HoneyCON
By HoneySec

ZEROLYNX

RED (S)TEAM

Diego León
Juan Antonio Calles

$> whoami

- Diego León
- Grado en Informática y Postgrado en Ciberseguridad
- Responsable de Seguridad Ofensiva de ZEROLYNX

OSANE CONSULTING

ZEROLYNX

OFFENSIVE security OSCP

C|EH Certified Ethical Hacker

$> whoami

- Juan Antonio Calles
- Doctor, Doble Postgrado e Ingeniero en Informática
- CEO de ZEROLYNX

OSANE CONSULTING

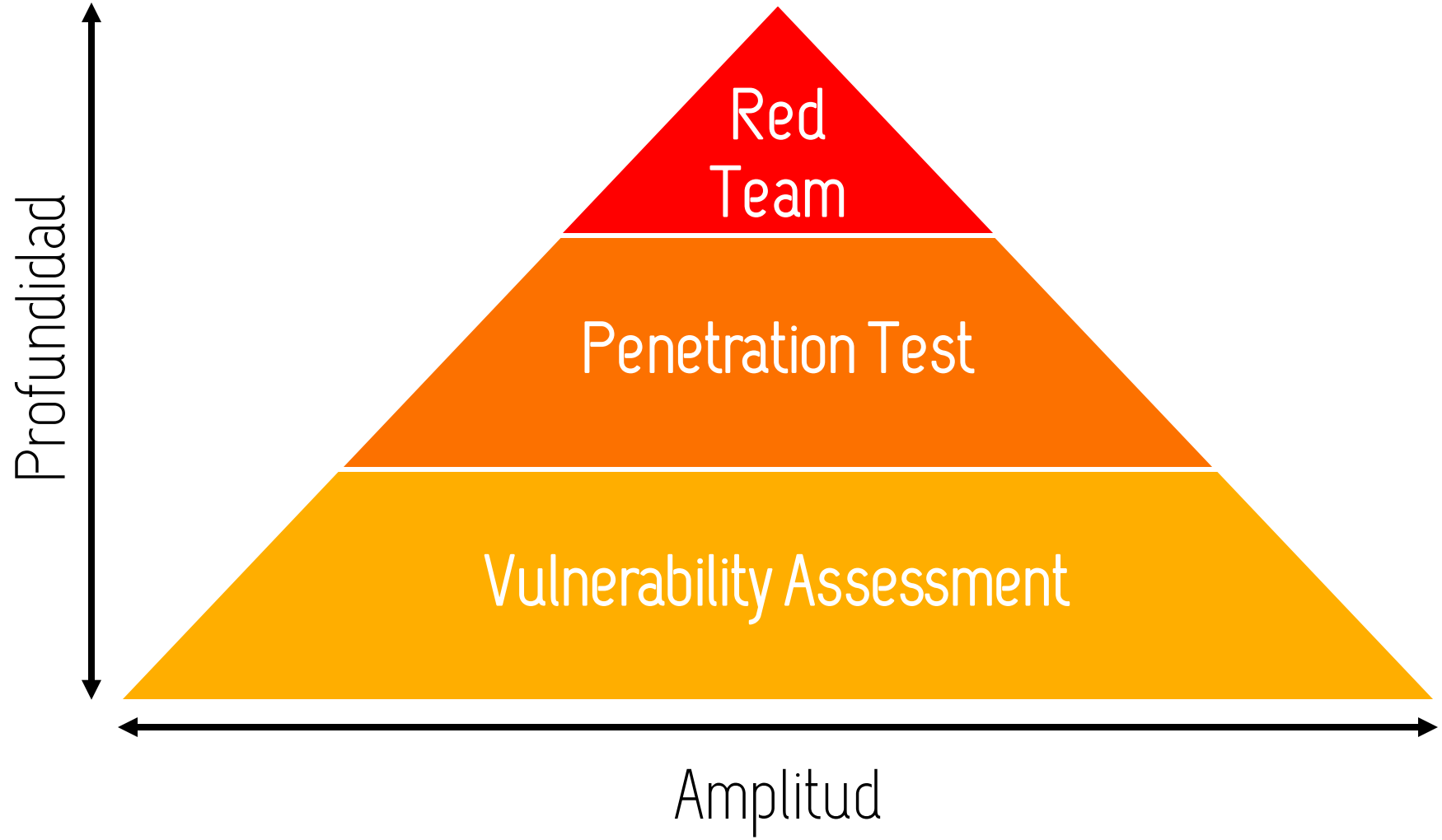
ZEROLYNX

internet para todos
X1 REDMASSEGURA

Índice de contenidos

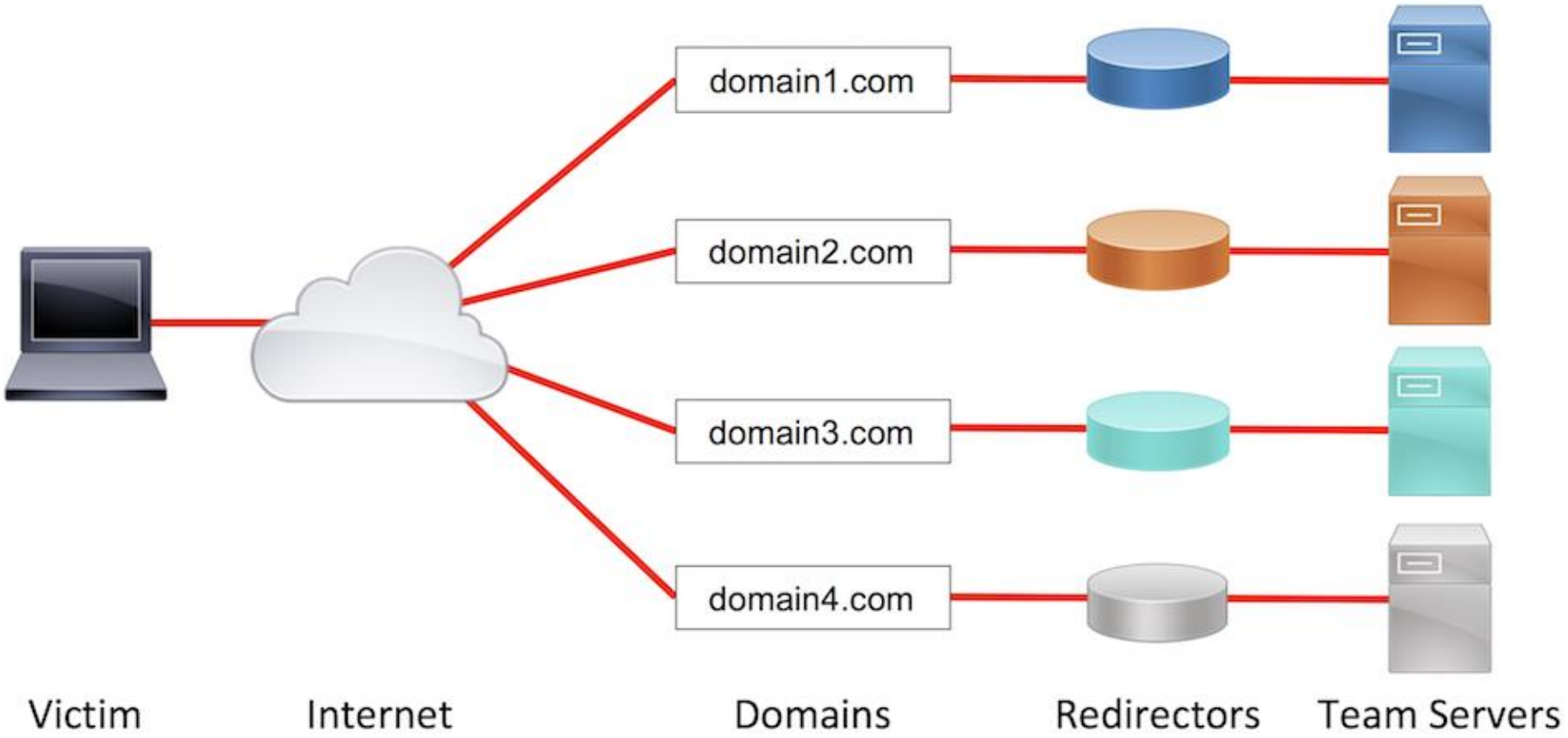
Ethical Hacking services

¿Tiempo infinito?
¿Alcance?



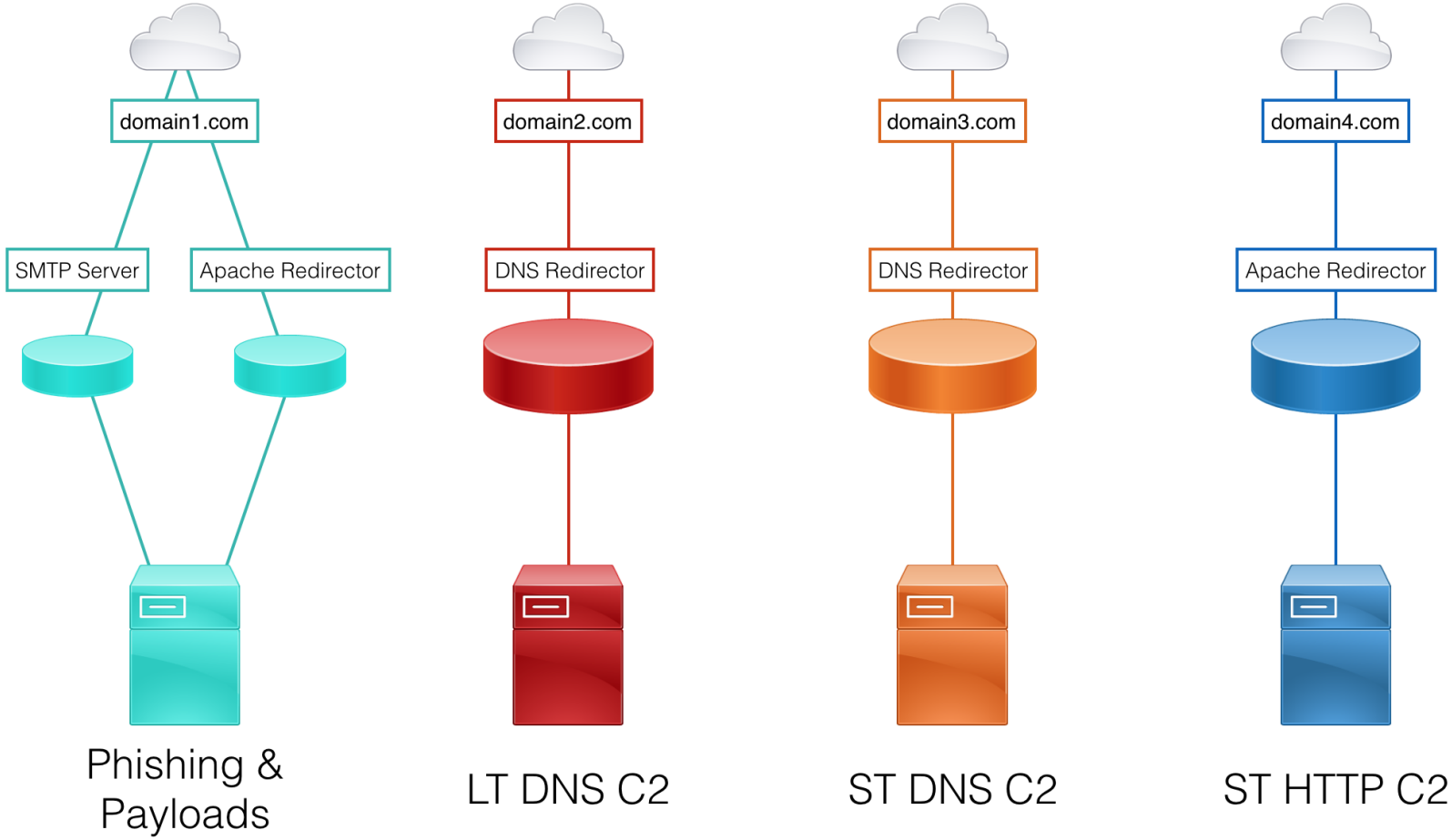
Índice de contenidos

Smoke…



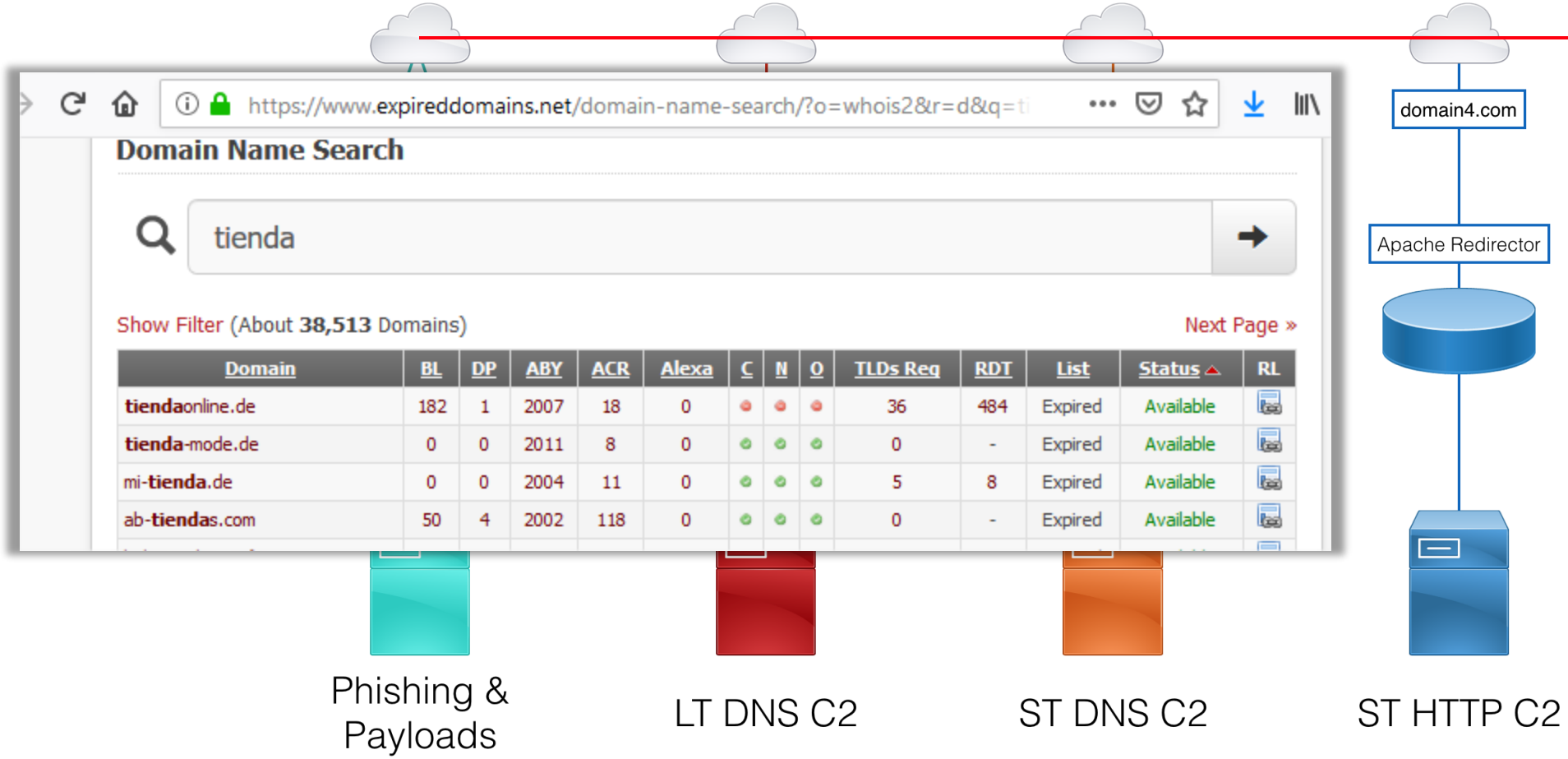
@Bluescreenofjeff (Jeff Dimmock's)

And more smoke…



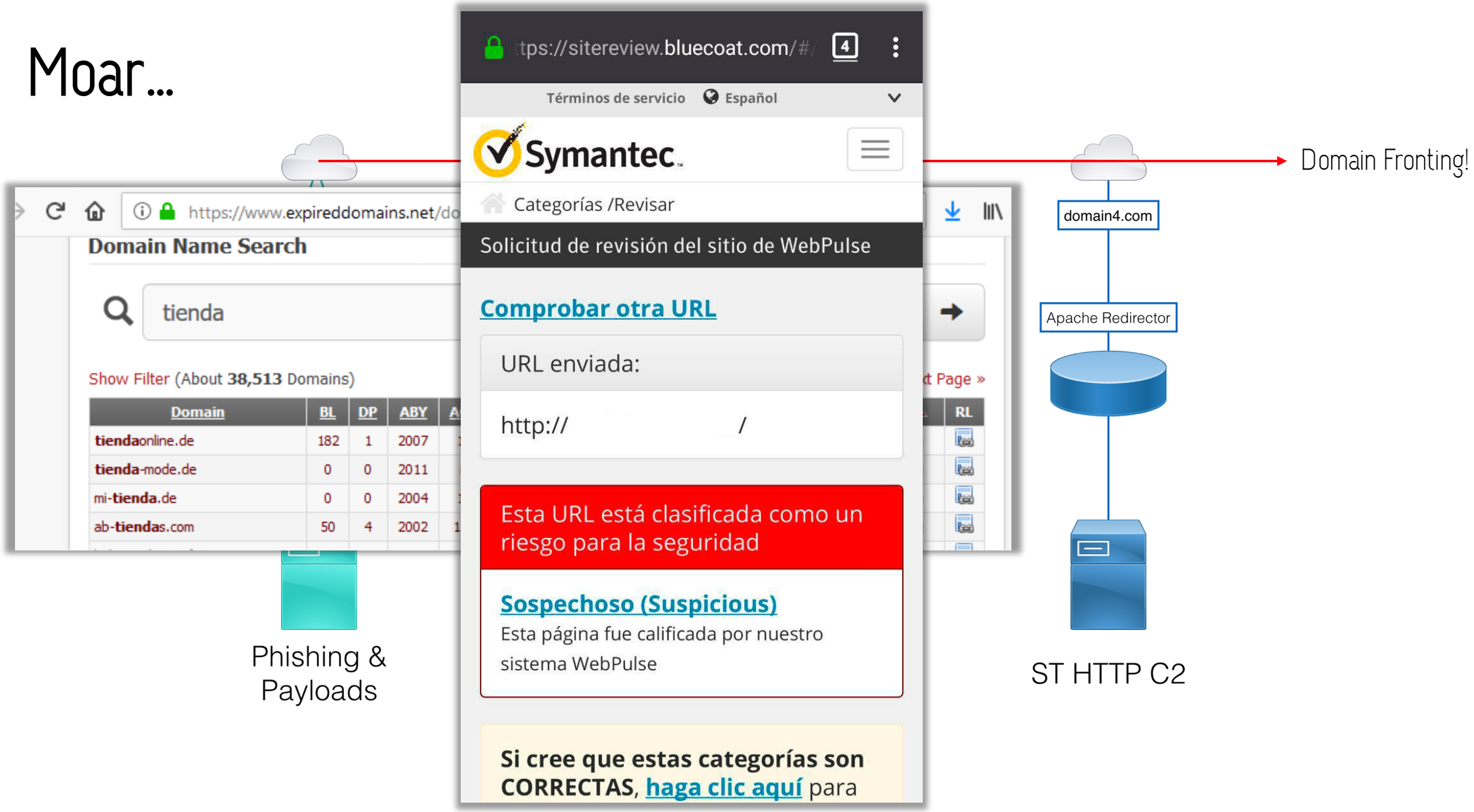
@Bluescreenofjeff (Jeff Dimmock's)

Moar...



@Bluescreenofjeff (Jeff Dimmock's)

Moar...


https://www.expireddomains.net/do
Domain Name Search
tienda
Show Filter (About 38,513 Domains)
Domain
BL
DP
ABY
tiendaonline.de
182
1
2007
tienda-mode.de
0
0
2011
mi-tienda.de
0
0
2004
ab-tiendas.com
50
4
2002
Phishing & Payloads
tps://sitereview.bluecoat.com/#/
Términos de servicio
Español
Symantec
Categorías /Revisar
Solicitud de revisión del sitio de WebPulse
Comprobar otra URL
URL enviada:
http://
/
Esta URL está clasificada como un riesgo para la seguridad
Sospechoso (Suspicious)
Esta página fue calificada por nuestro sistema WebPulse
Si cree que estas categorías son CORRECTAS, haga clic aquí para
Domain Fronting!
domain4.com
Apache Redirector
ST HTTP C2

Moar...

Si cree que estas categorías son CORRECTAS, haga clic aquí para obtener más información sobre su política de acceso a Internet.
Si cree que estas categorías son INCORRECTAS, complete el formulario a continuación para que se revise la URL.

Servicio de filtrado:

Seleccione uno

Requerido

Su categoría o categorías sugeridas (leer descripciones):

Seleccione una categoría

Requerido

Seleccione una categoría

☐ **Enviar los resultados de la revisión por correo electrónico**

Comentarios y descripción del sitio *(proporcione tantos detalles como sea posible)*:

Enviar para revisión

Moar...

Phishing & Payloads

Sus comentarios: [redacted]

Revisado: [redacted] 2018

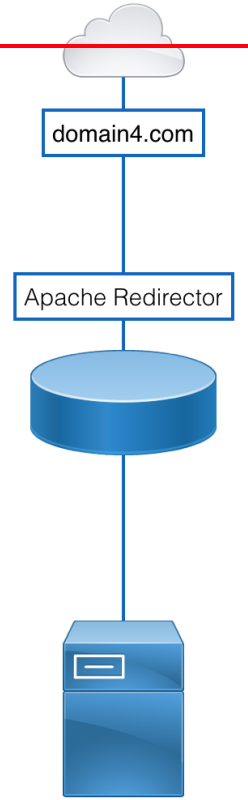
Según su recomendación y después de una evaluación cuidadosa del contenido web enviado, un analista de contenido web ha recategorizado esta URL como Tecnología/Internet.

Gracias,

El equipo de WebFilter de Blue Coat
filtering@bluecoat.com

Symantec + BLUE COAT

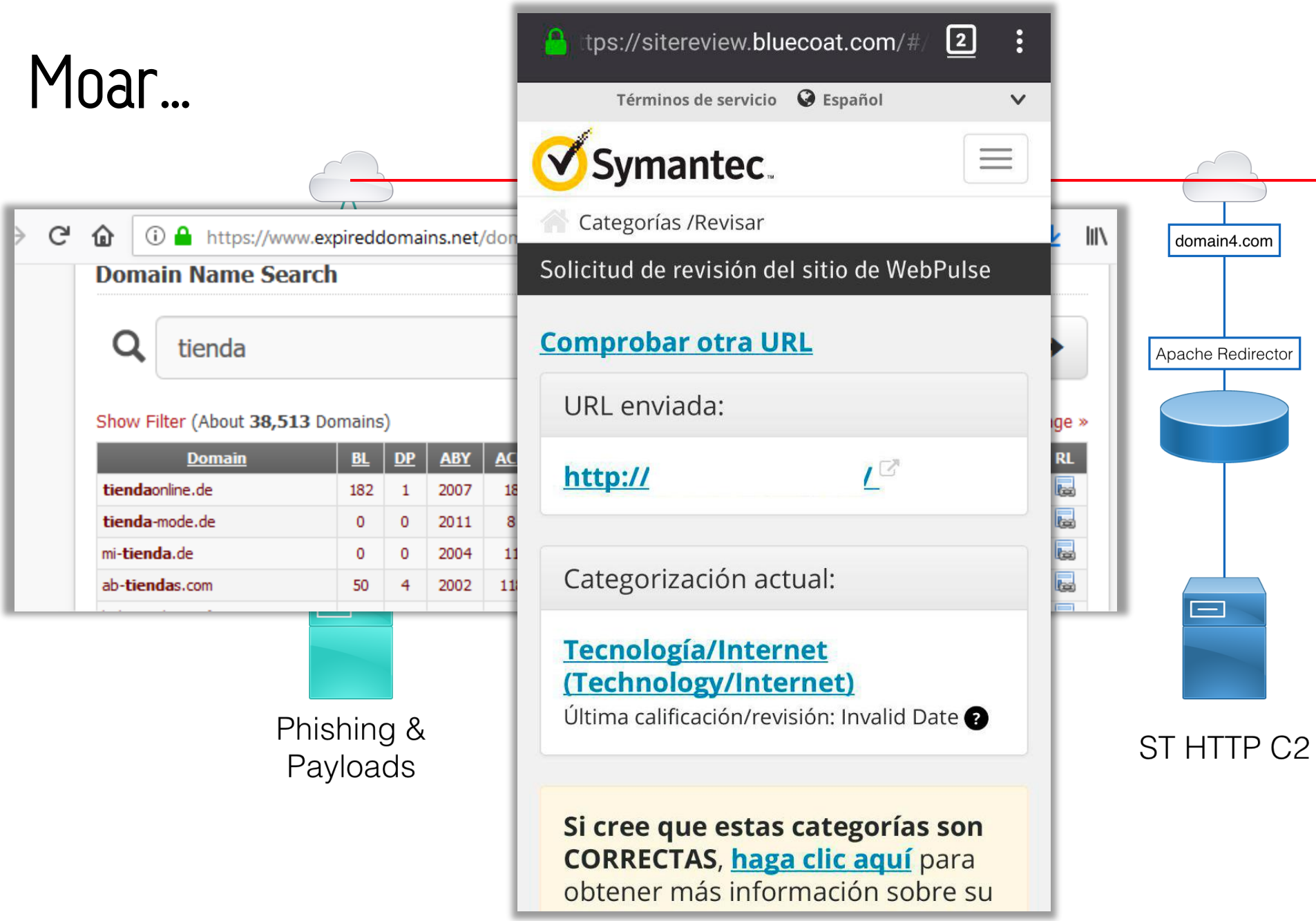
Es importante tener en cuenta que las nuevas categorizaciones forman parte de un ciclo de actualización diario proporcionado por Blue Coat, pero que los clientes de Blue Coat deben decidir con qué frecuencia actualizan su base de datos de categorización. WebFilter de Blue Coat no conoce la programación de actualización para sus clientes. Para obtener más información, haga clic aquí.



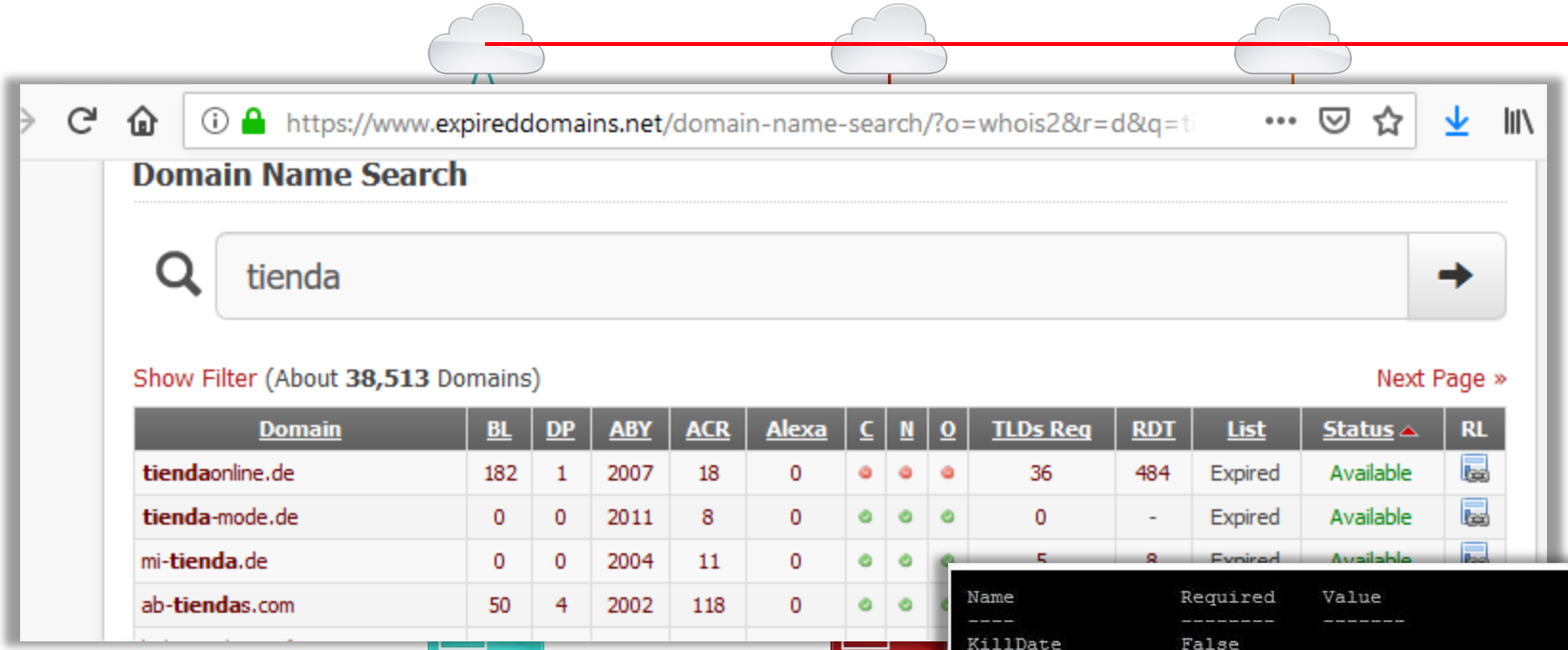
ST HTTP C2

Domain Fronting!

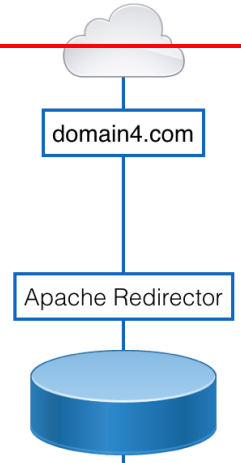
Moar...


https://www.expireddomains.net/don
Domain Name Search
tienda
Show Filter (About 38,513 Domains)
Domain
BL
DP
ABY
tiendaonline.de
182
1
2007
tienda-mode.de
0
0
2011
mi-tienda.de
0
0
2004
ab-tiendas.com
50
4
2002
tps://sitereview.bluecoat.com/#/
Términos de servicio
Español
Symantec
Categorías /Revisar
Solicitud de revisión del sitio de WebPulse
Comprobar otra URL
URL enviada:
http://
/
Categorización actual:
Tecnología/Internet (Technology/Internet)
Última calificación/revisión: Invalid Date
Si cree que estas categorías son CORRECTAS, haga clic aquí para obtener más información sobre su
Phishing & Payloads
domain4.com
Apache Redirector
ST HTTP C2
Domain Fronting!

Moar...



Domain Fronting!



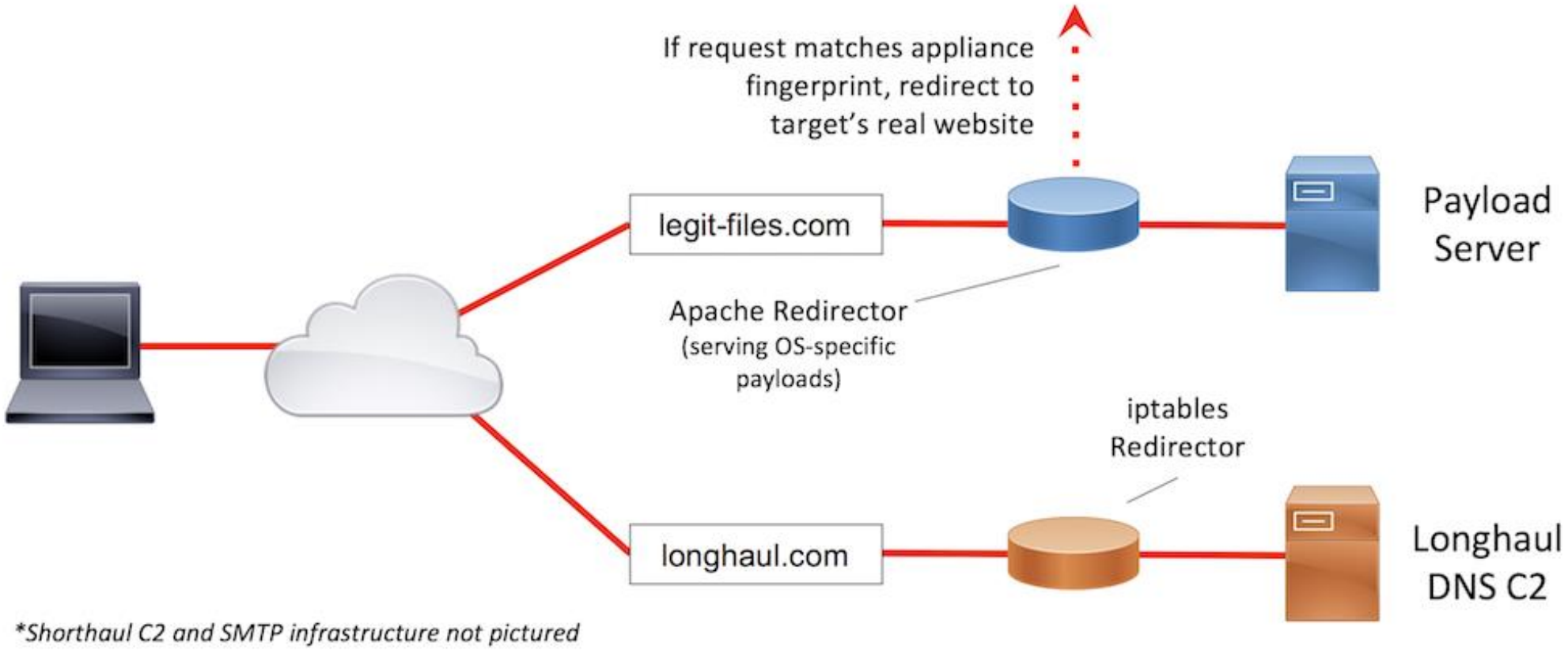
Phishing & Payloads

LT DNS (

@Bluescree

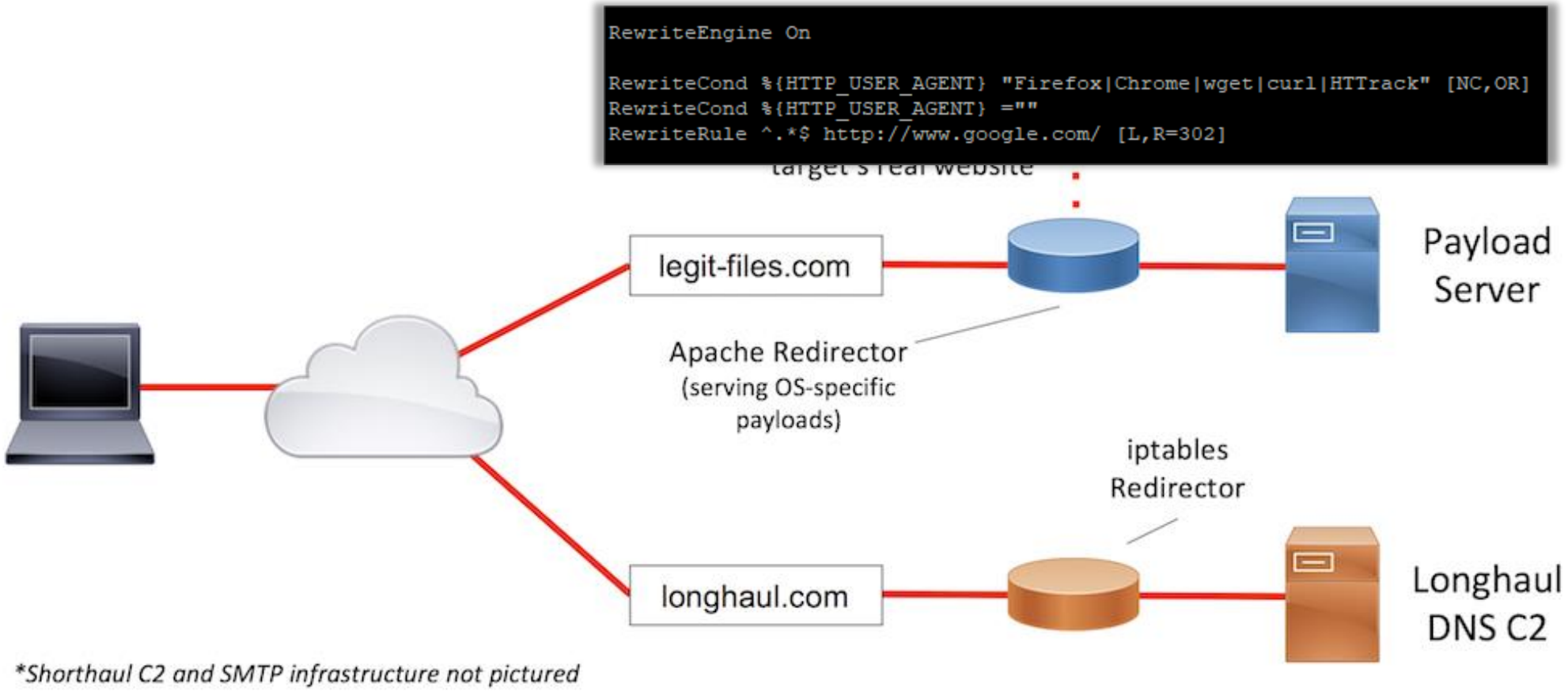
```
Name            Required    Value                          Description
----            --------    -------                        -----------
KillDate        False                                      Date for the listener to exit (MM/dd/yyyy).
Name            True        http                           Name for the listener.
Launcher        True        powershell -noP -sta -w 1 -enc Launcher string.
DefaultLostLimit True       60                             Number of missed checkins before exiting
StagingKey      True        aVEcl?!&]oTz8S*xHI~tKw2X}=^+jR@s Staging key for initial agent negotiation.
BindIP          True        0.0.0.0                        The IP to bind to on the control server.
DefaultProfile  True        /admin/get.php,/news.asp,/login/ Default communication profile for the agent.
                            process.jsp|Mozilla/5.0 (Windows
                            NT 6.1; WOW64; Trident/7.0;
                            rv:11.0) like Gecko|Host:
                            [redacted].cloudfront.net
ServerVersion   True        Apache                         Server header for the control server.
WorkingHours    False                                      Hours for the agent to operate (09:00-17:00).
Host            True        http://d0.awsstatic.com:80     Hostname/IP for staging.
CertPath        False                                      Certificate path for https listeners.
DefaultJitter   True        0.0                            Jitter in agent reachback interval (0.0-1.0).
DefaultDelay    True        5                              Agent delay/reach back interval (in seconds).
Port            True        80                             Port for the listener.
```

...plz stop.



@Bluescreenofjeff (Jeff Dimmock's)

…plz stop.



@Bluescreenofjeff (Jeff Dimmock's)

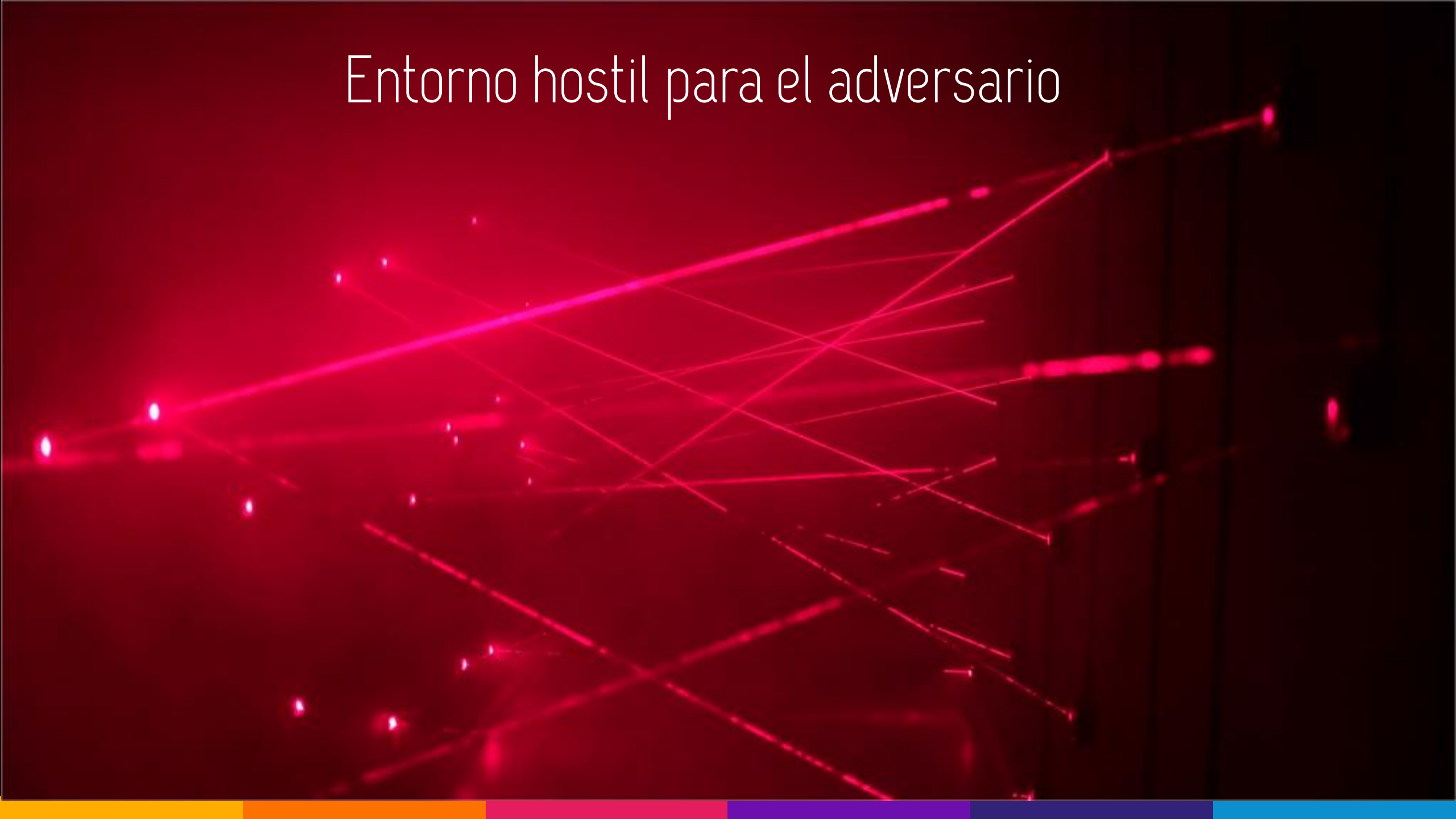
La dura realidad

Índice de contenidos

Seguridad Perimetral

Seguridad Perimetral

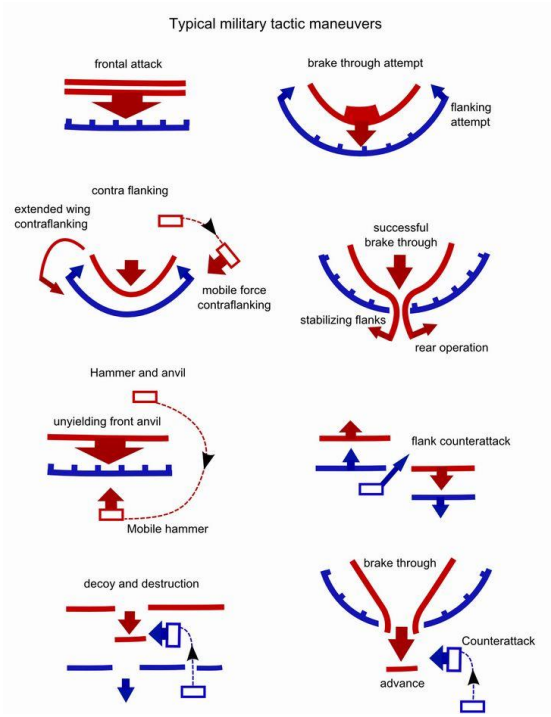
Entorno hostil para el adversario



Índice de contenidos

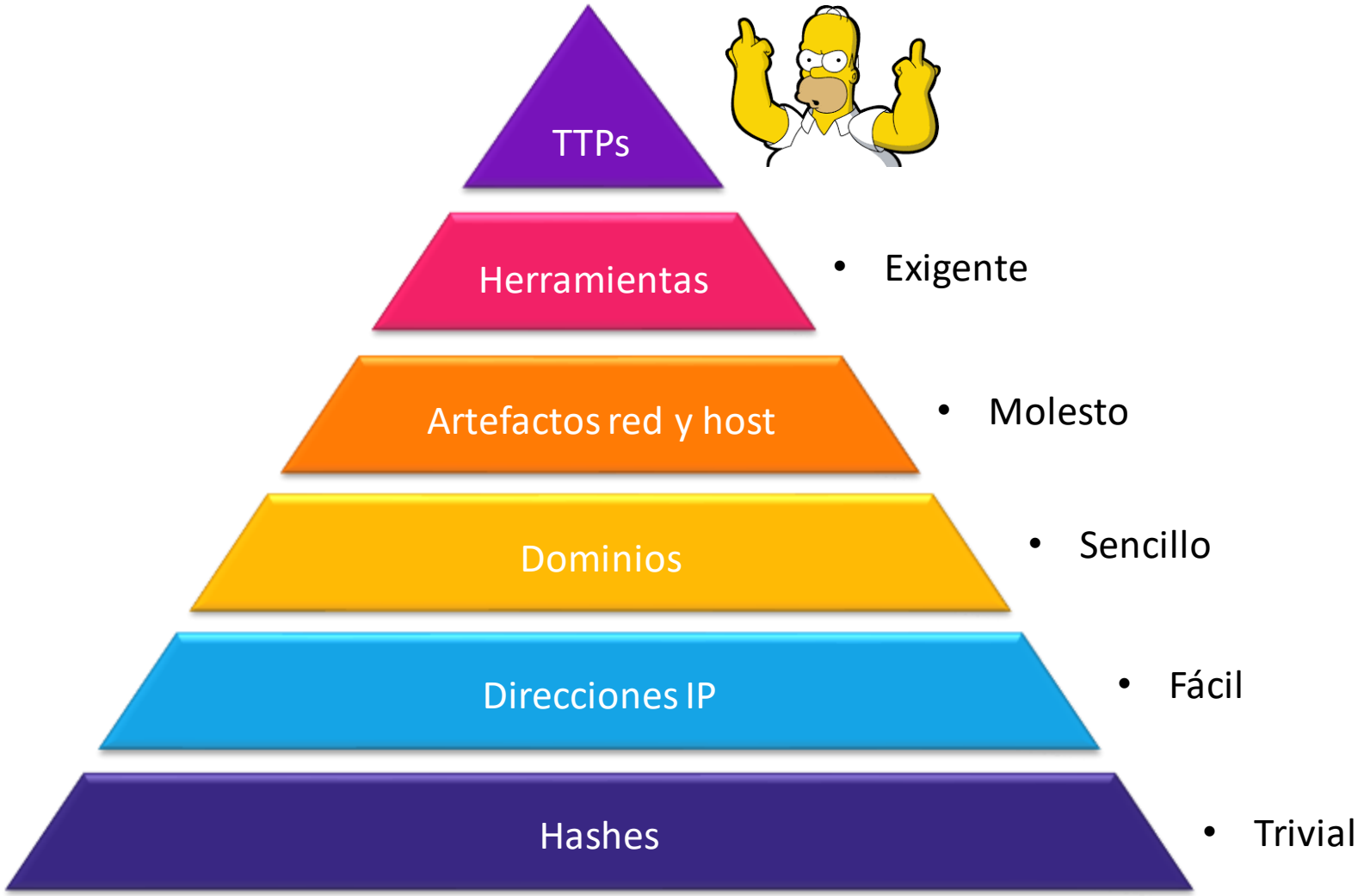
Simulación de Adversarios

TTP: Tácticas, técnicas y procedimientos



Concepto de origen militar: modeliza el comportamiento del adversario

Pyramid Of Pain: ¿cómo dificultar el trabajo al enemigo?



MITRE ATT&CK: modela el comportamiento de adversarios

Incluye técnicas de las diferentes etapas de la cadena de ataque:

Acceso Inicial, Ejecución, Persistencia, Escalada de Privilegios, etc.

PRE-ATT&CK™

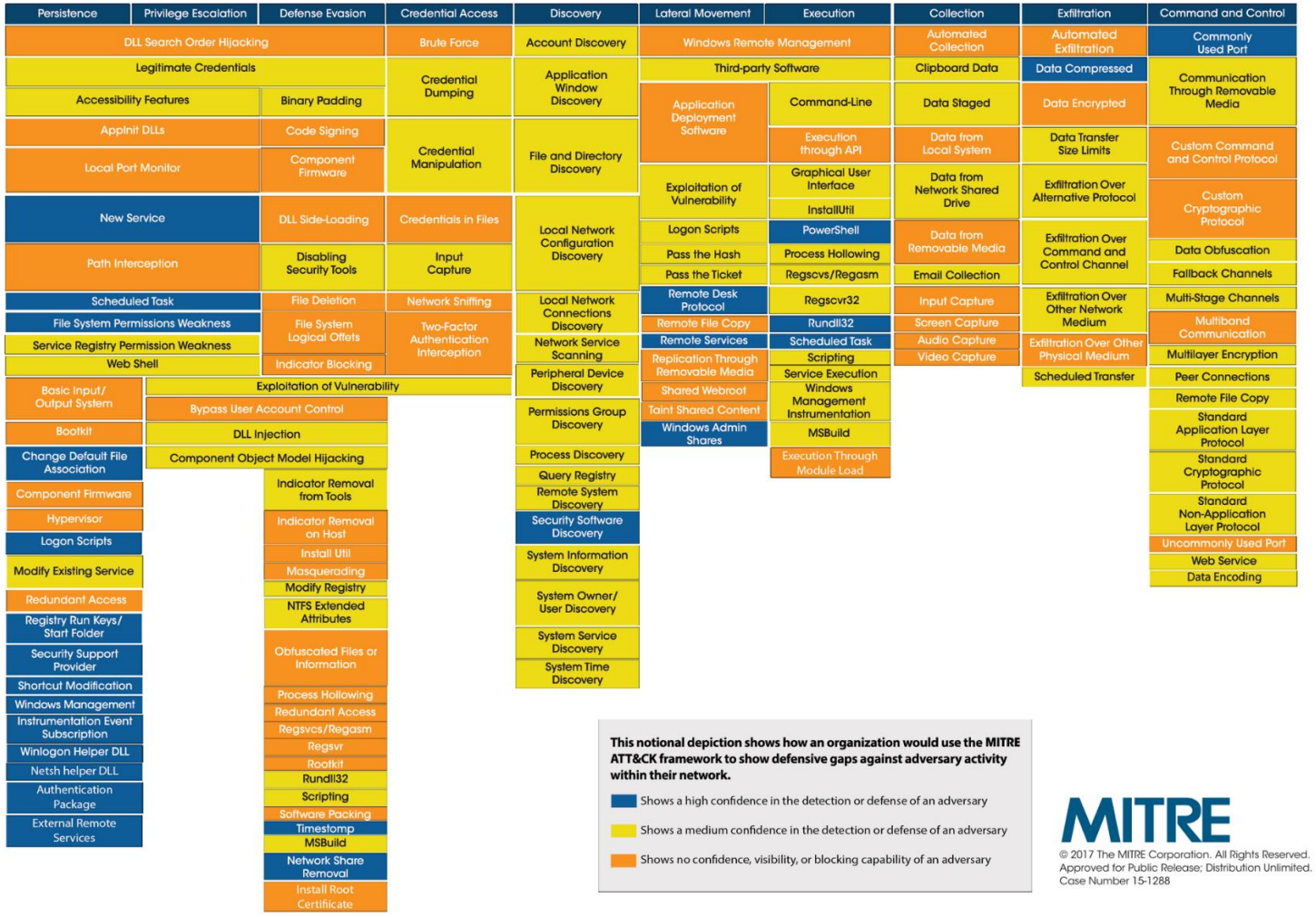
How is the adversary targeting you?

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	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	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

Heat Maps: Permite identificar las fortalezas y debilidades de nuestra organización



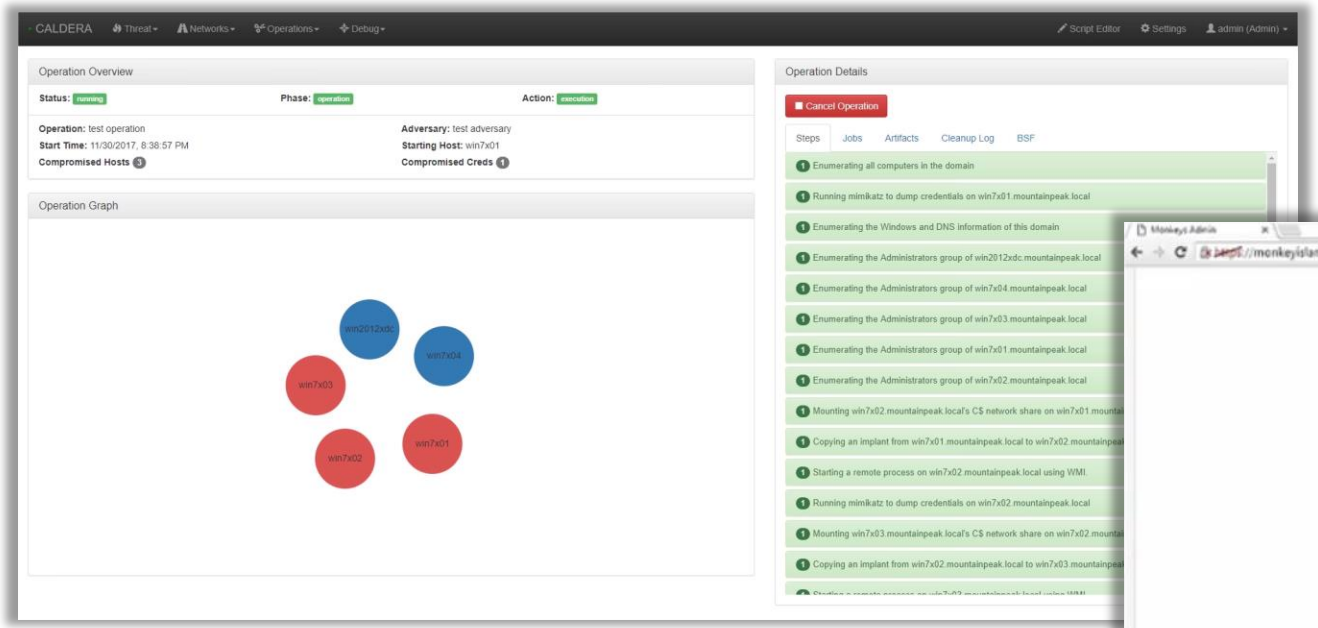
Heat Maps: permiten simular adversarios concretos

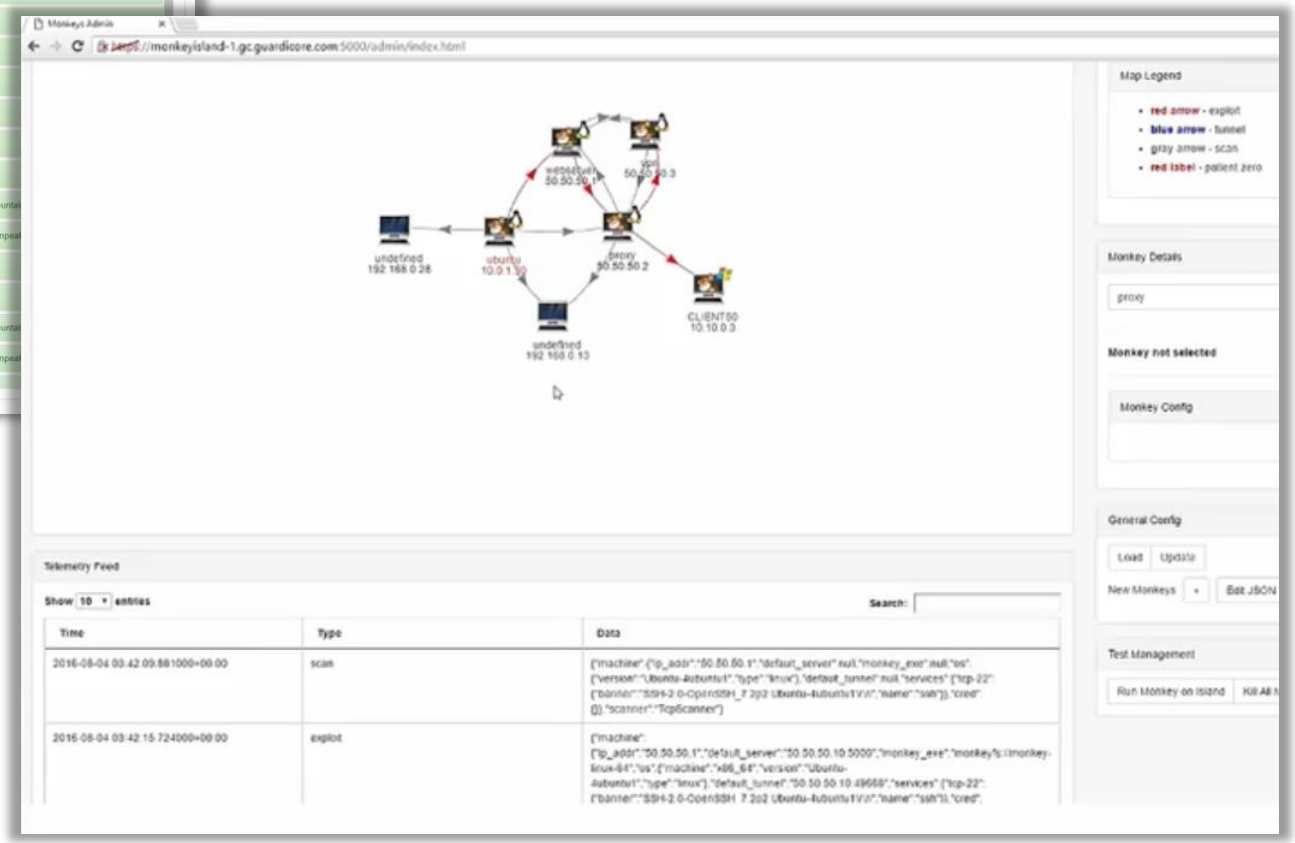
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Application Shimming	Audio Capture	Automated Exfiltration	Commonly Used Port
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Exploitation of Vulnerability	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account	File and Directory Discovery	Logon Scripts	Execution through API	Clipboard Data	Data Encrypted	Connection Proxy
Component Object Model Hijacking	Application Shimming	Code Signing	Credential Dumping	Network Service Scanning	Pass the Hash	Execution through Module Load	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
DLL Search Order Hijacking	Bypass User Account Control	Component Firmware	Credentials in Files	Network Share Discovery	Pass the Ticket	Graphical User Interface	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
External Remote Services	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	InstallUtil	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
File System Permissions Weakness	DLL Search Order Hijacking	DLL Injection	Input Capture	Permission Groups Discovery	Remote File Copy	PowerShell	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Hidden Files and Directories	Exploitation of Vulnerability	DLL Search Order Hijacking	Network Sniffing	Process Discovery	Remote Services	Process Hollowing	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Hypervisor	File System Permissions Weakness	Disabling Security Tools	Private Keys	Query Registry	Replication Through Removable Media	Regsvcs/Regasm	Input Capture	Scheduled Transfer	Multi-Stage Channels
Local Port Monitor	Local Port Monitor	Exploitation of Vulnerability	Two-Factor Authentication Interception	Remote System Discovery	Shared Webroot	Regsvr32	Screen Capture		Multiband Communication
Logon Scripts	New Service	File Deletion		Security Software Discovery	Taint Shared Content	Rundll32	Video Capture		Multilayer Encryption
Modify Existing Service	Path Interception	File System Logical Offsets		System Information Discovery	Third-party Software	Scheduled Task			Remote File Copy
New Service	Scheduled Task	Hidden Files and Directories		System Network Configuration Discovery	Windows Admin Shares	Scripting			Standard Application Layer Protocol
Redundant Access	Service Registry Permissions Weakness	Regsvcs/Regasm		System Network Connections Discovery	Windows Remote Management	Service Execution			Standard Cryptographic Protocol
Registry Run Keys / Start Folder	Valid Accounts	Regsvr32		System Owner/User Discovery		Third-party Software			Standard Non-Application Layer Protocol
Scheduled Task	Web Shell	Rootkit		System Service Discovery		Trusted Developer Utilities			Uncommonly Used Port
Shortcut Modification		Rundll32				Windows Remote Management			
System Firmware		Scripting							
Valid Accounts		Software Packing							
Web Shell		Timestomp							
Windows Management Instrumentation Event Subscription		Trusted Developer Utilities							
Winlogon Helper DLL		Valid Accounts							

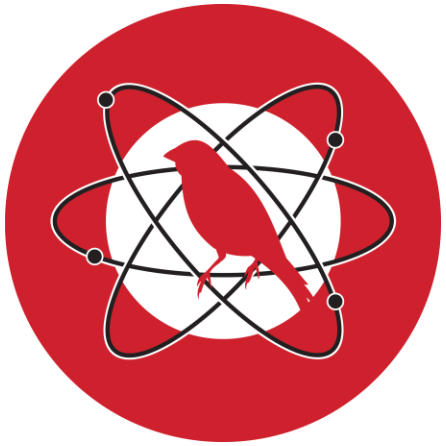
CrowdStrike Falcon-to-ATT&CK Mapping – colored cells considered relevant for Gothic Panda/APT3: Gray – not tested; Green – tested, detected; Yellow – tested, detection possible; Red – capability gaps

Índice de contenidos

Tools of the trade

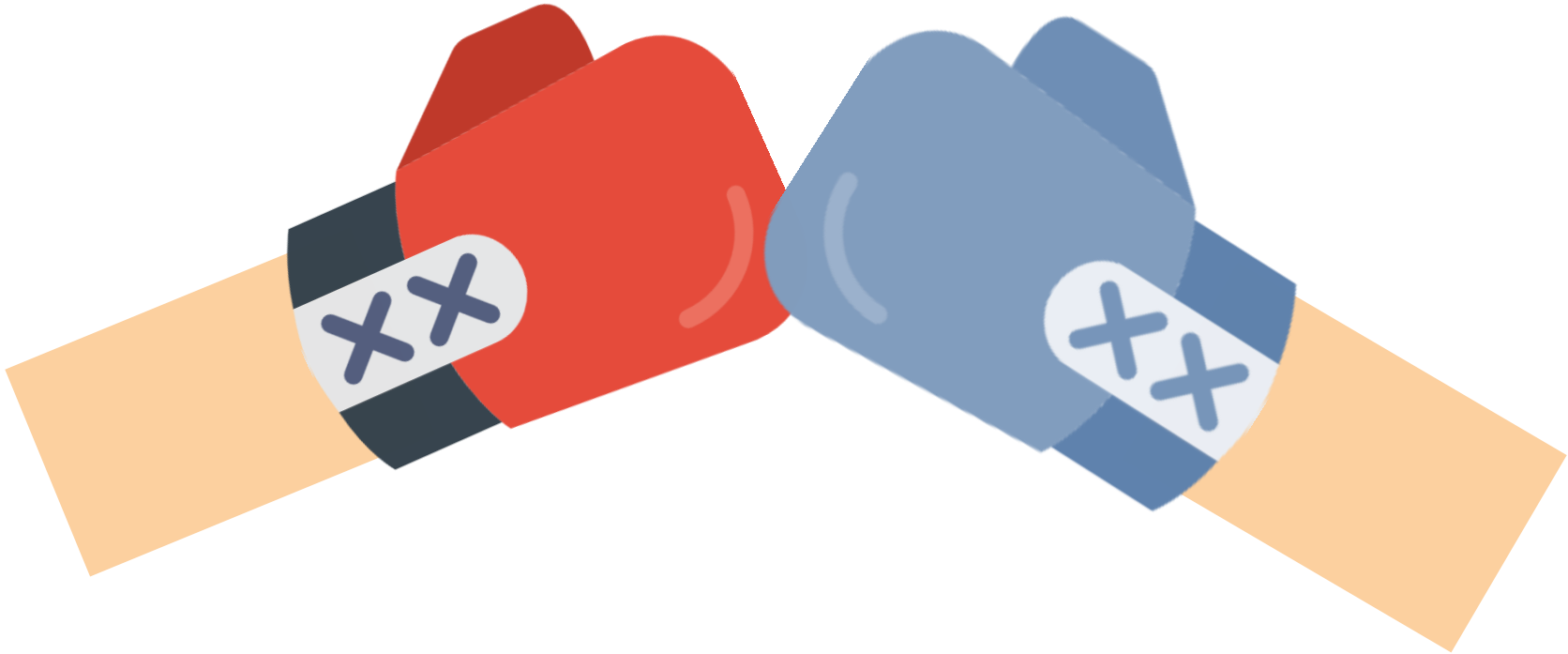


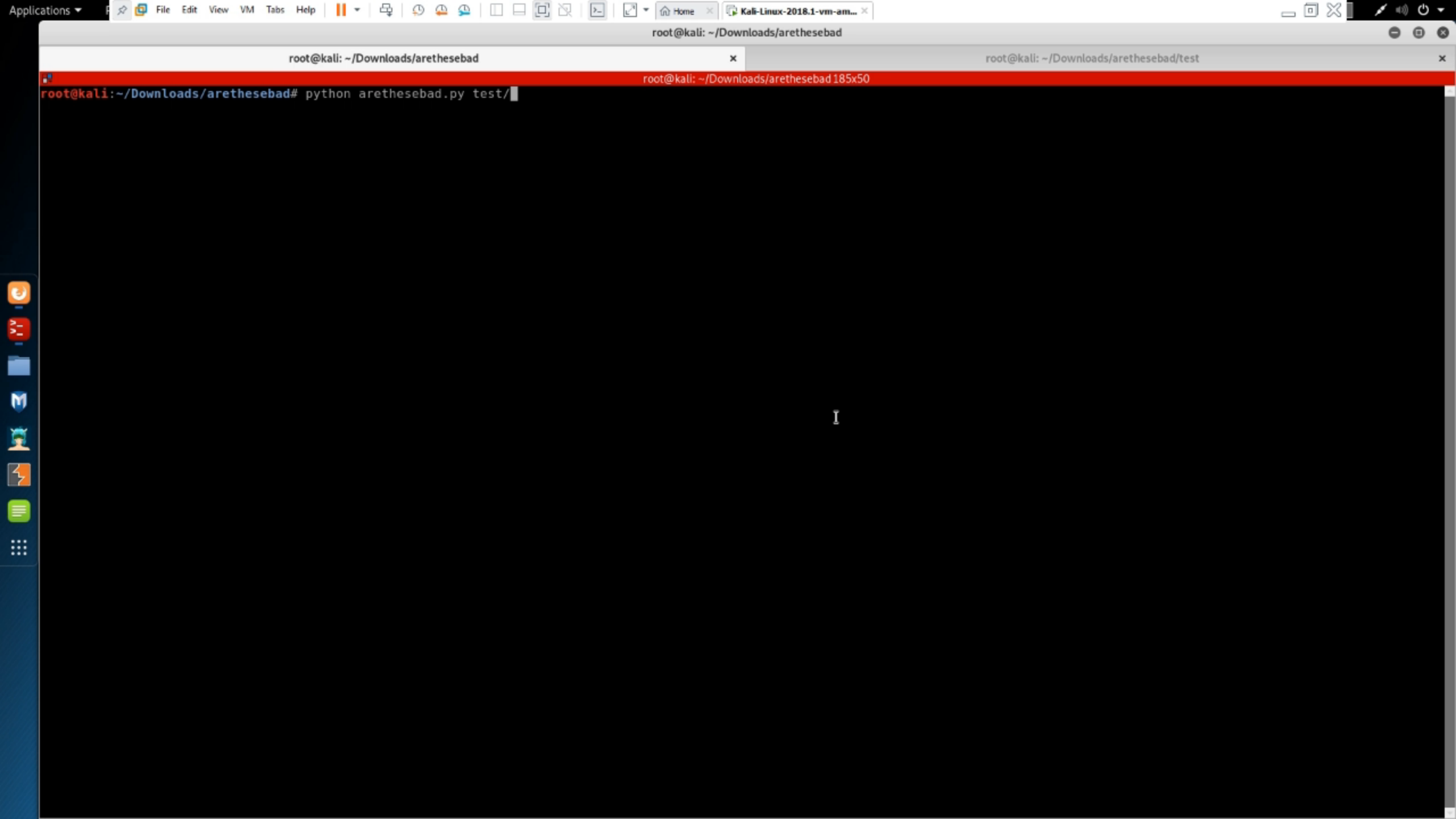




Índice de contenidos

Red Teaming




Applications
File Edit View VM Tabs Help
Home
Kali-Linux-2018.1-vm-am...
root@kali: ~/Downloads/arethesebad
root@kali: ~/Downloads/arethesebad
root@kali: ~/Downloads/arethesebad/test
root@kali: ~/Downloads/arethesebad 185x50
root@kali:~/Downloads/arethesebad# python arethesebad.py test/

Contacto

jcalles@zerolynx.com
dleon@zerolynx.com
info@zerolynx.com

@jantonioCalles
@león_krav
@ZerolynxOficial

www.zerolynx.com

www.github.com/zerolynx

www.facebook.com/zerolynx

www.linkedin.com/company/zerolynx

@ZeroLynxOficial

ZeroLynx Oficial

blog.zerolynx.com