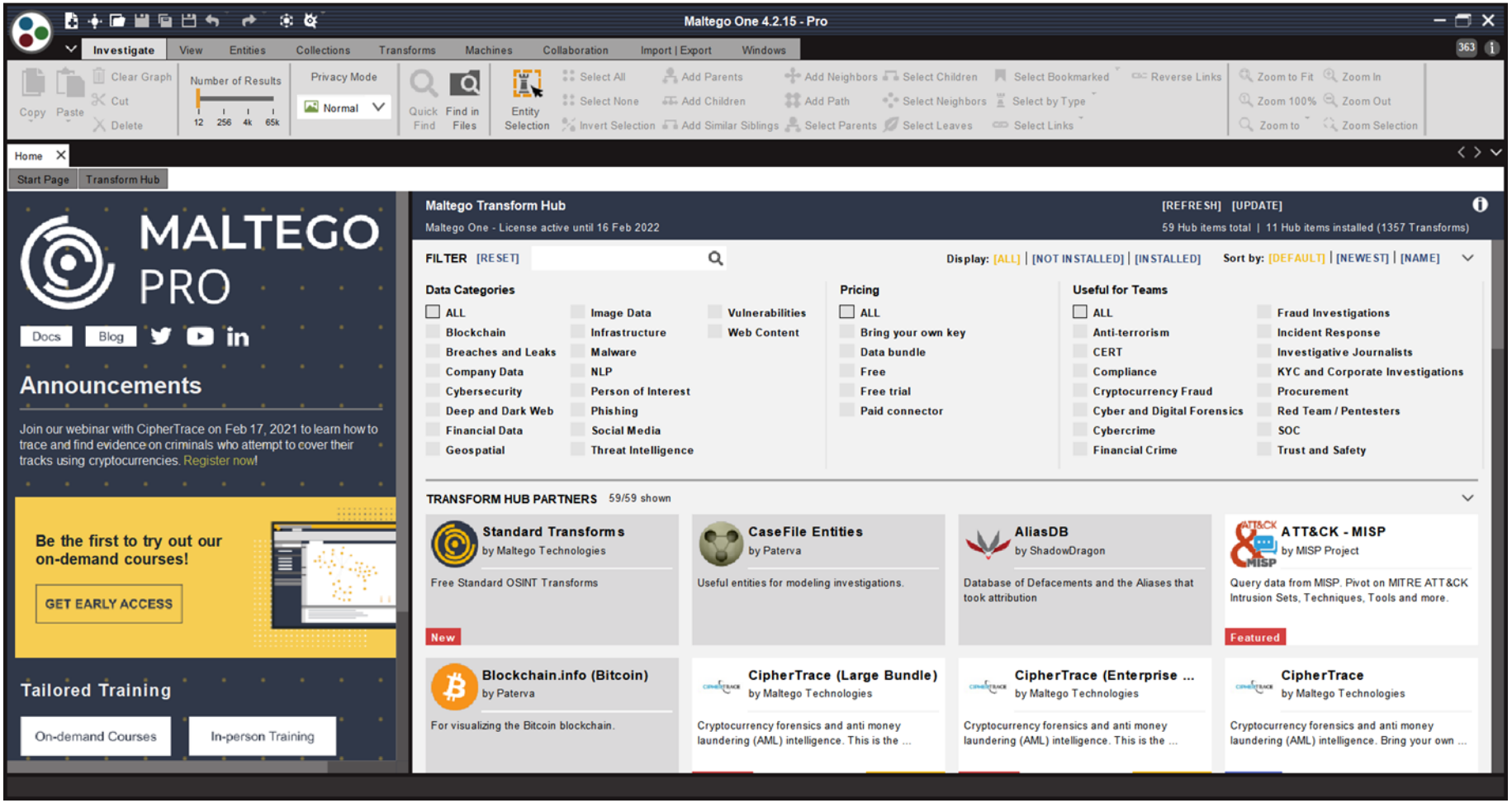
- host discovery
- vulnerability identification
- flaws exploitability
- compliance checks
- configuration auditing

Il prodotto si aggiorna continuamente per coprire le molteplici nuove vulnerabilità che vengono scoperte, non esiste un prodotto che vanta la stessa esperienza ed efficacia di Nessus nel mercato!
L'utente di Nessus dispone di un Support Portal dove può accedere a tutti i servizi professionali, messi a disposizione da Tenable.



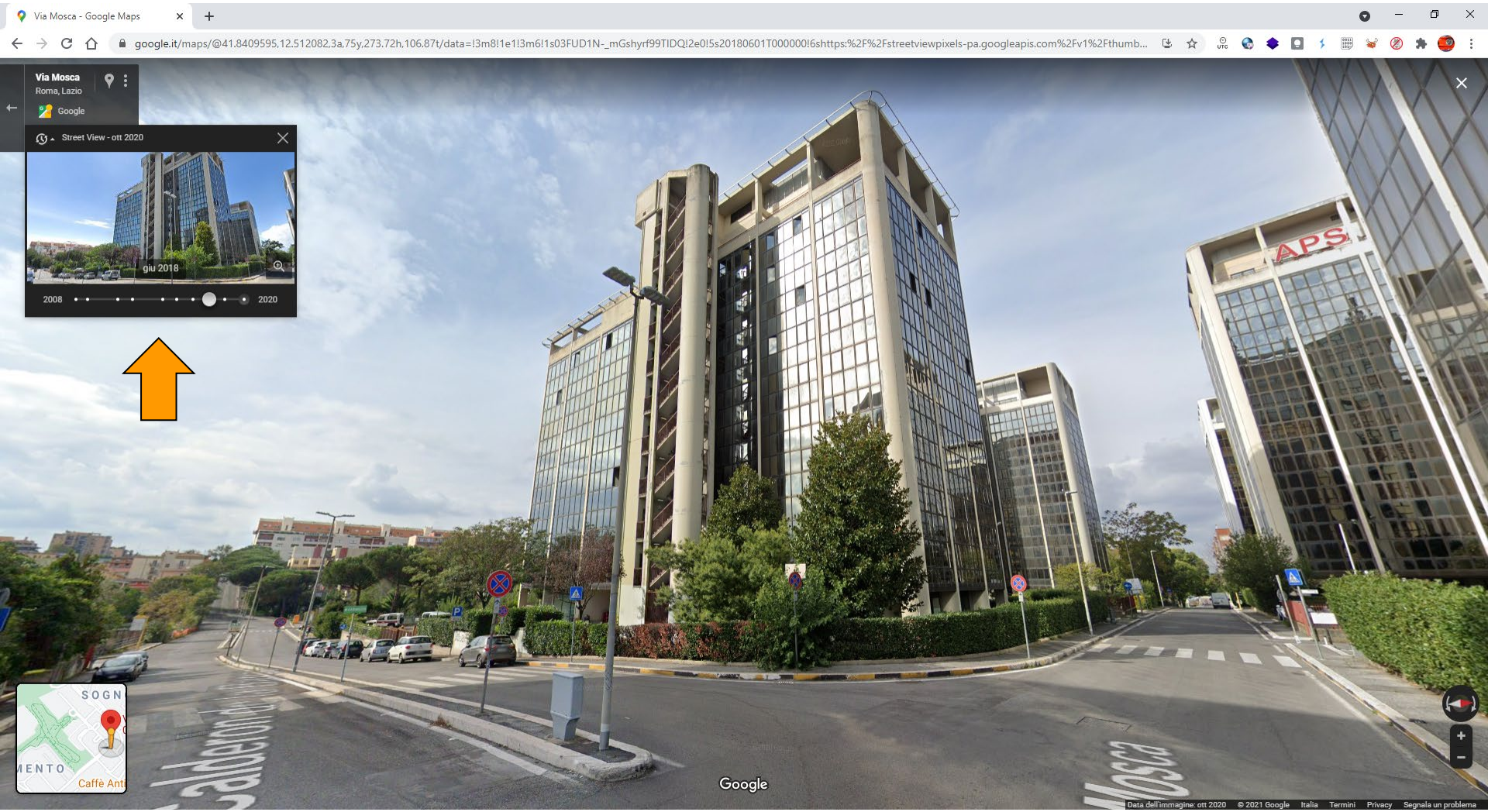


LA BACCHETTA MAGICA OSINT... ma solo con trasformate a pagamento...



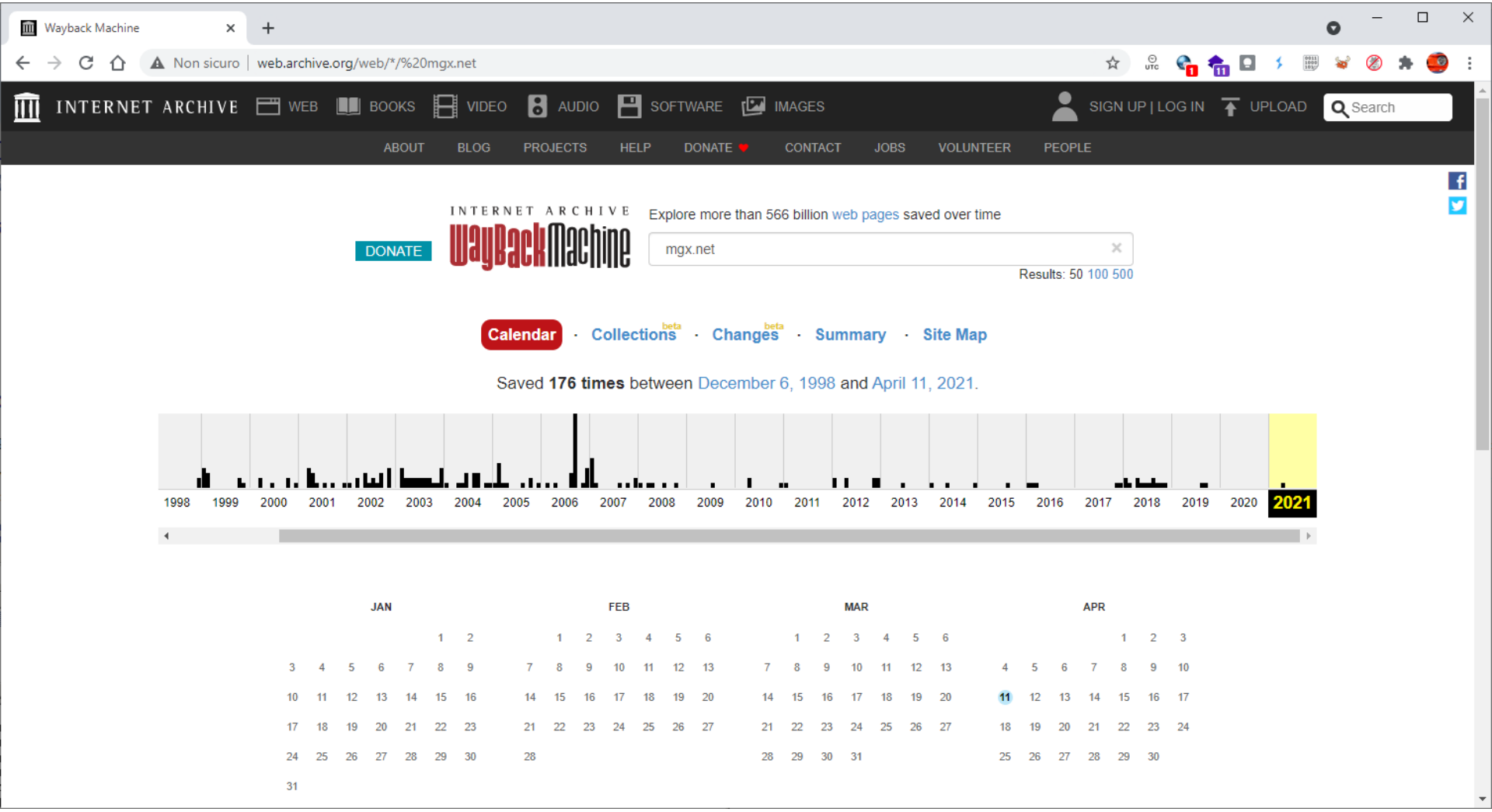
Agenda

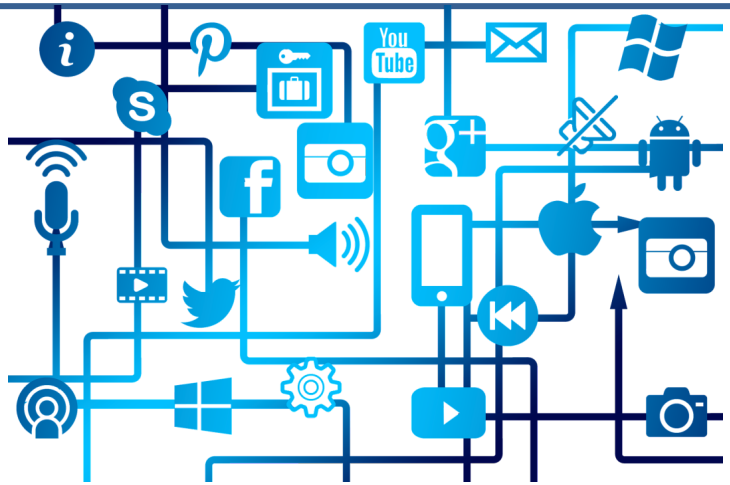
- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A


Via Mosca - Google Maps
google.it/maps/@41.8409595,12.512082,3a,75y,273.72h,106.87t/data=!3m8!1e1!3m6!1s03FUD1N-_mGshyrf99TIDQ!2e0!5s20180601T000000!6shttps:%2F%2Fstreetviewpixels-pa.googleapis.com%2Fv1%2Fthumb...
Via Mosca
Roma, Lazio
Google
Street View - ott 2020
giu 2018
2008
2020
APS
Google
Data dell'immagine: ott 2020
© 2021 Google
Italia
Termini
Privacy
Segnala un problema

Contenuti di siti rimossi o modificati (**i testimoni virtuali**)

- web.archive.org
- Whois plus (whois.domaintools.com, who.is)
- Reverse whois (reversewhois.io)
- Many tools (yougetsignal.com)
- spamhaus.org (rosko)
- esplorare i certificati SSL
- messaggi di errore con banner parlanti
- web-sniffer.net
- siteliner.com (copie di siti web)
  come scoprire se i contenuti del sito sono copiati da altri
- copia **cache** social network cache:https://www.facebook.com/ACMilan/


Wayback Machine
Non sicuro | web.archive.org/web/*/%20mgx.net
INTERNET ARCHIVE
WEB
BOOKS
VIDEO
AUDIO
SOFTWARE
IMAGES
SIGN UP | LOG IN
UPLOAD
Search
ABOUT
BLOG
PROJECTS
HELP
DONATE
CONTACT
JOBS
VOLUNTEER
PEOPLE
DONATE
INTERNET ARCHIVE
WayBackMachine
Explore more than 566 billion web pages saved over time
mgx.net
Results: 50 100 500
Calendar
Collections beta
Changes beta
Summary
Site Map
Saved 176 times between December 6, 1998 and April 11, 2021.
1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021
JAN
FEB
MAR
APR



Social network

- site:www.facebook.com cybera
- site:www.facebook.com “Mario Rossi” (Immagini)
- site:www.linkedin.com “Mario Rossi” (Immagini)
- https://independent.academia.edu/
- https://core.ac.uk/
- https://onemilliontweetmap.com/
- https://www.tweeplers.com/map/
- https://www.hashatit.com/hashtags/etna

Biblioteche internazionali

- https://www.loc.gov/search/?in=&q=graziani&new=true&st=
- https://www.loc.gov/resource/sn83030272/1908-02-02/ed-1/?st=gallery

Mappe della conoscenza

- https://openknowledgemaps.org/

Mappe arricchite

http://metrocosm.com/disputed-territories-map.html
https://www.healthmap.org/en/
https://www.marinetraffic.com/en/ais/home/centerx:10.5/centery:42.0/zoom:4
https://www.flightradar24.com/43.15,12.11/6
https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
https://acleddata.com/dashboard/#/dashboard
https://newspapermap.com/#38.13456,14.89197,8z

Vediamoli direttamente, non serve prendere appunti perché nelle slide on line troverete la solita sezione:

SITOGRAFIA con tutti gli URL aggiornati

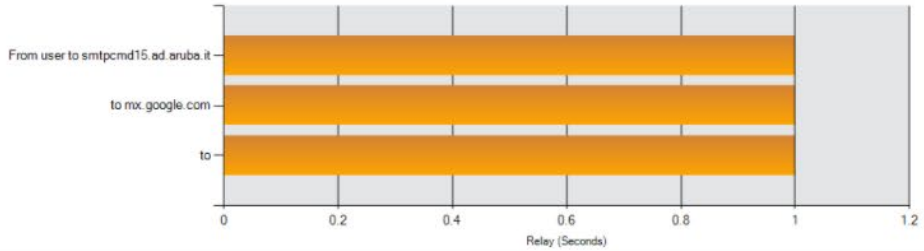
Vediamo prima come si analizzano alcuni dati pubblici come l'header della email e le pagine celate nel robots.txt

GHDB: Directory Listing e altro di riservato in rete

Email Header Analyzer, RFC822 H

mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=731ca78b-c44e-4558-a763-53dfc1e2442a

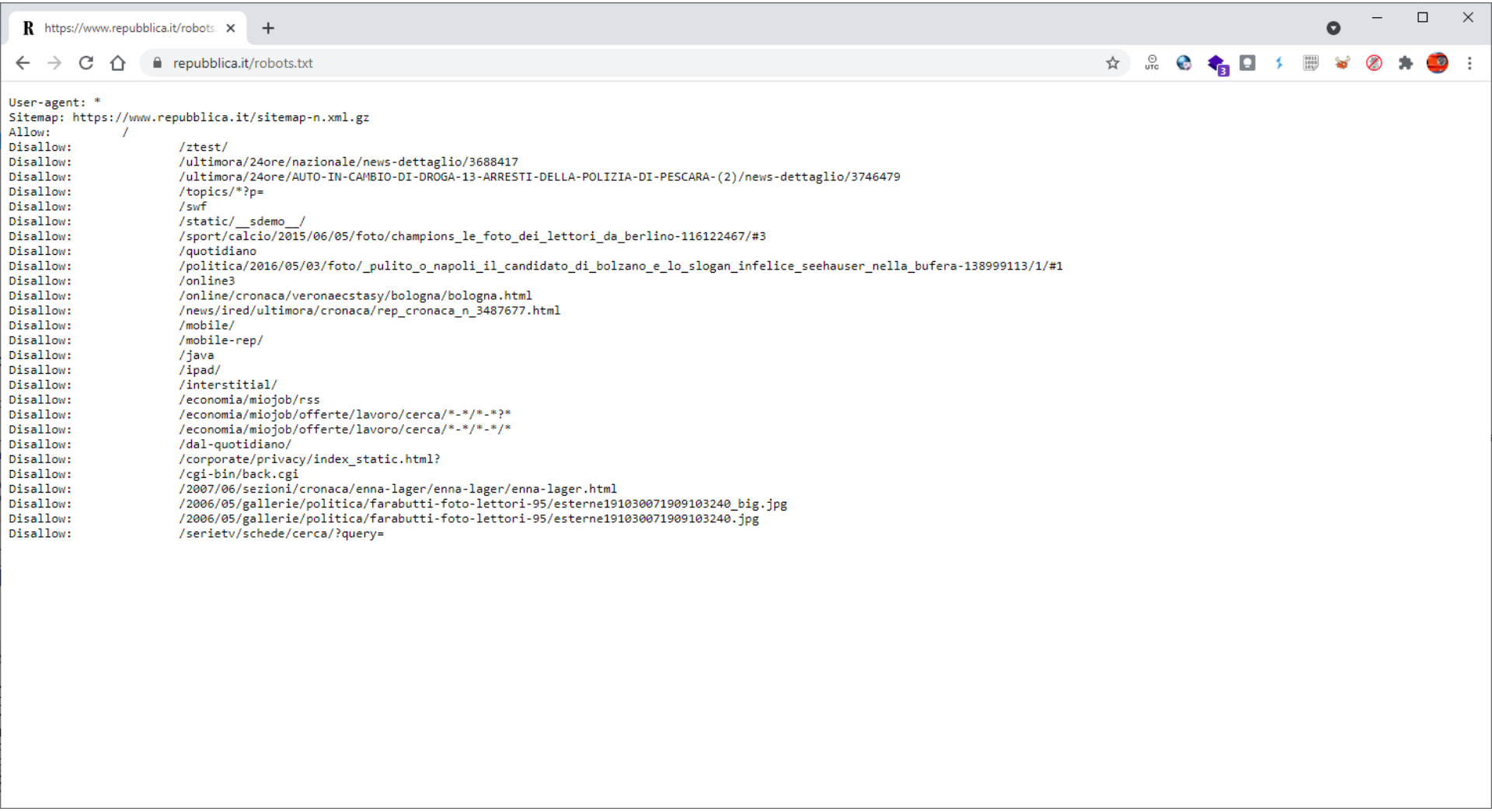
Delay:	

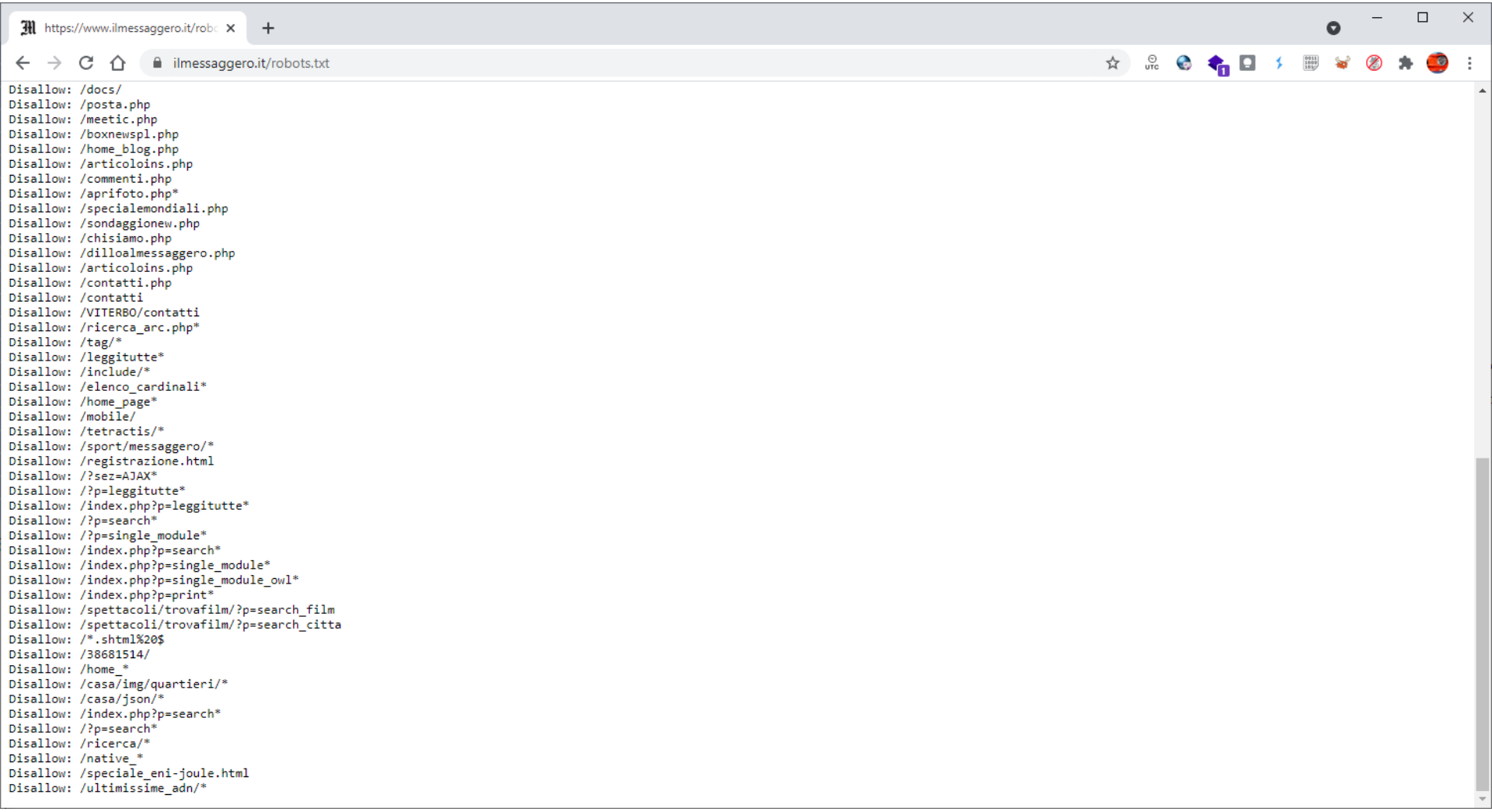


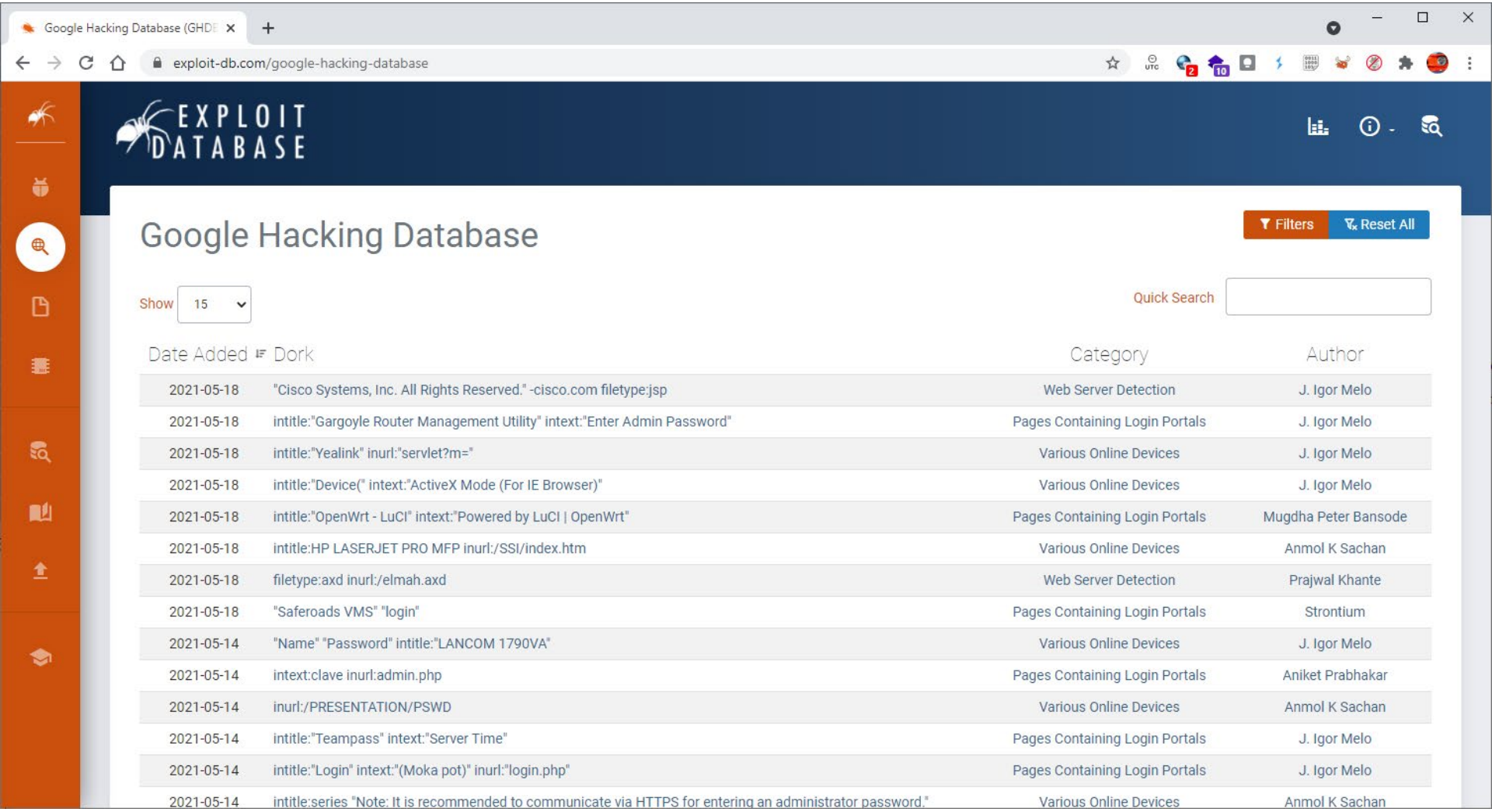
Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	user 151.30.122.253	smtpcmd15.ad.aruba.it	bizsmtp	9/12/2018 8:30:48 AM	
2	0 seconds	smtpcmd15178.aruba.it 62.149.156.178	mx.google.com	ESMTPS	9/12/2018 8:30:48 AM	
3	0 seconds		2002:a9d:2b70:0:0:0:0:0	SMTP	9/12/2018 8:30:48 AM	

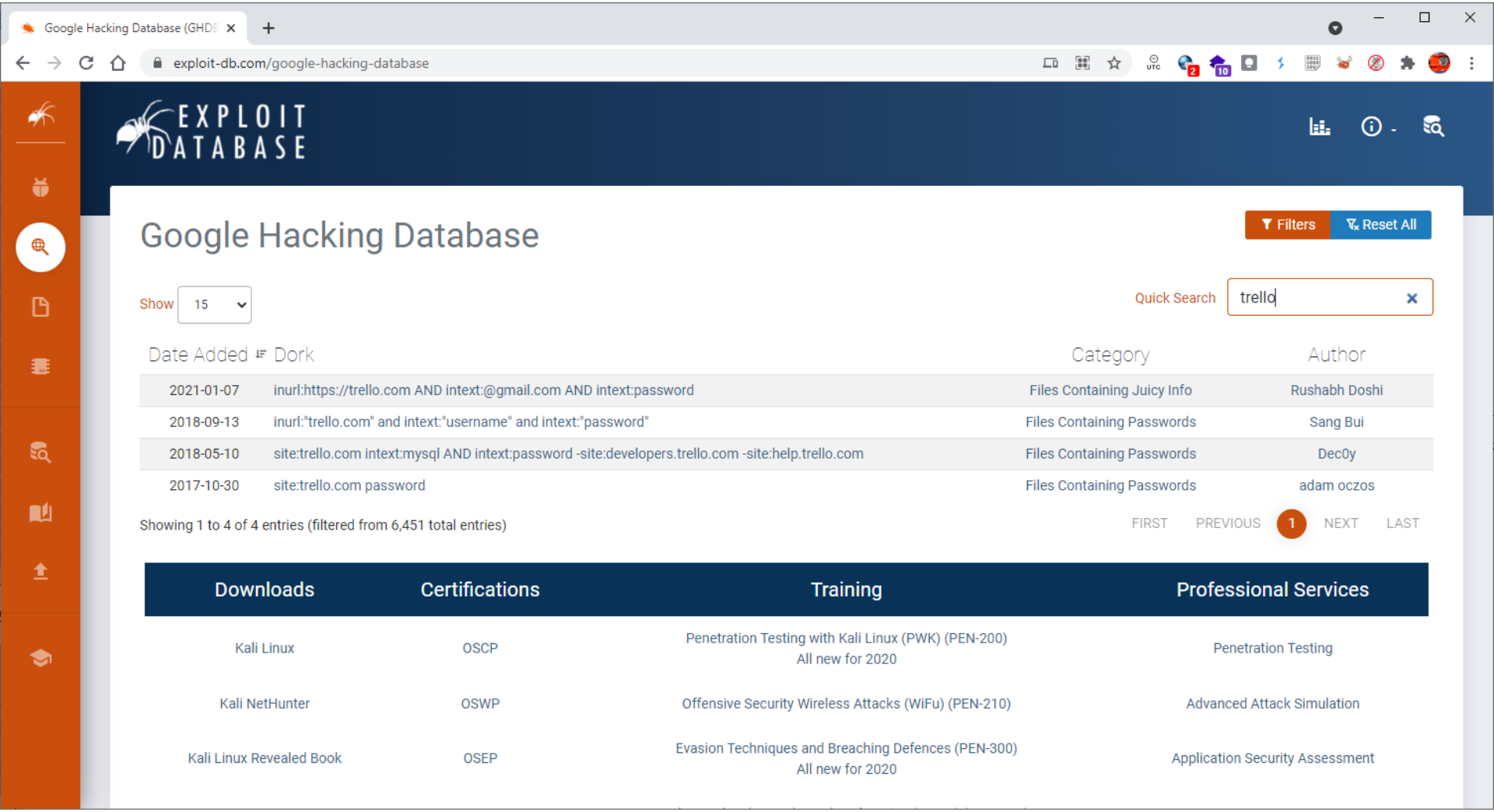
SPF and DKIM Information

dmarc:iqons.biz Hide Solve Email Delivery Problems

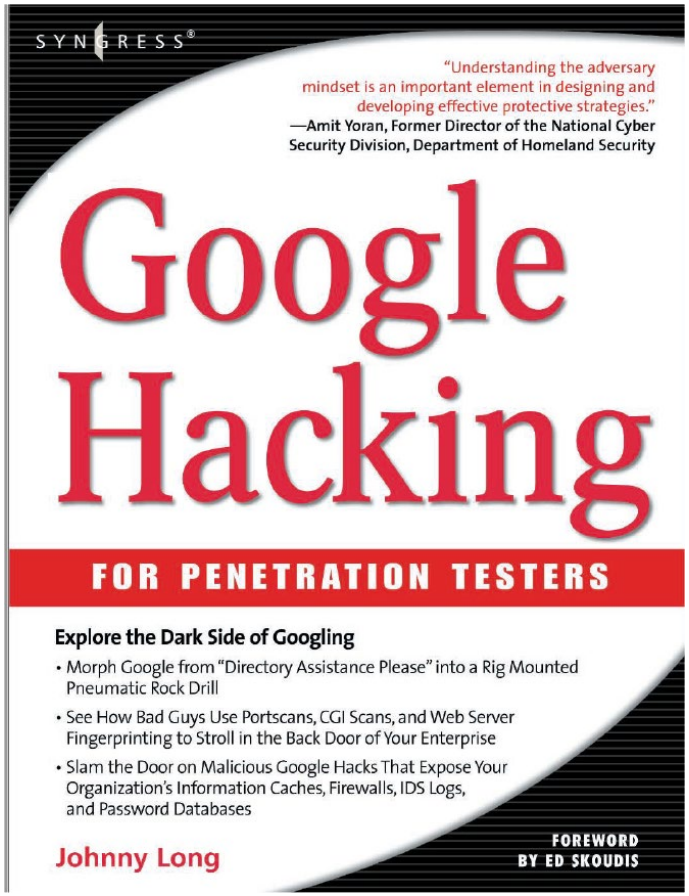



https://www.ilmessaggero.it/rob
ilmessaggero.it/robots.txt
Disallow: /docs/
Disallow: /posta.php
Disallow: /meetic.php
Disallow: /boxnewspl.php
Disallow: /home_blog.php
Disallow: /articoloins.php
Disallow: /commenti.php
Disallow: /aprifoto.php*
Disallow: /specialemondiali.php
Disallow: /sondaggionew.php
Disallow: /chisiamo.php
Disallow: /dilloalmessaggero.php
Disallow: /articoloins.php
Disallow: /contatti.php
Disallow: /contatti
Disallow: /VITERBO/contatti
Disallow: /ricerca_arc.php*
Disallow: /tag/*
Disallow: /leggitutte*
Disallow: /include/*
Disallow: /elenco_cardinali*
Disallow: /home_page*
Disallow: /mobile/
Disallow: /tetractis/*
Disallow: /sport/messaggero/*
Disallow: /registrazione.html
Disallow: /?sez=AJAX*
Disallow: /?p=leggitutte*
Disallow: /index.php?p=leggitutte*
Disallow: /?p=search*
Disallow: /?p=single_module*
Disallow: /index.php?p=search*
Disallow: /index.php?p=single_module*
Disallow: /index.php?p=single_module_owl*
Disallow: /index.php?p=print*
Disallow: /spettacoli/trovafilm/?p=search_film
Disallow: /spettacoli/trovafilm/?p=search_citta
Disallow: /*.shtml%20$
Disallow: /38681514/
Disallow: /home_*
Disallow: /casa/img/quartieri/*
Disallow: /casa/json/*
Disallow: /index.php?p=search*
Disallow: /?p=search*
Disallow: /ricerca/*
Disallow: /native_*
Disallow: /speciale_eni-joule.html
Disallow: /ultimissime_adn/*



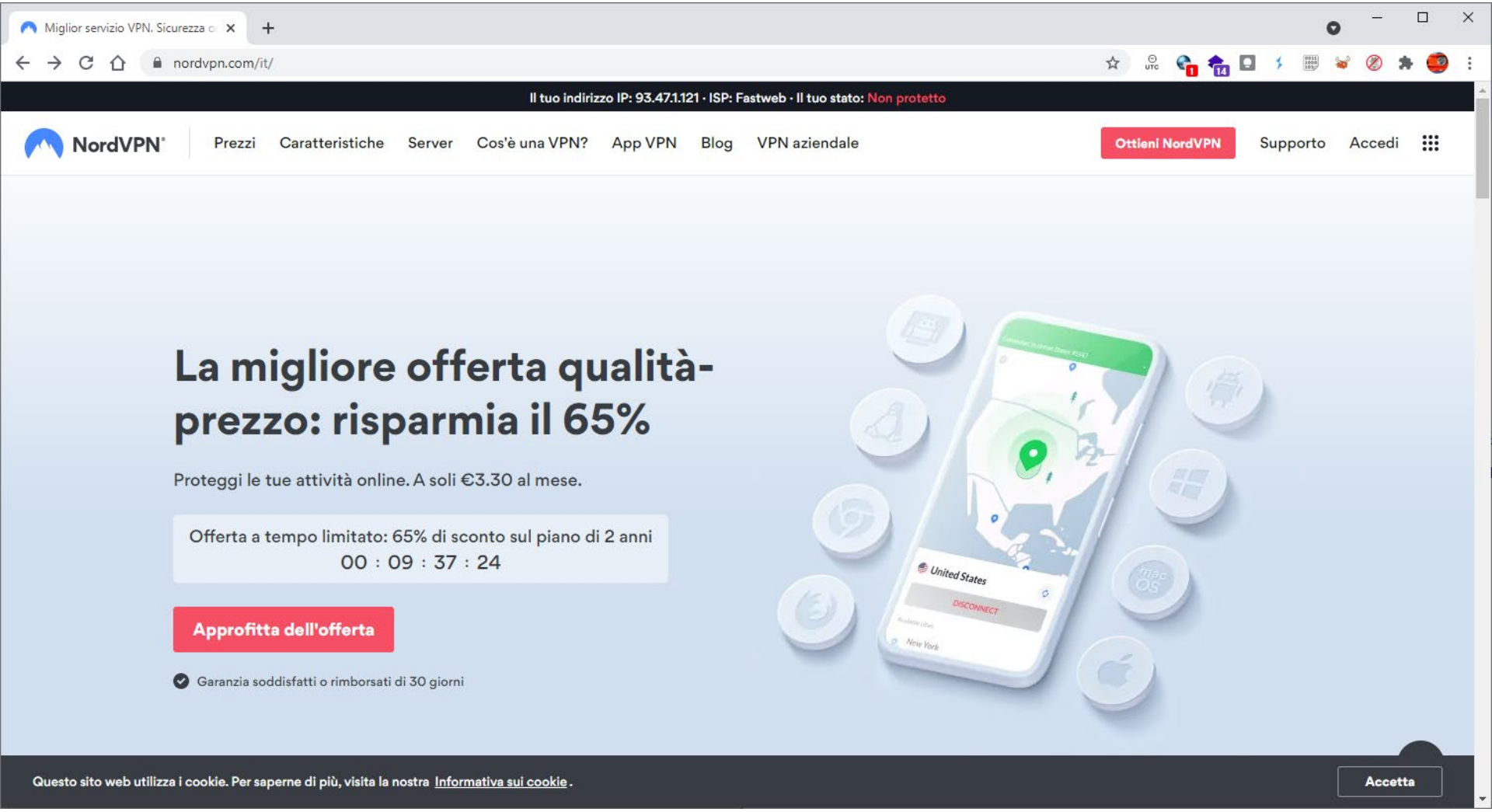


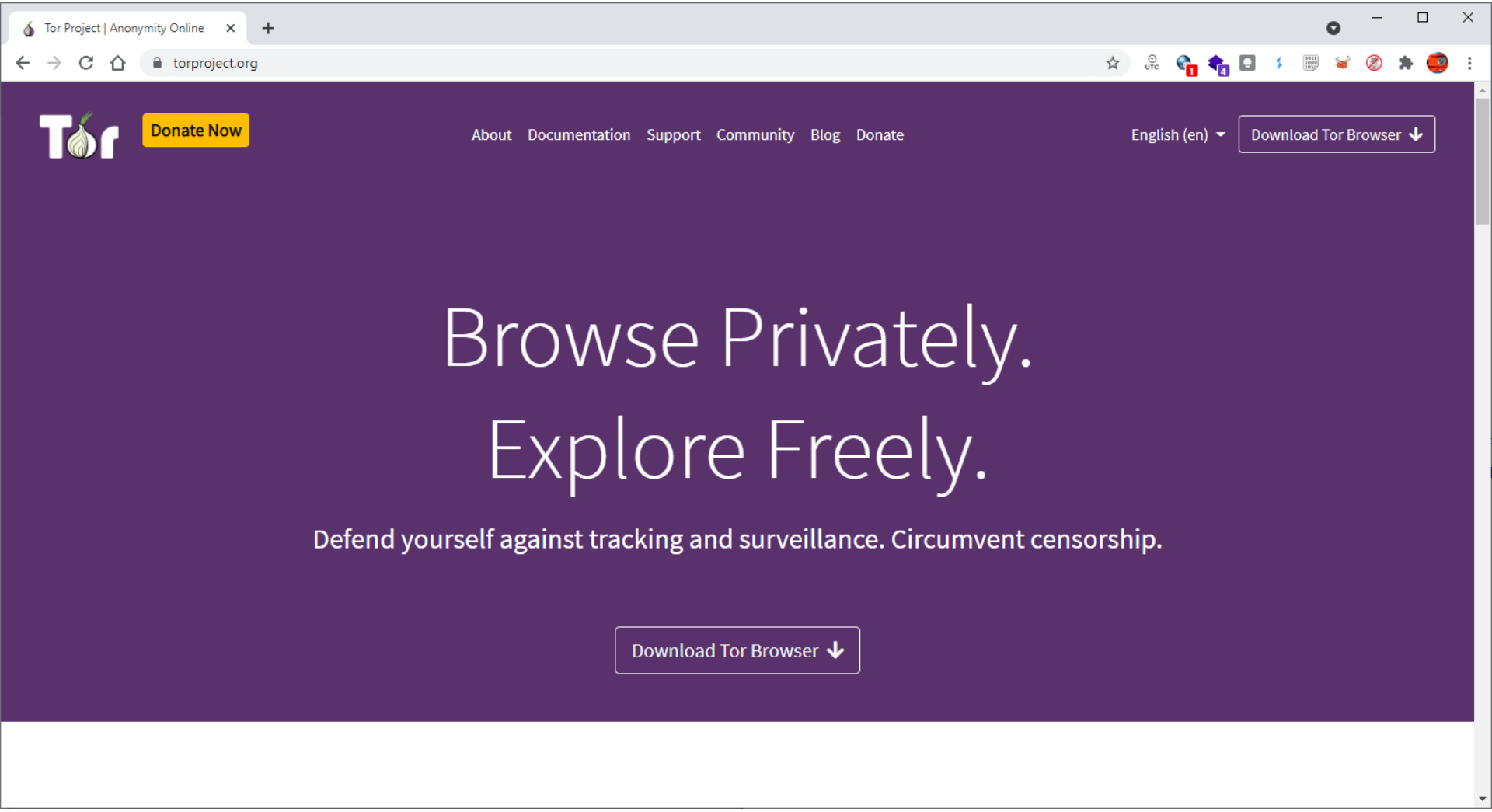
Google Hacking for penetration testers filetype:pdf

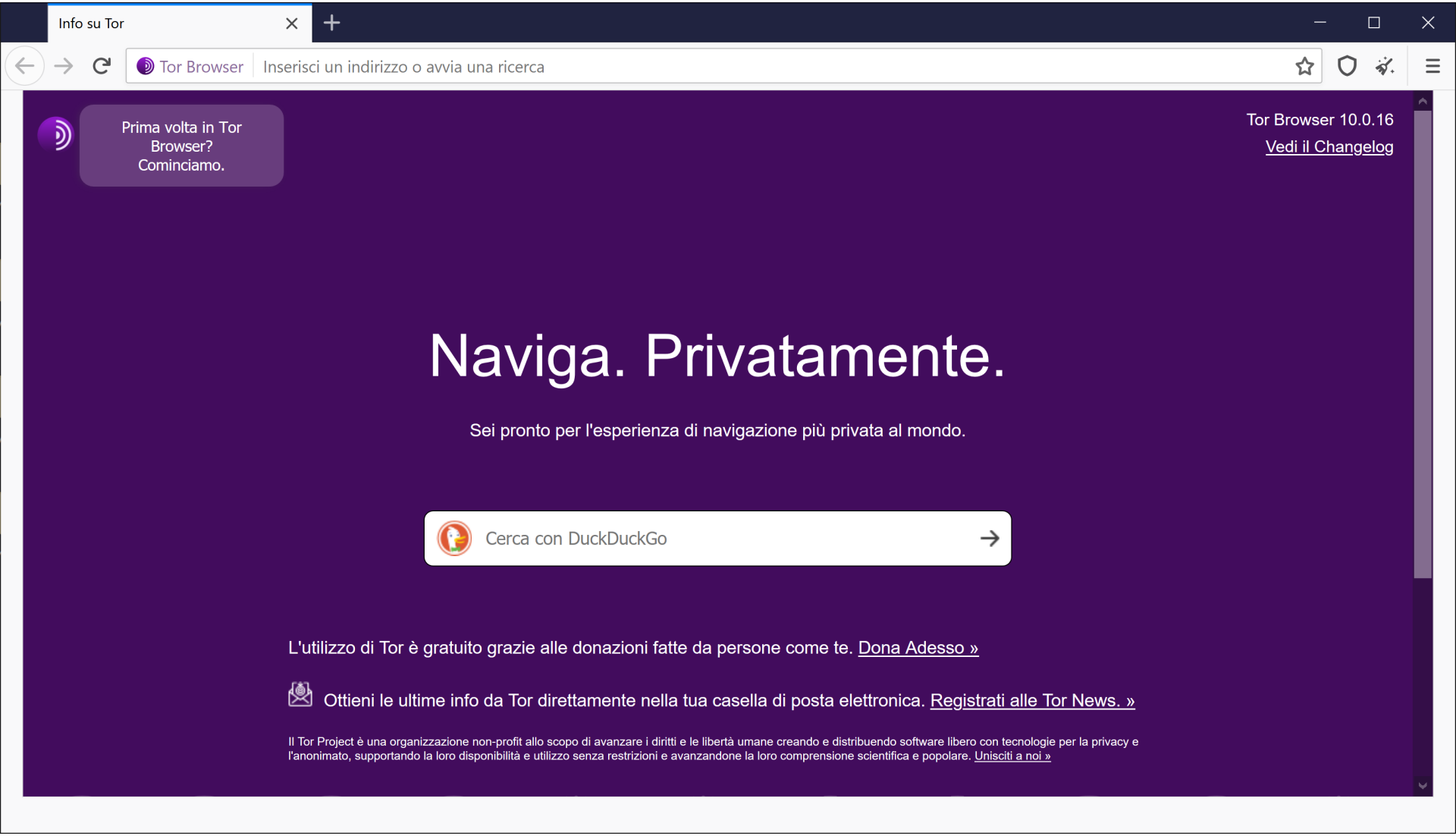


Agenda

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A



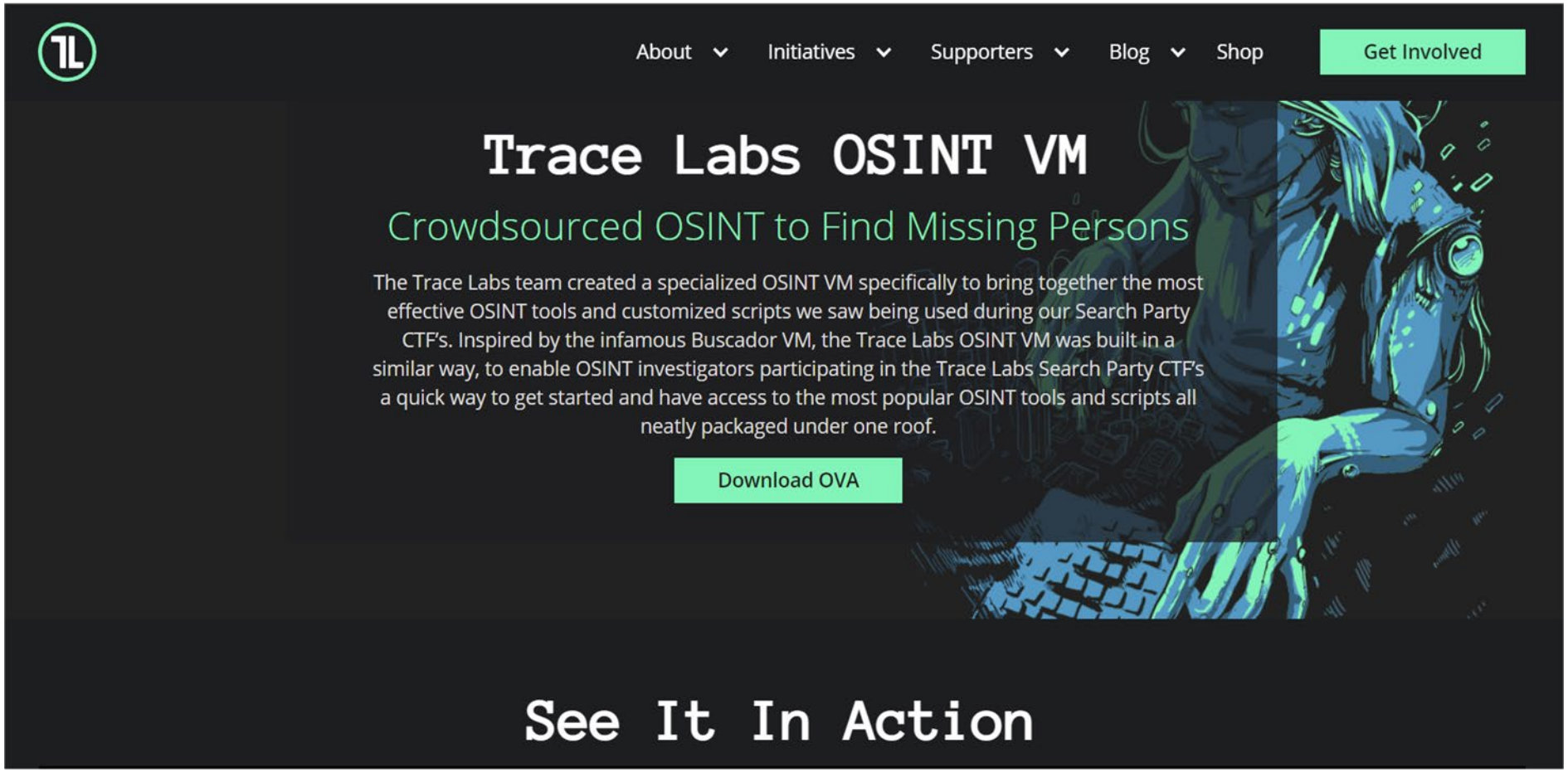




Agenda

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

La distro linux BUSCADOR non è più supportata: eccone una nuova disponibile



Agenda

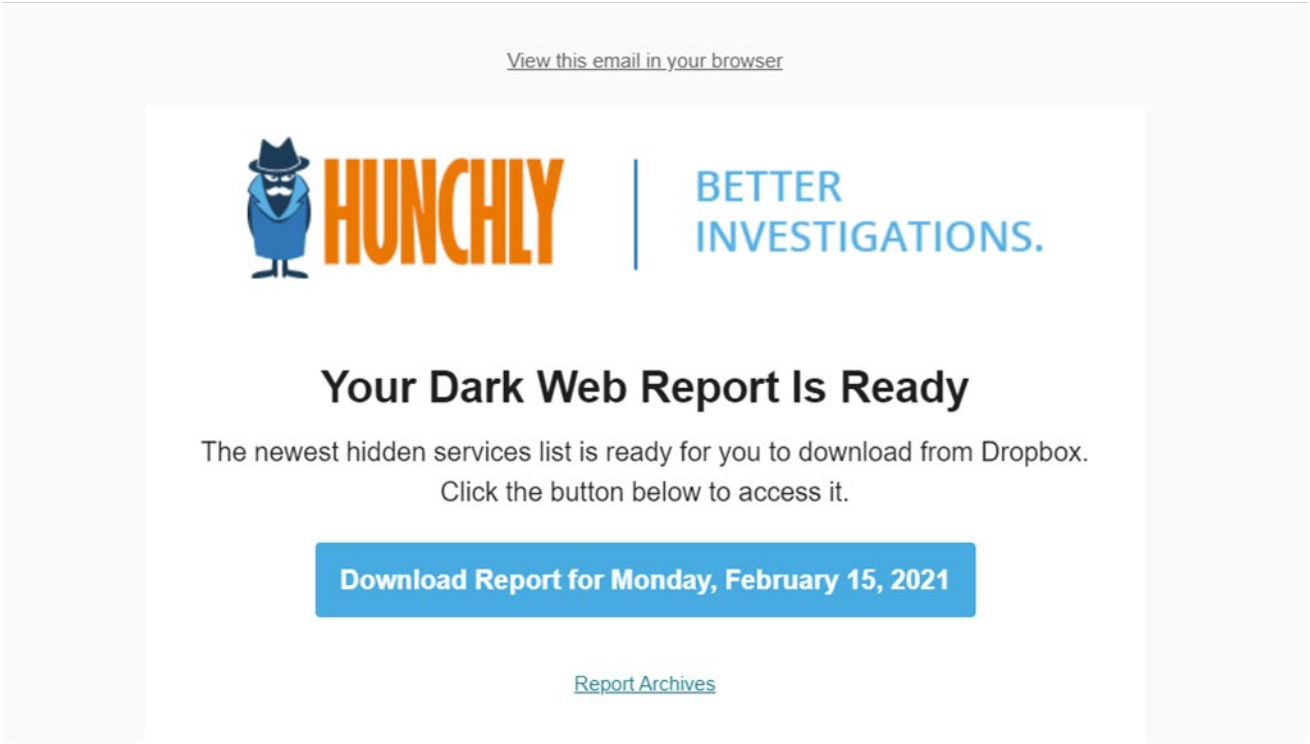
- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

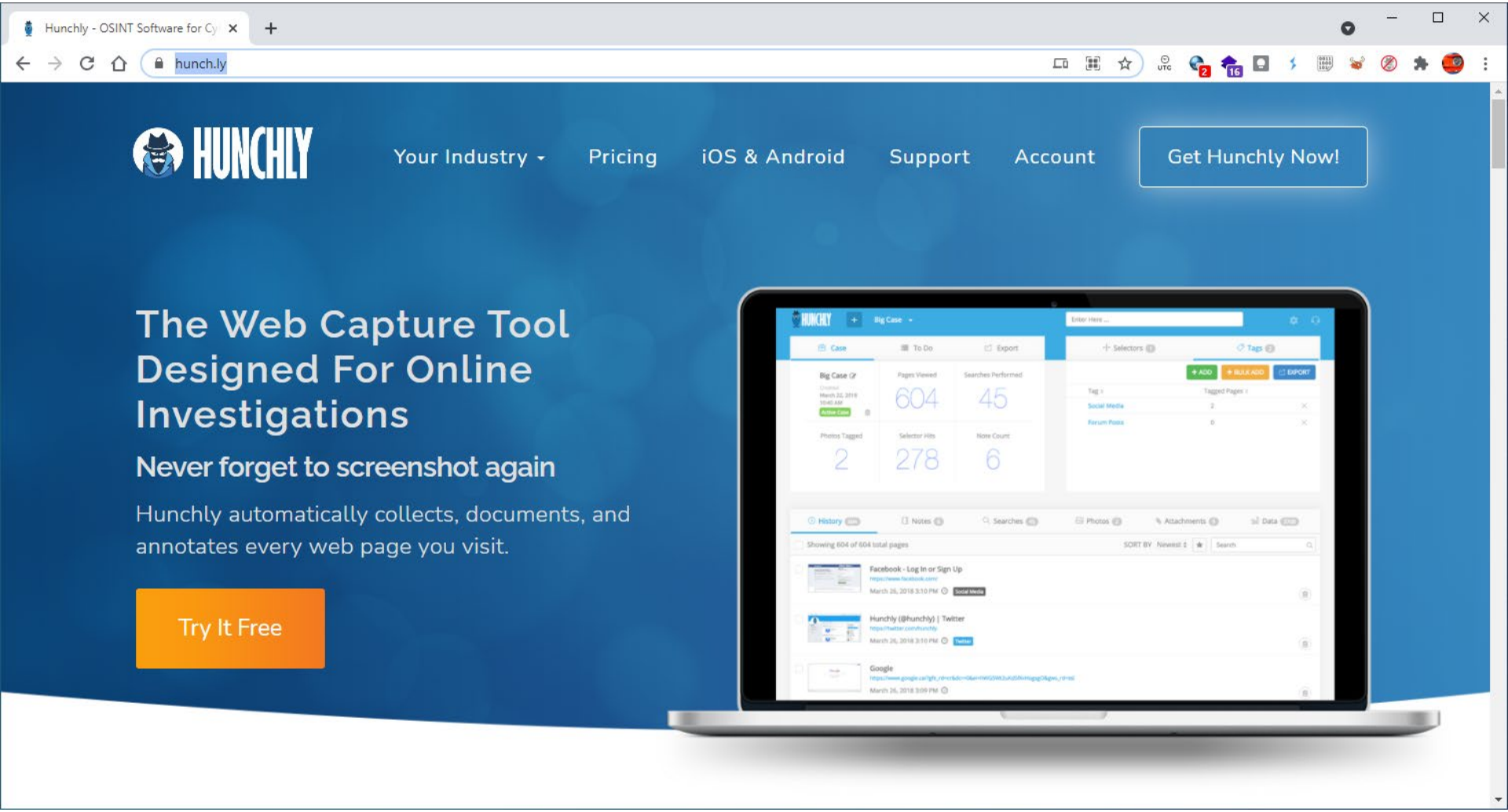
ATTENZIONE:

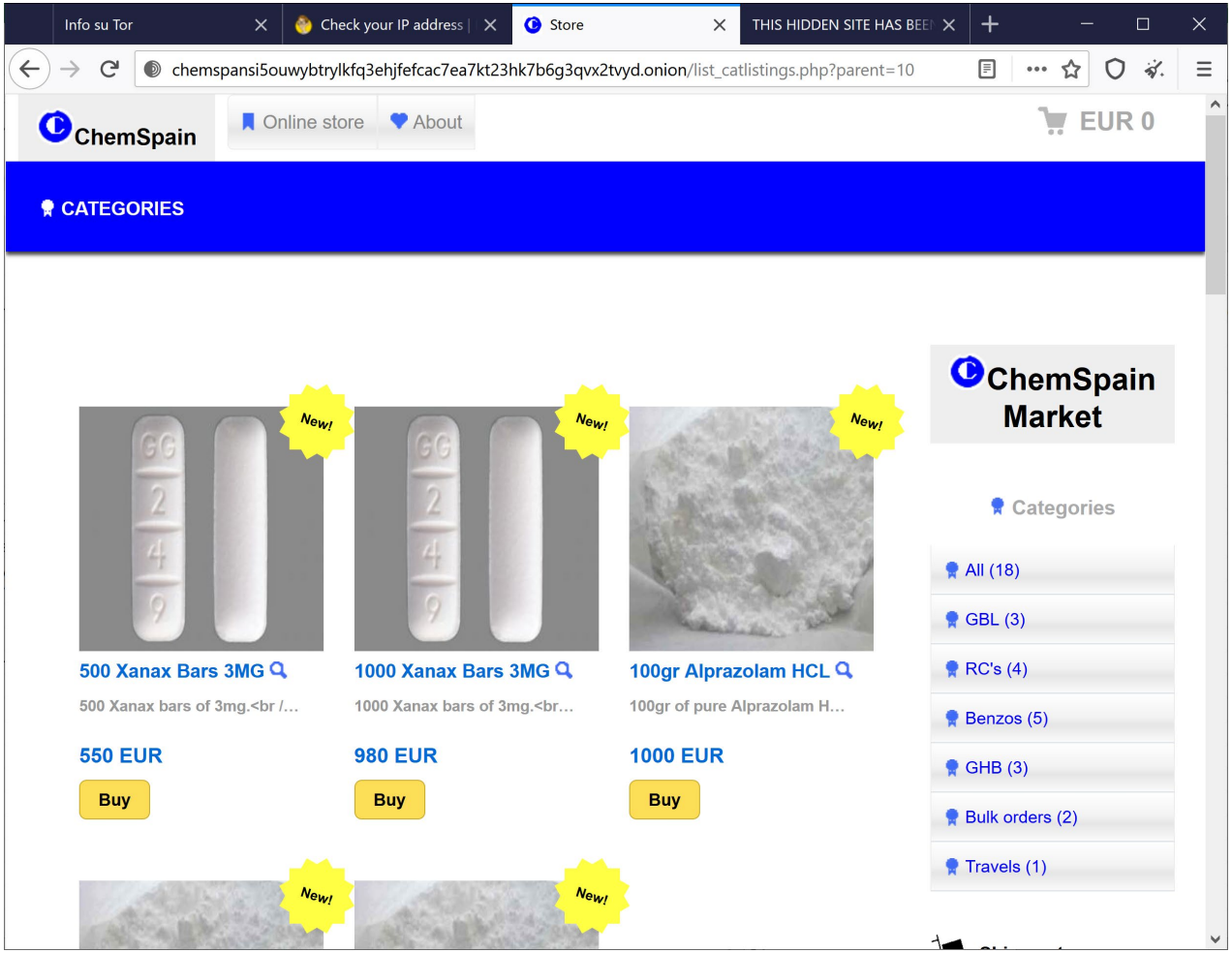
QUELLO CHE VEDRETE IN QUESTO SEMINARIO,
E' MATERIALE A SCOPO EDUCATIVO.

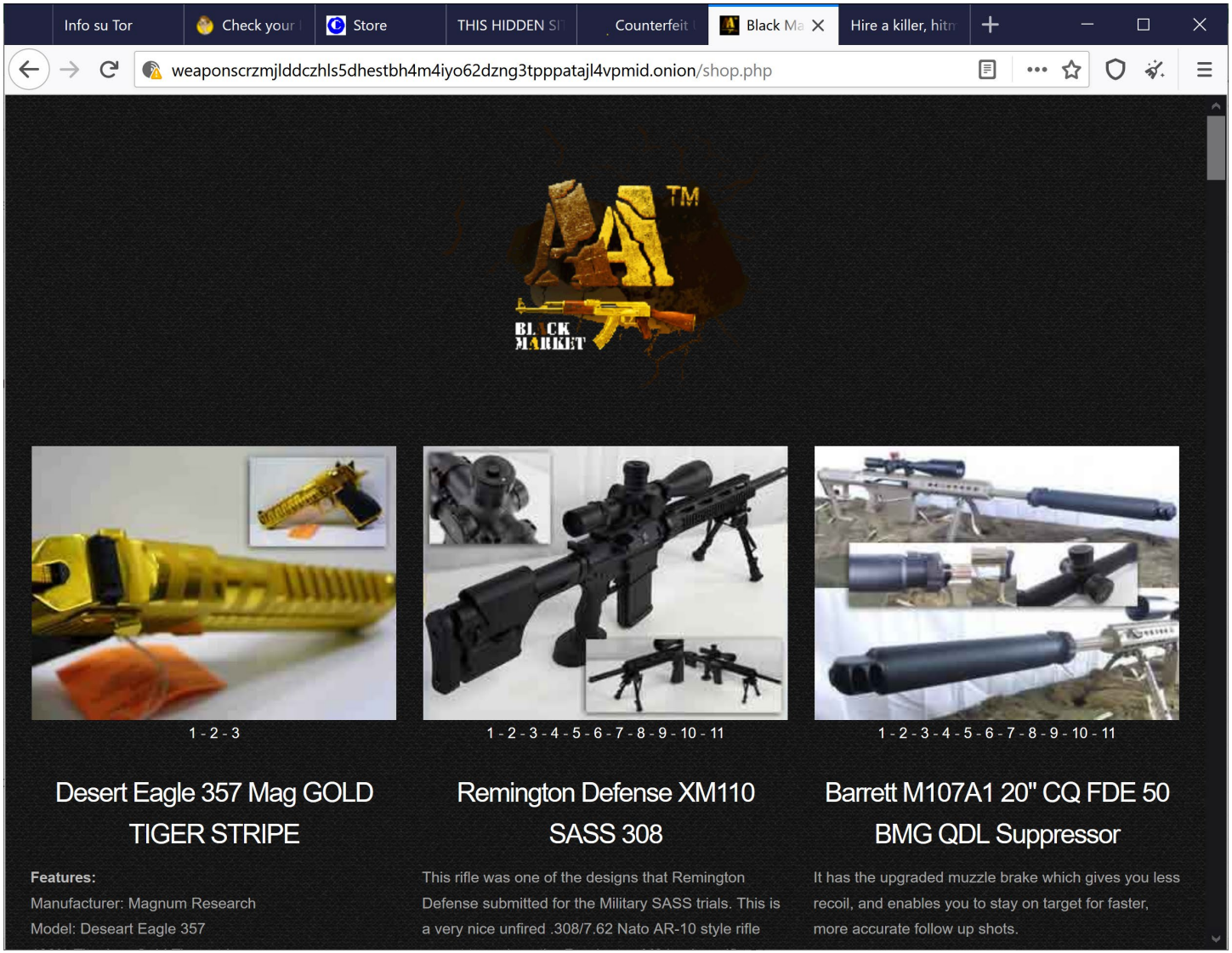
VI RICORDO CHE EFFETTUARE ACQUISTI SU DARK WEB DI DROGA, ARMI, E SERVIZI ILLEGALI, COME ANCHE NAVIGARE E SCARICARE CONTENUTI PEDOPORNOGRAFICI COSTITUISCE UN REATO.

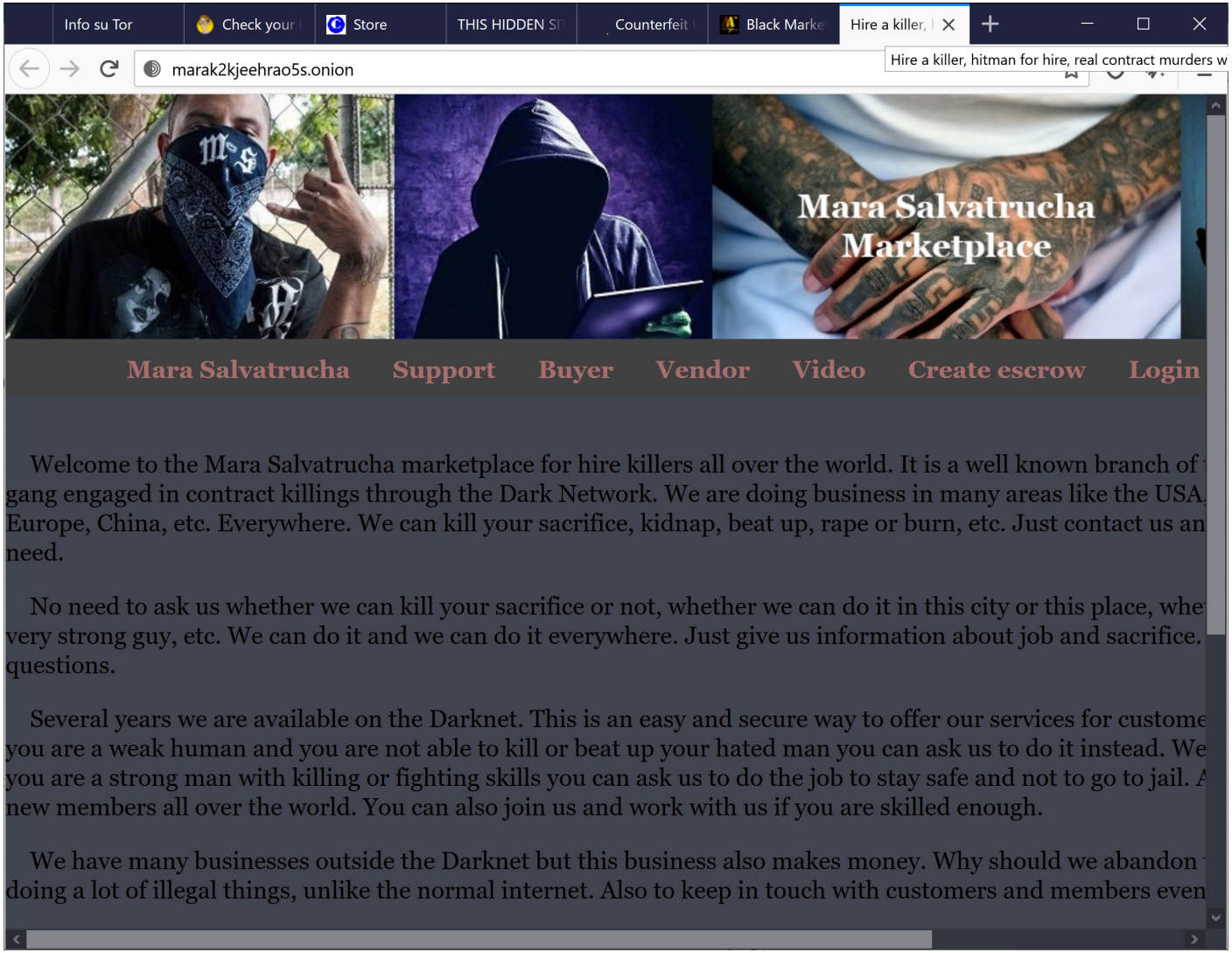
DARK WEB entriamo nella tana del bianconiglio…

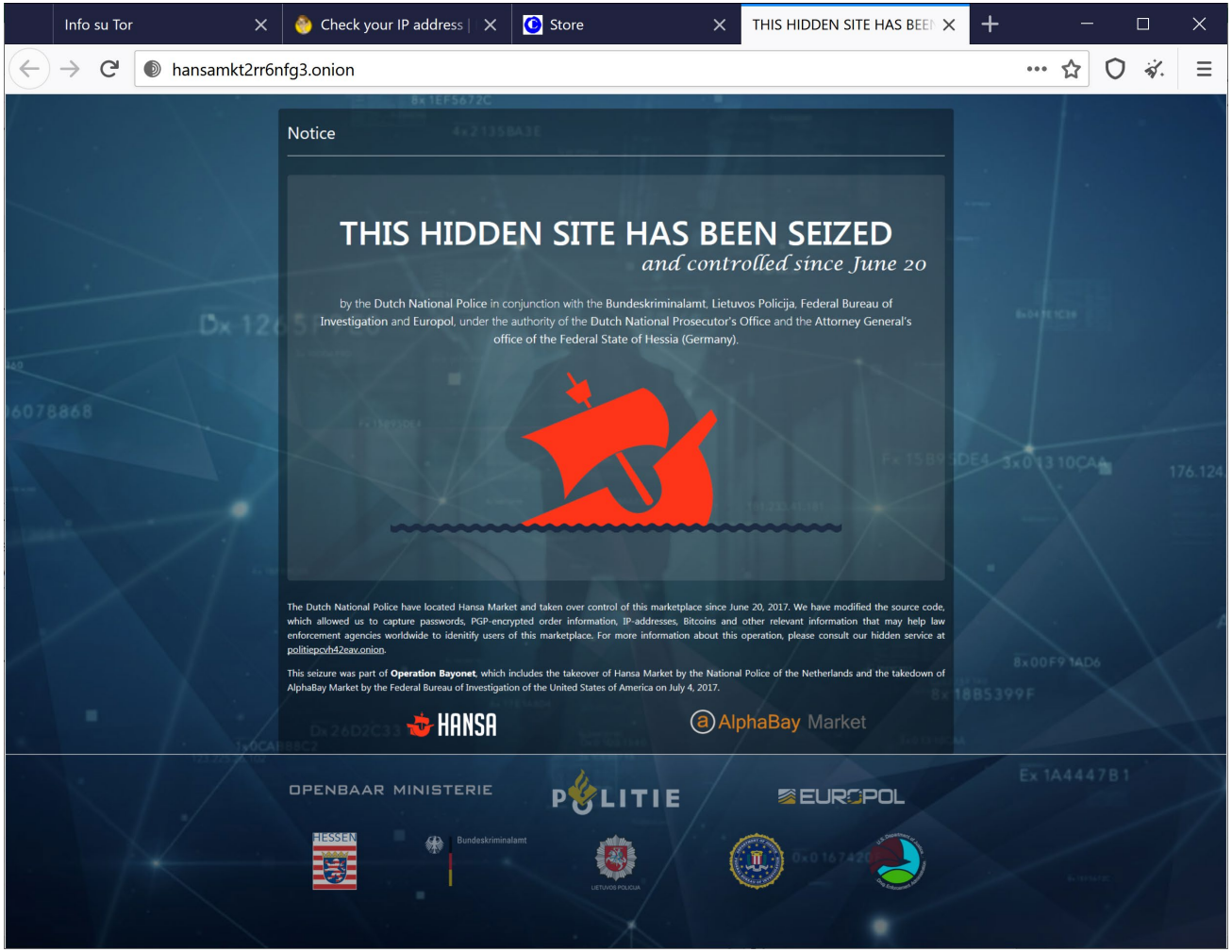












Agenda

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

Sessione domande e risposte

Sitografia in ordine di apparizione 1

http://www.websdr.org/ portale che raccoglie tutti i serve dei radioamatori mondiali, potete ascoltare tutte le frequenze disponibili da diverse antenne posizionate in tutto il mondo!
https://www.google.it/earth/versions/#download-pro per scaricare Google Earth Pro
https://nmap.org/ sito dove è possibile scaricare nmap anche per Windows
https://www.tenable.com/products/nessus
https://github.com/ElevenPaths/FOCA sito dove è possibile scaricare FOCA, richiede SQL Server
https://www.nirsoft.net/utils/dns_records_viewer.html sito dove è possibile scaricare DNS Data View
https://www.nirsoft.net/utils/domain_hosting_view.html sito dove è possibile scaricare Domain Hosting View
https://www.nirsoft.net/utils/ipnetinfo.html sito dove è possibile scaricare IP Net Info, vedere altri tool a piacere
https://www.repubblica.it/robots.txt esempio di disallow su robots.txt
https://www.ilmessaggero.it/robots.txt altro esempio di disallow su robots.txt
https://www.maltego.com/ tool specifico OSINT professionale
Https://www.exploit-db.com/google-hacking-database ricerche pronte per argomenti
https://www.google.com/search?q=Google+Hacking+for+penetration+testers+filetype%3Apdf
https://nordvpn.com/it migliore VPN per garantire anonimato su internet
https://www.torproject.org/ sito dove scaricate TOR Browser per navigare il Dark Web
https://www.tracelabs.org/initiatives/osint-vm macchina virtuale Linux con tool OSINT ready to go
https://www.learnallthethings.net/blog/2020/7/23/rage-against-the-virtual-machines
https://www.hunch.ly/ sito dove abbonarsi per elenco siti attivi su darkweb

Sitografia siti web OSINT

Social network

site:www.facebook.com cybera
site:www.facebook.com “Mario Rossi” (Immagini)
site:www.linkedin.com “Mario Rossi” (Immagini)
https://independent.academia.edu/
https://core.ac.uk/
https://onemilliontweetmap.com/
https://www.tweeplers.com/map/
https://www.hashatit.com/hashtags/etna

Biblioteche internazionali

https://www.loc.gov/search/?in=&q=graziani&new=true&st=
https://www.loc.gov/resource/sn83030272/1908-02-02/ed-1/?st=gallery

Mappe della conoscenza

https://openknowledgemaps.org/

Mappe arricchite

http://metrocosm.com/disputed-territories-map.html
https://www.healthmap.org/en/
https://www.marinetraffic.com/en/ais/home/centerx:10.5/centery:42.0/zoom:4
https://www.flightradar24.com/43.15,12.11/6
https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map
https://acleddata.com/dashboard/#/dashboard
https://newspapermap.com/#38.13456,14.89197,8z

Contatti

massimiliano.graziani@cybera.it

Dubbi, altre domande? Desiderate approfondimenti riguardo gli argomenti trattati? Scrivetemi, rispondo sempre a tutti!

Grazie…

Era il 6 giugno 2018 mentre ero relatore al Security Summit di Roma, non rispondevo al cellulare e non potevo soccorrere mio padre, colto da un infarto, mentre tutti mi chiamavano…

Tra sensi di colpa e rimorso per non essere arrivato in tempo per vederlo ancora vivo, per l'ultima volta…
…per questo dedico a Giuseppe, mio padre, ogni attività di divulgazione e condivisione accademica, perseguendo i valori che mi ha trasmesso: umiltà, generosità e sacrificio.

Grazie di tutto papà.