El Misterio de las Rutas que NO Querían Morir

Crónica de un route leak real

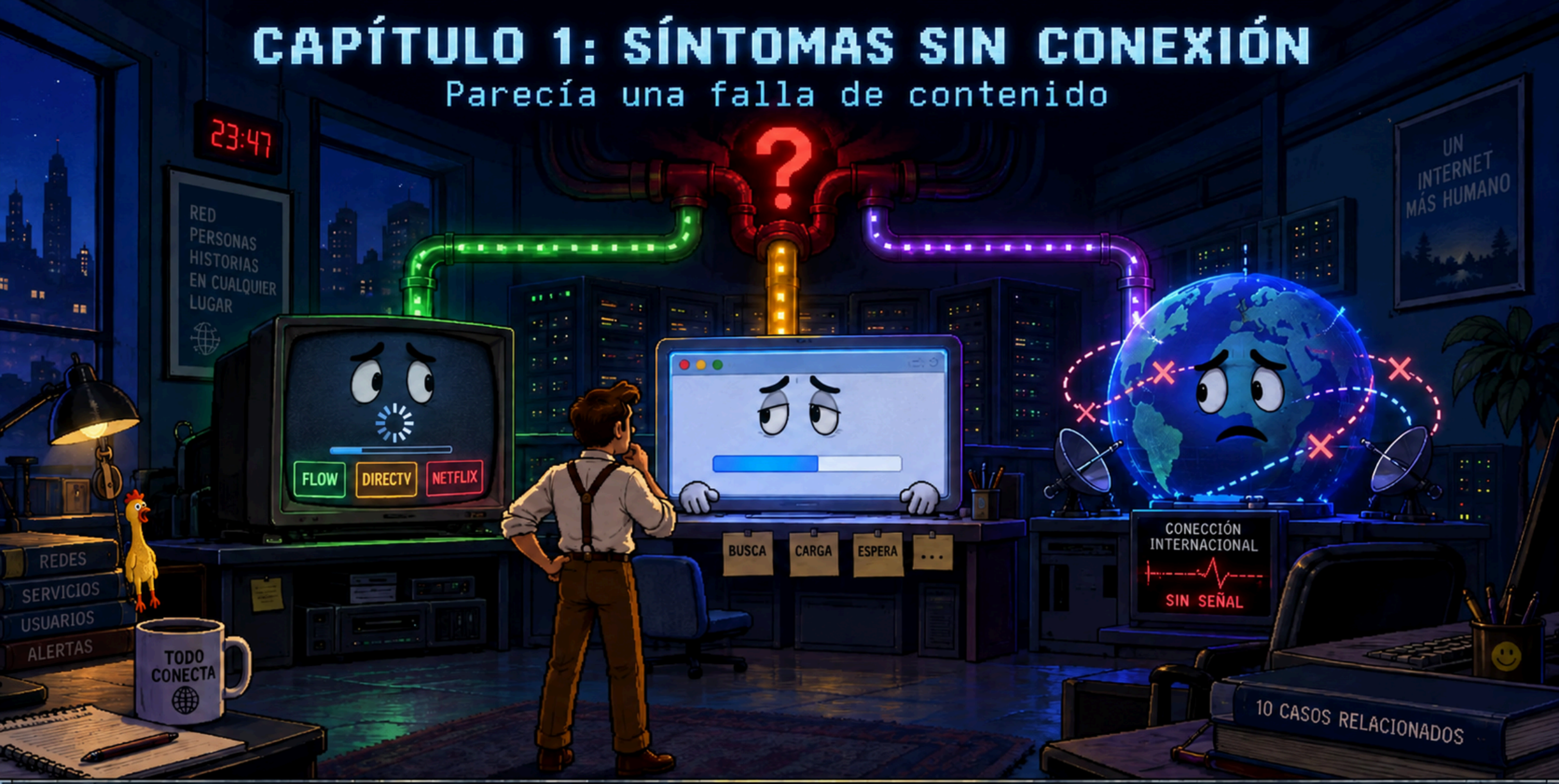
Andrés Pugawko
Gerente de Ingeniería — CABASE



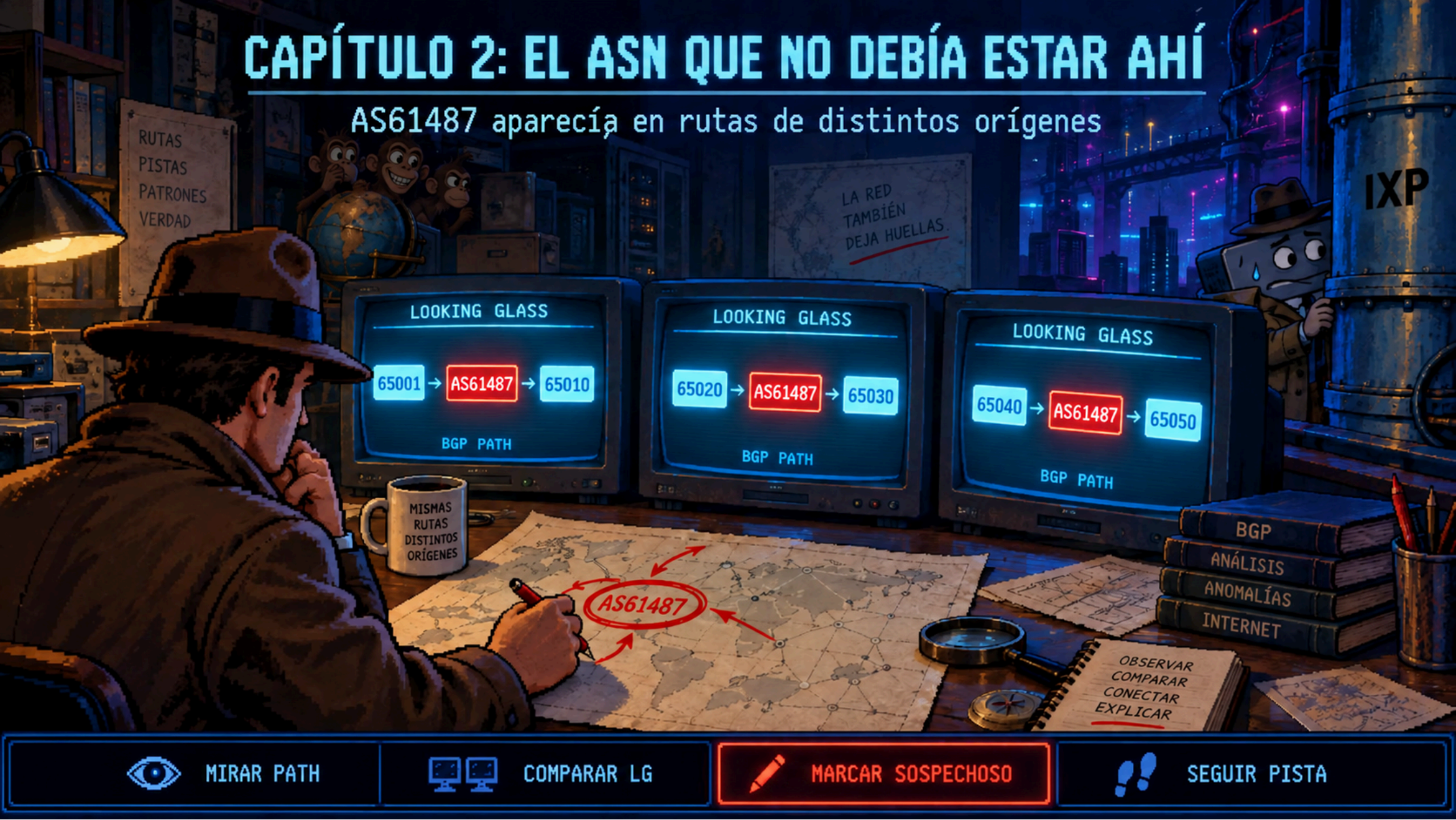
MIRAR | INVESTIGAR | SEGUIR RUTA | ESCALAR

CAPÍTULO 1: SÍNTOMAS SIN CONEXIÓN

Parecía una falla de contenido



MIRAR | COMPARAR | BUSCAR PATRÓN | DESCARTAR


CAPÍTULO 2: EL ASN QUE NO DEBÍA ESTAR AHÍ
AS61487 aparecía en rutas de distintos orígenes
RUTAS
PISTAS
PATRONES
VERDAD
LA RED
TAMBIÉN
DEJA HUELLAS.
IXP
LOOKING GLASS
65001 → AS61487 → 65010
BGP PATH
LOOKING GLASS
65020 → AS61487 → 65030
BGP PATH
LOOKING GLASS
65040 → AS61487 → 65050
BGP PATH
MISMAS
RUTAS
DISTINTOS
ORÍGENES
AS61487
BGP
ANÁLISIS
ANOMALÍAS
INTERNET
OBSERVAR
COMPARAR
CONECTAR
EXPLICAR
MIRAR PATH
COMPARAR LG
MARCAR SOSPECHOSO
SEGUIR PISTA


CAPÍTULO 3: LA PUERTA QUEDÓ ABIERTA
AS61487 exportó al tránsito rutas aprendidas en el IXP
AS7303
186.108.90.0/24
AS11014
200.63.88.0/24
AS22080
186.148.72.0/24
REDES INDEPENDIENTES — FUERA DEL IXP
IXP
AQUÍ SOLO INTERCAMBIAMOS RUTAS
MÁS PEERING UN INTERNET MEJOR
NEUTRAL ABIERTO PARA TODOS
IXP
PEERING HOY
UN INTERNET MÁS FUERTE
AS61487
186.108.90.0/24
200.63.88.0/24
186.148.72.0/24
EXPORTAR TODO
TRÁNSITO IP
186.108.90.0/24
200.63.88.0/24
186.148.72.0/24
HACIA EL RESTO DE INTERNET
UNA MALA CONFIGURACIÓN PUEDE VIAJAR MUY LEJOS
APRENDER RUTAS
REVISAR POLÍTICA
EXPORTAR TODO
DESHACER

CAPÍTULO 4: LA RUTA SE NEGÓ A DESAPARECER

El leak había cesado, pero el path seguía visible



RETIRAR RUTA | VERIFICAR LG | ESPERAR | ESCALAR

CAPÍTULO 5: TRES ORÍGENES, LA MISMA HUELLA

Los prefijos conservaban su origen legitimo



COMPARAR ORÍGENES | REVISAR AS-PATH | IDENTIFICAR PATRÓN | DESCARTAR HIJACK

CAPÍTULO 5 · PARTE 2: EL GUARDIÁN MIRABA EL ORIGEN

RPKI validó el origen, pero no la política de exportación



CAPÍTULO 6: EL LEAK SEGUÍA EN EL MAPA



CONTAR PREFIJOS | AGRUPAR ASN | MEDIR PERSISTENCIA | REVISAR EVIDENCIA

Capítulo 7: El Router Atrapado en el Tiempo



El leak terminó; la ruta seguía apareciendo


Capítulo 8: El Faro Falso
USUARIO REMOTO A
USUARIO REMOTO B
RUTA PERSISTENTE VÍA TATA /24
/24
ALGUNOS LLEGAN
OTROS NO LLEGAN
ISP: ÚNICO /24
INVENTARIO
/24
Con un único /24 no podía desviar el tráfico por prefijo más específico


Capítulo 8: Dos Cartas Náuticas
Ejemplo Hipotético
/24 gana a /22
/22
PERSISTENTE
/24
/22
OTRO
TRÁNSITO
ISP
ISLA
Caso Real: Único /24
Mismo /24: sin garantía
TATA:
/24
PERSISTENTE
USUARIO
REMOTO A
/24
USUARIO
REMOTO B
ISP
ISLA

CAPÍTULO 9: NOCs MANSION

CADA NOC VE SANA SU RED, PERO EL INCIDENTE SIGUE ABIERTO




CAPÍTULO 11: EL CASO DEL CONTACTO PERDIDO
PISTAS
REDES
PERSONAS
UN MUNDO CONECTADO
lacnic 46
lacnog 2026
19 - 22 OCTUBRE / MENDOZA, ARGENTINA
NANOG™
AR-IX
AS 52376
BÚSQUEDA DE CONTACTO
NOC DE TATA
TATA NOC
1 SALTO
2 SALTOS
3 SALTOS
CONTACTO OPERATIVO:
?
DIAL-UP
DIRECTORIO DE OPERADORES
LA COMUNIDAD AMPLIFICÓ LA BÚSQUEDA. EL CONTACTO TODAVÍA NO APARECÍA.

CAPÍTULO 12: EL CONTACTO CORRECTO



La evidencia llegó a quien podía actuar

CAPÍTULO 13: EL INVENTARIO PARA LA PRÓXIMA AVENTURA

La defensa combina políticas, validación, monitoreo y contactos




EPÍLOGO: EL CASO SIGUE ABIERTO PARA PREGUNTAS
Andrés Pugawko · CABASE
A UNA INTERNET MÁS ABIERTA
THE ROUTING TABLE
BUENAS RUTAS
MEJORES PERSONAS
SIEMPRE
MÁS HISTORIAS
EXPLORAR
ANALIZAR
ENTENDER
COMPARTIR
MISMAS PREGUNTAS MÁS INTERNET MEJOR
RPKI
¿PREGUNTAS?
in
ASN A
ASN B
ASN C
GROG
AS61487
RUTA RETIRADA
MISMOS PRINCIPIOS MÁS PERSONAS
CURIOSIDAD
COMUNIDAD
RESILIENCIA
PREGUNTAR
DEBATIR
COMPARTIR UN CASO
FIN