Vivir y Morir por el Threat Modelling

NICO WAISMAN

VP Latam en Immunity, Inc.

@nicowaisman

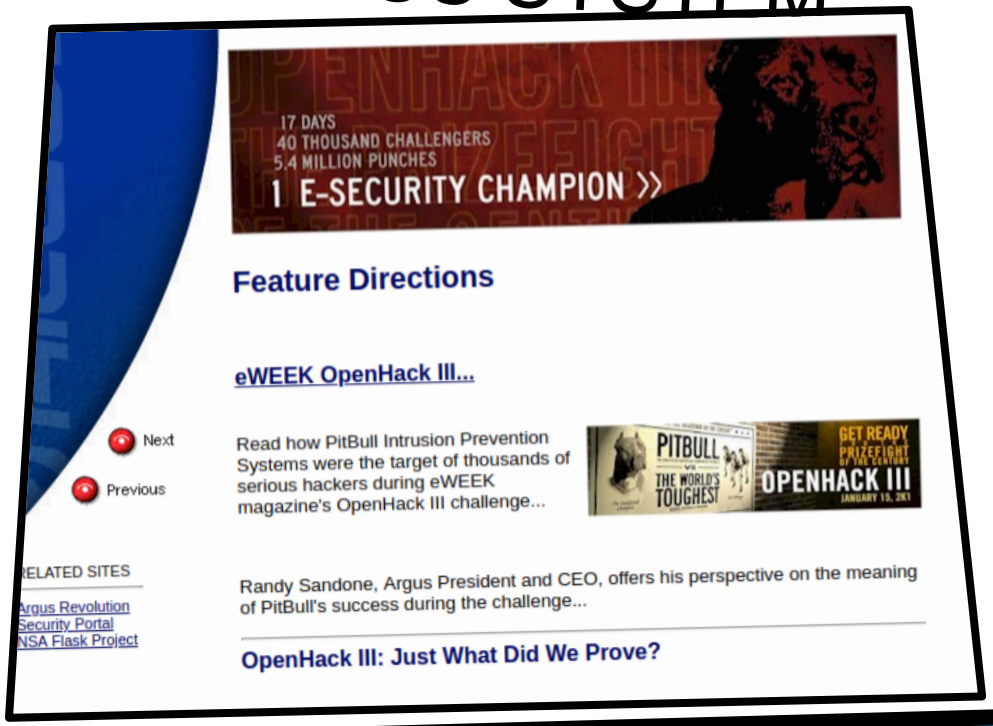

HACKING IN PROGRESS
GIFSec.com


freegifmaker.me

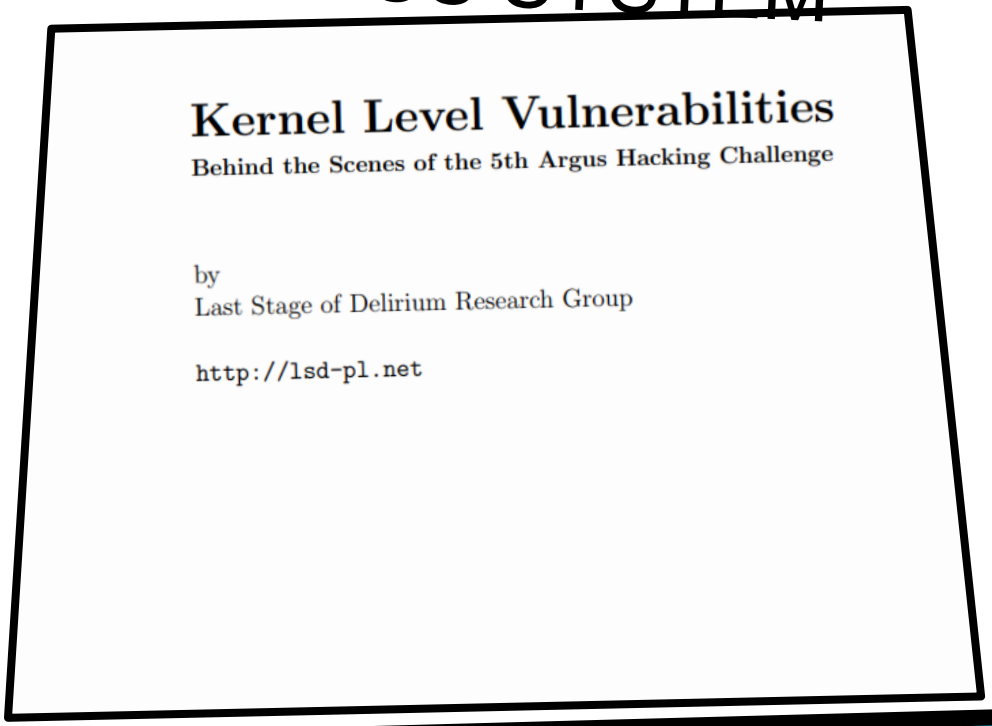
HACKERS

“Irrefrenable tendencias a cuestionar y reapropiarse de la tecnología”

LSD-PL vs ARGUS SYSTEM



LSD-PL vs ARGUS SYSTEM



Kernel Level Vulnerabilities

Behind the Scenes of the 5th Argus Hacking Challenge

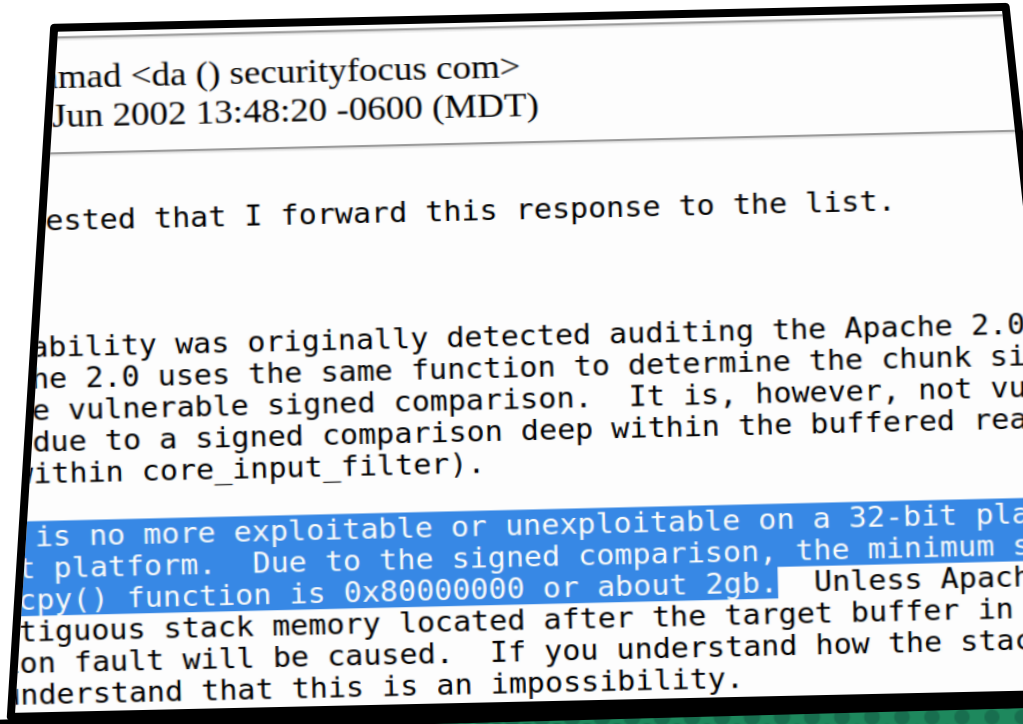
by
Last Stage of Delirium Research Group

`http://lsd-pl.net`

GOBBLES VS THE WORLD

- IIS X-Force pública una vulnerabilidad en Apache
- Un problema con los enteros en el *Chunked Encoding* de Apache, permite sobreescribir la stack
- El problema:
  - memcpy(stack, buffer, Size Negativo)

GOBBLES VS THE WORLD



mad <da () securityfocus com>
Jun 2002 13:48:20 -0600 (MDT)

ested that I forward this response to the list.

ability was originally detected auditing the Apache 2.0
he 2.0 uses the same function to determine the chunk siz
e vulnerable signed comparison. It is, however, not vul
due to a signed comparison deep within the buffered read
ithin core_input_filter).

is no more exploitable or unexploitable on a 32-bit plat
t platform. Due to the signed comparison, the minimum siz
cpy() function is 0x80000000 or about 2gb. Unless Apache
tiguous stack memory located after the target buffer in me
on fault will be caused. If you understand how the stack
nderstand that this is an impossibility.

Cancel all my meetings.

Someone on the internet is wrong.

someecards.com

GOBBLES

ApacheNoseJOB.C

```
andl   $3,%ecx
decl   %edi
decl   %esi
rep  movsb
movl    20(%esp),%ecx  // COPIA EL RESTANTE
shrl    $2,%ecx
subl    $3,%esi
subl    $3,%edi
rep movsl
```

GOBBLES

ApacheNoseJOB.C

```
andl   $3,%ecx
decl    %edi
decl    %esi
rep  movsb
movl    20(%esp),%ecx  // COPIA EL RESTANTE
shrl    $2,%ecx
subl    $3,%esi
subl    $3,%edi
rep movsl
```

GOBBLES

ApacheNoseJOB.C

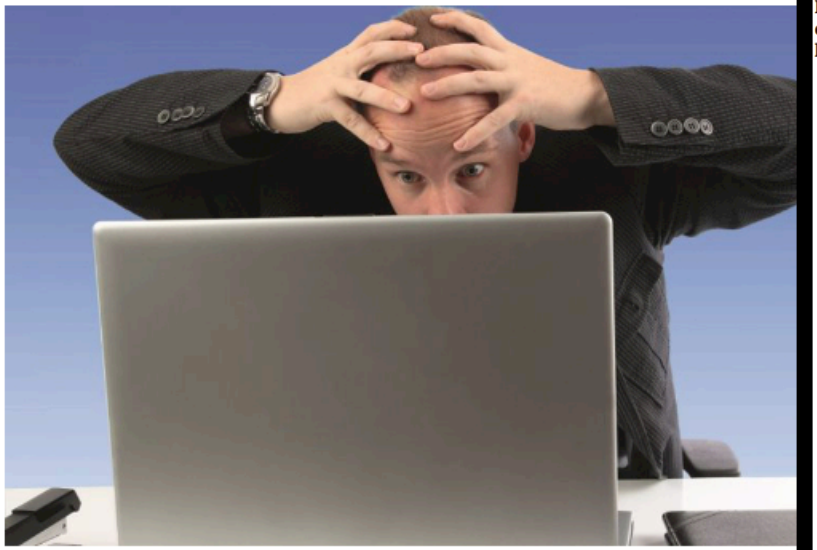
```
andl   $3,%ecx
decl   %edi
decl   %esi
rep  movsb
movl    20(%esp),%ecx  // COPIA EL RESTANTE
shrl    $2,%ecx
subl    $3,%esi
subl    $3,%edi
rep movsl
```

VULNERABILIDADES UNICORNIO

Son of Heartbleed poses a major new threat to the internet

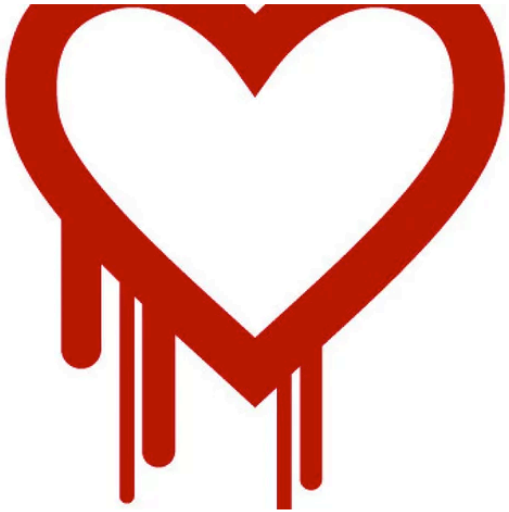
By Darren Allan September 20, 2017 Internet

OptionsBleed can be similarly exploited to cause data leakage



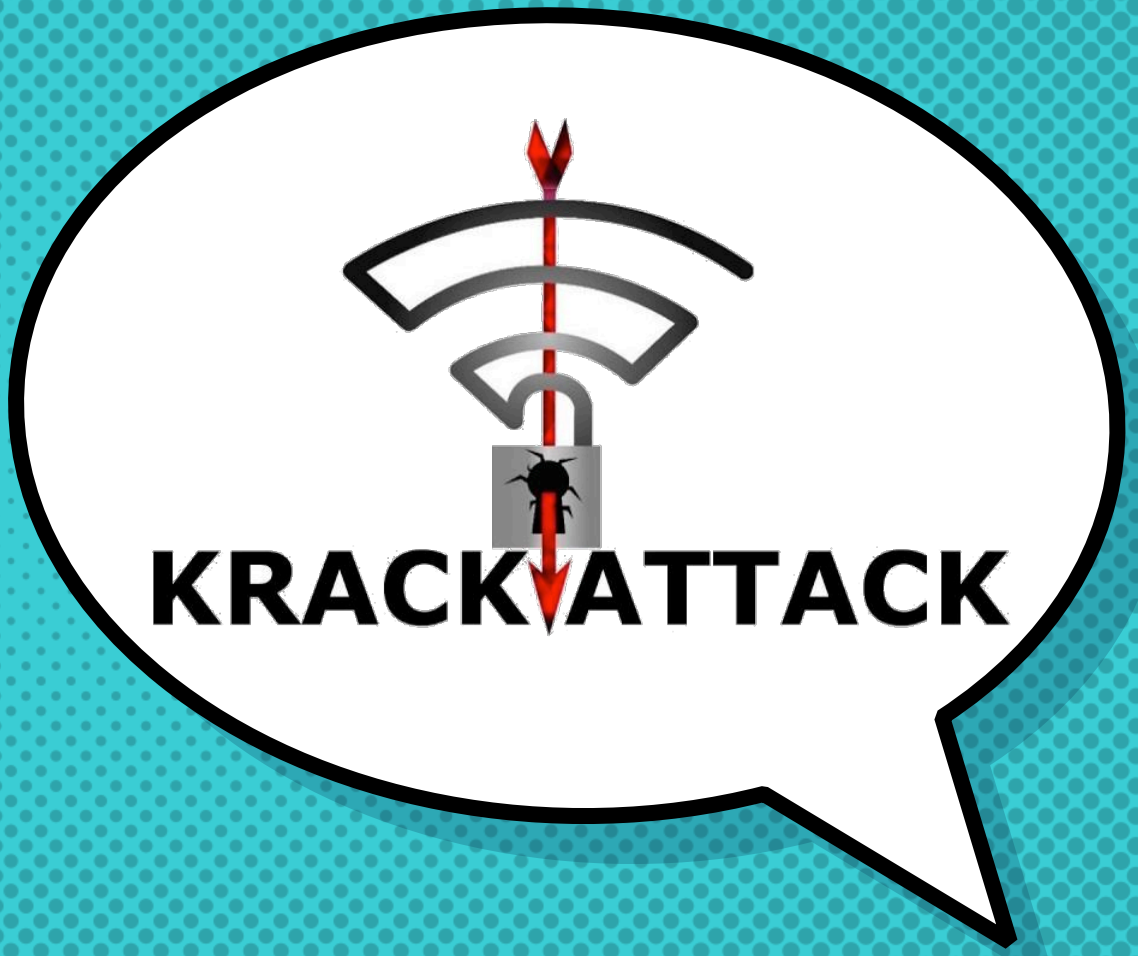
Heartbleed bug 'will cost millions'

Revoking all SSL certificates leaked by Heartbleed will cost millions of dollars, according to Cloudflare, which provides services to website hosts



▲ Image: Codenomicon

Revoking all the SSL certificates leaked by the Heartbleed bug will cost millions of dollars, according to Cloudflare, which provides services to website hosts.


KRACK ATTACK

KRACK attack: Wi-Fi connections vulnerable to hackers after flaw discovered

By Peter Marsh

Updated 23 Oct 201

A security flaw
be used to hac
Fi.

That includes yo
PlayStation and

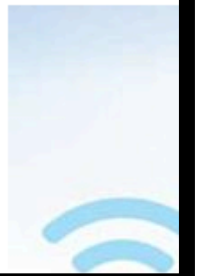
The key reinstal
discovered by B
and are so seric
Homeland Secu

How does

SECURITY NEWS

KRACK Vulnerability Means You Need to Change Your Wireless Approach

Tyler Lacoma November 22, 2017



WHY THE KRACK WI-FI MESS WILL TAKE DECADES TO CLEAN UP

MAR 3, 2017 @ 07:00 AM 1,450

My Toaster Hacked The Pentagon: What You Can Do To Secure Your IoT Devices

Forbes Technology Council

Elite CIOs, CTOs & execs offer firsthand insights on tech & business. FULL BIO

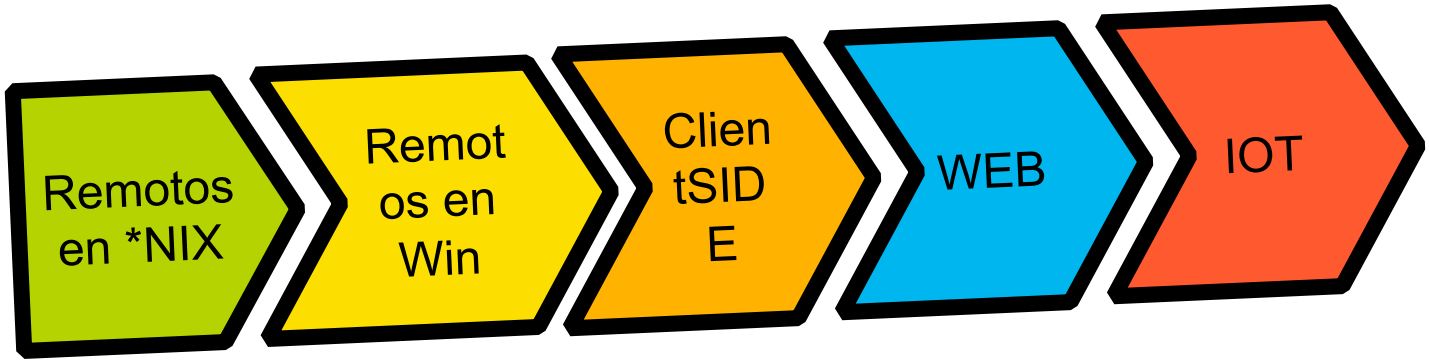
Opinions expressed by Forbes Contributors are their own.

POST WRITTEN BY

Forbes Technology Council

Successful CIOs, CTOs & executives from Forbes Technology Council offer firsthand insights on tech & business.

Research de VULNERABILIDADES

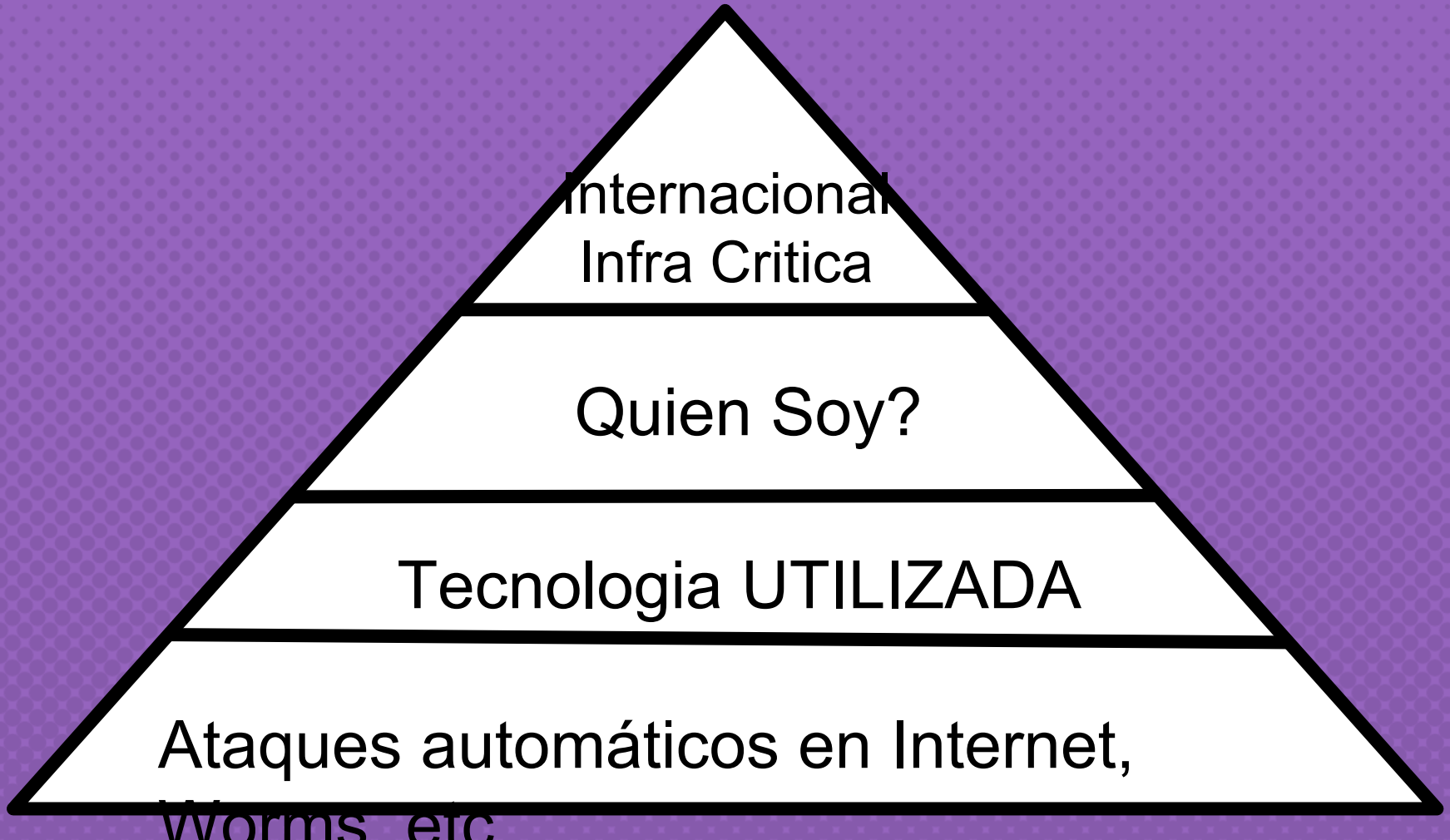


THRE

AT

Modelling

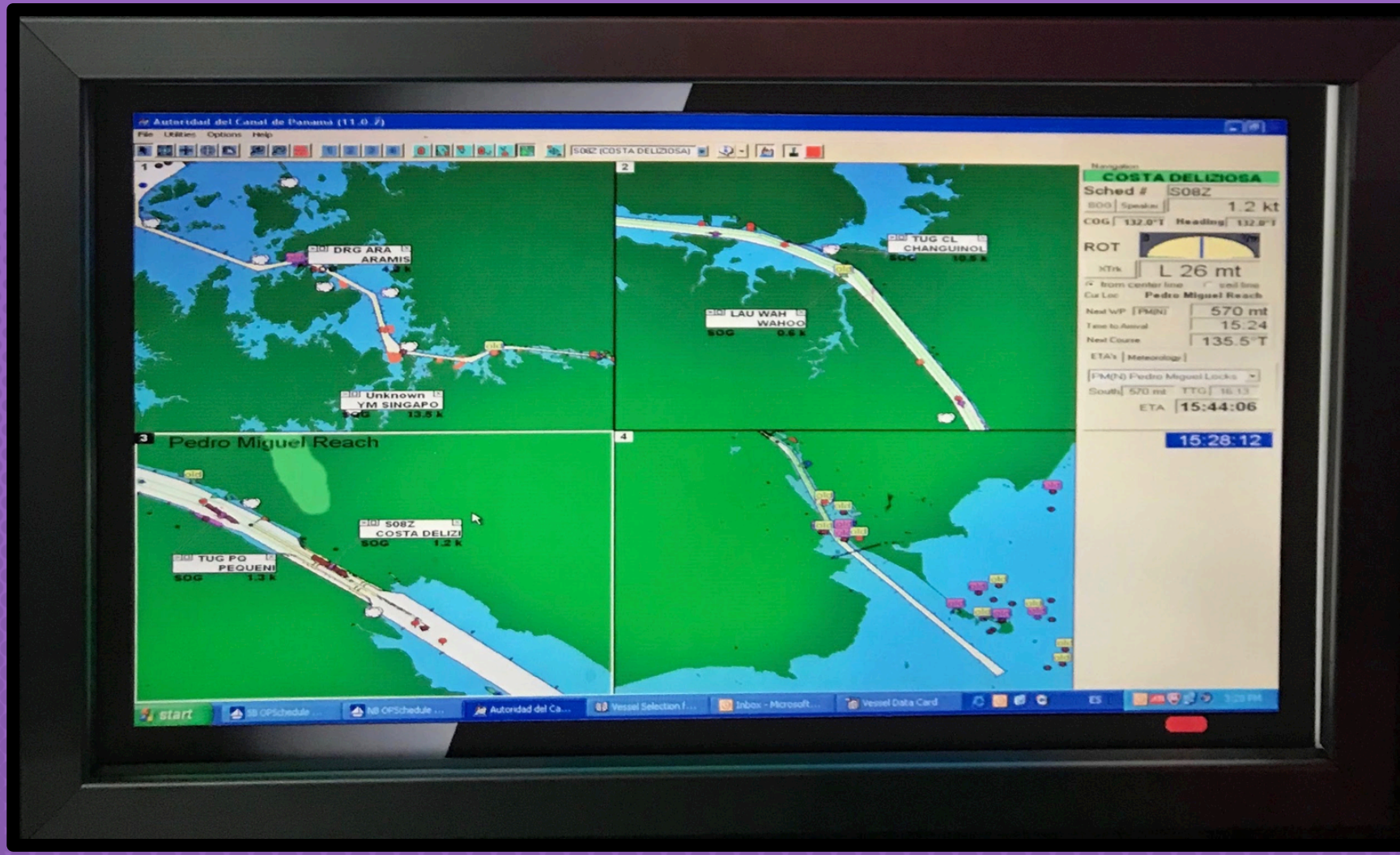
TU DESAFÍO NO ES EL MISMO QUE EL DE OTROS


Internacional
Infra Critica
Quien Soy?
Tecnologia UTILIZADA
Ataques automáticos en Internet,


MAERSK LINE
MAERSK SEALAND
MAERSK
msc

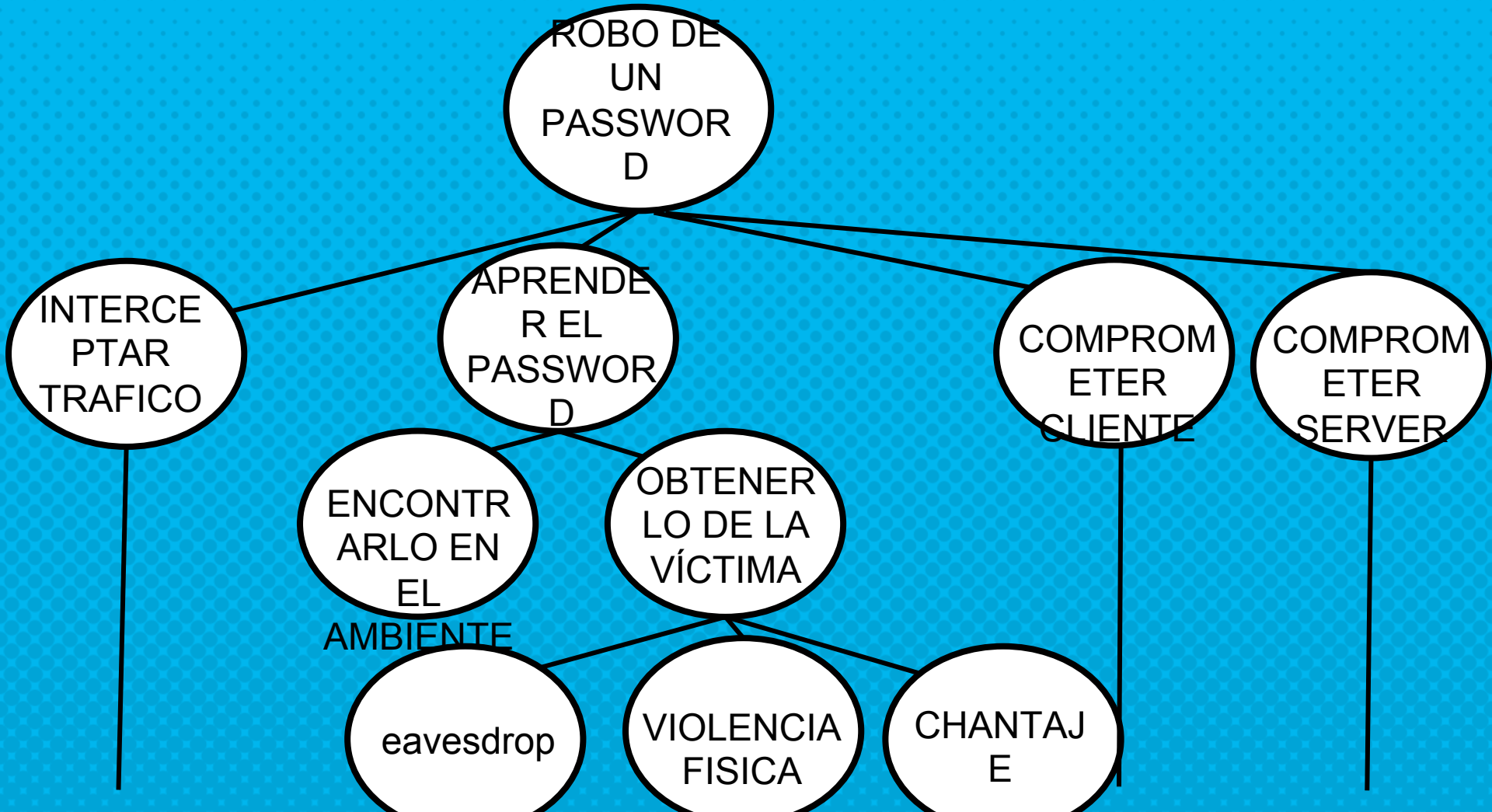

CANAL DE PANAMÁ

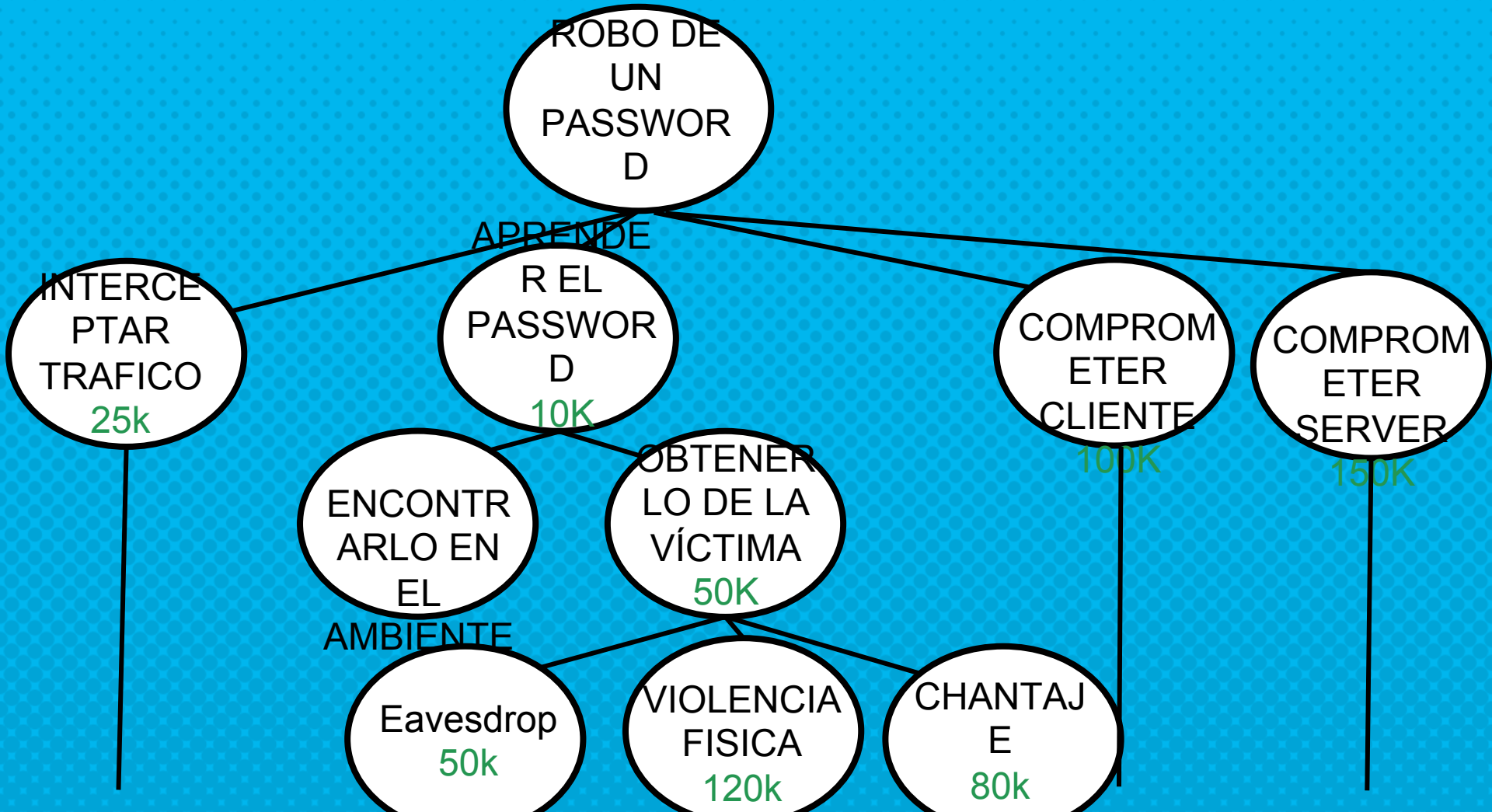

TORM TROILUS
JABIROO II
ZHUANG YUAN AO
JIAN GUO HAI
KNUD REEFER
SOUTHEND
CHICAGO HARMONY
LAGOON PHOENIX
STOLT SPAN
BBC RUSHMORE

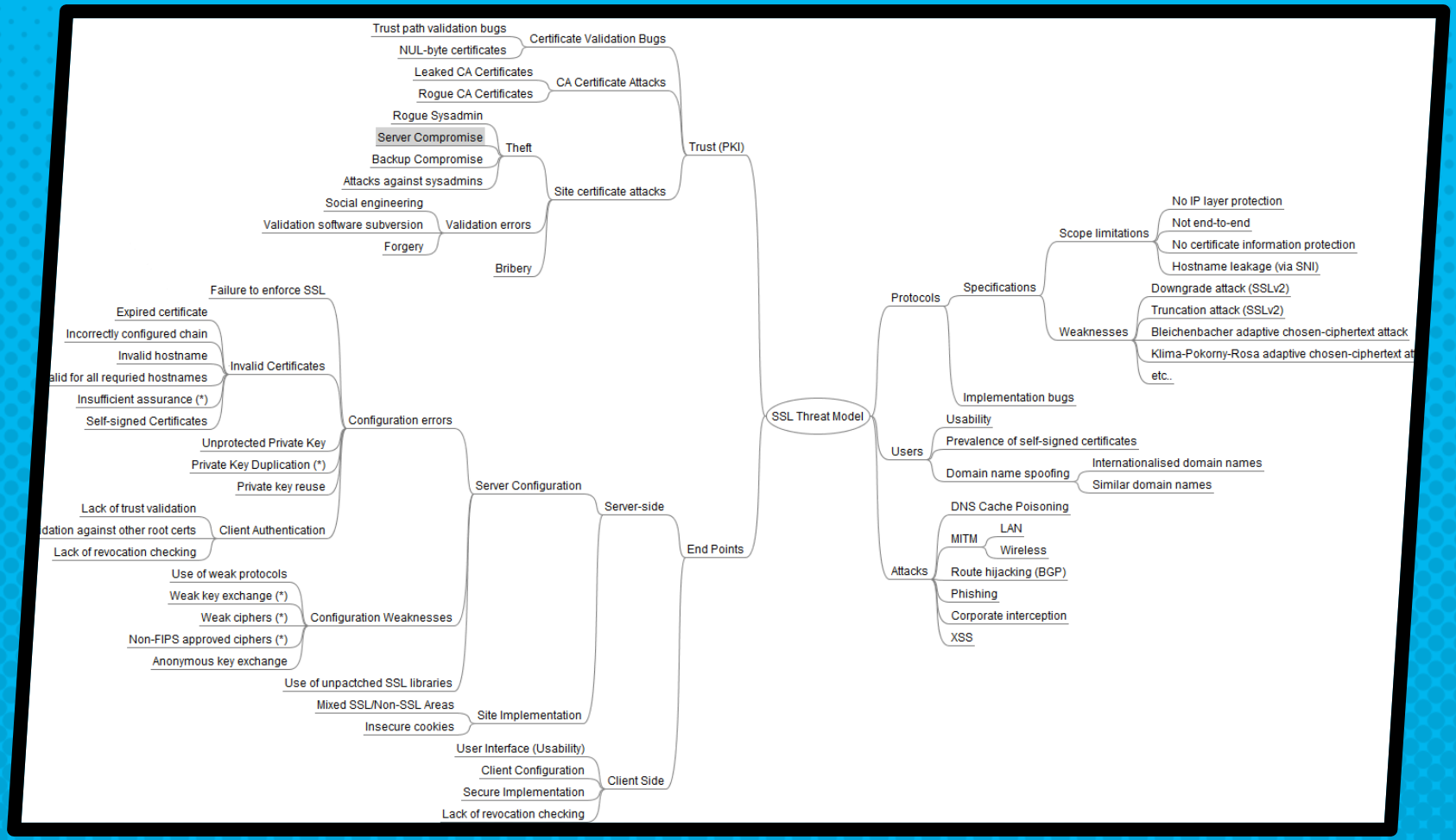

Autoridad del Canal de Panamá (11.0.2)
File Utilities Options Help
S08Z (COSTA DELIZIOSA)
1
DRG ARA
ARAMIS
Unknown
YM SINGAPO
SOG 13.5 k
2
TUG CL
CHANGUINOL
LAU WAH
WAHOO
SOG 0.6 k
3
Pedro Miguel Reach
S08Z
COSTA DELIZI
SOG 1.2 k
TUG PO
PEQUENI
SOG 1.3 k
4
Navigation
COSTA DELIZIOSA
Sched # S08Z
1.2 kt
COG 132.0°T Heading 132.0°T
ROT
XTrk L 26 mt
from center line
Cur Loc Pedro Miguel Reach
Next WP PMN 570 mt
Time to Arrival 15.24
Next Course 135.5°T
ETA's Meteorology
PMN Pedro Miguel Locks
South 570 mt TTG 16.13
ETA 15:44:06
15:28:12
start
Autoridad del Ca...
Vessel Selection f...
Inbox - Microsoft...
Vessel Data Card
ES

Attack Trees

“Proveen una forma formal y metódica de describir los riesgos a los cuales se puede afrontar un sistema”

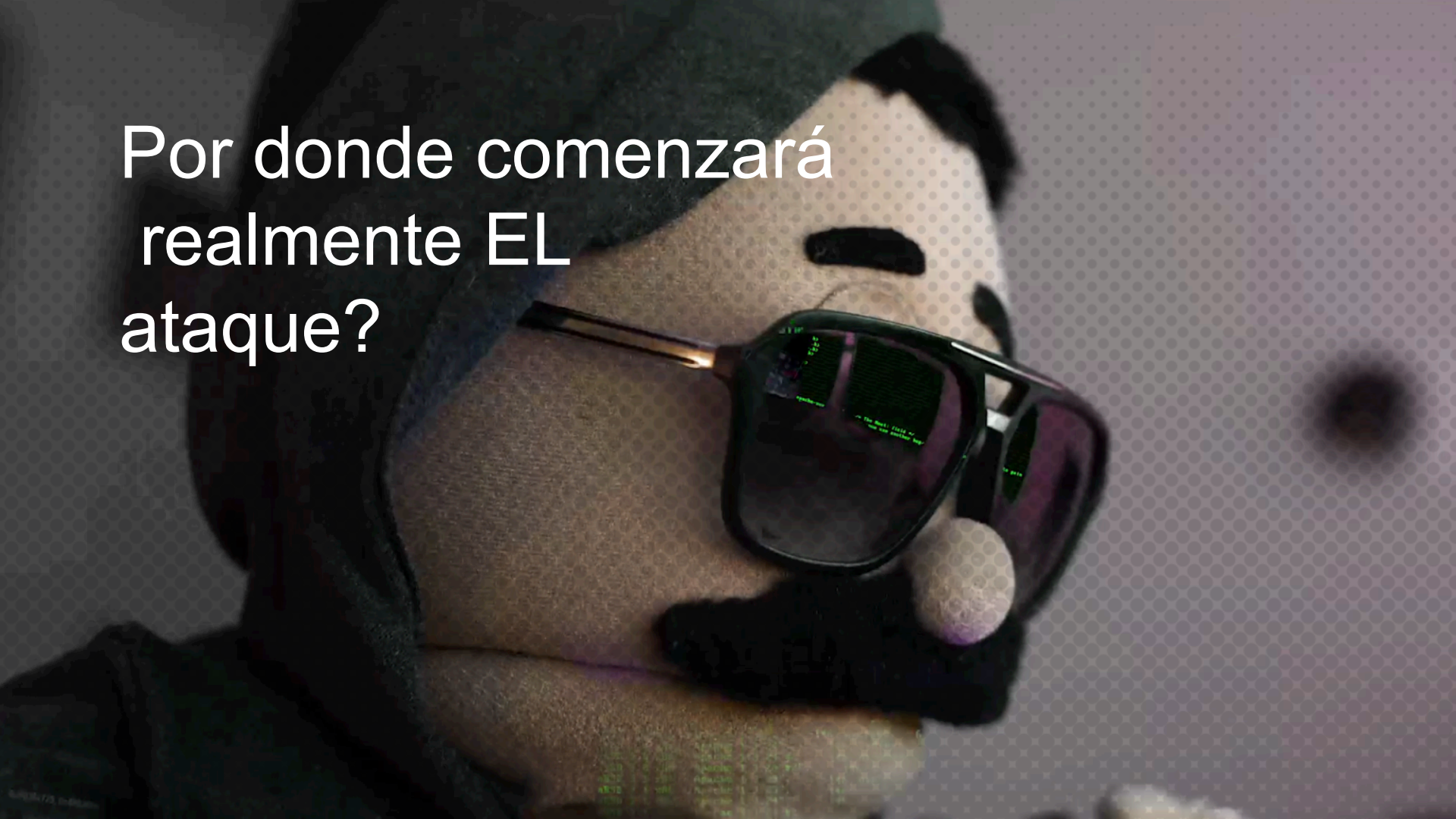

ROBO DE UN PASSWORD
INTERCEPTAR TRAFICO
APRENDER EL PASSWORD
COMPROMETER CLIENTE
COMPROMETER SERVER
ENCONTRARLO EN EL AMBIENTE
OBTENERLO DE LA VÍCTIMA
eavesdrop
VIOLENCIA FISICA
CHANTAJE


ROBO DE UN PASSWORD
INTERCEPTAR TRAFICO
25k
APRENDER EL PASSWORD
10K
COMPROMETER CLIENTE
100K
COMPROMETER SERVER
150K
ENCONTRARLO EN EL AMBIENTE
OBTENERLO DE LA VÍCTIMA
50K
Eavesdrop
50k
VIOLENCIA FISICA
120k
CHANTAJE
80k

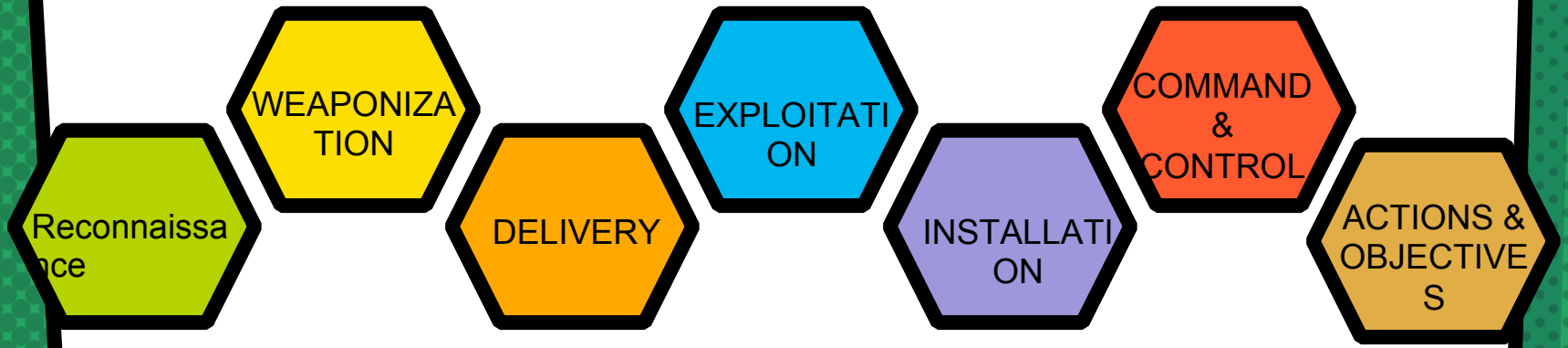


Source: Ivan Ristic Bl

KEEP CALM


Por donde comenzará realmente EL ataque?

INTEL-DRIVEN CND



Source: Lockeed Martin

SECURITY > NEWS

'Dear Valid LinkedIn User': Don't Fall for This Phishing Scam

by MARSHALL HONOROF Ja

UPDATE noon ET Monday: *fairly convincing replica of t*

Another day, another phishin
the delivery method for a cur

Yes, Your Users Are Dumb Enough To Fall For Phishing Scams

Angus Kidman
Sep 8, 2014, 12:30pm· Filed to: Australian Stories

Share

Dear Customer,

As part of our general security measures, we regularly check all the operations in the system. In a review we have recently encountered a problem associated with your account.

Please help us to bring to your account back in order. Until then, we have temporarily limited access to your account.

Where is the problem?
A recent change in your personal information (ie. change of address, email address, card information).

What should I do?
Please click on "Conflict Resolution" and confirm your identity by comparing your data to be the rightful owner.

INTEL-DRIVEN CND

Reconnaissance

WEAPONIZATION

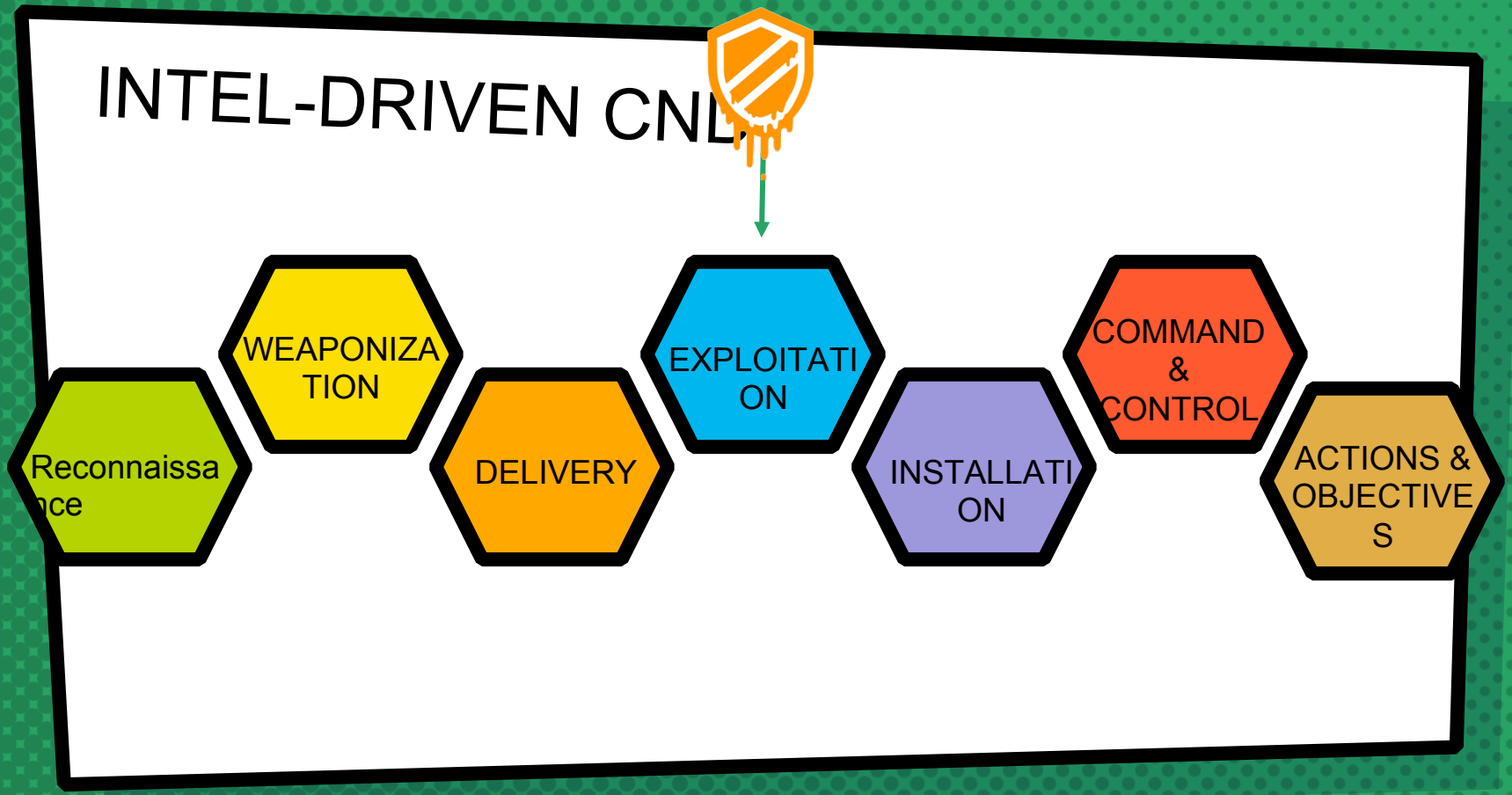
DELIVERY

EXPLOITATION

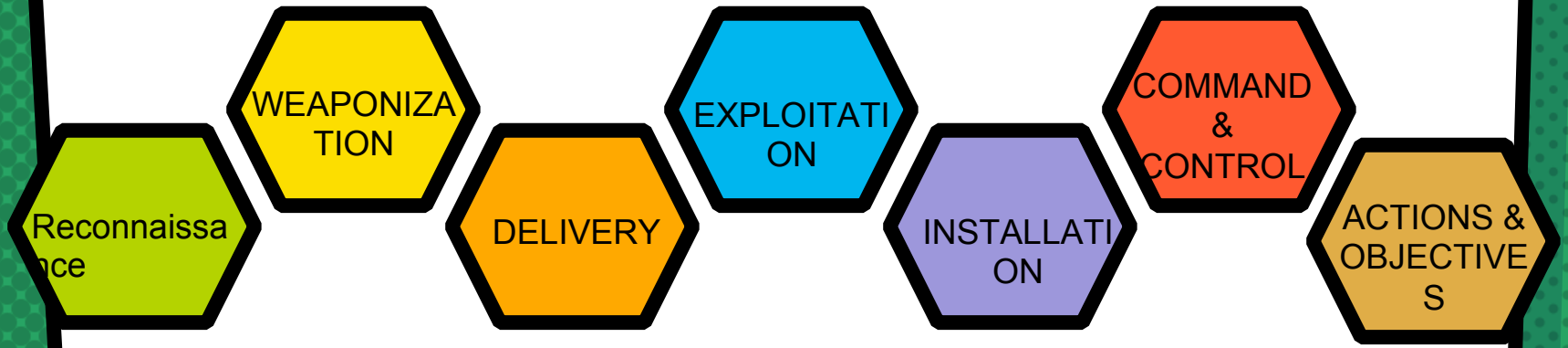
INSTALLATION

COMMAND & CONTROL

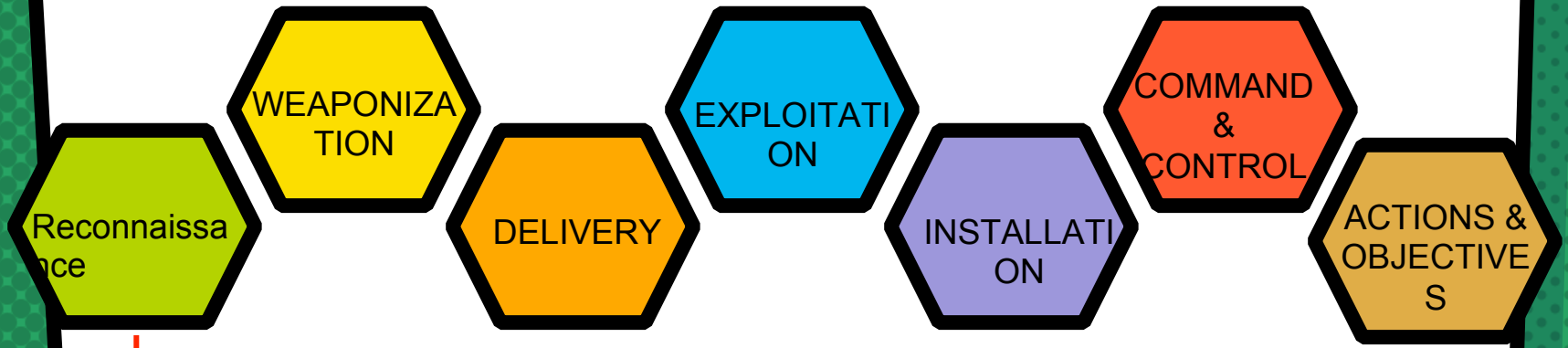
ACTIONS & OBJECTIVES


INTEL-DRIVEN CNL
Reconnaissa
nce
WEAPONIZA
TION
DELIVERY
EXPLOITATI
ON
INSTALLATI
ON
COMMAND
&
CONTROL
ACTIONS &
OBJECTIVE
S

“~~Estrictamente SECRETO Y~~
CONFIDENCIAL.PDF.JAR”

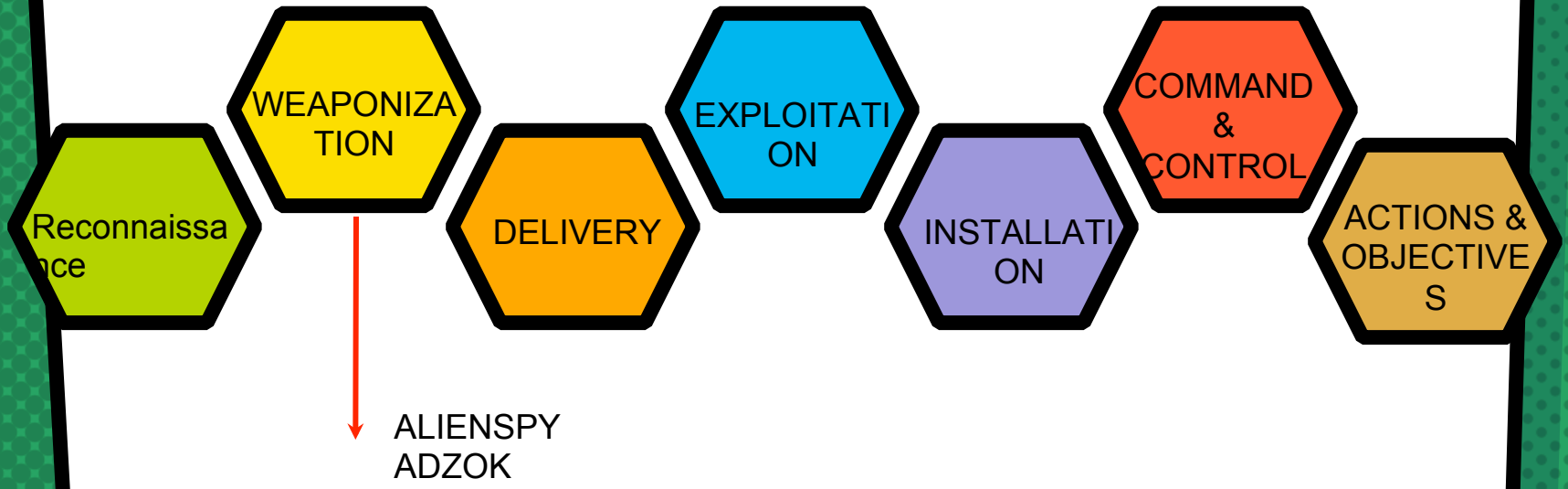


“Estrictamente SECRETO Y CONFIDENCIAL.PDF.JAR”

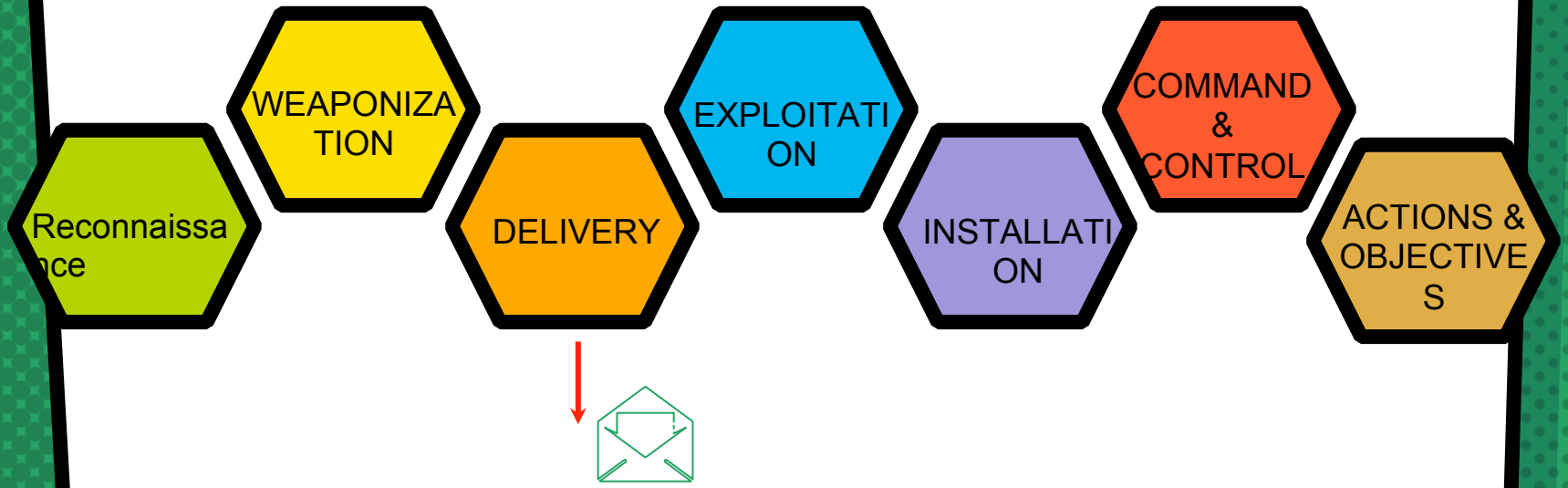


Políticos, JUECES Y Periodistas
Documentos a fines

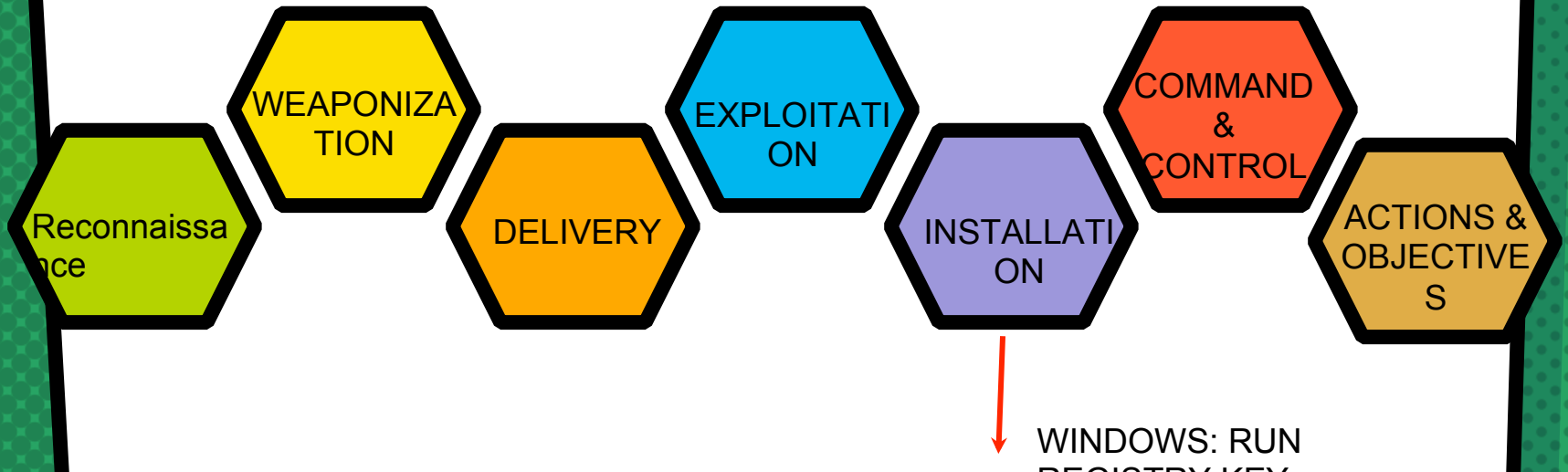
“Estrictamente SECRETO Y CONFIDENCIAL.PDF.JAR”



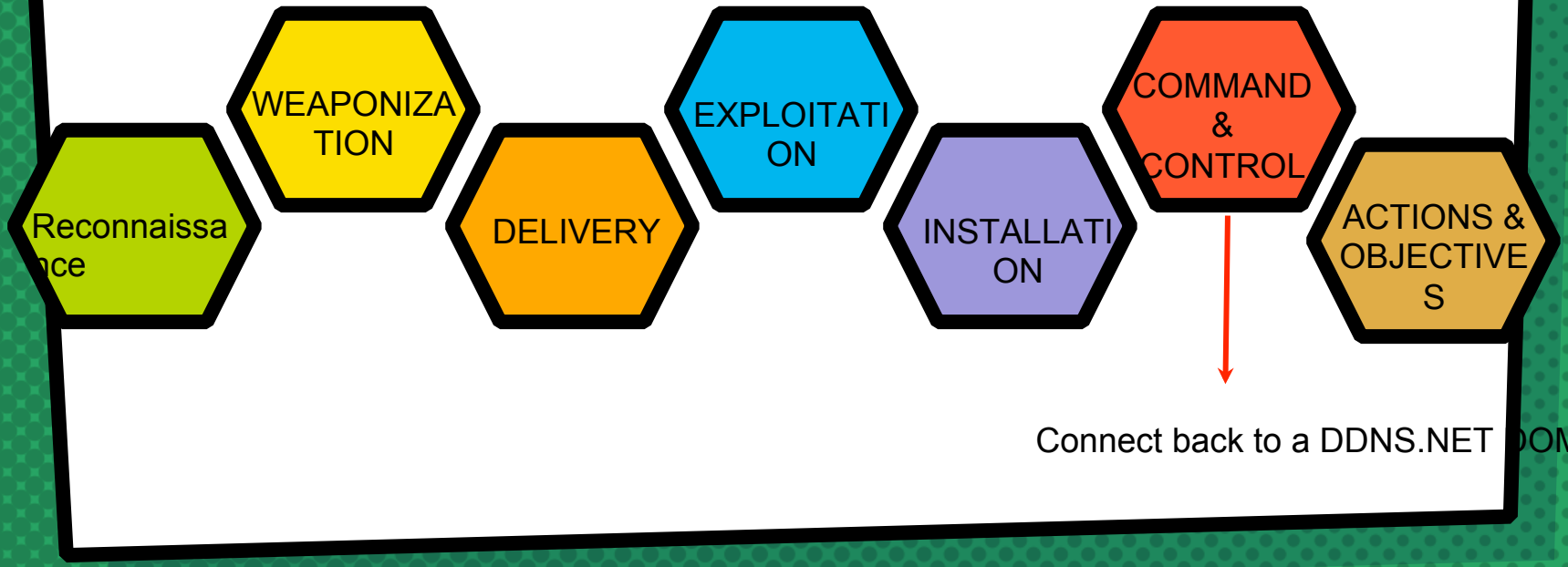
“Estrictamente SECRETO Y CONFIDENCIAL.PDF.JAR”



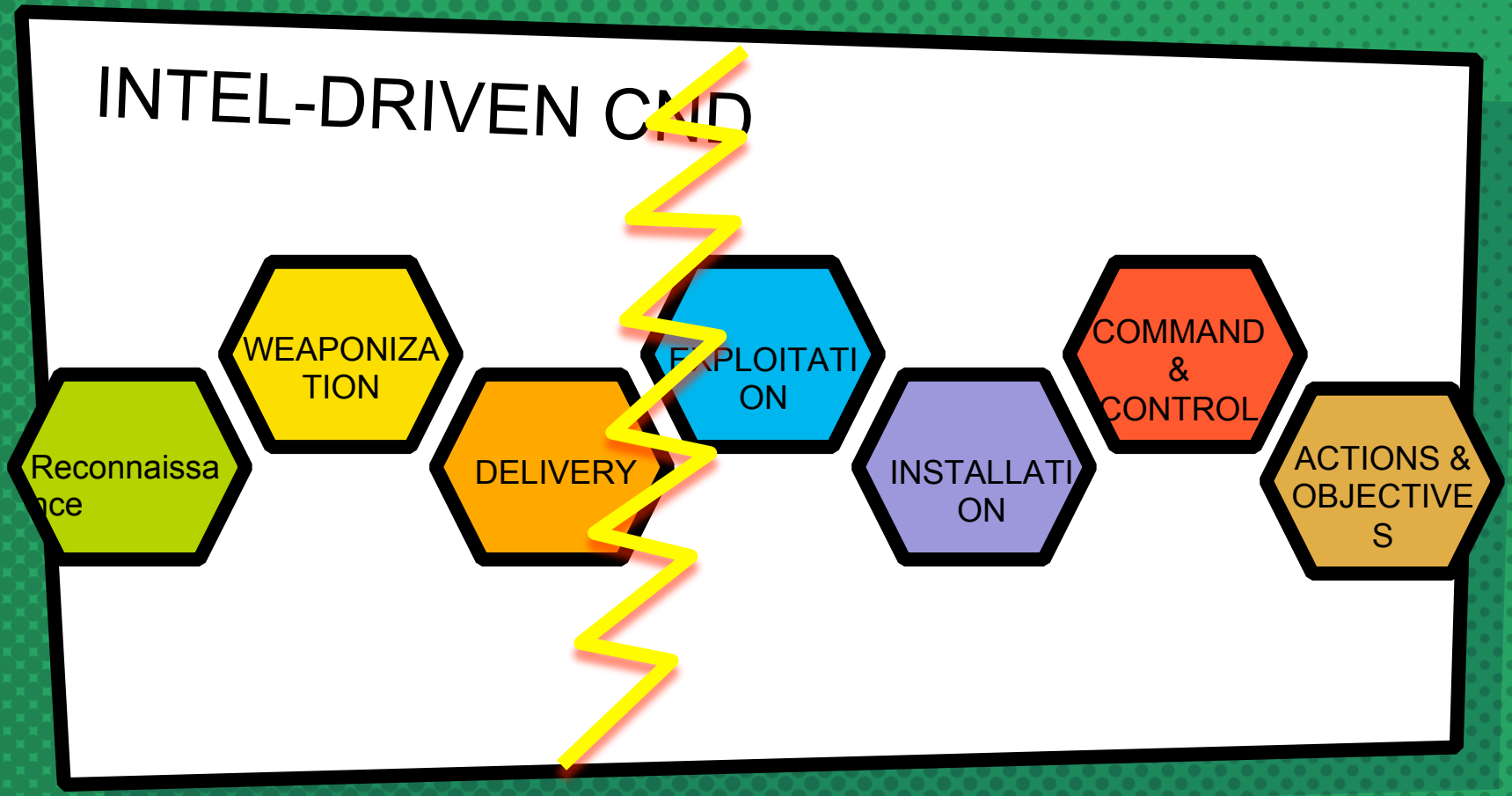
“Estrictamente SECRETO Y CONFIDENCIAL.PDF.JAR”



“Estrictamente SECRETO Y CONFIDENCIAL.PDF.JAR”



EL PERÍMETRO SON LOS PADRES


INTEL-DRIVEN CND
Reconnaissa
nce
WEAPONIZA
TION
DELIVERY
EXPLOITATI
ON
INSTALLATI
ON
COMMAND
&
CONTROL
ACTIONS &
OBJECTIVE
S

ior Enterprise

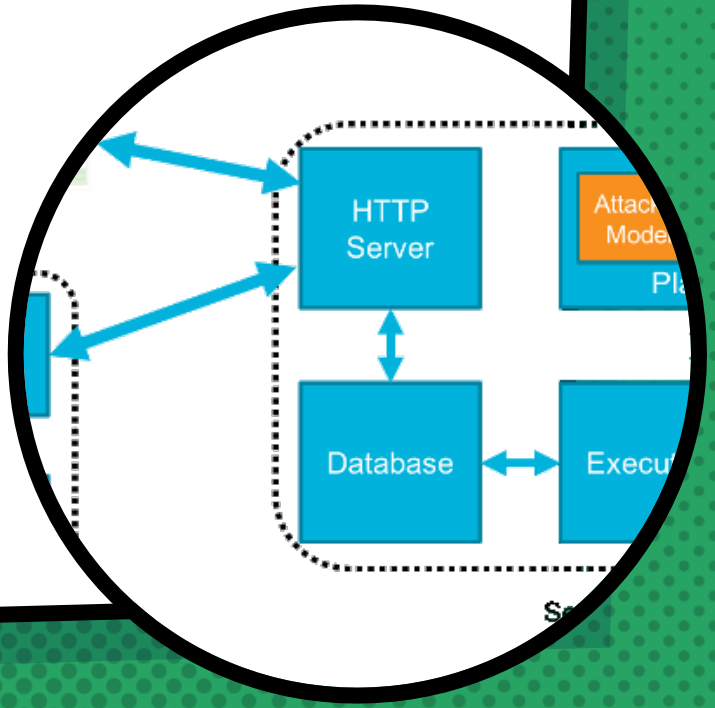
below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C C
AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Co
CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Co Th M
Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Co
Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Cu Co
Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Cu Pr
Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Da
Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Da
Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Da
Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fa
InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		M
LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		
hctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		

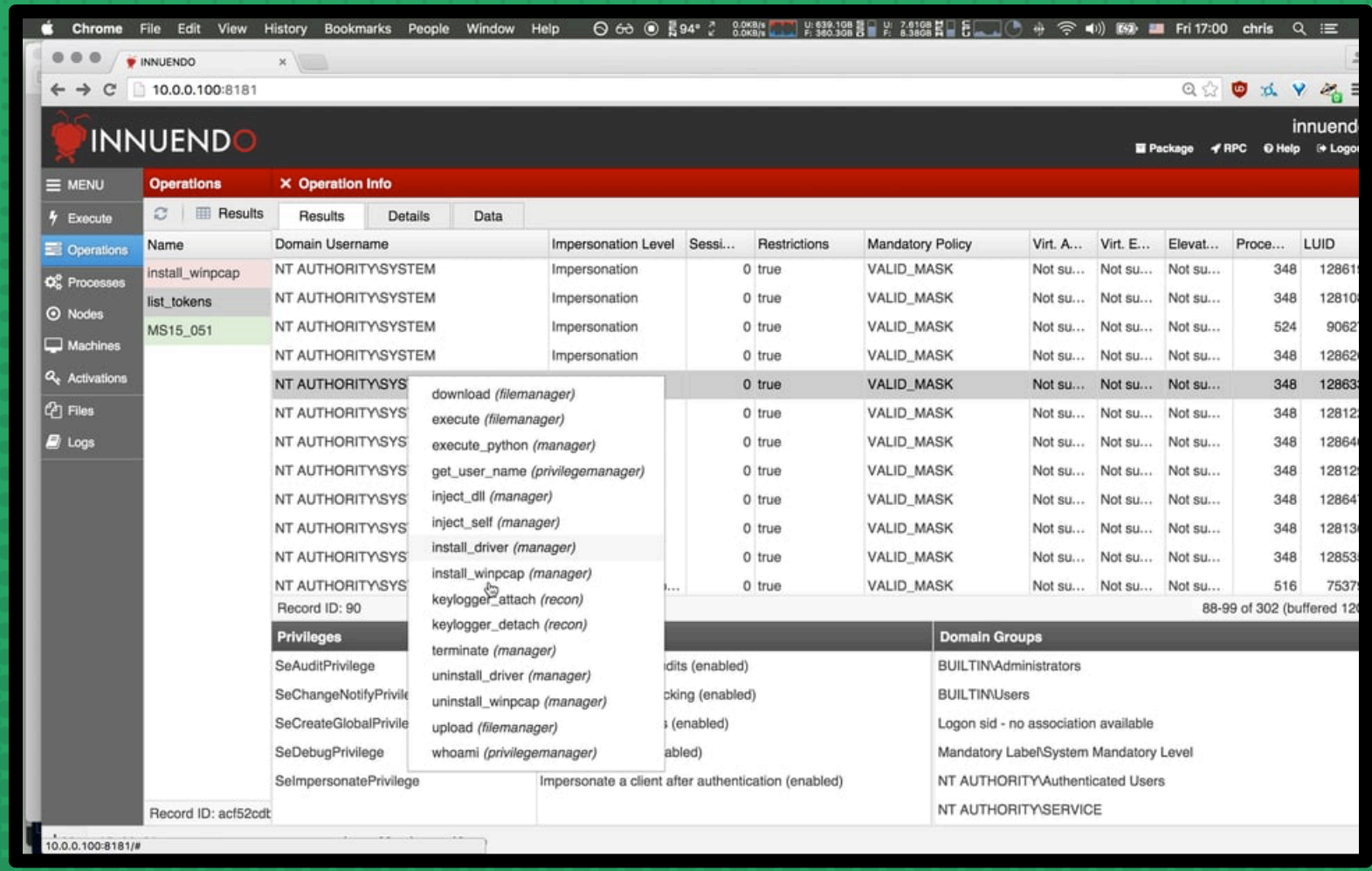
Source: Ivan Ristic Bl

INVOKE-ADVERSARY

MITRE CALDERA



EL ATAQUE EMPIEZA DONDE TERMINA EL CHECKLIST


Chrome File Edit View History Bookmarks People Window Help
Fri 17:00 chris
INNUENDO
10.0.0.100:8181
INNUENDO
innuend
Package RPC Help Logo
MENU
Execute
Operations
Processes
Nodes
Machines
Activations
Files
Logs
Operations
Operation Info
Results
Results Details Data
Name
install_winpcap
list_tokens
MS15_051
Record ID: acf52cdb
Domain Username Impersonation Level Sessi... Restrictions Mandatory Policy Virt. A... Virt. E... Elevat... Proce... LUID
NT AUTHORITY\SYSTEM Impersonation 0 true VALID_MASK Not su... Not su... Not su... 348
NT AUTHORITY\SYSTEM Impersonation 0 true VALID_MASK Not su... Not su... Not su... 348
NT AUTHORITY\SYSTEM Impersonation 0 true VALID_MASK Not su... Not su... Not su... 524
NT AUTHORITY\SYSTEM Impersonation 0 true VALID_MASK Not su... Not su... Not su... 348
NT AUTHORITY\SYS 0 true VALID_MASK Not su... Not su... Not su... 348
download (filemanager)
execute (filemanager)
execute_python (manager)
get_user_name (privilegemanager)
inject_dll (manager)
inject_self (manager)
install_driver (manager)
install_winpcap (manager)
keylogger_attach (recon)
keylogger_detach (recon)
terminate (manager)
uninstall_driver (manager)
uninstall_winpcap (manager)
upload (filemanager)
whoami (privilegemanager)
Record ID: 90
88-99 of 302 (buffered 12
Privileges
SeAuditPrivilege
SeChangeNotifyPrivile
SeCreateGlobalPrivile
SeDebugPrivilege
SeImpersonatePrivilege
Impersonate a client after authentication (enabled)
Domain Groups
BUILTIN\Administrators
BUILTIN\Users
Logon sid - no association available
Mandatory Label\System Mandatory Level
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SERVICE
10.0.0.100:8181/#


SHARK
REPELLENT
BATMAN
BATMAN
1/4TH SCALE COLLECTIBLE FIGURE
WB SHIELD: TM & © Warner

Gracias!

nico@immunityinc.com

(WE ARE HIRING!!)