Lunchlezing EY

Studievereniging Inter-Actief

25 November 2014

Building a better working world

Jeroen van der Meer

IT Auditor

Mobile: +31 6 21 25 14 55
jeroen.van.der.meer@nl.ey.com

nl.linkedin.com/pub/jeroen-van-der-meer/

Ernst & Young Advisory
Antonio Vivaldistraat 150
1083 HP Amsterdam
The Netherlands

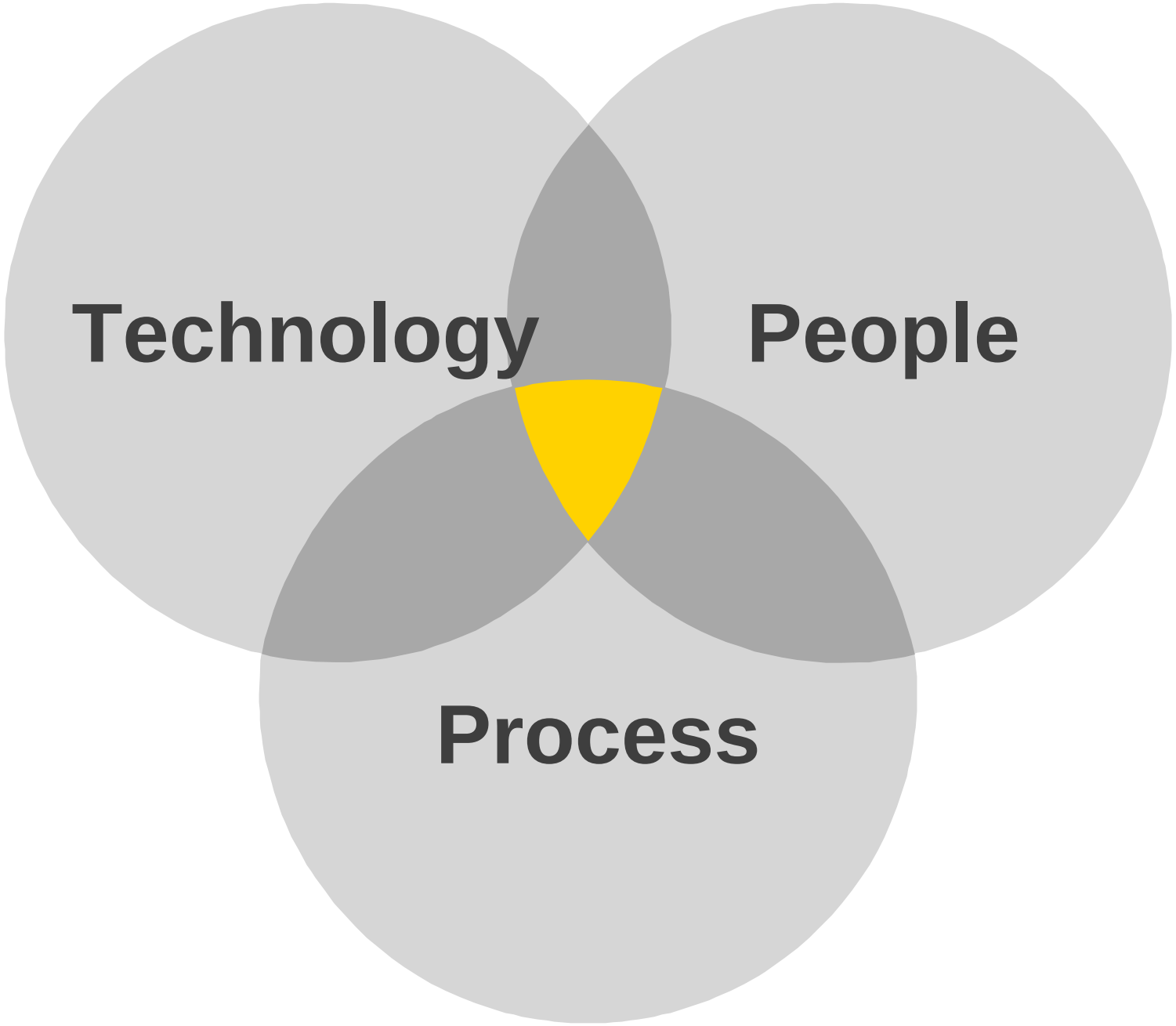
ey.nl

Agenda

- ✓ Introduction
- Information security
- EY eXtreme Hacking
- Demonstration
  - Hacking a WordPress website
  - Hacking Windows
- How to become a hacker
- Questions

“Information is …

*“Information is an **asset** that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably **protected**.”*


Technology
People
Process

Unsophisticated attackers

"Script kiddies"

Nieuws

Amerikaanse tiener opgepakt wegens wijzigen schoolcijfers

maandag 5 mei 2014, 10:34 door **Redactie**, 1 **reacties**

De Amerikaanse politie heeft een 18-jarige scholier opgepakt wegens het tegen betaling wijzigen van de schoolcijfers van andere scholieren, alsmede zijn eigen cijfers. **Volgens** de politie zou Jose Bautista op het schoolsysteem hebben ingebroken om vervolgens de cijfers aan te passen.

De tiener zou zijn scholieren begin dit jaar hebben benaderd of ze tegen betaling hun cijfers wilden laten aanpassen. Voor zover bekend hebben vier scholieren van de diensten van Bautista gebruik gemaakt. Exacte details over de werkwijze van de scholier zijn echter onbekend, behalve dat de database met schoolcijfers op illegale wijze werd benaderd.

NBC Miami zegt dat de tiener is aangeklaagd omdat hij in het kantoor van de rector inbrak en vervolgens diens computer gebruikte om de cijfers te wijzigen. In totaal werden er acht **aanklachten** tegen Bautista ingediend. Vier wegens het aanpassen van een programma en vier wegens het aanpassen van de gegevens van computergebruikers.

Sophisticated attackers

“Hackers”

"Onderwereld ontdekt internet"

ZATERDAG, 12 JULI 2014, 07:33 AANGEPAST OP 12-07-2014, 08:27 BINNENLAND

De politie maakt zich zorgen over de toename van internetcriminaliteit. In het FD spreekt Wilbert Paulissen, Hoofd Landelijke Recherche, van "een zeer zorgelijke trend die zich snel aan het ontwikkelen is".

Tot een paar jaar geleden was cybercrime volgens Paulissen alleen weggelegd voor mensen met veel technische kennis. Maar tegenwoordig zijn er ook veel IT-leken die zich toeleggen op internetcriminaliteit.

Paulissen wijst erop dat de aanschaf van malafide software steeds eenvoudiger wordt. Ook huren criminelen vaak professionele hulp in. Zo hackte vorig jaar een internationale drugsbende met behulp van IT-experts de netwerken van containerbedrijven in de haven van Antwerpen. Daardoor konden ze hun eigen containers met drugs onderscheppen voordat die bedrijven dat deden.

Corporate espionage

“Insiders”

National Security

Report: Cybercrime and espionage costs $445 billion annually

By Ellen Nakashima and Andrea Peterson June 9

Follow @nakashimae Follow @kansasalps

A Washington think tank has estimated the likely annual cost of cybercrime and economic espionage to the world economy at more than $445 billion — or almost 1 percent of global income.

The estimate by the Center for Strategic and International Studies is lower than the eye-popping $1 trillion figure cited by President Obama, but it nonetheless puts cybercrime in the ranks of drug trafficking in terms of worldwide economic harm.

State sponsored attacks

"Advanced Persistent Threats"

'Geavanceerde malware viel onder meer België aan'

Door Joost Schellevis, maandag 24 november 2014 08:16, reacties: 24, views: 6.494 • Feedback

Onderzoekers van Symantec hebben spionagemalware ontdekt die waarschijnlijk van een overheid afkomstig is en die onder meer Belgische computers zou hebben getroffen. De malware was onder meer in staat om bestanden te stelen.

Vijf procent van de bevestigde infecties van de geavanceerde malware vond plaats in België; de meeste infecties vonden plaats in Rusland en Saoedi-Arabië, respectievelijk 28 en 24 procent. De onderzoekers van Symantec geven niet aan welk land achter de malware zou zitten, maar opvallend is wel dat er geen infecties in de Verenigde Staten zouden hebben plaatsgevonden.

De malware, door de onderzoekers Regin gedoopt, is volgens de onderzoekers modulair opgebouwd. Daardoor kunnen de activiteiten van de malware per slachtoffer worden aangepast. De malware zou onder meer in staat zijn om wachtwoorden te stelen, screenshots te nemen, de muis over te nemen en netwerkverkeer te onderscheppen; gebruikelijke functies voor een spionagetrojan. Ook zou Regin in staat zijn om reeds verwijderde bestanden te achterhalen.

Lees meer over

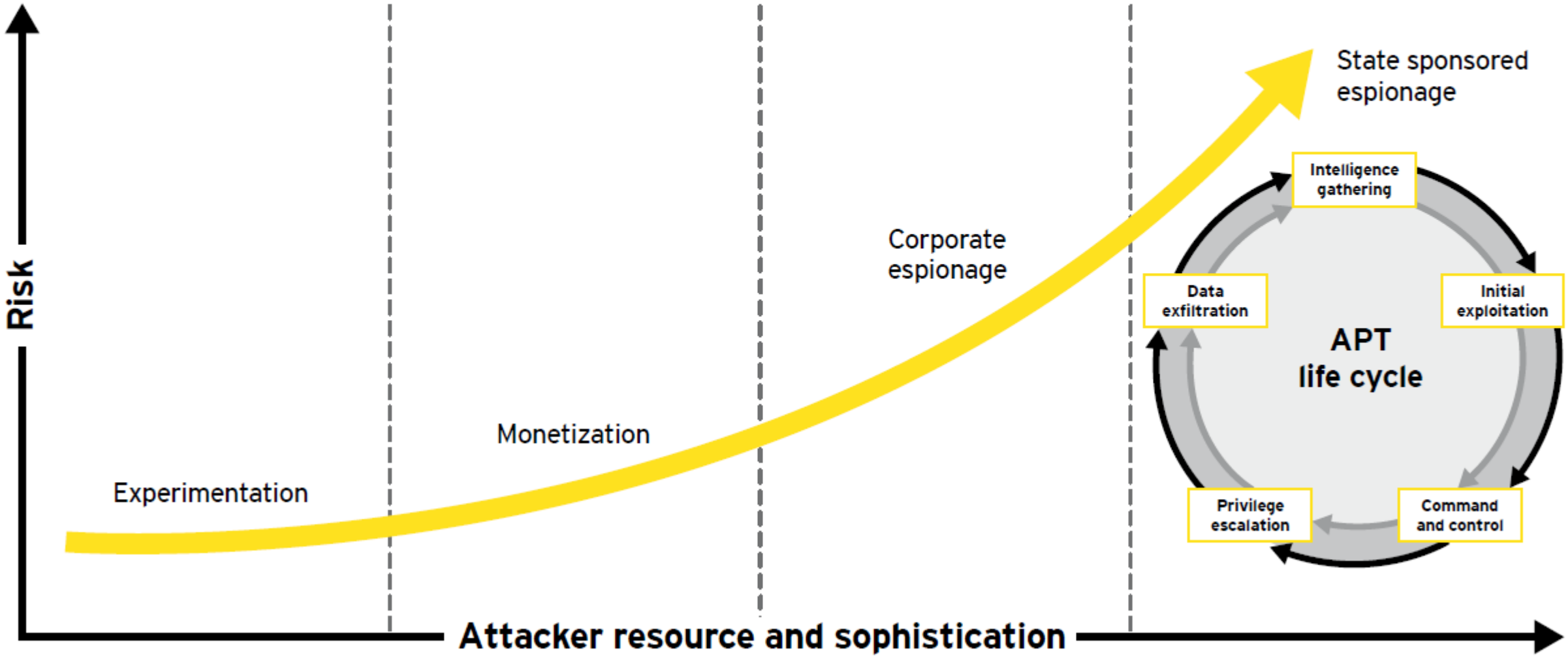
Beheer en beveiliging, België

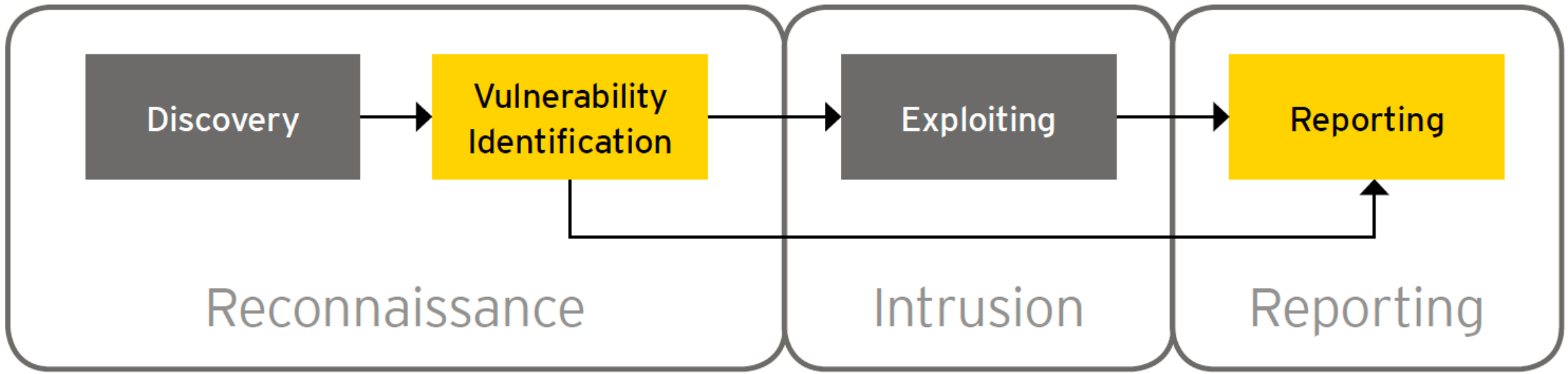
Unsophisticated attackers (script kiddies)
You are attacked because you are on the internet and have vulnerability.

Sophisticated attackers (hackers)
You are attacked because you are on the internet and have information of value.

Corporate espionage (insiders)
Your current or former employee seeks financial gain from selling your IP.

State-sponsored attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.




Discovery
Vulnerability Identification
Exploiting
Reporting
Reconnaissance
Intrusion
Reporting

Reconnaissance phase

- Goal:
  - Gathering information regarding the target **non-intrusively**
- Methods:
  - Explore public databases
  - Touching the internet infrastructure
  - Touching the applications
- Result:
  - A footprint matrix containing an overview of the internet infrastructure, application, and **potential** vulnerabilities

Google site:www.inter-actief.utwente.nl login +Jerc

Web Images Videos Maps News More Search tools

About 125 results (0.38 seconds)

Login – Amélie - Inter-Actief

https://www.inter-actief.utwente.nl/trac/amelie/**login** Translate this page

Trac · **Login** · Preferences · Probleem melden. Context Navigation. **Login**. Username: Password: Trac Powered. Powered by Trac 0.12.5. By Edgewall Software.

Login – MSDNAA - Inter-/Actief

https://www.inter-actief.utwente.nl/trac/msdnaa/**login**

Trac · **Login** · Preferences · Contact. Context Navigation. **Login**. Username: Password: Trac Powered. Powered by Trac 0.12.5. By Edgewall Software. Visit the ...

Login – Systeembeheer IA - Inter-Actief

https://www.inter-actief.utwente.nl/trac/beheer/**login** - Translate this page

Systeembeheer IA · **Login** · Preferences. Context Navigation. **Login**. Username: Password: Trac Powered. Powered by Trac 0.12.5. By Edgewall Software.

Inter-Actief SugarCRM

https://www.inter-actief.utwente.nl/.../index.php?...**Login**...**login**...**login**...

2004-2011 SugarCRM Inc. The Program is provided AS IS, without warranty. Licensed under AGPLv3. This program is free software; you can redistribute it ...

```
'REDIRECT_HTTPS': 'on',
'REDIRECT_SCRIPT_URI': 'https://www.inter-actief.utwente.nl/activiteiten/fotos/upload/',
'REDIRECT_SCRIPT_URL': '/activiteiten/fotos/upload/',
'REDIRECT_SSL_TLS_SNI': 'www',
'REDIRECT_STATUS': '200',
'REDIRECT_UNIQUE_ID': 'TVPamwoKAwUAABIrhG0AAAAH',
'REDIRECT_URL': '/activiteiten/fotos/upload/',
'REMOTE_ADDR': '130.89.162.13',
'REMOTE_PORT': '34104',
'REQUEST_METHOD': 'POST',
'REQUEST_URI': '/activiteiten/fotos/upload/',
'SCRIPT_FILENAME': '/data/htdocs/https/amelie.wsgi',
'SCRIPT_NAME': u'',
'SCRIPT_URI': 'https://www.inter-actief.utwente.nl/activiteiten/fotos/upload/',
'SCRIPT_URL': '/activiteiten/fotos/upload/',
'SERVER_ADDR': '10.10.3.5',
'SERVER_ADMIN': 'beheer@inter-actief.utwente.nl',
'SERVER_NAME': 'www.inter-actief.utwente.nl',
'SERVER_PORT': '443',
'SERVER_PROTOCOL': 'HTTP/1.1',
'SERVER_SIGNATURE': '<address>Apache Server at www.inter-actief.utwente.nl Port 443</address>\n',
'SERVER_SOFTWARE': 'Apache',
'SSL_TLS_SNI': 'www',
'UNIQUE_ID': 'TVPamwoKAwUAABIrhG0AAAAH',
'mod_wsgi.application_group': 'www.inter-actief.utwente.nl|/amelie.wsgi',
'mod_wsgi.callable_object': 'application',
'mod_wsgi.listener_host': 'zwarejongens-www',
'mod_wsgi.listener_port': '443',
'mod_wsgi.process_group': 'amelie-secure',
'mod_wsgi.reload_mechanism': '1',
```

Authentication

Server Key and Certificate #1

Common names	www.inter-actief.utwente.nl
Alternative names	www.inter-actief.utwente.nl *.ia.utwente.nl *.inter-actief.utwente.nl ia.utwente.nl inter-actief.utwente.nl
Prefix handling	Not required for subdomains
Prefix handling	Both (with and without WWW)
Valid from	Mon Apr 21 17:00:00 PDT 2014
Valid until	Fri Apr 21 16:59:59 PDT 2017 (expires in 2 years and 4 months)
Key	RSA 4096 bits
Weak key (Debian)	No
Issuer	TERENA SSL CA
Signature algorithm	SHA1withRSA WEAK
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	4 (4849 bytes)
Chain issues	Contains anchor

#2

Subject	TERENA SSL CA SHA1: 3a881764472b6441ddb3afdd47c6b8b76ee7ba1d

```
root@xscan1:~# host www.inter-actief.utwente.nl
www.inter-actief.utwente.nl is an alias for bb-www.ia.utwente.nl.
bb-www.ia.utwente.nl has address 130.89.148.136
bb-www.ia.utwente.nl has IPv6 address 2001:67c:2564:a119::136
```

```
root@xscan1:~# tcptraceroute www.inter-actief.utwente.nl
traceroute to www.inter-actief.utwente.nl (130.89.148.136), 30 hops max, 60 byte pa
ckets
 1  217-195-246-145.dsl.easynet.nl (217.195.246.145)  2.586 ms  2.588 ms  2.736 ms
 2  ae2.jnr02.Asd001A.surf.net (80.249.208.50)  2.906 ms  2.983 ms  2.966 ms
 3  AE0.500.JNR01.Asd002A.surf.net (145.145.80.81)  3.317 ms  3.302 ms  3.453 ms
 4  utwente-router.customer.surf.net (145.145.4.46)  7.141 ms  7.301 ms  7.388 ms
 5  bb-www.ia.utwente.nl (130.89.148.136) <syn,ack>  7.068 ms  7.212 ms  7.211 ms
```

```
root@xscan1:~# nmap -sS -sV -O -Pn --top-ports 100 www.inter-actief.utwente.nl

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-24 11:06 CET
Nmap scan report for www.inter-actief.utwente.nl (130.89.148.136)
Host is up (0.0093s latency).
rDNS record for 130.89.148.136: bb-www.ia.utwente.nl
Not shown: 97 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.2.22 ((Debian))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Debian))
Warning: OSScan results may be unreliable because we could not find at least 1 open
 and 1 closed port
Device type: general purpose|firewall|WAP|broadband router|terminal|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (93%), IPFire Linux 2.6.X (92%), D-L
ink embedded (90%), IGEL Linux 2.6.X (88%), QNAP Linux 3.X (86%), Axcient embedded
(85%)
```

https://www.i...ic/robots.txt

https://www.inter-actief.utwente.nl/sta

```
User-agent: *
Disallow: /admin/
Disallow: /leden/
Disallow: /login/
Disallow: /loguit/
Disallow: /home/
Disallow: /media/
Disallow: /autozoek/
Disallow: /test/
Disallow: /alv/
Disallow: /profiel/
Disallow: /bestanden/
Disallow: /feeds/
Disallow: /comments/
Disallow: /xml-rpc/
Disallow: /onderwijs/
Disallow: /site_media/
Disallow: /random_foto/
Disallow: /msdnaa/
Disallow: /api/

User-agent: Googlebot
Disallow: /admin/
Disallow: /leden/
Disallow: /login/
Disallow: /loguit/
Disallow: /home/
Disallow: /media/
Disallow: /autozoek/
Disallow: /test/
Disallow: /alv/
Disallow: /profiel/
Disallow: /bestanden/
Disallow: /feeds/
Disallow: /comments/
Disallow: /xml-rpc/
Disallow: /site_media/
Disallow: /random_foto/
Disallow: /msdnaa/
Disallow: /api/
Disallow: /activiteiten/*/*/*/*/*/fotos/willekeurig/
```

Document: 100% Images: 0/0 Loaded: 7 KB Speed: 22.15 KB/s Time: 0.318

Log in | Django site admin

https://www.inter-actief.utwente.nl/ad

Django administration

Username:

Password:

Log in

22:17
24-11-2014

Intrusion phase

- Goal:
  - Obtain unauthorized access to information and systems
- Methods:
  - Exploit known vulnerabilities in third party software
  - Exploit vulnerabilities in custom software
  - Exploit configuration mistakes
- Results:
  - Confidential information
  - Administrative access to systems
  - New information regarding internal network infrastructure

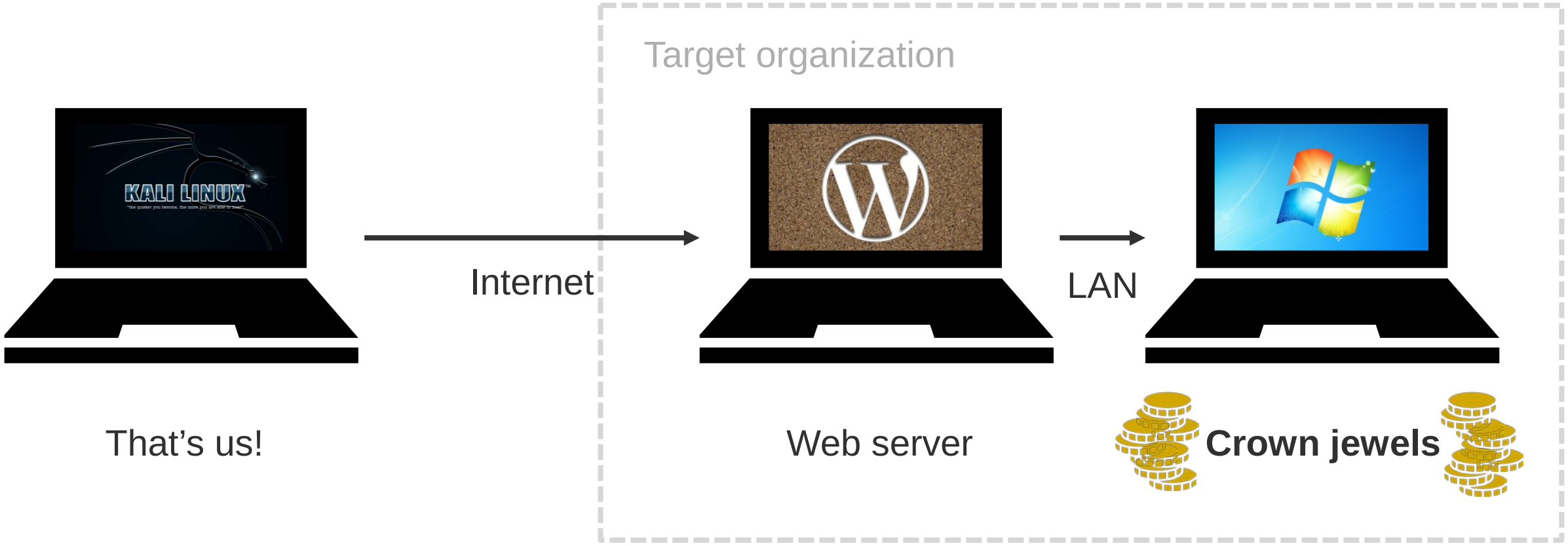
Demonstration

That’s us!

Web server

File station

Demonstration



Demonstration

Web server

- WordPress user enumeration
- Weak administrator password
- Vulnerable file manager plugin
- Web shell
- Meterpreter malware

File server

- Identical password
- Pass-the-hash
- Profit

How to become a hacker

Opportunities at EY

Internship

- Five months
- Obtain experience in projects
- Write your final thesis about state of the art information security topics:
  - Advanced Persistent Threats
  - Internet of Things
  - Threat Intelligence
  - Distributed Denial of Services

Advisor

- Attack & Penetration
  - External / Internal
  - Internet exposure
  - Web applications
  - WiFi
  - Mobile
- Secure code review
- Social engineering
- Information security management
- Data privacy
- Training en awareness

Rent-A-Hacker

Rent-A-Hacker

What ill do:
Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone
Ruining your opponents, bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.656 ฿	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR = 1.640 ฿	1 X Buy now

Be warned!

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132
(Rev. 3/2/82)

November 1992


Thank you! Questions?
EY
Building a better
working world