# Quels sont les outils de sécurité open source pertinents que vous devriez connaître et utiliser aujourd'hui ?

Marc Vael

Mardi 9 Octobre 2019
ISACA QUEBEC Conférence

# Clause de non-responsabilité

Les points de vue et opinions exprimés au cours de cette session sont ceux de l'orateur.

Rien dans cette séance ne doit être interprété comme un avis professionnel ou de sécurité.

Pour tous les outils présentés dans cette présentation, la qualité a été démontrée par des milliers d'utilisateurs qui les ont téléchargés, déployés et activement utilisés/révisés.

# Clause de non-responsabilité 2

Cette présentation n'est qu'une "entrée de 45 minutes" !

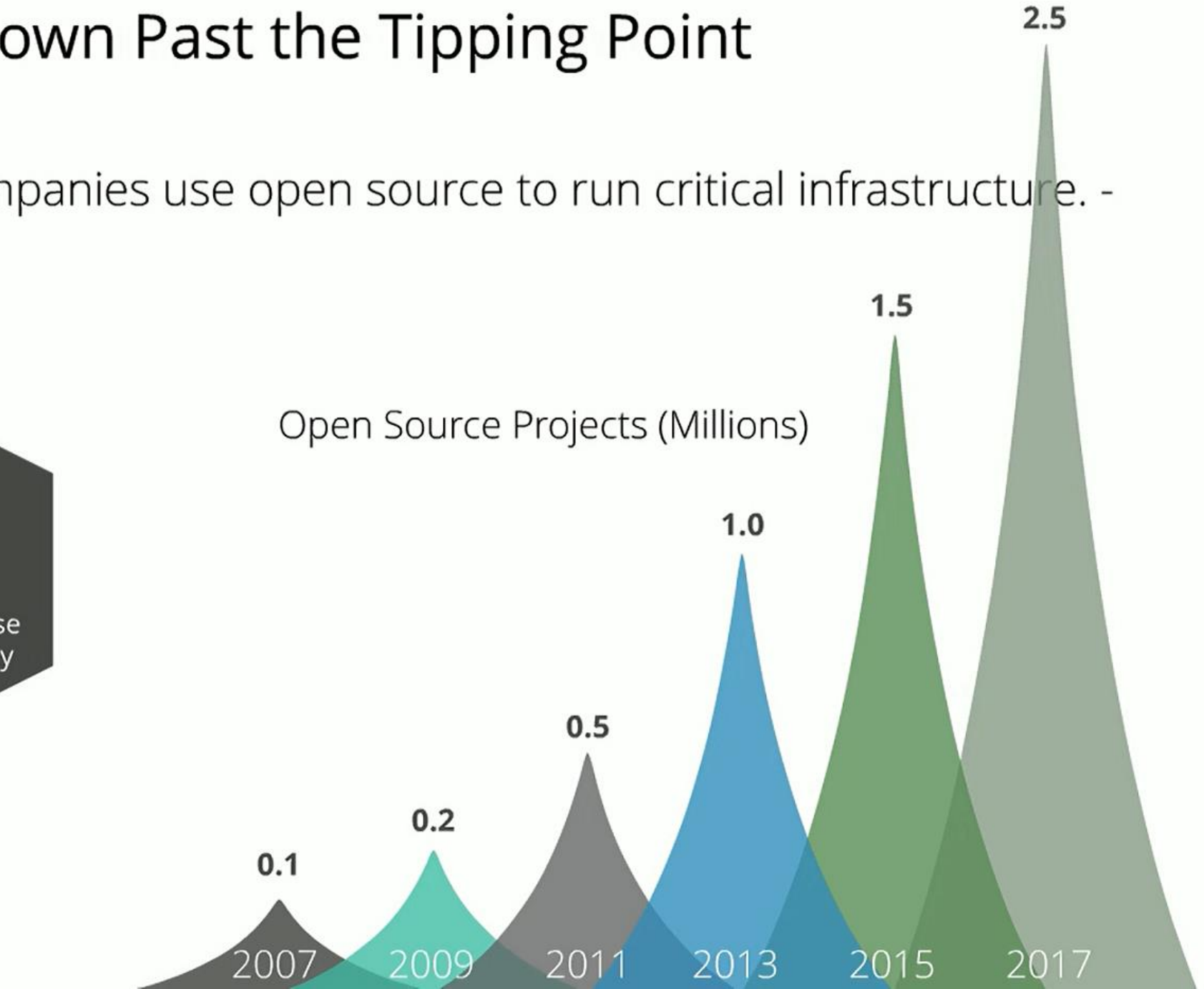
- Il existe de nombreux outils de sécurité open source dont nous ne parlerons pas aujourd'hui..... (plus d'informations à ce sujet plus tard)

# Open Source Has Blown Past the Tipping Point

Virtually all Global 2000 companies use open source to run critical infrastructure. - *Gartner*

**70%**
of apps will run on OSS databases by 2018

**50%**
of orgs face problems because of a lack of policy



# IBM buys Red Hat in $34 billion deal, adding Linux distributor

OCTOBER 29, 2018 / 8:20 AM / CBS/AP

Red Hat = société 100% open source

- IBM pouvait télécharger gratuitement tout leur code et l'utiliser
- IBM a quand même payé 34 000 000 000 000 USD

# Pourquoi utiliser des outils de sécurité open source ?

1. **Coût = l'une des raisons pour lesquelles les professionnels de la sécurité passent une partie de leur temps à travailler avec des outils de sécurité open source.**
2. **Apprendre, Expérimenter, Faire face à des situations nouvelles ou uniques ou de déployer sur une base de production = les professionnels de la sécurité considèrent les logiciels de sécurité open source comme une partie précieuse de leur boîte à outils.**
3. **Transparence = vous avez accès à tous les codes et vous êtes libre d'en faire ce que vous voulez !**
4. **Éviter de s'attacher à un fournisseur de services de sécurité particulier.**

# Facilitateurs d’outils de sécurité Open Source

GitHub

NIST
National Institute
of Standards
and Technology

source
forge



OWASP
Open Web Application
Security Project

# Catégories

Diviser tous les outils de sécurité open source en 3 catégories principales :

I. Audits de sécurité, tests et analyses forensiques
II. Surveillance et logging de la sécurité
III. Sécurité du système

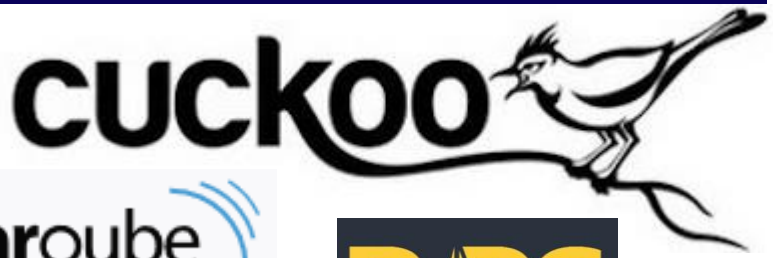
# Outils dont nous ne discuterons pas dans les prochaines minutes …


DELTA
SDN SECURITY ASSESSMENT FRAMEWORK

openNMS

moloch

cuckoo



bWAPP

sonarqube

hping

RAPS

GRR
RAPID RESPONSE

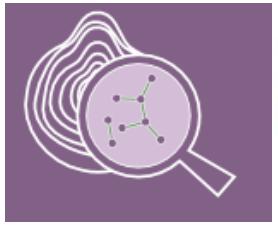
John the Ripper


BRAKEMAN

Kismet

Hardenize


MRTG
MULTI ROUTER TRAFFIC GRAPHER

PAROS

BabelEnterprise
OS Security Balanced Scorecard


SoRRy!

# I. Audits de sécurité, tests et analyses forensiques

https://www.kali.org/
https://tools.kali.org/tools-listing

# KALI

- Déesse hindoue, destructrice des forces du mal
- = une distribution Linux basée sur Debian et destinée aux tests de pénétration et à l'audit de sécurité avancés. Kali contient plusieurs centaines d'outils destinés à diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la criminalistique et l'ingénierie inverse.
- L'endroit idéal pour commencer si vous voulez commencer à utiliser des outils open source.
- Avant, on appelait cet outil backtrack
- De nombreux tutoriels disponibles

https://www.kali.org/
https://tools.kali.org/tools-listing

# KALI

## Comment utiliser KALI (1)

- Bootable usb
  - Live
  - Install
    - Utiliser des systèmes de fichiers cryptés !
- vm
  - Virtualbox, KVM ou vmware sur votre ordinateur portable.
  - @ cloud provider idéal pour l'audit de l’ “extérieur”
    - comme Azure, Google Cloud, etc.

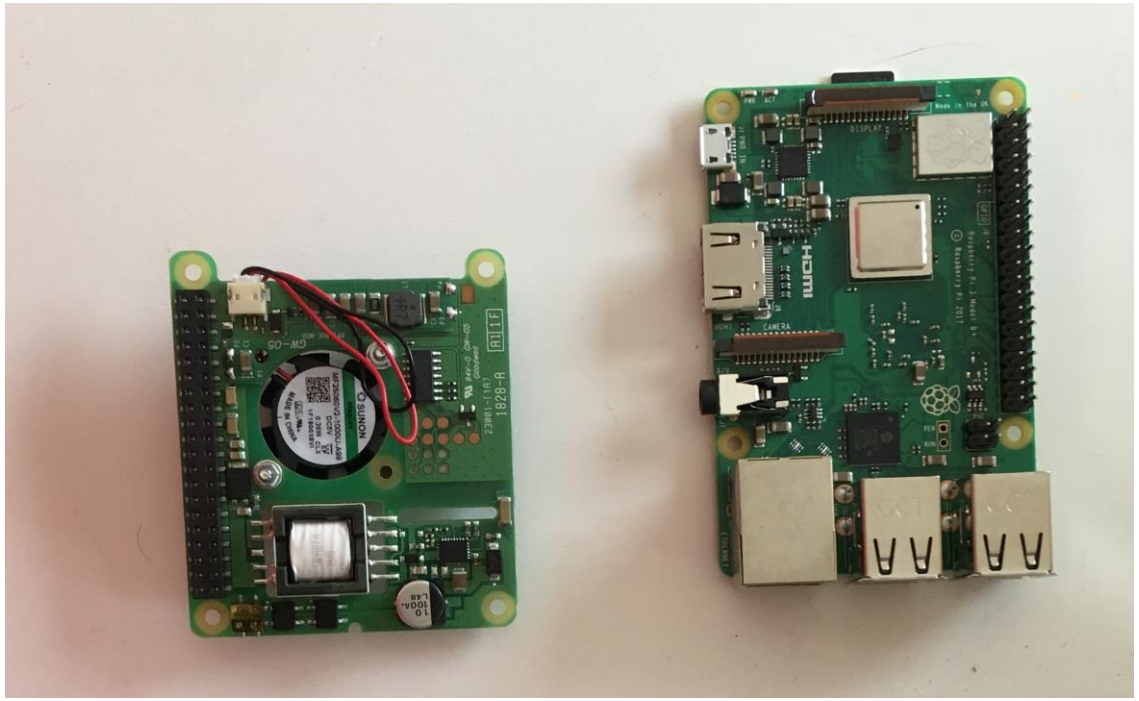
https://www.kali.org/
https://tools.kali.org/tools-listing

# KALI

## Utilisation avancée du Kali

Probe

- Nous utilisons un rasberry pi comme appareil d'audit.
  - +- 130€
- Laisser derrière chez les clients :
  - Set up a vpn, ssh or dns tunnel
  - Nous avons tous les outils disponibles pour le wifi, le réseau et autres audits



https://www.kali.org/
https://tools.kali.org/

KALI TOOLS

# KALI

1. **Collecte d'information**
   ace-voip,Amap,APT2,arp-scan,Automater,bing-ip2hosts,braa,CaseFile,CDPSnarf,cisco-torch,copy-router-config, DMitry, dnmap, dnsenum, dnsmap, DNSRecon, dnstracer,dnswalk,DotDotPwn,enum4linux,enumIAX,EyeWitness,Faraday,Fierce,Firewalk,fragroute,fragrouter,Ghost Phisher, GoLismero, goofile, hping3, ident-user-enum,InSpy,InTrace,iSMTP,lbd,Maltego Teeth,masscan,Metagoofil,Miranda,nbtscan-unixwiz, Nikto, Nmap, ntop, OSRFramework, p0f,Parsero,Recon-ng,SET,SMBMap,smtp-user-enum,snmp-check,SPARTA,sslcaudit,SSLsplit,sslstrip,SSLyze,Sublist3r,THC-IPV6, theHarvester, TLSSLed, twofi, Unicornscan, URLCrazy,Wireshark,WOL-E,Xplico
2. **Analyse de vulnérabilité**
   BBQSQL,BED,cisco-auditing-tool,cisco-global-exploiter,cisco-ocs,cisco-torch,copy-router-config,Doona,DotDotPwn,HexorBase,jSQL Injection, Lynis, Nmap, ohrwurm,openvas,Oscanner,Powerfuzzer,sfuzz,SidGuesser,SIPArmyKnife,sqlmap,Sqlninja,sqlsus,THC-IPV6,tnscmd10g,unix-privesc-check,Yersinia
3. **Attaques sans fil**
   Airbase-ng, Aircrack-ng, Airdecap-ng and Airdecloak-ng,Aireplay-ng,airgraph-ng,Airmon-ng,Airodump-ng,airodump-ng-oui-update,Airolib-ng,Airserv-ng,Airtun-ng,Asleap,Besside-ng,Bluelog,BlueMaho,Bluepot,BlueRanger,Bluesnarfer,Bully,coWPAtty,crackle,eapmd5pass,Easside-ng,Fern Wifi Cracker, FreeRADIUS-WPE, Ghost Phisher,GISKismet,Gqrx,gr-scan,hostapd-wpe,ivstools,kalibrate-rtl,KillerBee,Kismet,makeivs-ng,mdk3, mfcuk,mfoc, mfterm, Multimon-NG, Packetforge-ng,PixieWPS, Pyrit, Reaver, redfang, RTLSDR Scanner, Spooftooph, Tkiptun-ng, Wesside-ng, Wifi Honey, wifiphisher, Wifitap, Wifite, wpaclean
4. **Sécurité des applications Web**
   apache-users, Arachni, BBQSQL, BlindElephant, Burp Suite,CutyCapt,DAVTest,deblaze,DIRB,DirBuster,fimap,FunkLoad,Gobuster,Grabber,hURL,jboss-autopwn,joomscan,jSQL Injection, Maltego Teeth,Nikto,PadBuster,Paros,Parsero,plecost,Powerfuzzer,ProxyStrike,Recon-ng, Skipfish, sqlmap, Sqlninja, sqlsus,ua-tester,Uniscan,w3af,WebScarab,Webshag,WebSlayer,WebSploit,Wfuzz,WhatWeb,WPScan,XSSer,zaproxy
5. **Outils d'exploitation**
   Armitage, Backdoor Factory, BeEF, cisco-auditing-tool,cisco-global-exploiter,cisco-ocs,cisco-torch,Commix,crackle,exploitdb,jboss-autopwn,Linux Exploit Suggester, Maltego Teeth, Metasploit Framework,MSFPC,RouterSploit,SET,ShellNoob,sqlmap,THC-IPV6,Yersinia
6. **Tests de stress**
   DHCPig,FunkLoad,iaxflood,Inundator,inviteflood,ipv6-toolkit,mdk3,Reaver,rtpflood,SlowHTTPTest,t50,Termineter,THC-IPV6,THC-SSL-DOS

https://www.kali.org/
https://tools.kali.org/

KALI TOOLS

# KALI

7. **Outils forensiques**

   Binwalk,bulk-extractor,Capstone,chntpw,Cuckoo,dc3dd,ddrescue,DFF,diStorm3,Dumpzilla,extundelete,Foremost,Galleta,Guymager,iPhone Backup Analyzer,p0f,pdf-parser,pdfid,pdgmail,peepdf,RegRipper,Volatility,Xplico

8. **Sniffing & spoofing**

   bettercap, Burp Suite, DNSChef,fiked,hamster-sidejack,HexInject,iaxflood,inviteflood,iSMTP,isr-evilgrade,mitmproxy,ohrwurm,protos-sip, rebind, responder, rtpbreak,rtpinsertsound,rtpmixsound,sctpscan,SIPArmyKnife,SIPp,SIPVicious,SniffJoke,SSLsplit,sslstrip,THC-IPV6,VoIPHopper,WebScarab,Wifi Honey, Wireshark, xspy, Yersinia, zaproxy

9. **Attaques par mot de passe**

   BruteSpray, Burp Suite, CeWL,chntpw,cisco-auditing-tool,CmosPwd,creddump,crowbar,crunch,findmyhash,gpp-decrypt,hash-identifier, Hashcat, HexorBase, THC-Hydra, John the Ripper, Johnny, keimpx, Maltego Teeth, Maskprocessor, multiforcer, Ncrack, oclgausscrack, ophcrack, PACK, patator, phrasendrescher, polenum,RainbowCrack,rcracki-mt,RSMangler,SecLists,SQLdict,Statsprocessor,THC-pptp-bruter,TrueCrack,WebScarab,wordlists,zaproxy

10. **Maintenir accès**

    CryptCat,Cymothoa,dbd,dns2tcp,HTTPTunnel,Intersect,Nishang,polenum,PowerSploit,pwnat,RidEnum,sbd,shellter,U3-Pwn,Webshells,Weevely,Winexe

11. **Rétroingénierie**

    apktool,dex2jar,diStorm3,edb-debugger,jad,javasnoop,JD-GUI,OllyDbg,smali,Valgrind,YARA

12. **Hardware hacking**

    android-sdk,apktool,Arduino,dex2jar,Sakis3G,smali

13. **Outils de rapportage**

    CaseFile,cherrytree,CutyCapt,dos2unix,Dradis,MagicTree,Metagoofil,Nipper-ng,pipal,RDPY


Applications
Places
Fri 04:21
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Activities Overview
cewl
crunch
hashcat
john
johnny
medusa
ncrack
ophcrack
pyrit
rainbowcra...
rcracki_mt
wordlists

https://nmap.org/

# NMAP


- Nmap (Network Mapper) est un utilitaire gratuit et open source pour la découverte du réseau et l'audit de sécurité.
- De nombreux systèmes et administrateurs réseau le trouvent également utile pour des tâches telles que l'inventaire du réseau, la gestion des calendriers de mise à niveau des services et la surveillance de l'hôte ou du temps de disponibilité des services.
- Nmap utilise les paquets IP bruts de manière novatrice pour déterminer quels hôtes sont disponibles sur le réseau, quels services (nom d'application et version) ces hôtes offrent, quels systèmes d'exploitation (et versions d'OS) ils utilisent, quels types de filtres de paquets/pare-feu sont utilisés et des dizaines d'autres caractéristiques.
- Nmap a été conçu pour analyser rapidement les grands réseaux, mais fonctionne bien avec des hôtes uniques. En plus de l'exécutable Nmap en ligne de commande classique, la suite Nmap comprend une interface graphique avancée et un visualiseur de résultats (Zenmap), un outil flexible de transfert de données, de redirection et de débogage (Ncat), un utilitaire pour comparer les résultats de scan (Ndiff), et un outil de génération et de réponse par paquets (Nping). Nmap possède également des scripts qui peuvent détecter les problèmes liés au réseau.

https://nmap.org/

# NMAP


- Débutants : utiliser zenmap
  - Sélection facile de ce que vous voulez faire
    - Tous les types de scans, du balayage pingsweep au balayage intense
  - Belle façon d'afficher et de rapporter ce que vous trouvez
  - Mais : vous obtenez toujours la commande nmap cli pour une utilisation ultérieure
- Cool stuff :
  - NSE - toutes sortes de scripts pour vérifier les services et les tester
  - détection du système d'exploitation
  - Service fingerprinting

# Nmap Cheat Sheet

## Target Specification

| Switch | Example | Description |
|---|---|---|
| | nmap 192.168.1.1 | Scan a single IP |
| | nmap 192.168.1.1 192.168.2.1 | Scan specific IPs |
| | nmap 192.168.1.1-254 | Scan a range |
| | nmap scanme.nmap.org | Scan a domain |
| | nmap 192.168.1.0/24 | Scan using CIDR notation |
| -iL | nmap -iL targets.txt | Scan targets from a file |
| -iR | nmap -iR 100 | Scan 100 random hosts |
| --exclude | nmap --exclude 192.168.1.1 | Exclude listed hosts |

## Scan Techniques

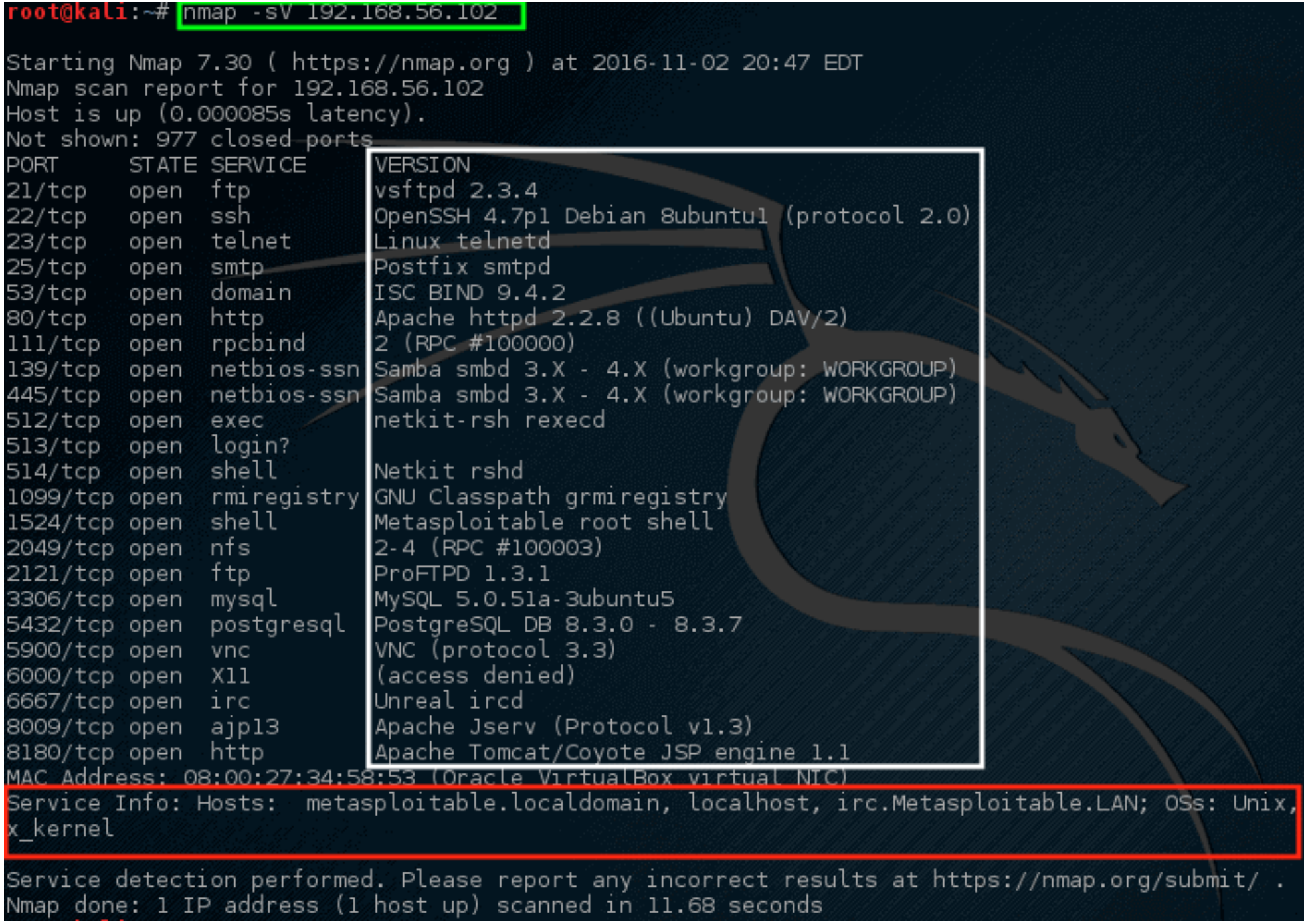
| Switch | Example | Description |
|---|---|---|
| -sS | nmap 192.168.1.1 -sS | TCP SYN port scan (Default) |
| -sT | nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU | nmap 192.168.1.1 -sU | UDP port scan |
| -sA | nmap 192.168.1.1 -sA | TCP ACK port scan |
| -sW | nmap 192.168.1.1 -sW | TCP Window port scan |
| -sM | nmap 192.168.1.1 -sM | TCP Maimon port scan |

## Host Discovery

| Switch | Example | Description |
|---|---|---|
| -sL | nmap 192.168.1.1-3 -sL | No Scan. List targets only |
| -sn | nmap 192.168.1.1/24 -sn | Disable port scanning |
| -Pn | nmap 192.168.1.1-5 -Pn | Disable host discovery |
| -PS | nmap 192.168.1.1-5 -PS22-25,80 | TCP SYN discovery on port x. Port 80 by default |
| -PA | nmap 192.168.1.1-5 -PA22-25,80 | TCP ACK discovery on port x. Port 80 by default |
| -PU | nmap 192.168.1.1-5 -PU53 | UDP discovery on port x. Port 40125 by default |
| -PR | nmap 192.168.1.1-1/24 -PR | ARP discovery on local network |
| -n | nmap 192.168.1.1 -n | Never do DNS resolution |

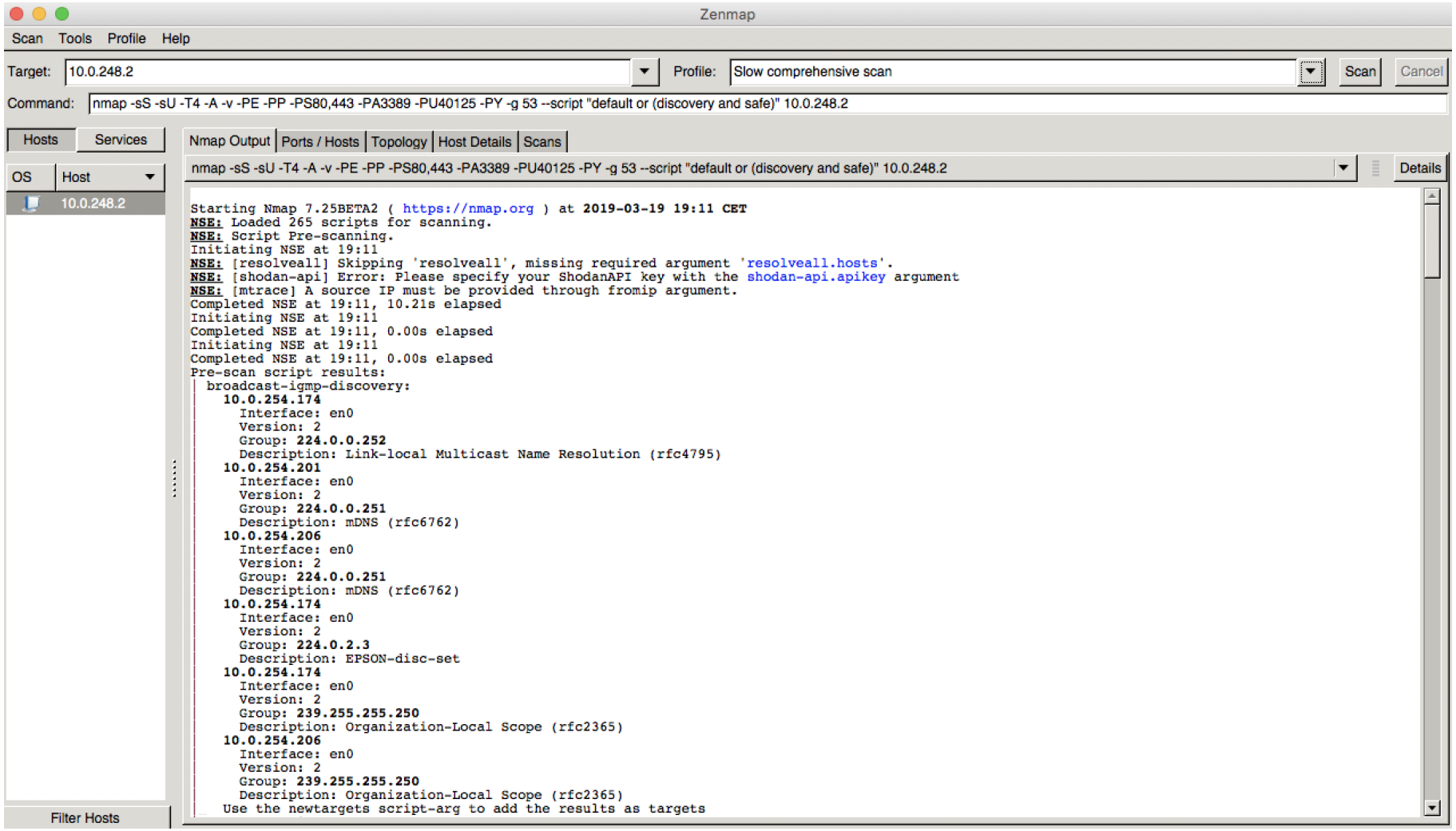
## Port Specification

| Switch | Example | Description |
|---|---|---|
| -p | nmap 192.168.1.1 -p 21 | Port scan for port x |
| -p | nmap 192.168.1.1 -p 21-100 | Port range |
| -p | nmap 192.168.1.1 -p U:53,T:21-25,80 | Port scan multiple TCP and UDP ports |
| -p- | nmap 192.168.1.1 -p- | Port scan all ports |
| -p | nmap 192.168.1.1 -p http,https | Port scan from service name |
| -F | nmap 192.168.1.1 -F | Fast port scan (100 ports) |
| --top-ports | nmap 192.168.1.1 --top-ports 2000 | Port scan the top x ports |
| -p-65535 | nmap 192.168.1.1 -p-65535 | Leaving off initial port in range makes the scan start at port 1 |
| -p0- | nmap 192.168.1.1 -p0- | Leaving off end port in range makes the scan go through to port 65535 |


root@kali:~# nmap -sV 192.168.56.102
Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:47 EDT
Nmap scan report for 192.168.56.102
Host is up (0.000085s latency).
Not shown: 977 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open rmiregistry GNU Classpath grmiregistry
1524/tcp open shell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc Unreal ircd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix,
x_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds

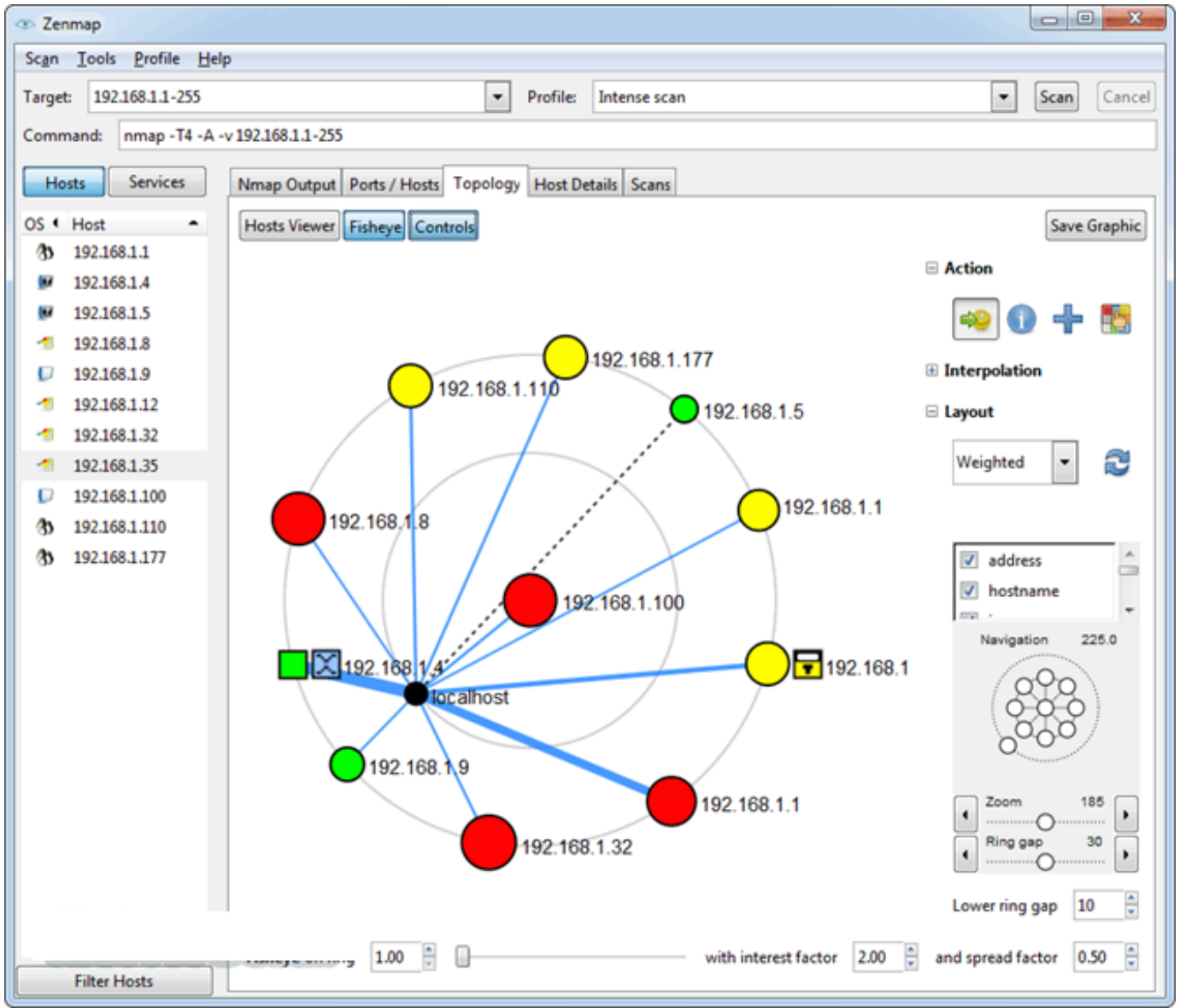
https://nmap.org/zenmap/

# Zenmap



https://nmap.org/zenmap/

# Zenmap



https://nmap.org/

# NMAP


Exemples

- `nmap --open 10.0.0.0/24 -p22`
  (moyen rapide de trouver tous les hôtes d'un réseau exécutant ssh)
- nmap --script http-headers -p80,443 www.ba.be
  - Vérifie les en-têtes du serveur web
- Nmap –script ssl-* -p443 storefront.marks.com
  - Vérifie la qualité ssl d'un serveur web (clés, vulnérabilités, etc.)
- Locate *.nse vous donne un aperçu de tous les plugins ( > 540 )
  - Toutes sortes de scripts pour le forçage brutal, la vérification de vulnérabilités connues, etc.

https://www.tenable.com/products/nessus/nessus-professional
http://www.openvas.org/

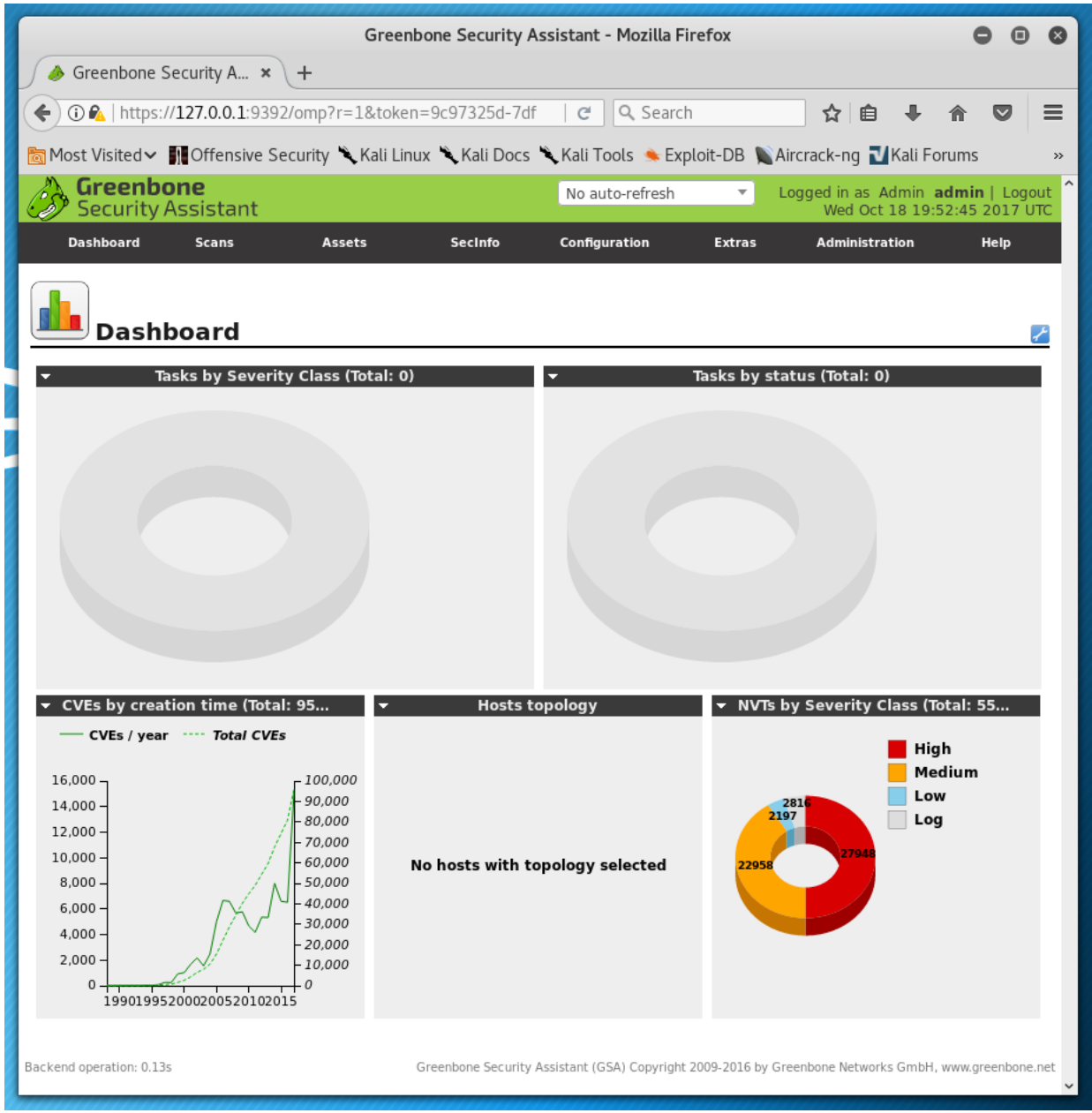
# OPENVAS

- Analyseur de vulnérabilité
  - Fourchette de l'outil open source NESSUS devenu commercial en 2005.
  - Nessus/Openvas est l'analyseur de vulnérabilité le plus populaire et le troisième programme de sécurité le plus populaire actuellement utilisé.
  - Se cache sous de nombreuses offres commerciales : Greenbone, Acunetix, Alienvault, etc.
- Utilise beaucoup d'outils (nmap, etc.) pour vérifier le service et crée un rapport détaillant toute vulnérabilité de sécurité trouvée.

http://www.openvas.org/

# OPENVAS

- Outil Web d'évaluation de la vulnérabilité
- L'alimentation des vulnérabilités est particulièrement importante!
  - Communauté
  - Des aliments commerciaux sont disponibles (réagissent plus rapidement)



# Summary

Scan started: **Wed Feb 13 04:26:48 2019 UTC**
Scan ended: Wed Feb 13 04:41:16 2019 UTC

| 3 | 4 | 0 |
|---|---|---|
| HIGH | MEDIUM | LOW |

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

## Host Summary

| Host | Start | End | High | Medium | Low | Log |
|---|---|---|---|---|---|---|
| 192.168.1.211 | Feb 13, 04:27 | Feb 13, 04:41 | 3 | 4 | 0 | 0 |
| Total: 1 | | | 3 | 4 | 0 | 0 |

## Vulnerability Summary

| Severity | Description | CVSS | Count |
|---|---|---|---|
| High | Webmin <= 1.900 RCE Vulnerability | 9.0 | 1 |
| High | HTTP Brute Force Logins With Default Credentials Reporting | 9.0 | 2 |
| Medium | Webmin 1.880 Information Disclosure Vulnerability | 5.0 | 1 |
| Medium | Cleartext Transmission of Sensitive Information via HTTP | 4.8 | 1 |
| Medium | SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... | 4.0 | 2 |


Speed UP!

https://github.com/rapid7/metasploit-framework
https://www.metasploit.com/

# METASPLOIT

- logiciel de pénétration open source, populaire parmi les pirates informatiques.
- meilleur outil pour tester le réseau de manière offensive contre des vulnérabilités ouvertes et connues. Il s'agit d'une combinaison de différents modules pour vérifier différents exploits. Il est également utilisé pour l'audit et la numérisation.
- aide les équipes à faire plus que simplement vérifier les vulnérabilités, gérer les évaluations de sécurité et améliorer la sensibilisation à la sécurité ; il donne la possibilité de toujours avoir une (ou deux) pas d'avance sur le jeu.
- utile pour la validation de l'exploitation. Lorsqu'un analyseur de vulnérabilité montre qu'une machine est vulnérable à un exploit, le test manuel est toujours une pratique préférable pour s'assurer qu'il ne s'agit pas d'un faux positif de l'analyseur. La validation manuelle permet au testeur de mieux comprendre l'exploit et comment s'en défendre correctement.
- Metasploit framework est utilisé pour exécuter des tests de sécurité internes. Il aide à identifier les faiblesses possibles des réseaux internes avant qu'un compromis ne se produise. Il est également utilisé pour justifier des mises à jour coûteuses des logiciels et des pratiques commerciales en illustrant l'utilisation possible d'une vulnérabilité dans la nature.

https://portswigger.net/burp

# BURP SUITE

- outil graphique pour tester la sécurité des applications Web.
- 3 éditions : une édition communautaire gratuite, une édition professionnelle et une édition entreprise.
- fournir une solution complète pour les contrôles de sécurité des applications Web.

•**HTTP Proxy**: interception, inspection & modification of raw traffic passing in both directions.
•**WebApp Scanner** performing automated vulnerability scans of web applications.
•**Intruder** perform automated attacks on web applications: test & detect SQL injections, cross-site scripting, parameter manipulation and vulnerabilities susceptible to brute-force attacks.
•**Spider** automatically crawling web applications.
•**Repeater** to manually test an application.
•**Decoder** transforming encoded data into its canonical form, or for transforming raw data into various encoded and hashed forms. capable of recognizing several encoding formats.
•**Comparer** performing a comparison (a visual "diff") between any two items of data.
•**Extender** allows to load Burp extensions, to extend Burp's functionality using security testers code
•**Sequencer** analyzing quality of randomness in sample of data items to test an application's session tokens or other data items intended to be unpredictable, such as password reset tokens, etc.

https://github.com/OWASP/www-project-zap
https://www.zaproxy.org/

# Zed Attack Proxy

- Scanner d'application web open source gratuit.
- Le meilleur outil pour trouver automatiquement les vulnérabilités de sécurité dans vos applications Web pendant que vous développez et testez vos applications.
- outil idéal pour les pentesters expérimentés à utiliser pour les tests de sécurité manuels.
- un "proxy man-in-the-middle" = se trouve entre le navigateur du testeur et l'application web afin qu'il puisse intercepter et inspecter les messages envoyés entre le navigateur et l'application web, modifier le contenu si nécessaire, puis transmettre ces paquets à la destination. Il peut être utilisé comme une application autonome, et comme un processus démon.
- Quelques fonctionnalités :
  - Traditional and AJAX spiders
  - Automated scanner
  - Passive scanner
  - Forced browsing
  - Dynamic SSL certificates
  - Smartcard and Client Digital Certificates support
  - Plug-n-Hack support
  - Authentication and session support

https://github.com/sqlmapproject/sqlmap
http://sqlmap.org/

# SQL MAP

- des logiciels libres pour détecter et exploiter les vulnérabilités des bases de données et fournir des options pour y injecter des codes malveillants
- un outil de test d'intrusion qui automatise le processus de détection et d'exploitation des failles d'injection SQL en fournissant son interface utilisateur
- En plus de cartographier et de détecter les vulnérabilités, le logiciel permet d'accéder à la base de données, de modifier et de supprimer des données et de visualiser les données dans des tableaux tels que les utilisateurs, les mots de passe, les sauvegardes, les numéros de téléphone, les adresses électroniques, les cartes de crédit et autres informations confidentielles et sensibles.
- support complet de plusieurs SGBD : MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird et SAP MaxDB.

https://www.wireshark.org/

# WIRESHARK

- analyseur de protocole réseau open source : visualisez le trafic réseau en direct en détail pour suivre les flux réseau et trouver les problèmes sur un réseau de toute taille. Très similaire à TCPDUMP.
- conçu pour tous ceux qui ont besoin de surveiller leur réseau pour des problèmes de sécurité ou de performance au moment de la capture des paquets.
  - Wireshark peut lire les informations capturées à partir d'applications telles que Snoop, Sniffer et Microsoft Network Monitor.
  - peut également mettre les contrôleurs d'interface réseau sans fil en mode moniteur.
- fonctionne sous Linux, macOS, BSD, Solaris et Microsoft Windows. Il existe également une version basée sur terminal (non-GUI) appelée TShark.
- beaucoup de tutoriels disponibles

https://www.ettercap-project.org/ettercap/

# ETTERCAP


- réseau d'essai de résistance aux attaques par l'homme au milieu (MITM) (depuis 2001)
- 4 modes de fonctionnement de base :
  - IP-based: packets are filtered based on IP source and destination.
  - MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
  - ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts (full-duplex).
  - PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (half-duplex).
- fonctionne sur divers systèmes d'exploitation de type Unix, notamment Linux, Mac OS X, BSD et Solaris, et sur Microsoft Windows.
- capable d'intercepter le trafic sur un segment de réseau, de capturer des mots de passe et d'effectuer une écoute active contre un certain nombre de protocoles communs.
- de fortes capacités pour les attaques MITM et une solide augmentation pour les fonctions d'analyse et de visibilité.

https://ghidra-sre.org/
https://github.com/NationalSecurityAgency/ghidra

# GHIDRA


- le cadre de rétro-ingénierie (SRE) des logiciels libres mis au point par la NSA. Il aide à analyser les codes malveillants et les logiciels malveillants tels que les virus, et peut donner aux professionnels de la cybersécurité une meilleure compréhension des vulnérabilités potentielles de leurs réseaux et systèmes.
- idéal pour les ingénieurs logiciels, en particulier les analystes de logiciels malveillants.
- incluent le désassemblage, l'assemblage, la décompilation, la création de graphiques et de scripts, ainsi que des centaines d'autres fonctionnalités.
- utilise Jython pour que les utilisateurs puissent développer leurs propres composants et/ou scripts de plug-in Ghidra en utilisant Java ou Python.
- L'existence de Ghidra a été révélée au public via WikiLeaks en mars 2017, mais le logiciel est resté indisponible jusqu'à sa déclassification/version officielle en mars 2019.

https://digital-forensics.sans.org/community/downloads#overview

# SIFT


- groupe d'outils d'intervention en cas d'incident et d'outils médico-légaux libres conçus pour effectuer des examens médico-légaux numériques détaillés dans une variété de contextes.
- peut correspondre à n'importe quel ensemble d'outils d'intervention en cas d'incident et de police scientifique.
- démontre que des capacités avancées d'intervention en cas d'incident et des techniques judiciaires numériques en plongée profonde contre les intrusions peuvent être réalisées à l'aide d'outils open-source de pointe qui sont librement disponibles et fréquemment mis à jour.
- La boîte à outils forensiques tout-en-un open source peut facilement être construite directement dans les environnements cloud.

http://binwalk.org/

# BINWALK

- un outil d'analyse, d'ingénierie inverse et d'extraction d'images de firmware et de recherche de fichiers et de code exécutable intégrés dans une image binaire donnée.
- conçu pour identifier les fichiers et le code intégrés à l'intérieur des images du firmware.
- Binwalk utilise la librairie libmagic, donc elle est compatible avec les signatures magiques créées pour l'utilitaire de fichiers Unix.
- Binwalk inclut également un fichier de signature magique personnalisé qui contient des signatures améliorées pour les fichiers que l'on trouve couramment dans les images de firmware telles que les fichiers compressés/archivés, les en-têtes de firmware, les noyaux Linux, les bootloaders, les systèmes de fichiers, etc.
- Analyse heuristique de compression / chiffrement inconnus
- Visualiser les données binaires

https://www.gnu.org/software/ddrescue/

# Ddrescue

- outil de récupération de données : copie les données d'un fichier ou d'un bloc de données (disque dur, cdrom, etc.) vers un autre, en essayant de sauver les bonnes parties en premier en cas d'erreurs de lecture.
- aide à faire des copies correctes et forensiques des disques (même lorsqu'ils sont endommagés)
- le fonctionnement de base de ddrescue est entièrement automatique.
- mapfile est sauvegardé périodiquement sur disque. Ainsi, en cas d'accident, vous pouvez reprendre le sauvetage avec peu de recopies.  De plus, le même fichier mapfile peut être utilisé pour plusieurs commandes qui copient différentes zones du fichier, et pour plusieurs tentatives de récupération sur différents sous-ensembles.
- dispose d'un "mode de remplissage" capable d'écraser sélectivement des parties du fichier de sortie, qui a un certain nombre d'utilisations intéressantes comme l'effacement de données, le marquage de mauvaises zones ou même, dans certains cas, la "réparation" des secteurs endommagés.
- interface-agnostic : peut être utilisé pour tout type de périphérique supporté par le noyau (ATA, SATA, SCSI, vieux lecteurs, disquettes, ou cartes flash comme SD).

https://www.xplico.org/



# XPLICO

- Outil d'analyse forensiques en réseau (NFAT) à code source libre.
- permet d'extraire les fichiers du trafic Internet pour capturer les données des applications contenues dans les fichiers
  - à partir d'un fichier pcap Xplico extrait chaque email (POP, IMAP, and SMTP protocols), tous les contenus HTTP, chaque appel VoIP (SIP), IRC, FTP, TFTP, etc.
- 4 macro-composants:
  - Decoder Manager (DeMa)
  - **IP decoder called Xplico**
  - ensemble de manipulateurs de données
  - système de visualisation pour visualiser les données extraites

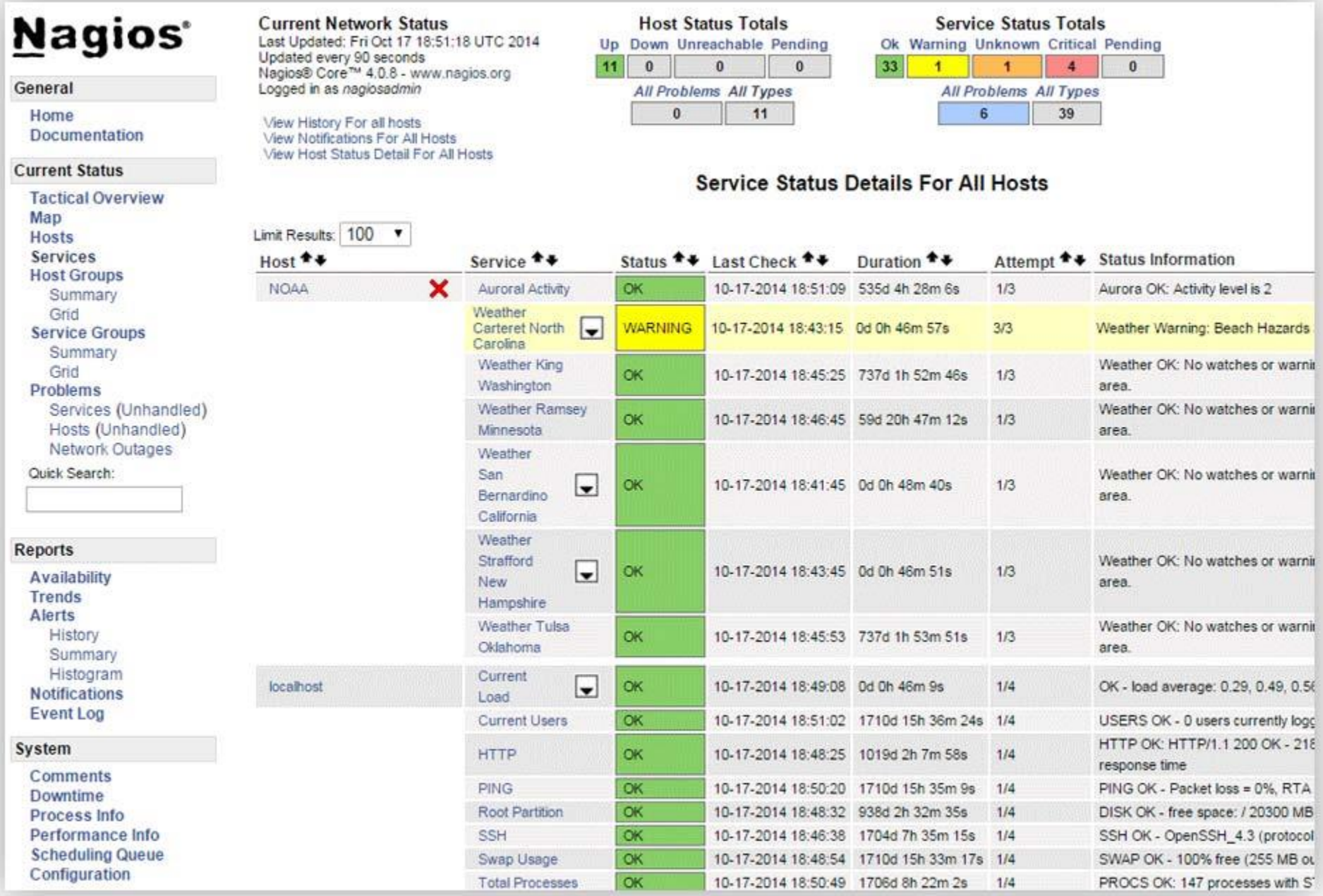
# II. Surveillance et logging de la sécurité

https://www.nagios.org/

# NAGIOS CORE

- application open source qui surveille les systèmes, les réseaux et l'infrastructure avec des services de surveillance et d'alerte pour les serveurs, commutateurs, applications et services.
- Il alerte les utilisateurs lorsque les choses tournent mal et les avertit une deuxième fois lorsque le problème a été résolu.  Nagios est également disponible en version commerciale.
- Les produits individuels peuvent être surveillés, et les tâches individuelles peuvent être effectuées, par des plug-ins ; environ 50 plug-ins "officiels" développés par Nagios & +3.000 plug-ins fournis par la communauté.
- L'interface utilisateur de Nagios peut être modifiée via un front-end pour la plate-forme desktop, web ou mobile, et la configuration peut être gérée via un des outils de configuration disponibles.

Nagios = “Nagios Ain't Gonna Insist On Sainthood”


Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
Current Network Status
Last Updated: Fri Oct 17 18:51:18 UTC 2014
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
11 0 0 0
All Problems All Types
0 11
Service Status Totals
Ok Warning Unknown Critical Pending
33 1 1 4 0
All Problems All Types
6 39
Service Status Details For All Hosts
Limit Results: 100
Host
Service
Status
Last Check
Duration
Attempt
Status Information
NOAA
Auroral Activity
OK
10-17-2014 18:51:09
535d 4h 28m 6s
1/3
Aurora OK: Activity level is 2
Weather Carteret North Carolina
WARNING
10-17-2014 18:43:15
0d 0h 46m 57s
3/3
Weather Warning: Beach Hazards
Weather King Washington
OK
10-17-2014 18:45:25
737d 1h 52m 46s
1/3
Weather OK: No watches or warni
area.
Weather Ramsey Minnesota
OK
10-17-2014 18:46:45
59d 20h 47m 12s
1/3
Weather OK: No watches or warni
area.
Weather San Bernardino California
OK
10-17-2014 18:41:45
0d 0h 48m 40s
1/3
Weather OK: No watches or warni
area.
Weather Strafford New Hampshire
OK
10-17-2014 18:43:45
0d 0h 46m 51s
1/3
Weather OK: No watches or warni
area.
Weather Tulsa Oklahoma
OK
10-17-2014 18:45:53
737d 1h 53m 51s
1/3
Weather OK: No watches or warni
area.
localhost
Current Load
OK
10-17-2014 18:49:08
0d 0h 46m 9s
1/4
OK - load average: 0.29, 0.49, 0.5
Current Users
OK
10-17-2014 18:51:02
1710d 15h 36m 24s
1/4
USERS OK - 0 users currently logg
HTTP
OK
10-17-2014 18:48:25
1019d 2h 7m 58s
1/4
HTTP OK: HTTP/1.1 200 OK - 218
response time
PING
OK
10-17-2014 18:50:20
1710d 15h 35m 9s
1/4
PING OK - Packet loss = 0%, RTA
Root Partition
OK
10-17-2014 18:48:32
938d 2h 32m 35s
1/4
DISK OK - free space: / 20300 MB
SSH
OK
10-17-2014 18:46:38
1704d 7h 35m 15s
1/4
SSH OK - OpenSSH_4.3 (protocol
Swap Usage
OK
10-17-2014 18:48:54
1710d 15h 33m 17s
1/4
SWAP OK - 100% free (255 MB ou
Total Processes
OK
10-17-2014 18:50:49
1706d 8h 22m 2s
1/4
PROCS OK: 147 processes with S

Nagios®

General
Home
Documentation

Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services
(Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:

Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log

System

## Host Information

Last Updated: Tue Dec 16 15:34:03 IST 2014
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

View Status Detail For This Host
View Alert History For This Host
View Trends For This Host
View Alert Histogram For This Host
View Availability Report For This Host
View Notifications For This Host

Host
**client**
**(client)**

Member of
**No hostgroups**

192.168.1.152

### Host State Information

| | |
|---|---|
| **Host Status:** | **UP** (for 0d 0h 1m 32s+) |
| **Status Information:** | PING OK - Packet loss = 0%, RTA = 1.30 ms |
| **Performance Data:** | rta=1.296000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0 |
| **Current Attempt:** | 1/5 (HARD state) |
| **Last Check Time:** | 12-16-2014 15:32:31 |
| **Check Type:** | ACTIVE |
| **Check Latency / Duration:** | 0.010 / 4.016 seconds |
| **Next Scheduled Active Check:** | 12-16-2014 15:37:35 |
| **Last State Change:** | N/A |
| **Last Notification:** | N/A (notification 0) |
| **Is This Host Flapping?** | **NO** (0.00% state change) |
| **In Scheduled Downtime?** | **NO** |
| **Last Update:** | 12-16-2014 15:34:00 ( 0d 0h 0m 3s ago) |

| | |
|---|---|
| **Active Checks:** | **ENABLED** |
| **Passive Checks:** | **ENABLED** |
| **Obsessing:** | **ENABLED** |
| **Notifications:** | **ENABLED** |
| **Event Handler:** | **ENABLED** |
| **Flap Detection:** | **ENABLED** |

### Host Commands

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Send custom host notification
- Schedule downtime for this host
- Schedule downtime for all services on this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host

### Host Comments

Add a new comment  Delete all comments

| Entry Time | Author | Comment | Comment ID | Persistent | Type | Expires | Actions |
|---|---|---|---|---|---|---|---|
| This host has no comments associated with it | | | | | | | |

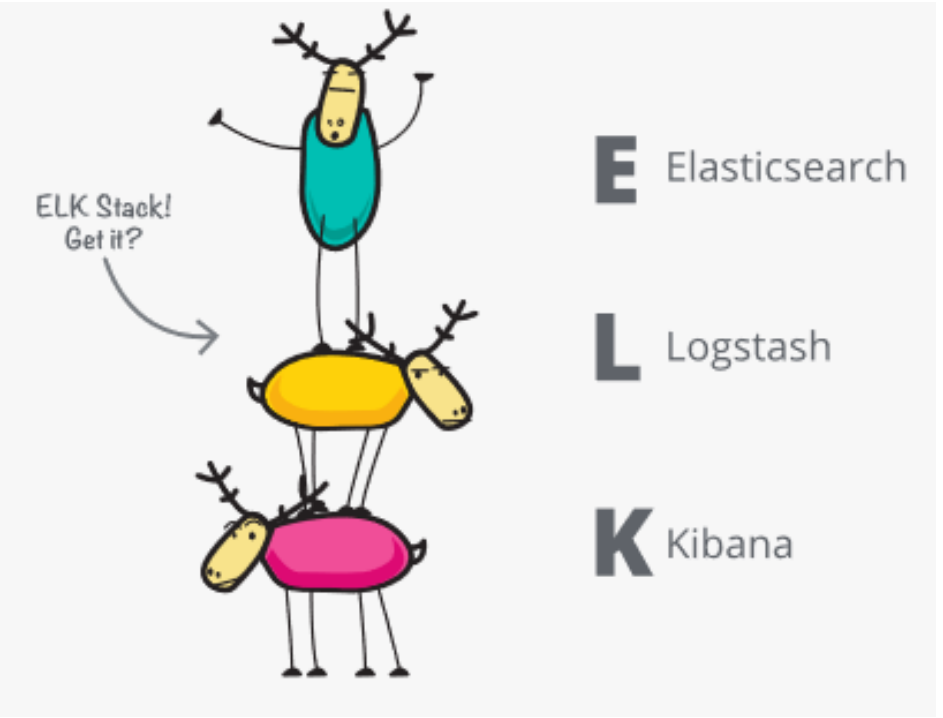
https://www.elastic.co/elk-stack

# ELK Stack



3 projets open source :

- **Elasticsearch** est un moteur de recherche et d'analyse.
- **Logstash** est un moteur de traitement de données côté serveur qui ingère des données provenant de plusieurs sources simultanément, les transforme, puis les envoie à une "stash" comme Elasticsearch.
- **Kibana** permet aux utilisateurs de visualiser les données à l'aide de tableaux et de graphiques dans Elasticsearch.



kibana

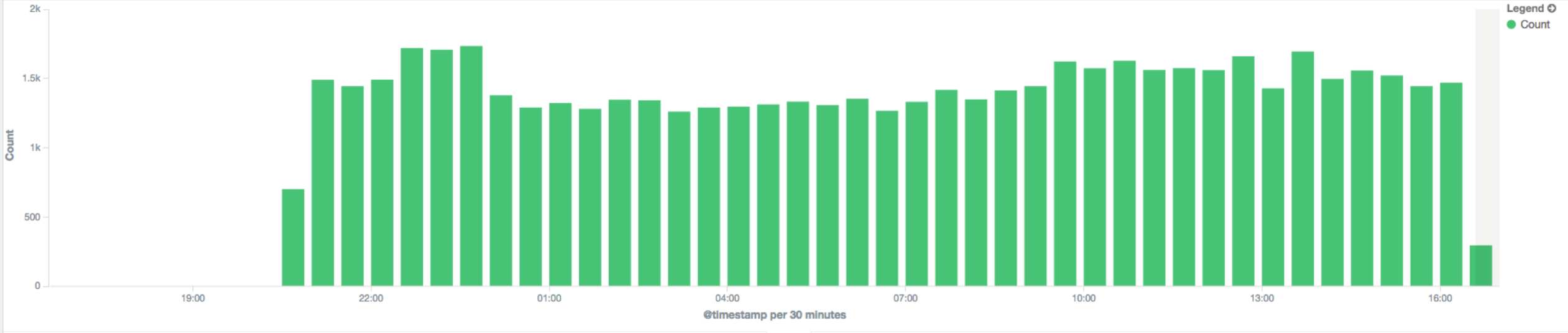
Discover | Visualize | Dashboard | Settings

5 minutes | Last 24 hours

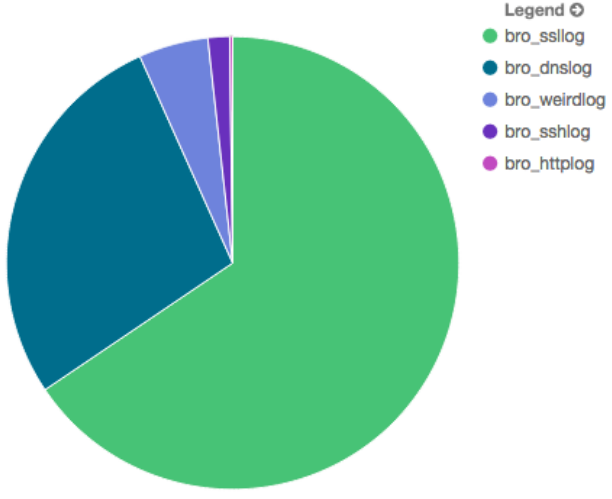
Bitcoinium

*

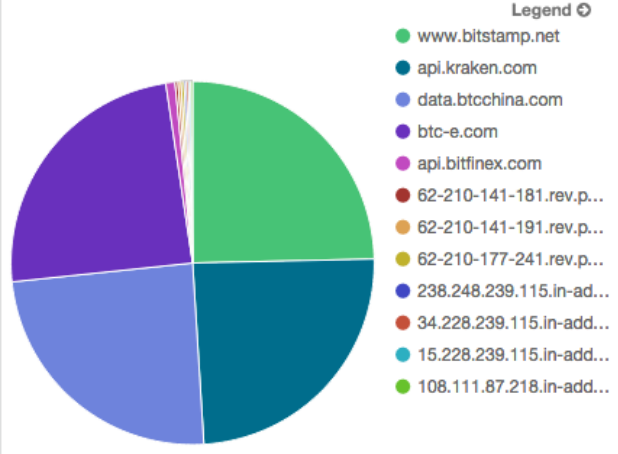
## Bitcoinium Total Count



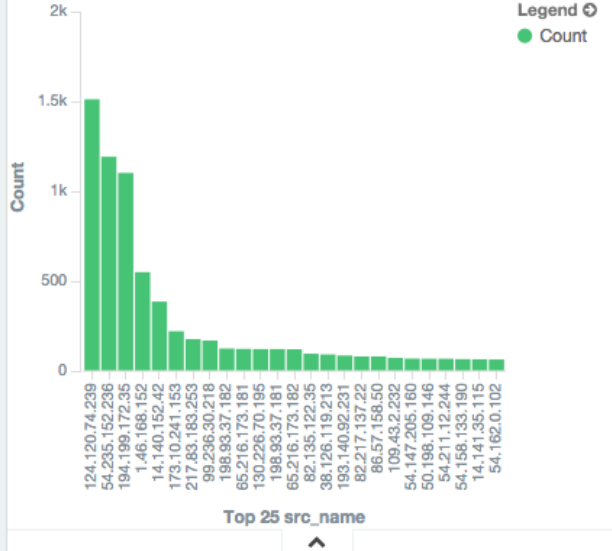

## Bitcoinium Type



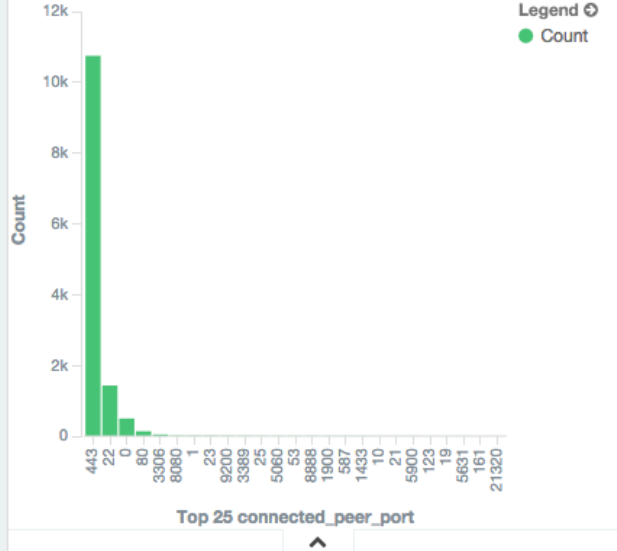

## Bitcoinium DNS Queries




## Bitcoinium Connected Hosts




## Bitcoinium Connected Ports

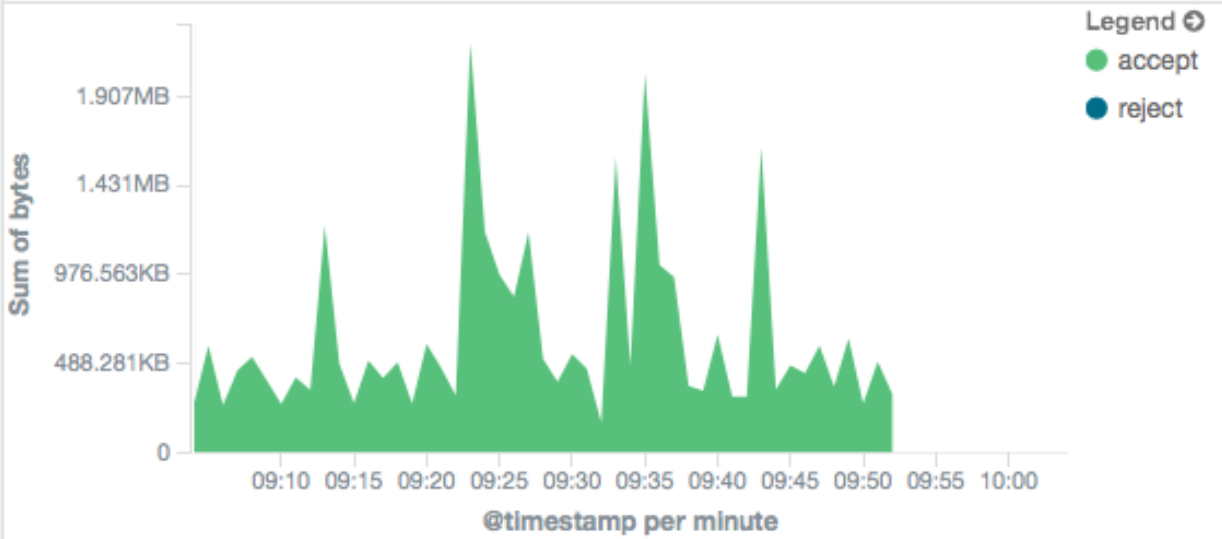


Discover | Visualize | Dashboard | Settings | Last 1 hour

# Dashboard

interface_id: "eni-97415ff0"

## Volume




## Traffic Counters

**30.137MB**
Sum of bytes

**59,673**
Sum of packets

## Top 10 Accepted Sources

| Top 10 srcaddr | Sum of packets | Sum of bytes |
|---|---|---|
| 172.31.39.253 | 25,380 | 22.382MB |
| 54.240.250.209 | 10,220 | 2.829MB |
| 54.240.252.197 | 7,065 | 1.921MB |
| 54.240.248.211 | 5,763 | 1.599MB |
| 172.31.44.254 | 3,958 | 571.024KB |
| 205.251.235.255 | 3,729 | 501.083KB |
| 172.31.3.225 | 1,533 | 93.633KB |
| 205.251.235.148 | 1,510 | 201.068KB |
| 54.240.250.221 | 388 | 63.584KB |
| 208.76.1.123 | 22 | 1.633KB |

Export: Raw Formatted

## Top 10 Rejected Sources

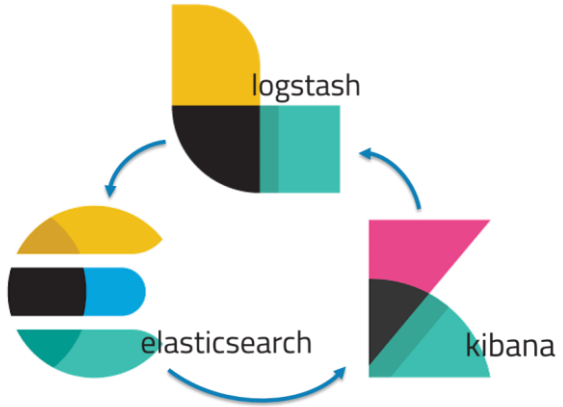
| Top 10 srcaddr | Sum of packets | Sum of bytes |
|---|---|---|
| 186.62.145.215 | 3 | 180B |
| 84.197.197.19 | 3 | 180B |
| 118.171.43.139 | 2 | 120B |
| 109.162.247.248 | 1 | 137B |
| 119.246.224.253 | 1 | 137B |
| 119.98.3.60 | 1 | 87B |
| 131.253.22.37 | 1 | 40B |
| 141.212.122.147 | 1 | 40B |
| 173.254.203.107 | 1 | 40B |
| 180.166.59.86 | 1 | 137B |

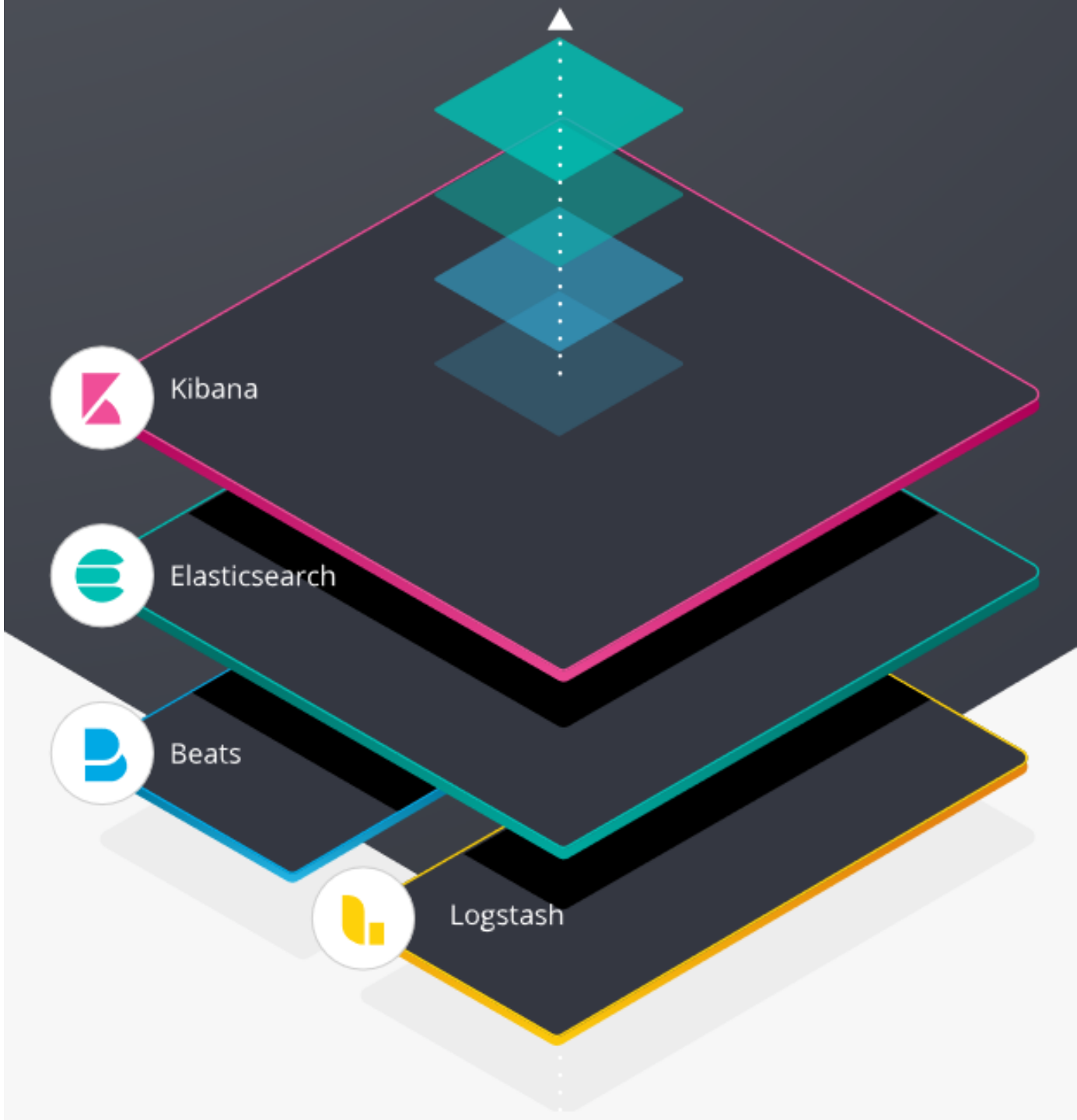
Export: Raw Formatted

https://www.elastic.co/elk-stack

# ELK Stack

- Elastic Stack est la prochaine évolution de l'ELK Stack, mais avec plus de flexibilité pour faire de grandes choses.
  - Intégration avec AWS et AZURE



# III. Sécurité du système

https://www.snort.org/

# SNORT


- Depuis plus d'une génération de professionnels de la sécurité, SNORT est le point de départ de la connaissance des systèmes de détection d'intrusion (IDS).
- Snort peut être configuré en trois modes distincts : renifleur réseau, enregistreur de paquets ou IDS complet. En tant que tel, il peut être au cœur d'un système de sécurité automatisé ou d'un composant qui se trouve à côté d'une gamme de produits commerciaux.
- Maintenant propriété de Cisco, Snort continue d'évoluer et d'être développé par une communauté active.
- Des règles IDS élaborées par la communauté sont disponibles, de même que des règles licenciées sur une base commerciale.

```
root@kali:~# snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.2 IPv6 GRE (Build 78)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 1998-2011 Sourcefire, Inc., et al.
           Using libpcap version 1.3.0
           Using PCRE version: 8.30 2012-02-04
           Using ZLIB version: 1.2.7

Commencing packet processing (pid=3599)
```

https://modsecurity.org/

modsecurity
Open Source Web Application Firewall

# MODSECURITY

- l'extension WAF (pare-feu d'application web open-source) pour Apache et NGINX ModSec vérifie toutes les sessions http/https entrantes sur la base de certaines directives de sécurité.
- fournit un langage de configuration de règles connu sous le nom de'SecRules' pour la surveillance, l'enregistrement et le filtrage en temps réel des communications HTTP basées sur des règles définies par l'utilisateur.
- fournir des protections contre les classes génériques de vulnérabilités à l'aide du jeu de règles de base de ModSecurity (CRS) de l'OWASP : un jeu de règles open-source écrit dans le langage SecRules de ModSecurity. Plusieurs autres ensembles de règles (commerciales) sont également disponibles.
- Le moteur ModSecurity est déployé embarqué dans le serveur web ou en tant que serveur proxy devant une application web. Cela permet au moteur d'analyser les communications HTTP entrantes et sortantes vers le terminal. En fonction de la configuration de la règle, le moteur décidera de la façon dont les communications doivent être gérées, ce qui inclut la possibilité de passer, déposer, rediriger, retourner un code d'état donné, exécuter un script utilisateur, et plus.

# Web Application Firewall

Here you can configure the web application firewall (ModSecurity).

Web application firewall mode

- ○ Off
  Incoming HTTP requests and related responses are not checked.
- ○ Detection only
  Each incoming HTTP request and the related response are checked against a set of rules. If the check succeeds, the HTTP request is passed to web site content. If the check fails, the event is logged, no other actions are performed.
- ◉ On
  Each incoming HTTP request and the related response are checked against a set of rules. If the check succeeds, the HTTP request is passed to web site content. If the check fails, the event is logged, a notification is sent, and the HTTP response is provided with an error code.

## Rule sets

A rule set is a package that contains files with specific security rules. Security rules are checked by the web application firewall engine for each incoming HTTP request.

Rule set

- ◉ Atomic Basic ModSecurity
  A starter version of the Atomic ModSecurity rules. Provides basic web application firewall functionality. Updated on a monthly basis.
- ○ OWASP ModSecurity
  The OWASP rule set is very restrictive and thus might block some functions, such as file sharing, webmail, and some web applications, including WordPress.
- ○ Advanced ModSecurity Rules by Atomicorp (subscription)
  The most complete advanced version of the Atomic ModSecurity rules, with all performance enhancements and new security features. Updated in real time. You need an active subscription to use this rule set.
- ○ Comodo ModSecurity (subscription)
  A web application firewall rule set released by Comodo. You need an active subscription to use this rule set.
- ○ Custom rule set
  Upload a custom web application firewall rule set. Supported formats: zip, tar.gz, tgz, tar.bz2, conf.

☑ Update rule sets  Daily ▾

https://cisofy.com/lynis/


# Lynis

- Lynis est un outil qui fait des listes - des listes des applications et utilitaires qu'il trouve sur les systèmes Unix, des listes des versions de ces systèmes, et des listes des vulnérabilités qu'il trouve dans le code ou les configurations de chacun.
- Avec le code source disponible sur GitHub, Lynis a une communauté de développement active, avec le support principal de Cisofy.
- L'une des capacités spéciales de Lynis est que, grâce à sa fondation Unix, il est capable de scanner et d'évaluer les cartes de développement IoT les plus populaires, dont Raspberry Pi.

```
[root@tecmint opt]# lynis audit system

[ Lynis 2.6.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           2.6.6
  Operating system:          Linux
  Operating system name:     CentOS
  Operating system version:  CentOS Linux release 7.4.1708 (Core)
  Kernel version:            4.17.6
  Hardware platform:         x86_64
  Hostname:                  tecmint
  ---------------------------------------------------
  Profiles:                  /usr/local/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/local/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]
```

https://certbot.eff.org/

# Certbot


- Le chiffrement est essentiel pour de nombreuses normes de sécurité, dont la nouvelle préférée de tous, RGPD. La mise en œuvre du chiffrement peut être compliquée et coûteuse, mais l'EFF a essayé d'en faire moins avec des outils comme Certbot, un client automatique open source qui récupère et déploie les certificats SSL/TLS pour votre serveur web.
- Certbot a commencé comme un frontal pour Let's Encrypt, mais il est devenu un client pour toutes les AC qui prennent en charge le protocole ACME.
- Le projet Certbot s'inscrit dans le cadre des efforts de l'EFF visant à "chiffrer l'Internet", un objectif qui a été adopté par de nombreux défenseurs de la vie privée et organismes gouvernementaux de réglementation. Assurer la sécurité de vos employés, partenaires et clients est à la fois un objectif valable et une responsabilité légale ; les outils open source peuvent vous aider à faire des pas dans cette direction.

https://www.veracrypt.fr/en/Home.html

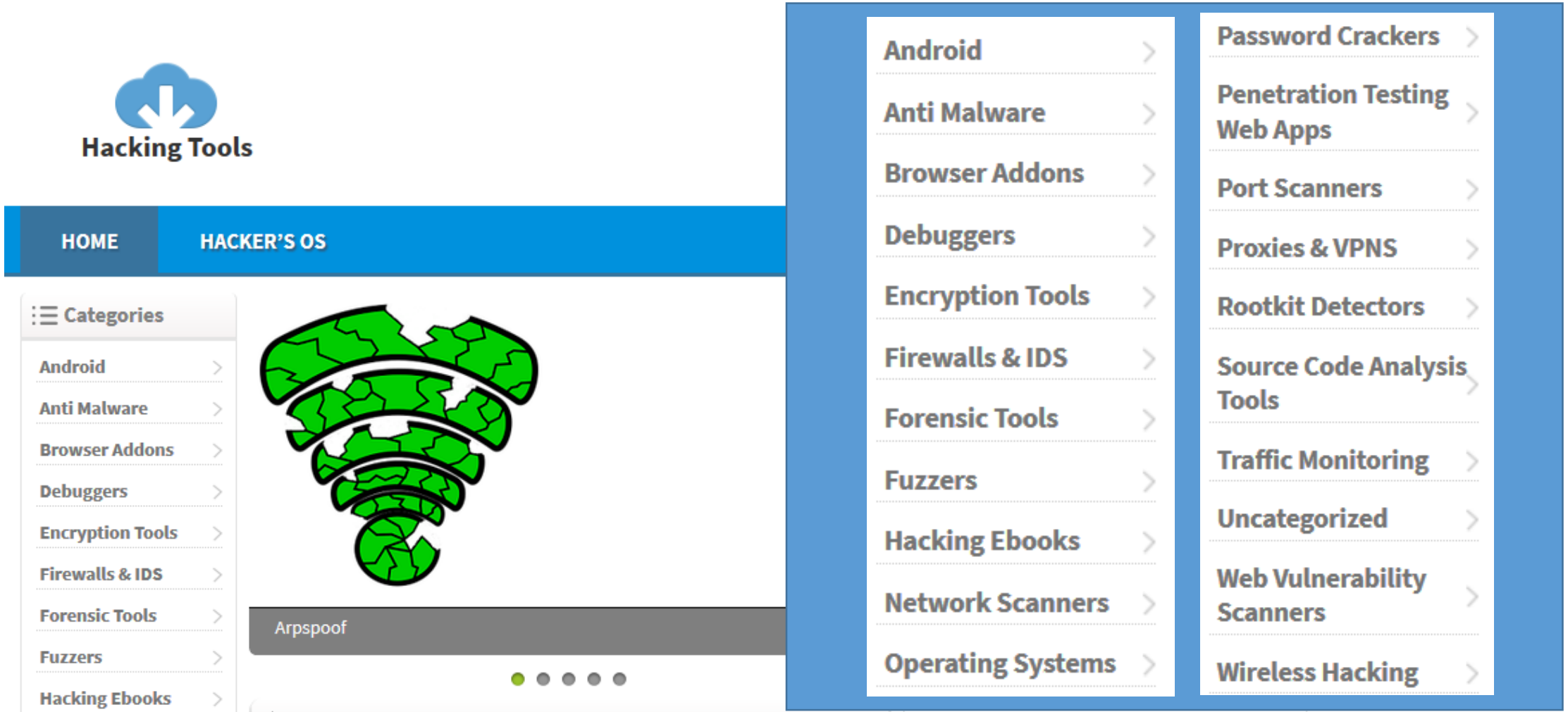
# VeraCrypt


- utilitaire de chiffrement de disque open source utilisé pour le chiffrement à la volée (OTFE).
- initialement sorti en juin 2013 et a produit sa dernière version (version 1.23) en septembre 2018.
- créer un disque virtuel crypté dans un fichier ou crypter une partition ou (sous Windows) l'ensemble du périphérique de stockage avec authentification au démarrage.
- inclut des implémentations optimisées de fonctions de hachage et de chiffrement cryptographiques qui améliorent les performances des processeurs modernes.
- supporte la négation plausible en permettant la création d'un seul "volume caché" à l'intérieur d'un autre volume. Les versions Windows de VeraCrypt ont la capacité de créer et d'exécuter un système d'exploitation crypté caché dont l'existence peut être refusée. La documentation de VeraCrypt énumère de nombreuses façons dont les fonctionnalités de déni de volume caché de VeraCrypt peuvent être compromises (par exemple par des logiciels tiers qui peuvent divulguer des informations par le biais de fichiers temporaires, de vignettes, sur des disques non cryptés) et les moyens possibles pour éviter cela.


"That's all Folks!"

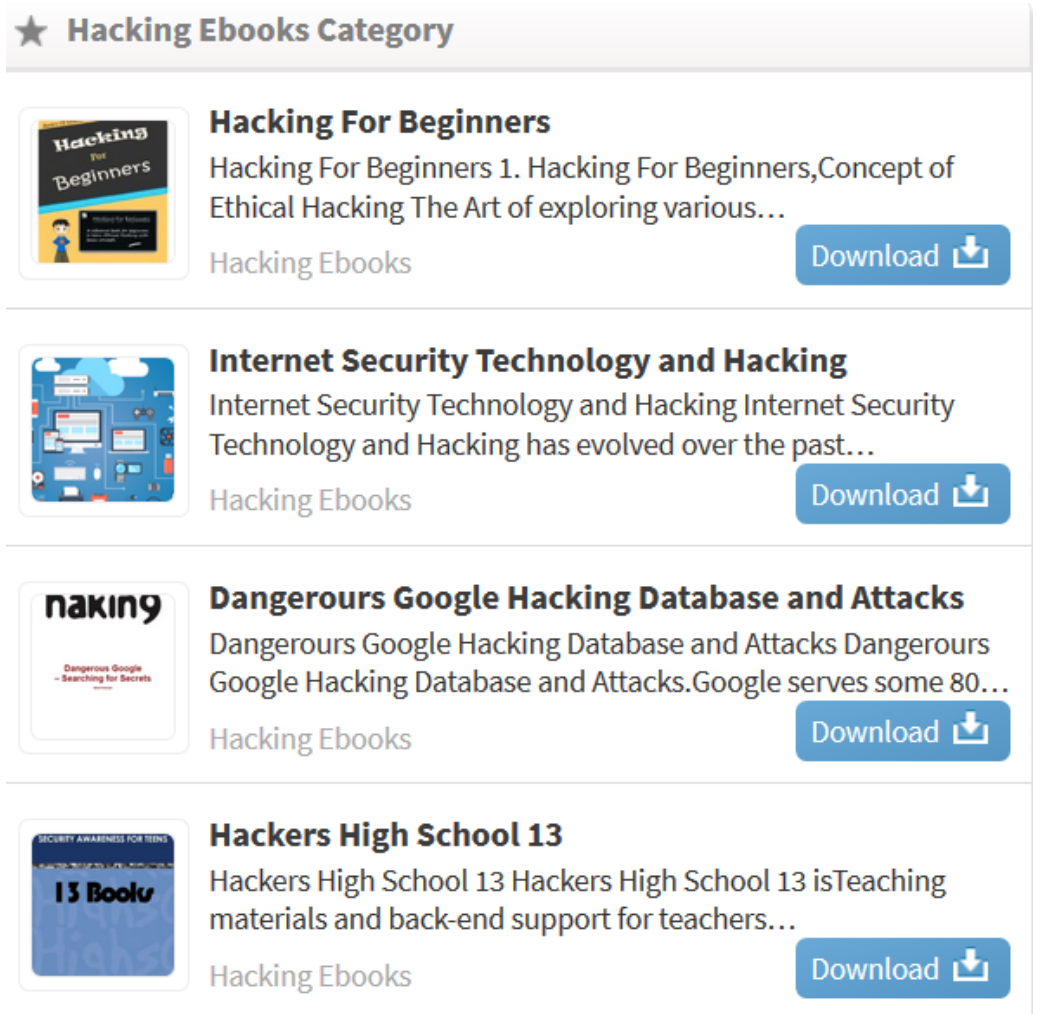
# Vous voulez en savoir plus sur les outils de sécurité open source ?

http://www.hackingtools.in/



# Vous voulez en savoir plus sur les outils de sécurité open source ?

http://www.hackingtools.in/



# Vous voulez en savoir plus sur les dernières nouveautés en matière de sécurité ?

**https://isc.sans.edu/podcast.html**

## Coordonnées de contact

Mr. Marc Vael

CISO

**Esko**

Kortrijksesteenweg 1095

9051 Gand

Belgique

**www.esko.com**

**marc@vael.net**

**http://www.linkedin.com/in/marcvael**

**@marcvael**