



# A decade of infosec tools from where we were to what we need now

May 2019, 9th

**Thomas DEBIZE** 

Who am I ? Well just another infosec passionate



01	A bit of context
02	Tools during the last decade
03	Make your tool great (again)
04	Wrapping it up

01	A bit of context
02	Tools during the last decade
03	Make your tool great (again)
04	Wrapping it up

#### The infosec field has quite evolved during the last decade, especially around tool crafting

Some **old sweet dreams** now come true

- Scan the entire IPv4 space in few minutes/hours/days
- Query all OSINT information you want
- Pwn large Windows corporate infrastructures
- **Fuzz** anything you want

• **Storing** entire earth's hashes and passwords

#### Coding became **social**

- Infosec people enhanced their coding skill
- Infosec people now with the will to write good and practical tools
- Some exhibitions **devoted** to the tool crafting art (Black Hat Arsenal)
- More security folks are writing more and more good quality and reliable tools

More tools allowing **attack AND defense** 

- More **recognition** for the Blue side
- Moving from the "breaking" era, to the "securing and building" era
- Finally taking advantage of **data visualization** (graphs etc.)

#### But in the same time we still rely on some old school core tools

Author : Fyodor ---[ Phrack Magazine Volume 7, Issue 51 September 01, 1997, article 11 of 17 ----- The Art of Port Scanning -----[ Fyodor <fyodor@dhp.com> [ Abstract ] This paper details many of the techniques used to determine what ports (or similar protocol abstraction) of a host are listening for connections. These ports represent potential communication channels. Mapping their existence facilitates the exchange of information with the host, and thus it is quite useful for anyone wishing to explore their networked environment, including hackers. Despite what you have heard from the media, the Internet is NOT all about TCP port 80. Anyone who relies exclusively on the WWW for information gathering is likely to gain the same level of proficiency as your average AOLer, who does the same. This paper is also meant to serve as an introduction to and ancillary documentation for a coding project I have been working on. It is a full featured, robust port scanner which (I hope) solves some of the problems I have encountered when dealing with other scanners and when working to scan massive networks. The tool, nmap, supports the following: vanilla TCP connect() scanning, - TCP SYN (half open) scanning, - TCP FIN (stealth) scanning, TCP ftp proxy (bounce attack) scanning - SYN/FIN scanning using IP fragments (bypasses packet filters), UDP recvfrom() scanning, - UDP raw ICMP port unreachable scanning, - ICMP scanning (ping-sweep), and reverse-ident scanning. The freely distributable source code is appended to this paper.



#### THC Releases

Welcome to the THC release section. Below you will find the collection of THC software applications. It includes sophisticated network analysis and penetration test tools, cryptographic utilities that mimic fingerprint collisions or extrapolate credit card numbers and a lot of other interesting stuff for the security expert's pleasure.

#### THC-Hydra

Version: 4.1

Date: 2004-05-22

OS: Unix Size: 168kb

Project website: /thc-hydra

THC-Hydra - the best parallized login hacker is available: for Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more. Includes SSL support and is part of Nessus. VISIT THE PROJECT WEB SITE TO DOWNLOAD WIN32, PALM and ARM BINARIES! Changes: A very nice GTK2 GUI was added (thanks to snakebyte) and a few bugfixes.

#### 2003 Top 75 Tools Results

From: Fyodor <fyodor () insecure org> Date: Sun, 4 May 2003 00:33:30 -0700

Hello everyone,

Thanks for the fantastic response to the Nmap user survey! It is now closed, but recorded 1854 responses -- that blew away our goal of 1500 and is over 50% greater than the 2000 survey! I haven't analyzed all the questions/comments yet, but I did go through your recommended tools and create a most-loved list as I did in 2000. Thanks to the increased responses. I was able to expand the list from "Top 50" to

It is worth noting that almost half of the 2003 top 50 are new to the list. Congratulations to these rising stars:

GFI LANguard: A commercial network security scanner for Windows Ettercap: In case you still thought switched LANs provide much extra security Nikto: A more comprehensive web scanner Kismet: A powerful wireless sniffer SuperScan: Foundstone's Windows TCP port scanner Fport: Foundstone's enhanced netstat Network Stumbler: Free Windows 802.11 Sniffer N-Stealth: Web server scanner AirSnort: 802.11 WEP Encryption Cracking Tool NBTScan: Gathers NetBIOS info from Windows networks Cain & Abel: The poor man's LOphtcrack XProbe2: Active OS fingerprinting tool SolarWinds Toolsets: A plethora of network discovery/monitoring/attack tools THC-Amap: An application fingerprinting scanner OpenSSL: The premier SSL/TLS encryption library Honeyd: Your own personal honeynet Achilles: A Windows web attack proxy Brutus: A network brute-force authentication cracker Stunnel: A general-purpose SSL cryptographic wrapper Paketto Keiretsu: Extreme TCP/IP SPIKE Proxy: HTTP Hacking THC-Hydra: Parallized network authentication cracker

The questions giving birth to this study

In this myriad of newly-created tools during that decade

- > How are these new tools **built** ?
- > Where are they **hosted**?
- > How **long** are they maintained ?
- > Are they **really better made** than the old ones ?

All in all, how did it **evolve** ?

01	A bit of context
02	Tools during the last decade
03	Make your tool great (again)
04	Wrapping it up

### Study scope and limitations

#### What did I do?

• Analyze metadata from **4 major publication sources** of infosec tools



#### How?

- With **Dataiku Data Science Studio** free edition, an amazing all-in-one tool. Mostly Excel on steroids.
- You should try it <u>https://www.dataiku.com/learn/portals/tutorials.html</u>

#### How many records have been analyzed ? On which period ?

Packetstorm	Toolswatch	Kitploit	n0where
6775 records	1620 records	2934 records	1052 records
From 01/1994 to 03/2019	From 12/2010 to 11/2018	From 12/2010 to 03/2019	From 06/2010 to 03/2019

## Slight off-topic greetings for vulners.com

vulners.com indexes a lot of cool sources and provides a freeAPI to get structured data

- Blogs
- Vulnerability feeds
- IOC feeds
- Exploit feeds
- Vendors
- General news websites
- • • •

Thanks to them !



Archive	2
GET	/archive/collection/ Get entire collection of bulletins in ZIP
GET	/archive/getsploit/ Get whole exploit database in ZIP
GET	/archive/distributive/ Get affected packages for specificied OS in ZI
GET	/archive/nasl/ Get NASL scripts in ZIP

First, the source dataset, also known as "the base of all biases"

### Distribution of records per source since 1994



Irrelevant dataset as solely Packetstorm was existing before 2010 ©

### Distribution of records per source since 2010



Relevant dataset as all sources have quite the same order of magnitude for publications since 2010

Then, some evolution figures

## Evolution of the number of publications (per quarter) since 2010



#### More and more publications

### Evolution of the **number of publications** per source since 2010



- Less and less publications from toolswatch on their website
- Packetstorm, the old school reference, used to maintain its rhythm of publications, but now tends to diminish it, while Kitploit the "decade newcomer" tends to become the new reference source

### Distribution of tool hosting platforms (to date)



#### Evolution of **Github, Sourceforge, Google Code and Bitbucket popularity** for infosec tools between 2010 and 2019



2010-Q1 2010-Q2 2010-Q3 2010-Q4 2011-Q1 2011-Q2 2011-Q3 2011-Q4 2012-Q1 2012-Q2 2012-Q3 2012-Q4 2013-Q1 2013-Q2 2013-Q3 2013-Q4 2014-Q1 2014-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2014-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2014-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2015-Q1 2015-Q2 2016-Q3 2016-Q4 2017-Q1 2017-Q2 2017-Q3 2017-Q4 2018-Q2 2018-Q3 2018-Q4 2019-Q1 2015-Q2 2015-Q3 2015-Q4 2015-Q1 2015-Q1 2015-Q2 2015-Q3 2015-Q4 2015-Q1 2015-Q1 2015-Q1 2015-Q2 2015-Q3 2015-Q4 2015-Q1 2015-Q2 2015-Q3 2015-Q4 2015-Q1 2015-Q1

#### Evolution of the **number of publications pointing to a Github repository** per source between 2010 and 2019



• **Packetstorm** is not following the trend, hence continuing to bring diversity for tool sources

Ok whatever, so if everything seems to be hosted on Github, let's focus on Github !

#### Some statistics about for the 2000+ Github repositories analyzed

Stars	Forks	Watchers	Releases	
Average: 1024 Median: 282	Average: 182 Median: 70	Average: 1024 Median: 282	Average: 4 Median: 0	
<b>Std Dev:</b> 2834	<b>Std Dev:</b> 424	<b>Std Dev:</b> 2834 (1 star induces 1 watch)	<b>Std Dev:</b> 15	
Size	Commits	Mainten	ance duration	
Average: 15 MB	Average: 516	in days, last comn	nit – first commit on mas	ster
Median: 951 KB	Median: 72	Avera	ge: 882 (2,4 years)	
Std Dev: 59 MB	<b>Std Dev:</b> 1908	<b>Median:</b> 603 (1,6 years)		
		Std Do	ev: 943 (2,5 years)	
AII	Open	All Pull	<b>Open Pull</b>	
Issues	issues	Requests	Requests	
Average: 226	Average: 24	Average: 66	Average: 2	
Median: 15	Median: 3	Median: 4	Median: 0	
Std Dev: 2138	Std Dev: 89	<b>Std Dev:</b> 370	Std Dev: 9	23

### Top 20 of the **most starred** infosec tools on Github

/nvbn/thefuck -				4	3.28k
/skylot/jadx –	18.35k	18.35k			
/danielmiessler/SecLists –	17.89k			_	
/jlund/streisand –	17.67k				
/rapid7/metasploit-framework –	16.18k				
/pi-hole/pi-hole -	15.02k				
/NationalSecurityAgency/ghidra –	14.91k				
/mitmproxy/mitmproxy -	14.84k				
/koalaman/shellcheck	14.4k				
/facebook/osquery -	14.08k				
/sqlmapproject/sqlmap –	14k				
/HelloZeroNet/ZeroNet -	13.68k				
/trailofbits/algo –	13.05k				
/fish-shell/fish-shell -	12.81k				
/StevenBlack/hosts -	12.39k				
/jesseduffield/lazygit –	12.06k				
/radare/radare2	10.1k	-			
/Konloch/bytecode-viewer –	10.05k				
/robertdavidgraham/masscan –	9,716				
/hwdsl2/setup-ipsec-vpn –	9,470				

### Top 20 of the **most forked** infosec tools on Github



## Top 20 of infosec tools on Github with the **biggest number of open issues**

/MISP/MISP -			:	1,336.0	
/packetbeat/packetbeat -			1	,330.0	
/radare/radare2 -			1,196.0		
/DynamoRIO/dynamorio –			1,150.0		
/andresriancho/w3af-		1,002.0			
/globaleaks/GlobaLeaks –	774				
/rapid7/metasploit-framework –	675				
/dnschneid/crouton-	672				
/cuckoobox/cuckoo -	663				
/zaproxy/zaproxy-	643				
/wazuh/wazuh	585				
/HelloZeroNet/ZeroNet -	569				
/rbei-etas/busmaster -	567				
/facebook/osquery -	544				
/firehol/netdata -	541				
/nmap/nmap –	531				
/capitalone/cloud-custodian-	491				
/fish-shell/fish-shell –	473				
/freedomofpress/securedrop -	465				
/koalaman/shellcheck –	398				
_					

## Top 20 of infosec tools on Github with the **biggest number of open pull requests**



## Top 20 of infosec tools on Github with the **longest maintenance period**

-		
/sleinen/samplicator-	7,107	
/mrash/psad -	6,444	
/hknutzen/Netspoc -	6,327	
/appneta/tcpreplay -	6,212	
/firehol/firehol -	6,023	
/Ettercap/ettercap -	5,894	
/royhills/ike-scan -	5,839	
/CoreSecurity/impacket -	5,680	
/troglobit/nemesis -	5,654	
/urwid/urwid -	5,293	
/nmap/nmap -	5,122	
/fish-shell/fish-shell -	4,968	
/ossec/ossec-hids -	4,958	
/kernelslacker/trinity-	4,706	
/aircrack-ng/aircrack-ng-	4,519	
/samhocevar/zzuf -	4,439	
/DNS-OARC/dnscap -	4,310	
/knipknap/exscript -	4,289	
/uxmal/reko –	4,253	
/EnableSecurity/sipvicious -	4,176	Avera
_		

## Top 20 of the **most frequent programming languages** in infosec tools



Ok whatever, so if infosec tools are mostly developed in Python, let's focus on Python !

## Top 20 of infosec tools in Python having the **biggest number of dependencies**

/linkedin/qark -		91	
/famavott/osint-scraper -		82	
/archerysec/archerysec -		81	
/yeti-platform/yeti -		74	
/Netflix/Stethoscope -	66		
/mozilla/MozDef-	65		
/airbnb/binaryalert -	61		
/dunbarcyber/cyphon -	57		
/log2timeline/plaso –	52		
/DefectDojo/django-DefectDojo -	49		
/Patrowl/PatrowlManager -	49		
/aliasrobotics/aztarna -	48		
/blabla1337/skf-flask –	42		
/ex0dus-0x/D0xk1t-	41		
/tomchop/malcom-	41		
/idanr1986/cuckoodroid-2.0 -	39		
/Den1al/JSShell -	38		
/sdnewhop/sdwan-harvester-	38		
/target/strelka –	36		
/Netflix/repokid -	35		

## Top 20 of the most used Python 3<sup>rd</sup>-party modules in infosec tools



### Distribution of Python crypto module choice for infosec tools



#### So you do want to access the data ?



### Code, details, and output datasets of the study are available on Github

https://github.com/maaaaz/adecadeofinfosectools

04	Wrapping it up
03	Make your tool great (again)
02	Tools during the last decade
01	A bit of context

#### Golden rules for modern tools (from my personal experience)

Use a standard argument	Package it and make it easily installable	Support NTLM authentication	
arguments		Sunnort Kerheros	
Build it with modularity to ease	Provide prebuilt binaries or containers	authentication	
Use asynchronous execution	defenders)	Support HTTP proxy traversal	
(IO bounded $\rightarrow$ multithreading CPU bounded $\rightarrow$ multiprocessing)	Encrypt traffic	Support SOCKS proxification	
Maka it ucabla warldwida			
UTF-8 ! UTF8 ! UTF-8 !		Allow single and bulk input	
Provide multiple verbosity levels	Provide easy-to-parse output CSV / JSON	Use non vulnerable dependencies	

[INSERT A CONCLUSION HERE]

## Good tools work, Better tools scale, Great tools last

## **Questions ?**

#### **Thomas DEBIZE**

- > tdebize@mail.com > https://github.com/maaaaz