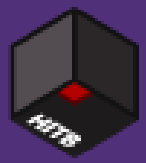
WAVESTONE




HITBSecConf

# Modern pentest tricks for faster, wider, greater engagements

HITB Amsterdam 2018 – CommSec Track – April, 12th

Thomas DEBIZE
thomas.debize@wavestone.com

# Who am I ? Basically an infosec auditor and incident responder

**Thomas DEBIZE**

- Guitar, riding, volley-ball
- Git pushing infosec tools
  - https://github.com/maaaaz

/ **01** What changed and why do you need to adapt?

/ **02** Modern tricks for modern pentesters

/ **03** Taking a step back

/ **01** What changed and why do you need to adapt?

/ **02** Modern tricks for modern pentesters

/ **03** Taking a step back

# What changed in the pentest domain during that decade ?

**In 2018, it is now easily possible to**

## Scan the entire IPv4 space in few minutes/hours/days

With **distributed (vulnerable) computing**

- Census 2012 http://census2012.sourceforge.net/paper.html

With **asynchronous programming**

- ZMap
- Masscan
- Unicornscan

With **third-party platforms** doing it **for you**, sometimes for **free**

- Shodan
- ZoomEye
- Scans.io
- Censys.io

## Query all OSINT information you want

**Offline**, by building your own platform

- "Modern Internet Scale Reconnaissance" https://github.com/hdm/2017-BSidesLV-Modern-Recon

**Online**, by querying a lot of cool services

- Recon-ng
- DomainTools
- Pastebin
- Certificate Transparency
- …

## Pwn large Windows corporate infrastructures

Starting with **reconnaissance**

- of assets: PowerView
- of admins: BloodHound

Then through **exploitation**

- CrackMapExec
- Responder

And just after, **post-exploitation**

- Mimikatz
- Invoke-Mimikatz
- Empire

Or…just **automate everything** in one tool

- Deathstar https://github.com/byt3bl33d3r/DeathStar

# Why do you need to adapt your techniques ?

Because more and more **security folks** are **writing** more and more **tools**

Because more and more **security folks** are writing more and more **good quality and reliable tools**

Because you will be asked to **faster cover wider scopes**

Because it has **already changed**
Current penetration testing assessments now require pentesters to…

S — C — A — L — E

/ 01 What changed and why do you need to adapt ?

/ 02 Modern tricks for modern pentesters

/ 03 Taking a step back

# 1. CSV for data analysis and processing, CSV, always CSV

**Pentesting involves a lot of iterative work**

`start:`

/ 1. Scan some **targets**

/ 2. **Exploit** them

/ 3. Harvest **new data on them** such credentials, IPs etc.

/ Use the **new found data** on new and old targets

`goto start`

➔ Being able to **quickly process** new data is crucial to scale

➔ Choosing a **good data format** is really important


From experience, **CSV** is the best format to use as:

/ It is a **common format** in programming languages

› Although Python 2 "`csv`" module does not support utf-8… (use `unicodecsv` instead)

/ It is a **human-readable** format

It's a **rather simple** format but there is **no standard** and common pitfalls are:

/ **Encoding**: please **use utf-8**

/ **Quoting and escaping**: please choose to have **all fields quoted** to prevent any unwanted stuff

Hah, and **one last thing:**

Beware of **CSV injection !** ☺
(http://georgemauer.net/2017/10/07/csv-injection.html)

```
UserId,BillToDate,ProjectName,Description,DurationMinutes
1,2017-07-25,Test Project,Flipped the jibbet,60
2,2017-07-25,Important Client,"Bop, dop, and giglip", 240
2,2017-07-25,Important Client,"=2+5+cmd|' /C calc'!A0", 240
```

In short, stick to the CSV format for **inputs and outputs**

# 1. CSV for data analysis and processing, CSV, always CSV

## Examples of common pentest / infosec tools offering CSV output

**nmaptocsv**

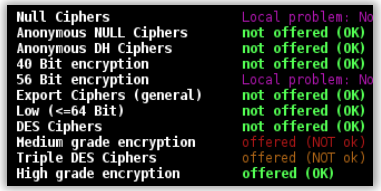
A simple script to convert Nmap output to CSV

https://github.com/maaaaz/nmaptocsv


**Wfuzz**

Web application fuzzer (URL enumeration etc.)

http://wfuzz.readthedocs.io/en/latest/




**testssl.sh**

SSL/TLS protocols and algorithms tester

https://testssl.sh/


**BloodHound**

Windows domain compromise path finder

https://github.com/BloodHoundAD/BloodHound


**Ophcrack**

Windows password cracker

http://ophcrack.sourceforge.net/

**Recon-ng**

OSINT reconnaissance framework

https://bitbucket.org/LaNMaSteR53/recon-ng

**Nikto**

Webserver scanner and fuzzer

https://cirt.net/Nikto2


**Nessus**

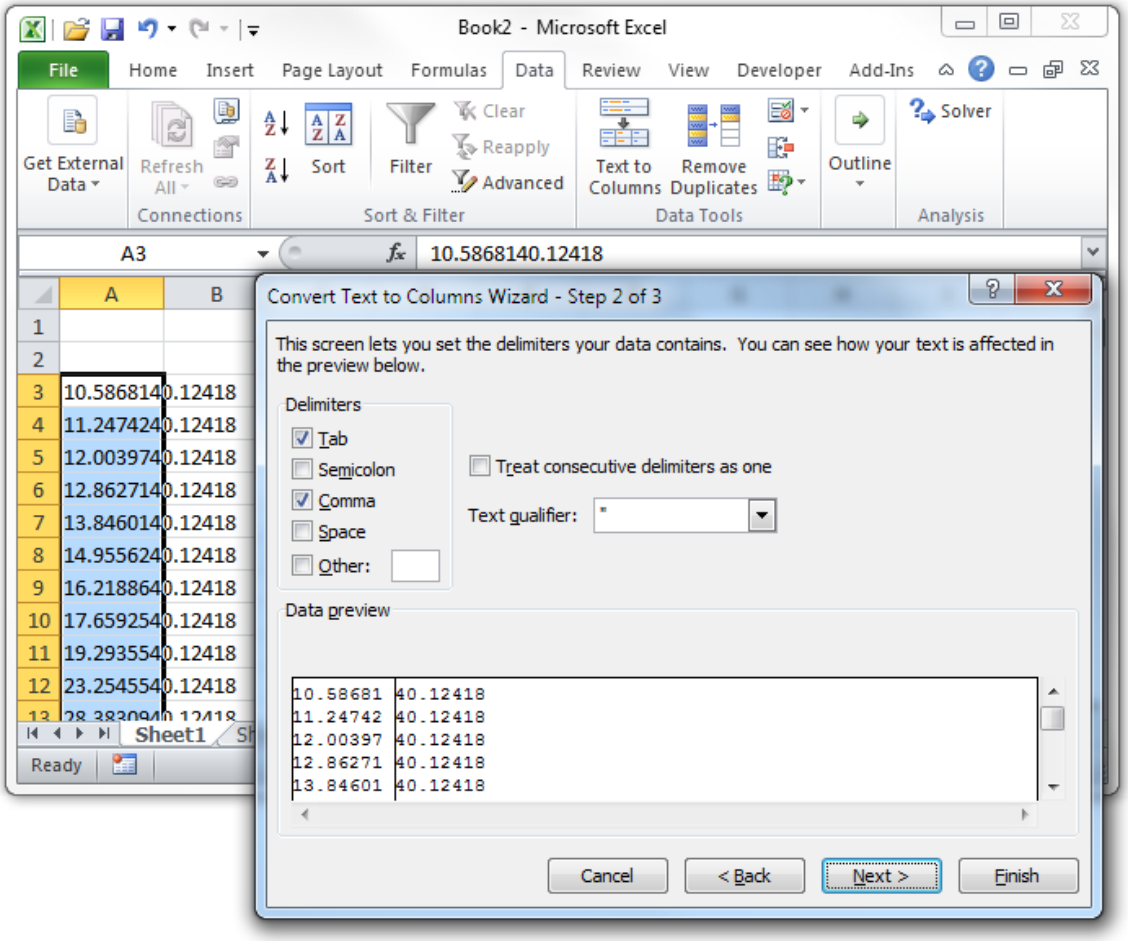
Infrastructure vulnerability scanner

https://www.tenable.com

# 1. CSV for data analysis and processing, CSV, always CSV

## 3 tool suites to handle CSV

### a) **Microsoft Excel,** with **"Text to Columns"** and then **"Filter"** functions




https://stackoverflow.com/questions/22905814/mid-function-for-microsoft-excel-to-obtain-column-txt-file

**Excel max number of line is 1 million: THIS IS a commonly encountered issue**

# 1. CSV for data analysis and processing, CSV, always CSV

## 3 tool suites to handle CSV

### b) csvkit / free and open-source / https://csvkit.readthedocs.io/

"csvkit is a suite of command-line tools for converting to and working with CSV, the king of tabular file formats."

/ **Input**

- `in2csv, sql2csv:` convert anything to csv
- **`csvclean, csvformat:` ensure your input or output files is correctly formatted**

/ **Processing**

- `csvcut:` just like UNIX "cut"
- `csvgrep:` not just like UNIX "grep", allows to search regex/patterns only in desired columns
- **`csvjoin:` execute a SQL-like join to merge CSV files on a specified column or columns**
- `csvsort:` not just like UNIX "grep", allows to sort desired fields
- `csvstack:` concatenate/merge multiple csv files

/ **Output and Analysis**

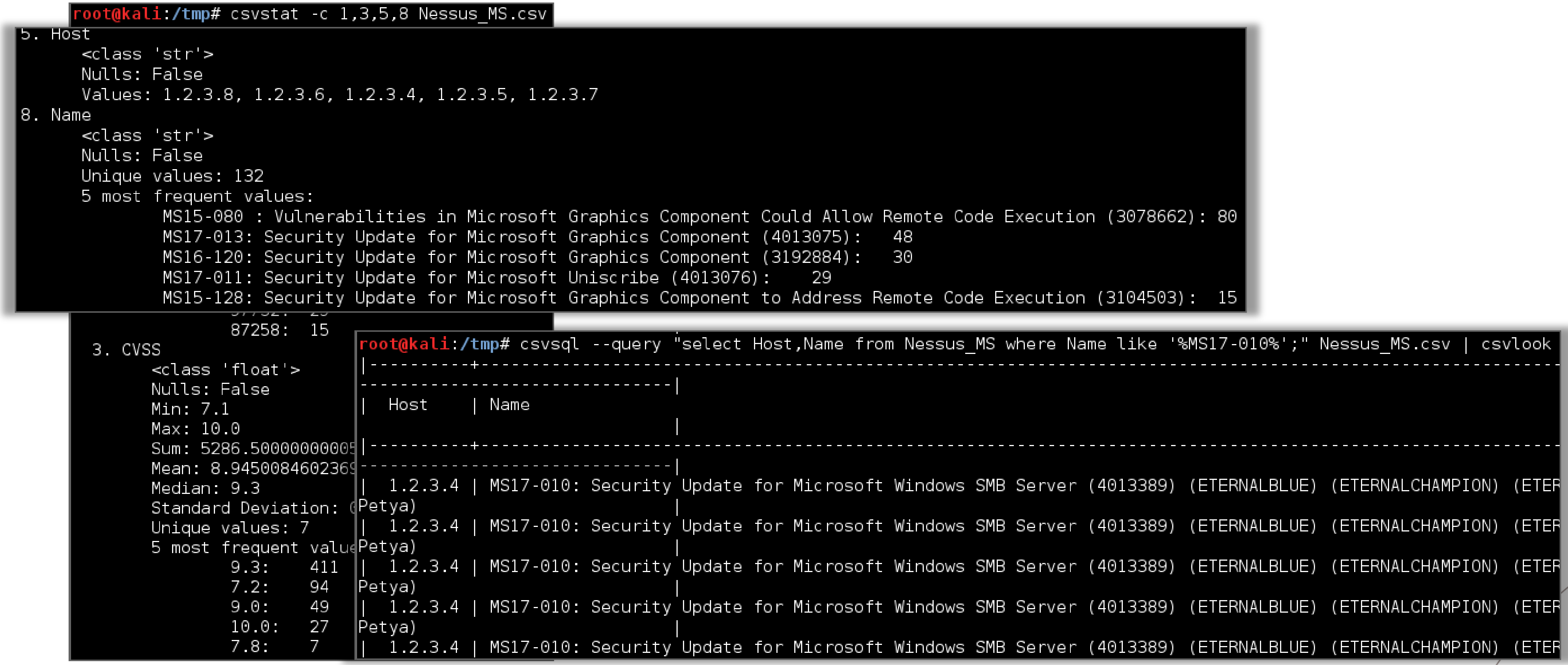
- `csvjson:` convert a CSV file into JSON
- `csvlook:` just admire the beauty of a CSV file in your interpreter
- `csvpy:` load a CSV file into a CSVKitReader object and then drops into a Python shell
- **`csvsql:` perform SQL queries on a CSV file**
- **`csvstat:` print some statistics per columns**

# 1. CSV for data analysis and processing, CSV, always CSV

## 3 tool suites to handle CSV

**b) csvkit** / free and open-source / https://csvkit.readthedocs.io/

## Demo time



```
root@kali:/tmp# csvstat -c 1,3,5,8 Nessus_MS.csv
```

```
5. Host
        <class 'str'>
        Nulls: False
        Values: 1.2.3.8, 1.2.3.6, 1.2.3.4, 1.2.3.5, 1.2.3.7
8. Name
        <class 'str'>
        Nulls: False
        Unique values: 132
        5 most frequent values:
                MS15-080 : Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662): 80
                MS17-013: Security Update for Microsoft Graphics Component (4013075):   48
                MS16-120: Security Update for Microsoft Graphics Component (3192884):   30
                MS17-011: Security Update for Microsoft Uniscribe (4013076):    29
                MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503):  15
```

```
                87258:  15
  3. CVSS
        <class 'float'>
        Nulls: False
        Min: 7.1
        Max: 10.0
        Sum: 5286.50000000005
        Mean: 8.945008460236
        Median: 9.3
        Standard Deviation:
        Unique values: 7
        5 most frequent value
                9.3:    411
                7.2:    94
                9.0:    49
                10.0:   27
                7.8:    7
```

```
root@kali:/tmp# csvsql --query "select Host,Name from Nessus_MS where Name like '%MS17-010%';" Nessus_MS.csv | csvlook
|----------+-----------------------------------------------------------------------------------------------------
-------------------------------|
|  Host    | Name
                               |
|----------+-----------------------------------------------------------------------------------------------------
-------------------------------|
|  1.2.3.4 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETER
Petya)                         |
|  1.2.3.4 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETER
Petya)                         |
|  1.2.3.4 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETER
Petya)                         |
|  1.2.3.4 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETER
Petya)                         |
|  1.2.3.4 | MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETER
```

# 1. CSV for data analysis and processing, CSV, always CSV

## 3 tool suites to handle CSV

### c) Dataiku Data Science Studio (DSS) / Free edition / Enterprise / https://www.dataiku.com/dss/trynow/

Dataiku DSS is a **data science** tool that allows to perform the **same kind of processing than Excel but without size limitation**

- I find it **very intuitive, user-friendly** and efficient
  - **4 hours** on a 4 cores + 16 GB RAM machine to join the **"hash" column a 30 GB uncompressed DB** dump with a **4 GB "hash : cleartext" file**

- Some **cool tutorials** on their site to comprehend the concepts (datasets, recipes etc.)
  - https://www.dataiku.com/learn/guide/tutorials/basics.html

**Demo time**

# 1. CSV for data analysis and processing, CSV, always CSV

## 3 tool suites to handle CSV

### c) Dataiku Data Science Studio (DSS) / Free edition / Enterprise / https://www.dataiku.com/dss/trynow/

Modern pentest tricks | DATASETS

Nessus_MS_large

Summary | Explore | Charts | Status | History | Settings | LAB | ACTIONS

Viewing dataset sample  Configure sample

4950 rows, 13 cols

DISPLAY

Name (1 value)

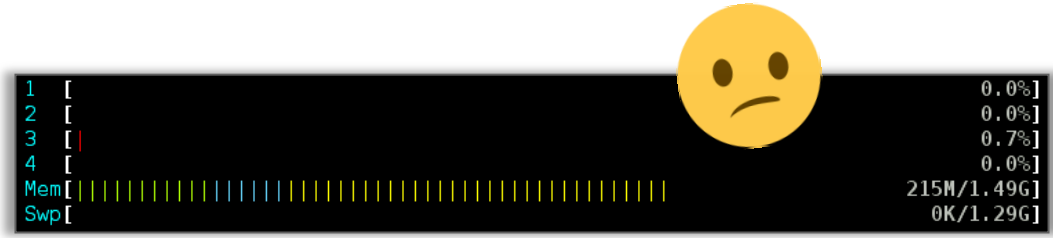
66 matching rows

| Plugin ID | CVE | CVSS | Risk | Host | Protocol | Port | Name | Synopsis | Description |
|---|---|---|---|---|---|---|---|---|---|
| string Integer | string Date (unparsed) | string Decimal | string Text | string IP address | string Text | string Integer | string Text | string Natural lang. | string Natural lang. |
| 97833 | CVE-2017-0143 | 10.0 | Critical | 10.34.253.17 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by th |
| 97833 | CVE-2017-0144 | 10.0 | Critical | 10.34.253.17 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by th |
| 97833 | CVE-2017-0145 | 10.0 | Critical | 10.34.253.17 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by th |
| 97833 | CVE-2017-0146 | 10.0 | Critical | 10.34.253.17 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by th |
| 97833 | CVE-2017-0147 | 10.0 | Critical | 10.34.253.17 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by th |
| 97833 | CVE-2017-0148 | 10.0 | Critical | 10.34.253.17 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by th |
| 97833 | CVE-2017-0143 | 10.0 | Critical | 10.68.187.16 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0144 | 10.0 | Critical | 10.68.187.16 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0145 | 10.0 | Critical | 10.68.187.16 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0146 | 10.0 | Critical | 10.68.187.16 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0147 | 10.0 | Critical | 10.68.187.16 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0148 | 10.0 | Critical | 10.68.187.16 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0143 | 10.0 | Critical | 10.2.30.52 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0144 | 10.0 | Critical | 10.2.30.52 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0145 | 10.0 | Critical | 10.2.30.52 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0146 | 10.0 | Critical | 10.2.30.52 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0147 | 10.0 | Critical | 10.2.30.52 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0148 | 10.0 | Critical | 10.2.30.52 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0143 | 10.0 | Critical | 10.93.183.123 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |
| 97833 | CVE-2017-0144 | 10.0 | Critical | 10.93.183.123 | tcp | 445 | MS17-010: Security Update for Microsoft Windows SMB... | The remote Windows host is affected by multiple v... | The remote Windows host is affected by the |

# 2. Parallel execution

**Pentesting involves a lot of parallel work**

- Extracting the results of a tool output on multiple targets
- Launching the same bruteforce on multiple targets
- …




➔ Being able to **launch simultaneous actions** is crucial to be able to scale on **wide scopes**

**GNU Parallel** is a Perl script to parallelize **any command** in order to maximize your I/O and CPU usage

- It's a drop-in replacement of `GNU xargs`, and is mostly an xargs **"on steroids"**
- **A *lot more* option than** `GNU xargs` but the ones you will love are:
  - `--progress:` a percentage of done/to be done
  - `--bar:` a nice progress bar
  - `--joblog:` a log of executed tasks, allow resuming
  - `--resume:` resume to your current execution status

GNUparallel

In short, use **as much** GNU Parallel **as you can**

# 2. Parallel execution

**Example of a parallel processing involving multiple tools for URL discovery**

```
$ parallel
   -a target_list.txt
   --joblog joblog
   --progress
   --bar
   "wfuzz
      -f 'results/result_wfuzz_{= s/[:\/]/_/g =}.json',json
      --filter 'c<403'
      -R 3 -Z -c
      -z file,'/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt'
      {1}/FUZZ"
```

```
http://foo
https://foobar
https://bar:4443
...
```

sed expression to remove bad chars in filename

```
$ ls ./results/result_wfuzz_*.json |
  parallel
 "cat {} | jq '.[] | if (.code == 200) then .url else empty end' | sed 's/"//g' >>
 list_to_webscreenshot.txt"
```

**"webscreenshot" is a simple tool to take screenshots of URLs**
(https://github.com/maaaaz/webscreenshot)

# 3. High-level scripting languages for easier static and dynamic analysis

**Pentesting involves sometimes reversing "custom-wtf" obfuscation or encryption**

- Especially true for **Android and Java thick-client applications**
  - No I'm **kidding**, it affects any technology. People do not understand crypto.
  - But still, very usual during Android application engagements
- Sometimes you **don't want to go down the rabbit hole** to figure out how it works
- Sometimes you just **can't replicate/rip the code** into your favourite language
  - For example, **Oracle WebLogic Server** encrypts local passwords with **PBKDF PKCS#12 SHA1 + RC2**:
    - No **Python** module was (is?) implementing that cryptosystem…

So use a **high-level scripting** language for instrumentation !

For **static analysis** of Android and Java applications, use **Jython**:

- Writing **Java code** in Python…
- …that can use **Java classes**…
- …AND **Python libraries** in the same snippet

Jython

For **dynamic analysis** of everything else, use **Frida**:

- Writing **Python or JS or QML or Swift or .NET**…
- …injecting **C++** scripted in **JS** (Google v8)
- …to instrument **ASM, Objective-C or Dalvik**
- …on **Windows, Mac, Linux, Android, iOS**

FRIDA

# 3. High-level scripting languages for easier static and dynamic analysis

## Example of ripping a Java custom-wtf routine in Jython

```
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;


public CharSequence decode(String paramString) throws
Exception
  {
    try {
      this.seed = <whatever>
      this.key = <whatever>
      IvParameterSpec localIvParameterSpec = new
IvParameterSpec(resizeParam(this.seed).getBytes("UTF-8"));
      SecretKeySpec localSecretKeySpec = new
SecretKeySpec(this.key.getBytes("UTF-8"), "AES");
      Cipher localCipher =
Cipher.getInstance("AES/CBC/PKCS5Padding");
      localCipher.init(2, localSecretKeySpec,
localIvParameterSpec);
      paramString = new
String(localCipher.doFinal(Base64.decode(paramString, 0)),
"ISO-8859-1");
      return paramString;} }
}
```

```
from javax.crypto import *
from javax.crypto.spec import *
from java.security import *
```

**A real-life example: `weblogicpassworddecryptor`**

https://github.com/maaaaz/weblogicpassworddecryptor/

```
seed = <whatever>
key = <whatever>

localIvParameterSpec = IvParameterSpec(seed)

localSecretKeySpec = SecretKeySpec(key, "AES")
localCipher = Cipher.getInstance("AES/CBC/PKCS5Padding")

localCipher.init(Cipher.DECRYPT_MODE, secretKeySpec,
localIvParameterSpec)
cleartext =
localCipher.doFinal(encrypted_stuff).tostring().decode('utf-
8')
```

# 4. Compile Python scripts on-the-fly

**Pentesting involves sometimes to have compiled version of tools**

- Because the **target** you are onto does not the **proper tool execution environment** (dependencies, interpreter) and you **can't install it** (no root, no outgoing connection, laziness, etc.)
- Because you **can't just have a proper reverse-shell** or meterpreter
- Because you need to **evade antivirus**

➔ So compile Python tools with **PyInstaller**

PyInstaller **bundles the script** with a Python interpreter

To install it on Windows:

- Install "Visual C++ Compiler for Python" https://wiki.python.org/moin/WindowsCompilers
- `$ pip install pyinstaller`

You can apparently even **cross-compile** for Windows from Linux, with **wine**:

- Google translate this http://thanat0s.trollprod.org/2017/04/crosscompiler-un-python-en-pe-pour-windows-avec-juste-ton-linux-console/

- The most useful options are:
  - `--onefile:` creates a **standalone executable file** which is a UPX-compressed-self-extracting zip payload
  - `--onedir:` creates a **single directory** with everything inside, if you don't want a standalone executable file as **large standalone** (> 18 MB) take *time* to unzip before execution
  - `--key <key>:` a **specific key** to encrypt the zip payload, of course included in the executable (https://0xec.blogspot.fr/2017/02/extracting-encrypted-pyinstaller.html)
  - `--icon <icon_file>:` for visual fanciness

# 4. Compile Python scripts on-the-fly

## Example of Python scripts compiled with PyInstaller

Impacket examples

https://github.com/maaaaz/impacket-examples-windows

https://blog.ropnop.com/practical-usage-of-ntlm-hashes/

```
PS C:\tools\impacket-examples-windows> .\wmiexec.exe -hashes :24cf95f179a809554d9b061ad76a2117 kbryant@ordws01.cscou.lab

Impacket v0.9.15-dev - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
cscou\kbryant
```

- GetADUsers.exe
- GetUserSPNs.exe
- LICENCE
- README.md
- atexec.exe
- esentutl.exe
- getArch.exe
- getPac.exe
- goldenPac.exe
- ifmap.exe
- karmaSMB.exe
- lookupsid.exe
- loopchain.exe
- mimikatz.exe
- mmcexec.exe
- mqtt_check.exe
- mssqlclient.exe
- mssqlinstance.exe
- netview.exe
- nmapAnswerMachine.exe
- ntfs-read.exe
- ntlmrelayx.exe
- opdump.exe
- opdump.exe
- os_ident.exe
- ping.exe
- ping6.exe
- psexec.exe
- raiseChild.exe
- rdp_check.exe
- reg.exe
- registry-read.exe
- rpcdump.exe
- sambaPipe.exe
- samrdump.exe
- secretsdump.exe
- services.exe
- smbclient.exe
- smbexec.exe
- smbrelayx.exe
- smbserver.exe
- smbtorture.exe
- sniff.exe
- sniffer.exe
- split.exe
- ticketer.exe
- tracer.exe
- ticketer.exe
- tracer.exe
- uncrc32.exe
- wmiexec.exe
- wmipersist.exe
- wmiquery.exe

# 4. Compile Python scripts on-the-fly

## Example of Python scripts compiled with PyInstaller

Patator

https://github.com/maaaaz/patator-windows/

This script depends on a **lot of third-party modules**…

- paramiko
- ajpy
- pysnmp
- cx_Oracle
- psycopg2
- IPy
- dnspython
- Pycurl

…and these dependencies have their **own dependencies**:

- appdirs
- asn1crypto
- cffi
- cryptography
- enum34
- idna
- impacket
- ipaddress
- packaging
- pcapy
- ply
- pyasn1
- pycparser
- pycryptodome
- pyOpenSSL
- pyparsing
- pypiwin32
- pysmi
- pysnmp
- six

```
D:\DONT_SCAN>patator.exe -h
Patator v0.7-beta (https://github.com/lanjelot/patator)
Usage: patator.py module --help

Available modules:
  + ftp_login     : Brute-force FTP
  + ssh_login     : Brute-force SSH
  + telnet_login  : Brute-force Telnet
  + smtp_login    : Brute-force SMTP
  + smtp_vrfy     : Enumerate valid users using SMTP VRFY
  + smtp_rcpt     : Enumerate valid users using SMTP RCPT TO
  + finger_lookup : Enumerate valid users using Finger
  + http_fuzz     : Brute-force HTTP
  + ajp_fuzz      : Brute-force AJP
  + pop_login     : Brute-force POP3
  + pop_passd     : Brute-force poppassd (http://netwinsite.com/poppassd/)
  + imap_login    : Brute-force IMAP4
  + ldap_login    : Brute-force LDAP
  + smb_login     : Brute-force SMB
  + smb_lookupsid : Brute-force SMB SID-lookup
  + rlogin_login  : Brute-force rlogin
  + vmauthd_login : Brute-force VMware Authentication Daemon
  + mssql_login   : Brute-force MSSQL
  + oracle_login  : Brute-force Oracle
  + mysql_login   : Brute-force MySQL
  + mysql_query   : Brute-force MySQL queries
  + rdp_login     : Brute-force RDP (NLA)
  + pgsql_login   : Brute-force PostgreSQL
  + vnc_login     : Brute-force VNC
  + dns_forward   : Forward DNS lookup
  + dns_reverse   : Reverse DNS lookup
  + snmp_login    : Brute-force SNMP v1/2/3
  + ike_enum      : Enumerate IKE transforms
  + unzip_pass    : Brute-force the password of encrypted ZIP files
  + keystore_pass : Brute-force the password of Java keystore files
  + umbraco_crack : Crack Umbraco HMAC-SHA1 password hashes
  + tcp_fuzz      : Fuzz TCP services
  + dummy_test    : Testing module
```

**➔ ….But PyInstaller managed to include all of them in an standalone executable !**

# 4. Compile Python scripts on-the-fly

## Example of Python scripts compiled with PyInstaller

CrackMapExec

(old version 2 yes, but utf-8 compatible ☺)

https://github.com/maaaaz/CrackMapExecWin

```
C:\temp\CrackMapExecWin-master>crackmapexec.exe -u Test -p test 192.168.56.101 --shares
04-08-2018 21:58:03 [*] 192.168.56.101:445 is running Windows 5.1 (name:PC) (domain:PC)
04-08-2018 21:58:03 [+] 192.168.56.101:445 Login successful PC\Test:test
04-08-2018 21:58:03 [+] 192.168.56.101:445 Available shares:
04-08-2018 21:58:03            SHARE     Permissions
04-08-2018 21:58:03            -----     -----------
04-08-2018 21:58:03       SharedDocs     READ, WRITE
04-08-2018 21:58:03       PDFCreator       NO ACCESS
04-08-2018 21:58:03           print$            READ
04-08-2018 21:58:03             IPC$       NO ACCESS
04-08-2018 21:58:03      Imprimante2       NO ACCESS
```

jdwp-shellifier

https://github.com/maaaaz/jdwp-shellifier-windows

```
C:\Temp>jdwp-shellifier.exe -h
usage: jdwp-shellifier.exe [-h] -t IP [-p PORT] [--break-on JAVA_METHOD]
                           [--cmd COMMAND]

Universal exploitation script for JDWP by @_hugsy_

optional arguments:
  -h, --help            show this help message and exit
  -t IP, --target IP    Remote target IP (default: None)
  -p PORT, --port PORT  Remote target port (default: 8000)
  --break-on JAVA_METHOD
                        Specify full path to method to break on (default:
                        java.net.ServerSocket.accept)
  --cmd COMMAND         Specify full path to method to break on (default:
                        None)
```

## Demo time

/ **01** What changed and why do you need to adapt ?

/ **02** Modern tricks for modern pentesters

/ **03** Taking a step back

# Main messages

**CSVKit all the things**

**Dataiku all the things**

**GNU Parallel all the things**

**Jython all the things**

**Frida all the things**

**PyInstall all the things**

WAVESTONE

# Questions ?

**Thomas DEBIZE**
thomas.debize@wavestone.com

wavestone.com

@wavestoneFR
@secuinsider