PWNED!

José Ignacio Rojo Rivero
Daniel Fernández Rodriguez
Equipo Español

European Cyber Security Challenge 2016

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

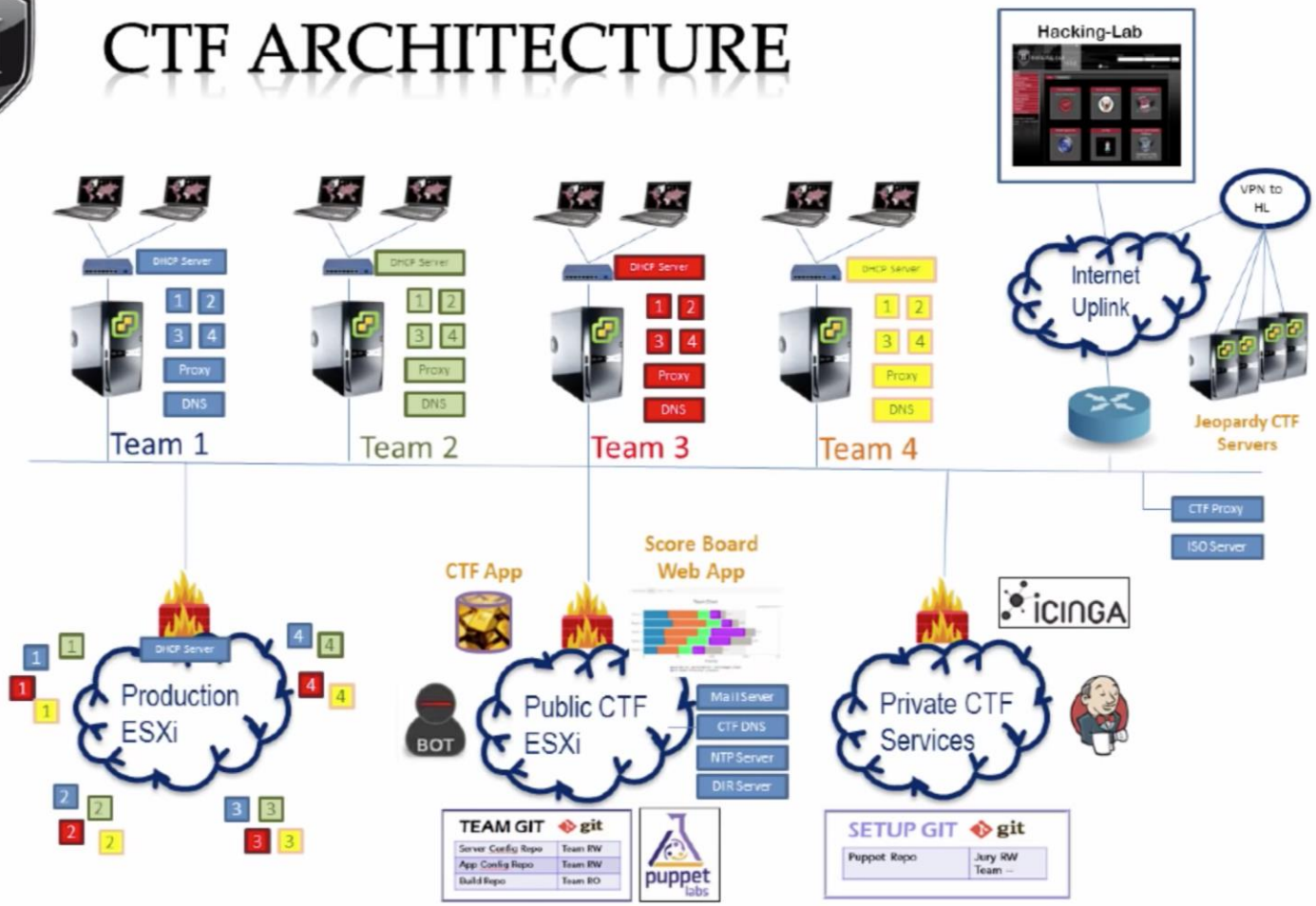
El equipo

ECSC 2016 – Categorías

- **CTF: Ataque y Defensa**
  - Disponibilidad
  - Parcheo de código
  - Ataque
  - Defensa
  - PWN
- **CTF: Jeopardy**
  - Retos variados
- **Logros**
  - Configurar una CA intermedia
  - Control de acceso en función de certificados emitidos por nuestra CA

European Cyber Security Challenge 2016

CTF ARCHITECTURE



ECSC 2016 – Jeopardy: RSA Crypto

```
1  -----BEGIN RSA PRIVATE KEY-----
2  ********************************************************************************
3  ********************************************************************************
4  ********************************************************************************
5  ********************************************************************************
6  ********************************************************************************
7  ********************************************************************************
8  ********************************************************************************
9  ********************************************************************************
10 HlNb/M95n4zO2tk0V53/hxwWZrAgoBsDNQJBALHlrJ5D1TxPy8JQHyaVP48SRWuK
11 xQBk3F5nqikVEZiGFZ/SeAgCSxKovU5pH0reRlHhZJX+Abrugr6TYKFzwpkCQEx+
12 6vU1nu4MCIxmC99fOx+ZOaGMKHhzwgkl1VQ8U2GqxuFCXcqmJ8fIolmsLRWaoZ/y
13 qNL4cCu+KoNbB9KGym0CQAt2Qs77w3Iny+JPRpsbbQSQoyP2YhbXXFBwVmdYbNrA
14 fT4RcpUCfOennMmpG77xkWB6UFOu0WBH8eX+OtaSfFY=
15 -----END RSA PRIVATE KEY-----
16
```

ECSC 2016 – Jeopardy: RSA Crypto (DER)

1e535bfccf799f8ccedad934579dff871c1666b020a01b0335 (final de q)

0241 (dp)

**00b1e5ac9e43d53c4fcbc2501f26953f8f12456b8ac50064dc5e67aa29
15119886159fd27808024b12a8bd4e691f4ade4651e16495fe01baee8
2be9360a173c299**

0240 (dq)

**4c7eeaf5359eee0c088c660bdf5f3b1f9939a18c287873c20925d5543c
5361aac6e1425dcaa627c7c8a259ac2d159aa19ff2a8d2f8702bbe2a8
35b07d286ca6d**

0240 (qi)

**0b7642cefbc37227cbe24f469b1b6d0490a323f66216d75c507056675
86cdac07d3e117295027ce7a79cc9a91bbef191607a5053aed16047f1
e5fe3ad6927c56**

ECSC 2016 – **C**hinese **R**emainder **T**heorem

- **Qué tenemos:**
  - **q**: últimos bytes del número primo
  - **dp**: exponente CRT de p => d * mod(p-1)
  - **dq**: exponente CRT de q
  - **qi**: coeficiente CRT
- **Qué necesitamos:**
  - **q**: segundo nº primo (completo)
  - **p**: primer nº primo
  - **e**: exponente público (0x10001)
  - **d**: exponente privado
  - **n**: módulo (n = (p-1)(q-1))

Fórmulas necesarias

$e * dp === 1 \pmod{(p-1)} = d \bmod (p-1)$
$e * dq === 1 \pmod{(q-1)} = d \bmod (q-1)$
$q * qi === 1 \pmod{p} = q^{-1} \bmod p$

Fórmulas finales

$(e * dp - 1) / k + 1 = p$
$(e * dq - 1) / j + 1 = q$
$(q * qi - 1) / l = p$

ECSC 2016
RSA Crypto

python script

```
def is_prime(num, public):
  if num < 2 or num%2 == 0: return False
  if num%3 == 0: return False
  print "\nchecking prime: ",num
  result = (((public/num)*num)==public)
  print "Returned ",result
  return result


def recover_parameters2(dp, dq, qinv, e, n):
    results = []
    d1p = dp * e - 1
    for k in range(3, e):
        if d1p % k == 0:
            hp = d1p // k
            p = hp + 1
            if is_prime(p, n):
                print("P: ",p)
                q = n / p
                print("q: ",q)
                if (qinv * q) % p == 1 or (qinv * p) % q == 1:
                    results.append((p, q))
                    #print(p, q, e) #debug
    return results
```

ECSC 2016 – RSA Crypto

- **Resumiendo:**

  - Necesitamos obtener los primos **p** y **q** que conforman la clave privada.

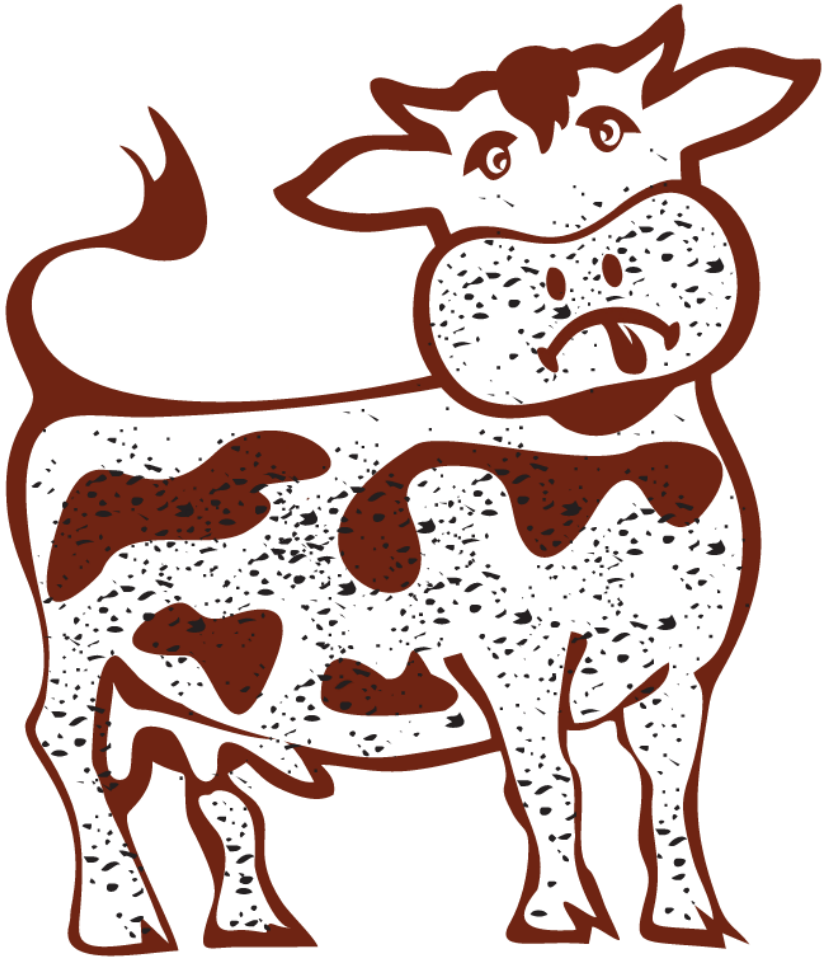
  - A partir de los números que hemos podido leer, obtenemos, mediante fórmulas matemáticas, los primos **p** y **q**.

ECSC 2016 – App vulnerable

- **Backdoor escondida en la app**
  - Información embebida en una imagen, en los LSB (bit menos significativo)
  - Se ejecutaba en el servidor el código incrustado en la imagen.
  - Por lo tanto, con una imagen prefabricada con malicia, se obtenía RCE.
- **Aún no sabemos cómo se suponía que había que arreglar esa app…**
  - No podíamos quitar el backdoor en código, ya que no teníamos acceso (legal) a esa parte del código
  - Nos auto-atacamos y neutralizamos el backdoor…
  - Por alguna razón el resto de equipos no hizo lo mismo

ECSC 2016 – RCE == PWN

- **PWN: Categoría especial con puntaje propio.**
  - Se consigue cuando se obtiene acceso **root** a una máquina de otro equipo.
- **Necesitábamos escalar privilegios…**
  - Hicimos una porra previa al evento:
    - Hay una vulnerabilidad concreta que seguro que no han arreglado…
  - Pero… seguro que lo han arreglado… no perdamos el tiempo…
  - Pero… ¿y si no lo han arreglado?



ECSC 2016 – dirtyc0w

- **Efectivamente, no lo habían arreglado -.-’**

- **Este exploit es muy inestable.**
- **Recordemos que el reglamento de la competición prohíbe expresamente el sabotaje de máquinas de otros equipos.**
- **Este exploit es MUY inestable.**

ECSC 2016 – dirtyc0w – exploit

echo '0' > /proc/sys/vm/dirty_writeback_centisecs
/bin/bash

Básicamente, lo primero que haremos al conseguir aprovecharnos del *race condition* será deshabilitar la *flag* del *kernel* para evitar que la copia temporal del archivo modificado en memoria intente sobrescribir el nuevo fichero, provocando un *kernel panic* al estar corrupta la memoria por nuestra modificación, y así estabilizar el sistema.

Los *ingleses* no lo hicieron…

ECSC 2016 – Comité de emergencia

- **El *equipo inglés* utilizó posteriormente este mismo *exploit* contra el equipo de *Liechtenstein*.**
- **Las máquinas del equipo de *Liechtenstein* quedaron anegadas.**
- **Se organizó un comité de emergencia para evaluar la situación de sabotaje, totalmente en contra de las reglas.**
- **El *equipo inglés* tuvo que jurar que no hubo mala intención y que fue accidental al utilizar dicho *exploit* sin comprenderlo en su totalidad.**
- **Como ejemplo de buena práctica, se consideró la ejecución del mismo *exploit* por parte del *equipo español* y sin daños colaterales.**

ECSC 2016 - Equipo

$$1 + 1 > 2$$

Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL